VECTRA
SECURITY THAT THINKS

FORSCHUNGSSTUDIE

Die Sicherheit von Microsoft 365 im öffentlichen Raum unter die Lupe genommen:

Die Lücke zwischen Angreifern und Verteidigern schließen

VECTRA
SECURITY THAT THINKS

Inhaltsverzeichnis

Vorwort

Microsoft 365 dominiert heute die Produktivitätslandschaft in Unternehmen, bei Regierungen, in Gesundheits- und Bildungseinrichtungen. Als Anfang 2020 die Covid-19-Pandemie ausbrach, konnten Unternehmen, die weltweit kritische öffentliche Dienstleistungen bereitstellen, schnell auf die Arbeit im Homeoffice und die Bereitstellung der Dienstleistungen aus der Ferne umstellen, da Microsoft 365 agile und flexible Arbeitspraktiken unterstützt. Es gab die Möglichkeit, dass Regierungsmitarbeiter von Zuhause aus arbeiten, Ärzte ihren Patienten Video-Sprechstunden anbieten und Lehrer online unterrichten. Dies macht deutlich, dass die Nutzung von Microsoft 365 weiter verbreitet ist als jemals zuvor.

Mit zunehmender Nutzung der Public Cloud in Unternehmen, die kritische öffentliche Dienstleistungen bereitstellen, vergrößerte sich auch die Angriffsfläche, die von Hackern ausgenutzt werden kann. Regierungen, Gesundheits- und Bildungseinrichtungen müssen sich jetzt sicher sein, dass sie in der Lage sind, die Microsoft 365-Umgebungen vor Kriminellen zu schützen, die wertvolle Daten bei schwerwiegenden Cyberangriffen abschöpfen wollen.

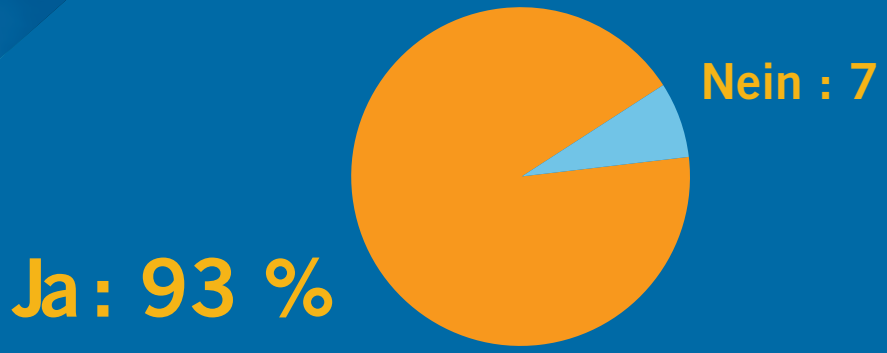
In diesem eBook finden Sie neue Erkenntnisse über die Microsoft 365-Landschaft. Wir haben eine weltweite Umfrage bei mehr als 1.100 Entscheidungsträgern im Bereich der IT-Sicherheit durchgeführt, und dieses eBook konzentriert sich auf die Antworten von den 302 Fachleuten, die für Regierungs-, Gesundheits- und Bildungsorganisationen und -einrichtungen auf der ganzen Welt arbeiten. Wir haben nicht nur ihre Ansichten zu den größten Bedrohungen in ihren Microsoft 365-Umgebungen zusammengetragen, sondern auch danach gefragt, wie gut sie ihrer Meinung nach davor geschützt sind.

Zudem werden wir praktische Maßnahmen vorstellen, mit denen Sie die Sicherheit der Microsoft 365-Infrastruktur und von Azure Active Directory verbessern können. Dazu gehört auch, wie Sie Angriffe im Hinblick auf Kontoübernahmen erkennen und unverzüglich stoppen können.

VECTRA
SECURITY THAT THINKS

Cloudnutzung im öffentlichen Dienst steigt während der Pandemie rasant

Da sich Cloud-Funktionen in der Pandemie schnell von einem strategischen Vorteil zu einer geschäftlichen Notwendigkeit entwickelt haben, wurde die Nutzung von Microsoft 365 im öffentlichen Dienst rasant ausgeweitet. Tatsächlich wurde im vergangenen Jahr die Strategie zur Umstellung auf die Cloud bei öffentlichen Dienstleistungen um mehrere Jahre beschleunigt.



93 Prozent der befragten Entscheidungsträger für IT-Sicherheit haben infolge der Pandemie die Nutzung von Microsoft Office 365 verstärkt.

VECTRA
SECURITY THAT THINKS

Da die Arbeit im Homeoffice zur neuen Normalität wurde, verwundert es nicht wirklich, dass die Unternehmen fast ausnahmslos die Nutzung von Microsoft 365 ausgeweitet haben. Dies konnte in der gesamten Unternehmenslandschaft beobachtet werden: Microsoft meldete im März 2020 ganze 258 Millionen aktive Nutzer von Microsoft Teams. Dies entspricht einem Zuwachs von mehr als 70 Millionen im Vergleich zum Vorjahr.

„Durch die Lösung von Vectra wurde die Zeit, die wir brauchen, um auf einen Angriff zu reagieren, verkürzt. Früher war es schwierig zu erkennen, ob etwas vor sich ging, weil wir keinen Überblick hatten. Jetzt geht das bei uns sehr schnell, da wir einen Überblick darüber haben, was vor sich geht."

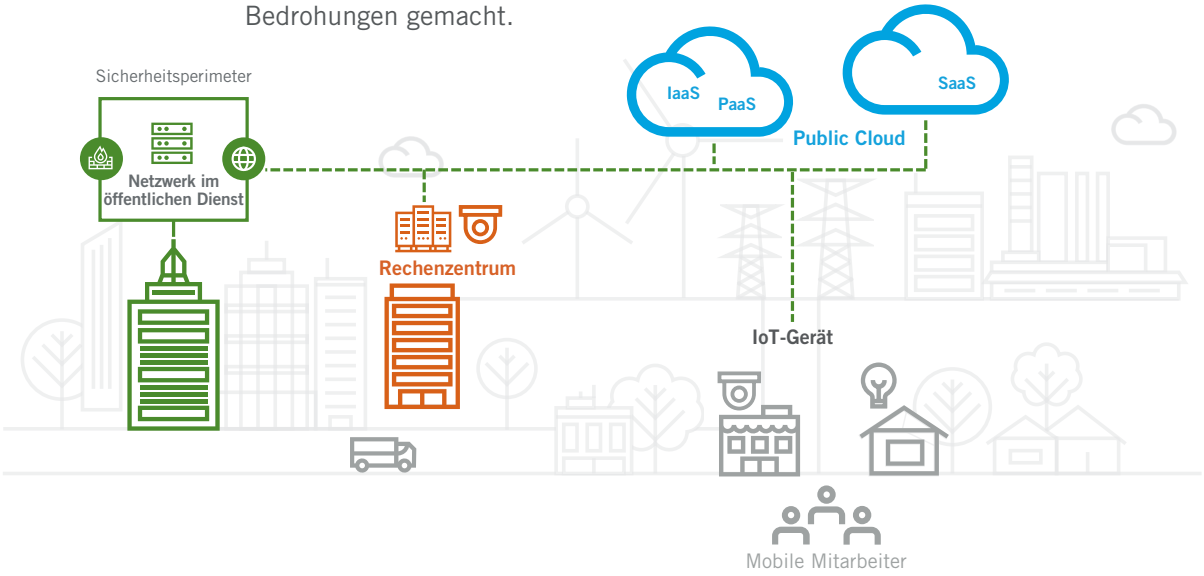
Projektmanager einer Universität

Diese erzwungene Verlagerung hat die IT-Landschaft nachhaltig verändert. Als wir IT-Sicherheitsexperten in Regierungs-, Gesundheits- und Bildungsorganisationen nach den Auswirkungen der Pandemie auf ihre Arbeit gefragt haben, berichteten mehr als 80 Prozent von ihnen, dass sie ihre Strategie zur Umstellung auf die Cloud und zur digitalen Transformation infolgedessen beschleunigt haben. Erstaunlicherweise gab ein Fünftel von ihnen an, dass eine Beschleunigung um mehr als zwei Jahre erfolgt ist. Bei Mitarbeitern in Regierungsorganisationen sagten dies sogar 25 Prozent der Befragten.

Die Veränderung der IT-Landschaft und die erzwungene Beschleunigung der Cloud-Migration hat diese Unternehmen auch anfälliger für Cyber-Bedrohungen gemacht.

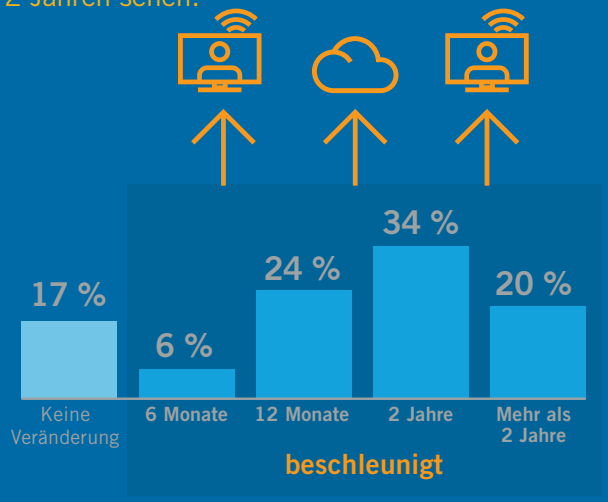
Und obwohl es in den letzten zwölf Monaten für viele eine Art Feuerprobe war, scheint diese Beschleunigung greifbare Vorteile gebracht zu haben. Knapp über 40 Prozent der Befragten berichteten von mehr Zufriedenheit am Arbeitsplatz, und ein ähnlich hoher Anteil hat höhere Produktivität angeführt.

Allerdings ist auch klar, dass die Belastungen durch die Pandemie auch zu einem deutlichen Anstieg des Stressniveaus geführt haben. Etwas weniger als die Hälfte der Entscheidungsträger im Bereich der IT-Sicherheit in den von uns befragten Einrichtungen des öffentlichen Dienstes gab an, dass der Stress während des Lockdowns zugenommen hat. Abgesehen von den Auswirkungen auf die Mitarbeiter hat die Veränderung der IT-Landschaft und die erzwungene Beschleunigung der Cloud-Migration die meisten dieser Organisationen auch anfälliger für Cyber-Bedrohungen gemacht.



83 %

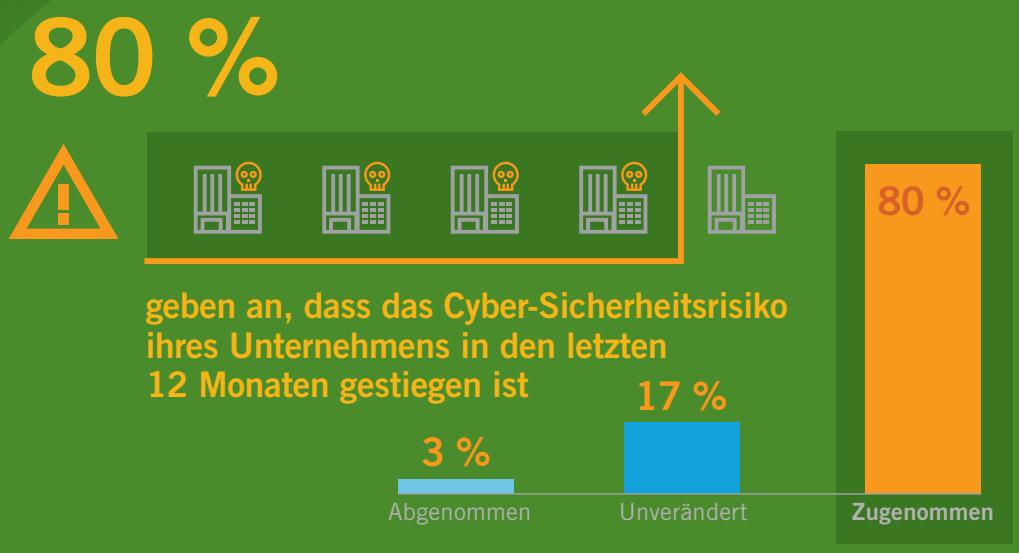
haben festgestellt, dass sich die Umstellung ihres Unternehmens auf die Cloud und die digitale Transformation **während der Pandemie beschleunigt** hat, wobei 20 % eine Beschleunigung von mehr als 2 Jahren sehen.



VECTRA
SECURITY THAT THINKS

Die sich rasch verändernde Bedrohungslandschaft

Die vermehrte Arbeit im Homeoffice und die zunehmende Nutzung von Microsoft 365 und Azure AD haben unweigerlich zu einer größeren Angriffsfläche geführt. Viele Sicherheitsexperten standen mit dem Rücken zur Wand und hatten damit zu kämpfen, diese veränderte Umgebung zu verstehen und zu schützen. Die etablierten Sicherheitstools und -richtlinien vor Ort waren oftmals unzureichend, um Nutzer effektiv zu überwachen und zu schützen. Angreifer fackelten natürlich nicht lange und nutzten diese sich verändernde Landschaft aus und verstärkten ihre Angriffe – im April 2020 meldete Google, dass weltweit täglich mehr als 18 Millionen COVID thematisierende Phishing- und Malware-E-Mails blockiert wurden.



Auch wenn der Anteil der COVID-Phishing-Angriffe seither zurückgegangen sein mag: die Sicherheitslücken im Zusammenhang mit den zunehmenden Cloud-Implementierungen bleiben weiter bestehen. Die Mehrheit der Entscheidungsträger im Sicherheitsbereich von Regierungs-, Gesundheits- und Bildungsorganisationen ist der Überzeugung, dass die Risiken im Laufe der letzten 12 Monate zugenommen haben.

Drei Fünftel der Entscheidungsträger im Sicherheitsbereich glauben, dass sich die Kluft hinsichtlich der Fähigkeiten von Angreifern und Verteidigern vergrößert.

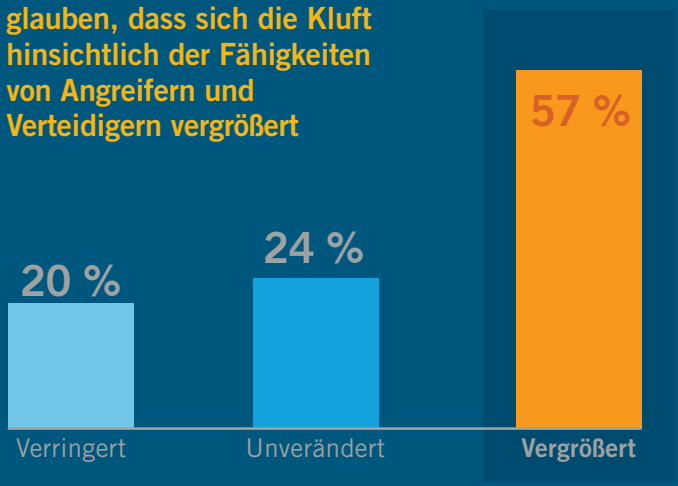
Angreifer werden immer cleverer und wenden ihre Erfahrung hinsichtlich der Navigation und Nutzung dieses neuen Terrains an. Wir konnten eine Verlagerung von traditionellen Malware-basierten Angriffen hin zu solchen feststellen, die sich auf Konten, Anmeldeinformationen, Berechtigungen und Rollen konzentrieren – ein Bereich, den herkömmliche Sicherheitstools nicht erkennen können.

Angesichts der Tatsache, dass Hacker sowohl den Umfang als auch die Raffinesse ihrer Angriffe weiter erhöhen, blicken viele der Entscheidungsträger für IT-Sicherheit im öffentlichen Dienst ziemlich pessimistisch in die Zukunft – fast drei von fünf glauben, dass sich die Kluft zwischen den Fähigkeiten der Angreifer und Verteidiger vergrößert.

Die Mehrheit der Entscheidungsträger im Sicherheitsbereich von Regierungs-, Gesundheits- und Bildungsorganisationen ist der Überzeugung, dass die Risiken im Laufe der letzten 12 Monate zugenommen haben.

57 %

glauben, dass sich die Kluft hinsichtlich der Fähigkeiten von Angreifern und Verteidigern vergrößert



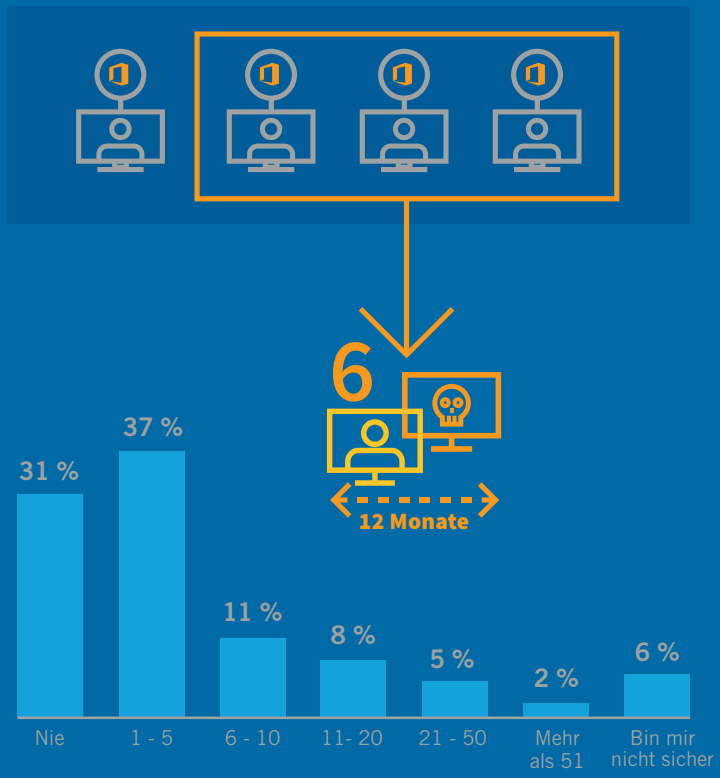
In der Tat bedeuten Tools, beispielsweise für Bedrohungserkennung und Response (z. B. NDR) und KI-gestützte Analysen, dass das Gegenteil der Fall ist. Sobald Angreifer in eine Umgebung eingedrungen sind, verlassen sie sich traditionell auf ihre Fähigkeit, sich im Trubel des normalen Geschäftsbetriebs zu verstecken. Vorsichtig agierende Angreifer können sich über Wasser halten, indem sie legitime Geschäftsanwendungen und dazugehörige Tools, einschließlich der in die Microsoft 365-Suite integrierten Anwendungen wie Power Automate und eDiscovery, nutzen, um sich lateral zu bewegen, sich zu verstecken und Daten auszuschleusen. KI-gestützte, in Cloud-Anwendungen und -Dienste integrierte NDR-Lösungen können diese Tarnung auffliegen lassen und erkennen selbst kleinste Indizien dafür, dass ein Eindringling am Werk ist.

KI-gestützte, in Cloud-Anwendungen und -Dienste integrierte NDR-Lösungen können diese Tarnung auffliegen lassen und erkennen selbst kleinste Indizien dafür, dass ein Eindringling am Werk ist.

Natürlich kann allein das Vorhandensein dieser Tools nicht bewirken, dass die Lücke zwischen Angreifern und Verteidigern kleiner wird. Nur die Unternehmen, die in diese Möglichkeiten investiert haben, können die subtilen Anzeichen für böswillige Aktivitäten erkennen. Wir werden wohl leider erstmal weiterhin beobachten, dass Angreifer ungeschützte Cloud-Infrastrukturen ausnutzen, indem sie beispielsweise legitime Benutzerkonten übernehmen, um auf sensible Daten zugreifen zu können. Mehr als drei von fünf der von uns befragten Regierungs-, Gesundheits- und Bildungsorganisationen haben im letzten Jahr jeweils mindestens einen Angriff im Hinblick auf Kontoübernahmen erlebt, bei denen ihre Microsoft 365-Nutzer zum Angriffsziel wurden.

> Wir werden wohl leider weiterhin beobachten, dass Angreifer ungeschützte Cloud-Infrastrukturen ausnutzen.

63 % der Organisationen im öffentlichen Dienst haben **im letzten Jahr** eine Kontoübernahme eines legitimen Benutzerkontos erlebt



VECTRA
SECURITY THAT THINKS

Der Schutz von Microsoft 365 hat oberste Priorität

Regierungs-, Gesundheits- und Bildungsorganisationen sind das Hauptziel von Cyber-Kriminellen, da sie dort wertvolle Daten abschöpfen können. Daher müssen sich IT-Sicherheitsteams weiterhin auf eine Vielzahl an Cyber-Bedrohungen einstellen. Zu den größten Sorgen der Befragten in Regierungs-, Gesundheits- und Bildungseinrichtungen gehören Bedrohungen, die sich auf IoT und verbundene Geräte beziehen, identitätsbasierte Bedrohungen, bei denen autorisierte Nutzer das Ziel sind, sowie die zunehmende Bedrohung durch Ransomware.

Die Hälfte der Befragten gab an, dass ihre größte Sorge das Risiko ist, dass die in Microsoft 365 gespeicherten Daten kompromittiert werden

Die größte Sorge aber waren Angriffe auf in Microsoft 365 gespeicherte Daten, dicht gefolgt von dem Risiko, dass Hacker ihre Spuren verwischen können, indem sie legitime Microsoft-Tools wie Power Automate und eDiscovery nutzen. Microsoft 365 ist für die Arbeit in Regierungs-, Gesundheits- und Bildungseinrichtungen unerlässlich geworden, da es einen Großteil der Datenspeicherung und -freigabe ermöglicht und als Identity-Provider Zugriff auf eine Vielzahl anderer SaaS-Anwendungen erlaubt. Dies macht die Microsoft 365-Umgebung zu einem lohnenswerten Ziel für Hacker, und bei mehr als 250 Millionen Nutzern im Monat gibt es zieltechnisch keinen Mangel. Unser aktueller Spotlight Report in Bezug auf Office 365 beinhaltete die Untersuchung von mehr als vier Millionen Konten und kam zu dem Ergebnis, dass 96 Prozent Anzeichen von Lateral Movement aufwiesen.

Microsoft 365 ist für die Arbeit in Regierungs-, Gesundheits- und Bildungseinrichtungen unerlässlich geworden, da es einen Großteil der Datenspeicherung und -freigabe ermöglicht und als Identity-Provider Zugriff auf eine Vielzahl anderer SaaS-Anwendungen erlaubt.

Viele Befragte waren auch besorgt über das Risiko des Missbrauchs von Anmeldedaten, was zu einer Kontoübernahme durch nicht autorisierte Nutzer führen kann.

Der große Umfang an Funktionen und Daten, die einem Microsoft 365-Benutzer zur Verfügung stehen, bedeutet, dass die erfolgreiche Kompromittierung eines Kontos es dem Angreifer ermöglichen kann, ganz einfach massiven Schaden anzurichten. Privilegierte Konten können ausgenutzt werden, um Lateral Movement zu beschleunigen und systemische Änderungen vorzunehmen, die es leichter machen, dauerhaft vor Ort und unentdeckt zu bleiben. Im Mittelpunkt der Strategien für Cloud-Sicherheit muss daher stehen, diese Konten zu schützen und deren unberechtigte Nutzung zu erkennen und zu stoppen.

Der große Umfang an Funktionen und Daten, die einem Microsoft 365-Benutzer zur Verfügung stehen, bedeutet, dass die erfolgreiche Kompromittierung eines Kontos es dem Angreifer ermöglichen kann, ganz einfach massiven Schaden anzurichten.

Auf die Frage nach den beunruhigendsten Bedrohungen für die Sicherheit im Jahr 2021 ergab die Umfrage Folgendes:

43 %

Es wird vermehrt Angriffe über IoT/verbundene Geräte geben

43 %

Der Trend hinsichtlich identitätsbasierten Angriffen auf unsere autorisierten Benutzer wird zunehmen

40 %

Ransomware-Angriffe werden sich häufen

40 %

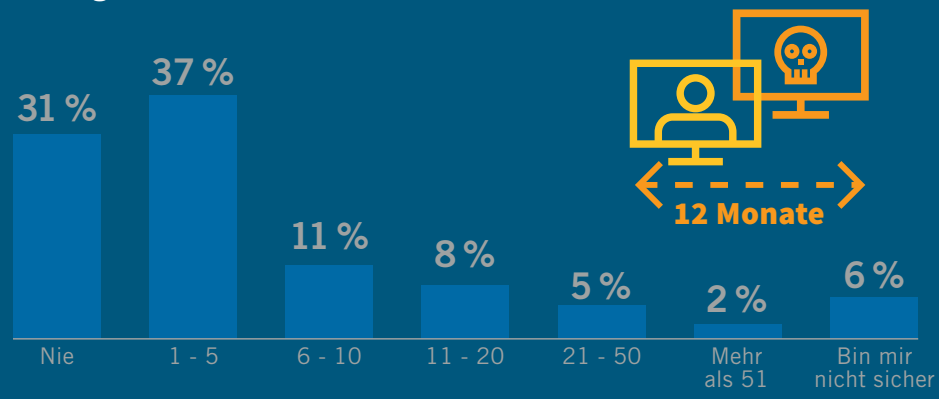
Wir werden eine rasante Beschleunigung bei Cloud-basierten Angriffen erleben

VECTRA
SECURITY THAT THINKS

Die steigende Bedrohung durch Kontoübernahmen

Die Agilität und Konnektivität, die Anwendungen wie die in der Microsoft 365-Suite bieten, sind ein großer Segen für den Durchschnittsarbeitnehmer, aber Gleiches gilt für Hacker. Cloud-Umgebungen sind deutlich zugänglicher als traditionelle Anwendungen, die durch ein Netzwerk-Perimeter geschützt sind. Microsoft 365-Angreifer wissen nur allzu gut, dass es kein Problem ist, Microsoft 365-Umgebungen auszukundschaften, um Nutzer und deren Namenskonventionen ausfindig zu machen.

Entscheidungsträger im Bereich der IT-Sicherheit erlebten durchschnittlich **6 Kontoübernahmen** von legitimen Benutzerkonten in den letzten 12 Monaten



Von hier aus können Angreifer hoch automatisierte Angriffe mit versuchten Anmeldungen auf Tausende von Konten durchführen. Bei einem Unternehmen reicht ein einziger Benutzer mit schlechtem Passwortmanagement, damit der Angreifer Zugang erhält, wobei die Umgehung einer mehrstufigen Authentifizierung (MFA) oft keine Herausforderung darstellt. Dieser Ansatz ist für Cyber-Kriminelle äußerst attraktiv, da er enorme Gewinne erzielen kann, ohne dass ein zeit- und ressourcenintensiver gezielter Angriff erforderlich ist.

Kompromittierte Microsoft 365-Konten können dazu verwendet werden, innerhalb kürzester Zeit deutlichen Schaden anzurichten.

Cloud-Umgebungen ermöglichen es Angreifern zudem, ihren Angriffszyklus drastisch zu verkürzen, da die für die Erkundung benötigte Zeit stark reduziert wird.

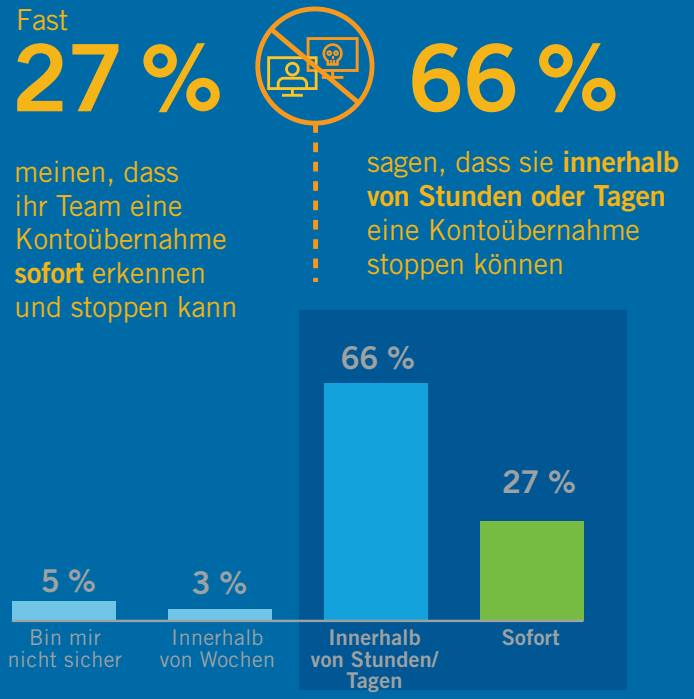
Demnach berichteten Entscheidungsträger im Bereich der IT-Sicherheit innerhalb von Regierungs-, Gesundheits- und Bildungsorganisationen, dass sie in den letzten 12 Monaten durchschnittlich die Übernahme von sechs Konten von autorisierten Nutzern erlebt haben.

Auffallend ist, dass trotz der Anzahl der Vorfälle und des Risikos, das eine solche Verletzung darstellt, die Mehrheit der von uns befragten Entscheidungsträger im Sicherheitsbereich im öffentlichen Dienst in Bezug auf ihre Fähigkeit, mit Kontoübernahmen fertig zu werden, recht zuversichtlich ist.

Nahezu sieben von zehn Befragten sind der Meinung, dass ihr Team eine Kontoübernahme binnen weniger Tage oder sogar Stunden erkennen und stoppen kann. Darüber hinaus glauben fast drei von zehn Befragten, dass sie einen solchen Angriff sofort stoppen könnten.

Kompromittierte Microsoft 365-Konten können in sehr kurzer Zeit erheblichen Schaden anrichten. Also selbst wenn die Erkennung einer Übernahme nur wenige Tage dauert, kann ein Unternehmen dadurch deutlich geschwächt werden. Es ist zwingend erforderlich, dass Sicherheitsteams verdächtiges Verhalten vor Ort und in der Cloud in Echtzeit erkennen können, um einen Angreifer zu entdecken, bevor Schaden entsteht.

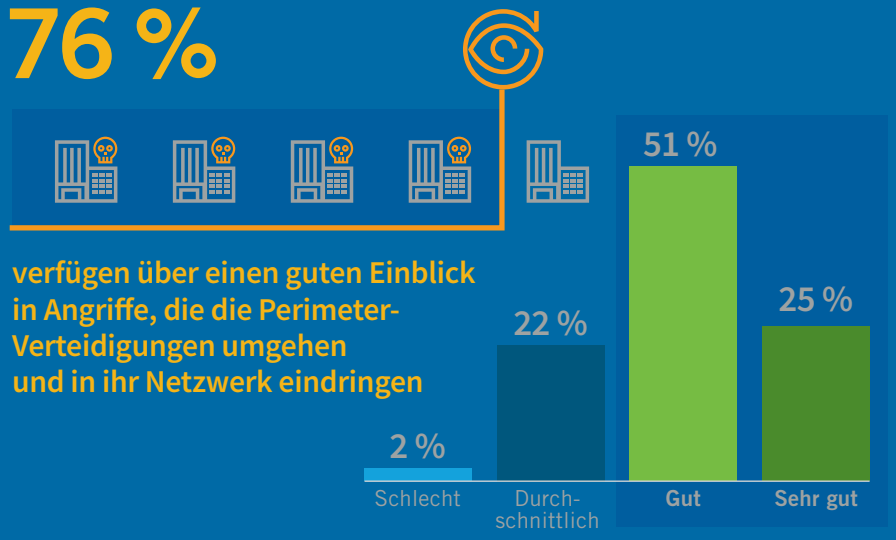
Diejenigen, die glauben, eine Kompromittierung sofort erkennen zu können, sollten sicher sein, dass ihre Zuversicht wirklich begründet ist – oder sie müssen sich im Falle einer Sicherheitslücke auf ein böses Erwachen gefasst machen.



VECTRA
SECURITY THAT THINKS

MangeInde Sichtbarkeit ist trügerisch für das Vertrauen

Das Vertrauen der Entscheidungsträger für IT-Sicherheit in ihre Fähigkeit, Angriffe in Bezug auf Kontoübernahmen zu verhindern, steht in krassem Gegensatz zur steigenden Anzahl von Angriffen und den langen Verweilzeiten, die in der Branche im Allgemeinen vermeldet werden. Die durchschnittliche Verweilzeit bei einem Angriff liegt bei schätzungsweise 43 Tagen – und lediglich 3 Prozent der Befragten gaben an, dass ihr Team Wochen benötigen würde, um sich um ein kompromittiertes Konto zu kümmern.



Die Befragten waren im Allgemeinen auch hinsichtlich ihrer Fähigkeit, andere Formen von Angriffen zu erkennen und zu stoppen, recht zuversichtlich. Die meisten waren der Meinung, sie hätten einen guten Überblick in Bezug auf Angriffe, die ihre Schutzmaßnahmen umgehen und wären in der Lage, Lateral Movement zu erkennen und einzudämmen. Dem wiederum steht die Tatsache gegenüber, dass 96 Prozent der von uns untersuchten Microsoft 365-Umgebungen Anzeichen von Lateral Movement aufwiesen.

Die durchschnittliche Verweilzeit liegt bei schätzungsweise 43 Tagen – und lediglich drei Prozent der Befragten gaben an, dass ihr Team Wochen benötigen würde, um sich um ein kompromittiertes Konto zu kümmern.

Die positive Einstellung hat nichts mit der Realität zu tun, auf die wir bei der Recherche in Unternehmen gestoßen sind. Während einige der Befragten ihre Behauptungen zweifellos untermauern können, ist ein Großteil dieses Vertrauens wahrscheinlich unangebracht.

Die Befragten auf Managementebene waren im Vergleich zu Führungskräften in Verantwortungspositionen und im Top-Management allgemein weitaus pessimistischer eingestellt. Das deutet darauf hin, dass ein falsches Gefühl der Zuversicht den verzerrten Messungen und Zielen auf höheren Ebenen entstammen kann, die nicht mit der Realität der Sicherheitsaktivitäten an vorderster Front übereinstimmen.

Ein falsches Gefühl der Zuversicht könnte den verzerrten Messungen und Zielen auf höheren Ebenen entstammen, die nicht mit der Realität der Sicherheitsaktivitäten an vorderster Front übereinstimmen.

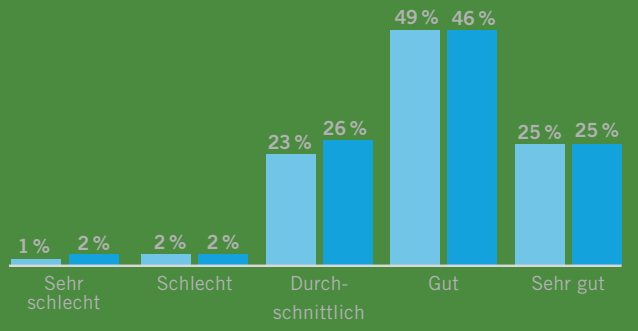
Ein Security Operations Center (SOC) zum Beispiel kann sich täglich um Hunderte Bedrohungen kümmern. Wird die Anzahl der vereitelten Incidents als Leitindikator für den Erfolg angesetzt, ist das fantastisch. Dieser Ansatz hat jedoch keinen realen Kontext - wie lange gab es die Bedrohungen, bevor sie erkannt und beseitigt wurden? Bei wie vielen davon handelte es sich um sich wiederholende Probleme? Die Fähigkeit, eine große Anzahl von volumetrischen Angriffen auf niedriger Ebene zu stoppen, hat so gut wie keinen Einfluss auf die Erkennung ausgefeilter Bedrohungen, insbesondere solcher, die auf Benutzer abzielen.

74 %

bezeichnen ihr Unternehmen bei der **Erkennung von Angriffen** als gut

71 %

bezeichnen ihr Unternehmen bei der **Vermeidung von Angriffen** als gut



VECTRA
SECURITY THAT THINKS

In Bezug auf Angriffe wie z. B. Kontoübernahmen haben sich die Indikatoren für eine Kompromittierung auf Verhaltensfaktoren verlagert, die schwieriger zu definieren sind und sich über mehrere Umgebungen hinweg in einer Weise ausbreiten können, die nicht sofort offensichtlich ist.

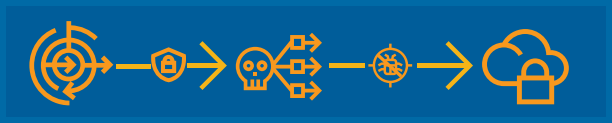
Die Realität ist jedoch, dass Hacker an ihren Vorgehensweisen ständig feilen, um alle Hindernisse zu überwinden, die sich ihnen in den Weg stellen.

Schließlich kann dieses trügerische Vertrauen auch der Vorstellung entspringen, dass die Anwendung der besten Sicherheitspraktiken Schutz vor Angriffen garantiert. Die Realität ist jedoch, dass Hacker an ihren Vorgehensweisen ständig feilen, um alle Hindernisse zu überwinden, die sich ihnen in den Weg stellen.

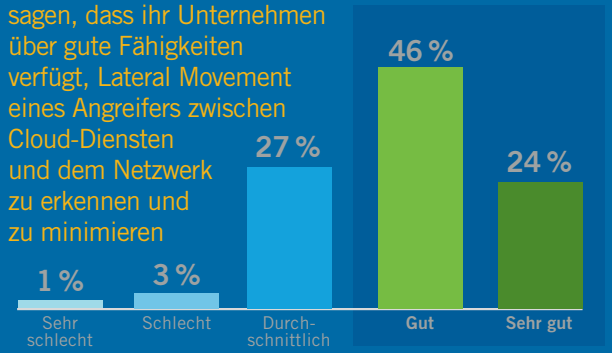
Eine mehrstufige Authentifizierung zum Beispiel ist mittlerweile fast überall zu finden und viele sind der Meinung, dass sie gegen den Versuch einer Kontoübernahme immun ist. Nichtsdestotrotz hat Microsoft kürzlich vor Schwachstellen in SMS- und anrufbasierter MFA gewarnt. In den USA hat die Cybersecurity and Infrastructure Security Agency (CISA) eine neue „Umgeh-den-Cookie"-Technik gemeldet, die die Authentifizierung beim Zugriff auf Cloud-Dienste umgehen kann. Sicherheitsmaßnahmen können Angreifer lediglich ausbremsen, aber nicht vollständig stoppen.

Microsoft hat kürzlich vor Schwachstellen, wie SMS- und anrufbasierte MFA, gewarnt.

70 %



sagen, dass ihr Unternehmen über gute Fähigkeiten verfügt, Lateral Movement eines Angreifers zwischen Cloud-Diensten und dem Netzwerk zu erkennen und zu minimieren



96 %

von vier Millionen Unternehmen, die von Vectra befragt wurden, zeigten Anzeichen von Lateral Movement*

* Vectra Spotlight Report

VECTRA
SECURITY THAT THINKS

Gewährleisten, dass Vertrauen der Realität entspricht

Das Erreichen eines exakten Bildes der Sicherheitsmaßnahmen beginnt mit den richtigen Messungen. Die drei wichtigsten Messfaktoren sind:

1. Mittlere Zeit bis zur Erkennung einer Bedrohung (MTTD)
2. Mittlere Zeit der Reaktion (MTTR)
3. Häufigkeit, in der die gleichen Probleme erneut auftauchen

Die Analyse dieser drei Faktoren liefert wichtige Anhaltspunkte dafür, wie gut die Sicherheitsmaßnahmen des Unternehmens funktionieren. Angriffe, die eine lange Verweilzeit erreichen, stellen die größte Bedrohung dar, insbesondere wenn sie ein kompromittiertes Microsoft 365-Konto mit Zugriff auf eine Reihe von Daten und Anwendungen betreffen, bei denen schon wenige Sekunden ausreichen, um dem Unternehmen richtige Kopfschmerzen zu bereiten. Auch ist es wichtig, festzustellen, wo das gleiche Problem immer wieder angesprochen wird, da dies ein Hinweis darauf ist, dass eine grundlegende Änderung der Politik oder der Infrastruktur erforderlich sein könnte.

Jede Messung muss sich auf ein ausreichendes Maß reproduzierbarer Daten gründen.

Jede Messung muss sich auf ein ausreichendes Maß reproduzierbarer Daten gründen. Sicherheitsanalysten können durch den Einsatz von Penetrationstests und Red-Team-Übungen beispielsweise ein größeres Volumen an zuverlässigen Bedrohungsdaten erzeugen. So ist schnell erkennbar, wo die Sicherheitsstrategie Lücken aufweist und wie effektiv die Abwehrmaßnahmen tatsächlich sind.

Abgesehen vom messtechnischen Aspekt ist dies eine ganz wesentliche Fähigkeit des SOC-Teams, denn es muss Sicherheitsmaßnahmen nicht nur durchbrechen, sondern auch wieder herstellen können.

Angriffe, die lange Verweilzeiten erreichen, stellen die größte Bedrohung für das Unternehmen dar.

„Wir sind jetzt zuversichtlicher, dass wir den Missbrauch von Anmeldedaten, der in Office 365 üblich geworden ist, erkennen und stoppen können.“

Kevin Orritt
ICT-Sicherheitsmanager
Greater Manchester Mental Health

VECTRA
SECURITY THAT THINKS

Sicherheitsmaßnahmen 2021 verbessern

Erfreulicherweise haben die meisten Entscheidungsträger im Sicherheitsbereich in Regierungs-, Gesundheits- und Bildungsorganisationen einen ziemlich vorausschauenden Ansatz gewählt, um ihre Sicherheitsmaßnahmen im Jahr 2021 zu verbessern. Nahezu drei Fünftel von ihnen planen nicht nur, größere Investitionen in Technologie und Personal zu tätigen, sondern es gibt zusätzlich eine deutliche Präferenz hinsichtlich der Nutzung von Lösungen, die Microsoft 365-Umgebungen effektiv vor Bedrohungen wie Kontoübernahmen schützen.

VECTRA
SECURITY THAT THINKS

Der Einsatz von KI-Lösungen und die verstärkte Automatisierung waren zwei der beliebtesten Entscheidungen hinsichtlich der Investitionen im Jahr 2021. Diese Maßnahmen sind wesentlich, um große Mengen an Bedrohungsdaten effektiv zu analysieren und die subtilen Verhaltenssignale zu erkennen, die auf eine Kompromittierung hinweisen. Darüber hinaus kann der Einsatz von KI zur Arbeitserleichterung auf die Schwierigkeit zurückgeführt werden, Mitarbeiter einzustellen und an das Unternehmen zu binden.

Bemerkenswert ist auch, dass nahezu 40 Prozent der Befragten NDR als eine der zwei wichtigsten Lösungen für ihre SOC-Teams anführten.

Der vermehrte Einsatz von KI- und Automatisierungslösungen sind eine beliebte Entscheidung hinsichtlich der Investitionen im Jahr 2021.

Der Schlüssel zur Sicherheit in einer komplexen Cloud-Umgebung liegt in der Fähigkeit, den täglichen Datenverkehr zu durchdringen und Anzeichen verdächtiger Aktivitäten in der gesamten Umgebung zu erkennen, wobei On-Premises- und Cloud-Netzwerke als ein einheitliches Ganzes behandelt werden. KI-gestützte Bedrohungserkennung und Response sorgen für diese Fähigkeit.

Schließlich waren auch die vermehrte Nutzung von Threat Intelligence und höhere Investitionen in Threat Hunting sowie sonstige proaktive Maßnahmen beliebte Themenschwerpunkte, die den Sicherheitsteams im öffentlichen Dienst dabei helfen, ihre Sicherheitsmaßnahmen besser zu verstehen und Schwachstellen und Angriffspfade zu erkennen, bevor es Probleme gibt.

„Vor dem Einsatz von Vectra hatten wir nur begrenzten Einblick in böswilliges Verhalten im Netzwerk-Traffic oder in Microsoft Office 365. Wir sind von dem, was wir sehen können beeindruckt."

Kevin Orritt
ICT-Sicherheitsmanager
Greater Manchester Mental Health

Auch ergab die Umfrage:

59 %
planen, 2021 mehr Geld in Technologie und Mitarbeiter zu investieren, um ihre Sicherheitslage zu verbessern.

49 %
beabsichtigen, vermehrt Automatisierung und KI einzusetzen.

45 %
möchten Threat Intelligence stärker nutzen.

41 %
werden proaktives Threat Hunting betreiben.

10 Schritte, um Microsoft 365 vor identitätsbasierten Angriffen zu schützen

Da Microsoft 365 im laufenden Geschäftsbetrieb weiterhin eine wesentliche Rolle spielen wird, müssen Organisationen im öffentlichen Dienst sicherstellen, dass sie über die notwendigen Fähigkeiten zur Sicherung ihrer Cloud-Umgebungen verfügen. Dies ist eine besonders dringliche Herausforderung für diejenigen Regierungs-, Gesundheits- und Bildungseinrichtungen, die ihre Abläufe im letzten Jahr schnell anpassen mussten und denen es schwerfallen dürfte, perimeterbasierte Abwehrmaßnahmen an die dürftig gesicherten „Grenzen“ einer Cloud anzupassen. Der Schutz vor Kontoübernahmen sollte oberste Priorität haben.

Hier sind die 10 wichtigsten Schritte für Unternehmen, um ihre Microsoft 365-Umgebung vor der Kompromittierung von Konten zu schützen:

Privilegierte Konten verstehen. Sie müssen über fundierte Kenntnisse verfügen, welche Konten auf sensible Daten zugreifen oder leistungsstarke Microsoft 365-Tools wie eDiscovery nutzen können. Diese Konten sind das Hauptziel von Hackern. Die strikte Beschränkung von System- und Tool-Zugriff auf die für die jeweiligen Aufgaben erforderlichen Funktionen begrenzt den Schaden, den ein kompromittiertes Konto anrichten kann.

Die richtigen Metriken messen. Alle Metriken zur Messung der Sicherheitseffektivität müssen den "Na und?"-Test bestehen - sie müssen die Maßnahmen steuern, nicht nur informieren. Die Messung der Zeit bis zur Erkennung, der Zeit bis zur Reaktion, der wiederholten Incidents und der Wiederansteckungsraten liefert stichhaltige Indizien darauf, wie effektiv Ihr Team Bedrohungen identifiziert und beendet.

MFA implementieren. Mehrstufige Authentifizierung mag nicht der Goldstandard zur Sicherung von Konten sein, ist aber immer noch ein wichtiges Tool, um Angreifern das Leben schwer zu machen. Sofern Sie nicht bereits MFA verwenden, sollten Sie sicherstellen, dies für alle Konten einzuführen.

Konfigurationsaufwand minimieren. Übergangstechnisch ausgelegte Hybrid-Cloud-Umgebungen sind in puncto Sicherheit das Schlechtmöglichste und schaffen Redundanzen und tote Winkel, die ausgenutzt werden können. Langwierige Umstellungen belasten Ihre IT- und Sicherheitsressourcen und erhöhen das Risiko. Versuchen Sie daher, sich auf die Beschleunigung des Prozesses zu konzentrieren, um Ihre Umgebung zu vereinfachen und zu optimieren.

Regelmäßige Tests durchführen. Aufgaben wie Penetrationstests und Red-Teaming helfen dabei, die Grundlage Ihres Vertrauens in die Sicherheit zu bewerten, indem sie Schwachstellen und Angriffswege aufzeigen. Tests müssen in regelmäßigen Abständen wiederholt werden, um sicherzustellen, dass Korrekturen die Sicherheit verbessern.

Alle Mitarbeiter schulen – auch in puncto Sicherheit. Während Sie Abläufe weiter verändern, müssen Sie sicherstellen, dass Ihre Mitarbeiter wissen, wie sie die neuen Tools sicher anwenden und sie auch über Bedrohungen, wie z.B. über Angreifer, die sich in Phishing-E-Mails als IT-Team ausgeben, aufklären. Ein größeres Bewusstsein verringert den Erfolg erster Kompromittierungsversuche. Außerdem müssen Sie sicherstellen, dass Ihre Sicherheitsbeauftragten mit der neuen Umgebung vertraut sind und sich von traditionellen, perimeterbasierten Strategien auf die offeneren „Grenzen“ der Cloud umstellen können.

Verstehen, wie Tools verwendet werden. Microsoft 365-Tools wie eDiscovery und Power Automate können in den falschen Händen fatale Auswirkungen haben. Sie müssen im Kontext erfassen, wie diese Tools verwendet werden, und sich ein genaues Bild davon machen, wie diese Tools normalerweise reagieren. Unzulässige und böswillige Aktivitäten müssen sofort erkannt und gestoppt werden, bevor Schaden entstehen kann.

Sich eine einheitliche Darstellung Ihrer Umgebungen verschaffen. Angreifer werden sich bei der Verfolgung ihrer Ziele ungehindert zwischen Ihren traditionellen und Cloud-Netzwerken bewegen, deshalb ist es schwierig, eine Verbindung zwischen den jeweiligen Sicherheitstools, die die verschiedenen Umgebungen überwachen, herzustellen. Sie müssen in der Lage sein, böswilliges Verhalten in Ihrem IT-Netzwerk, Ihrer SaaS-Cloud-Umgebung, Ihrem Rechenzentrum und weiteren Anwendungen, die Angreifer ausnutzen könnten, zu identifizieren. Wesentlich ist hierbei NDR.

KI nutzen, um Reaktionszeiten zu beschleunigen und zu automatisieren. Nicht nur Sie profitieren von der erhöhten Geschwindigkeit und Skalierung der Cloud, Hacker tun das auch. Die Verwendung von klar definierten APIs bedeutet, dass Angreifer die Erkundungsphase drastisch verkürzen und viel schneller mit der Ausführung ihres Angriffs starten können. Durch KI und maschinelles Lernen verbesserte Analysen sind der Schlüssel zur schnellen Erkennung von Anzeichen böswilliger Aktivitäten und zur Automatisierung von Response-Maßnahmen.

Den täglichen Datenverkehr durchdringen. Schnelle Response-Maßnahmen sind wichtig, aber nur die halbe Miete. Ohne ein dynamisches Signal, das den täglichen Datenverkehr durchdringt, können überzogene automatisierte Abwehrmaßnahmen durch False-Positives ausgelöst werden. KI-gestützte Bedrohungserkennung stellt sicher, dass die nachgelagerte Response-Orchestrierung genau, zuverlässig und schnell ist.

VECTRA
SECURITY THAT THINKS

Wie Vectra Microsoft 365 und Azure AD schützt

Cognito, die KI-gestützte Lösung von Vectra für Bedrohungserkennung und Response, kann Angreifer, die in Ihrer Microsoft 365-Umgebung und jeder verbundenen SaaS-Anwendung mit Azure AD agieren, identifizieren und stoppen. Uns ist klar, dass Angreifer nicht in Silos operieren, und wir können Anzeichen für das Verhalten von Angreifern im gesamten Unternehmen, in hybriden Systemen, im Rechenzentrum, bei IaaS und SaaS verfolgen, und das alles von einem einzigen Kontrollpunkt aus.

VECTRA
SECURITY THAT THINKS

Vectra Cognito bietet dynamische, zuverlässige, nach Prioritäten geordnete Warnungen, statt lediglich nur das Volumen der ständigen Sicherheitswarnungen zu verstärken. Kritische Bedrohungen, wie z. B. die Verwendung von privilegierten Konten, werden identifiziert und priorisiert, sodass sie ausgeschaltet werden können, bevor der Eindringling die Chance hat, seinen Angriff auszuführen.

Stellen Sie in Minuten einen Cloud-nativen Ansatz bereit, der Angriffe schnell überwacht, erkennt und stoppt.

Erhalten Sie umfassenden, anwendungsüberspannenden Schutz für Microsoft 365, Azure AD und Ihre lokale IT-Infrastruktur.

Stoppen Sie bekannte und unbekannte Angriffe und Kontoübernahmen in Echtzeit, bevor diese zu Datenverletzungen führen.

„Vectra erlaubt es mir, pro-aktiv statt reaktiv zu sein. Für uns eine ganz große Sache. Statt Warnungen aus bedeutungslosen Protokollen nachzujagen, verbringe ich mehr Zeit damit, mit unserer Benutzer-Community zusammenzuarbeiten, um Bewusstsein für wichtige Sicherheitspraktiken zu schaffen."

Kevin Orritt
ICT-Sicherheitsmanager
Greater Manchester Mental Health

VECTRA
SECURITY THAT THINKS

Anhänge

Methodik

Die Studie wurde von Vectra in Auftrag gegeben und von Sapio Research durchgeführt. Bei der gesamten Studie wurden 1.112 Entscheidungsträger im Bereich der IT-Sicherheit in Unternehmen mit mehr als 1.000 Mitarbeitern befragt, die Microsoft 365 nutzen. Für die Erstellung der Statistik in diesem eBook wurde eine Teilgruppe von 302 Befragten herangezogen, die alle in Regierungs-, Gesundheits- oder Bildungseinrichtungen tätig sind.

Insgesamt sind die Ergebnisse bei ± 2,9 % mit einer 95 %-Vertrauensgrenze und unter der Annahme eines Ergebnisses von 50 % genau.

Die Befragung wurde im Februar 2021 online mittels E-Mail-Einladung und Online-Fragebogen durch Sapio Research durchgeführt.

Um herauszufinden, wie Vectra Ihnen helfen kann, Ihre Microsoft Office 365- und Azure AD-Umgebung gegen Kontenübernahme und andere führende Bedrohungen zu schützen, können Sie uns gern unter **info_dach@vectra.ai** kontaktieren.

E-Mail: info_dach@vectra.ai vectra.ai/de

Version **071521**