HORNETSECURITY

CYBERSECURITY REPORT 2025

Eine detaillierte Analyse der Microsoft 365-Bedrohungslandschaft basierend auf Erkenntnissen aus

55,6 Milliarden E-Mails

hornetsecurity.com

HORNETSECURITY
CSR2025

ÜBER HORNETSECURITY

Hornetsecurity ermöglicht es Unternehmen und Organisationen jeder Größe, sich auf ihr Kerngeschäft zu konzentrieren, indem M365-Workloads und die E-Mail-Kommunikation geschützt, Daten gesichert und Geschäftskontinuität und Compliance mit Cloud-basierten Lösungen der nächsten Generation gewährleistet werden.

Das Flaggschiffprodukt 365 Total Protection ist die umfassendste Cloud-Security-Lösung für Microsoft 365 auf dem Markt. Angetrieben von Innovation und Cybersecurity-Exzellenz, sorgt Hornetsecurity mit seinem preisgekrönten Portfolio für eine sicherere digitale Zukunft und eine nachhaltige Sicherheitskultur bei seinen Kunden und Partnern.

WAS IST DER CYBERSECURITY REPORT?

Der Cybersecurity Report von Hornetsecurity ist eine jährliche Analyse der Microsoft 365-Bedrohungslandschaft. Diese basiert auf realen Daten, die vom Security Lab von Hornetsecurity gesammelt und untersucht wurden. In den Produkten von Hornetsecurity werden **jeden Monat mehr als 4,5 Milliarden E-Mails verarbeitet**. Durch die Analyse der in diesen E-Mails enthaltenen Bedrohungen, kombiniert mit einer detaillierten Kenntnis der breiteren Bedrohungslandschaft, zeigt das Security Lab wichtige Sicherheitstrends und Aktionen von Bedrohungsakteuren auf. Außerdem können fundierte Prognosen für die Zukunft der Microsoft 365-Sicherheitsbedrohungen erstellt werden, sodass Unternehmen entsprechend handeln können. Detaillierte Erkenntnisse und Daten dazu finden Sie in diesem Report.

WAS IST DAS SECURITY LAB?

Das Security Lab ist eine Abteilung von Hornetsecurity, die forensische Analysen aktueller und kritischer Sicherheitsbedrohungen durchführt und auf die E-Mail-Sicherheit im Microsoft 365-Ökosystem spezialisiert ist. Das multinationale Team von Sicherheitsspezialisten verfügt über umfangreiche Erfahrungen in der Sicherheitsforschung, Softwaretechnik und Datenwissenschaft.

Ein tiefgreifendes Verständnis der Bedrohungslandschaft, das durch die Untersuchung von realen Phishing-Angriffen, Malware, Ransomware-Banden und mehr gewonnen wird, ist für die Entwicklung effektiver Gegenmaßnahmen von entscheidender Bedeutung. Die detaillierten Erkenntnisse des Security Labs dienen als Grundlage für die Cybersecurity-Lösungen der nächsten Generation von Hornetsecurity.

SECURITY LAB
CYBERSECURITY INSIGHTS & ANALYSIS

INHALTSVERZEICHNIS

CYBERSECURITY REPORT 2025

KAPITEL 1
ZUSAMMENFASSUNG

KAPITEL 1 – ZUSAMMENFASSUNG

Durch den großen Bestand an Nutzerdaten ist Hornetsecurity in der Lage, eine detaillierte Untersuchung von E-Mail-basierten Bedrohungen sowie von Bedrohungen, die auf Microsoft 365 abzielen, durchzuführen. Dies ermöglicht dem Security Lab, diese Daten in wichtige Erkenntnisse für IT-Teams und Sicherheitsexperten zu konvertieren. Im vergangenen Jahr wurden mehr als 55,6 Milliarden E-Mails analysiert, von denen 36,9 % als "unerwünscht" klassifiziert wurden. 97,8 % der unerwünschten E-Mails sind Spam oder werden aufgrund externer Indikatoren bereits im Voraus abgelehnt. 2,3 % der unerwünschten E-Mails wurden als bösartig eingestuft.

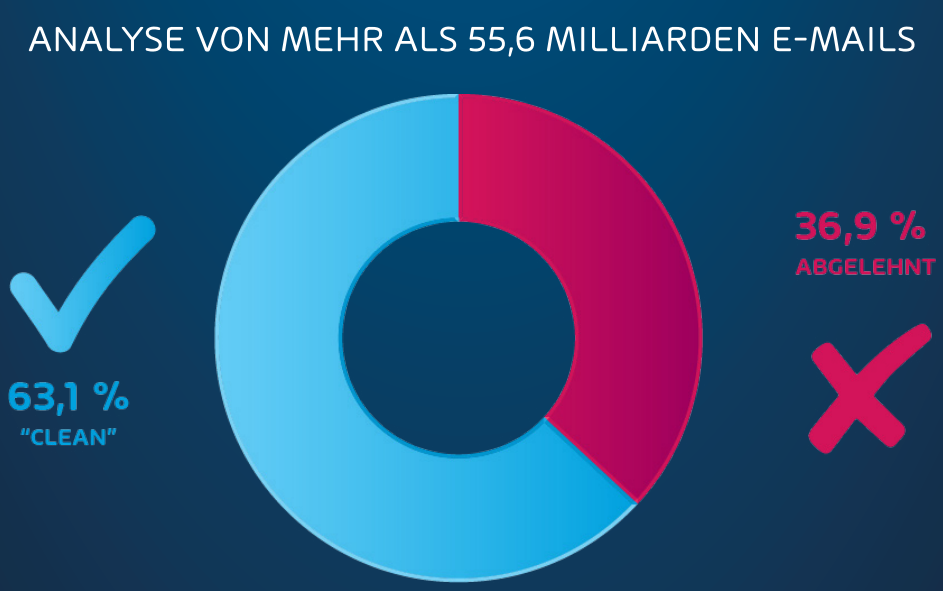


ABB 1. KLASSIFIKATION DER GESCANNTEN E-MAILS DURCH HORNETSECURITY

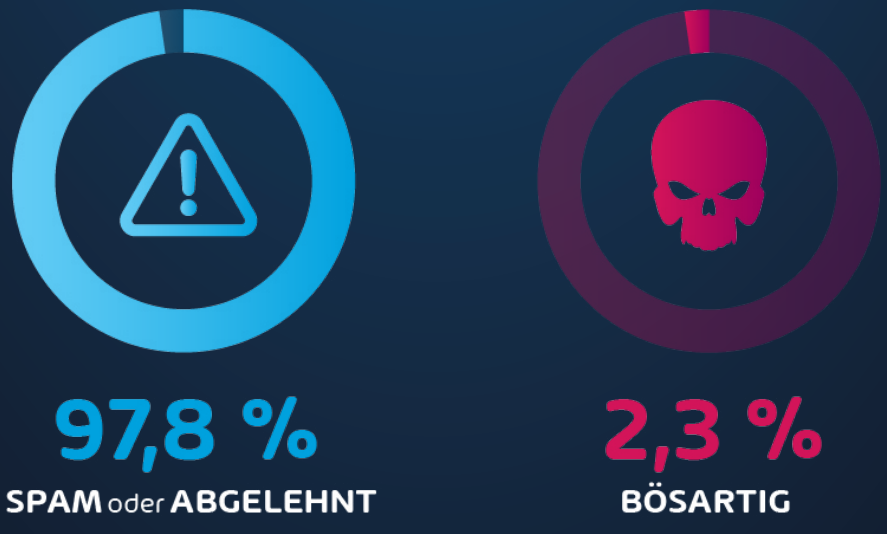


ABB 2. KLASSIFIKATION VON UNERWÜNSCHTEN E-MAILS

“PHISHING: 33,3% DER ANGRIFFE”

Betrachtet man die bei E-Mail-Angriffen verwendeten Angriffsarten, so bleibt Phishing mit 33,3 % der Angriffe die am weitesten verbreitete Angriffsmethode. Dicht gefolgt von bösartigen URLs, die 22,7 % der Fälle ausmachen. Diese Zahlen stimmen mit den Angriffsarten überein, die im vergangenen Jahr bei Bedrohungsakteuren an Beliebtheit gewonnen haben - vor allem bei Angriffen im Stil von Reverse-Proxy-Angriffen zum Diebstahl von Anmeldedaten, bei denen Social Engineering und bösartige Links eine große Rolle spielen.

Die erneute Konzentration auf Social Engineering und den Diebstahl von Sicherheitstoken und Anmeldeinformationen ist auch in unseren Daten zu bösartigen Dateitypen erkennbar. Wir verfolgen die Dateitypen, die für die Übermittlung bösartiger Payloads in E-Mail-Angriffen verwendet werden, und mussten feststellen, dass die Verwendung bösartiger Anhänge deutlich zurückgegangen ist. Nahezu jeder bösartige Dateityp verzeichnete einen Rückgang im Vergleich zum Vorjahr. HTML-, PDF- und Archivdateien bleiben jedoch wie im Vorjahr auf den ersten drei Plätzen.

Die Bedrohungsakteure haben im Berichtszeitraum eine erhöhte Anzahl an leicht zu erkennenden (und letztlich „abgewiesenen“) E-Mail-Angriffen gestartet. Dies zeigt die leicht rückläufige Zahl bösartiger E-Mails, die als „Bedrohungen“ und „AdvThreats“ eingestuft wurden. Infolgedessen sank der Bedrohungsindex für fast alle Branchen während des Untersuchungszeitraums. Das ist damit zu erklären, dass unser Branchen-Bedrohungsindex die Anzahl der sauberen E-Mails mit dem Volumen der „Bedrohungen“ und „AdvThreats“ vergleicht. Bemerkenswert ist die Tatsache, dass es kaum Unterschiede zwischen den einzelnen Branchen gibt. Zwar gibt es einige, die stärker betroffen sind als andere, doch die Daten belegen erneut, dass keine Branche vor Cyberkriminalität geschützt ist. DHL ist unter den am häufigsten imitierten Marken zwar weiterhin die Nummer 1, doch die Anzahl der Imitationsversuche ist stark zurückgegangen. Die Anzahl der Imitationsversuche von FedEx hat sich dagegen verdreifacht. Bei Docusign und Facebook hat sich die Anzahl der Imitationsvesuche verdoppelt. Auch bei Mastercard und Netflix ist ein deutlicher Anstieg zu verzeichnen.

Beim Thema Sicherheit von Daten in der Cloud konnten wir in diesem Jahr bei den Angreifern eine zunehmende Verwendung von Toolkits zum Diebstahl von Anmeldeinformationen/Token über einen Adversary-in-the-Middle-Angriff beobachten. Im Vergleich zu den Vorjahren sind diese Angriffe bei Cyberkriminellen sehr beliebt geworden.

Dies liegt daran, dass sie mit minimalem Aufwand eine große Anzahl von Opfern mit überzeugenden Zielseiten ansprechen können. Die Toolkits sind so konzipiert, dass sie auch die MFA-Authentifizierung (Multi-Faktor-Authentifizierung) berücksichtigen, von der viele Unternehmen (fälschlicherweise) annehmen, dass sie sie zu 100 % vor diesen Angriffen schützt. Die Cybersicherheitsbranche bemüht sich weiterhin, dieses Problem durch bessere Scanning-Mechanismen, Security Awareness Schulungen und Phishing-resistente Anmeldetechnologien wie Passkeys zu lösen. Da solche Maßnahmen allerdings eine gewissen Implementationszeit benötigen, können Unternehmen in der Überbrückungszeit Angriffen zum Opfer fallen.

Da diese Art von Angriffen nach wie vor stark auf E-Mail-Kommunikation und zunehmend auch auf Chat-Kommunikation wie Microsoft Teams zurückgreift, ist eine robuste Sicherheitsstrategie für E-Mail und Microsoft 365 unerlässlich, um in der heutigen digitalen Welt sicher zu agieren.

CYBERSECURITY
REPORT 2025

KAPITEL 2

DIE AKTUELLE MICROSOFT 365-BEDROHUNGSLANDSCHAFT

KAPITEL 2 – DIE AKTUELLE MICROSOFT 365-BEDROHUNGSLANDSCHAFT

Jährlich überprüft das Hornetsecurity Security Lab die erhobenen Datensätze und analysiert den Stand der weltweiten E-Mail-Bedrohungen und Kommunikationsstatistiken. Darüber hinaus führt das Team regelmäßig Trainings zu vorausschauendem Denken durch und gibt Einblicke in potenzielle zukünftige Bedrohungen. Dieses Kapitel konzentriert sich auf die Überprüfung von Datenpunkten aus dem definierten Datenzeitraum vom 1. November 2023 bis zum 31. Oktober 2024, der die Grundlage für die in Kapitel 4 dargestellten Prognosen zur Entwicklung der Bedrohungslandschaft bildet.

TRENDS BEI DER E-MAIL-SICHERHEIT

Trotz der zunehmenden Nutzung von Kollaborations- und Instant-Messaging-Software wie Microsoft Teams ist die E-Mail nach wie vor das größte Einfallstor bei Cyberangriffen. Wir haben einen kontinuierlichen Rückgang der als Bedrohungen/AdvThreats eingestuften E-Mails beobachtet – 2,3 % in diesem Jahr, verglichen mit 3,7 % im letzten Jahr und 5,5 % im Jahr davor (innerhalb der der „unerwünschten" E-Mails). Dennoch bleibt das Risiko für Unternehmen rund um den Globus hoch. Dies ist in erster Linie auf den verstärkten Einsatz von Social-Engineering-Techniken zurückzuführen, bei denen mit geringem Aufwand, E-Mail-Angriffe im Spray-Stil durchgeführt werden, die darauf abzielen, den Zielbenutzer auf irgendeine Weise zu einer Interaktion zu bewegen.

Bei der Überprüfung von mehr als 55,6 Milliarden E-Mails, die im aktuellen Berichtszeitraum (1. November 2023 bis 31. Oktober 2024) gesammelt wurden, hat das Security Lab die folgenden Feststellungen gemacht:

SPAM, MALWARE, ADVANCED THREAT METRIKEN

Die erhobenen Daten aus dem Berichtszeitraum stufen 36,9 % aller E-Mails als „unerwünscht" ein - ein Anstieg um 0,6 Prozentpunkte gegenüber 2023. Die Definition von „unerwünscht" bezieht sich auf E-Mails, die keine echte, vom Empfänger gewünschte Kommunikation darstellen. Das folgende Diagramm zeigt unsere Aufschlüsselung der unerwünschten E-Mails zusammen mit den sauberen E-Mails.

Dies steht im Gegensatz zu der im letzten Jahr gemeldeten Zahl von 36,3 % aller E-Mails, die als „unerwünscht" eingestuft wurden, was einen leichten Anstieg der unerwünschten E-Mails im Vergleich zum Vorjahr zeigt.

Wenn man bedenkt, dass wir im Jahr 2024 55,6 Milliarden E-Mails verarbeitet haben, macht die Zahl der „unerwünschten" E-Mails etwa 20,5 Milliarden aus, die im Berichtszeitraum an Unternehmen gesendet wurden.

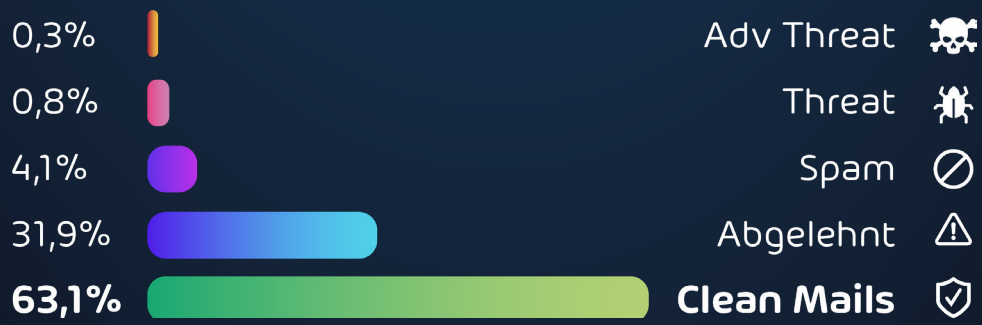


ABB 3. 2024 UNERWÜNSCHTE E-MAILS NACH KATEGORIE, EINSCHLIESSLICH SAUBERER E-MAILS

Für eine übersichtliche Aufschlüsselung der prozentualen Anteile an „unerwünschten" E-Mails haben wir diese wie folgt klassifiziert:

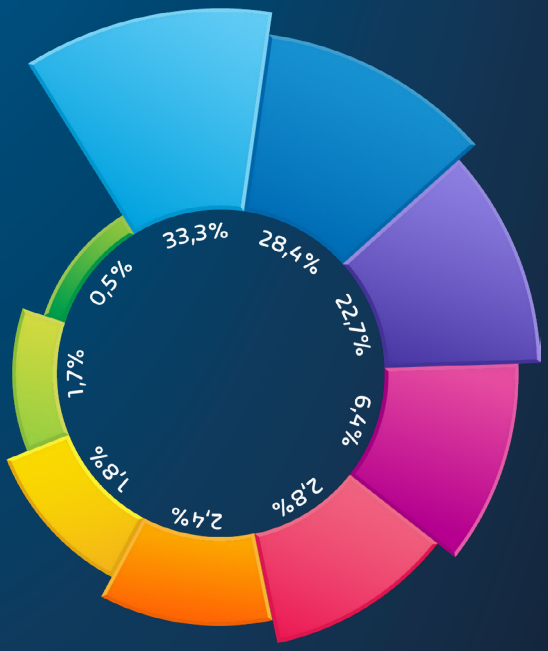
ABB 4. 2024 UNERWÜNSCHTE E-MAILS NACH KATEGORIE

KATEGORIE	BESCHREIBUNG
Spam	Diese E-Mails sind unerwünscht und enthalten oft Werbung oder betrügerische Inhalte. Die E-Mails werden gleichzeitig an eine große Anzahl von Empfängern gesendet.
Threat	Diese E-Mails enthalten schädliche Inhalte, z. B. bösartige Anhänge oder Links, oder sie werden zu kriminellen Zwecken wie Phishing verschickt.
AdvThreat	Advanced Threat Protection hat in diesen E-Mails eine Bedrohung erkannt. Die E-Mails werden für illegale Zwecke verwendet und beinhalten ausgeklügelte technische Mittel, die nur mit fortschrittlichen dynamischen Verfahren abgewehrt werden können.
Abgelehnt	Unser E-Mail-Server lehnt diese E-Mails direkt bei der ersten Verbindung vom sendenden E-Mail-Server aufgrund äußerer Merkmale wie der Identität des Absenders ab, und die E-Mails werden nicht weiter analysiert.

ANMERKUNG: Die Kategorie „Abgelehnt" bezieht sich auf E-Mails, die von den Hornetsecurity-Diensten während des SMTP-Dialogs aufgrund von externen Merkmalen wie der Identität oder der IP-Adresse des Absenders abgelehnt wurden. Wenn ein Absender bereits als kompromittiert identifiziert wurde, fährt das System nicht mit der weiteren Analyse fort. Der SMTP-Server verweigert die E-Mail-Übertragung gleich zu Beginn der Verbindung aufgrund der negativen Reputation der IP-Adresse und der Identität des Absenders.

ANGRIFFSTECHNIKEN BEI E-MAIL-ANGRIFFEN IM JAHR 2024

Bei der Datenanalyse der E-Mails aus dem Berichtszeitraum haben wir die folgende Aufschlüsselung der bei E-Mail-Angriffen verwendeten Angriffsarten beobachtet:



ANGRIFFSTECHNIK	
PHISHING	33.3%
„ANDERE"	28.4%
URL	22.7%
VORKASSEBETRUG	6.4%
ERPRESSUNG	2.8%
.EXE IN DISK IMAGE / ARCHIV	2.4%
IDENTITÄTSDIEBSTAHL	1.8%
HTML	1.7%
MALDOC	0.5%

ABB 5. ANGRIFFSTECHNIKEN BEI E-MAIL-ANGRIFFEN IM JAHR 2024

ANMERKUNG: In den vergangenen Jahren konnten wir die Veränderung des Auftretens von Angriffsarten von Jahr zu Jahr verfolgen. Aufgrund von Änderungen in der Art und Weise, wie wir bösartige Objekte und unerwünschte E-Mails identifizieren, gibt es jedoch eine Untergruppe von Vorkommnissen, die als „Andere" gekennzeichnet sind. Diese Kategorie umfasst verschiedene Angriffsmethoden, die sich nicht eindeutig in eine der Hauptkategorien einordnen lassen, die wir in den vergangenen Jahren aufgeführt haben. Wir können zwar eine Aufschlüsselung der Angriffsarten für den aktuellen Datenzeitraum liefern, aber ein direkter Vergleich dieser Daten mit dem letzten Jahr würde keine genaue Darstellung ergeben.

Was unsere Daten für diesen Zeitraum zeigen, ist, dass Phishing nach wie vor die häufigste Angriffsart bei E-Mail-basierten Angriffen ist, gefolgt von bösartigen URLs. Die wachsende Beliebtheit bösartiger URLs bei Angreifern ist vor allem auf ihre Verwendung bei Reverse-Proxy-Angriffen zum Sammeln von Anmeldeinformationen zurückzuführen, bei denen Tools wie Evilginx eingesetzt werden.

Der Vorkassebetrug bleibt beliebt, gefolgt von Erpressung auf Platz 4. Hier halten Angreifer die Daten der Opfer nicht mehr nur zurück, sondern drohen auch mit der Veröffentlichung dieser.

VERWENDUNG UND ARTEN VON ANHÄNGEN BEI ANGRIFFEN

E-Mail-Anhänge wurden auch im Jahr 2024 von Bedrohungsakteuren für die Übermittlung bösartiger Payloads verwendet. Angreifer nutzen Anhänge, um Malware zu verstecken und ihrer bösartigen Kommunikation Authentizität zu verleihen, je nachdem, welcher Dateityp angehängt ist. Außerdem sind einige rudimentäre Spam-/Malware-Filter möglicherweise nicht in der Lage, bestimmte Dateitypen zu scannen, was zu einer Infektion durch komplexere Angriffe wie **HTML-Schmuggel** führt. Die Verwendung von HTML-Dateien steht nach wie vor an erster Stelle der meistverwendeten Dateitypen in bösartigen E-Mails, wie unten dargestellt.

Die Aufschlüsselung der Dateitypen, die für die Übermittlung bösartiger Payloads während des Untersuchungszeitraums verwendet wurden, ist hier dargestellt:

DATEITYP	2023	2024
HTML	37,5%	20,4%
PDF	22,8%	19,2%
ARCHIV	19,4%	17,6%
EXECUTABLE	3,5%	3,2%
EXCEL	3,2%	3,0%
WORD	3,0%	2,5%
DISK IMAGE FILES	2,2%	2,2%
ANDERE	8,4%	31,9%

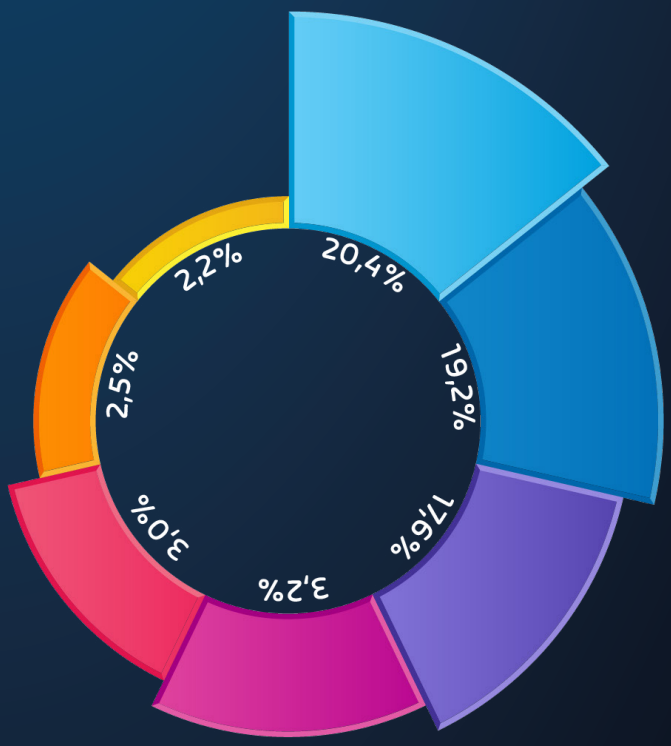


ABB 6. DATEITYPEN FÜR BÖSARTIGE PAYLOADS IM JAHR 2024

17.1 PROZENTPUNKTE RÜCKGANG VON
HTML-DATEIEN
2024 IM VERGLEICH ZU 2023

- Die Nutzung von **PDF-Dateien** ist 2024 um 3,6 Prozentpunkte zurückgegangen.
- Bei **Archivdateien** ist ein ähnlicher Trend zu beobachten: ein Rückgang von 1,8 Prozentpunkten im Jahr 2024.
- Wir beobachteten einen fast durchgängigen Rückgang bei allen **bösartigen Dateitypen**, da die Angreifer auf andere Angriffsarten umschwenken.

Im vergangenen Jahr war die Verwendung bösartiger Anhänge für Angreifer nicht mehr so effektiv wie in der Vergangenheit. Daher beobachten wir einen Trend, bei dem Angreifer verstärkt auf Social-Engineering-Taktiken setzen, mit dem Ziel, das Opfer zu einer anderen Handlung zu bewegen, anstatt einfach nur einen Anhang zu öffnen. So wurden während des Untersuchungszeitraums beispielsweise häufig Reverse-Proxy-Adversary-in-the-Middle-Toolkits eingesetzt. Dies ist darauf zurückzuführen, dass Angreifer mit der zunehmenden Verbreitung der Multi-Faktor-Authentifizierung (MFA) es immer häufiger auf den Diebstahl von Token über Tools wie Evilginx und PyPhisher abgesehen haben. Es ist einfacher, das Authentifizierungs-Token zu beschaffen, als sich den Kopf darüber zu zerbrechen, wie man Zugriff auf die MFA-Methode des Ziels erhält.

E-MAIL-BEDROHUNGSINDEX FÜR VERSCHIEDENE BRANCHEN

Einer der wichtigsten Bereiche, die wir jährlich (und monatlich) analysieren, ist die Anzahl der Bedrohungen, die auf die verschiedenen Industriezweige abzielen. So können wir feststellen, ob es spezielle Kampagnen oder gezielte Angriffe auf bestimmte Branchen gibt. Darüber hinaus liefert dies einige Erkenntnisse, anhand derer Unternehmer feststellen können, ob sie einem erhöhten Angriffsrisiko ausgesetzt sind oder nicht.

Am bemerkenswertesten an den diesjährigen Daten ist die Tatsache, dass in JEDER vertikalen Branche ein Rückgang des entsprechenden E-Mail-Bedrohungsindex zu verzeichnen war. Dies korreliert mit unseren obigen Daten, die zeigen, dass die Anzahl der als „Bedrohungen" und „AdvThreats" eingestuften E-Mails im Vergleich zum letzten Jahr abgenommen hat.

Dennoch gab es einige Branchen, die etwas stärker betroffen waren als andere.

- **Bergbauindustrie** – Die meisten Bergbauunternehmen haben die gleichen Probleme und Herausforderungen wie Fertigungsunternehmen. Außerdem handeln sie häufig mit Edelmetallen, was sie zu einem bevorzugten Ziel für Bedrohungsakteure macht, die mit Hilfe von Ransomware versuchen, die Unternehmen zu erpressen.
- **Unterhaltungsindustrie** – Unternehmen dieser Art sind in der Regel im Bereich Glücksspiel, Kartenverkauf usw. tätig. Diese Organisationen sind aufgrund der hohen Geldbeträge, um die es geht, zu einem Ziel geworden. Man erinnere sich an die Angriffe auf MGM und Caesars Entertainment im Jahr 2023, auf die wir weiter unten näher eingehen.
- **Fertigungsindustrie** – Die Fertigungsindustrie ist in der Vergangenheit häufig Ziel von Bedrohungsakteuren gewesen. Dies liegt in der Regel daran, dass Angreifer es auf geistiges Eigentum abgesehen haben und/oder Lösegeld erpressen wollen. Viele betrachten diesen Sektor aufgrund der besonderen Eigenschaften seiner Netzwerksicherheit als ein leichtes Ziel für doppelte Erpressungen und Produktionsunterbrechungen. Hinzu kommt, dass in der Branche häufig eine große Anzahl unsicherer IoT-Geräte (Internet of Things) und speicherprogrammierbarer Steuerungen (PLCs) verwendet wird.

ABB 7. JÄHRLICHER BRANCHEN-BEDROHUNGSINDEX

ANMERKUNG: Der Wert des Bedrohungsindexes wird anhand der folgenden Berechnung ermittelt:

Bedrohungsindex-Prozentsatz = Anzahl der bösartigen E-Mails (Bedrohung+AdvThreat) / (Anzahl der bösartigen E-Mails (Bedrohung+AdvThreat) + Anzahl der sauberen E-Mails) multipliziert mit 100 – Spam und Info-Mails werden dabei nicht berücksichtigt

Hinweis zur Methodologie

Organisationen unterschiedlicher Größe erhalten eine unterschiedliche absolute Anzahl von E-Mails. Daher berechnen wir den prozentualen Anteil der bedrohlichen E-Mails an den bedrohlichen und sauberen E-Mails jeder Organisation, um die Organisationen zu vergleichen. Anschließend berechnen wir den Median dieser Prozentwerte für alle Unternehmen derselben Branche, um den endgültigen Bedrohungswert für die Branche zu ermitteln.

BRAND IMPERSONATION

Die Markenimitation ist auch im Jahr 2024 eine der am häufigsten genutzten E-Mail-Angriffstechniken, die auf Endbenutzer und Unternehmen abzielt.

Den größten Rückgang bei Versuchen der Markenimitation hat wohl das Versandunternehmen DHL erlebt. Im Jahr 2024 gab es im Vergleich zu 2023 nur einen Bruchteil solcher Versuche. Trotzdem bleibt DHL weiterhin auf Platz eins unserer Liste der am häufigsten imitierten Marken, dicht gefolgt von FedEx.

Logistikmarken sind nach wie vor beliebte Angriffsziele, da sie über Phishing und Smishing leicht in Social-Engineering-Angriffe eingebunden werden können. Wenn Mitteilungen im Rahmen dieser Attacken eine hohe Ähnlichkeit mit der eigentlichen Kommunikation der Unternehmen aufweisen, kann es weniger geschulte Benutzer leicht dazu verleiten, persönliche Daten und/oder Zahlungsinformationen preiszugeben.

Weitere bemerkenswerte Daten in diesem Bereich:

- Die Anzahl der Imitationen der Marken FedEx und Facebook hat sich im letzten Jahr verdreifacht.
- Die Anzahl der Nachahmungen der Marke Docusign hat sich im Untersuchungszeitraum verdoppelt.
- Mastercard und Netflix sind zwei weitere bekannte Marken, die ebenfalls einen deutlichen Anstieg zu verzeichnen haben.

Unsere vollständigen Daten über den Untersuchungszeitraum zeigen die am häufigsten imitierten Marken:

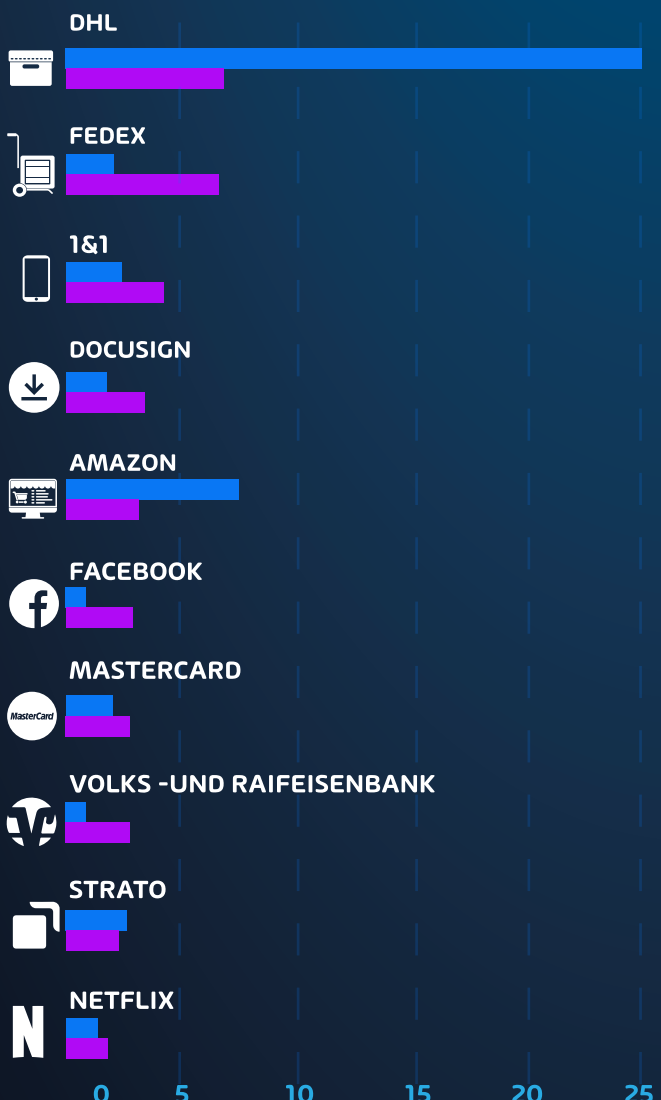


ABB 8. TOP 10 MARKEN-IMITATIONEN

ANMERKUNG: Daten zur Markenimitation werden stark durch regionale Unterschiede beeinflusst. Aufgrund unseres großen Kundenstamms in Deutschland sind hier mehrere deutsche Marken aufgeführt.

Unsere Analyse von 10.743.561 aktiven E-Mail-Versanddomains im Jahr 2024 zeigt Lücken in der Implementierung der E-Mail-Authentifizierung, wodurch viele Unternehmen anfällig für Marken-Impersonationsangriffe und E-Mail-Spoofing sind.

> **NUR 35,4 %**
> HABEN DMARC-PROTOKOLLE

Nur 35,4 % der analysierten Domains haben DMARC-Protokolle (Domain-based Message Authentication, Reporting, and Conformance) implementiert, was bedeutet, dass fast zwei Drittel der Domains nicht über diese kritische Sicherheitsmaßnahme verfügen. Nur 16,6 % aller Domains nutzen RUA-Funktionen (Aggregate Reporting URI), die einen wichtigen Einblick in die Ergebnisse der E-Mail-Authentifizierung ermöglichen.

RUA-Datensätze sind eine wichtige Komponente von DMARC, die es Domainbesitzern ermöglicht, detaillierte Berichte über E-Mails zu erhalten, die über ihre Domain gesendet wurden. Diese Berichte umfassen:

- Volumen der empfangenen Nachrichten
- IP-Adressen, die E-Mails im Namen der Domain versenden
- Pass/Fail-Raten bei der Authentifizierung
- Versendende Quellen und ihre Übereinstimmung mit den Domainrichtlinien

Von den Domains, die DMARC implementiert haben, nutzen 47 % die RUA-Funktionen, was zeigt, dass viele Organisationen, die DMARC einführen Überwachung und Transparenz für wichtig halten.

Durch die RUA-Überwachung sind Unternehmen in der Lage, einen Anstieg von gefälschten E-Mails zu beobachten, die von zuvor unbekannten IPs stammen, und können so ihre Kunden über die spezifische Phishing-Kampagne informieren. Finanzinstitute nutzen die RUA-Überwachung häufig, um innerhalb weniger Stunden nach dem Start einer Phishing-Kampagne Gegenmaßnahmen einzuleiten.

SICHERHEIT VON DATEN IN DER CLOUD

Die „Cloud" gibt es nun schon seit mehr als zehn Jahren, aber wir erleben gerade erst, dass Unternehmen entweder massenhaft auf Cloud-Dienste umsteigen oder sich als 100%ig in der Cloud gehostete Unternehmen etablieren. Nehmen wir zum Beispiel die Speicherung von Geschäftsdaten. Vor zehn Jahren hatten die meisten Unternehmen noch eine Art lokalen Dateiserver, auf dem die wichtigen Daten des Unternehmens gespeichert waren. Heute wird dafür immer häufiger auf Cloud-Speicher zurückgegriffen. SharePoint Online und OneDrive for Business werden zunehmend zu dem Ort, an dem Daten gespeichert und mit Diensten wie Microsoft Entra gesichert werden. Daher ist die Sicherheit von Daten in der Cloud nicht nur für die M365-Cloud, sondern für Cloud-Dienste im Allgemeinen zu einem wichtigen Thema geworden. Während wir uns in diesem Report auf Microsoft 365 und das Microsoft Cloud-Ökosystem konzentrieren, gilt vieles von dem, was hier besprochen wird, auch für andere Cloud-Anbieter.

Die grundlegenden Schutzmaßnahmen in der Microsoft Cloud haben sich im Laufe der Jahre verbessert, sind aber noch lange nicht perfekt. Immer mehr Unternehmen nutzen neuere Sicherheitsfunktionen wie die Multi-Faktor-Authentifizierung (MFA) und grundlegende E-Mail-Sicherheit durch Dienste wie Exchange Online Protection, aber das reicht oft noch nicht aus. Angreifer entwickeln sich ständig weiter, was sich deutlich mit den Adversary-in-the-Middle-Angriffen zeigt.

PASSKEYS UND ADVERSARY-IN-THE-MIDDLE-ANGRIFFE

Wo die Verteidiger hingehen, folgen die Angreifer. Seit mehreren Jahren befürworten wir hier bei Hornetsecurity, wie auch alle anderen sicherheitsbewussten Personen und Unternehmen, MFA als einen sichereren Ersatz für den traditionellen Einsatz von Benutzername und Passwort bei der Anmeldung in Systemen. Die Akzeptanz verschiedener Formen von MFA, von SMS-Textnachrichten bis hin zu Hardware-Sicherheitsschlüsseln, hat langsam und stetig zugenommen. Es ist jedoch nicht so, dass die Kriminellen die Hände in den Schoß legen und ihr lukratives „Geschäft" aufgeben würden, sondern sie haben sich angepasst.

Ihr Hauptansatz besteht darin, Reverse-Proxy-Phishing-Kits zu nutzen, sei es in Form von Open-Source- oder „kommerziellen" Paketen. Diese Kits helfen sowohl beim Erstellen überzeugender E-Mail-Köder, um Benutzer zum Klicken auf einen Link zu bewegen, als auch beim Einrichten von Proxy-Diensten mit täuschend echten Anmeldeseiten. Wenn ein Benutzer auf den Link klickt und auf eine gefälschte Anmeldeseite gelangt, auf der er seinen Benutzernamen und sein Kennwort eingeben muss, werden diese Anmeldedaten an die echte Website weitergegeben und vom Angreifer abgefangen. Sobald dann die MFA-Eingabeaufforderung erscheint, ermöglichen es diese Reverse-Proxy-Toolkits dem Endbenutzer, seinen MFA-Code einzugeben oder die Aufforderung wie üblich zu bestätigen, wobei diese Informationen ebenfalls im Hintergrund an die echte Anmeldeseite weitergeleitet werden. Gleichzeitig stiehlt der Angreifer den Token, den der Ziel-Identitätsdienst generiert hat (z. B. Entra ID), und kann ihn nun verwenden, um sich als Benutzer anzumelden; daher wird diese Methode als Adversary-in-the-Middle (AitM) bezeichnet.

Um diese raffinierten Angriffe abzuwehren, benötigt man eine phishing-resistente MFA-Methode. Diese neueren Methoden sind in der Wirtschaft (noch) nicht allzu weit verbreitet. Einige Beispiele sind Windows Hello for Business, FIDO2-Hardware-USB-Schlüssel und neuerdings auch Passkeys. Diese MFA-Methoden binden die Authentifizierung ausschließlich an die legitime URL der Website. Selbst wenn der Benutzer dazu verleitet wird, eine täuschend echte Anmeldeseite zu besuchen, verweigert die Technologie die Funktion, weil sie erkennt, dass die Adresse der Website nicht übereinstimmt.

Das Problem ist, dass Windows Hello for Business spezielle Hardware erfordert (und nur für Windows funktioniert), während FIDO2-Hardwareschlüssel kostspielig sind, weshalb sie nur eingeschränkt angenommen wurden. Ein Passkey nutzt die gleichen Technologien wie ein FIDO2-Schlüssel, verlässt sich aber auf den Sicherheitschip im iPhone oder Android-Telefon, sodass keine zusätzliche Hardware erforderlich ist. Auch hier hat sich der Schlüssel nur langsam durchgesetzt, aber immer mehr Dienste unterstützen ihn jetzt und wer für die Sicherheit in seinem Unternehmen verantwortlich ist, sollte ihn unbedingt noch heute ausprobieren. Wir gehen davon aus, dass die Akzeptanz von Passkeys in den nächsten 12 Monaten drastisch zunehmen wird, da nun auch Microsoft Entra ID, Google Workspace und AWS sowie Facebook und viele andere Dienste Passkeys unterstützen.

Übermäßige Abhängigkeit von einzelnen Anbietern vertieft Bedenken hinsichtlich der Sicherheit von Cloud-Daten

Übermäßige Abhängigkeit von Anbietern bedeutet, viele oder fast alle Kerngeschäftsprozesse und -verfahren in die Hände eines Anbieters zu legen. Das Problem dabei ist, dass das Unternehmen in Schwierigkeiten gerät, wenn der Anbieter in irgendeiner Weise Probleme hat (sei es hinsichtlich Sicherheit oder aus anderen Gründen).

Wir haben in unseren Monthly Threat Reports und im Podcast The Security Swarm bereits ausführlich über die potenzielle übermäßige Abhängigkeit von Anbietern gesprochen, die einige Unternehmen mit Microsoft haben könnten. Natürlich ist dies ein Problem, das fortbesteht und sich wahrscheinlich noch verschärfen wird, wenn Microsoft seinen Marktanteil in verschiedenen Bereichen weiter ausbaut.

Hinzukommt, dass im Laufe des letzten Jahres neue Bedenken bekannt wurden, die die Problematik noch einmal unterstreichen. Vor dem Hintergrund der anhaltenden Serie erfolgreicher Sicherheitsverletzungen bei Microsoft erschien im Juni 2024 ein interessanter Artikel.

Zusammengefasst: Andrew Harris, der zu dem Zeitpunkt bei Microsoft arbeitete, entdeckte eine schwerwiegende Schwachstelle in Active Directory Federation Services (ADFS) und versuchte verzweifelt, sie zu beheben. Seine Befürchtungen wurden heruntergespielt, und da die US-Bundesregierung im Begriff war, einen milliardenschweren Vertrag mit Microsoft für ihre Cloud-Dienste zu unterzeichnen, wurde das Problem im Wesentlichen unter den Teppich gekehrt. Nachdem er Microsoft im Jahr 2020 verlassen hatte, wurde der SolarWinds-Angriff, der wahrscheinlich größte Angriff aller Zeiten auf eine Lieferkette, aufgedeckt. Während der Fokus auf SolarWinds und ihr kompromittiertes Orion-Produkt gerichtet war, breiteten sich russische Angreifer über Netzwerke aus, indem sie die ADFS-Schwachstelle ausnutzten. Dies geschah natürlich lange vor dem weiter unten erwähnten Bericht des Cyber Safety Review Board (CSRB) und lange bevor die Secure Future Initiative (SFI) bei Microsoft ernsthaft in Angriff genommen wurde, aber die Zeit wird zeigen, ob das „neue" Microsoft tatsächlich Sicherheit über neue Funktionen stellt, was für jedes kommerzielle Unternehmen eine Herausforderung darstellt.

Jedes Unternehmen muss selbst entscheiden, inwieweit es sich von einzelnen Anbietern wie Microsoft abhängig machen möchte. Angesichts der über Jahre hinweg aufgetretenen Sicherheitsbedenken und der klar begrenzten Verantwortung Microsofts für die Daten seiner Kunden sollte diese Entscheidung jedoch eindeutig ausfallen.

> **WOFÜR IST MICROSOFT VERANTWORTLICH?**

Viele fragen sich: „Wenn Microsoft sich nicht um meine Daten und meine Sicherheit kümmert, wofür sind sie dann wirklich verantwortlich?“ Die aktuelle Haltung von Microsoft zu dieser Frage hat sich auch 2024 nicht geändert. Um dies zu verstehen, muss man mit dem Modell der geteilten Verantwortung von Microsoft vertraut sein.

Das Modell der geteilten Verantwortung besagt, dass:

DIE „VERANTWORTUNG IMMER BEIM KUNDEN LIEGT“:

- Informationen und Daten
- Geräte (Handys und PC)
- Konten and Identitäten

Im Wesentlichen ist der Kunde für die Sicherung und den Schutz seiner Informationen und Daten verantwortlich. Microsoft ist es nicht. Wenn Unternehmen in die Cloud wechseln, müssen sie dies bei der Implementierung von Schutzstrategien berücksichtigen.

Ein weiterer erwähnenswerter Punkt ist einer, den wir bereits im letzten Jahr in diesen Bericht aufgenommen hatten. Für viele bestehende M365-Kunden ist dies immer noch eine Überraschung, sodass es auch in diesem Jahresbericht Erwähnung finden sollte. Microsoft hat seine langjährige Haltung zur Verwendung von Backup-Anwendungen mit M365 im Jahr 2023 geändert. Auf einer Microsoft-Konferenz im vergangenen Jahr kündigte Microsoft das Microsoft 365 Backup an. Es wurde ein Dienst vorgestellt, der grundlegende Backup-Funktionen für M365 bereitstellt. Der wichtige Teil dieser Ankündigung ist nicht der Dienst selbst, sondern die Änderung von Microsofts langjähriger Haltung „Sie brauchen keine Daten in M365 zu sichern“. Viele in der Branche sind der Meinung, dass dies auf zwei Faktoren zurückzuführen ist:

1. Microsoft hat endlich kapituliert und stimmt nun zu, dass ein Fokus auf die Datenspeicherung allein in M365 NICHT ausreichend ist
2. Microsoft möchte einfach ein Stück vom M365-Backup-Markt abhaben, nachdem sie gesehen haben, dass es einen großen Markt für einen solchen Dienst gibt

Beide Optionen scheinen wahrscheinlich, wobei Option 2 durch die Tatsache gestärkt wird, dass Microsoft auch eine Backup-API auf den Markt gebracht hat, die Anbieter gegen eine Gebühr nutzen können. Unabhängig davon ist die Botschaft klarer denn je. Unternehmen **SIND** für den Schutz der Daten verantwortlich, die sie in Microsoft Cloud-Diensten speichern.

Die Schwierigkeiten, die durch mehrere Tenants in der Microsoft Cloud auftreten

Da die zentralen Cloud-Dienste von Microsoft seit mehr als einem Jahrzehnt auf dem Markt sind, befinden sich viele Unternehmen in einer Situation, in der sie mehrere Microsoft 365-Umgebungen verwalten und pflegen müssen. Dabei kann es sich um ein Unternehmen handeln, das mehrere Fusionen und Übernahmen durchgeführt hat oder vielleicht handelt es sich um einen Managed Services Provider (MSP), der IT-

Dienste für mehrere Kunden anbietet. In beiden Fällen erkennen viele dieser Unternehmen die Schwierigkeiten bei der Verwaltung mehrerer M365-Tenants.

Wenn wir über den personellen Mehraufwand sprechen, der mit diesem erhöhten Verwaltungsaufwand verbunden ist, kann dies direkte Auswirkungen auf die Sicherheit der Daten in der Cloud haben. In einem Unternehmen wurden höchstwahrscheinlich Standards für bewährte Sicherheitsverfahren und die Aktivierung von Funktionen in den verwalteten M365-Umgebungen definiert. Viele Administratoren stellen fest, dass die Durchsetzung von Standards und die Begrenzung von Konfigurationsabweichungen bzw. -fehlern innerhalb mehrerer unterschiedlicher M365-Tenants äußerst schwierig ist. Bei Cloud-Diensten kann eine einzige Fehlkonfiguration den Unterschied zwischen einem sicheren Unternehmen und einer schwerwiegenden Datenpanne ausmachen.

Die Tenant-Verwaltung wird für Unternehmen, die ihre M365-Daten schützen wollen, immer wichtiger. Microsoft bietet zwar ein Dienstprogramm namens Lighthouse an, aber es hat einige Einschränkungen und viele MSPs sind der Meinung, dass es an Funktionen und Umfang mangelt. Einige Softwareanbieter haben Lösungen entwickelt, um diesen Verwaltungsbedarf für MSPs zu decken, wie z. B. der 365 Multi-Tenant Manager für MSPs von Hornetsecurity. Eine ordnungsgemäße Verwaltung wird in der heutigen Cloud-first-Welt immer wichtiger und die Führungsteams müssen sich der Gefahren bewusst sein, die diese Herausforderungen für die Sicherheit der Daten in der Cloud mit sich bringen.

365 MULTI-TENANT MANAGER FOR MSPs

MEHR ERFAHREN

CYBERSECURITY
REPORT 2025

KAPITEL 3

EINE ANALYSE DER WICHTIGSTEN SICHERHEITSVORFÄLLE UND CYBERSECURITY-NACHRICHTEN DES JAHRES 2024

KAPITEL 3 – EINE ANALYSE DER WICHTIGSTEN SICHERHEITSVORFÄLLE UND CYBERSECURITY-NACHRICHTEN DES JAHRES 2024

Die letzten 12 Monate waren ein Auf und Ab, was die weltweiten Cyber-Ereignisse angeht. Wenn wir alle (großen) Ereignisse abdecken würden, wäre dieser Bericht doppelt so lang. Daher konzentrieren wir uns auf die wichtigsten, die entweder erhebliche gesellschaftliche Auswirkungen haben oder Organisationen einen Einblick in Handlungsoptionen geben, wie sie ihre Cybersicherheitslage verbessern können.

DER CROWDSTRIKE VORFALL

Am 19. Juli 2024 ereignete sich der wohl größte IT-Ausfall aller Zeiten. Innerhalb weniger Minuten stürzten etwa 8,5 Millionen Windows-Systeme weltweit, auf denen der Crowdstrike-Falcon-Agent lief, ab bzw. zeigten nur noch Bluescreens, starteten permanent neu und stürzten wiederholt ab, bis sie manuell repariert wurden. Dieses Endpoint Detection and Response (EDR)-Tool ist (wie alle anderen unter Windows) auf einen Kernel-Treiber angewiesen und ein bestimmtes Signatur-Update wies einen logischen Fehler auf, der das System zum Absturz brachte, nachdem es Daten in einen Teil des Speichers geschrieben hatte, der dafür nicht vorgesehen war. Die geschätzten Kosten der betroffenen Fortune-500-Unternehmen belaufen sich auf über 5,4 Milliarden USD.

Im September veranstaltete Microsoft ein Gipfeltreffen für alle Anbieter von Cybersicherheitslösungen, die Agenten für Windows herstellen, um das weitere Vorgehen zu besprechen und dafür zu sorgen, dass sich ein derartiger Ausfall nie wiederholen kann. Viele schlugen vor, Microsoft solle den Ansatz von macOS übernehmen und den EDR-Agenten keinen Zugriff auf den Kernel, sondern nur auf die API gewähren. Andere Experten, darunter auch wir hier bei Hornetsecurity, sind der Ansicht, dass dies zu drastisch wäre, sowie Innovation hemmt und Microsoft scheint dem zuzustimmen. Es sieht so aus, als ob künftige Windows-Versionen mehr Schutzmechanismen gegen diese Art von Risiken haben werden, ohne jedoch den Kernel-Zugriff ganz zu blockieren.

CHANGE HEALTHCARE

IIm Februar 2024 wurde Change Healthcare, eine Tochtergesellschaft von UnitedHealth, Opfer eines massiven Ransomware-Angriffs, der die persönlichen, finanziellen und medizinischen Daten von etwa 100 Millionen US-Amerikanern kompromittierte. Dieser Angriff wurde der in Russland ansässigen BlackCat-Ransomware-Bande zugeschrieben und gilt als der größte

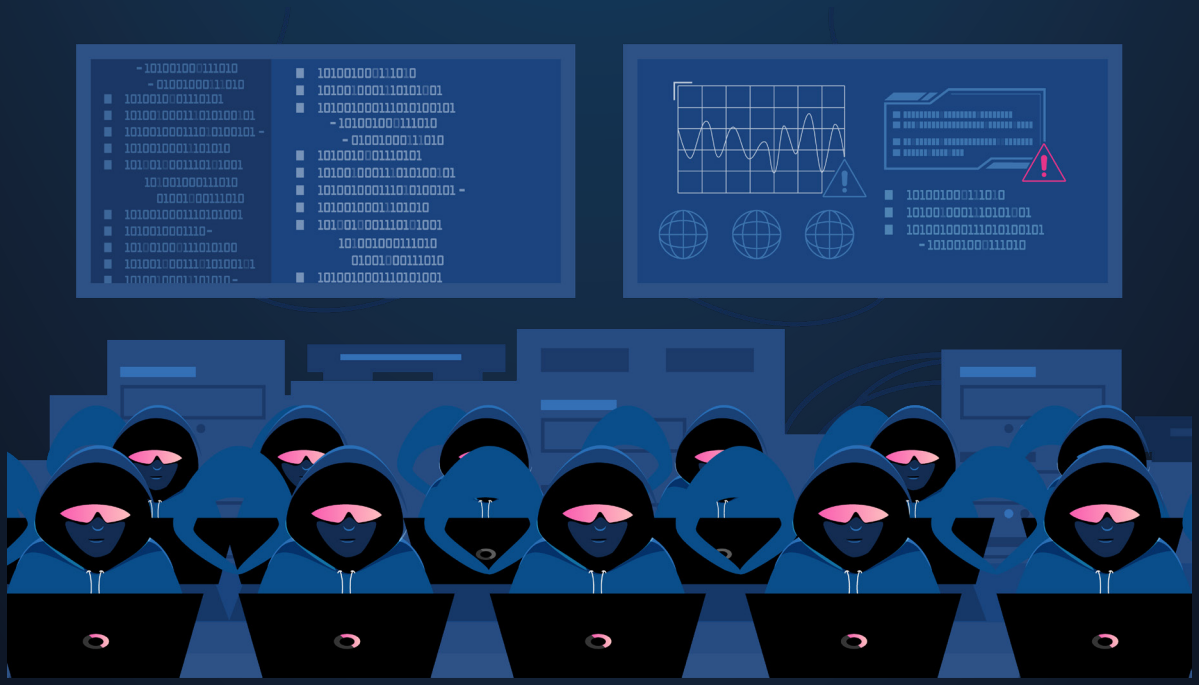
bekannte Angriff auf geschützte Gesundheitsdaten in den USA. Die Angreifer nutzten Schwachstellen im Netzwerk des Unternehmens aus und verschafften sich so Zugang zu sensiblen Daten, darunter Krankengeschichten, Versicherungsdaten und Zahlungsinformationen der Patienten. Die Sicherheitsverletzung deckte nicht nur die Unzulänglichkeiten in der Cybersicherheitsabwehr von Change Healthcare auf, sondern unterstrich auch die breiteren Schwachstellen im US-Gesundheitssektor.

Nach dem Angriff bemühte sich Change Healthcare um Schadensbegrenzung und arbeitete eng mit den Bundesbehörden zusammen, um den Vorfall zu untersuchen. Das Unternehmen sah sich erheblichem Druck seitens der Öffentlichkeit und der Aufsichtsbehörden ausgesetzt, was zu Forderungen nach strengeren Datenschutzbestimmungen im Gesundheitswesen führte.

Eine weitere bemerkenswerte Tatsache an diesem Angriff war, dass es sich um einen von immer mehr Fällen handelt, in denen ein Cyberangriff einen sehr ECHTEN menschlichen Tribut forderte. In diesem Fall gab es Patienten in den USA, die nicht in der Lage waren, wichtige Medikamente rechtzeitig zu erhalten. Ein anderes Beispiel für einen Vorfall mit sehr realen menschlichen Folgen ist ein ähnlicher Angriff auf den britischen NHS (den nationalen Gesundheitsdienst). Diese Angriffe zeigen, dass die Angreifer immer mehr darauf achten, wen sie ins Visier nehmen, und dass sie sich sogar Ziele im Gesundheitswesen aussuchen, um die Wahrscheinlichkeit eines hohen Profits zu erhöhen.

NATIONAL PUBLIC DATA

Die Datenpanne bei National Public Data (NPD), die sich Anfang 2024 ereignete, ist eine der größten Datenpannen der Geschichte, bei der bis zu 2,9 Milliarden Datensätze offengelegt wurden. Betroffen waren rund 170 Millionen Menschen in den USA, Großbritannien und Kanada. Zu den gestohlenen Daten gehörten hochsensible persönliche Informationen wie vollständige Namen, Sozialversicherungsnummern, Postanschriften, E-Mail-Adressen und Telefonnummern. Die Sicherheitsverletzung wurde entdeckt, als sich ein böswilliger Akteur im Dezember 2023 Zugang zu den Systemen des Unternehmens verschaffte und die Daten von April bis Sommer 2024 ins Dark Web stellte.



Die mit dieser Sicherheitsverletzung verbundenen Risiken sind beträchtlich, da die offengelegten Daten für verschiedene Cyberstraftaten und betrügerische Aktivitäten ausgenutzt werden können. Für die von der Sicherheitsverletzung betroffenen Personen besteht das erhöhte Risiko, dass sie Opfer werden von Identitätsdiebstahl, unbefugten Finanzaktivitäten und gezielten Phishing-Angriffen. Das Besondere an diesem Datenschatz ist, dass Bedrohungsakteure ihn für die Vernetzung von Personen nutzen können. So können sie immer überzeugendere Social-Engineering-Angriffe auf künftige Opfer durchführen.

HACKERANGRIFF AUF MGM UND CAESAR'S CASINO

Dieser Angriff ereignete sich Ende Oktober 2023, als wir gerade dabei waren, den letzten Schliff am Bericht für 2023 vorzunehmen. Er ist uns hier eine Erwähnung wert, da die Auswirkungen in den Datenzeitraum für diesen Bericht fallen. Hinzu kommt, dass es sich um einen der folgenreichsten Angriffe der letzten 12 Monate handelte, vor allem aufgrund der Größe der betroffenen Unternehmen.

Im Oktober 2023 waren sowohl MGM als auch Caesar's Casinos und Resorts von Ransomwarangriffen betroffen. MGM hat das Lösegeld nicht gezahlt und erwartet, dass die Wiederherstellung 100 Millionen USD kosten wird, während Caesar's zahlte, etwa 15 Millionen USD. Die Lektion hier ist nicht die Zahlung des Lösegelds, sondern die Art und Weise, wie die Angreifer sich überhaupt Zugang verschaffen konnten: mit unerbittlichem Social Engineering gegen Helpdesk-Mitarbeiter, einschließlich des Angebots von Bestechungsgeldern.

DATENLECK BEIM DNA-TESTDIENST 23ANDME

Die große Sicherheitslücke beim DNA-Testdienst 23andMe wurde von dem Unternehmen mehrere Monate lang heruntergespielt, bis im Dezember 2023 klar wurde, dass die Daten von 6,9 Millionen Kunden gestohlen wurden (aber nicht an die Öffentlichkeit gelangten), während die Daten von 1 Million Kunden mit jüdischem Erbe auf BreachForums, einem inzwischen nicht mehr existierenden populären Hackerforum, geleakt wurden. MFA gab es nicht, ist aber jetzt für alle Nutzer verpflichtend. 23andMe steht derzeit vor ernsthaften finanziellen Problemen, die zum Teil auf den Verstoß zurückzuführen sind.

LOCKBIT'S FÜHRENDE KÖPFE ENTTARNT

Im Februar 2024 wurden die führenden Köpfe von LockBit, einst eine der größten kriminellen Ransomware-Banden, unter der Leitung der britischen National Crime Agency selbst gehackt und ihr Anführer als Dmitry Yuryevich Khorosev identifiziert. Dies ist Teil eines interessanten Trends, bei dem die Strafverfolgungsbehörden identifizierte Kriminelle nicht ausliefern oder verhaften können, weil sie sich in Russland oder in anderen Ländern befinden, in denen die Behörden kein Problem damit haben, Kriminellen Unterschlupf zu gewähren (solange sie keine inländischen Ziele angreifen). Deshalb ist „Doxing" oder die Offenlegung der Identität einer Person eine Möglichkeit, ihnen indirekt das Leben schwer zu machen. Denn wenn andere Kriminelle wissen, wer sie sind und wo sie sich aufhalten, könnten sie ihnen einen Besuch abstatten.

XZ UTILS BACKDOOR

Die spannende Geschichte rund um die XZ Utils Backdoor wurde im März 2024 aufgedeckt. Hier bauten gefälschte Identitäten über mehrere Jahre hinweg eine Beziehung zum Betreuer des Open-Source-Softwarepakets (OSS) XZ Utils auf. Sie halfen bei der Aktualisierung des Codes und der Erstellung von Dokumentationen mit dem Ziel, selbst die Verantwortung für das Paket zu übernehmen, und schleusten dann einen bösartigen Payload ein, mit der jede Secure Shell (SSH)-Verbindung entsperrt werden konnte, wenn man den speziellen Schlüssel hatte.

Das Malware-Paket gelangte nur in Alpha-/Testversionen verschiedener Linux-Distributionen und wurde von Andres Freund (Microsoft) entdeckt, der beim Testen eines Open-Source-Datenbankpakets seltsame CPU-Spitzen bemerkte. Hätte es das Paket in das Mainstream-Linux (und andere Systeme, die auf SSH angewiesen sind) geschafft, hätte es weitreichende Auswirkungen haben können. Für diesen Angriff wurde offiziell noch kein Schuldiger benannt, aber die meisten Experten sind sich einig, dass es sich um russische Spione handelt. Die Schlussfolgerung daraus ist, dass man, wenn man firmeneigene Software entwickelt, die auf OSS-Komponenten beruht (was fast immer der Fall ist), deren Sicherheitslage (und auch die ihrer Bausteine) bei der Risikobewertung in Betracht ziehen muss.

EIN JAHR VOLLER MICROSOFT-SICHERHEITSDRAMEN

Microsoft hatte in den letzten Jahren kein einziges gutes Jahr, wenn es um die Sicherheit ging. Im Juni 2023 kompromittierte die chinesische Gruppe (Storm-0558) die E-Mail-Postfächer von 22 Organisationen weltweit, darunter das US-Außenministerium (60.000 gestohlene E-Mails).

Im Januar 2024 brach Midnight Blizzard (Russland) in die Firmenpostfächer von Microsoft ein und verschaffte sich durch Erraten von Passwörtern Zugang zu einem Test-Tenant, der über eine OAuth-Anwendung über Zugriff auf die Produktionsumgebung verfügte. Dem vorausgegangen waren bereits Angriffe von Midnight Blizzard im Jahr 2020 (SolarWinds) und der Hackingangriff vom Juli 2021, bei dem sie Informationen über eine begrenzte Anzahl von Kunden stahlen. Im März 2024 folgte ein weiterer Angriff, bei dem auf einige interne Systeme und Quellcode-Repositories zugegriffen wurde, wobei die bei dem Angriff im Januar gestohlenen Authentifizierungsdaten verwendet wurden.

Im April 2024 veröffentlichte das Cyber Safety Review Board (CSRB) seinen dritten Bericht, der sich diesmal auf den oben erwähnten chinesischen Hackerangriff im Jahr 2023 konzentrierte. Der Bericht enthielt eine vernichtende Bewertung der Gründe für die Kompromittierung von Microsoft, beschrieb eine Reihe von Versäumnissen, die zu der Sicherheitsverletzung führten, und enthielt 25 Empfehlungen für Verbesserungen.

Dieser Bericht und die Angriffe haben Microsoft dazu veranlasst, die Secure Future Initiative (SFI) zu initiieren, die ursprünglich eher wie ein Marketing-Flyer aussah, aber aufgrund derer jetzt alle Microsoft-Mitarbeiter jährlich auf ihre Sicherheit hin überprüft werden. Das neue Mantra von Satya Nadella lautet: „Sicherheit steht an erster Stelle". Wir werden sehen, wie sich das in den nächsten ein oder zwei Jahren entwickeln wird.

CYBERSECURITY
REPORT 2025

KAPITEL 4

VORHERSAGE DER BEDROHUNGSLANDSCHAFT IM JAHR 2025

KAPITEL 4 – VORHERSAGE DER BEDROHUNGSLANDSCHAFT IM JAHR 2025

LAGEN WIR MIT UNSEREN VORHERSAGEN DES LETZTEN JAHRES RICHTIG?

Ein Rückblick auf unsere verschiedenen Vorhersagen im Cybersecurity Report ist eine interessante Übung, denn es ist immer eine Herausforderung, die Zukunft vorherzusagen. Wir haben bei einigen Aspekten definitiv richtig gelegen und einige Vorhersagen haben sich nicht so entwickelt, wie wir erwartet hatten.

$459 MIO. USD

LÖSEGELD BEZAHLT IM ERSTEN HALBJAHR 2024

Im Jahr 2024 gibt es mehr Ransomware-Gruppen und mehr Einträge auf Leak-Sites als im Jahr 2023, was darauf hindeutet, dass Ransomware nach wie vor auf dem Vormarsch ist und Unternehmen noch stärker gefährdet sind als im letzten Jahr. Obwohl die Prognose lautete, dass 2024 ein "furchtbareres" Jahr werde als 2023, belief sich der ungefähre Betrag der 2023 gezahlten Lösegelder auf 1,1 Mrd. USD, während die Statistik für das erste Halbjahr 2024 459 Mio. USD ausweist. Dies ist zum Teil auf höhere Zahlungen für schwerwiegendere Sicherheitsverletzungen zurückzuführen, wobei das bisher höchste bekannte Lösegeld 75 Millionen USD betrug (von einem unbekannten Fortune 50-Unternehmen).

Wir hatten erwartet, dass MFA-Fatigue-Angriffe und MFA-Bypass-Angriffe zunehmen würden, und das war auch der Fall. Die Anzahl und Verbreitung sowohl von Open-Source- als auch von „kommerziellen" Kits für die Erstellung von E-Mail-Ködern und die Einrichtung von Proxy-Diensten, die vorgeben, eine echte Anmeldeseite zu sein, ist als Reaktion auf die zunehmende Verbreitung von MFA-Optionen mit Push-Benachrichtigung explodiert. Um dies im Unternehmen zu bekämpfen, sollte man nach phishing-resistenten MFA-Lösungen wie Windows Hello for Business, FIDO2-Hardwareschlüssel oder Passkeys suchen, bei denen ein Smartphone als FIDO2-Schlüssel verwendet wird, sodass keine zusätzliche Hardware gekauft werden muss. Diese Technologien sind an die legitime Anmeldeseite gebunden, sodass die Anmeldetechnologie nicht funktioniert, wenn der Benutzer auf eine gefälschte Website gelockt wird, weshalb sie auch als phishing-resistent bezeichnet werden. Unsere Empfehlungen für passwortlose Sicherheit aus dem Cybersecurity Report 2024 gelten auch heute noch, mit dem einzigen Zusatz von Passkeys, die ebenfalls passwortlos und phishing-resistent sind.

Wir haben einige Risiken mit dem alten Microsoft Teams-Client erkannt, der auf der Elektron-Plattform aufgebaut war. Glücklicherweise wurde er jetzt durch den neuen Teams-Client ersetzt, der nicht so viele

Schwachstellen zu haben scheint. Teams ist nach wie vor ein Angriffsvektor für Phishing-Köder, auch wenn dies nicht mehr so häufig vorkommt, seit Microsoft die Standardoptionen für die Annahme von Mitteilungen von externen Parteien geändert hat und Warnungen anzeigt, wenn ein neuer Kontakt versucht, einen Nutzer zu erreichen.

Spyware und Malware auf Smartphones sind ein ständiges Thema, wobei sowohl die EU als auch die USA Maßnahmen ergriffen haben, um die Verbreitung von Anbietern und deren Einsatz Spyware und Malware in demokratischen Gesellschaften einzudämmen, wie wir es vorausgesagt haben.

Wie wir bereits erwähnt haben, haben die Angriffe auf Anwendungsprogrammierschnittstellen (APIs) im Jahr 2024 gegenüber 2023 zugenommen (verschiedene Quellen schätzen zwischen 20 und 29 %). Diese sind oft ein „versteckter" Angriffsvektor und daher bei Kriminellen beliebt, da die Überwachung und Alarmierung bei APIs nicht so robust sind, wie bei anderen Systemen. Wenn ein Unternehmen APIs für seine Webanwendungen öffentlich zugänglich macht, sollte es sicherstellen, dass es über ein robustes Sicherheitsmodell für den Zugriff verfügt, und diese auf böswillige Nutzung, einschließlich DDOS-Angriffe überwachen.

Wie wir vorausgesagt haben, ist die Verwaltung der Cybersicherheit von Microsoft 365-Tenants nach wie vor eine Herausforderung. Wir möchten jedoch auf ein neues Tool hinweisen, das derzeit als öffentlichen Vorschauversion für alle M365-Tenants verfügbar ist – Exposure Management. Es gibt einen Einblick in die Sicherheitskonfiguration und -lage der Tenants sowie in Initiativen, auf die man sich konzentrieren kann, um bestimmte Bereiche wie die Abwehr von BEC-Angriffen oder Ransomware zu verbessern.

Die Time-to-Exploit (die Zeit zwischen dem Bekanntwerden einer Schwachstelle und der Verfügbarkeit eines funktionierenden Exploits für diese Schwachstelle) ist von 63 Tagen im Jahr 2018/2010 auf 32 Tage im Jahr 2021/2022 und auf fünf Tage im Jahr 2023 gesunken. Die Statistiken für 2024 liegen zwar noch nicht vor, aber es gab bereits mehrere erfolgreiche Angriffe innerhalb weniger Tage nach Bekanntwerden einer Sicherheitslücke. Dies stellt eine weitere Belastung für die Verteidiger dar, da das Patchen kontinuierlicher Aufwand ist und nicht alles auf einmal gepatcht werden kann. Es müssen Prioritäten gesetzt werden,

um sicherzustellen, dass die dem Internet ausgesetzten Geräte auf dem neuesten Stand gehalten werden.

Wir haben uns IoT-Geräte als Vektor für Angriffe in Unternehmensnetzwerken angesehen, und in den ersten fünf Monaten des Jahres 2024 ist die Zahl der Angriffe um 107 % gegenüber dem gleichen Zeitraum im Jahr 2023 gestiegen.

Obwohl wir 2024 einige überzeugende Deep Fakes gesehen haben, haben wir trotz der Unterstützung von KI-Tools für die Generierung von Bildern, Audio und Video noch keine größeren Sicherheitsverletzungen gesehen, die durch diese verursacht wurden. Wir gehen jedoch davon aus, dass diese Tools immer einfacher und leistungsfähiger werden und wir mehr Angriffe und allgemeine Desinformationskampagnen sehen werden, die sich auf sie stützen.

DIE VORHERSAGEN DES SECURITY LABS

Im Rahmen dieses Berichts untersucht das Security Lab-Team von Hornetsecurity jedes Jahr den Zustand der Branche, unsere Daten, Angriffstrends und mehr, um eine Reihe von Prognosen für das kommende Jahr zu erstellen.

Dies dient dazu, Unternehmen darüber zu informieren, welchen potenziellen Bedrohungen sie im kommenden Jahr ausgesetzt sein werden und wie sich die Branche verändern könnte. Im Folgenden finden Sie die Vorhersagen von Security Lab für das Jahr 2025.

SECURITY LAB CYBERSECURITY INSIGHTS & ANALYSIS

Es dürfte nicht überraschen, dass viele unserer Vorhersagen in diesem Bericht mit KI zu tun haben. Einige dieser Vorhersagen lassen sich leicht in Gruppen zusammenfassen, andere sind spezifischer. Wir haben diese Vorhersagen in diesem Abschnitt aufgeschlüsselt.

LLMS IN DEN HÄNDEN DER ANGREIFER

Letztes Jahr haben wir uns mit dem Aufstieg von ChatGPT und anderen Large Language Models (LLMs) und deren Auswirkungen auf die Cybersicherheit sowohl für Angreifer als auch für Verteidiger beschäftigt. Die ursprünglichen Befürchtungen, dass LLMs fehlerfreien Schadcode schreiben könnten, haben sich nicht bewahrheitet, und die Integration von KI-Chat-Schnittstellen und anderen Automatisierungen in Sicherheitslösungen hat eher den Verteidigern geholfen.

Wir haben einige aktuelle Fälle gesehen, bei denen LLMs von Angreifern auf Microsoft genutzt wurden, darunter der Fall von Forest Blizzard, einer mit dem russischen Staat in Verbindung stehende Bedrohungsgruppe, die LLMs zur Erforschung von Satelliten- und Radartechnologien, wahrscheinlich zur Unterstützung des Krieges in der Ukraine, sowie zur Unterstützung von Skripting-Aufgaben, einschließlich der Manipulation von Dateien, verwendete. Emerald Sleet aus Nordkorea hingegen setzt Phishing in großem

Umfang ein, um seine Ziele anzulocken, und nutzte LLMs, um bekannte Schwachstellen zu verstehen und die Sprache und den Ton in Phishing-Nachrichten zu verbessern. Crimson Sandstorm (Iran, mit Verbindung zum Korps der Islamischen Revolutionsgarden) nutzte LLMs für Social-Engineering, Fehlerbehebung und zur Unterstützung bei der .NET-Entwicklung. Bemerkenswert ist, dass fast alle diese Anwendungsfälle auch mit gewöhnlichen Suchmaschinenabfragen hätten erfüllt werden können, die es Microsoft nicht ermöglicht hätten, diese Erkenntnisse zu sammeln. Die Angreifer haben also bei ihrer operativen Sicherheit (OpSec) versagt, als sie ein öffentliches LLM für ihre Recherchen nutzten.

Angriffe auf LLMs selbst nehmen weiter zu und MITRE hat ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) geschaffen, um die verschiedenen Arten zu verfolgen, ähnlich wie die Enterprise-Matrix ATT&CK.

In Anbetracht all dessen ist es wahrscheinlich, dass KI/LLM im kommenden Jahr aus mehreren Gründen ein Thema in Diskussionen über Cybersicherheit sein wird:

1. **KI wird zunehmend für die Aufklärung und Informationsbeschaffung eingesetzt werden**
2. **KI wird Angreifern dabei helfen, auf der Grundlage der bereitgestellten Daten den besten Zeitpunkt für Angriffe zu ermitteln**
3. **KI wird weiterhin eingesetzt werden, um nahezu jeden Angriffsvektor für Bedrohungsakteure zu verbessern, einschließlich E-Mail, Sprache, Social Engineering ... usw.**
4. **KI wird zunehmend eingesetzt werden, um leicht auszunutzende Objekte in schwachen Infrastrukturen schnell zu identifizieren**
5. **KI-gestützte Tools werden sich weiterentwickeln, um Verteidiger zu unterstützen**

KI-GESTÜTZTE DEEPFAKES WERDEN FÜR SPEAR-PHISHING UND ZUR BEEINFLUSSUNG DER ÖFFENTLICHKEIT EINGESETZT

Der Einsatz von Deepfake-Technologie bei Spear-Phishing-Angriffen ist ein wachsendes Problem und wir werden diese Kombination im Jahr 2025 wahrscheinlich öfter sehen. Deepfakes können äußerst realistische Videos und Audioaufnahmen erstellen, die das Aussehen und die Stimme echter Personen imitieren. Mit dieser Technologie können überzeugende Phishing-Nachrichten erstellt werden, die den Empfänger dazu verleiten, vertrauliche Informationen preiszugeben oder Aktionen auszuführen, die die Sicherheit gefährden.

Das Aufkommen fortschrittlicher Deepfake-Technologie stellt auch eine potenzielle Bedrohung für die öffentliche Meinung und das Vertrauen dar. Deepfakes können äußerst realistische Videos und Audioaufnahmen erstellen, die nur schwer von echten Inhalten zu unterscheiden sind. Diese Technologie wurde bereits zur Verbreitung von Fehlinformationen eingesetzt und wird von Bedrohungsakteuren weiterhin verstärkt genutzt werden. Dies wird zu einer Erosion des Vertrauens in die digitalen Medien führen.

WIR WERDEN BALD BEMERKENSWERTE ANGRIFFE AUF LLM-PRODUKTE SEHEN

Large Language Models (LLMs) werden immer beliebter, sind aber auch selbst anfällig für verschiedene Arten von Angriffen. Dazu gehören Injection-Angriffe, Datenexfiltration und Jailbreaks, bei denen böswillige Akteure die Eingabedaten manipulieren, um das Modell zu täuschen oder sensible Informationen zu extrahieren. Diese Schwachstellen können die Integrität, die Sicherheit und letztlich auch das Vertrauen in LLM-basierte Systeme beeinträchtigen.

Angesichts der zunehmenden Abhängigkeit von diesen Systemen würden Bedrohungsakteure (insbesondere Nationalstaaten) nichts lieber tun, als ein beliebtes LLM zu ihrem Vorteil zu nutzen. Ob es sich dabei um Desinformation, die Verbreitung von bösartigen Links oder etwas anderes handelt, bleibt abzuwarten.

ES WIRD DURCH DEN EINSATZ VON KI ZU RECHTSFÄLLEN UND ZU EINER REGULIERUNG KOMMEN

Seit ChatGPT auf dem Markt für Aufsehen sorgte, wird dies ausführlich diskutiert. Die Frage der Rechtmäßigkeit, des Urheberrechts und der Eigentumsverhältnisse hat KI-generierte Inhalte in fast jeder Phase der Entwicklung begleitet. Dennoch werden wir wahrscheinlich einen Punkt erreichen, an dem es aufgrund der Nutzung von LLMs zu häufigeren und wirkungsvolleren Rechtsstreitigkeiten kommt.

Infolgedessen wird es wahrscheinlich auch zu einer Art staatlicher Regulierung des Einsatzes von KI durch große Nationalstaaten kommen. Dabei wird es wahrscheinlich vor allem um den Datenschutz gehen, insbesondere in Regionen wie der EU, die mit ihrem KI-Gesetz bereits eine Vorreiterrolle einnimmt. Diese neuen Vorschriften werden nicht nur die Aufmerksamkeit der LLM-Entwickler selbst erfordern, sondern auch die von Unternehmen, die generative KI in ihren eigenen Organisationen einsetzen wollen.

NEUE REGULATORISCHE RAHMENBEDINGUNGEN UND HERAUSFORDERUNGEN

Apropos Regulierung: Die Einführung neuer Regelwerke wie NIS2, DORA, CRA und KRITIS (nur in Deutschland) wird Unternehmen vor große Herausforderungen stellen. Diese neuen Rahmenwerke zielen darauf ab, die Cybersicherheit und den Datenschutz zu verbessern und sind dringend erforderlich, aber ihre

Einhaltung wird für viele Unternehmen schwierig und ressourcenintensiv werden. Darüber hinaus wird sich die Rolle des Compliance-Beauftragten in vielen Unternehmen weiterentwickeln und zunehmend an Bedeutung gewinnen.

Nebenbei bemerkt wird auch die Zahl der Unternehmen zunehmen, die eine bestimmte Art der Einhaltung von Vorschriften verlangen, um mit ihnen Geschäfte zu machen. Angriffe auf die Lieferkette werden immer häufiger und schädlicher, und anstatt Partnern wie früher uneingeschränkt zu vertrauen, verlangen viele Unternehmen von ihren Kunden und/oder Lieferanten, dass sie sich an dieselben rechtlichen Rahmenbedingungen halten, an die sie selbst auch gebunden sind.

KORRUPTION DER OPEN-SOURCE-GEMEINSCHAFT

Viele Jahre lang galt Free und Open Source Software (FOSS) als so etwas wie eine Oase in einem als sicherheitsarm empfundenen Software-Ökosystem. Seit dem XZ Utils-Vorfall, den wir weiter oben in diesem Bericht besprochen haben, und mehreren anderen bekannten Sicherheitslücken ist diese Einschätzung nicht mehr zutreffend. Bei XZ Utils versuchte ein sehr entschlossener Bedrohungsakteur, ein sehr beliebtes Open-Source-Paket für einen weit verbreiteten Supply-Chain-Angriff zu nutzen. Angesichts dieses (beinahe) Erfolgs ist es wahrscheinlich, dass Angreifer etwas Ähnliches mit anderen branchenkritischen Open-Source-Paketen versuchen werden. Die Zahl der bösartigen Open-Source-Pakete hat bereits deutlich zugenommen und die jüngsten Vorfälle mit dem PyPi-Software-Repository sind wahrscheinlich nur ein Vorgeschmack auf das, was noch kommen wird.

FORTGESETZTE VORHERSAGEN FÜR DAS QUANTENCOMPUTING

In früheren Berichten haben wir über eine Bedrohung gesprochen, die zwar nicht unmittelbar bevorsteht, aber sich am Horizont abzeichnet: Quantum Computing. Obwohl wir noch einige Jahre von einem kryptografisch relevanten Quantencomputer (CRQC) entfernt sind, schätzen einige Experten, dass dies 2037, minus 5 bis plus 20 Jahre, der Fall sein wird. Die Entwicklung schreitet rasch voran. Der Tag, an dem diese Computer Realität werden, wird als Q-Day bezeichnet. Und wenn Unternehmen heute sensible Daten in verschlüsselter Form speichern, auf die sie voraussichtlich auch in zehn Jahren noch zugreifen müssen, sollten sie sich jetzt damit befassen. Denn die NSA und vermutlich auch ihre Pendants in anderen Ländern erfassen riesige Datenmengen, die sie zwar heute noch nicht entschlüsseln können, aber vielleicht in Zukunft in der Lage sein werden.

Das NIST in den USA stimmt dem zu und hat drei Post-Quantum-Verschlüsselungsalgorithmen standardisiert:

- ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)
- ML-DSA (Module-Lattice-Based Digital Signature Algorithm)
- SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)

Ein vierter Standard ist ebenfalls in Vorbereitung. Die neuen Namen geben an, in welchem Bereich der Kryptografie sie eingesetzt werden sollen.

Microsoft nimmt diese aufkommende Bedrohung durch das Quantum Safe Program ebenfalls ernst und kündigte kürzlich an, dass seine Open-Source-Kryptobibliothek SymCrypt, die in Windows 10 und 11, im Windows Server, Azure und Microsoft 365 verwendet wird, nun ML-KEM unterstützt, wobei die Unterstützung von ML-DSA und SLH-DSA bald folgen wird.

Die Herausforderung bei Quantencomputern ist die Skalierung, sowohl was die Anzahl der physikalischen Qubits (ein CRQC benötigt viele Tausend) als auch die Fehlerkorrektur betrifft, die erforderlich ist, um ein zuverlässiges logisches Qubit zu erzeugen, gegen das programmiert werden kann. Wir empfehlen nach wie vor, dass wenn Unternehmen über sensible Daten verfügen, die sie voraussichtlich/aufgrund gesetzlicher Vorschriften über zehn Jahre aufbewahren müssen, herausfinden sollten, wie sie diese mit einem quantensicheren Algorithmus verschlüsseln können, insbesondere jetzt, da die Standards ratifiziert wurden.

VERMEHRTE EINFÜHRUNG VON „MEMORY SAFE"-SPRACHEN

Software ist seit langem von Sicherheitsproblemen betroffen, die auf Probleme bei der Speicherverwaltung zurückzuführen sind. Dazu gehören Dinge wie Pufferüberläufe und Use-after-free-Fehler. Infolgedessen hat die Branche begonnen, auf „Memory Safe"-Sprachen wie Rust und/oder Swift umzustellen.

Diese Sprachen verfügen über einen integrierten Schutz gegen viele gängige speicherbezogene Schwachstellen und erleichtern Softwareentwicklern das Schreiben von sicherem Code. Angesichts der bevorstehenden Regulierung der Softwarebranche werden Entwickler diese Sprachen wahrscheinlich verstärkt einsetzen, um ihre Software nicht nur sicherer zu machen, sondern sich auch rechtzeitig auf die genannten Vorschriften vorzubereiten.

WIE GEFÄHRDET WIRD MEIN UNTERNEHMEN IM JAHR 2025 SEIN?

Unsere Antwort auf diese Frage ist im Großen und Ganzen dieselbe wie in den Vorjahren: Wenn eine Organisation in der Lage ist, ein Lösegeld zu zahlen, oder sie über Informationen über geistiges Eigentum verfügen, die gewinnbringend verkauft werden können, **SIND** sie ein Ziel.

Dies wird durch unsere Daten zum E-Mail-Bedrohungsindex belegt, die zeigen, dass Cyberkriminelle weiterhin alle Branchen ins Visier nehmen. Wenn ein Unternehmen jedoch mit sensiblen Daten arbeitet, im Verteidigungssektor oder in der kritischen Infrastruktur tätig ist oder über sehr wertvolles geistiges Eigentum verfügt, ist es ein Ziel mit noch höherer Priorität.

WAS ORGANISATIONEN TUN SOLLTEN, UM SICH ZU VERTEIDIGEN

MIT DEN GRUNDLAGEN BEGINNEN

Organisationen neigen dazu, auf spezifische Bedrohungen zu reagieren und punktuelle Sicherheitslösungen für jeden Bereich zu implementieren. Sie konzentrieren sich somit auf technologische Lösungen, anstatt sich zunächst mit den Grundlagen der Sicherheitshygiene zu befassen. Die überwiegende Mehrheit der Unternehmen, die Opfer eines Angriffs werden, fällt nicht einem obskuren Zero-Day-Exploit oder einer fortgeschrittenen Hacking-Technik zum Opfer. Ihre Abwehrmechanismen versagen, 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 Backups nicht durch das Testen von Wiederherstellungsverfahren validiert werden, kann ein Ransomware-Angriff sehr unangenehme Folgen haben, ebenso wie eine nachlässige Patching-Politik.

Mit anderen Worten: Man sollte sich zuerst um eine grundlegende Sicherheitshygiene kümmern, die sowohl die Technologie als auch die Prozesse und Mitarbeiter umfasst. Der erste Schritt ist eine Zero-Trust-Mentalität:

- **Jede Verbindung überprüfen** - nur weil ein Gerät verwaltet wird, ist es nicht automatisch sicher, und nur weil ein Benutzer eine Verbindung von einem bekannten Netzwerk aus herstellt, heißt das nicht, dass es sich nicht um einen Angreifer handelt, der gestohlene Anmeldedaten verwendet.

- **Das Prinzip der geringsten Privilegien verwenden** – Benutzern und Workload-Identitäten sollten nur die Berechtigungen gegeben werden, die sie zur Erfüllung ihrer Aufgaben benötigen. Regelmäßige Überprüfungen stellen sicher, dass sich die erteilten Berechtigungen nicht anhäufen.

- **Von einer Sicherheitsverletzung ausgehen** – Unternehmen sollten ihre Abwehr so stark aufbauen, wie es ihr Budget zulässt, aber arbeiten Sie auch die möglichen Szenarien durch, wenn diese fehlschlagen. Wie werden Sie feststellen, dass ein Angreifer einen Benutzer kompromittiert hat? Wie können Sie die Fähigkeit eines Angreifers einschränken, sich lateral in Ihrer Umgebung zu bewegen?

Eine ausführlichere Liste finden Sie in den ZT-Geboten von Open Groups.

AUF DEN AUFBAU EINER SICHERHEITSKULTUR KONZENTRIEREN

Ein Unternehmen in ein cyber-resilientes Unternehmen zu verwandeln, erfordert Zeit, Mühe und Ausdauer. Man kann sein Unternehmen nicht in eine gut verteidigte Cyberfestung verwandeln, ohne alle Mitarbeiter einzubeziehen und ihnen zu verdeutlichen, wie sie davon betroffen sind und warum sie Teil der Lösung sein müssen.

Wenn es an der Zeit ist, MFA einzuführen, sollte man sicherstellen, dass die Unternehmensleitung mit gutem Beispiel vorangeht und dass sie (und der Vorstand) den Grund für die zusätzlichen Schwierigkeiten bei der Authentifizierung verstehen. Zu diesem Kulturwandel gehört auch die Einsicht, dass Cyber-Resilienz nicht die Aufgabe der IT-Abteilung oder der Sicherheitsabteilung ist. Wenn die Marketingabteilung eine Website und eine SaaS-Lead-Tracking-Lösung einführt, ohne die IT- und Sicherheitsabteilung einzubeziehen, liegt das Risiko, das dadurch entsteht, bei der Marketingabteilung. Jede Technologie- oder Prozessentscheidung, die die Arbeitsweise eines Unternehmens bestimmt, birgt ein Risiko. Die Art und Weise, wie dieses Risiko gemanagt wird, muss für das Unternehmen transparent sein, damit es gute Entscheidungen treffen kann.

Eine wichtige Lektion für IT- und Sicherheitsabteilungen besteht darin, die richtige Sprache zu sprechen - das Risikomanagement. Wer anfängt, über technische Details zu sprechen und darüber, wie etwas funktioniert, wird alle anderen im Unternehmen verlieren, aber wer Technologie- und Prozessänderungen in die Sprache der Geschäftsrisiken (oder Geschäftschancen) übersetzt, hat die Aufmerksamkeit aller.

Und dieses cyberresistente Unternehmen ist nicht statisch, sondern unterliegt wie andere Geschäftsrisiken (geopolitische, wirtschaftliche, konkurrierende) einem ständigen Wandel und das Unternehmen muss ständig lernen und sich anpassen. Jüngste Beispiele sind die Art und Weise, wie Angreifer „schwächere" Formen von MFA mit Attacker-in-the-Middle-Toolkits oder MFA-Fatigue-Angriffen umgehen oder überwinden. Und Social Engineering ist ein allgegenwärtiges Risiko – wäre der Helpdesk bei der Verteidigung des eigenen Unternehmens erfolgreicher gewesen als die Helpdesks von Caesar's oder MGM?

EINE AUSGEWOGENE SICHERHEITSSTRATEGIE

Um die Herausforderungen des heutigen Sicherheitsökosystems zu meistern, müssen Unternehmen über die Implementierung eines ausgewogenen Sicherheitsansatzes nachdenken – ein Ansatz, der sich mit fortschrittlichen, branchenspezifischen Bedrohungen befasst und gleichzeitig sicherstellt, dass die grundlegenden Sicherheitsmaßnahmen fest etabliert sind.

Sich auf ein einziges Sicherheitstool oder eine einzige Lösung zu verlassen, ist nicht mehr ausreichend. Unternehmen sollten eine mehrschichtige Strategie implementieren, die vor gängigen Angriffsvektoren schützt und gleichzeitig die für ihre Branche typischen Bedrohungen abwehrt. Diese Strategie sollte Folgendes umfassen:

- Spam-/Malware-Erkennung der nächsten Generation mit ATP für die Verhaltensanalyse zum Schutz vor der anhaltenden Flut von E-Mail-basierten Bedrohungen, die wir in dieser Branche erleben.
- Sicherheitsschulungen für Endbenutzer zur Erkennung von Social-Engineering- und Spear-Phishing-Angriffen.
- Sicherungs- und Wiederherstellungsfunktionen sowohl für Daten vor Ort als auch für Daten, die in Cloud-Diensten wie M365 gespeichert sind, um sie im Falle eines Ransomware-Angriffs wiederherstellen zu können.
- Compliance- und Governance-Funktionen, die vor versehentlichen Datenlecks schützen und sicherstellen, dass die Compliance-Kontrollen eingehalten werden.

MEHR LERNEN

Die hier genannten Methoden zum Schutz von Unternehmen sind nur der Anfang. Neben dem Risikomanagement, der Bewertung von Anbietern und der Schulung gibt es ständig wechselnde Vorschriften und Sicherheitsanforderungen. Nicht jedes Unternehmen kann ein Experte in Sachen Sicherheit sein. Sie sollten sich deshalb stets versichern, dass sie vertrauenswürdige Anbieter einsetzen, die nicht nur für die Sicherheit des Unternehmens sorgen, sondern auch die Möglichkeit bieten, von ihrem umfassenden Wissen im Bereich der Cybersicherheit zu profitieren.

Vielleicht verfügt das unternehmenseigene Security-Team über fundierte Kenntnisse zum Schutz vor Datenverlusten, aber es fehlt ihm an Wissen über fortgeschrittene E-Mail-Angriffe. Durch die Zusammenarbeit mit einem vertrauenswürdigen Security-Anbieter wie Hornetsecurity können Unternehmen sowohl das Wissen des Anbieters als auch ihr eigenes nutzen. Gemeinsam können wir alle zusammenarbeiten, um die Sicherheit zu verbessern.

Wenden Sie sich also unbedingt an Ihre Security-Anbieter, um mehr zu erfahren und zu schauen, wie Sie enger zusammenarbeiten können.

HORNETSECURITY
CSR2025

365 TOTAL PROTECTION

NEXT-GEN MICROSOFT 365 SECURITY

BUSINESS

PLAN 1

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

ENTERPRISE

PLAN 2

INCLUDES ALL BENEFITS OF PLAN 1

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

ENTERPRISE BACKUP

PLAN 3

INCLUDES ALL BENEFITS OF PLAN 1 + 2

- AUTOMATIC BACKUP OF M365 DATA
- GRANULAR RECOVERY WITH END USER SELF SERVICE
- UNLIMITED STORAGE IN ONE ALL-INCLUSIVE FEE

COMPLIANCE & AWARENESS

PLAN 4

INCLUDES ALL BENEFITS OF PLAN 1 + 2 + 3

- SECURITY AWARENESS
- PHISHING & ATTACK SIMULATION
- ESI® REPORTING
- PERMISSION MANAGEMENT
- PERMISSION ALERTS
- PERMISSION AUDIT
- DMARC REPORTING & MANAGEMENT
- ENHANCED EMAIL REPUTATION & DELIVERY
- EASY DNS MANAGEMENT & OPTIMISATION
- AI RECIPIENT VALIDATION
- COMMUNICATION PATTERN ANALYSIS
- SENSITIVE DATA CHECK

JETZT ANFRAGEN

ÜBER UNSERE AUTOREN

Andy Syrewicze

Andy Syrewicze verfügt über mehr als 20 Jahre Erfahrung in der Bereitstellung von Technologielösungen in verschiedenen Branchen. Er ist spezialisiert auf IT-Infrastruktur, Cloud und die Microsoft 365 Suite.

Andy Syrewicze ist Microsoft MVP in den Bereichen Cloud und Datacenter Management und einer der wenigen, die auch VMware-Experte sind.

Paul Schnackenburg

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

Paul ist ein angesehener Tech-Autor und in der Community aktiv. Er schreibt ausführliche technische Artikel, die sich auf Hyper-V, System Center, private und hybride Clouds sowie Office 365 und Azure Public Cloud-Technologien konzentrieren.

Er besitzt die Zertifizierungen MCSE, MCSA und MCT.

HORNETSECURITY
CSR2025

KAPITEL 5
QUELLEN

- https://attack.mitre.org/techniques/T1027/006/
- https://github.com/kgretzky/evilginx2
- https://www.techtarget.com/searchSecurity/definition/double-extortion-ransomware
- https://www.csoonline.com/article/569273/what-is-smishing-how-phishing-via-text-message-works.html
- https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/
- https://youtu.be/SScaV2PjFcg?si=Ivjyfnk7YmwUUnVh
- https://www.hornetsecurity.com/de/category/threat-reports/
- https://www.youtube.com/watch?v=o3JFNaNES0Q&list=PLyKOQIbp_zWzsfkSUQ0F-Ved_0bZXts70W&index=13
- https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers
- https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb
- https://www.microsoft.com/en-us/trust-center/security/secure-future-initiative?msocki=35a127b0490c698b23e234bd4819680d
- 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/de/services/365-multi-tenant-manager/
- https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-blackcat-pharmacy-outages/
- https://en.wikipedia.org/wiki/2024_National_Public_Data_breach
- https://cybernews.com/security/mgm-caesars-ransomware-attack-timeline/
- https://www.theverge.com/2024/9/13/24243986/23andme-settlement-dna-data-breach-lawsuit
- https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned
- https://en.wikipedia.org/wiki/XZ_Utils_backdoor
- https://www.cisa.gov/resources-tools/resources/CSRB-Review-Summer-2023-MEO-Intrusion
- https://www.bleepingcomputer.com/news/security/ransomware-rakes-in-record-breaking-450-million-in-first-half-of-2024/
- https://www.politico.eu/article/eu-commission-national-security-does-not-justify-spying-document/

- https://home.treasury.gov/news/press-releases/jy2581
- https://virtualizationreview.com/Articles/2024/03/25/exposure-management.aspx
- https://wca.org/security-attacks-on-iot-devices-surge-by-107-in-early-2024/
- https://atlas.mitre.org/matrices/ATLAS
- https://attack.mitre.org/matrices/enterprise/
- https://www.infosecurity-magazine.com/news/156-increase-in-oss-malicious/
- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- https://www.microsoft.com/en-us/security/blog/2023/11/01/starting-your-journey-to-become-quantum-safe
- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-s-quantum-resistant-cryptography-is-here/ba-p/4238780
- https://github.com/microsoft/SymCrypt
- https://en.wikipedia.org/wiki/Buffer_overflow
- https://en.wikipedia.org/wiki/Dangling_pointer
- https://securityboulevard.com/2024/10/eu-cra-good-intentions-impossible-requirements/
- https://pubs.opengroup.org/security/zero-trust-commandments/
- https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

HORNETSECURITY