DESIGNED FOR Microsoft 365 ENVIRONMENTS

2024

CYBER SECURITY REPORT

EINE AUSFÜHRLICHE ANALYSE DER
BEDROHUNGSLAGE FÜR MICROSOFT 365

EBERTLANG

Vorwort von Adrian Brandtner von EBERTLANG

Der Cyber Security Report 2024 ist da!

In der sich ständig wandelnden Landschaft der IT-Sicherheit bleibt eine Konstante bestehen: die unabdingbare Notwendigkeit, informiert und vorbereitet zu sein. Daher freuen wir uns, Ihnen den diesjährigen Cyber Security Report unseres Partners Hornetsecurity zu präsentieren – das entscheidende Werkzeug für alle, die im Bereich der IT-Security tätig sind.

Jede größere Cyberattacke, die Schlagzeilen macht, wirft wichtige Fragen auf: Hätte sie verhindert werden können? Sind meine Kunden vor solchen Szenarien ausreichend geschützt? Fundiertes Wissen über aktuelle Bedrohungen und Trends ist dabei der Schlüssel zur Vorbeugung. Genau hier setzt der Report von Hornetsecurity an. Durch die Analyse von über 3,5 Milliarden E-Mails pro Monat bietet der Hersteller wertvolle Erkenntnisse, die Ihnen dabei helfen, die Natur dieser Bedrohungen zu verstehen und entsprechende Gegenmaßnahmen für die von Ihnen betreuten Unternehmen zu entwickeln.

Der Cyber Security Report bietet einen faszinierenden Einblick in die sowohl aktuellen als auch zukünftigen Cyber-Bedrohungen und ist damit unverzichtbar für jeden, der sich in der digitalen Welt sicher bewegen möchte. Als Systemhaus und Managed Services Provider spielen Sie eine zentrale Rolle in der Sicherung der digitalen Infrastruktur Ihrer Kunden. Deshalb teilen wir diesen Bericht in der Überzeugung, dass er Ihnen helfen wird, Ihre Sicherheitsstrategien zu stärken und Ihren Kunden einen besseren Schutz zu bieten.

Ihr

Adrian Brandtner

HORNETSECURITY

CYBERSECURITY REPORT 2024

Über Hornetsecurity

Wir von Hornetsecurity ermöglichen es Unternehmen und Organisationen jeder Größe, sich auf ihr Kerngeschäft zu konzentrieren, indem wir die E-Mail-Kommunikation schützen, Daten sichern und die Geschäftskontinuität und Compliance mit umfassenden Lösungen gewährleisten. Unser Flaggschiff 365 Total Protection ist die umfassendste Cloud-Sicherheitslösung für Microsoft 365 auf dem Markt, einschließlich E-Mail-Sicherheit, Compliance und Backup.

Was ist der Cyber Security Report?

Der Cyber Security Report (ehemals Cyber Threat Report) ist eine jährliche Analyse der aktuellen Cyber-Bedrohungslage, basierend auf realen Daten, die von Hornetsecuritys engagiertem Security Lab Team gesammelt und analysiert werden. Hornetsecurity verarbeitet mehr als 3,5 Milliarden E-Mails pro Monat. Durch die Analyse der in diesen Mitteilungen identifizierten Bedrohungen, in Kombination mit einer detaillierten Darstellung der breiteren Bedrohungslage, zeigt das Security Lab wichtige Trends auf und kann fundierte Prognosen für die Zukunft der Microsoft 365-Sicherheitsbedrohungen erstellen, damit Unternehmen entsprechend handeln können. Die Ergebnisse und Daten sind in diesem Bericht enthalten.

Was ist das Security Lab?

Das Security Lab ist eine Abteilung von Hornetsecurity, die forensische Analysen der aktuellsten und kritischsten E-Mail-Sicherheitsbedrohungen durchführt. Das multinationale Team von Sicherheitsspezialisten verfügt über umfangreiche Erfahrung in den Bereichen Sicherheitsforschung, Softwaretechnik und Data Science.

Ein tiefgreifendes Verständnis der Bedrohungslage, das durch die praktische Untersuchung von realen Viren, Phishing-Angriffen, Malware usw. gewonnen wird, ist für die Entwicklung wirksamer Gegenmaßnahmen von entscheidender Bedeutung. Die detaillierten Erkenntnisse des Security Labs dienen als Grundlage für die Next-Gen Cybersecurity-Lösungen von Hornetsecurity.

Wie dieser Bericht inhaltlich aufgebaut ist

Dieser Bericht ist in 5 Kapitel unterteilt:

Kapitel 1 enthält die Zusammenfassung des Berichts. Wenn Sie nur an den Highlights interessiert sind, sollten Sie sich diesen Abschnitt ansehen.

Kapitel 2 befasst sich mit der aktuellen Bedrohungslage der Microsoft 365-Plattform.

Kapitel 3 befasst sich mit aktuellen Herausforderungen und Diskussionen über die größten Bedrohungen und Trends seit Beginn des Jahres 2023.

Kapitel 4 enthält Prognosen des Security Labs über die Bedrohungen der Cybersicherheit im Jahr 2024 sowie Empfehlungen und Leitlinien zum Schutz Ihres Unternehmens.

Kapitel 5 führt alle in diesem Bericht verwendeten Verweise, unterstützende Links und Datensätze auf.

Inhaltsverzeichnis

Kapitel 1 – Zusammenfassung 5

Kapitel 2 – Die aktuelle Bedrohungslage für Microsoft 365 8

- Trends im Bereich der E-Mail-Sicherheit 8
- Spam, Malware, fortgeschrittene Bedrohungsmetriken 8
- Verwendung von Angriffstechniken bei E-Mail-Angriffen 9
- Bei Angriffen verwendete Dateitypen 10
- E-Mail-Threat Index in unterschiedlichen Geschäftsbereichen 11
- Markenimitation 12
- Datensicherheit in der Cloud 13
- Was bedeutet "Vendor Overdependence"? 14
- Was fällt unter die Verantwortung von Microsoft? 15
- Die Herausforderungen einer effektiven Berechtigungsverwaltung in M365 16

Kapitel 3 – Eine Analyse der größten Sicherheitsvorfälle und Cybersecurity-Nachrichten von 2023 17

- Storm-0558 17
- nOAuth 17
- Die Cyberangriffe auf MGM / Caesars Entertainment 18
- Microsoft Exchange-Schwachstellen 19
- Die Zerschlagung von Qakbot 19
- Der MOVEit Supply-Chain-Angriff 20

Kapitel 4 – Prognose zur Bedrohungslage im Jahr 2024 21

- Haben sich unsere Vorhersagen vom letzten Jahr bestätigt? 21
- Die Prognosen des Security Labs für 2024 22
- KI wird die Cybersecurity-Branche weiter vorantreiben 22
- LLM (Large Language Model) Sparring-Partner für Blue Teams 24
- Technologien wie Co-Pilot werden die Nachfrage nach erhöhter Code-Sicherheit und Code-Qualitäts-Scans vorantreiben 24
- MFA-Bypass-Angriffe werden zunehmen 25
- XDR- und MDR-Einsatz nimmt zu 25
- Zunahme von Angriffen auf Lieferketten 25
- Die steigende Komplexität der Cloud wird auch im kommenden Jahr zu Sicherheitsvorfällen führen 26
- Zunehmende Nutzung von 5G und die Abhängigkeit der Netzbetreiber von Network Slicing VNI werden Angriffe auf Mobilfunknetze vorantreiben 26
- Stärkere Ransomware-Gruppen und kürzere Dwell Time 27
- Update zu Quantum Computing und Encryption 27
- Wie stark ist mein Unternehmen im Jahr 2024 gefährdet? 27
- Wie sich Unternehmen am besten schützen können 28
- Mit den Grundlagen beginnen 28
- Die Sicherheitskultur ist das A und O 28
- Eine ausgewogene Sicherheitsstrategie 29

Kapitel 5 – Quellenangaben 32

Kapitel 1 – Zusammenfassung

Durch die Verwendung des eigenen, sehr umfangreichen Datenbestandes, ist Hornetsecurity in der einzigartigen Position, eine detaillierte Analyse von E-Mail-basierten Bedrohungen durchzuführen und diese in wichtige Erkenntnisse für IT-Sicherheitsexperten zu bündeln.

Die E-Mail bleibt ein unverzichtbarer Kommunikationskanal. In unserer Analyse von über 45 Milliarden E-Mails zeigen sich 36,4 % als "unerwünscht". Dabei entfallen 96,4 % auf Spam oder werden aufgrund äußerer Indikatoren direkt abgelehnt, während knapp über 3,6 % als bösartig eingestuft werden.

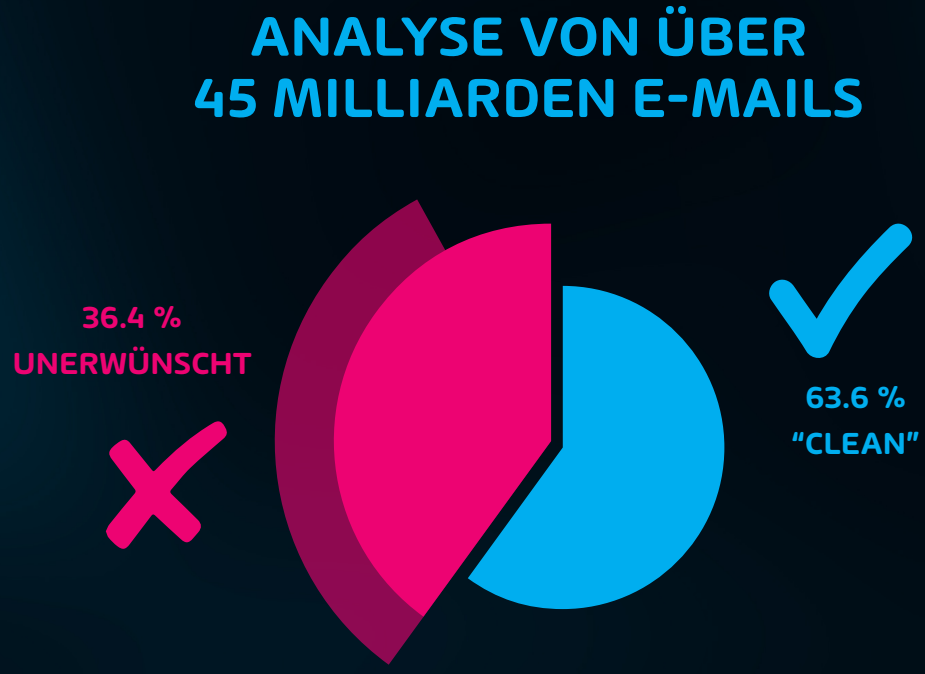


Fig. 1: Klassifizierung der durch Hornetsecurity gescannten E-Mails

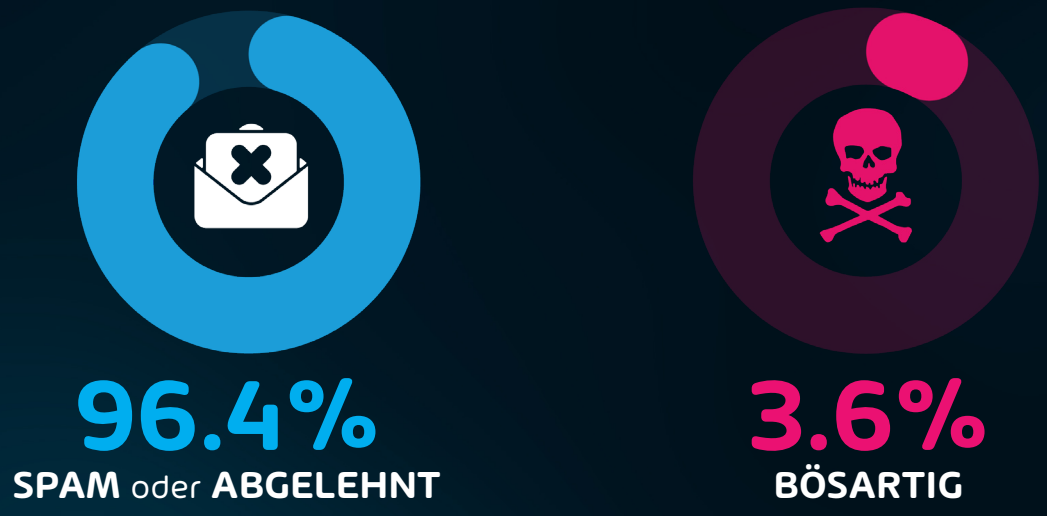


Fig. 2: Klassifizierung von unerwünschten E-Mails

Ein weiterer wichtiger Aspekt, den wir bei E-Mail-basierten Angriffen betrachten, ist die Angriffsmethode. Unsere Ergebnisse aus dem Datenerhebungszeitraum zeigen, dass Phishing weiterhin die Spitzenposition behält und für 43,3 % der E-Mail-basierten Angriffe verantwortlich ist. Dies bedeutet eine fast 4%ige Steigerung im Vergleich zum Vorjahr. Die zweithäufigste Angriffsmethode im Jahr 2023 war die Verwendung von bösartigen URLs in E-Mails mit 30,5 %, was einen signifikanten Anstieg um 18 Prozentpunkte gegenüber dem Vorjahresbericht darstellt.

43.3% DER E-MAIL-BASIERTEN ANGRIFFE

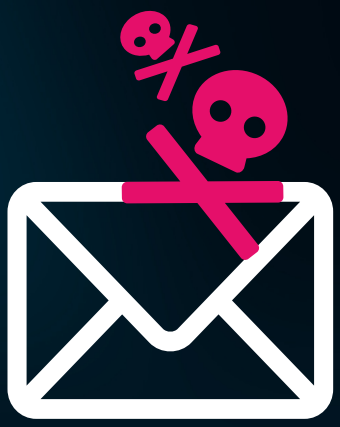


Fig. 3: 43,3 % E-Mail-basierte Angriffe sind Phishing

Neben den verschiedenen Angriffsmethoden überwachen wir auch die Verwendung von Anhängen und Dateitypen bei Angriffen. HTML-Dateien (37,1 %) und PDFs (23,3 %) wurden während des betrachteten Zeitraums am häufigsten beobachtet, gefolgt von Archivdateien (20,8 %) auf dem dritten Platz. Die Verwendung von HTML-Dateien durch Cyberkriminelle stieg von 21 % auf 37,1 % , ebenso wie die Nutzung von PDF-Dateien, die von 12,4 % auf 23,3 % anstieg. Dies wurde weitgehend durch Bedrohungen wie Qakbot und ähnliche Botnets vorangetrieben, die diese Dateitypen nutzen, um die Verbreitung ihrer Malware zu erleichtern. Auch erwähnenswert ist ein deutlicher Rückgang der Verwendung von DOCX-Dateien um 9,5 Prozentpunkte und XLSX-Dateien um 6,7 Prozentpunkte.

Diese Dateitypen waren früher bei Cyberkriminellen sehr beliebt, doch seit Microsoft dazu übergegangen ist, Makros in Office standardmäßig zu deaktivieren, ist die Verwendung dieser Dateitypen drastisch gesunken.

Der branchenbezogene E-Mail-Threat-Index war während des Datenerhebungszeitraums in den meisten Geschäftsbereichen ungefähr gleich. Dieser E-Mail-Bedrohungsindex ist eine von uns verfolgte Kennzahl, die die Anzahl der versuchten E-Mail-Angriffe im Verhältnis zur Anzahl der gutartigen E-Mails misst, die je nach Branche zugestellt wurden. Dies gibt einen guten Überblick darüber, welche Arten von Unternehmen derzeit im Fokus von Cyberkriminellen stehen. Wie im letzten Jahr zeigt unsere Datenanalyse, dass nahezu jede Art von Unternehmen derzeit bedroht ist. Kurz gesagt, wenn Ihre Organisation in der Lage ist, Lösegeld zu zahlen, sind Sie ein potenzielles Ziel. Dennoch befinden sich Forschungseinrichtungen, der Unterhaltungssektor und die Fertigungsindustrie am oberen Ende des Spektrums.

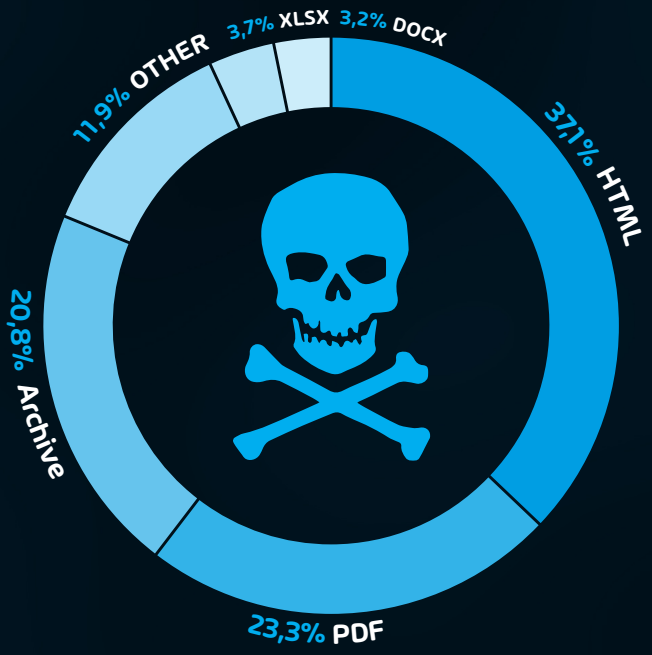


Fig. 4: Am häufigsten verwendete Dateitypen in bösartigen E-Mails

Ein weiterer Bereich der E-Mail-Sicherheit, den wir im Auge behalten, betrifft die Imitation von Marken. Diese Information ermöglicht es uns, unsere Produktteams, Kunden und die Öffentlichkeit darüber auf dem Laufenden zu halten, welche Arten von markenorientiertem Phishing derzeit im Einsatz sind.

Unsere Daten für diesen Bericht zeigen, dass Versanddienstleister nach wie vor eine beliebte Wahl darstellen. Beispielsweise haben DHL (26,1 %), Amazon (7,7 %) und FedEx (2,3 %) alle einen Platz in den Top 10. Weitere bedeutende Namen auf der Liste sind Microsoft (2,4 %), LinkedIn (2,4 %) und Netflix (2,2 %). In den meisten Fällen zielen Cyberkriminelle darauf ab, Anmeldeinformationen von Endnutzern zu erlangen, entweder um diese zu verkaufen oder für den Einsatz bei anderen Angriffen zu nutzen.

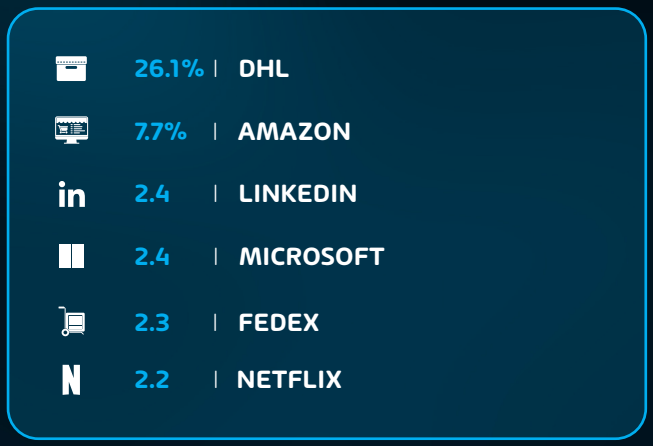


Fig. 5: Imitierte Marken/Unternehmen

Die Sicherheit von Daten in der Microsoft-Cloud ist nach wie vor ein zentraler Aspekt in den aktuellen Cloud-Diskussionen. Jüngste Sicherheitsvorfälle (darunter einer durch Cyberkriminelle aus China) haben dazu geführt, dass viele Unternehmen und Organisationen, einschließlich der US-Regierung, ihre Sicherheitsstrategien im Zeitalter der Cloud überdenken. Diese Entwicklungen werfen auch die Frage nach einer möglichen Überabhängigkeit von Anbietern auf und betonen, wie wichtig es ist, die richtige Balance zu finden und nicht ausschließlich auf einen einzelnen Anbieter zu setzen.

Microsoft hat seine langjährige Haltung zur Notwendigkeit von Backups für M365-Daten geändert. Über einen längeren Zeitraum hinweg lautete ihr einfacher Standpunkt: "Backups sind nicht erforderlich", wobei der Cloud-Anbieter ausschließlich auf die in M365 integrierten Speicherfunktionen setzte. Allerdings hat Microsoft diese Empfehlung im Sommer mit einer überraschenden Ankündigung revidiert, die eine neue M365-Backup-Anwendung sowie eine dazugehörige API einschloss. Trotzdem gibt es bisher keine weiteren Neuigkeiten zu diesem angekündigten Backup-Produkt.

Die optimale Anpassung von Nutzer- und Freigabeberechtigungen in M365 sind ebenfalls zentrale Themen in diesem Bericht. Mit der einfachen Möglichkeit zur Freigabe und Zusammenarbeit in M365 besteht die Herausforderung, dass sensible Daten versehentlich oder böswillig den M365-Tenant verlassen und in falsche Hände geraten. SharePoint Online und OneDrive for Business sind schon seit einiger Zeit die "Dateiserver" des Cloud-Zeitalters. Viele Organisationen stehen nun vor der Herausforderung, Freigaben und Berechtigungen in M365 zu verwalten, nachdem sie außer Kontrolle geraten sind. Dies wird auch 2024 ein Bereich sein, den Unternehmen genau im Auge behalten sollten und der als potenzielle Quelle für Datenlecks künftig weiter an Bedeutung gewinnen könnte.

In der Welt der Cybersicherheit bleibt E-Mail nach wie vor eine der führenden Methoden, die von Cyberkriminellen genutzt werden, um Angriffe zu starten. Eine durchdachte und umfassende E-Mail-Sicherheitsstrategie ist somit unerlässlich, um im Jahr 2024 gegen aufkommende Cyberbedrohungen gewappnet zu sein.

Kapitel 2 – Die aktuelle Bedrohungslage für Microsoft 365

Jährlich wertet das Security Lab von Hornetsecurity den umfangreichen Datensatz des Unternehmens aus und analysiert den Stand globaler Bedrohungen im Bereich E-Mail sowie weitreichende Kommunikationsstatistiken. Darüber hinaus führt das Team regelmäßig Prognosen durch und gibt Einblicke in potenzielle künftige Bedrohungen. Dieses Kapitel konzentriert sich auf die Auswertung der Daten aus dem Zeitraum 1. November 2022 bis zum 1. November 2023, die die Grundlage für die in Kapitel 4 dargelegten Prognosen über die sich verändernde Bedrohungslage bilden.

Trends im Bereich der E-Mail-Sicherheit

Trotz der wachsenden Nutzung von Kollaborations- und Instant Messaging Software wie Microsoft Teams, bleibt die E-Mail nach wie vor ein zentraler Fokus für Cyberangriffe. Obwohl wir in diesem Jahr einen leichten Rückgang bei den als "Threats/AdvThreats" kategorisierten E-Mails verzeichnen, 3,6 % im Vergleich zu 5,48 % im Vorjahr (bei "unerwünschten" E-Mails), bleibt das Risiko für Unternehmen weltweit hoch. Mit zunehmend komplexen Angriffen und dem Anstieg KI-gestützter Bedrohungen ist es entscheidend, dass Unternehmen wachsam bleiben und ihre Sicherheitsstrategie nicht vernachlässigen. Weitere Einzelheiten finden Sie unten.

Nach sorgfältiger Analyse von über 45 Milliarden E-Mails, die im aktuellen Berichtszeitraum (1. November 2022 - 1. November 2023) gesammelt wurden, hat das Security Lab folgende Erkenntnisse gewonnen:

Spam, Malware, fortgeschrittene Bedrohungsmetriken

Die E-Mail ist weiterhin eine der Hauptmethoden, die Cyberkriminelle nutzen, um Angriffe zu starten. Dies spiegelt sich in unseren Daten wider, die 36,4 % aller E-Mails als "Unerwünscht" klassifizieren, was bedeutet, dass es sich nicht um authentische Kommunikation handelt, die vom Empfänger gewünscht ist. Die folgende Grafik zeigt die Aufschlüsselung der unerwünschten E-Mails im Verhältnis zu den „sauberen" E-Mails.

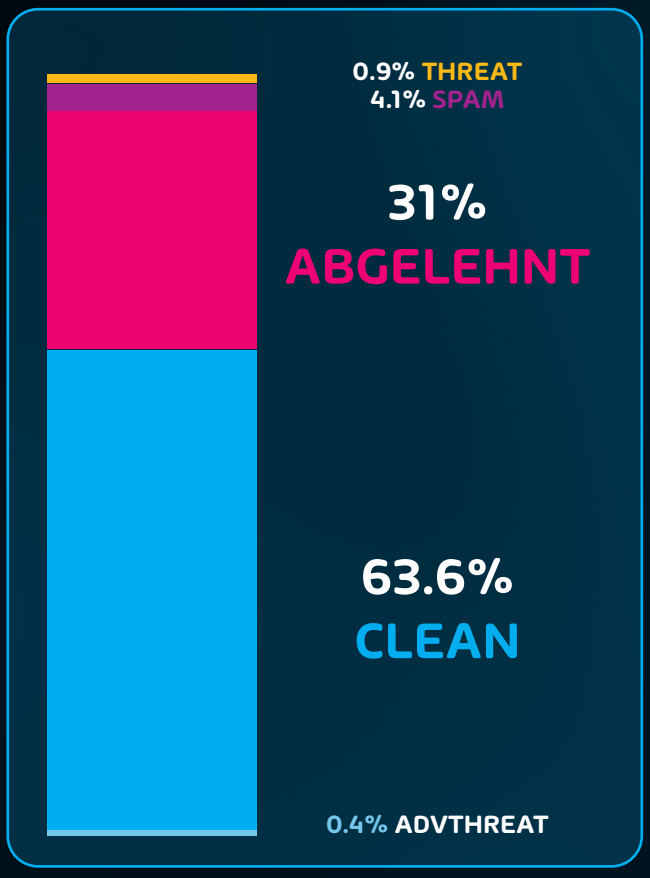


Fig. 6: Unerwünschte E-Mails zusammen mit sauberen E-Mails

Im Vergleich zum letzten Jahr, wo wir einen Wert von 40,5 % "unerwünschter" E-Mails verzeichneten, zeigt sich dieses Jahr ein Rückgang (wenn auch nur geringfügig) auf 36,4 %. Zu vermerken ist allerdings, dass wir in diesem Jahr 45 Milliarden E-Mails analysiert haben, im vergangenen Jahr waren es nur 25 Milliarden. Dennoch bleibt die aktuelle Bedrohung durch E-Mail-basierte Gefahren auf einem HOHEN Niveau.

Im Verlauf dieses Jahres ergab sich die Aufschlüsselung für unerwünschte E-Mails wie folgt:

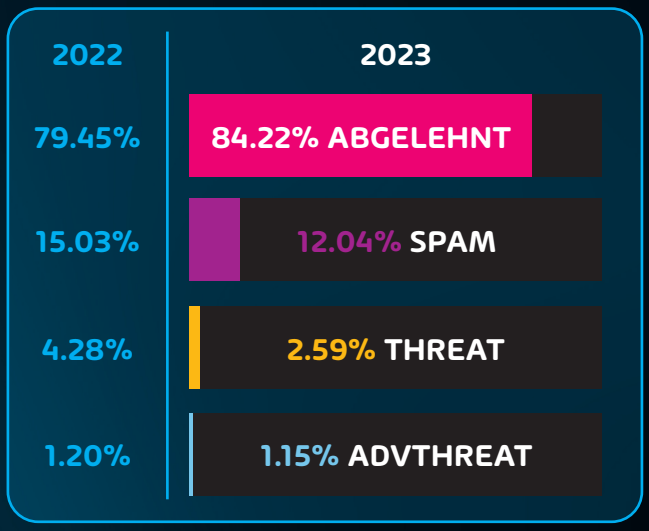


Fig. 7: 2023 - Unerwünschte E-Mails nach Kategorie

KATEGORIE	BESCHREIBUNG
AdvThreat	Diese E-Mails enthalten Bedrohungen, die von Hornetsecuritys Advanced Threat Protection erkannt wurden. Sie werden für illegale Zwecke eingesetzt und beinhalten ausgeklügelte technische Mittel, die nur mit fortschrittlichen dynamischen Verfahren abgewehrt werden können.
Content	Diese E-Mails haben einen ungültigen Anhang. Welche Anhänge ungültig sind, legen die Administratoren im Modul Content Control fest.
Abgelehnt	Diese E-Mails werden aufgrund externer Merkmale, die z. B. die Identität des Absenders betreffen können, im Laufe des SMTP-Dialogs direkt von unserem E-Mail-Server abgelehnt und nicht weiter analysiert.
Spam	Diese E-Mails sind unerwünscht und haben häufig einen werblichen oder betrügerischen Charakter. Die E-Mails werden gleichzeitig an eine große Anzahl von Empfängern verschickt.
Threat	Diese E-Mails enthalten gefährliche Inhalte wie z.B. bösartige Anhänge oder Links oder werden zur Begehung von Straftaten wie Phishing verschickt.

HINWEIS: Die Kategorie "Abgelehnt" bezieht sich auf E-Mails, die von den Hornetsecurity-Diensten während des SMTP-Dialogs aufgrund äußerer Merkmale, wie der Identität des Absenders oder der IP-Adresse, abgelehnt wurden. Wenn ein Absender bereits als kompromittiert erkannt wurde, erfolgt keine weitere Analyse. Der SMTP-Server blockiert die Verbindung bereits beim ersten Verbindungspunkt aufgrund der negativen Reputation der IP und der Identität des Absenders.

Verwendung von Angriffstechniken bei E-Mail-Angriffen

In unserer Datenanalyse haben wir folgende Aufschlüsselung der Angriffstypen beobachtet:

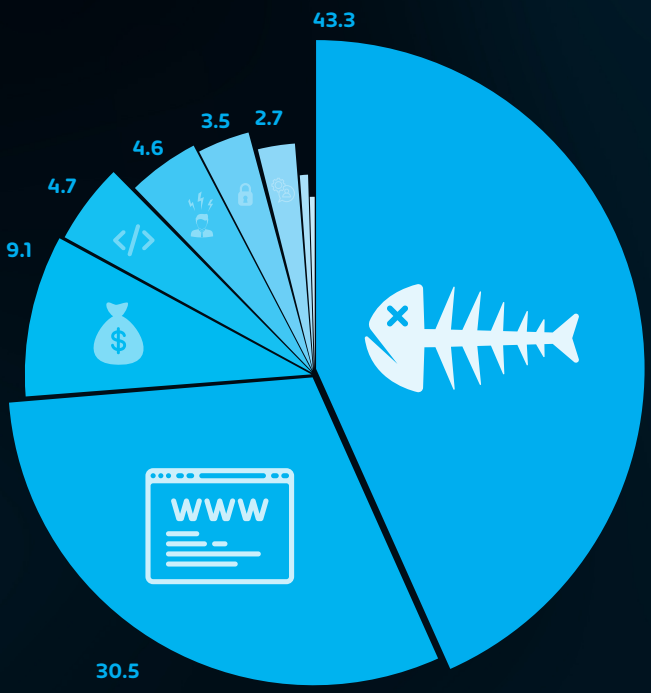


Fig. 8: Verwendung von Angriffstechniken bei E-Mail-Angriffen in 2023

Wenig überraschend nehmen Phishing und die Nutzung von bösartigen URLs nach wie vor einen Spitzenplatz ein und zählen zu den bevorzugten (und äußerst erfolgreichen) Angriffstypen. Ein Blick auf die Daten des letzten Jahres (siehe unten) ermöglicht interessante Vergleiche:

2022 %	2023 %	ANGRIFFSTECHNIK
39.6	43.3	Phishing
12.5	30.5	URL
8.2	9.1	Advanced-Fee Scam
1.8	4.7	HTML
3.7	4.6	Extortion
3.5	3.5	Exe. in Archive/Disk-Image
1.1	2.7	Impersonation
2.8	1.0	Maldoc
0.4	0.6	PDF

Fig. 9: Verwendung von Angriffstechniken bei E-Mail-Angriffen in 2022

Betrachtet man nur die Statistiken über die Verwendung bösartiger URLs und lässt alle anderen Angriffsarten außer Acht, so ergibt sich ein Anstieg von 144 % im Vergleich zum Vorjahreszeitraum. Das bedeutet, dass sich der Anteil an bösartigen URLs, die wir in E-Mail-Bedrohungen gesehen haben, im letzten Jahr mehr als verdoppelt hat.

Social Engineering und bedrohliche E-Mail-Techniken bleiben weiterhin eine der führenden Methoden, die Cyberkriminelle nutzen, um einen Zugang zu den Systemen ihrer Opfer zu erhalten. Zusätzlich haben wir eine Zunahme von Fällen beobachtet, in denen gezielt Nutzer durch Social Engineering dazu verleitet werden, mit einem bösartigen Link zu interagieren. Daher geht der Einsatz von schädlichen URLs mit dem allgemeinen Anstieg von Phishing einher.

Bei Angriffen verwendete Dateitypen

E-Mail-Anhänge bleiben auch im Jahr 2023 eine der am häufigsten genutzten Methoden zur Übermittlung von gefährlichen Payloads bei Angriffen. Angreifer setzen Anhänge weiterhin ein, um Malware zu verbergen und ihrer bösartigen Kommunikation den Anschein von Authentizität zu verleihen.

Zusätzlich können rudimentäre Spam-/Malware-Filter komprimierte Anhänge nicht durchgängig scannen, was die Erfolgschancen für Cyberkriminelle erhöht. Die Aufschlüsselung der verwendeten Dateitypen für die Bereitstellung bösartiger Payloads wird unten dargestellt:

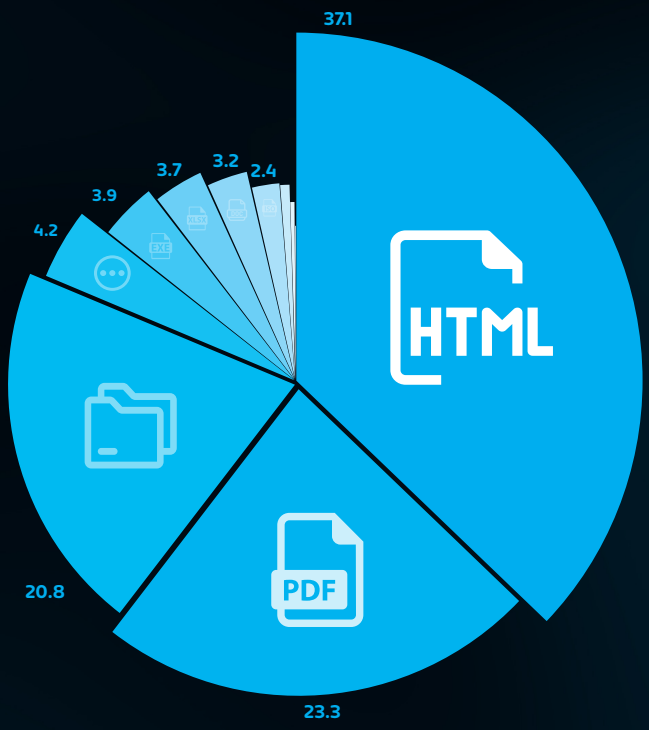
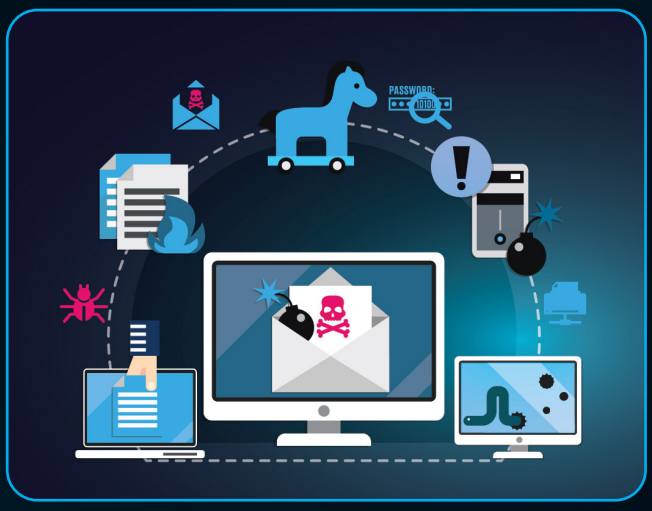


Fig. 10: Bei Angriffen verwendete Dateitypen in 2023

HTML-Dateien bleiben der bevorzugte Dateityp bei E-Mail-Angriffen. An zweiter Stelle steht PDF, gefolgt von Archiv-Dateien auf dem dritten Platz. Dass HTML an erster Stelle steht, überrascht nicht, da HTML-Dateien unabhängig vom Betriebssystem des Zielnutzers geöffnet werden können, was die Erfolgschancen für den Angreifer erhöht.



Vergleicht man diese Daten mit dem Vorjahr (wie unten dargestellt), fallen mehrere bemerkenswerte Unterschiede auf.

	2022	2023	
HTML	21.0	37.1	HTML
PDF	12.4	23.3	PDF
	28.0	20.8	ARCHIVE
	4.8	4.2	OTHER
EXE	4.3	3.9	EXECUTABLE
XLSX	10.4	3.7	EXCEL
DOC	12.7	3.2	WORD
ISO	5.4	2.4	DISK IMAGE FILES
	0.7	0.8	SCRIPT FILE
	0.0	0.4	ONENOTE
	0.1	0.1	EMAIL
LNK	0.1	0.0	LNK FILE
PPTX	<0.1	0.0	POWERPOINT

Fig. 11: Bei Angriffen verwendete Dateitypen in 2022 und 2023

Im vergangenen Jahr gab es einige Aktivitäten von Cyberkriminellen sowie Ereignisse in der Branche, die diese Veränderungen erklären können. Trotz seiner Zerschlagung durch weltweite Behörden im Sommer 2023, lässt sich der Anstieg von HTML- und PDF-Dateien teilweise auf Qakbot zurückführen. Qakbot zeigte im Verlauf dieses Jahres eine beachtliche Aktivität und bediente sich dabei sowohl an HTML als auch PDF-Dokumenten, um die Infektion von Zielrechnern voranzutreiben. Dieser Ansatz wird zweifellos auch in Zukunft ein bevorzugter Verbreitungsmechanismus für kommende Malware- und Botnetzbetreiber bleiben.

Der markante Rückgang bei der Verwendung von DOCX- und XLSX-Dateien im Vergleich zum Vorjahr ist auf Microsofts neue Praxis zurückzuführen, Makros in Office standardmäßig zu blockieren. Dies hat zur Folge, dass diese Dateitypen für Angreifer weniger attraktiv erscheinen.

E-Mail-Threat Index in unterschiedlichen Geschäftsbereichen

Einer der zentralen Aspekte, die wir jährlich (und monatlich) gründlich analysieren, ist die Anzahl der Bedrohungen, die auf verschiedene Industriezweige abzielen. Diese Untersuchung ermöglicht es uns, festzustellen, ob spezifische Kampagnen oder gezielte Angriffe auf bestimmte Unternehmen im Gange sind. Zugleich liefert sie wertvolle Erkenntnisse, die Unternehmen nutzen können, um festzustellen, ob sie einem erhöhten Angriffsrisiko ausgesetzt sind.

Die Daten des vergangenen Jahres zeigen, dass der Bedrohungsindex in allen Sektoren etwa gleich hoch war. Diese Erkenntnis untermauert die Schlussfolgerung, dass es unerheblich ist, in welchem Geschäftsbereich man tätig ist. Wenn Ihre Organisation in der Lage ist ein Lösegeld zu zahlen, sind Sie ein potenzielles Ziel. Die Daten für dieses Jahr (siehe unten) zeigen, dass dieser Trend weiterhin besteht. Der E-Mail-Threat Index bleibt weitgehend konstant, selbst unter den zehn wichtigsten Branchen.

Dennoch gab es einige Branchen, die etwas stärker ins Visier genommen wurden.

- **Forschungsbranche**: Forschungsorganisationen geraten oft ins Visier, nicht zuletzt aufgrund des geistigen Eigentums, wie etwa der Entwicklung neuer Medikamente.
- **Unterhaltungsbranche**: Organisationen dieser Art fallen typischerweise in die Bereiche Glücksspiel oder Ticketverkauf. Diese Unternehmen werden aufgrund der beträchtlichen Geldsummen, die im Spiel sind, zu bevorzugten Zielen. Ein Beispiel hierfür ist der Angriff auf MGM und Caesars Entertainment im Jahr 2023.

- **Produktion:** Die Fertigungsbranche hat eine lange Historie häufiger Angriffe von Cyberkriminellen. Dies ist oft auf das Abzielen geistigen Eigentums zurückzuführen. Viele sehen diesen Sektor als anfälliges Ziel für Ransomware und Produktionsstörungen, bedingt durch die Netzwerksicherheit und die Tatsache, dass hier oft eine große Anzahl unsicherer IoT-Geräte genutzt wird.

Die folgende Tabelle zeigt den E-Mail-Threat Index für die unterschiedlichen Branchen:

3.0	RESEARCH INDUSTRY
3.0	ENTERTAINMENT INDUSTRY
3.0	MANUFACTURING INDUSTRY
2.9	MEDIA INDUSTRY
2.9	HEALTHCARE INDUSTRY
2.7	TRANSPORT INDUSTRY
2.6	HOSPITALITY INDUSTRY
2.6	AUTOMOTIVE INDUSTRY
2.5	UTILITIES
2.5	INFORMATION TECHNOLOGY
2.5	EDUCATION INDUSTRY
2.4	UNKNOWN
2.4	CONSTRUCTION INDUSTRY
2.4	MINING AND METAL INDUSTRY
2.4	FINANCIAL INDUSTRY
2.4	AGRICULTURE INDUSTRY
2.3	PROFESSIONAL SERVICE
2.3	RETAIL INDUSTRY
2.2	REAL ESTATE INDUSTRY
1.8	LOGISTICS INDUSTRY
2.4	GLOBAL MEDIAN
99.3	GLOBAL MAXIMUM

Fig. 12: Jährlicher Branchenbedrohungsindex

ANMERKUNG: Der E-Mail-Threat Index wird durch die folgende Berechnung ermittelt:

Prozentualer Threat Index = Anzahl der bösartigen E-Mails / (Anzahl der bösartigen E-Mails + Anzahl der gültigen E-Mails) multipliziert mit 100 – ausgenommen Spam und Info-Mails

Anmerkung zur Methodik

Verschieden große Organisationen empfangen eine unterschiedliche Gesamtanzahl von E-Mails. Daher ermitteln wir den prozentualen Anteil bedrohlicher E-Mails im Verhältnis zu den bedrohlichen und unbedenklichen E-Mails jeder Organisation, um einen Vergleich zwischen den Organisationen zu ermöglichen. Im nächsten Schritt berechnen wir den Median dieser Prozentsätze für alle Organisationen innerhalb derselben Branche, um den abschließenden Bedrohungsindex für die Branche zu ermitteln.

Markenimitation

Auch im Jahr 2023 ist das Imitieren von Marken eine der häufigsten Angriffstechniken, die auf Endnutzer abzielen.

Im betrachteten Zeitraum setzen sich die bekannten Trends erfolgreich fort: DHL, Amazon und FedEx gehören weiterhin zu den Spitzenreitern. Dieser anhaltende Aufwärtstrend ist keine Neuigkeit. Die COVID-Pandemie trieb einen erheblichen Anstieg des Online-Shoppings voran und diese Gewohnheit hat sich seitdem fest in den Konsumgewohnheiten verankert. Diese Entwicklung bleibt den Angreifern nicht verborgen und wenn es ihnen gelingt, eine überzeugende Phishing-Nachricht mit Bezug zum Versand der Bestellung zum richtigen Zeitpunkt in das Postfach ihres Opfers zu senden, steigen ihre Erfolgsaussichten erheblich.

Ebenso bemerkenswert ist die Platzierung von Microsoft, LinkedIn und Netflix unter den Top 10. Die Tatsache, dass Microsoft hier vertreten ist, ist in erster Linie auf die Versuche zurückzuführen, Zugang zu den Anmeldedaten für Microsoft Cloud-Dienste zu erlangen, indem die derzeit beliebten Adversary-in-the-Middle-Angriffe mit Hilfe von Reverse-Proxy-Toolkits wie dem W3ll Phishing Kit durchgeführt werden. Diese Arten von Angriffen umgehen geschickt MFA-Schutzmaßnahmen und können sehr schwer zu erkennen sein.

Die Imitation der Marken LinkedIn und Netflix ist für Cyberkriminelle etwas komplexer. Kompromittierte LinkedIn-Konten verschaffen Angreifern Zugang zu umfangreichen Informationen über das betroffene Konto sowie über die Verbindungen des kompromittierten Kontos. Es gab auch Fälle, in denen Cyberkriminelle ein kompromittiertes LinkedIn-Konto nutzten, um letztendlich einen anderen LinkedIn-Nutzer anzugreifen, indem sie sich als vertrauenswürdige Geschäftskontakte ausgaben. Die Imitation der Netflix-Marke wird in erster Linie als Mittel gesehen, um Konten zu übernehmen und diese entweder zu verkaufen oder die gleichen Anmeldedaten in Credential-Stuffing-Angriffen zu verwenden.

Fig. 13: Top 10 der imitierten Marken im Jahr 2023

Hinweis: Die Daten zur Markenimitation werden maßgeblich von regionalen Unterschieden beeinflusst. Aufgrund unserer umfangreichen Kundenbasis in Deutschland finden sich hier mehrere deutsche Marken.

Datensicherheit in der Cloud

Wenn wir den Sicherheitszustand im Bereich Microsoft 365 betrachten, wird deutlich, dass dieses Thema weit über den Rahmen von E-Mails hinausgeht. M365 hat die Art und Weise, wie Organisationen ihre Geschäfte führen, grundlegend verändert und immer mehr Unternehmen dazu verleitet, auch die erweiterten Funktionen von M365 zu verwenden.

In den folgenden Abschnitten dieses Berichts werden zahlreiche Sicherheitsaspekte innerhalb der Microsoft Cloud-Services behandelt. Es ist jedoch ebenso wichtig, den Gesamtzustand der aktuellen Microsoft-Sicherheit zu betrachten. Ehrlicherweise präsentiert sich die Situation derzeit nicht optimal. Microsoft war in den letzten Jahren mit verschiedenen Sicherheitsvorfällen konfrontiert, darunter Sicherheitsverletzungen wie die Situation mit Storm-0558, mehrere Schwachstellen in lokalen Exchange Servern und der Vorfall mit dem Leck von 32 TB Daten aus einem Cloud-Speicherkonto.

Hinweis

Für eine umfassendere Diskussion zu aktuellen Sicherheitsproblemen in der Microsoft Cloud können Sie diese Podcast-Episode anhören, in der Andy Syrewicze und Paul Schnackenburg das Thema ausführlich besprechen.

Es ist nicht verwunderlich, dass viele in der Branche die Sicherheitskultur von Microsoft derzeit kritisch hinterfragen und das Thema "Lieferantenüberabhängigkeit" in den Fokus rücken.

Was bedeutet "Vendor Overdependence"?

"Vendor Overdependence", auch als "Lieferantenüberabhängigkeit" bekannt, bezieht sich auf eine Situation, in der ein Unternehmen zu stark von einem bestimmten Anbieter oder Lieferanten abhängig ist. Diese Abhängigkeit kann in verschiedenen Aspekten auftreten, einschließlich technologischer, logistischer oder finanzieller Abhängigkeiten. Das Problem bei dieser Konstellation besteht darin, dass bei Problemen seitens des Lieferanten das Geschäft unverhältnismäßig stark beeinträchtigt wird.

Einige Beispiele:

1. Offsite-Backups sind schon lange eine bewährte Praxis im IT-Bereich. Dies gilt auch für Daten, die in M365 gespeichert sind. Sich allein auf die Speicherfunktionen von M365 zu verlassen oder das Backup-Produkt von Microsoft (wenn es irgendwann veröffentlicht wird) zu nutzen, ist vergleichbar mit der Speicherung von Backups auf demselben Speicher/Plattform wie das Produktionssystem. Wenn die Microsoft-Cloud nicht verfügbar ist, sind möglicherweise auch die Methoden zur Datenwiederherstellung nicht zugänglich.
2. Die Größe und der Umfang der Microsoft Cloud machen sie zu einem Ziel für Cyberkriminelle. Angreifer wissen, dass das Überlisten der Exchange Online Protection eines einzelnen Kunden höchstwahrscheinlich bedeutet, dass mit der gleichen Methode ALLE M365-Kunden überlistet werden können. Hier zeigt sich, dass eine Sicherheitslösung von Drittanbietern oft überlegene Fähigkeiten im Vergleich zum nativen Anbieter bietet, insbesondere bei komplexen Angriffen.
3. Es mag selten vorkommen, aber es gab Fälle, in denen die Microsoft Cloud vorübergehend nicht verfügbar war. Insbesondere im letzten Jahr traten einige Ausfälle im Azure Active Directory (jetzt als Azure Entra bekannt) auf, die es Kunden erschwerten, auf ihre Daten in M365 zuzugreifen.

Microsoft hat derzeit einen äußerst großen Marktanteil mit Microsoft 365. Viele in der Branche stellen es in Frage, denselben Anbieter sowohl für Produktivitäts- und Kollaborationssoftware als auch für Sicherheitslösungen zu verwenden. Es besteht ein potenzieller Interessenkonflikt, da im Falle eines Ausfalls oder eines Problems mit einem Sicherheitsprodukt dieses Anbieters die Gefahr besteht, dass solche Probleme nicht angemessen offengelegt oder behoben werden, um das Risiko des Verlusts von Geschäften im Bereich Produktivität und Kollaboration zu minimieren.

Organisationen stehen somit vor der Herausforderung, individuelle Entscheidungen in dieser Angelegenheit zu treffen. Angesichts aktueller Sicherheitsbedenken und der Frage, bis zu welchem Punkt Microsoft für die Sicherheit der Daten verantwortlich ist, gewinnt die Notwendigkeit individueller Lösungen immer mehr an Bedeutung.

Was fällt unter die Verantwortung von Microsoft?

Viele stellen sich die Frage: "Wenn sich Microsoft nicht um meine Daten und Sicherheit kümmert, wofür sind sie dann überhaupt verantwortlich?" Die aktuelle Haltung von Microsoft zu dieser Frage hat sich im Jahr 2023 nicht verändert. Um dies vollständig zu verstehen, ist es hilfreich, das Modell der Gemeinsamen Verantwortung von Microsoft zu kennen.

Der wichtigste Punkt dieses Modells besagt, dass die Verantwortung für folgende Aspekte beim Kunden liegt:

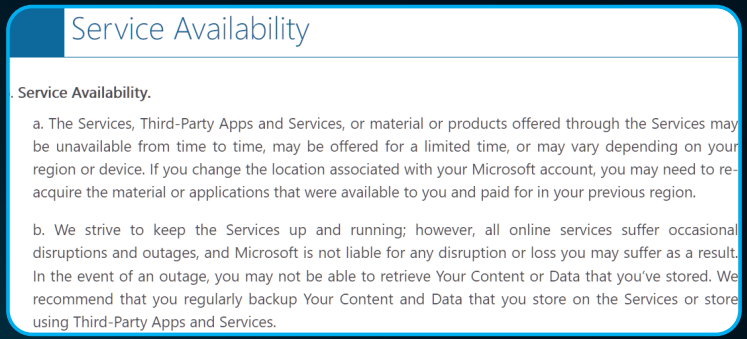
- Informationen und Daten
- Geräte (Mobilgeräte und PCs)
- Konten und Identitäten

Es liegt also grundsätzlich in der Verantwortung des Kunden, seine Informationen und Daten zu sichern und zu schützen. Microsoft übernimmt diese Aufgabe nicht. Wenn Organisationen in die Cloud wechseln, müssen sie dies berücksichtigen.

Trotz dieser langjährigen Positionierung hat Microsoft im Jahr 2023 auf einer Konferenz eine bemerkenswerte Änderung in Bezug auf die Verwendung von Backup-Anwendungen mit M365 bekanntgegeben. Mit Microsoft 365 Backup wurde ein Service vorgestellt, der grundlegende Backup-Funktionen für M365 bereitstellt. Interessanterweise wurde seit dieser Ankündigung nur sehr wenig bis gar keine zusätzliche Information veröffentlicht. Das Wesentliche an dieser Ankündigung liegt nicht nur im Service selbst, sondern in der Veränderung von Microsofts bisherigem Standpunkt, der besagte, es sei nicht notwendig, Daten im M365 zu sichern. Viele Experten in der Branche sehen dies als Ergebnis einer von zwei möglichen Ursachen:

1. Microsoft hat schließlich nachgegeben und stimmt nun zu, dass allein der Fokus auf die Datenspeicherung in M365 nicht ausreicht.
2. Microsoft möchte einen Teil des M365-Backup-Marktes abbekommen, nachdem sie erkannt haben, dass es eine hohe Nachfrage nach einem solchen Service gibt.

Beide Optionen erscheinen wahrscheinlich, wobei die zweite Option durch die Tatsache gestärkt wird, dass Microsoft auch eine Backup-API für Anbieter veröffentlicht hat, die gegen Gebühr genutzt werden kann. Dennoch ist die Kernbotschaft klarer denn je: Unternehmen tragen die Verantwortung für den Schutz aller Daten, die sie in den Microsoft Cloud-Services platzieren.



Service Availability

. Service Availability.

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.

Die Herausforderungen einer effektiven Berechtigungsverwaltung in M365

Die Verwaltung von Freigabeberechtigungen in SharePoint und OneDrive for Business ist eine besonders anspruchsvolle Aufgabe für die IT. In der heutigen Geschäftswelt arbeiten kollaborative virtuelle Teams oft in verschiedenen Unternehmen und tauschen Dokumente auf unterschiedliche Weise aus. Eine restriktive Verwaltung dieser Prozesse ist nicht praktikabel, da sie Benutzer dazu verleiten könnte, nicht autorisierte Formen des Dokumentenaustauschs in der Cloud zu nutzen und die Transparenz der IT zu beeinträchtigen. Auf der anderen Seite ist es auch nicht ratsam, die Tür weit offen zu lassen, so dass Links zu sensiblen Daten unkontrolliert weitergegeben werden könnten. Die integrierten Tools zur Verwaltung dieser Aspekte in Microsoft 365 sind über verschiedene Portale fragmentiert und in großem Umfang schwer zu handhaben. Dies macht das Berechtigungsmanagement in der Microsoft Cloud zu einem wichtigen Thema für die Sicherheit in M365. In diesem Zusammenhang erleichtert der einzigartige 365 Permission Manager von Hornetsecurity die Verwaltung von Freigaberichtlinien über Tausende von Konten hinweg. Mit dieser Lösung kann nicht nur kontrolliert werden, wer Zugriff auf welche Ressourcen hat, sondern auch der Zugriff auf verschiedene Sites kann an die Risikomanagementrichtlinien des Unternehmens angepasst werden.

Kapitel 3 – Eine Analyse der größten Sicherheitsvorfälle und Cybersecurity-Nachrichten von 2023

Im Verlauf des Jahres 2023 traten mehrere bedeutende Angriffe und Sicherheitsbedenken auf, die direkt mit den für diesen Bericht gesammelten Daten in Verbindung stehen. Dieser Abschnitt widmet sich speziell diesen Angriffen.

Storm-0558

In den letzten 12 Monaten gab es mehrere aufsehenerregende Sicherheitsvorfälle, die den Cloud-Dienst Microsoft 365 betrafen, aber der folgenreichste war sicherlich der Angriff von Storm-0558. Zusammenfassend lässt sich sagen, dass die chinesische staatlich geförderte Hackergruppe, die Microsoft als Storm-0558 bezeichnet, im Jahr 2021 das Konto eines Ingenieurs kompromittierte. Obwohl die Produktionsumgebung vom Unternehmensnetzwerk isoliert war, stürzte im April 2021 ein Consumer Signing System (Teil von Azure AD, jetzt Entra ID) ab und erzeugte einen Crash Dump. Dieser wurde zur Fehlersuche in das Produktionsnetzwerk verschoben und das automatisierte System, das die Zugangsdaten in den Dumps erkennen sollte, versagte. Als die Angreifer also in dieses eine Konto eindrangen, erhielten sie Zugriff auf den Dump und den Schlüssel.

Dies stellt möglicherweise die schwerwiegendste Cloud-Sicherheitsverletzung aller Zeiten dar, die die Identitätsplattform in einer Weise kompromittiert hat, die das Vertrauen in die Cloud und in die Plattform(en) von Microsoft eindeutig untergräbt. Das Erkennen dieser bösartigen Aktivität war äußerst schwierig. Erst im Juni 2023 entdeckte ein Sicherheitsanalyst bei einer US-Bundesbehörde verdächtige „MailItemsAccessed"-Ereignisse und meldete dies umgehend an Microsoft und die CISA (Cybersecurity and Infrastructure Security Agency). Diese Behörde hatte Zugriff auf diese Protokolle, weil sie für die hochwertigste M365-Lizenz-SKU von Microsoft, E5, zahlten.

Diese Sicherheitsverletzung hatte folgende Auswirkungen: Microsoft hat endlich seinen Ansatz für die Verfügbarkeit von Protokollen für verschiedene Lizenzstufen geändert, und alle SKUs für Unternehmen haben jetzt erweiterten Zugriff auf Protokolle.

Diese Änderung wurde erstmals im Jahr 2020 nach dem Solarwinds-Angriff gefordert. Darüber hinaus wird sich der nächste Bericht des US Cyber Security Review Board (CSRB) auf diese Sicherheitsverletzung konzentrieren. Es bleibt abzuwarten, inwieweit diese Verletzung Microsoft zu einer kritischen Bestandsaufnahme und Verbesserung seiner allgemeinen Sicherheitsstrategie veranlassen wird.

nOAuth

Eine weitere Sicherheitslücke namens nOAuth nutzte die häufige Verwendung von E-Mail-Konten als Identifikator und in Entra ID (ehemals Azure AD) registrierte Anwendungen, die Anmeldungen mit Verbraucherkonten ermöglichten, aus. Microsoft warnt zwar ausdrücklich vor der Verwendung von E-Mail als Identifikator in diesen Fällen, aber das schmälert nicht die Komplexität und die Risiken, die mit der Registrierung von mandantenfähigen Anwendungen in Azure verbunden sind.

Die Cyberangriffe auf MGM / Caesars Entertainment

Die Cyberangriffe auf die Casinos von MGM und Caesars Entertainment gehören zu den bedeutendsten Sicherheitsverletzungen der letzten Monate. Obwohl die Angriffe unterschiedliche Symptome aufwiesen, enthalten sie dennoch wichtige Lektionen für den Schutz Ihres Unternehmens. Im Fall von MGM nutzte ein Angreifer von der Gruppe Scattered Spider in einem Telefonat Social Engineering, um einen Mitarbeiter des Helpdesks zu täuschen und alle MFA-Methoden für das Okta-Superadministrator-Konto zurückzusetzen. Dies ermöglichte es dem Angreifer, eine föderierte Identitätsverwaltung einzurichten und sich als Benutzer auszugeben. Nach der Kompromittierung wurden angeblich 6 TB Daten entwendet, und Unternehmensdaten wurden dann in einem Ransomware-Angriff verschlüsselt.

MGM entschied sich kein Lösegeld zu zahlen und berichtet, dass die Gesamtkosten für sie voraussichtlich 100 Millionen US-Dollar betragen werden. Offenbar verfügen sie über eine Cybersicherheitsversicherung mit einer Deckung von bis zu 200 Millionen US-Dollar. Während sie an der Wiederherstellung arbeiteten, kam es zu umfangreichen Systemausfällen und die Rufschädigung dürfte wahrscheinlich weit über die finanziellen Auswirkungen hinausgehen, insbesondere da die Angreifer sensible Daten aus Kundeninteraktionen vor März 2019 erbeuteten.

Caesars wurde durch eine Sicherheitslücke bei einem externen IT-Dienstleister kompromittiert und entschied sich für die Zahlung des Lösegelds (ursprünglich forderten die Angreifer 30 Millionen US-Dollar, aber dies wurde auf 15 Millionen US-Dollar heruntergehandelt). Aus diesen Angriffen lassen sich einige Lehren für die Verbesserung der Cyber-Resilienz Ihres Unternehmens ziehen:

- Wäre Ihr Helpdesk-Personal aufmerksam genug, um diesen Angriff frühzeitig zu erkennen? Sensibilisieren Sie Ihre Nutzer darauf, alle potenziellen Angriffswege im Blick zu haben, nicht nur bei Phishing-E-Mails. Vishing („Voice Phishing“) erweist sich als wirkungsvoller als einfache E-Mails, insbesondere weil die benötigten persönlichen Details zur Imitation oft öffentlich auf Plattformen wie LinkedIn, Facebook und Unternehmenswebsites verfügbar sind. Auch Qishing (QR-Code-Phishing) gewinnt an Beliebtheit.

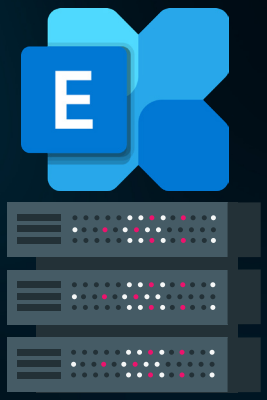
- Verhindern Sie, dass Ihr Helpdesk-Personal MFA und Passwörter für hochprivilegierte Konten zurücksetzen kann. Die Sicherheit Ihrer Authentifizierung steht und fällt mit den Reset-Methoden. Wenn es jemandem gelingt, einen Helpdesk-Mitarbeiter zu täuschen und MFA-Methoden hinzuzufügen oder zurückzusetzen, kann dies das Ende für die Sicherheit bedeuten.

- Überwachen Sie das Hinzufügen von föderierten Organisationen zu Ihrem IdP (Identity Provider), sei es Okta, Ping, Entra ID in Microsoft 365 oder Google, und schlagen Sie Alarm. Dieser Vektor wurde von den Angreifern des Solarwinds-Angriffs im Jahr 2020 verwendet und ist nach wie vor beliebt.

- Verlangen Sie von Ihren Drittanbietern einen Nachweis über ihre Widerstandsfähigkeit im Bereich der Cybersicherheit. Moderne Unternehmen sind miteinander vernetzt. Selbst wenn Ihre Mitarbeiter alles richtig machen, kann es sein, dass Sie aufgrund mangelnder Sicherheitsvorkehrungen eines vertrauenswürdigen Dienstleisters zu Schaden kommen.

Microsoft Exchange-Schwachstellen

Trotz des zunehmenden Trends zur Nutzung von Microsoft 365 setzen einige Organisationen nach wie vor auf lokale Exchange-Server, oft in einer hybriden Konfiguration. Bedauerlicherweise bleiben diese Server ein bevorzugtes Ziel für Angreifer. Im Jahr 2021 traten Probleme wie ProxyShell auf, gefolgt von ProxyNotShell im Jahr 2022. Schließlich wurden im August 2023 Patches für drei Schwachstellen zur Remote-Code-Ausführung veröffentlicht. Diese Zeitreise durch die Herausforderungen zeigt, dass es im Jahr 2021 insgesamt 31 Exchange Server-Schwachstellen gab, gefolgt von 18 im Jahr 2022 und bisher 23 im Jahr 2023.



JAHR	EXCHANGE-SERVER-SCHWACHSTELLEN
2023	23 bis jetzt
2022	18
2021	31

Fig. 14: Exchange-Server-Schwachstellen

In Anbetracht dieser fortwährenden Bedrohungen weisen wir dringend darauf-hin, die lokal betriebenen Exchange Server außer Dienst zu stellen und die Migration zu Exchange Online so rasch wie möglich abzuschließen. Diese proaktive Maßnahme wird nicht nur die Sicherheit Ihrer Infrastruktur stärken, sondern auch eine solide Grundlage für zukünftige Herausforderungen schaffen.

Die Zerschlagung von Qakbot

Qakbot war ein bekanntes bösartiges Botnetz, das über einen beträchtlichen Zeitraum von Cyberkriminellen verwendet wurde. Es zeichnete sich durch unzählige Angriffe im gesamten Internet aus und erfuhr ausgiebige Berichterstattung in der Cybersecurity-Medienlandschaft sowie durch Sicherheitsforscher – und natürlich auch durch unser Team!

Im August dieses Jahres gelang es dem FBI in Zusammenarbeit mit Strafverfolgungsbehörden weltweit, die Kontrolle über Qakbot zu übernehmen und das Botnetz erfolgreich stillzulegen. Diese Errungenschaft ist zweifellos positiv, hinterlässt jedoch auch eine Art Vakuum. Die Cyberkriminellen, die zuvor mit Qakbot in Verbindung standen, werden ihre Angriffe nicht einfach aufgeben. Sie werden entweder daran arbeiten, Qakbot zurückzubringen, oder sie werden sich anderen Tools zuwenden. Wie wir in einer Episode des Security Swarm Podcasts besprochen haben, scheint die Malware DarkGate ein möglicher Anwärter zu sein, um die entstandene Lücke zu füllen. Sicherheitsteams müssen wachsam bleiben und sowohl nach dieser Malware als auch nach anderen potenziellen Bedrohungen im Laufe von 2024 Ausschau halten.

Der MOVEit Supply-Chain-Angriff

Ein Jahr in der Welt der Cybersecurity-News OHNE bedeutende Supply-Chain-Angriffe wäre undenkbar, und so bildete 2023 keine Ausnahme. Unter den verschiedenen Vorfällen stach der MOVEit Supply-Chain-Angriff als besonders schwerwiegend heraus. MOVEit ist eine weitverbreitete Softwareanwendung, die Dateiübertragungsdienste für zahlreiche Unternehmen weltweit bereitstellt. Der Angriff nutzte mehrere Schwachstellen, vor allem SQL-Injektionsschwachstellen, im MOVEit-Code aus und wurde dazu verwendet, die persönlichen Informationen unzähliger Opfer zu stehlen. Unter den Betroffenen befanden sich Organisationen wie die BBC, das US Department of Energy, American Airlines und andere.

Diese Art von Angriffen macht deutlich, wie wichtig effektive und flexible Patching-Prozesse in den IT-Abteilungen von Unternehmen sind. Trotz der Bereitstellung von Maßnahmen und Patches blieben viele Organisationen über einen zu langen Zeitraum anfällig für derartige Angriffe. Die Sicherheitsbranche und Softwareanbieter setzen sich kontinuierlich dafür ein, Lösungen zu entwickeln, um die Auswirkungen künftiger Supply-Chain-Angriffe zu minimieren.

Haben sich unsere Vorhersagen vom letzten Jahr bestätigt?

In unserem Cyber Security Report des vergangenen Jahres haben wir Prognosen über die Art der Angriffe für 2023 erstellt und lagen damit größtenteils richtig.

Einige kriminelle Gruppen haben ihre Angriffe auf Regierungsziele in der südlichen Hemisphäre verlagert. Im Jahr 2022 waren Costa Rica, Ecuador und Chile betroffen, gefolgt von Brasilien, Bermuda und Kolumbien im Jahr 2023. Nicht zu vergessen sind zahlreiche Ziele in der Region Ostasien. Obwohl wir erwartet haben, dass der "Business E-Mail Compromise" Ransomware als den beliebtesten Angriffsvektor ablösen würde, zeigt sich, dass das "Geschäft" mit Ransomware nach wie vor florierend ist. Es steuert auf sein insgesamt zweithöchstes Einkommensjahr in 2023 zu, mit etwa 900 Millionen US-Dollar (nach 939 Millionen US-Dollar im Jahr 2021).

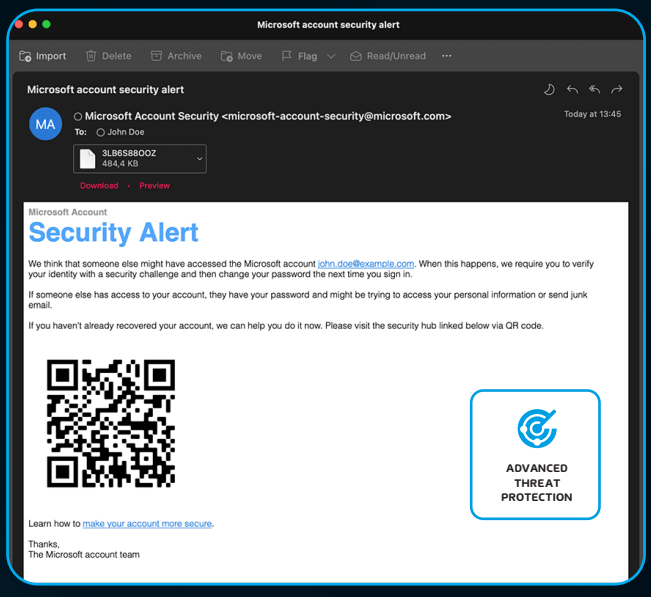
Die Tricks, um Multi-Faktor-Authentifizierungen (MFA) zu umgehen, werden immer ausgeklügelter und einfacher, genau wie wir es vorhergesagt haben. Das liegt daran, dass immer mehr Unternehmen MFA verwenden, um Identitäten zu schützen. Wir haben festgestellt, dass geschäftstüchtige Angreifer die externen Nachrichten von Teams als Köder für Phishing nutzen. Viele Nutzer sind sich dieses Vektors nicht bewusst, aber der neue Teams-Client, der nicht in Electron integriert ist, wird zumindest den Client sicherer machen.

Diebstähle von Tokens von kompromittierten Rechnern und ihre erneute Verwendung in weiteren Angriffen haben zugenommen, genauso wie insgesamt der Cookie-Raub zur Unterstützung des Identitätsdiebstahls, verkörpert durch die Zerschlagung des Genesis-Marktplatzes durch das FBI im April 2023 in der Operation Cookie Monster.

Wir haben uns auch mit mobiler Spionagesoftware und ihrer Bedeutung befasst. Predator und Pegasus werden von verschiedenen Nationen eingesetzt, nicht nur um Kriminelle auszuspionieren, sondern auch Dissidenten, politische Gegner und Journalisten (Griechenland ist ein Beispiel dafür).

Microsoft 365 als Plattform ist nicht weniger komplex geworden, was die sichere Konfiguration angeht. Wie von uns vorhergesagt, verkürzt sich die Zeitspanne zwischen der öffentlichen Bekanntgabe einer Sicherheitslücke und der Bereitstellung eines Exploit-Codes stetig, sodass SOC-Teams kaum noch mithalten können.

Information Operations (IO) und Desinformation stellen zunehmend eine Bedrohung für Unternehmen und die Gesellschaft im Allgemeinen dar. Ein auffälliges Beispiel ist die mangelnde Inhaltsmoderation bei X (ehemals Twitter) unter der neuen Leitung. Gleichzeitig machen Plattformen wie ChatGPT und andere große generative KI (Large Language Model) es einfacher als je zuvor, Desinformationen im großen Stil zu verbreiten.



Eine "Vorhersage", die nicht im letzten Cyber Security Report besprochen wurde, aber sich als besonders wichtig herausgestellt hat, ist die Integration von QR-Code-Phishing in Hornetsecuritys Advanced Threat Protection-Plattform. In den letzten Monaten hat dieser Angriffsvektor erheblich zugenommen, und andere E-Mail-Sicherheitslösungen hatten Schwierigkeiten, Endnutzer vor schädlichen Links in QR-Codes zu schützen.

Zusätzlich haben sich unsere Vorhersagen bezüglich des Aufkommens von passwortlosen Lösungen als richtig erwiesen, auch wenn wir nicht erwartet hatten, dass Passkeys im Verbraucherumfeld so populär werden würden.

Die Angriffe auf APIs nehmen ebenfalls rapide zu, wie wir im letzten Bericht feststellten. Das ist ein Bereich, dem Sicherheitsteams besondere Aufmerksamkeit schenken müssen, da er oft im "Hintergrund, als Teil der Infrastruktur" agiert und wenig Überwachung erhält. Ein Beispiel dafür ist der Sicherheitsvorfall bei Optus in Australien Ende 2022, bei dem 10 Millionen Kunden betroffen waren, aber es gibt noch viele andere.

Die Prognosen des Security Labs für 2024

Jedes Jahr untersucht das Security Lab von Hornetsecurity im Rahmen dieses Berichts den Stand der Branche, unsere Daten, Angriffstrends und vieles mehr, um eine Reihe von Prognosen für das kommende Jahr zu erstellen.

Dies dient dazu, Unternehmen darüber zu informieren, vor welchen potenziellen Bedrohungen sie im kommenden Jahr stehen könnten, und wie sich die Branche voraussichtlich verändern wird. Im Folgenden präsentieren wir die Vorhersagen des Security Lab für 2024.

KI wird die Cybersecurity-Branche weiter vorantreiben

Die Einführung von ChatGPT von OpenAI Ende 2022 und seine zunehmenden Popularität Anfang 2023 haben die Welt der generativen KI grundlegend verändert. Es wird immer offensichtlicher, dass selbst weniger erfahrene Angreifer generative KI nicht nur für Angriffe nutzen können, sondern sogar lernen können, WIE man solche Angriffe durchführt. Tatsächlich haben wir im Security Lab eigene Forschung zu diesem Thema betrieben und einige unserer Erkenntnisse in der allerersten Episode des Security Swarm Podcast geteilt.

Diese neuen Möglichkeiten führten zu einem Anstieg von Cyberangriffen im Verlauf des Jahres und verschärften die Besorgnis um ein Vielfaches. Eine gute Nachricht gibt es jedoch in Bezug auf die Nutzung generativer KI durch Cyberkriminelle.

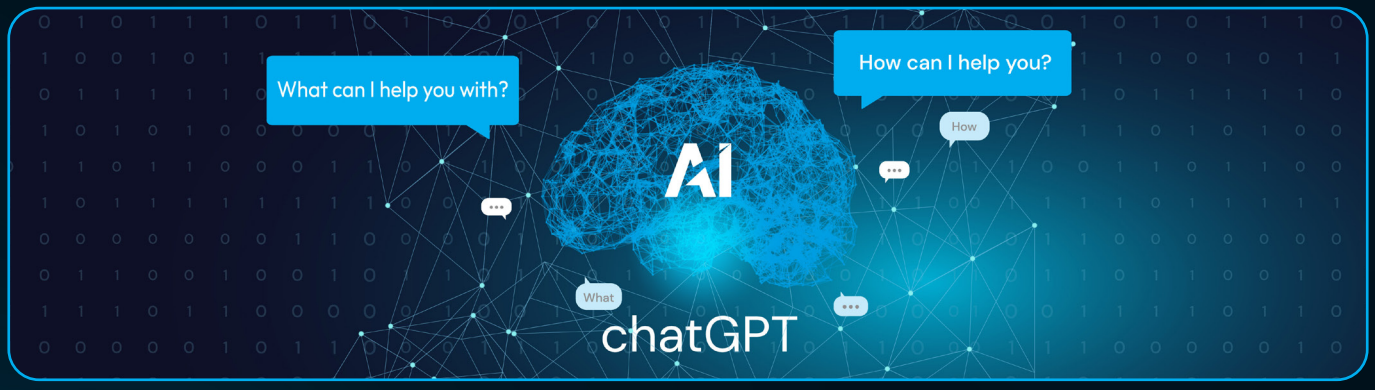
Tatsache ist, dass erfahrene Angreifer bereits über diese Fähigkeiten verfügen. Das bedeutet, dass unerfahrene Angreifer, die Tools wie ChatGPT für Angriffe nutzen wollen, immer noch viel Zeit investieren müssen, um die gesamte Angriffskette für einen bestimmten Angriff zu verstehen. Generative KI kann das nicht automatisch für sie erledigen.

Dennoch gehen wir davon aus, dass Angreifer im kommenden Jahr weiterhin ihre Darkweb-Varianten von ChatGPT (wie DarkBERT und WormGPT) weiter entwickeln werden, um zusätzliche Teile der Angriffskette besser zu verstehen und zu automatisieren. Dies wird die Fähigkeiten für unerfahrene Angreifer erweitern und die Geschwindigkeit von Cyberangriffen in der Branche erhöhen. Die Fähigkeit von LLMs, Texte glaubwürdig in andere Sprachen zu übersetzen, eröffnet Kriminellen auch „neue Märkte", zumal viele dieser Länder kulturell nicht so an Phishing-Angriffe gewöhnt sind.

Darüber hinaus haben wir bisher noch keine groß angelegten Angriffe von Cyberkriminellen GEGEN einen generativen KI-Dienst gesehen. Ein solcher Angriff würde höchstwahrscheinlich subtil und heimlich durchgeführt werden, mit dem Ziel, die Antworten der KI zu manipulieren, um gezielt Fehlinformationen zu verbreiten. Ein derartiger Angriff wäre äußerst anspruchsvoll und wahrscheinlich eher staatlich gesteuert, wenn es überhaupt so weit kommen sollte.

Während sich die Berichterstattung in der Cybersecurity-Welt fast ausschließlich auf die negativen Auswirkungen von generativer KI konzentriert hat, gibt es auch positive Entwicklungen. Während das Wettrüsten im Bereich der Cybersicherheit weitergeht, setzen Sicherheitsexperten und Anbieter generative KI auch für die Verteidigung ein. Es gibt sogar Initiativen von KI-Organisationen wie OpenAI, die spezielle Förderprogramme ins Leben gerufen haben, um Cybersecurity-Unternehmen bei der „KI-Fähigkeit" ihrer Angebote zu unterstützen. Unsere Vorhersage ist, dass sich dies auf verschiedene Arten zeigen wird - von der Verwendung von KI für die Erkennung von Ausreißern, Log-Analyse, simulierte Angriffe (siehe unten) bis hin zu der Modellierung von Bedrohungen und mehr.

Unternehmen werden sich über diese Entwicklungen auf dem Laufenden halten und im kommenden Jahr ihre Sicherheitsstrategie entsprechend anpassen müssen.



LLM (Large Language Model) Sparring-Partner für Blue Teams

Diese Prognose schließt sich zwar der vorherigen Diskussion über generative KI an, ist jedoch so faszinierend, dass sie einen eigenen Abschnitt verdient.

Eine Sache, die für Blue Teams bisher immer schwierig war, ist die präzise Simulation von Cyberkriminellen. Natürlich könnten Sie eine externe Organisation beauftragen oder einen eigenen Penetrationstester einstellen, aber deren Sicht auf die Zielumgebung könnte durch vorheriges Wissen beeinträchtigt sein. Auch die Kosten könnten ein Problem darstellen.

Und genau dies ist ein Bereich, in dem Large Language Models (LLMs) eine wichtige Rolle bei Sicherheitsoperationen spielen könnten. Ein KI-simulierter Angreifer könnte mehrere Angriffssimulationen gegen Ihr Unternehmen durchführen. Das spielt nicht nur eine wichtige Rolle beim Auffinden unbekannter Schwachstellen in Ihrer Infrastruktur, sondern dient auch dazu, Teammitglieder darin zu schulen, richtig auf Angriffe zu reagieren.

Wir gehen daher davon aus, dass Large Language Models (LLMs) vermehrt in neuen Softwarelösungen eingesetzt werden, um diesen Bedarf zu decken.

Technologien wie Co-Pilot werden die Nachfrage nach erhöhter Code-Sicherheit und Code-Qualitäts-Scans vorantreiben

Eine weitere Prognose im Zusammenhang mit künstlicher Intelligenz, aber eine wichtige: Tools wie Co-Pilot vereinfachen das Programmieren erheblich. Sie stellen jedoch ein grundlegendes Problem dar, denn wenn viele Programmierer Code verwenden, der mit Co-Pilot generiert wurde, besteht die Möglichkeit, dass ähnlicher Code über verschiedene Entwicklungen hinweg entsteht. Was passiert, wenn ein Dienst wie Co-Pilot Opfer eines sogenannten LLM-Poisoning-Angriffs wird? Könnten Angreifer Co-Pilot als Grundlage nutzen, um zu verstehen, wie ihre Opfer Anwendungen erstellen?

Wie können Organisationen sicherstellen,

1. dass der von Co-Pilot generierte Code einzigartig ist und keine rechtlichen Probleme verursacht?
2. dass der Code sowohl einzigartig als auch sicher ist, um nicht zu einem leichten Ziel für Cyberkriminelle zu werden?
3. dass der von KI-Tools generierte Code frei von schädlichem Code ist?
4. dass die notwendigen Prozesse für angemessene Code-Reviews im Zusammenhang mit solchen Tools umgesetzt werden, um die vorherigen Punkte zu adressieren?

Wir gehen davon aus, dass all diese Anliegen im kommenden Jahr die Notwendigkeit für verbesserte Prozesse zur Sicherung und Qualitätsprüfung von Code verstärken werden.

MFA-Bypass-Angriffe werden zunehmen

Die Angriffe zur Umgehung der Mehrfaktorauthentifizierung werden voraussichtlich sowohl in ihrer Häufigkeit als auch in ihrer Raffinesse zunehmen. Unternehmen setzen vermehrt auf sicherere Authentifizierungsmethoden, um sich von den anfälligeren Benutzernamen und Passwörtern zu distanzieren, und die Angreifer passen sich entsprechend an. Es sind eine Reihe von „MFA-Bypass-Kits" aufgetaucht, die den Prozess der Einrichtung eines Proxys vereinfachen, um als „Attacker-in-the-Middle" zu agieren. Hierbei wird dem Benutzer eine überzeugende Anmeldeseite präsentiert. Sobald die Anmeldedaten eingegeben werden (einschließlich einer MFA-Abfrage), werden diese an die echte Anmeldeseite weitergeleitet, so dass sich der Benutzer beim legitimen Dienst anmeldet. Währenddessen fängt das Kit eine Kopie der Sitzungscookies ab, sodass sich der Angreifer als der Benutzer ausgeben kann. Beispiele für solche Kits sind Evilginx (Open Source) sowie das W3LL-Panel und die damit verbundenen Tools zur Erleichterung von Business Email Compromise. Die verschiedenen MFA-Technologien haben unterschiedliche Stärken. Stellen Sie sicher, dass Ihr Unternehmen die stärksten Technologien für den Zugriff auf sensible Daten und Anwendungen nutzt.

XDR- und MDR-Einsatz nimmt zu

Die Nachfrage nach erhöhter Sicherheit nimmt weiter zu und als Reaktion darauf erwarten wir, dass XDR (Extended Detection and Response) und MDR (Managed Detection and Response) Lösungen in allen Bereichen verstärkt eingesetzt werden. Da Cyberbedrohungen allgegenwärtig sind, reicht keine Einzellösung aus. Unternehmen sollten einen mehrschichtigen Ansatz verfolgen. Dazu gehört auch die ordnungsgemäße Protokollierung und Weitergabe von Sicherheitsvorfällen über das gesamte digitale Vermögen eines Unternehmens. Ohne eine angemessene Transparenz bleiben viele Angriffe unbemerkt, weshalb CISOs und Technologieverantwortliche verstärkt daraufsetzen, dem Grad ihrer Sicherheitstransparenz Priorität einzuräumen.

Zunahme von Angriffen auf Lieferketten

Angriffe auf Lieferketten sind in unserer Branche nichts Neues. In jüngster Zeit gab es mehrere Angriffe auf Lieferketten, darunter ein Angriff im März 2023, bei dem 3CX betroffen war, sowie der bekannte MOVEit-Angriff im Sommer 2023. Das Problem bei dieser Art von Angriff ist das potenzielle Ausmaß der Auswirkungen. Beide oben erwähnten Fälle haben unzählige Organisationen und die privaten Daten von Millionen von Menschen gefährdet.

In dem Maße, in dem digitale Services in unsere Gesellschaft Einzug halten, werden sie immer weitreichender und letztlich auch zu einem attraktiveren Ziel für Cyberkriminelle. Angreifer wissen, dass sie, wenn sie einen Anbieter solcher Dienste hacken können, wahrscheinlich ein beträchtliches Lösegeld erhalten. Sie können nicht nur Lösegeld für die Daten erpressen, sondern viele werden die gestohlenen Daten auch in einer

doppelten Erpressungskampagne im Darknet verkaufen. Das ist jedoch nicht das einzige Risiko. Im Fall des MOVEit-Angriffs auf die Lieferkette ermöglichte die Schwachstelle den Angreifern einfachen Zugang zu jeder betroffenen Organisation. Statt nur eine einzelne Organisation anzugreifen, war JEDER Betrieb, der die betroffene Software verwendete, einem Risiko für Datenverlust und Erpressung ausgesetzt.

Daher können wir mit ziemlicher Sicherheit vorhersagen, dass solche Angriffsarten im kommenden Jahr weiter zunehmen werden.

Die steigende Komplexität der Cloud wird auch im kommenden Jahr zu Sicherheitsvorfällen führen

Eine unserer Prognosen aus dem letzten Jahr bezog sich darauf, dass die zunehmende Komplexität der Cloud zu weiteren Sicherheitsvorfällen führen würde. Wir werden diese Vorhersage auch für das kommende Jahr wiederholen.

Da Unternehmen weiterhin in rasantem Tempo Cloud-Technologien einführen und die Zahl der Cloud-bezogenen Innovationen in der Branche zunimmt, scheint die Sicherheit gelegentlich in den Hintergrund zu rücken. Zahlreiche Beispiele von ungesicherten Amazon S3-Buckets und sogar einem Datenleck von 38 TB aufgrund eines falsch konfigurierten Azure-Speicherkontos, verdeutlichen dies. Diese Vorfälle sind nur Beispiele, die Cloud-Speicher betreffen. Ganz zu schweigen von der massiven Nutzung von Cloud-APIs, immer komplexeren Netzwerkkonfigurationen und einer wachsenden Belegschaft, die vermehrt mobil arbeitet. Mit dieser Komplexität steigt auch die Wahrscheinlichkeit, dass Fehler gemacht werden, und das wird im kommenden Jahr zu weiteren Sicherheitsverletzungen führen.

Zunehmende Nutzung von 5G und die Abhängigkeit der Netzbetreiber von Network Slicing VNI werden Angriffe auf Mobilfunknetze vorantreiben

Mobilgeräte sind im täglichen Leben allgegenwärtig geworden. Um dem ständig wachsenden Bedarf der Gesellschaft nach mehr Bandbreite gerecht zu werden, haben die meisten Mobilfunkanbieter die 5G-Infrastruktur in ihren Netzen eingeführt. Um dies zu ermöglichen, setzen viele Anbieter auf eine Strategie namens Network Slicing. Dabei unterteilen sie ihr Netzwerk in mehrere logische Netzwerke auf verschiedenen Ebenen und setzen dann auf softwaredefinierte Netzwerke (SDN), um Routing, Switching und Traffic Management zu handhaben.

Das Problem bei softwaredefinierten Netzwerken liegt im „Software"-Teil. Software ist (im Allgemeinen) schwieriger zu schützen und kann von Cyberkriminellen für Angriffe genutzt werden. Tatsächlich haben die NSA und das CISA einen Bericht über die Gefahren des Network Slicings veröffentlicht und einige Anleitungen zu dieser Praxis gegeben.

Angesichts der zunehmenden Verbreitung von 5G, der wachsenden Abhängigkeit von mobilen Netzwerken und der stärkeren Nutzung von SDN erwarten wir für das kommende Jahr mehr Angriffe auf mobile Netzwerke.

Stärkere Ransomware-Gruppen und kürzere Dwell Time

Da Ransomware-Gruppen immer leistungsfähiger und komplexer werden, beobachten wir ein erneutes Bemühen, Angriffe in Rekordzeit auszuführen. Infolgedessen ist die Dwell Time im letzten Jahr deutlich gesunken und wir erwarten, dass sich dieser Trend fortsetzt. Die Dwell Time ist die Zeitspanne, die Bedrohungsakteure in Netzwerken verbringen, bevor sie aggressive Handlungen vornehmen, die Sicherheitssysteme alarmieren oder ihre Anwesenheit bekannt machen könnten. Angesichts der zunehmenden Zahl von Zero-Days und einer Cybersecurity-Industrie, die fieberhaft versucht, Schritt zu halten, wissen die Angreifer, dass sie ihre Angriffe in Rekordzeit ausführen müssen, bevor die Abwehrmaßnahmen ergriffen werden.

Ein weiterer Faktor ist die fortschreitende Raffinesse von kriminellen Gruppen wie CONTI, die aktiv neue Schwachstellen testen, Antiviren-Anwendungen analysieren und Workarounds und Exploits entwickeln. Dies lässt auf eine erhöhte Wahrscheinlichkeit von Ransomware-Angriffen im kommenden Jahr schließen, begleitet von gezielten Bemühungen, Daten-Backups zu löschen.

Update zu Quantum Computing und Encryption

In unserem letzten Bericht haben wir uns mit einem zukünftigen Risiko befasst: Quantencomputer könnten die heutigen Verschlüsselungsstandards mühelos knacken. Im Gegensatz zu anderen Risiken in diesem Bericht ist dies noch nicht unmittelbar bevorstehend (kommerziell verfügbare Quantencomputing-Dienste sind noch sehr fehleranfällig), aber es ist von großer Bedeutung, schon jetzt mit der Planung entsprechender Maßnahmen zu beginnen, da verschlüsselte Daten und heute aufgezeichneter Netzwerkverkehr möglicherweise in der Zukunft leicht geknackt werden könnten.

Die Cybersecurity and Infrastructure Security Agency (CISA), die National Security Agency (NSA) und das National Institute of Standards and Technology (NIST) stimmten dem zu und veröffentlichten ein kurzes Informationsblatt. Drei der vier Standards, die wir im letzten Jahr erwähnt haben, befinden sich nun im Entwurfsstadium und sollen voraussichtlich im Jahr 2024 finalisiert werden.

Wie stark ist mein Unternehmen im Jahr 2024 gefährdet?

Ganz einfach gesagt: Wenn Ihr Unternehmen in der Lage ist, ein Lösegeld zu zahlen, sind Sie ein Ziel. Diese Erkenntnis basiert auf unseren Daten zum branchenweiten E-Mail-Bedrohungsindex über alle Sektoren hinweg. Es ist jedoch wichtig zu beachten, dass Organisationen, die sensible Daten verarbeiten, im Verteidigungsbereich oder kritischer Infrastruktur tätig sind oder wertvolles geistiges Eigentum besitzen, ein besonders attraktives Ziel für Cyberkriminelle darstellen.

Wie sich Unternehmen am besten schützen können

Mit den Grundlagen beginnen

Oft neigen Unternehmen dazu, auf spezifische Bedrohungen zu reagieren und punktuelle Sicherheitslösungen für jeden Bereich zu erwerben, anstatt sich zunächst auf die Grundlagen der Sicherheitshygiene zu konzentrieren. Die Mehrheit der Unternehmen, die gehackt werden, werden nicht Opfer eines obskuren Zero-Day-Exploits oder einer fortgeschrittenen Hacking-Technik. Ihre Abwehr versagt, weil sie keine starke Authentifizierung (MFA, vorzugsweise Phishing-resistente Hardware) implementiert haben, einfache Passwörter zulassen, Benutzer als lokale Administratoren auf ihren Geräten einrichten oder die Benutzer nicht darin schulen, beim Klicken auf Links in E-Mails vorsichtig zu sein. Wenn Sie Backups nicht durch Testen der Wiederherstellungsprozeduren validieren, kann ein Ransomware-Angriff sehr unangenehme Folgen haben, ebenso wie eine nachlässige Patching-Politik.

Mit anderen Worten: Um sich effektiv zu schützen, sollten Sie sich zuerst um grundlegende Sicherheitshygiene kümmern, die sowohl die Technologie als auch die Prozesse und Menschen umfasst. Beginnen Sie mit einer Zero-Trust-Mentalität:

- **Überprüfen Sie jede Verbindung:** Verlassen Sie sich nicht darauf, dass ein verwaltetes Gerät automatisch sicher ist. Auch wenn ein Benutzer sich von einem bekannten Netzwerk aus verbindet, könnte es ein Angreifer mit gestohlenen Zugangsdaten sein.
- **Nutzen Sie das Prinzip der geringsten Privilegien:** Gewähren Sie Nutzern und Workload-Identitäten nur die Berechtigungen, die sie zur Erfüllung ihrer Aufgaben benötigen, und führen Sie regelmäßige Überprüfungen durch, um unnötige Berechtigungen zu vermeiden.
- **Gehen Sie von einem möglichen Angriff aus:** Stärken Sie Ihre Verteidigungsmaßnahmen so weit wie möglich, aber denken Sie auch darüber nach, was passiert, wenn diese Maßnahmen versagen. Wie können Sie es erkennen, wenn ein Angreifer einen Benutzer kompromittiert? Wie können Sie eine laterale Bewegung durch einen Angreifer in Ihrer Umgebung einschränken?

Eine umfassendere Liste ist in den Zero-Trust-Geboten der Open Group verfügbar.

Die Sicherheitskultur ist das A und O

Die Transformation eines Unternehmens zu einem cyberresilienten Betrieb erfordert Zeit, Mühe und Durchhaltevermögen. Sie können Ihr Unternehmen nicht in eine gut verteidigte Cyber-Festung verwandeln, ohne alle Mitarbeiter einzubeziehen und ihnen zu zeigen, wie sehr sie davon betroffen sind und warum sie Teil der Lösung sein müssen.

Wenn beispielsweise Multi-Faktor-Authentifizierung (MFA) eingeführt wird, sollte die Führungsebene mit gutem Beispiel vorangehen und auch den Grund für die zusätzlichen Anforderungen an die Authentifizierung verstehen. Ein wesentlicher Teil dieses Kulturwandels besteht darin zu erkennen, dass Cyberresilienz nicht nur die Aufgabe der IT- oder Sicherheitsabteilung ist. Die IT kann nur schützen, was sie kennt. Wenn beispielsweise die Marketingabteilung eine Website und eine SaaS-Lösung einführt, muss dies in Absprache mit der IT-Abteilung erfolgen, da sonst Risiken entstehen. Jede technologische oder prozessuale Entscheidung, die bestimmt, wie ein Unternehmen geführt wird, birgt ein Risiko, und wie dieses Risiko verwaltet wird, muss für das Unternehmen transparent sein, damit es gute Entscheidungen treffen kann.

Eine wichtige Erkenntnis für IT- und Sicherheitsabteilungen besteht darin, die richtige Sprache zu sprechen: Risikomanagement. Wenn man über technische Details und Funktionsweisen spricht, verliert man schnell alle, die nicht mit der Materie vertraut sind. Stattdessen sollte man Technologie- und Prozessänderungen in die Sprache von Geschäftsrisiken (oder Geschäftschancen) übersetzen, um alle im Unternehmen mitzunehmen.

Und dieses cyber-resiliente Unternehmen ist nicht statisch, genau wie andere Risiken für das Geschäft (geopolitisch, wirtschaftlich, Wettbewerber), es verändert sich ständig und das Unternehmen muss kontinuierlich lernen und sich anpassen. Ein aktuelles Beispiel ist die Art und Weise, wie Angreifer „schwächere" Formen der Multi-Faktor-Authentifizierung umgehen, sei es durch „Attacker-in-the-Middle"-Toolkits oder MFA Fatigue-Angriffe. Auch Social Engineering bleibt ein ständiges Risiko, das auf keinen Fall vernachlässigt werden sollte.

Eine ausgewogene Sicherheitsstrategie

Es ist klar, dass das heutige Sicherheits-Ökosystem komplexer und bedrohlicher ist als je zuvor. Daher sollten Unternehmen über einen ausgewogenen Sicherheitsansatz nachdenken. Das bedeutet, sich der fortschrittlichen Bedrohungen bewusst zu sein und Maßnahmen zu ergreifen, um diese zu entschärfen. Gleichzeitig ist es wichtig sicherzustellen, dass auch die grundlegenden Sicherheitsprinzipien beachtet werden.
Es ist nicht ratsam, sich allein auf eine einzige Sicherheitsanwendung oder Gerät zu verlassen. Stattdessen sollte ein mehrstufiger Ansatz verfolgt werden, der die gängigsten Angriffsvektoren als auch diejenigen abdeckt, die für Ihr Unternehmen spezifisch sind. Dazu gehören:

- Next-Gen Spam/Malware-Erkennung mit ATP für Verhaltensanalyse zum Schutz vor der anhaltenden Flut von E-Mail-basierten Bedrohungen.
- Security Awareness Training für Endnutzer, um diese darin zu schulen, Social Engineering-Angriffe und Spear-Phishing-Angriffe zu erkennen.
- Backup- und Wiederherstellungsfunktionen sowohl für lokal gespeicherte Daten als auch für Daten in Cloud-Diensten wie M365, um im Falle eines Ransomware-Angriffs eine Wiederherstellung zu ermöglichen.
- Compliance- und Governance -Funktionen, die vor versehentlichen Datenleaks schützen und sicherstellen, dass Compliance-Standards eingehalten werden.

Wenn Sie Ihre Sicherheitsstrategien mit diesen Funktionen ausstatten, können Sie sich im kommenden Jahr auf Ihre Sicherheit verlassen.

HORNETSECURITY | EBERTLANG

365 TOTAL PROTECTION

VERBESSERN SIE IHRE SICHERHEIT

365 Total Protection von Hornetsecurity wurde speziell für Microsoft 365 entwickelt. Die Lösung bietet umfassenden Schutz für Microsoft Cloud-Services durch eine nahtlose Integration. 365 Total Protection vereinfacht Ihr IT-Sicherheitsmanagement von Anfang an, denn es ist einfach einzurichten und leicht zu bedienen.

PLAN 1	PLAN 2	PLAN 3	PLAN 4
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT
			PHISHING & ATTACK SIMULATION
			COMMUNICATION PATTERN ANALYSIS
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS
			SECURITY AWARENESS
			AI RECIPIENT VALIDATION
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT
			ESI® REPORTING
			SENSITIVE DATA CHECK

KOSTENLOSER DOWNLOAD

Die Autoren

Unterstützt von den Daten direkt aus dem Security Lab

VERFASST VON

Andy Syrewicze

Andy Syrewicze verfügt über mehr als 20 Jahre Erfahrung in der Erarbeitung von Technologielösungen für verschiedene Industriezweige.

Er ist ausgezeichnet als Microsoft Most Valuable Professional (MVP) im Bereich Cloud und Datacenter Management sowie als VMware-Experte.

Paul Schnackenburg

Paul Schnackenburg begann seine Karriere in der IT-Branche, als DOS und 286er Prozessoren der letzte Schrei waren. Er ist Inhaber von Expert IT Solutions, ein IT-Beratungsunternehmen für kleine Unternehmen an der Sunshine Coast, Australien. Außerdem arbeitet er als IT-Trainer an einer Microsoft IT-Akademie.

Paul ist ein angesehener Technologiewissenschaftler und sehr aktiv in der Community. Seine technischen Artikel konzentrieren sich auf Hyper-V, System Center, private und hybride Clouds sowie Office 365 und Azure Public Cloud-Technologien. Er trägt die Zertifizierungen MCSE, MCSA und MCT.

Kapitel 5 – Quellenangaben

- https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked
- https://www.bleepingcomputer.com/news/security/w3ll-phishing-kit-hijacks-thousands-of-microsoft-365-accounts-bypasses-mfa/
- https://www.hornetsecurity.com/us/podcast-us/can-you-trust-microsoft-security/
- https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- https://techcommunity.microsoft.com/t5/microsoft-syntex-blog/welcome-to-microsoft-inspire-2023-introducing-microsoft-365/ba-p/3874887
- https://www.hornetsecurity.com/us/services/365-permission-manager/
- https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
- https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
- https://www.microsoft.com/en-us/security/blog/2023/07/19/expanding-cloud-logging-to-give-customers-deeper-security-visibility/
- https://www.descope.com/blog/post/noauth
- https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
- https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
- https://www.hornetsecurity.com/us/podcast-us/monthly-threat-report-discussion-october-2023/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
- https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/
- https://www.hornetsecurity.com/us/podcast-us/we-used-chatgpt-to-create-ransomware/
- https://www.zdnet.com/article/wormgpt-what-to-know-about-chatgpts-malicious-cousin/
- https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/
- https://www.hornetsecurity.com/us/podcast-us/generative-ai-in-defensive-tools/

- https://openai.com/blog/openai-cybersecurity-grant-program
- https://github.com/features/copilot
- https://github.com/kgretzky/evilginx2
- https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
- https://www.bleepingcomputer.com/news/security/the-moveit-hack-and-what-it-taught-us-about-application-security/
- https://www.theregister.com/2023/05/17/another_security_calamity_for_capita/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-leaks-38tb-of-private-data-via-unsecured-azure-storage/
- https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3459888/esf-members-nsa-and-cisa-publish-second-industry-paper-on-5g-network-slicing/
- https://therecord.media/ransomware-deployment-dwell-time-decreasing
- https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
- https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers
- https://pubs.opengroup.org/security/zero-trust-commandments/
- https://salt.security/api-security-trends?

HORNETSECURITY

ebertlang.com/hornetsecurity | hornetsecurity@ebertlang.com | +49 6441 67118-842