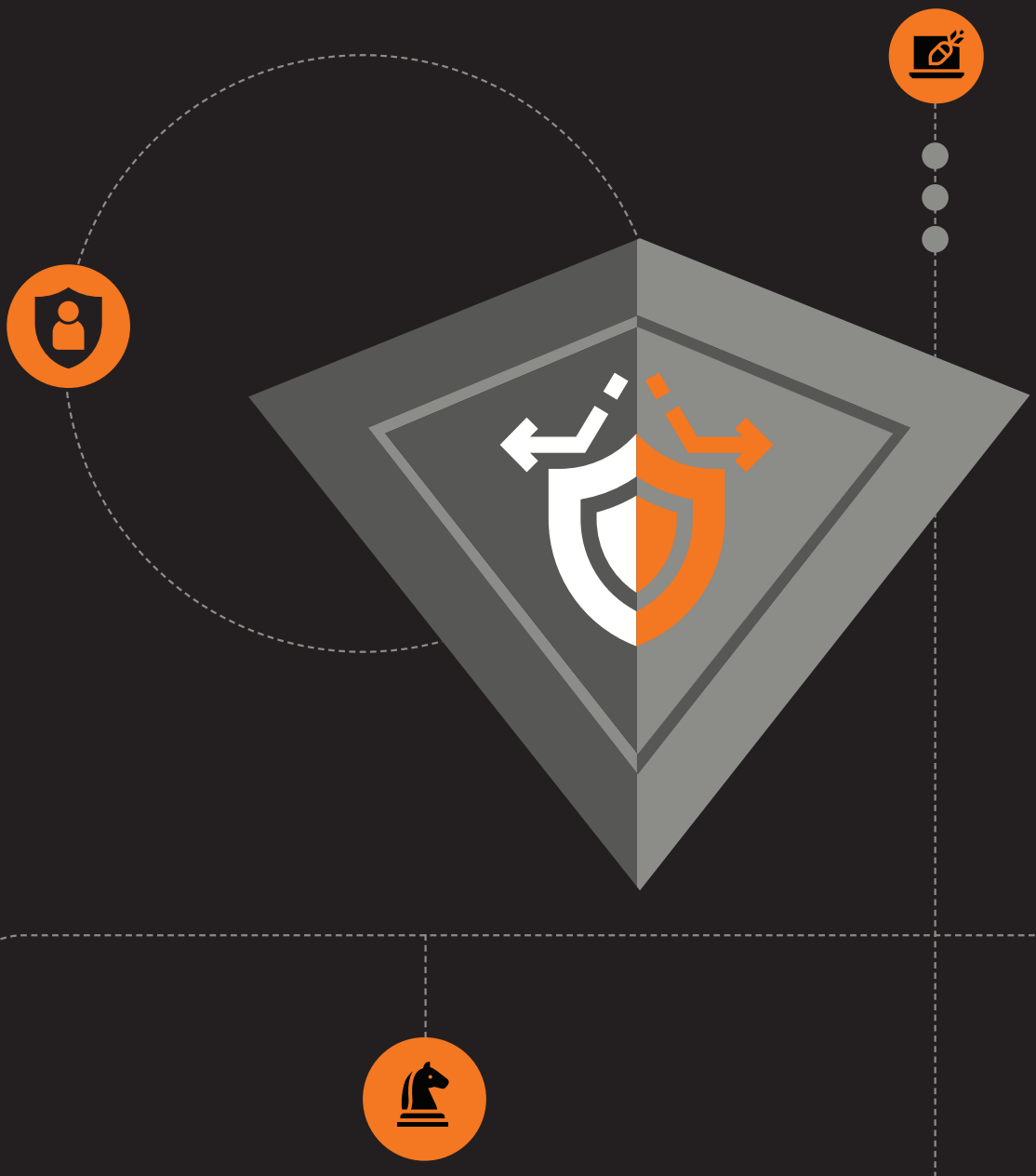
Orange Cyberdefense

Optimieren Sie Ihre Microsoft-Security

Maximieren Sie den Wert Ihrer Microsoft-Security-Technologie mit einer Strategie, die für Ihr Unternehmen geeignet ist.



Einleitung

Microsoft ist ein globales Technologieunternehmen und in vielen Bereichen der Cybersicherheit führend. Die Möglichkeit, seine Sicherheitstechnologie im Rahmen von Unternehmensvereinbarungen zu erwerben, verleitet Unternehmen dazu, so viel Microsoft-Sicherheitstechnologie wie möglich einzusetzen.

Bei einer soliden Sicherheitsstrategie geht es jedoch nicht nur um die Technologie. Sie müssen auch auf die Strategie, den Fachkräftemangel sowie die Prozesse und Abläufe achten, die es Ihnen ermöglichen, den maximalen Nutzen aus den von Ihnen gewählten Lösungen zu ziehen.

Hier bieten wir einen fundierten, unabhängigen Standpunkt zu diesen Fragen und einen Leitfaden für Sicherheitsverantwortliche in Bezug auf Microsoft Security, damit Sie einen Ansatz wählen können, der sowohl effektiv als auch kosteneffizient ist.

Orange Cyberdefense, 2023

Die Vor- und Nachteile eines Microsoft Enterprise Agreements, das Sicherheitstechnologie umfasst.

Ein Microsoft Enterprise Agreement richtet sich in erster Linie an große kommerzielle Organisationen mit 500 oder mehr Benutzern/Geräten oder Regierungsorganisationen mit 250 oder mehr Nutzern/Geräten, die Software und Cloud über einen Zeitraum von mindestens 3 Jahren lizenzieren möchten. Diese Verträge geben Organisationen die Möglichkeit, Produkte und Dienste im Laufe der Zeit hinzuzufügen und anzupassen und die Änderungen durch einen jährlichen “True-up”-Prozess abzustimmen. Unternehmensverträge beinhalten eine Abonnementoption, die die anfänglichen Lizenzkosten senkt und es ermöglicht die Anzahl der Abonnements auf jährlicher Basis zu erhöhen oder zu verringern.

Es gibt drei Gründe, warum ein Microsoft Enterprise Agreement für Unternehmen attraktiv ist:

- Die Möglichkeit den Wert der Investitionen in Microsoft-Technologie zu maximieren, indem sie die besten Preise erhalten.
- Die Flexibilität, neue Technologien zu übernehmen, wenn sie auftauchen und deren Umfang je nach Bedarf anzupassen.
- Die Möglichkeit, das Lizenzmanagement zu rationalisieren und die Anzahl der Anbieter zu konsolidieren.

Die Palette der Microsoft-Unternehmenslizenzen reicht von E1 bis E5 (E steht für Enterprise), wobei E5 Microsoft-Sicherheitstechnologien und erweiterte Funktionen für Compliance und Analysen umfasst und die Lizenzmodelle F1 bis F5 für Organisationen gedacht sind, die Mitarbeiter an vorderster Front beschäftigen.

Die Server- und Cloud-Registrierung ist eine Option im Rahmen des Microsoft Enterprise Agreement, mit der sich Unternehmen für eine oder mehrere wichtige Server- und Cloud-Technologien von Microsoft, einschließlich damit verbundener Sicherheitsprodukte, entscheiden können. Produkte wie Defender for Cloud, Microsoft Sentinel und Netzwerksicherheit wie Azure Firewall sind verbrauchsabhängig.

So maximieren Sie den Wert Ihres Microsoft Enterprise Agreements

Trotz der offensichtlichen Vorteile von Enterprise Agreements, gibt es einige potenzielle Fallstricke, wenn Sie sich bei der Beschaffung Ihrer Sicherheitstechnologie ausschließlich auf Enterprise Agreements verlassen.

Ein Risiko besteht darin, dass das Enterprise Agreement Produkte enthält, von denen Ihr Unternehmen zwar profitieren könnte, für die es aber nicht die nötigen Fähigkeiten oder den nötigen Reifegrad besitzt.

Ein weiteres Risiko besteht darin, dass Ihr Unternehmen Technologien anschafft, ohne über eine klare Sicherheitsstrategie und die richtigen Prozesse zu verfügen. Bevor Sie mit der Implementierung von Sicherheitsprodukten beginnen, benötigen Sie zunächst eine klare Sicherheitsstrategie, die den Anforderungen Ihres Unternehmens entspricht.

> **Und schließlich müssen Sie, um den Wert Ihres Enterprise Agreements zu maximieren, die Technologie durch Services ergänzen, wie z. B. Security Consulting, Sicherheitsstrategie, Vulnerability Assessments, Penetrationtests/Ethical Hacking, Managed Detection and Response Services oder Security Operations Services.**

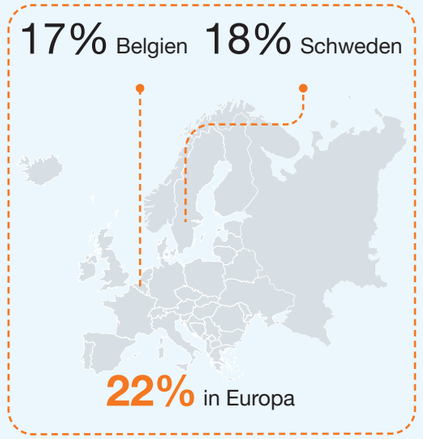
Orange Cyberdefense, 2023

Fachkräftemangel in der Sicherheitstechnologie

Im Jahr 2022 fehlten weltweit 3,4 Millionen Arbeitskräfte im Bereich der Cybersecurity.[1] In der EMEA-Region betrug das Defizit 317.000, eine Zahl, die im Vergleich zum Vorjahr um 59 % gestiegen war. 74 % der Cybersecurity-Teams mit Personalmangel glauben, dass der Fachkräftemangel ihr Unternehmen einem moderaten bis extremen Angriffsrisiko aussetzt.

Microsoft hat in einer eigenen Studie[2] festgestellt, dass die Nachfrage nach Cybersicherheitskompetenzen von 2021 auf 2022 europaweit um 22 %, in Belgien um 17 % und in Schweden um 18 % gestiegen ist. Die europäischen Bemühungen um die Vermittlung von Cyberkompetenzen haben mit der steigenden Nachfrage nach Cybersecurity-Fachkräften nicht Schritt gehalten, was zeigt, dass sowohl öffentliche als auch private Organisationen dringend etwas unternehmen müssen, um die Lücke zu schließen.

Bedarf an Cybersicherheits-kompetenzen
(2022 gegenüber dem Vorjahr)



Angesichts der zunehmenden Häufigkeit und Komplexität von Cyber-Bedrohungen, des sich beschleunigenden Wandels Europas hin zu einer digital ausgerichteten Wirtschaft und der steigenden Anforderungen an die Cybersicherheit in der europäischen Gesetzgebung war der Bedarf an qualifiziertem Sicherheitspersonal noch nie so hoch wie heute. Microsoft bietet Kunden, Partnern und Dienstanbietern viele gute Schulungen an, um Sicherheitsexperten für ihre Sicherheitstechnologie zu schulen.

Microsoft investiert in eine Initiative in Europa und arbeitet eng mit lokalen Bildungseinrichtungen, gemeinnützigen Organisationen, Regierungen und Unternehmen zusammen, um ein Programm für Cybersicherheitskompetenzen zu entwickeln, das den besonderen Anforderungen des Marktes entspricht. Hierbei ist Diversität ein Bereich, der weiter vorangetrieben werden muss, und es werden besondere Anstrengungen unternommen, um den niedrigen Frauenanteil im Bereich der Cybersicherheit zu überwinden.

> In dieser Situation ist die Verwendung von Microsoft-Sicherheitsprodukten ein Vorteil gegenüber einem Ansatz mit mehreren Anbietern, bei dem Sie für die Technologien der einzelnen Anbieter separate Kenntnisse benötigen. Die Microsoft-Plattform hat den Vorteil einer einheitlichen Verwaltungsschnittstelle, die es einfacher macht, mehrere Microsoft-Lösungen mit weniger Ressourcen zu verwalten.

Es geht nicht mehr nur um On-Prem, sondern um Multi-Cloud

Heutzutage nutzen Unternehmen nicht nur On-Premise- und SaaS-Dienste, sondern viele verwenden mehrere Cloud-Anbieter, SaaS-Plattformen und On-Premise-Rechenzentren gleichzeitig. Diese komplexen Umgebungen sind aufwendiger zu sichern. Sie müssen wissen, wie Sie jedes einzelne Element absichern können. Daher müssen Sie sich in der Absicherung aller Cloud-, SaaS- und On-Premise-Lösungen Ihrer Anbieter schulen lassen – ein längerer Entwicklungsweg als bei einer Schulung in allgemeiner Sicherheitstechnologie.

> Der Vorteil ist jedoch, dass eine Ausbildung in der zugrundeliegenden Technologie und der sie überlagernden Sicherheit Sie zu einem vielseitigeren Sicherheitsexperten macht – und weil Sie die zugrundeliegende Technologie verstehen, können Sie sie effektiver schützen.

Orange Cyberdefense, 2023

Strategien zur Überwindung des Fachkräftemangels

Im Großen und Ganzen gibt es vier Möglichkeiten, mit Fachkräftemangel umzugehen: Einstellung neuer Mitarbeiter, Schulung vorhandener Mitarbeiter, Einsatz von Auftragnehmern und Outsourcing.

1. Einstellung von neuen Mitarbeitern ist schwierig aufgrund des Mangels an qualifizierten Fachkräften, des Wettbewerbs um ihre Fähigkeiten und der hohen Gehälter, die sie verlangen.

2. Schulung vorhandener Mitarbeiter ist eine effektive und günstige Möglichkeit. Solange Fachkräftemangel besteht, droht jedoch auch das Risiko, dass sie abgeworben werden.

3. Auftragnehmer und Freelancer können eine gute Lösung darstellen. Personen mit gefragten Qualifikationen neigen dazu, selbstständig zu arbeiten, weil sie so mehr verdienen können. Das macht sie entsprechend teurer als ähnlich qualifizierte Arbeitnehmer – und sie können schnell zum nächsten Projekt wechseln.

4. Outsourcing ist eine echte Option. Wenn die Nachfrage nach Qualifikationen das Angebot übersteigt, wird der Qualifikationsmangel durch Outsourcing zum Problem eines anderen. Es ist ein schnellerer Weg zur Wertschöpfung aus Ihren Microsoft Security-Produkten als Einstellung oder Schulung von Mitarbeitern.

> Outsourcing kann der schnellste und kostengünstigste Weg sein, um Zugang zu Microsoft-Sicherheitskompetenzen und den allgemein benötigten Sicherheitskompetenzen zu erhalten – wenn Sie den richtigen Anbieter wählen. Sie müssen sich von der Glaubwürdigkeit des Managed Service Providers überzeugen. Ist er tatsächlich ein Sicherheitsexperte oder nur ein Microsoft-Experte? Das ist ein großer Unterschied.

Das Unternehmen mag vielleicht seit 20 Jahren Microsoft-Partner sein, das sagt aber nichts über die Verfügbarkeit der erforderlichen Sicherheitskompetenzen und -fähigkeiten aus. Die Erfahrung mit der Installation von Sicherheitssoftware auf den Laptops der Mitarbeiter ist weit davon entfernt, einen ausgeklügelten Angriff in Ihrer Hybrid-Cloud-Umgebung zu verfolgen und in Echtzeit zu entschärfen.

Die Akkreditierung in der Microsoft-Sicherheitstechnologie ist ein kluger Karriereweg für einen aufstrebenden Sicherheitsexperten. Es ist ein schneller Weg, um ein geschätztes Mitglied der Cybersecurity-Branche zu werden. Allerdings sollten die Microsoft-Kenntnisse durch allgemeinere Sicherheitskenntnisse, die von Organisationen wie dem SANS Institute vermittelt werden, ergänzt werden, um zu einem vollwertigen Sicherheitsexperten zu werden.

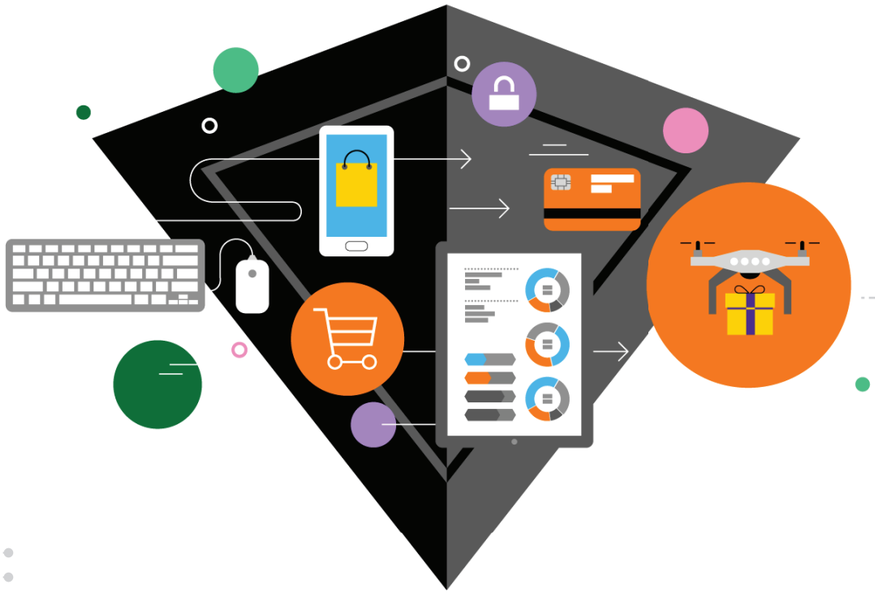
> Welchen Weg Sie auch immer wählen, um den Fachkräftemangel zu überwinden, denken Sie daran, dass Sie nicht nur eine bestimmte Anzahl zertifizierter Fachkräfte benötigen. Sie brauchen auch die Organisation und die Prozesse, um konsistente Sicherheitsergebnisse zu erzielen, z. B. die Reduzierung der Angriffsfläche oder die Analyse von sicherheitsrelevanten Ereignisdaten, um Angriffe zu erkennen und darauf zu reagieren.

Orange Cyberdefense, 2023

Die Bedeutung eines strategischen Ansatzes für die Sicherheit

Im Allgemeinen haben die meisten Unternehmen eine Sicherheitsstrategie, aber der Reifegrad dieser Strategie und ihre Umsetzung liegen meist weit auseinander. Unvermeidlich gibt es auch viele reaktive, taktische Aktivitäten als Reaktion auf bestimmte Bedrohungen. Wenn Sie von einem Ransomware-Angriff betroffen sind, können Sie ihn nicht einfach ignorieren und an Ihrer Strategie festhalten – Sie müssen reagieren.

Unternehmen, die im Bereich der Sicherheit überwiegend reaktiv vorgegangen sind, haben sich eine Vielzahl von Tools zugelegt.[3] Ein durchschnittliches Unternehmen verwendet heute 76 Sicherheits-Tools. Oft arbeiten diese Tools nicht zusammen, was die Sicherheitsabläufe unnötig komplex und ineffizient macht.



Strategie ist mehr als Technologie

Aber es ist nicht nur eine Frage der Technologie. Unternehmen ohne eine angemessene Sicherheitsstrategie haben inkonsistente Prozesse. Sie beherrschen einige Dinge sehr gut, andere dafür aber überhaupt nicht. Wichtige Prozesse, wie z. B. Incident Response, können undokumentiert und ungetestet sein, so dass sie im Falle eines Zwischenfalls nicht darauf vorbereitet sind.

Aus der Sicht der Mitarbeiter kann ein unzureichender strategischer Ansatz zu unklaren Rollen innerhalb der Sicherheits- und IT-Abteilungen führen. Die Rollen können veraltet sein und nicht mehr mit den technologischen Entwicklungen mithalten. Die Sicherheit ist möglicherweise kein förmlicher Bestandteil der Aufgabenbeschreibung einer Person, und wenn diese Person ausscheidet, könnte eine Neueinstellung entsprechend ihrer Stellenbeschreibung eine Kompetenzlücke hinterlassen.

Wenn Unternehmen kein strategisches Sicherheitskonzept verfolgen, führt das häufig dazu, dass sie Opfer eines Ransomware-Angriffs werden, der sie für Tage oder sogar Wochen betriebsunfähig macht. Dies führt zu Umsatzeinbußen, schadet dem Ruf des Unternehmens und verursacht enorme Wiederherstellungskosten – nicht nur die Kosten für die Wiederherstellung von Daten, sondern auch für den Wiederaufbau von Netzwerken und die Implementierung von Maßnahmen, die sicherstellen, dass sich so etwas nicht wiederholt. Ganz zu schweigen von den Kosten des Lösegelds selbst.

> Die durchschnittlichen Kosten eines Ransomware-Angriffs (ohne die Kosten für das Lösegeld) beliefen sich im Jahr 2022 auf 4,5 Millionen Dollar[4] – eine Zahl, die die Kosten eines strategischen Sicherheitsansatzes bei weitem übersteigt. Natürlich ist die Entwicklung einer robusten Sicherheitsstrategie mit Kosten verbunden, aber diese sind auf lange Sicht weitaus geringer als die Kosten für die Wiederherstellung nach einem größeren Vorfall.
>
> **Orange Cyberdefense, 2023**

Wie sieht ein strategischer Ansatz aus?

Eine gute Sicherheitsstrategie ist eigentlich eine Übung im Risikomanagement und umfasst Menschen, Prozesse und Technologien. Der erste Schritt besteht darin, sich einen Überblick über Ihre Risiken zu verschaffen; dann können Sie eine strategische Entscheidung darüber treffen, wie viel Risiko Sie zu akzeptieren bereit sind. Wir würden gerne alle Risiken für Unternehmen ausschalten, aber realistischerweise hat niemand das Budget, die Mitarbeiter, die Prozesse oder die Zeit, um das Risiko auf Null zu reduzieren.

Ein großer Teil einer wirksamen Sicherheitsstrategie hat nichts mit Technologie zu tun.
Die Technologie ist nur ein Hilfsmittel. Sie müssen über Ihre Risikobereitschaft entscheiden, Ihre Richtlinien festlegen und die Governance für deren Durchsetzung einrichten. Sie brauchen Menschen mit Fähigkeiten und Erfahrung, dokumentierte und getestete Prozesse und die organisatorischen Fähigkeiten, zum Betrieb der vorhandenen Technologie.

Automatisierung ist nützlich – wenn man sie strategisch einsetzt

Auf dem Markt wird derzeit viel über Automatisierung und KI im Sicherheitsbereich geredet, und sie spielen sicherlich eine wichtige Rolle bei der Steigerung der Effizienz. Aber sie sind kein Ersatz für eine Strategie.

Wenn ein stückweiser Ansatz für die Sicherheit eine kritische Lücke in Ihren Prozessen hinterlassen hat, kann keine noch so große KI-gestützte Automatisierung diese Lücke schließen.

Die Ausarbeitung einer wirksamen Cybersicherheitsstrategie ist ein Gleichgewicht zwischen Komplexität und Zeit. Je größer die Organisation ist, desto komplexer ist sie wahrscheinlich, desto breiter ist ihr digitaler Fußabdruck und desto größer sind auch die Risiken. Mit Zeit wäre es für eine solche Organisation möglich, selbst eine wirksame Sicherheitsstrategie zu entwickeln. Aber wer hat schon die Zeit, wenn die fortschrittlichen, anhaltenden Bedrohungen täglich raffinierter werden?

Die meisten Chief Information Security Officers sind keine technischen Experten in allen Bereichen; ihr Schwerpunkt liegt auf der Befähigung von Teams und deren Aufsicht. Selbst die Besten in den größten Unternehmen brauchen in der Regel etwas Hilfe bei der Ausarbeitung und Umsetzung ihrer Sicherheitsstrategie, da diese sehr komplex ist und die Zeit gegen sie läuft.

Der Unterschied zwischen einem Unternehmen, das eine solide Sicherheitsstrategie verfolgt, und einem, das dies nicht tut, lässt sich daran erkennen, wie gut es mit einer großen öffentlich gemachten Sicherheitsverletzung umgeht. Unternehmen, die nicht in die Sicherheit investiert haben (um keine Namen zu nennen), kommunizieren nicht offen mit ihren Kunden und fügen ihrer Marke schweren Schaden zu. Diejenigen, die dies tun, wissen, was sie sagen sollten und was nicht, erhalten das Vertrauen ihrer Kunden und erleiden insgesamt weniger Schaden, selbst wenn das Ausmaß der Sicherheitsverletzung größer ist.

Fazit

Zusammenfassend lässt sich sagen, dass Sie sich nicht nur auf einen Anbieter verlassen können, wenn Sie sich eine effektive Sicherheitsstrategie wünschen:

- Vergewissern Sie sich vor der Beschaffung einer Technologie, dass Sie eine klare Sicherheitsstrategie haben.
- Möglicherweise können Sie einen Großteil der von Ihnen benötigten Technologie über Ihr Enterprise Agreement beziehen.
- Wahrscheinlich werden Sie auch einige Technologien von anderen Anbietern beziehen müssen – versuchen Sie jedoch, die Anzahl der Anbieter gering zu halten.
- Und nicht alles, was eine solide Sicherheitsstrategie ausmacht, ist Technologie – Richtlinien, Menschen und Prozesse sind ebenfalls wichtig.

Im Allgemeinen ist es für ein Unternehmen am besten, einen erfahrenen, unabhängigen Security Services Provider einzuschalten, um das Beste aus den Sicherheitstechnologien herauszuholen, die es mit seinem Microsoft Enterprise Agreement erhält.

So können sie vermeiden, dass es zu Überschneidungen, Lücken oder einer suboptimalen Nutzung der Technologie kommt. Es wird ihnen helfen, mit dem Mangel an Fähigkeiten im Bereich der Cybersicherheit im Allgemeinen umzugehen. Und es wird ihnen eine umfassende, robuste Sicherheitsstrategie an die Hand geben – und die Fähigkeit, diese umzusetzen.

Wir können Kunden dabei helfen, die Anzahl der Anbieter zu reduzieren, Sicherheitslücken zu minimieren und Ihr Unternehmen rund um die Uhr zu schützen.

Um mehr darüber zu erfahren, wie Orange Cyberdefense bei Ihrer Microsoft-Sicherheit helfen kann, besuchen Sie Security für Microsoft oder kontaktieren Sie einen Microsoft-Spezialisten über info@de.orangecyberdefense.com.

1. (ISC)² Cybersecurity Workforce Study 2022
2. The urgency of tackling Europe's cybersecurity skills shortage, März, 2022
3. Panaseer 2022 Security Leaders Peer Report
4. Cost of a data breach report, IBM, 2022

orange™