proofpoint

BERICHT

Der Faktor Mensch 2022

Personenzentrierte Cybersicherheit vor dem Hintergrund zunehmender Anwenderrisiken

proofpoint.com/de

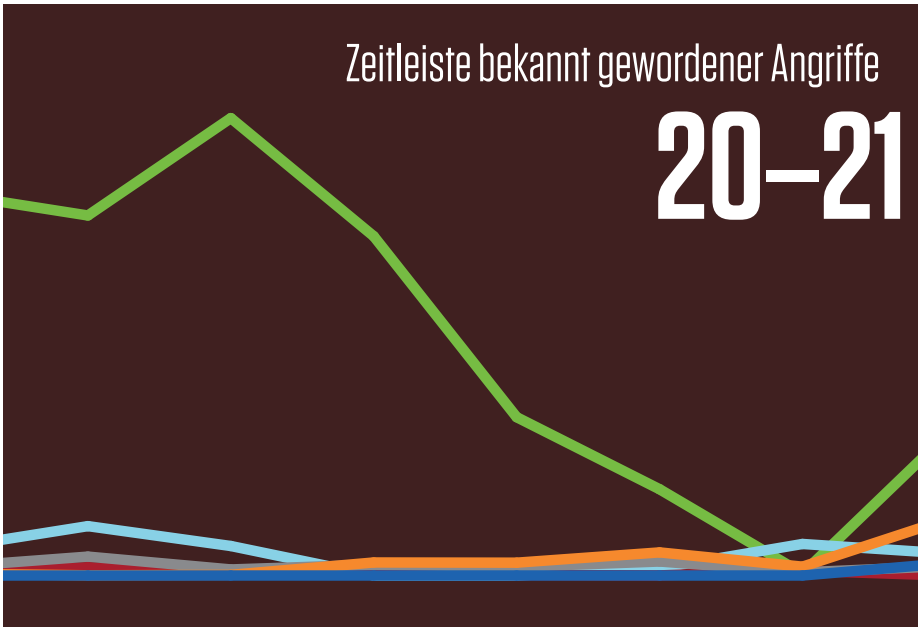
EINFÜHRUNG

Für viele Menschen begann das Jahr 2021 mit einem Hoffnungsschimmer, als COVID-19-Impfstoffe großflächig verfügbar wurden. Und obwohl ein großer Teil dieses Jahres durch kleine Schritte auf dem Weg in die Normalität geprägt war, sah es in der Welt der Cyberkriminellen ganz anders aus.

In Bezug auf die Cybersicherheit war 2021 das Wendejahr, als finanziell motivierte Cyberkriminalität zu einem landesweiten Sicherheitsproblem wurde. Gleichzeitig war dieses Jahr geprägt von der hartnäckigen Kreativität und Raffinesse von Bedrohungsakteuren, die neue Wege zum Unterlaufen digitaler Schutzmaßnahmen suchten und die vielen Gelegenheiten ergriffen, die ihnen diese Zeit der Unsicherheit bot.

Dieser Bericht zeigt auf, wie Ransomware die Treibstoffversorgung an der US-amerikanischen Ostküste lahmlegte, warum eine Justin Bieber-Konzerttournee zu einem Telefongespräch mit einem Malware-Verbreiter führen konnte und was zunehmendes SMS-Phishing für die Sicherheit von Mobilgeräten bedeutet. Wir beleuchten auch die immer engeren Verflechtungen zwischen Malware-Verbreitern und einer der erfolgreichsten Ransomware-Gruppen der Welt und decken auf, wie legale Cloud-Dienste mittlerweile die Infrastruktur für eine Vielzahl böswilliger Aktivitäten bereitstellen.

Nach einem Jahr, das die Welt veränderte, zeigt sich, dass manche Dinge gleich bleiben: Angreifer sind weiterhin skrupellos wie eh und je, sodass der Schutz von Menschen vor Cyberbedrohungen weiterhin eine – häufig faszinierende – Herausforderung darstellt.



Inhaltsverzeichnis

INFORMATIONEN ZU DIESEM BERICHT

Seit 2014 beleuchtet der Bericht „Der Faktor Mensch“ das einfache Prinzip, dass Menschen – und nicht Technologien – die kritischste Variable bei aktuellen Cyberbedrohungen sind.

Seit damals ist der scheinbare Widerspruch zu einem weithin anerkannten Fakt geworden. Cyberangreifer nehmen gezielt Menschen ins Visier und nutzen deren Schwächen aus. Letztlich sind Menschen einfach menschlich.

Um aktuelle Bedrohungen und Compliance-Risiken effektiv zu verhindern, zu erkennen und darauf zu reagieren, müssen IT-Sicherheitsexperten die personenbezogenen Dimensionen der Anwenderrisiken kennen: Schwachstellen, Angriffe und Berechtigungen. Praktisch betrachtet werden Antworten auf diese Fragen benötigt:

- Wo liegen die größten Schwachstellen der Anwender?
- Wie nutzen Angreifer das aus?
- Wie groß ist die potenzielle Gefahr für Daten, wenn privilegierter Zugriff auf Daten, Systeme und andere Ressourcen kompromittiert wird?

Der richtige Umgang mit diesen Fragen, die die menschlichen Faktoren der Cybersicherheit beschreiben, steht im Mittelpunkt einer modernen Verteidigung.

JEDEN TAG ANALYSIEREN WIR BILLIONEN DATENPUNKTE AUF ALLEN WICHTIGEN DIGITALEN KANÄLEN.

2,6 Mrd.
E-Mail-Nachrichten

49 Mrd.
URLs

1,9 Mrd.
Anhänge

28,2 Mio.
Cloud-Konten

1,7 Mrd.
verdächtige Mobilgerätenachrichten

Inhalt dieses Berichts

Dieser Bericht stellt die drei Facetten von Anwenderrisiken im Detail vor. Er beleuchtet die wichtigsten Entwicklungen in der Bedrohungslandschaft und untersucht die immer engeren Verflechtungen zwischen Cybercrime-Gruppen sowie die Folgen für Anwender sowie Unternehmen auf der ganzen Welt. Außerdem erfahren Sie, wie personenzentrierter Schutz die Anwender widerstandsfähiger macht, Angriffe abwehrt und Berechtigungen verwaltet.

Dieser Bericht stellt die Bedrohungen vor, die im Jahr 2021 bei Proofpoint-Bereitstellungen entdeckt, abgewehrt und behoben wurden. Damit basiert er auf einem der größten und vielfältigsten Datensätze in der Cybersicherheitsbranche.

Wir konzentrierten uns in erster Linie auf Bedrohungen, die zu einer umfassenderen Angriffskampagne und somit zu einer Serie von Aktionen gehören, die von einem Angreifer zum Erreichen eines Ziels durchgeführt werden. Manchmal können wir diese Kampagnen einem bestimmten Bedrohungsakteur zuordnen. Dieser Prozess wird als Attribution bezeichnet.

Umfang

Die Daten in diesem Bericht stammen aus dem Proofpoint Nexus Threat Graph und wurden aus Proofpoint-Bereitstellungen auf der ganzen Welt erhoben. Jeden Tag analysieren wir mehr als 2,6 Milliarden E-Mails, 49 Milliarden URLs, 1,9 Milliarden Anhänge, 28,2 Millionen Cloud-Konten, 1,7 Milliarden verdächtige Mobilgerätenachrichten und vieles mehr. Insgesamt erheben wir dabei Billionen Datenpunkte auf allen wichtigen digitalen Kanälen.

Dieser Bericht erfasst den Zeitraum vom 1. Januar bis zum 31. Dezember 2021. Die genannten konkreten Kampagnen wurden von unserem weltweiten Bedrohungsforscher-Netzwerk unmittelbar beobachtet. Kampagnen werden definiert als eine Reihe zusammenhängender Aktivitäten, die von einem einzigen Angreifer durchgeführt werden, um ein bestimmtes Ziel zu erreichen.

In einigen wenigen Fällen waren die Daten für das ganze Jahr entweder nicht verfügbar oder verfälschten unsere Aussage. Daher weisen wir gesondert darauf hin, wenn wir einen kürzeren Zeitrahmen oder eine andere Datenquelle gewählt haben.

DIE WICHTIGSTEN ERKENNTNISSE

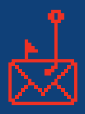
50 %

Manager und Führungskräfte machen nur 10 % der Anwender aus, stellen aber gleichzeitig fast 50 % der schwerwiegendsten Angriffsrisiken dar.

Schädliche URLs sind drei- bis viermal so häufig wie schädliche Anhänge.

100.000

Angreifer versuchen täglich, mehr als 100.000 Telefonangriffe durchzuführen.



Smishing-Versuche haben sich in den USA im Vergleich zum Vorjahr mehr als verdoppelt. In Großbritannien drehen sich über 50 % der Köder um Versand-benachrichtigungen.

Mit mehr als 20 Millionen Nachrichten wurde versucht, Malware zu übermitteln, die zu Ransomware-Angriffen führte.

>80 %

Mehr als 80 % aller Unternehmen werden pro Monat mithilfe eines kompromittierten Lieferantenkontos angegriffen.

Die Zahl der Warnungen zu Datenverlustprävention hat sich stabilisiert, da die Unternehmen dauerhafte Hybrid-Arbeitsmodelle implementieren.

35 %

35 % der Cloud-Mandanten, die eine verdächtige Anmeldung feststellten, verzeichneten auch verdächtige Aktivitäten nach dem Zugriff.

DEFINITION VON CYBERSICHERHEITSRISIKEN

In der Cybersicherheit werden Risiken wie folgt definiert:

Ein personenzentriertes Modell berücksichtigt also folgende Aspekte:

- Die Wahrscheinlichkeit, dass jemand angegriffen wird (Angriffe)
- Die Wahrscheinlichkeit, dass Personen mit einem schädlichen Inhalt interagieren, der ihnen zugesendet wurde (Anfälligkeit)
- Die Folgen einer Kompromittierung ihrer Anmeldedaten (Berechtigung)

Dieser Bericht beleuchtet jeden dieser Aspekte im Hinblick auf unser personenzentriertes Anwenderrisiko-Modell – Schwachstellen, Angriffe und Berechtigungen – und gibt Empfehlungen dazu, wie die jeweiligen Probleme behoben werden können.

Ein genauer Blick auf Anwenderrisiken

Ebenso wie jeder Mensch einzigartig ist, sind auch sein Wert für die Cyberangreifer und das Risiko für den Arbeitgeber individuell. Menschen haben individuelle digitale Gewohnheiten und Schwachstellen. Sie werden mit unterschiedlichen Mitteln und wechselnder Intensität angegriffen und verfügen jeweils über ganz eigene Zugriffsberechtigungen für Daten, Systeme und Ressourcen. Diese miteinander verknüpften Faktoren bestimmen das individuelle Gesamtrisiko eines Anwenders.

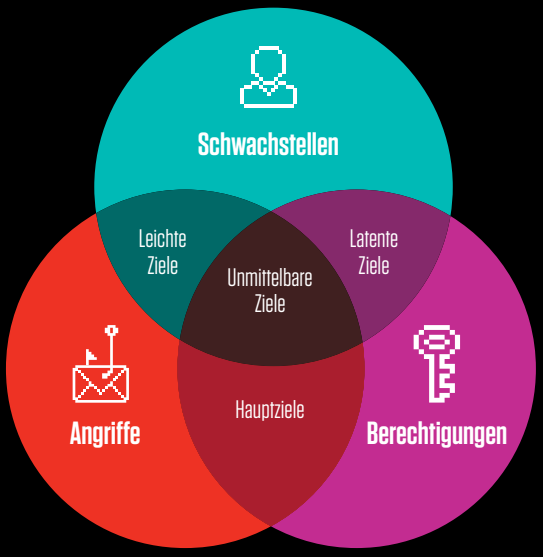


Abb. 1: Zusammenspiel der drei Risikotypen.

Schwachstellen

Die erste Schwachstelle der Anwender ist ihr digitales Verhalten – wie sie arbeiten und worauf sie klicken. Viele Mitarbeiter arbeiten vielleicht im Homeoffice oder haben über ihre privaten Geräte Zugriff auf geschäftliche E-Mails. Oder sie nutzen Cloud-basierte Dateispeicher und installieren Drittanbieter-Add-ons für ihre Cloud-Anwendungen. Manche Mitarbeiter gehen auf riskantere Weise mit Daten um als ihre Kollegen. Und einige von ihnen sind besonders empfänglich für die E-Mail-Phishing-Taktiken der Angreifer.

Angriffe

Nicht alle Cyberangriffe sind gleich. Auch wenn jeder einzelne Angriff gefährlich sein kann, sind einige schädlicher, gezielter oder raffinierter als andere. Einige Malware-Familien sind relativ eng mit Ransomware-Betreibern verbunden, während eine Nachricht von einem kompromittierten Lieferanten ein höheres Schadenspotenzial hat als Betrug mit Gutscheinkarten. „Standard"-Bedrohungen, die in großer Masse versendet werden, mögen häufiger sein als raffiniertere Bedrohungstypen, sie sind jedoch bekannt und können leichter blockiert werden. (Das sollte jedoch kein Grund sein, sie zu unterschätzen, da sie ebenso großen Schaden anrichten können.) Andere Bedrohungen kommen vielleicht nur bei einigen wenigen Angriffen zum Einsatz, können jedoch eine größere Gefahr darstellen, da sie raffinierter oder hinsichtlich der angesprochenen Personen extrem zielgerichtet sind.

Berechtigungen

Bei den Berechtigungen werden alle potenziell hochwertigen Assets erfasst, auf die Menschen Zugriff haben (z. B. Daten, finanzielle Befugnisse, wichtige Kontakte). Die Ermittlung dieses Risikoaspekts ist unverzichtbar, da er den potenziellen Gewinn für Angreifer repräsentiert – und das Unternehmen bei einer Kompromittierung schädigt. Die Position des Anwenders im Organigramm ist natürlich ein wichtiger Faktor bei der Bewertung der Berechtigungen. Sie ist jedoch nicht der einzige Faktor – und häufig noch nicht einmal der wichtigste. Für die Angreifer kann jeder Mitarbeiter ein lohnenswertes und nützliches Ziel darstellen.

Abschnitt 1

Schwachstellen

Die Bewertung der Anfälligkeit von Anwendern ist eine wichtige Komponente jeder guten Cyberabwehr. Um diesen Aspekt unseres Risikomodells im Griff zu behalten, müssen Sie wissen, wer in Ihrem Unternehmen am ehesten auf clever gemachtes Social Engineering hereinfällt.

Social Engineering ist erfolgreich, weil es die menschliche Natur ausnutzt. Die meisten Menschen treffen ihre unzähligen alltäglichen Entscheidungen basierend auf Heuristik und kognitiven Verzerrungen – also Vorurteilen. Und da die Anforderungen an unsere Zeit und Aufmerksamkeit steigen, setzen wir immer häufiger auf diese Annahmen und Faustregeln. Cyberangreifer wissen das und suchen ihre potenziellen Opfer daher bevorzugt in anspruchsvollen Berufen oder stressigen Abteilungen. Sie wissen, dass diese Personen nicht die Zeit haben, um eine Nachricht gründlich zu überprüfen, bevor sie auf einen Link klicken oder einen Anhang herunterladen.

Quantifizierung der Anfälligkeit

Die einfachste Möglichkeit zum Quantifizieren der Anfälligkeit, ohne dabei das Unternehmen zu gefährden, sind Tests der Mitarbeiterreaktionen auf simulierte Bedrohungen. Die von unserem Tool für Phishing-Simulationen erfassten Daten aus dem letzten Jahr zeigen – abhängig vom getesteten Angriff – eine Fehlerquote von 4 % bis 20 %.

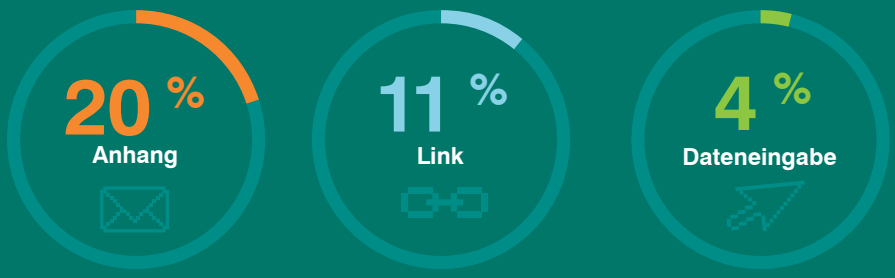


Abb. 2: Fehlerquoten für simulierte Phishing-Angriffe, 2021.

Aufgeschlüsselt nach Abteilung schwanken die Fehlerquoten zwischen 6 % und 12 %, wobei der Durchschnitt bei 11 % liegt. Mehrere wichtige (und häufig angegriffene) Abteilungen besetzen den unteren Bereich der Tabelle, beispielsweise die IT-, Rechts- und Finanzabteilung. Es gibt jedoch auch mehrere potenziell lukrative Ziele, die im Durchschnitt oder darüber liegen, darunter die Abteilungen für betriebliche Abläufe und den Einkauf.

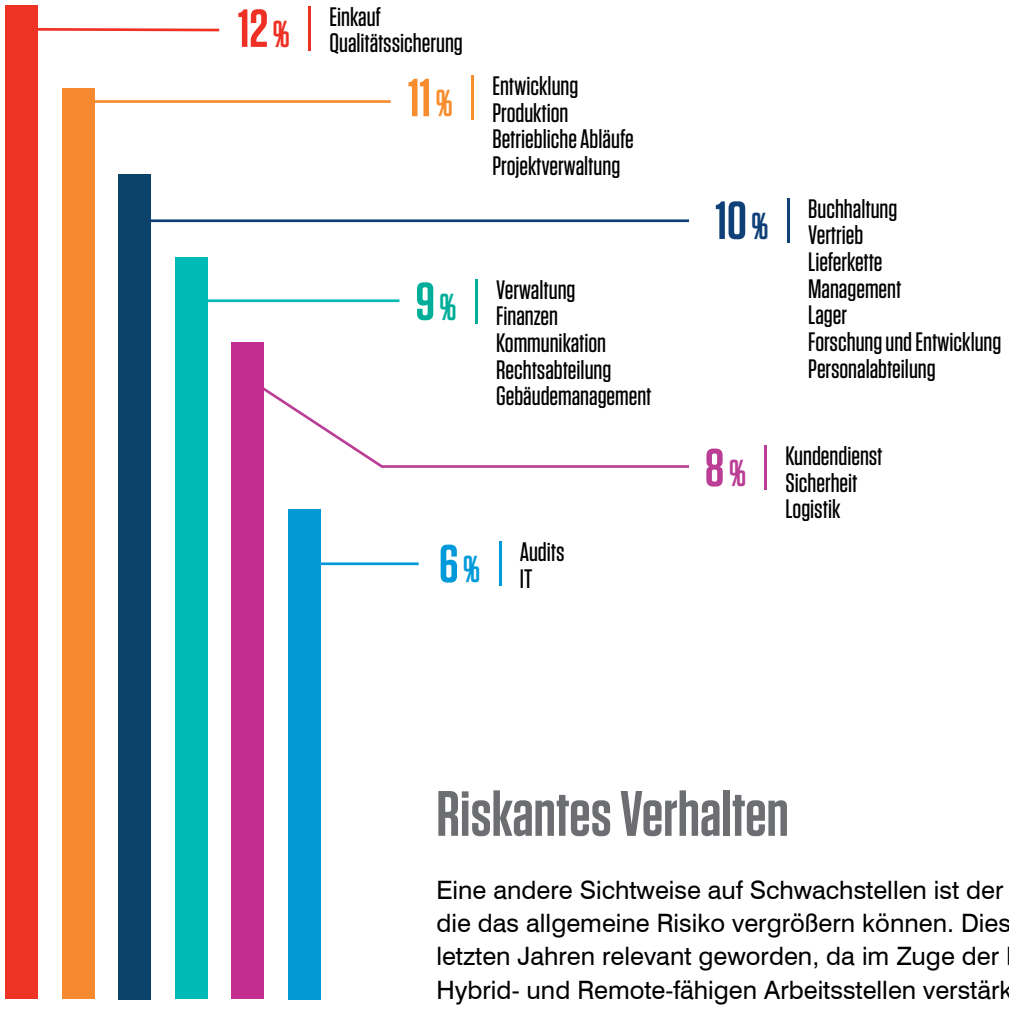


Abb. 3: Durchschnittliche Fehlerquoten bei Phishing-Simulationen nach Abteilung, 2021.

Riskantes Verhalten

Eine andere Sichtweise auf Schwachstellen ist der Blick auf Verhaltensweisen, die das allgemeine Risiko vergrößern können. Dies ist insbesondere in den letzten Jahren relevant geworden, da im Zuge der Pandemie bei verschiedenen Hybrid- und Remote-fähigen Arbeitsstellen verstärkt auf das Homeoffice gesetzt wird. Ein Bereich, in dem die Pandemie erhebliche Auswirkungen hatte, waren Bedrohungen durch Insider. Laut dem Bericht des Ponemon Institute für 2022 nahm die Zahl der Insider-Zwischenfälle seit dem Jahr 2020 um 44 % zu.

Laut unserem jährlichen „State of the Phish"-Bericht ist fast die Hälfte aller befragten berufstätigen Erwachsenen aufgrund von COVID-19 ins Homeoffice gewechselt. Dies hat jedoch dazu geführt, dass sich Berufliches und Privates vermischen, was sich besonders deutlich darin zeigt, wie diese Angestellten ihre privaten und unternehmenseigenen Geräte nutzen. Fast drei Viertel der Befragten nutzen ihre privaten Geräte für berufliche Zwecke, während 77 % mit unternehmenseigenen Geräten auf private Konten zugreifen. Am meisten besorgt uns jedoch, dass 55 % der Umfrageteilnehmer ihren Freunden und Familienmitgliedern gestatten, unternehmenseigene Computer und Smartphones zu nutzen.

Private Geräte verfügen oft nicht über den gleichen Schutz wie unternehmens-eigene Geräte, während Freunde und Familienmitglieder nicht immer über das gleiche Sicherheitsbewusstsein verfügen wie Angestellte. Die Frage, wie der Konflikt zwischen Benutzerfreundlichkeit und Sicherheit gelöst werden soll, wird lebhaft diskutiert. Fakt ist jedoch, dass Telearbeit drastisch die Umgebung verändert hat, in der sich die meiste Cyberkriminalität abspielt.

Abschnitt 2

Angriffe

In diesem Abschnitt stellen wir die konkreten Strategien, Techniken und Tools vor, die **BEDROHUNGSAKTEURE** im Jahr 2021 eingesetzt haben. Einige der hier genannten Kampagnen sind wegen ihres enormen Ausmaßes bemerkenswert, andere wegen ihrer Raffinesse. In fast allen Fällen mussten die Opfer mit erheblichen finanziellen Verlusten bzw. Rufschädigung rechnen.

In unserem Risikomodell legen **Angriffe** die **Schwachstellen** und **Berechtigungen** offen. Je heimlicher, raffinierter oder überzeugender ein Angriff vorgeht, desto größer ist die Wahrscheinlichkeit, dass selbst sicherheitsbewusste Opfer darauf hereinfallen. Angreifer suchen nach immer neuen Methoden, um Schutzlücken aufzuspüren. Es ist daher wichtig, dass automatisierte Sicherheitsmaßnahmen dynamisch genug sind, um auch bei neuen Bedrohungen anzuschlagen. Sicherheitsschulungen sollten regelmäßig mit Informationen aus den letzten Kampagnen aktualisiert werden.

Wir beleuchten einige Aspekte dieser Situation, bevor wir uns den Bedrohungen für E-Mails, Mobilgeräte und die Cloud widmen.

BEDROHUNGSAKTEUR:

Ein Branchenbegriff für Personen oder Gruppen, die Cyberangriffe durchführen. Zu Bedrohungsakteuren werden finanziell motivierte Cyberkriminelle, staatlich unterstützte APT-Gruppen (Advanced Persistent Threats), die Spionage und Sabotage betreiben, sowie „Hacktivisten“ gezählt, die politische oder soziale Ziele erreichen möchten. Manchmal verschwimmen diese Grenzen, da einige APT-Akteure bereits beim Diebstahl von Geld beobachtet wurden.

Russlands Cyberunterstützer

Während wir an diesem Bericht schrieben, begann die russische Invasion in der Ukraine. Obwohl sie nicht innerhalb des hier behandelten Zeitraums stattfand, sind die damit verbundenen Konsequenzen so fundamental, dass sie Erwähnung finden müssen.

Bereits vor Beginn der Invasion wurde zerstörerische Wiper-Malware gegen ukrainische Unternehmen und zentrale Kommunikationseinrichtungen eingesetzt. Als die Invasion begann, verzeichneten unsere Forscher erheblich verstärkte Aktivitäten bekannter APT-Akteure (Advanced Persistent Threat, hochentwickelte permanente Bedrohung) mit Russland-Bezug.

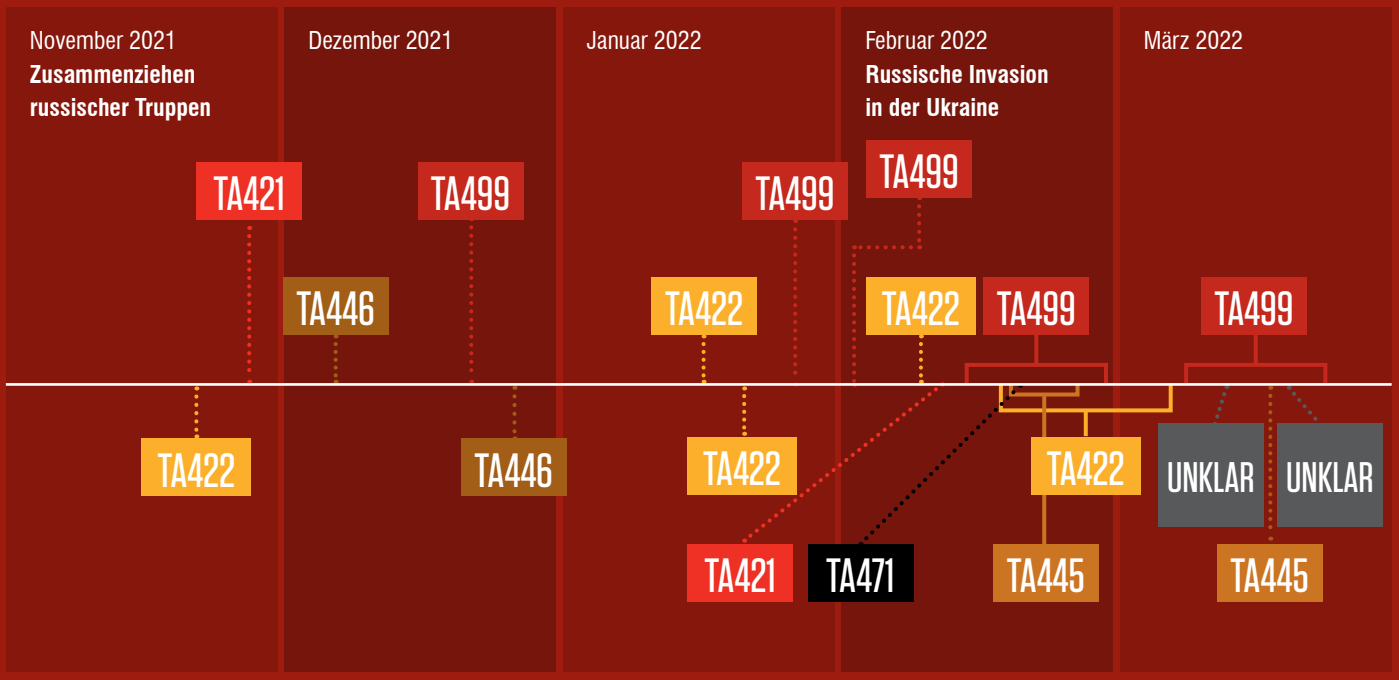


Abb. 4: Zeitleiste der mit Russland verbundenen APT-Aktivitäten, November 2021 bis März 2022.

Auch APT-Gruppen mit Verbindungen zu anderen Staaten reagierten auf die Situation. In den Wochen seit Beginn der Invasion verzeichneten wir Aktivitäten von Akteuren mit Bezug zu Weißrussland und China, die sich insbesondere gegen EU-staatliche Einrichtungen für Asyl- und Hilfsmaßnahmen richteten.

Wie wir weiter unten in diesem Bericht zeigen werden, lässt diese Invasion nicht nur die Grenze zwischen physischer und virtueller Kriegsführung verschwimmen. Da ein großer Teil der finanziell motivierten Cyberkriminalität von diesen beiden Ländern ausgeht, wurden viele der weltweit erfolgreichsten Cyberkriminellen gezwungen, sich für eine Seite zu entscheiden. Vor Beginn dieses Konflikts vermieden die meisten dieser Gruppen Angriffe auf Ziele in Russland, der Ukraine sowie den Nachbarländern – möglicherweise um von den Behörden in Ruhe gelassen zu werden. Doch seit Mitte Februar registrieren wir einen starken Anstieg bei Attacken auf Mitarbeiter internationaler Unternehmen in Russland und der Ukraine. Russische Angestellte werden inzwischen so häufig angegriffen wie Angestellte im Rest der Welt.

Verständlicherweise gelangen APT-Attacken häufig in die Schlagzeilen. Zu beachten ist dabei jedoch, dass nur ein äußerst geringer Anteil unserer Kunden jemals mit staatlich unterstützten Akteuren (ganz zu schweigen von den Akteuren einer Weltmacht) in Berührung kommt. Sollte es bei Ihnen zu einem Cyberzwischenfall kommen, wird das praktisch immer von gewöhnlichen Cyberkriminellen und nicht von einem feindlich gesonnenen Staat ausgehen.

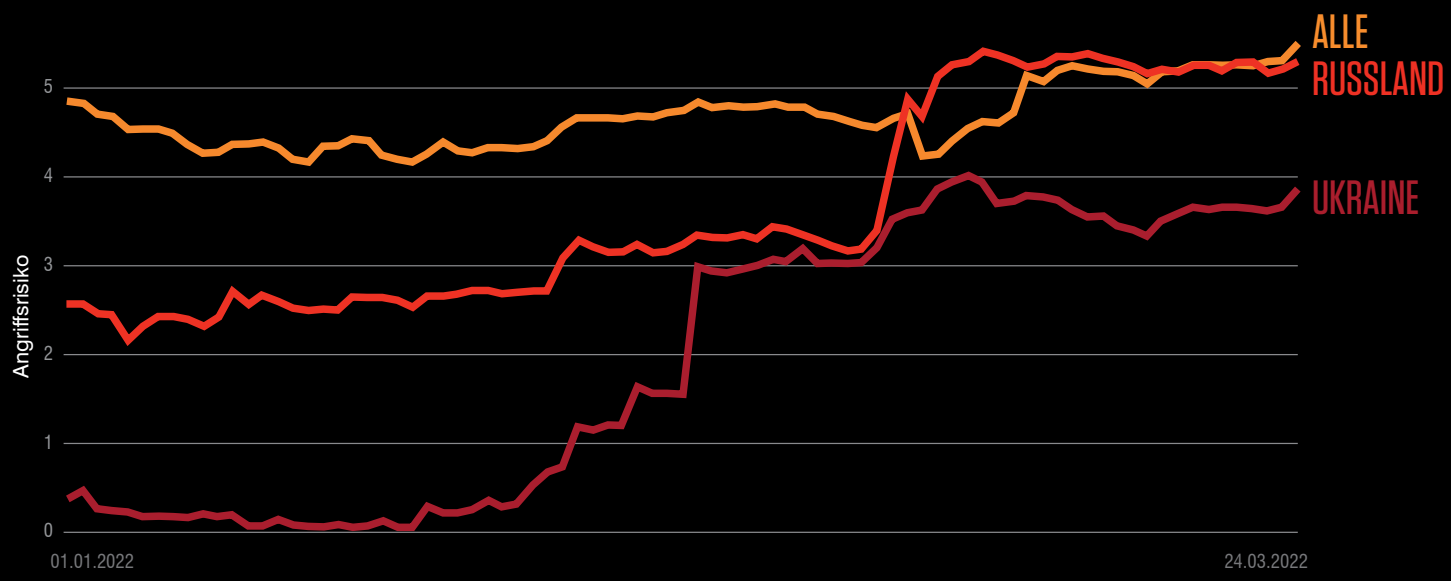


Abb. 5: Angriffsrisiko von Angestellten in Russland, der Ukraine und weltweit (basierend auf dem Proofpoint-Angriffsindex) für Angestellte eines großen multinationalen Unternehmens, Januar bis März 2022.

Emotet taucht wieder auf

Im Januar 2021 legte eine groß angelegte Aktion internationaler Strafverfolgungsbehörden das Botnet **EMOTET** lahm. Damit verschwand über Nacht eine Bedrohung, die für fast 10 % der schädlichen E-Mail-Aktivitäten im letzten Jahr verantwortlich war.

Doch da sich Cyberkriminelle in erster Linie durch ihren Opportunismus auszeichnen, waren andere Akteure nur zu gern bereit, diese Lücke zu schließen. Im Jahr 2021 tauchte eine Gruppe auf, die wir als **TA511** bezeichnen. Sie ist beim Volumen schädlicher E-Mails unangefochten in Führung und versendet dreimal mehr Nachrichten als der Zweitplatzierte der aktivsten Angreifer.

EMOTET:

Vor der Abschaltung der Infrastruktur im Jahr 2021 war Emotet die weltweit am häufigsten verteilte Malware. Nach ihrer Rückkehr Ende des letzten Jahres wurden die Entwickler von Emotet mit den Gruppen TrickBot und Conti in Verbindung gebracht.

TA511:

Eine finanziell motivierte Cybercrime-Gruppe, die für umfangreiche Kampagnen gegen verschiedenste Branchen bekannt ist. Im Laufe der Zeit wurde TA511 bei der Nutzung unterschiedlicher Malware-Typen beobachtet.

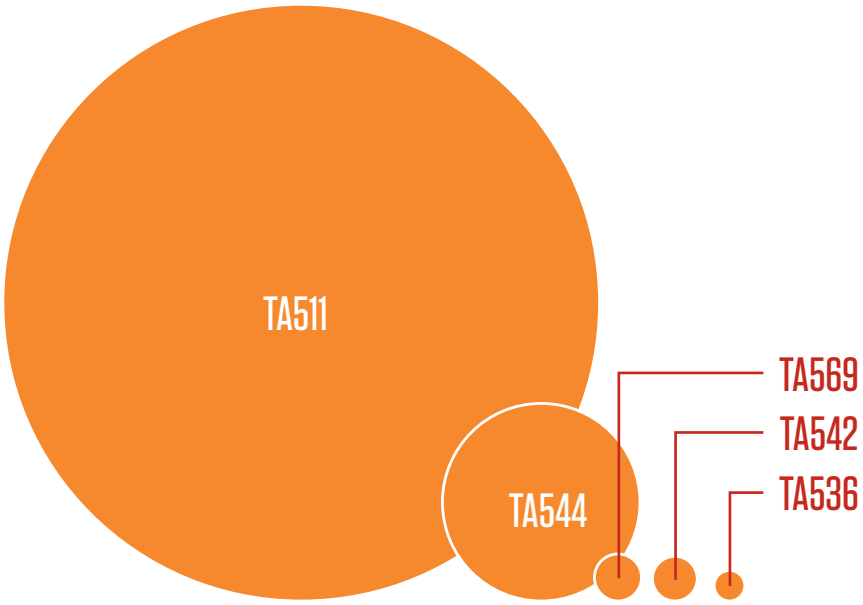


Abb. 6: Die aktivsten Bedrohungsakteure nach Nachrichtenvolumen, 2021.
(Größe der Kreise repräsentiert das relative Nachrichtenvolumen.)

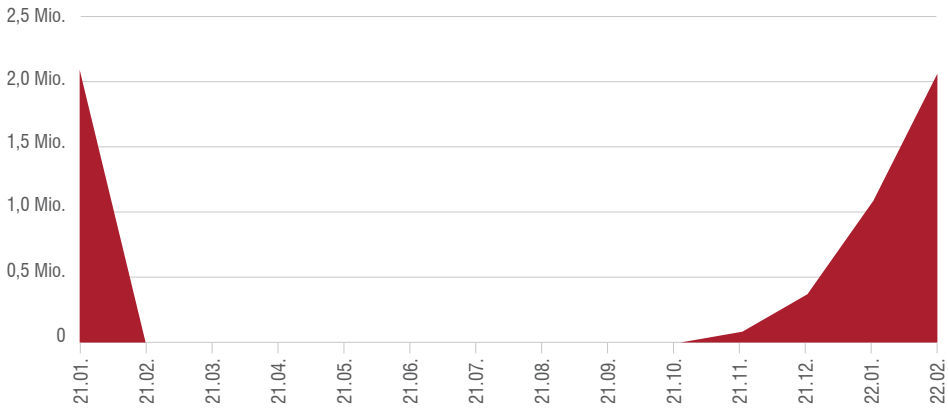


Abb. 7: Nachrichtenvolumen von Emotet, Januar 2021 bis Februar 2022.

Im November 2021 nahm Emotet seine Aktivitäten wieder auf, doch die Malware erreichte ihr Niveau aus dem Jahr 2020 nicht sofort. In den ersten Monaten nach der Rückkehr der Gruppe TA542 (der Bedrohungsakteur hinter Emotet) lag das Nachrichtenvolumen bei lediglich einigen zehntausend E-Mails. Doch seit März dieses Jahres scheint Emotet wieder zu seiner bisherigen Stärke zurückgefunden zu haben: Einige Kampagnen verteilen jeweils mehrere Millionen Nachrichten. Weiter unten in diesem Bericht gehen wir detailliert darauf ein, da aktuelle Untersuchungen starke Indizien für Verbindungen zwischen Emotet und der Ransomware-Gruppe Conti offengelegt haben.

Das Who is Who bei Malware

Da das Tool **TORDAL** von TA511 eingesetzt wird, nahm es wenig überraschend den Spitzenplatz in unserer Liste der häufigsten Malware ein. Auch wenn Tordal exklusiv von TA511 genutzt wird, gibt es für die übrige Malware aus den Top 5 mehrere Verbreiter (Ficker Stealer wird meist als sekundäre Payload von Tordal heruntergeladen). Daher können diese Malware-Familien in sehr unterschiedlichen Kontexten eingesetzt werden – je nachdem, welche Social-Engineering-Taktiken die Angreifer einsetzen. Beispielsweise wurde **FORMBOOK** mithilfe von COVID-19-Ködern, generischen geschäftlichen E-Mails zur Informationsanfrage und sogar in einer Kampagne verteilt, in der sich der Angreifer als Fußballagent ausgab, der junge Spieler aus Afrika und Südamerika vertritt.

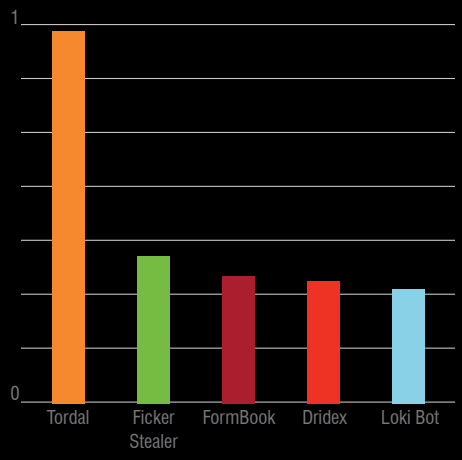


Abb. 8: Die größten Malware-Familien nach Nachrichtenaufkommen, 2021.
(Hinweis: Skala ist normalisiert, um vertrauliche Proofpoint-Daten zu schützen)

TORDAL:

Tordal ist auch als Hancitor bekannt und dient als Downloader für sekundäre Malware wie – in mindestens einem Fall – für Cobalt Strike. Die Ursprungsversion von Tordal nutzte noch das anonyme Tor-Netzwerk zur Kommunikation, während spätere Versionen auf gewöhnliches HTTP setzten.

FORMBOOK:

Diese Malware-as-a-Service wird seit 2016 in Foren verkauft. Die Preise sind vergleichsweise günstig, daher ist FormBook bei Angreifern sehr beliebt und wird für verschiedenste Angriffe mit ganz unterschiedlichen Social-Engineering-Taktiken und Übertragungsmethoden verwendet.

Social-Engineering-Strategien

Da die Pandemie im Laufe des Jahres weiterhin Anstiege und Rückgänge zeigt, bleiben COVID-19-Köder bei den Cyberkriminellen sehr beliebt. Der erste Anstieg fiel mit der größer werdenden Verfügbarkeit von Impfstoffen Anfang 2021 zusammen, was letztendlich zu einem Rückgang des Kampagnenvolumens führte, da immer größere Teile der Bevölkerung geimpft wurden. Das Sommerhoch durch die Delta-Variante des Virus führte jedoch zu einem erneuten Aktivitätsschub.

Abb. 9: Aufkommen von Nachrichten mit Pandemiebezug, 2021.

TA451:

Ein Akteur mit Iran-Bezug, der mindestens seit 2017 aktiv ist. Diese Gruppe erlangt mithilfe von Phishing den Erstzugriff und greift häufig Rüstungshersteller mit Jobangeboten an. Im Laufe der Jahre verteilte die Gruppe verschiedenste proprietäre und Standard-Malware.

TA425:

Dieser Akteur, der möglicherweise staatlich unterstützt wird, sitzt in Indien. Meist greift TA425 Universitäten, Think Tanks, Tech-Unternehmen und Behörden in verschiedenen Ländern an.

TA421:

Ein staatlich unterstützter Akteur, der in Russland sitzt. Laut FBI, CISA und NSA soll die Gruppe mit dem russischen Auslandsgeheimdienst (SWR) in Verbindung stehen. Daher geht sie entsprechend raffiniert vor und nutzt proprietäre Malware.

COBALT STRIKE:

Dieses legitime „Red Team"-Tool wird von Sicherheitsteams zum Testen der Netzwerksicherheit eingesetzt. Es ist aber auch bei Bedrohungsakteuren beliebt, die gecrackte oder illegal erworbene Versionen dieser Software für ihre Angriffsketten nutzen.

Abb. 10: Von TA425 genutzte Landing Page zum Fälschen des pakistanischen nationalen Immunisierungssystems (NIMS).

Obwohl die Mehrheit der pandemiebezogenen böswilligen Aktivitäten von finanziell motivierten Kriminellen durchgeführt wurde, nutzten auch einige staatlich unterstützte Angreifer COVID-19-Köder. Anfang 2021 führte der mit dem Iran verbundene Akteur **TA451** eine Phishing-Kampagne gegen ein US-amerikanisches Rüstungsunternehmen durch. Später in dem Jahr griff der mit Indien verbundene Akteur **TA425** Anwender in Pakistan mit Ködern zu Booster-Impfungen an. Der russische staatlich unterstützte Angreifer **TA421** sprang ebenfalls auf diesen Zug auf und griff Unternehmen auf der ganzen Welt mit COVID-19-Ködern an, die **COBALT STRIKE** verteilen sollten.

Squid Game-Betrüger: So nutzen Angreifer die Popkultur aus

Abgesehen von COVID-19 gab es im Jahr 2021 auch die üblichen Dauerbrenner wie Steuerbescheide, Jobangebote und Schnäppchenpreise zur Weihnachtzeit. Anstatt uns jedoch auf Altbekanntes zu konzentrieren, werfen wir einen Blick auf ein Beispiel dafür, wie schnell Angreifer auf aktuelle soziale und kulturelle Ereignisse reagieren können.

Die Fernsehserie „Squid Game“ startete im September des vergangenen Jahres und erwies sich als Riesenhit für Netflix. In weniger als einem Monat kamen die Zuschauer auf insgesamt 1,65 Milliarden Stunden mit dieser Serie, was diese damit zum beliebtesten jemals ausgestrahlten Netflix-Inhalt machte. Im Oktober ergriffen Cyberkriminelle ihre Chance: Der für großvolumige Kampagnen bekannte Akteur TA575 verschicke E-Mails mit Squid Game-Bezug an Opfer in den USA, in denen frühzeitiger Zugang zur nächsten Staffel oder sogar die Möglichkeit versprochen wurde, beim Dreh zukünftiger Folgen mitmachen zu können.

Wenn die Opfer sich davon überzeugen ließen, die angehängte Microsoft Excel-Datei herunterzuladen und Makros zu aktivieren, wurde der Bank-Trojaner Dridex auf ihrem System installiert.

Solche Kampagnen können ebenso schnell wie die kulturellen Ereignisse, auf die sie sich beziehen, auftauchen und wieder verschwinden. Selbst gut ausgestatteten Bedrohungsforscher-Gruppen fällt es schwer, hier den Überblick zu behalten. Daher benötigen Unternehmen automatisierte E-Mail-Schutzmaßnahmen, die dynamische Bedrohungen sofort erkennen können.

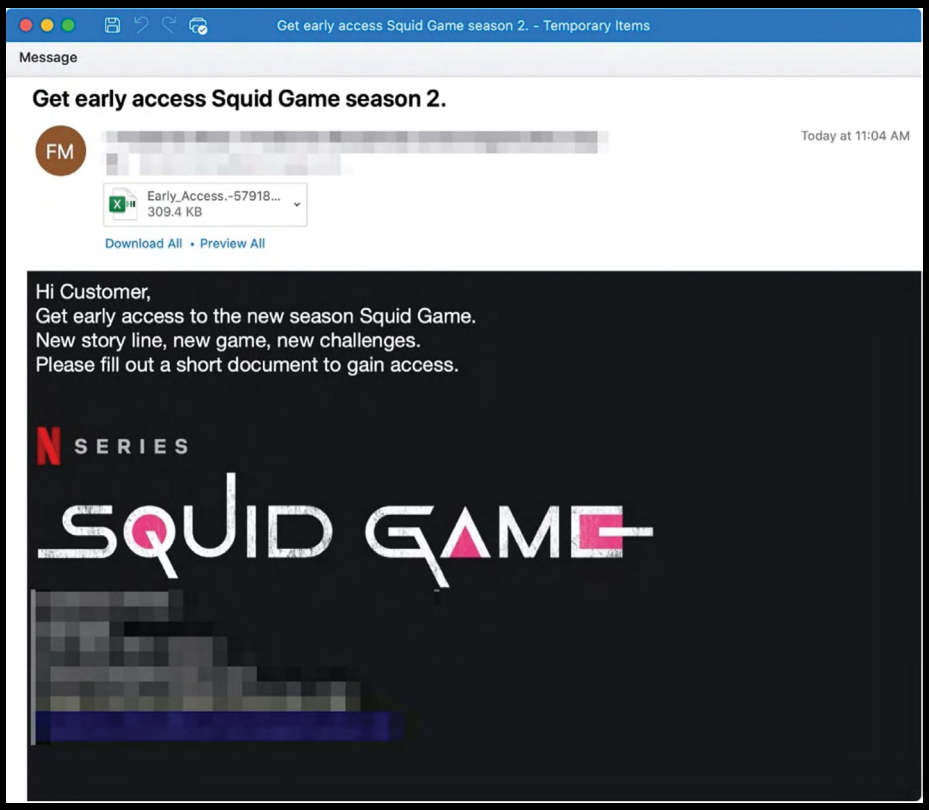


Abb. 11: Beispiel für einen E-Mail-Köder mit Squid Game-Bezug.

Ransomware: ein Jahr im Rückblick

Im Jahr 2021 machte Ransomware so viele Schlagzeilen wie nie zuvor, als eine Reihe medienwirksamer Angriffe zeigte, dass diese Cyberbedrohung die Treibstoffversorgung, Lebensmittelsicherheit sowie medizinische Behandlung der Bevölkerung gefährden konnte. Ein aktueller Bericht des FBI über das letzte Jahr kommt auf mindestens 649 Ransomware-Angriffe auf Anbieter kritischer Infrastrukturen.[1]

Im vergangenen Jahr konnten mehrere Erfolge im Kampf gegen Ransomware verbucht werden. Strafverfolgungsbehörden konnten etwa die Hälfte des Lösegeldes zurückerlangen, das Colonial Pipeline gezahlt hatte, während die Folgen des Kaseya-Ransomware-Lieferkettenangriffs dank eines veröffentlichten Entschlüsselungsschlüssels schnell beseitigt werden konnten. Doch trotz dieser kleinen Siege verfestigt sich der Eindruck, dass eine schattenhafte Cybercrime-Elite jederzeit die größten und wichtigsten Unternehmen der Welt angreifen kann.

Ende Februar 2022 fand sich die Ransomware-Unterwelt jedoch plötzlich unerwartet im Rampenlicht wieder. Der unbekannte Twitter-Nutzer @ContiLeaks veröffentlichte Chat-Protokolle und weitere Daten der **CONTI**-Gruppe. Forscher stürzten sich auf diese Informationen und erkannten schnell, dass diese Leaks einen einzigartigen Blick auf das Innenleben eines der erfolgreichsten – und geheimnisvollsten – Ransomware-Betreibers erlaubten.

Eine der interessantesten Erkenntnisse aus den geleakten Chats ist die Organisationsstruktur von Conti: Die Gruppe agiert wie ein ganz normales Unternehmen mit angestellten Mitarbeitern, Urlaubsgeld und einer Personalabteilung. Sie scheint auch streng hierarchisch organisiert zu sein und über mehrere Führungsebenen zu verfügen. Die Leaks enthalten unzählige Nachrichten über Arbeitsbedingungen, die Bezahlung und andere alltägliche Beschwerden.

Besonders ins Auge fällt, dass die Führung der Gruppe die Abteilungen gezielt isoliert, sodass die rechte Hand nicht immer weiß, was die linke tut. Dies wird durch ein Gespräch zwischen zwei Conti-Mitarbeitern von Oktober 2020 deutlich, die sich überrascht über die Ähnlichkeit ihrer Kampagnen und denen von **RYUK** austauschen – einer Ransomware-Gruppe, die nach ihrer Überzeugung in keinem Zusammenhang mit Conti steht. Das deutet darauf hin, dass die unteren Organisationsebenen nicht über die zahlreichen Schnittpunkte zwischen Conti, Ryuk und den verschiedenen Malware-Anbietern für den Erstzugriff informiert sind.

Anbieter für den Erstzugriff sind mittlerweile ein fester Bestandteil des Ransomware-Ökosystems. Anstatt die Ransomware direkt per E-Mail zu verteilen, nutzen die Betreiber von Conti, REvil und anderen bereits vorhandene Malware-Kompromittierungen aus, um Geräte und Systeme zu infizieren. Im letztjährigen Bericht beleuchteten wir die Beziehung zwischen verschiedenen Malware-Gruppen und Ransomware-Betreibern, doch die Conti-Leaks bieten den besten Beweis für die enge Zusammenarbeit zwischen Malware-Botnets und Ransomware.

CONTI:

Einer der erfolgreichsten und einigen Berichten zufolge auch skrupellosesten Ransomware-Betreiber. Bekannt wurde Conti Anfang 2021 durch Angriffe auf das Gesundheitswesen in den USA und Irland, obwohl dieser Sektor üblicherweise tabu ist.

RYUK:

Eine Ransomware-Familie, die eng mit den Bank-Trojaner TrickBot in Verbindung steht. Aktuelle Leaks legen nahe, dass die Entwickler von Ryuk auch hinter der Ransomware Conti stehen.

REvil:

Diese Ransomware-Gruppe wurde der breiten Öffentlichkeit zum ersten Mal durch Angriffe auf 22 Gemeinden in Texas bekannt. Im Januar 2022 führten russische Behörden mehrere Verhaftungen durch und gaben bekannt, die Infrastruktur von REvil stillgelegt zu haben. Im April 2022, während der russischen Invasion in der Ukraine, tauchte die Gruppe jedoch wieder auf.

DARKSIDE:

DarkSide erlangte durch den Angriff auf Colonial Pipeline plötzlich weltweite Bekanntheit. Im Juni 2021 gab die Gruppe ihre Auflösung bekannt, da der Druck angeblich zu groß wäre. Möglicherweise hat sie sich jedoch einfach in BlackMatter umbenannt. Das FBI hat die Gruppe auch mit Alphv und BlackCat in Verbindung gebracht.

1 FBI: „2021 Internet Crime Report“ (Bericht zu Internetkriminalität 2021), April 2022.

Malware für Erstzugriff-Vermittlung + Bekannt gewordene Ransomware-Angriffe

Nachrichtenaufkommen der Malware, die von Conti für den Erstzugriff genutzt wird, sowie größere Conti-Attacken, Januar 2021 bis Februar 2022.

Januar 2021

Der polnische Entwickler hinter einer der weltweit beliebtesten Computer-Rollenspielreihe wurde erfolgreich mit der HelloKitty-Ransomware angegriffen. Dabei wurden die Server verschlüsselt und der Quellcode gestohlen sowie zum Verkauf gestellt.

Februar 2021

Eines der größten Versicherungs-unternehmen der USA soll Berichten zufolge ein Lösegeld von 40 Millionen US-Dollar gezahlt haben, nachdem Ransomware-Angreifer mithilfe eines gefälschten Browser-Updates in das Netzwerk gelangen konnten.

März 2021

Ein Schulbezirk in Florida wurde von der Conti-Gruppe angegriffen, die ursprünglich 40 Millionen US-Dollar für die Entsperrung der IT-Systeme verlangte. Normalerweise haben Angreifer einen relativ genauen Überblick über die finanziellen Möglichkeiten ihrer Opfer, doch diese Lösegeldsumme konnte der Schulbezirk unmöglich zahlen.

April 2021

In einem der bekanntesten Angriffe des Jahres zwang die Ransomware DarkSide die zeitweise Abschaltung einer Pipeline, mit der die US-amerikanische Ostküste mit Treibstoff versorgt wird. Das Unternehmen zahlte ein Lösegeld in Höhe von 4,4 Millionen US-Dollar, wovon die Hälfte wieder zurückerlangt werden konnte.

Mai 2021

Der Angriff von REvil auf einen großen Fleischverarbeiter weckte Sorgen vor Lebensmittelknappheit und zwang das Unternehmen, ein Lösegeld von 11 Millionen US-Dollar zu zahlen.

Ein europäischer nationaler Gesundheitsdienstleister wurde von der Conti-Gruppe angegriffen. Dabei konnten die Cyberkriminellen etwa 80 % der IT-Systeme verschlüsseln, was die Behandlung vieler Patienten verzögerte.

Juni 2021

Durch einen Angriff von REvil auf einen Managed Software Provider wurden plötzlich tausende nachgelagerte Kunden verwundbar. Schnelle Aktionen von Strafverfolgungs-behörden ermöglichten jedoch die Stilllegung der REvil-Infrastruktur sowie die Bereitstellung eines Schlüssels für die Entschlüsselung bei den Opfern.

August 2021

Der LockBit-Gruppe gelang es, die Systeme eines weltweiten IT- und Management-Beratungsunternehmens zu verschlüsseln und die Daten zu stehlen. Das Unternehmen konnte seine Systeme aus Backups wiederherstellen, ohne das Lösegeld von 50 Millionen US-Dollar zahlen zu müssen. Als Reaktion darauf veröffentlichten die Gruppe jedoch die Daten.

September 2021

Zwei große Anbieter audiovisueller Elektronik wurden von den Ransomware-Gruppen Conti und BlackMatter angegriffen.

Oktober 2021

Eines der größten Netzwerke lokaler Fernsehstationen der USA wurde von einem Angriff getroffen, der die Sendung unterbrach. Die Angreifer konnten sich mithilfe von Active Directory zwischen den verschiedenen Kanälen des Netzwerks bewegen.

November 2021

Dezember 2021

Eine Online-Fotoplattform wurde von Conti getroffen. Dabei wurden Mitarbeiterdaten kompromittiert und einige Produktionsprozesse unterbrochen. Anschließend veröffentlichte die Gruppe die gestohlenen Daten.

Januar 2022

Februar 2022

Die Gruppe BlackCat griff erfolgreich einen weltweiten Flugdienstleister an und konnte den Flugbetrieb unterbrechen. Das Unternehmen verfügte jedoch über Notfallsysteme und konnte die Systeme ohne erhebliche Verzögerungen wiederherstellen.

Eine beliebte britische Snack-Marke wurde von Conti angegriffen, was zu Unterbrechungen bei der Bestellung und Auslieferung von Produkten an den Einzelhandel führte.

BLACKMATTER:

Dieser Ransomware-as-a-Service-Betreiber ist möglicherweise der neue Auftritt von DarkSide. Die Gruppe hat zumindest enge Verbindungen zum Angreifer von Colonial Pipeline, obwohl einige Mitglieder darauf beharren, lediglich Partner anderer Gruppen zu sein.

TRICKBOT:

Nachdem dieser Bank-Trojaner im Jahr 2016 auftauchte, erreichte er weithin Bekanntheit. Das könnte auch sein Ende besiegelt haben, da die Entwickler bekannt gaben, ihre Malware Anfang 2022 in Rente zu schicken.

BAZALOADER:

BazaLoader wurde zuerst im April 2020 entdeckt und wird genutzt, um andere Malware herunterzuladen. Die Malware wird immer noch aktiv weiterentwickelt und soll für die Ransomware Conti den Erstzugriff bereitstellen.

Das Diagramm auf den Seiten 20 und 21 zeigt die Nachrichtenvolumen bekannter Malware-Familien, die einem oder mehreren Ransomware-Betreibern den Erstzugriff bereitstellen. Außerdem sind hier auch einige der bekanntesten Ransomware-Angriffe des letzten Jahres aufgeführt. In den meisten Fällen sind die Verbindungen zwischen Malware- und Ransomware-Betreibern auf Einzelfälle beschränkt oder zufällig (obwohl Forscher Hinweise auf Verbindungen zwischen dem Malware-Verteiler **FIN7** und den Ransomware-Betreibern **DARKSIDE**, **BLACKMATTER** und **REvil** fanden). Dank der Conti-Leaks verfügen wir jedoch über den endgültigen Beweis dafür, dass Conti stark auf **BAZALOADER**, **TRICKBOT** und Emotet setzt. Im Falle der letzteren beiden scheint es, dass die Stilllegung von TrickBot und das plötzliche Wiederauftauchen von Emotet zu Beginn Anfang 2022 direkt in Beziehung stehen. Emotet ist inzwischen für Conti das Mittel der Wahl für den Erstzugriff.

Wie die Verbindungen zwischen TrickBot, Emotet und Conti zeigen, schützen Sie sich am besten vor dieser Art von Erpressung, indem Sie gar nicht erst zulassen, dass Malware überhaupt in Ihr Unternehmen gelangt. Und da sämtliche im Diagramm gezeigte Malware über schädliche E-Mails verteilt wird und auf menschliche Fehler setzt, sind starke E-Mail-Sicherheit und geschulte Anwender wichtige erste Schritte, um Ransomware-Angreifer aus Ihrer Umgebung fernzuhalten.

Große Technologieanbieter sind unsere Rettung – oder nicht?

Cyberangreifer verlassen sich nicht nur auf ihre eigene Raffinesse, um Vertrauen zu wecken, sondern nutzen auch legitime Anbieter wie Microsoft OneDrive, Google Drive und Dropbox für ihre Kampagneninfrastruktur. Das liegt zum einen an der Benutzerfreundlichkeit dieser Services, aber auch daran, dass die Opfer eher geneigt sind, einem Link zu einem bekannten Service zu vertrauen.

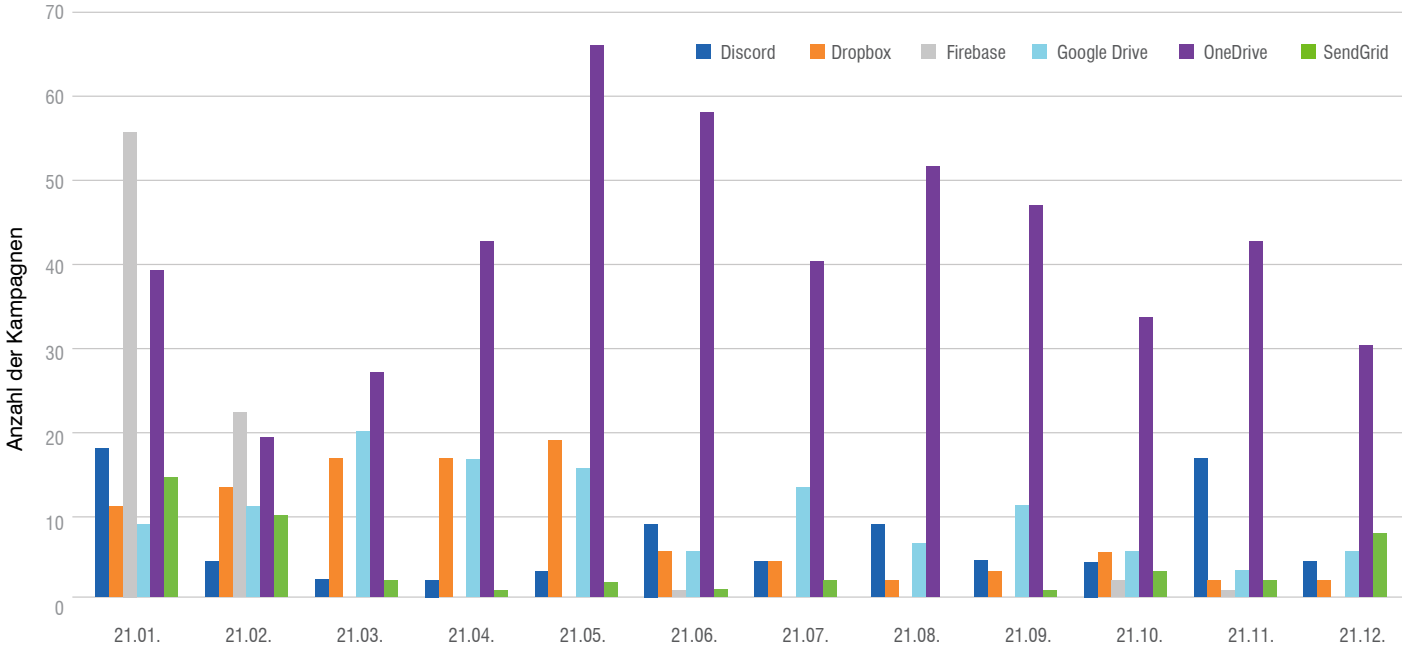


Abb. 12: Kampagnen, die legitime Services nutzen, 2021.

TA571:

Ein finanziell motivierter Malware-Verbreiter, der mehrere Branchen in Nordamerika angreift und Mitte 2019 zum ersten Mal beobachtet wurde.

URSNIF:

Ein verbreiteter Bank-Trojaner, der sich aus einer Malware-Familie namens Gozi entwickelte, deren Quellcode 2015 geleakt wurde. Ursnif ist die beliebteste mehrerer aus Gozi entstandenen Varianten, zu denen beispielsweise Dreambot, ISFB und Papras gehören.

TA579:

Ein finanziell motivierter Malware-Verbreiter, der mehrere Branchen in Nordamerika angreift und Mitte 2021 zum ersten Mal beobachtet wurde.

Microsoft OneDrive und Google Drive waren die am häufigsten eingesetzten legitimen Infrastrukturen, die von den durch uns beobachteten Top-Cybercrime-Akteuren genutzt werden. Üblicherweise sind Links zu diesen Services entweder direkt im Textteil einer schädlichen Nachricht enthalten oder in eine angehängte PDF-Datei eingebettet. Da die Webmail-Produkte von Google und Microsoft integrierte Virenscans besitzen, gehen die Opfer möglicherweise davon aus, dass von diesen Services gehostete Dateien die gleichen Prüfungen durchlaufen.

Unter den Cyberkriminellen mit großem Nachrichtenvolumen setzt die Gruppe **TA571** verstärkt auf OneDrive und Google Drive zur Verbreitung ihrer Malware. Die TA571-Kampagnen enthalten meist einen E-Mail-Link zu einer ZIP-Datei, die auf einem der beiden Services gehostet wird. In diesem komprimierten Ordner befindet sich eine Excel-Datei, die bei aktivierten Makros die Malware **URSNIF** ablegt.

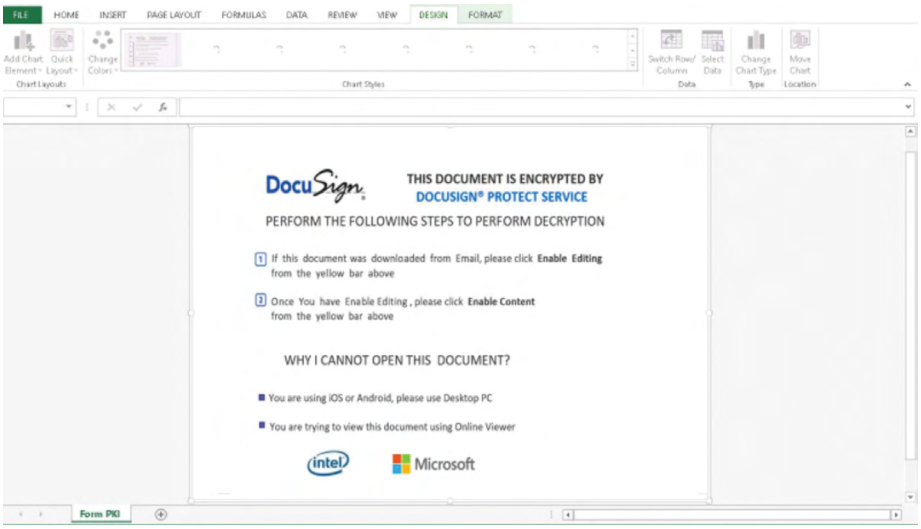


Abb. 13: Ein Dokument mit Schaddaten von TA571.

TA571 und der Bedrohungsakteur **TA579** setzen außerdem stark auf OneDrive, um BazaLoader zu verteilen. Damit sind legitime Infrastrukturen ein Kernbestandteil von Kampagnen, die Conti, Ryuk und ihresgleichen den Erstzugriff bereitstellen.

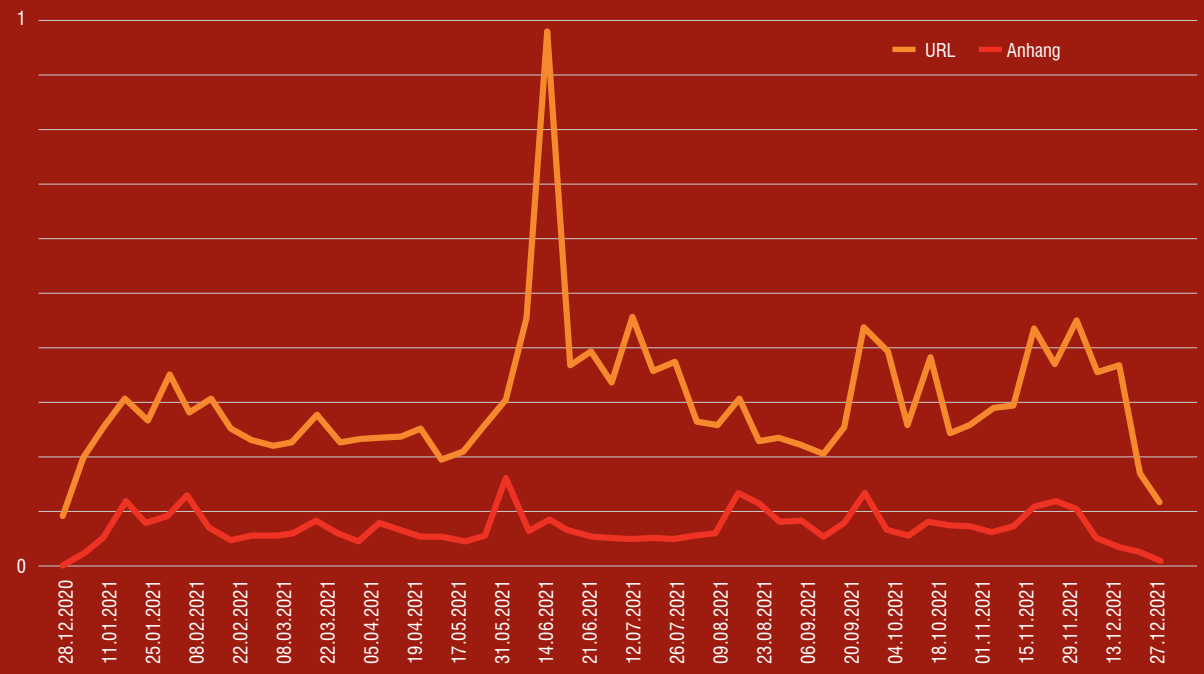


Abb. 14: Nachrichtenaufkommen von Angriffen mit URLs und Anhängen, 2021.
(Hinweis: Skala ist normalisiert, um vertrauliche Proofpoint-Daten zu schützen)

E-Mail-Bedrohungen

E-Mails sind universell, für moderne Unternehmen unverzichtbar – und grundsätzlich unsicher! Das E-Mail-Kommunikationssystem wurde entwickelt, lange bevor das Internet zum Mainstream wurde. Dabei spielten Privatsphäre und Sicherheit zunächst überhaupt keine Rolle. In den 45 Jahren, die seitdem vergangen sind, haben sich E-Mails zu einer grundlegenden Säule der modernen Geschäftskommunikation entwickelt – und zu einem zentralen Punkt für alle Arten von Angriffen.

Gefährliche Anhänge und Links

Viele Menschen glauben immer noch, Malware würde typischerweise über verdächtige Anhänge im Posteingang verbreitet. Laut unseren Daten sind jedoch E-Mails mit schädlichen Links 3 bis 4 Mal so häufig wie Angriffe mit Anhängen.

Auch wenn URL-basierte Bedrohungen häufiger sind, zeigen die Daten aus unserem aktuellen „State of the Phish"-Bericht, dass die Fehlerquoten bei Anhang-basierten Angriffen fast doppelt so hoch sind. (Das bedeutet, dass Anwender doppelt so häufig schädliche Dateien herunterladen, wie sie auf einen schädlichen Link klicken.)

Die meisten Menschen verstehen mittlerweile, dass Cyberangriffe sowohl Unternehmen als auch Einzelpersonen gefährden. In einer solchen hektischen und stressigen Umgebung kann angelesenes Wissen jedoch kontraproduktiv sein. Regelmäßige Schulungen, die auf die neuesten von Angreifern genutzten Taktiken, Techniken und Prozeduren eingehen, sensibilisieren Ihre Mitarbeiter zuverlässig für Gefahren und stärken Ihre letzte Verteidigungslinie.

„Freundliche“ Betrüger

Ein grundlegender Bestandteil von Social Engineering ist Vertrauen. Um jemanden davon zu überzeugen, mit einem schädlichen Inhalt zu interagieren, muss diese Person dazu gebracht werden, der Quelle des Inhalts zu vertrauen – oder das Misstrauen zumindest so lange abzulegen, bis das Ziel erreicht ist. Im letzten Jahr erlebten wir immer häufiger, dass Cyberkriminelle erst mit einigem Aufwand das Vertrauen ihrer Opfer gewannen, bevor sie den Angriff durchführten.

Die häufigste Form von Konversationsbedrohungen nutzt aufgabenorientierte Köder, d. h. eine Form von Business Email Compromise (BEC, auch als Chefmasche bezeichnet). Solche Angriffe beginnen typischerweise mit einer harmlosen Anfrage, ob der Empfänger eine einfache Aufgabe durchführen kann. Wenn sich das Opfer darauf einlässt, bittet der Angreifer um Geld, Gutscheinkarten oder um die Änderung einer Rechnung. In einem durchschnittlichen Monat verzeichnen wir rund 80.000 E-Mails mit Aufgabenbetrug.

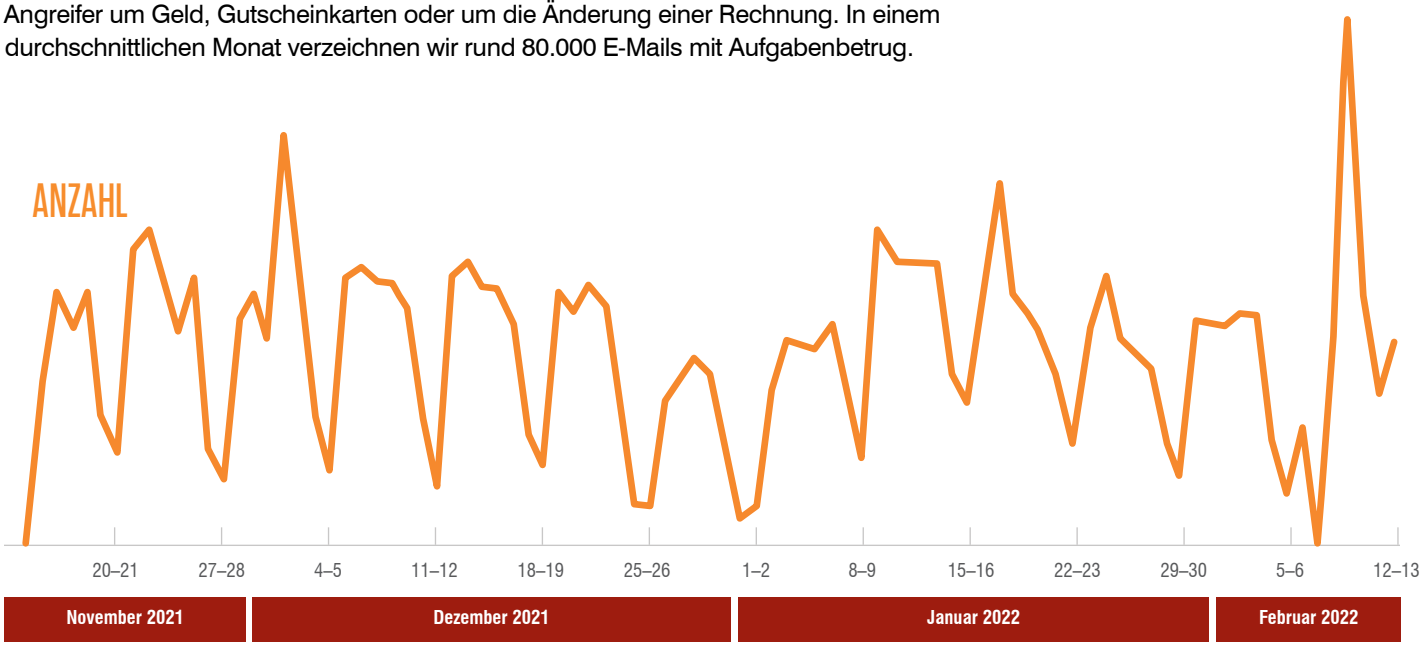


Abb. 15: BEC-Betrugsversuche mit Aufgaben.

TA576:

Dieser Bedrohungsakteur ist bekannt für Angriffe auf Buchhaltungsunternehmen und Finanzinstitute in der typischen Abgabezeit für Steuererklärungen. Dabei versucht TA576, Remote-Zugriffs-Trojaner mithilfe von steuerbezogenen E-Mail-Ködern zu verteilen. Wurde 2018 zum ersten Mal beobachtet.

Der Konversationsansatz lässt sich auch für die Verbreitung von Malware nutzen. Der von uns als **TA576** geführte Angreifer ist vor allem für Kampagnen mit geringem Nachrichtenvolumen bekannt, die sich in erster Linie gegen Buchhaltungs- und Finanzabteilungen richten. Als Köder dienen meist Bitten um Hilfe bei Steuerfragen. Wenn jemand bei der angegriffenen Abteilung reagiert, antwortet TA576 mit einer E-Mail, die einen Link zum Remote-Zugriffs-Trojaner NetWire enthält.

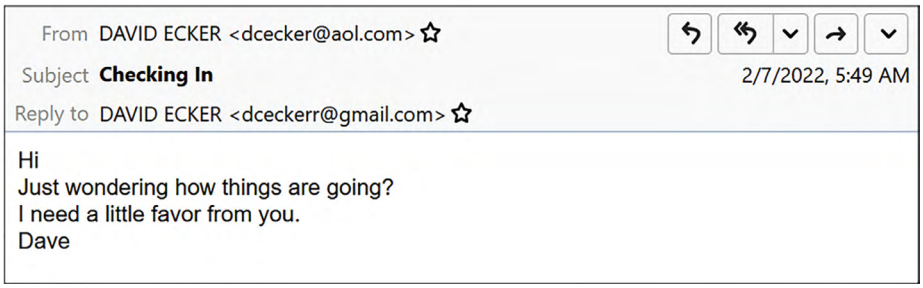


Abb. 16: Beispiel für eine schädliche E-Mail mit Aufgabenbetrug.

DEMONWARE:

Eine Ransomware-Familie, die für die Versuche ihres Betreibers bekannt ist, Insider zum Durchführen von Angriffen zu rekrutieren.

TA499:

Ein Bedrohungsakteur, der mit dem russischen Staat in Verbindung stehen soll. Er ist darauf spezialisiert, oppositionelle Politiker, Prominente und Sportler mit peinlichen Informationen zu kompromittieren. Die Angriffe werden mithilfe harmloser E-Mails durchgeführt, die Informationen erfragen und gefälschte Video-Chats anbahnen.

TA453:

Ein mit dem Iran in Verbindung stehender APT-Akteur. Die Gruppe verfolgte stets die Interessen der Islamischen Revolutionsgarden und griff Dissidenten, Akademiker, Diplomaten und Journalisten an.

Die größten Ransomware-Bedrohungen werden meist nicht direkt per E-Mail verbreitet, was jedoch nicht heißen soll, dass Ransomware-Gruppen diesen Kanal ignorieren. Im Sommer 2021 stellten wir fest, dass die Ransomware-Gruppe **DEMONWARE** Nachrichten versendet, die Angestellte zum Infizieren ihrer eigenen Computer verleiten sollte, um dafür einen Teil des Profits zu erhalten. Abgesehen vom Angebot an den Empfänger, sich an kriminellen Handlungen zu beteiligen, enthielt die E-Mail keine weitere schädlichen Elemente. Interessierte Mitarbeiter sollten einen Telegram-Chat-Kanal besuchen und dort weitere Anweisungen erhalten.

2021 fanden wir auch zahlreiche Fälle, bei denen staatlich unterstützte Angreifer bzw. APT-Akteure längere Gespräche nutzten, um die Basis für einen Angriff zu schaffen. Eine Kampagne des mit Russland verbundenen Akteurs **TA499** nutzte Anfang 2021 vertrauensbildende E-Mails, um die Empfänger zu Telefon- oder Video-Chat-Gesprächen zu verleiten. Das Ziel bestand wahrscheinlich darin, die russische Opposition negativ dastehen zu lassen. Ebenso hat der mit dem Iran in Verbindung stehende Angreifer **TA453** häufig Konversationskampagnen durchgeführt. Dabei nutzte er unter anderem Telefonanrufe, um Vertrauen zu schaffen, bevor er Informationen und Anmeldedaten anforderte.

Hijacking von Gesprächen

Eine der einfachsten Möglichkeiten, das Vertrauen eines potenziellen Opfers zu erlangen, besteht in der Übernahme der Identität eines vertrauenswürdigen Kontakts. Deshalb ist das Thread-Hijacking bzw. die Übernahme von Gesprächen bei einigen finanziell motivierten Angreifern mit hohem Nachrichtenvolumen sehr beliebt.

Für das Thread-Hijacking benötigt der Angreifer Zugriff auf ein kompromittiertes Postfach, den er durch Anmeldedaten-Phishing, eine bestehende Malware-Infektion oder Password Spraying erlangt hat. Bei stark verbreiteten Botnets erfolgt dies automatisiert. In erfassten E-Mails, deren Betreffzeilen „Re:" oder „Fwd:" enthalten, werden Inhalte oberhalb des Threads eingefügt und zurück an die Anwender in der Kette geschickt. BEC-Angriffe nutzen diese Technik ebenfalls häufig, wobei sie manuell arbeiten und die Nachrichten dadurch für ihre anvisierten Opfer anpassen können. Sobald der Angreifer Zugriff auf ein Postfach erhält, antwortet er auf einen vorhandenen E-Mail-Thread und hängt meist einen schädlichen Anhang bzw. eine URL an oder fordert zu einer Aktion im Sinne des Angreifers auf.

Da die E-Mail von einem legitimen Konto gesendet wird, wirkt sie wie echte Korrespondenz und erhöht dadurch die Wahrscheinlichkeit, dass der Empfänger sich wunschgemäß verhält.

Malware-Kampagnen mit Thread-Hijacking, 2021

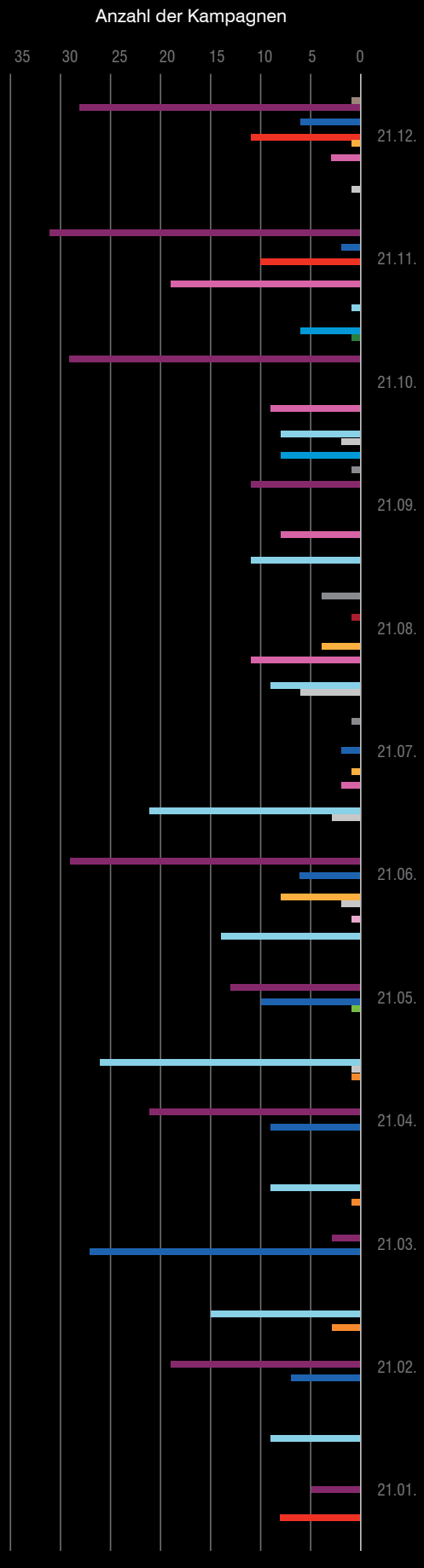


Abb. 17: Malware-Kampagnen mit Thread-Hijacking, 2021.

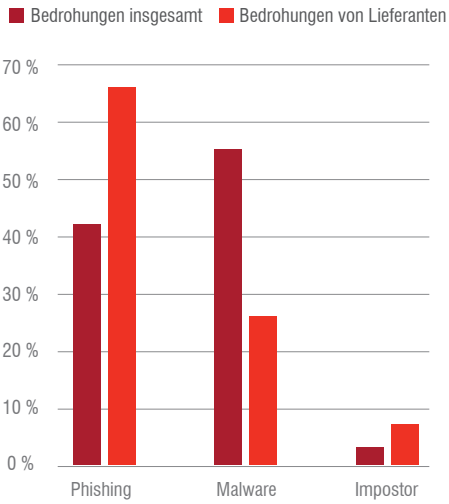


Abb. 18: Lieferantenbedrohungen und sonstige Bedrohungen (30-Tage-Zeitraum, 22. Februar bis 23. März 2022).

Unterbrechung der Lieferkette

Angriffe, die von einer Lieferantendomäne gesendet werden, haben einen anderen Aufbau als andere Attacken. Jeden Monat erhalten mehr als 80 % unserer Kunden eine Bedrohung, die von einem ihrer Lieferanten zu stammen scheint. Diese Zahl ist nur etwas geringer als der Anteil der Kunden, die überhaupt eine Bedrohung erhalten hat.

Lieferkettenbedrohungen unterscheiden sich insbesondere bei der wahrscheinlichen Angriffsrichtung. Wie dieses Diagramm zeigt, handelt es sich bei Lieferantenbedrohungen im Gegensatz zu den sonstigen Bedrohungen in erster Linie um Phishing- oder Impostor-Angriffe. Außerdem kommt nur sehr selten Malware zum Einsatz.

Phishing- und Impostor-Bedrohungen nutzen vor allem das Vertrauen des Opfers und seine Bekanntschaft mit dem vermeintlichen Absender aus. Noch auffälliger wird diese Dynamik bei einem Blick auf die Verteilung stark und moderat gezielter sowie breitgefächerter Bedrohungen[2], die von Lieferantendomänen gesendet werden. Bei ansonsten gleichen Bedingungen könnte man glauben, dass Unternehmen weniger stark gezielte Bedrohungen erhalten, da die Ausforschung zeitraubend ist, was zu weniger E-Mail-Aufkommen führt. Bei einer gefälschten oder kompromittierten Lieferantendomäne können Cyberkriminelle jedoch leichter detaillierte Angriffe erstellen, was zu einer außergewöhnlich großen Zahl äußerst gezielter Angriffe führt.

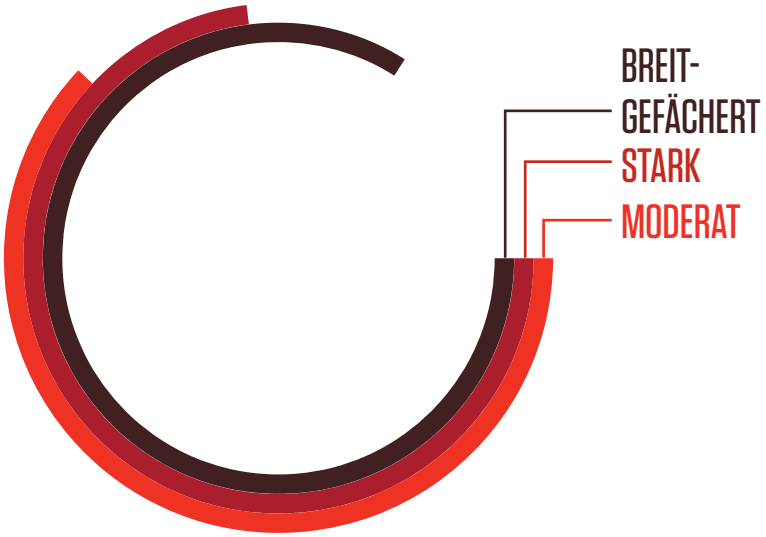


Abb. 19: Verteilung von Angriffstypen von Lieferantendomänen (30 Tage).

Auch wenn Malware-Angriffe von kompromittierten Lieferanten nicht ausgeschlossen werden können, sollten Sicherheitsschulungen insbesondere auf das Risiko gezielter Social-Engineering-Angriffe über Lieferantenkonten eingehen. Cyberkriminelle erledigen ihre Hausaufgaben und verhalten sich wie bekannte (Geschäfts-)Partner, sodass der Schutz vor kompromittierten Lieferanten sehr schwierig ist. Allerdings ist E-Mail-Sicherheit mit Machine Learning darauf trainiert, die kleinen Details zu erkennen, die solche Angriffe entlarven.

2 Stark: an weniger als 5 unterschiedliche Zieldomänen gesendet; Moderat: an 5 bis 39 unterschiedliche Zieldomänen gesendet; Breitgefächert: an mehr als 40 unterschiedliche Zieldomänen gesendet

Der TOAD kam per Telefon

Eine der Entwicklungen, die wir in diesem Jahr am wenigsten erwartet hatten, war die starke Zunahme von Angriffen per Telefon (Telephone-Oriented Attack Delivery, TOAD). Diese Angriffe erfordern sehr direkte Interaktionen, da bei den per E-Mail verschickten Ködern keine Malware oder schädlichen URLs zum Einsatz kommen. Stattdessen sollen die Opfer dazu verleitet werden, einen Fake-Kundendienst anzurufen. Wenn das Opfer den Köder geschluckt hat, weist der Angreifer es per Telefon an, ihm Remote-Zugriff auf seinen Computer zu geben oder Malware manuell herunterzuladen. Laut unseren Daten gibt es jeden Tag mehr als 100.000 Angriffsversuche dieser Art.

Es ist nicht einfach, Opfer zu einem Telefonanruf zu verleiten, und die TOAD-Köder des letzten Jahres nutzten enorm kreatives Social Engineering. Die Verbreiter der Malware BazaLoader verwendeten sehr kreative Kampagnen, z. B. für Fake-Websites für Streaming-Filme oder gefälschte Konzertkarten für Größen wie Justin Bieber und The Weeknd.

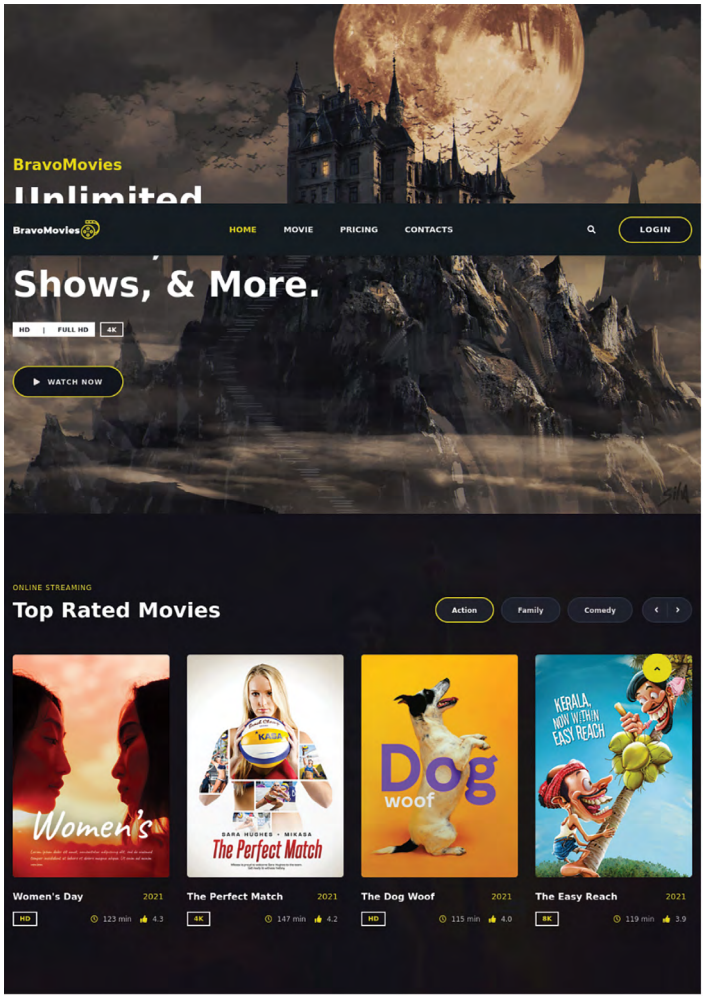


Abb. 20: Ein Fake-Service für Streaming-Filme, der bei Angriffen per Telefon genutzt wurde.

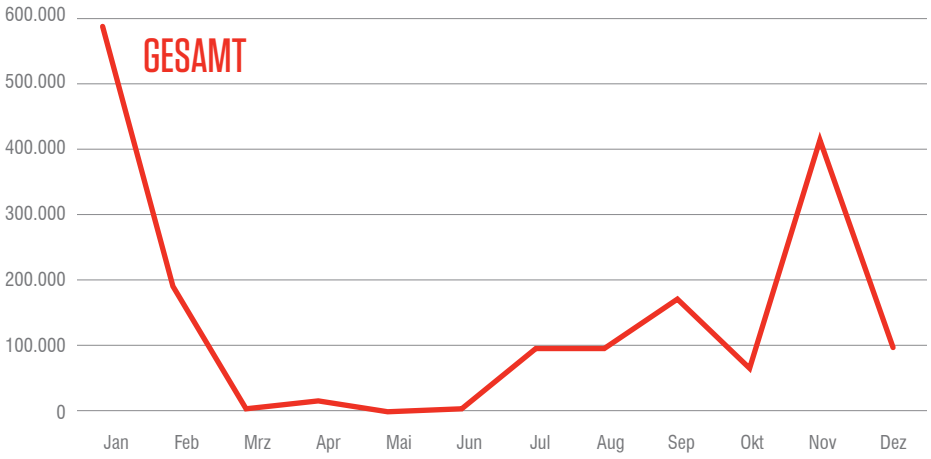


Abb. 21: Nachrichtenaufkommen von BazaLoader, 2021. (Hinweis: nicht alle Kampagnen nutzten die TOAD-Methode.)

Bedrohungen für Mobilgeräte

Smartphones sind absolut persönliche Geräte. Sie enthalten detaillierte Momentaufnahmen unseres Lebens, einschließlich wertvolle Informationen über unsere Beziehungen, Finanzen sowie Vorlieben und Abneigungen. Doch wie bereits oben erwähnt, lassen diese Geräte auch die Grenze zwischen dem Privat- und Berufsleben verschwimmen. Mit einer einzigen Kompromittierung stehen einem Angreifer nicht nur die Finanzen seines Opfers offen, sondern möglicherweise auch das Netzwerk von dessen Arbeitgeber. Das macht Smartphones zu einem sehr attraktiven Angriffsziel.

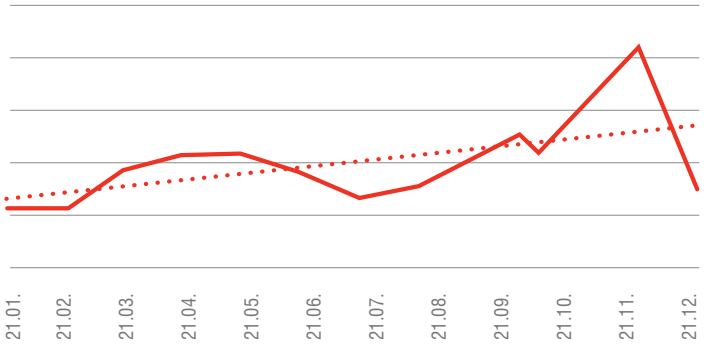


Abb. 22: Berichte über Phishing-Versuche per SMS in den USA, 2021.

State of the Smish

Im diesjährigen „State of the Phish"-Bericht räumten 54 % der Umfrageteilnehmer ein, dass sie ihre privaten Smartphones für berufliche Zwecke nutzen. Mit anderen Worten: Das Smartphone enthält die Schlüssel zum privaten und beruflichen Leben. Wenig überraschend möchten auch Cyberkriminelle diese doppelte Gelegenheit nutzen und haben dementsprechend ihre Angriffe auf Mobilgeräte gesteigert.

Die Köder bei SMS-Phishing (auch als Smishing bezeichnet) versuchen meist, Dringlichkeit zu erzeugen und Verlustaversion auszunutzen. Diese psychologischen Auslöser wirken insbesondere bei Smartphones sehr stark, da Menschen bei SMS-Nachrichten deutlich eher reagieren als bei E-Mails oder Nachrichten auf dem Computer.

In Großbritannien konzentrierten sich Mobilgeräte-Angreifer wegen der höchsten Erfolgsquote immer stärker auf Benachrichtigungen für Paketlieferungen. In den letzten drei Monaten des Jahres 2021 machen diese Nachrichten mehr als die Hälfte der SMS-Köder aus. Gleichzeitig gab es einen starken Rückgang bei Banking-Ködern, was möglicherweise auf Sensibilisierungskampagnen durch die Finanzbranche zurückzuführen ist.

Bei Verbrauchern in den USA sieht die Smishing-Situation ähnlich aus. Da Amazon jedoch einen Großteil seiner eigenen Logistik übernimmt, waren die Benachrichtigungsköder in die Kategorien Zustellungen und Händler aufgeteilt.

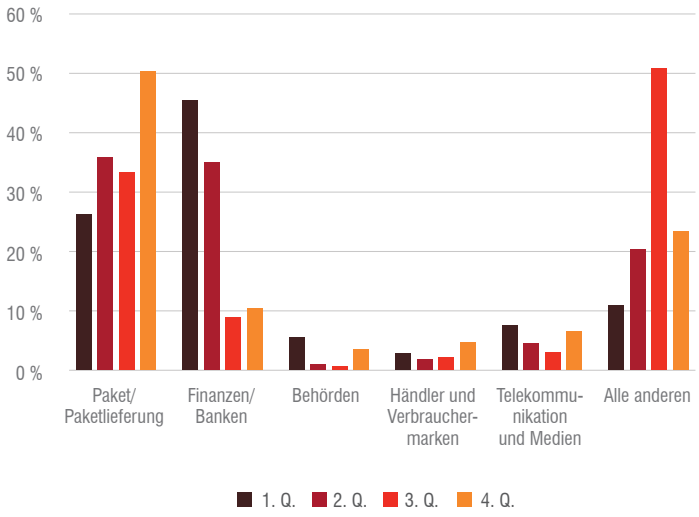


Abb. 23: Kategorien der SMS-Köder in Großbritannien, 2021.

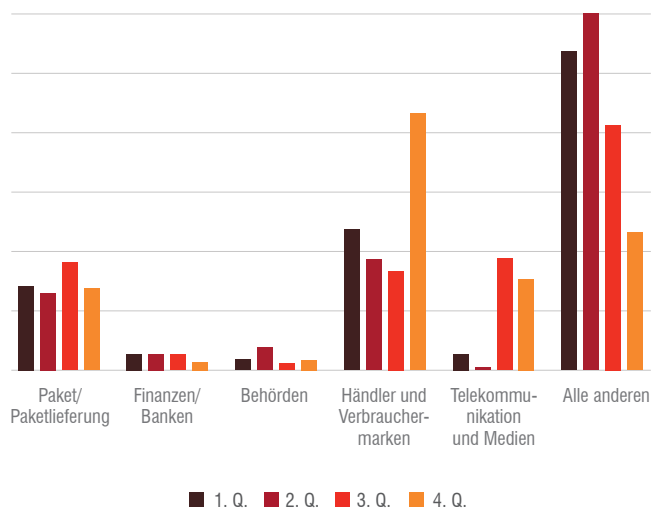


Abb. 24: Kategorien der SMS-Köder in den USA, 2021.

Kopfschmerzen durch FluBot

Smartphones sind nicht nur ein Ziel für Smishing-Aktivitäten, sondern auch im Visier von Malware-Entwicklern.

Abb. 25: Meldungen zu FluBot.
(Hinweis: Skala ist normalisiert, um vertrauliche Proofpoint-Daten zu schützen)

FLUBOT:

Eine leistungsstarke Android-Malware, die Daten exfiltrieren, Anrufe und Nachrichten abfangen sowie überlagernde Bildschirmmasken zum Diebstahl von Anmeldedaten für viele beliebte Banking-Apps einblenden kann.

FLUBOT ist eine raffinierte, wurmartige Malware, die Ende 2020 in Erscheinung trat. Zum ersten Mal wurde sie in Spanien entdeckt, von wo sie sich auf andere Länder ausbreitete und im März 2021 Großbritannien erreichte. Die Malware verbreitet sich, indem sie auf das Adressbuch infizierter Geräte zugreift und neue infizierte Nachrichten an die darin enthaltenen Telefonnummern verschickt. Durch die Kombination mit einem überzeugenden Köder (z. B. einer Lieferbenachrichtigung) konnte sich diese Malware besonders virulent ausbreiten.

Sobald FluBot in einem System Fuß gefasst hat, kann die Malware Nachrichten lesen und versenden, andere installierte Apps löschen, Telefonanrufe durchführen, auf das Internet zugreifen und Bildschirmmasken für Anmelde-datendiebstahl bei verschiedenen Banking-, Makler und sonstigen Finanz-Apps einblenden. Da mitunter mehrere Finanzkonten auf dem gleichen Gerät verwaltet werden, kann eine einzige FluBot-Infektion verheerende Folgen haben.

Bedrohungen für die Cloud

Die Cloud-Infrastruktur ist mittlerweile eine unverzichtbare Komponente der meisten IT-Umgebungen. Parallel zur Verbreitung der Cloud-Technologie haben jedoch auch Angriffe auf Cloud-Konten Einzug gehalten.

Erfassung von Cloud-Angriffen

Unsere Daten für das Jahr 2021 zeigen, dass jeden Monat mehr als 90 % der überwachten Cloud-Mandanten angegriffen wurden. Fast ein Viertel (24 %) der Cloud-Mandanten wurde erfolgreich angegriffen, wobei der Gesamtanteil der kompromittierten Mandanten im Laufe des Jahres auf 63 % stieg. (Hinweis: Nicht alle Mandanten mit konfigurierten Warnungen nutzen automatische Behebungs- oder Schutzmaßnahmen.) Mit anderen Worten: Ebenso wie E-Mail-basiertes Phishing und Malware-Übertragung hat sich auch die Kompromittierung von Cloud-Konten zu einer festen Größe in der Bedrohungslandschaft entwickelt.

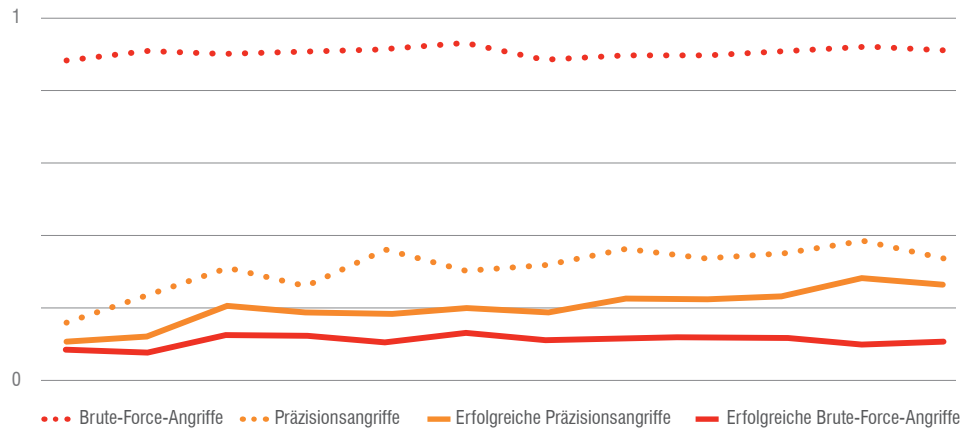


Abb. 26: Brute-Force- und Präzisionsangriffe auf Cloud-Konten – Umfang und Erfolgsraten, 2021.
(Hinweis: Skala ist normalisiert, um vertrauliche Proofpoint-Daten zu schützen)

BRUTE-FORCE-ANGRIFFE:

95 %

Brute-Force-Angriffe kamen bei 95 % der angegriffenen Unternehmen zum Einsatz. Außerdem wurde fast ein Drittel (32 %) der Cloud-Mandanten 2021 auf diese Weise kompromittiert.

Brute-Force-Attacken sind für die meisten Bedrohungsakteure auch weiterhin das Mittel der Wahl und kamen bei 95 % der angegriffenen Unternehmen zum Einsatz. Außerdem wurde fast ein Drittel (32 %) der Cloud-Mandanten 2021 auf diese Weise kompromittiert. Veränderungen gab es bei der Häufigkeit und Raffinesse von Präzisionsangriffen. Die Zahl der Präzisionsangriffe auf Cloud-Mandanten stieg im Laufe des Jahres stetig und zeichnete sich durch wachsenden Erfolg aus.

Insgesamt verzeichneten 75 % der Cloud-Mandanten einen Präzisionsangriff, wobei 60 % dadurch kompromittiert wurden. Während sich Brute-Force-Attacken gegen dreimal so viele Mandanten wie bei Präzisionsangriffen richteten, waren letztere doppelt so erfolgreich. Außerdem wurden per Präzisionsangriff kompromittierte Konten später häufiger für die Erstellung und Verteilung von Cloud-Malware missbraucht.

Abschnitt 3

Berechtigungen

Wie aktuelle Cloud-Kompromittierungen gezeigt haben, kann ein Satz SSO-Anmeldedaten (Single Sign-On, einmalige Anmeldung) Zugriff auf vertrauliche Daten, Organisationsstrukturen und Unternehmenssysteme gewähren. In unserem Risikomodell lassen sich anhand der **Berechtigungen** für die Systeme und Daten, auf die Ihre Anwender Zugriff haben, die möglichen Schäden durch eine Kompromittierung ermitteln.

Dies ist wahrscheinlich auch der einzige Bereich unseres Modells, in dem Unternehmen potenziell die größte Kontrolle haben. Wie jedoch viele schlagzeilenträchtige Ereignisse aus dem letzten Jahr zeigen, ist die Kontrolle und Verwaltung von Berechtigungen bei einigen Unternehmen noch „in Arbeit“.

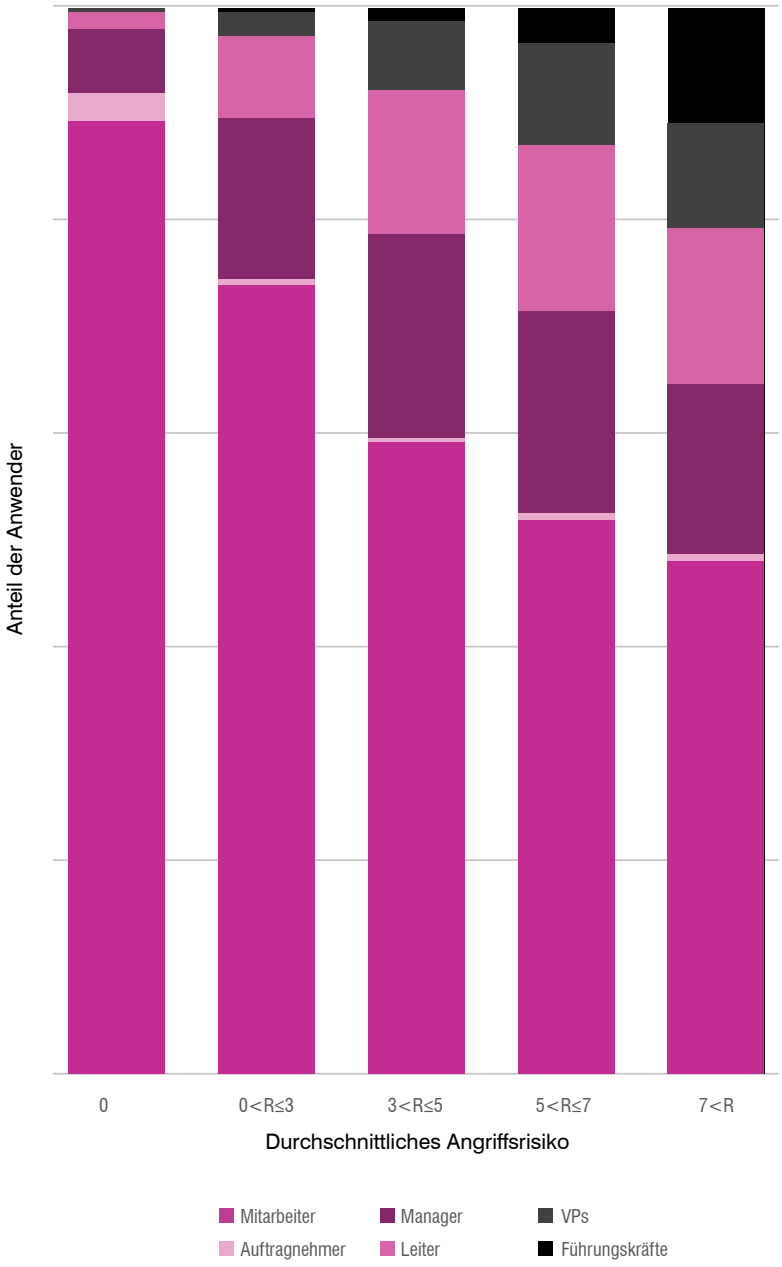


Abb. 27: Durchschnittliches Angriffsrisiko nach Position, 2021.

Anwender mit umfangreichen Berechtigungen besonders häufig angegriffen

In den Unternehmen unseres Datensatzes werden etwa 10 % der Anwender als Manager, Leiter oder Führungskräfte eingestuft. Unsere Daten zeigen jedoch, dass gerade für diese Gruppe das größte Angriffsrisiko besteht.

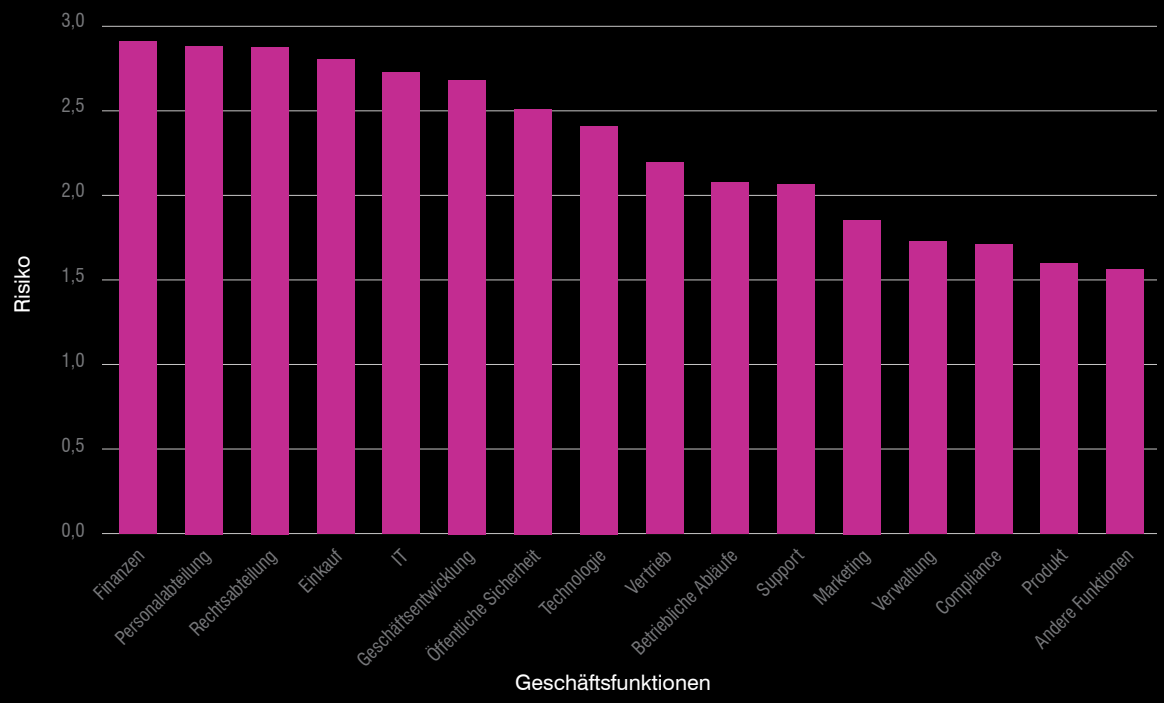


Abb. 28: Durchschnittliches Angriffsrisiko nach Abteilung, 2021.

Ebenso gelten Abteilungen, die mit vertraulichen Informationen arbeiten (z. B. die Finanz-, Rechts- und Personalabteilung), als stärker gefährdet als beispielsweise die Marketing- und Produktabteilung.

Wenn Sie wissen, wo die größten berechtigungsbasierten Risiken bestehen (ganz gleich, ob das für Einzelpersonen oder Abteilungen gilt), ist das bereits ein wichtiger Schutz Ihres Unternehmens vor Angriffen. Anwender mit umfangreichen Berechtigungen können zusätzliche Schulungen erhalten, die speziell auf die erhöhte Gefährdungslage zugeschnitten sind. Ebenso dürften Abteilungen, die mit vertraulichen oder wertvollen Daten arbeiten, von zusätzlichen Sicherheits- oder Aufsichtsebenen profitieren.

Verdächtige Cloud-Aktivitäten

Für den Zugriff auf viele Unternehmenssysteme ist heute nur noch ein einziger Satz Anmeldeinformationen notwendig, was zu einer erheblichen Zunahme von berechtigungsbasierten Risiken geführt hat. In den falschen Händen kann ein Konto dauerhaften Zugriff auf schädliche Anwendungen, die Manipulation und potenzielle Exfiltration vertraulicher Informationen und Dateien und sogar das Einschleusen von schädlichem Code in freigegebene Repositorys ermöglichen. In mehreren Fällen fanden wir schädliche **OAUTH**-Anwendungen, die in kompromittierten Cloud-Umgebungen erstellt wurden. Dank ihres Status als vertrauenswürdiger Ersteller konnten die Angreifer mithilfe dieser Anwendungen anschließend weitere Cloud-Konten infizieren.

Im Verlauf des Jahres stellte unser Cloud-Sicherheitsteam fest, dass 35 % der Mandanten mit einer verdächtigen Anmeldung anschließend verdächtige Dateiaktivitäten verzeichneten. Zudem fanden wir mehr als 200 schädliche Anwendungen, die gegen mehr als 55 % der Cloud-Mandanten eingesetzt wurden. Im Durchschnitt fand sich in der IT-Umgebung von etwa 10 % der Unternehmen mindestens eine autorisierte und aktive schädliche Anwendung.

OAUTH:

Ein offenes Standard-Authentifizierungsprotokoll, das mithilfe von Token Zugriff auf Online-Dienste gewährt, ohne dass Kennwörter erforderlich sind. Kommt zum Einsatz, wenn Facebook- oder Google-Anmeldedaten für den Zugriff auf externe Websites und Anwendungen genutzt werden, aber auch in einigen unternehmenseigenen Cloud-Umgebungen.

Datenverlustprävention

Insider-Bedrohungen stellen ein wachsendes Risiko für Unternehmen dar. Das liegt auch daran, dass Cyberkriminelle unseren Beobachtungen zufolge verärgerte Mitarbeiter zu rekrutieren versuchen.

Im Jahr 2020 waren die meisten Unternehmen hektisch bemüht, sich auf die plötzliche Notwendigkeit von Telearbeit einzustellen, konnten das neue System jedoch bis Anfang 2021 auf breiter Front einführen. Im Verlauf des Jahres entwickelten viele Firmen Pläne für dauerhafte Hybrid-Arbeitsmodelle, bei denen Angestellte ebenso viel Zeit im Büro wie zu Hause verbringen.

Trotz dieser Veränderungen verzeichneten wir nur wenig Bewegung bei Warnungen zu Datenverlustprävention. Nicht gelistete USB-Geräte bereiten weiterhin die größten Sorgen, obwohl auch der Download potenziell schädlicher Dateien und die Exfiltration von Daten per USB zunehmend als Problem angesehen werden. Das Drucken großer Mengen von Papierdokumenten zu ungewöhnlichen Zeiten schaffte es wieder in die Top 10, nachdem diese Gefahr während der Pandemie verständlicherweise aus der Liste gefallen war.

AKTION	RANG 2021	RANG 2020
Anschließen eines nicht gelisteten USB-Geräts	1	1
Kopieren großer Dateien oder Ordner	2	2
Exfiltrieren einer überwachten Datei ins Internet per Upload	3	3
Herunterladen von Dateien mit potenziell schädlichen Erweiterungen	4	5
Öffnen einer Klartextdatei, die Kennwörter enthalten könnte	5	4
Exfiltrieren einer Datei auf nicht gelistetes USB-Gerät	6	7
Installation von Hacker- oder Spoofing-Tools	7	8
Zugriff auf Cloud-Dienste für Upload und Freigabe	8	9
Öffnen des ObserveIT-Agenten-Ordners	9	10
Drucken großer Seitenzahlen zu ungewöhnlichen Zeiten	10	11

Tabelle 1: Häufigste von Kunden konfigurierte DLP-Warnungen, 2021.

In vielen Fällen ist die zunehmende Einführung von Hybrid-Arbeit erst der Anfang. Wenn jedoch immer mehr Mitarbeiter ins Büro zurückkehren, rechnen wir damit, dass Risikobewertungen für Berechtigungen das berücksichtigen werden. Die Angriffsfläche verändert sich ständig – und die Prioritäten und Schwerpunkte der Sicherheitsteams müssen dem Rechnung tragen.

Fazit

Aktuelle, auf menschliches Verhalten zielende Bedrohungen können nur mit einem auf den Mensch ausgerichteten Schutz abgewehrt werden.

In den meisten Fällen spielt der Faktor Mensch eine größere Rolle als die technischen Aspekte eines Angriffs. Cyberkriminelle suchen nach Beziehungen, die ausgenutzt, Vertrauensstellungen, die missbraucht und Zugriffsmöglichkeiten, die eingesetzt werden können.

Verwenden Sie daher eine Lösung, die Ihnen zeigt, wer wie angegriffen wird und ob die angegriffene Person geklickt hat. Berücksichtigen Sie dabei das individuelle Risiko der einzelnen Anwender, einschließlich der Informationen dazu, wie sie angegriffen werden, auf welche Daten sie zugreifen können und wie leicht sie sich täuschen lassen.

Wir empfehlen folgende Maßnahmen für personenzentrierten Schutz:

Schwachstellen

Die meisten Cyberangriffe sind nur dann erfolgreich, wenn Menschen darauf hereinfallen. Das Schließen von Schwachstellen beginnt mit Schulungen zur Sensibilisierung für Sicherheit und mit risikobasierten Kontrollen.

- Schulen Sie Ihre Anwender darin, schädliche E-Mails zu erkennen und zu melden. Mit regelmäßigen Schulungen und simulierten Angriffen lassen sich viele Angriffe stoppen und die Menschen identifizieren, die besonders gefährdet sind. Die besten Simulationen imitieren reale Angriffstechniken. Wählen Sie daher eine Lösung, die hierfür aktuelle Trends und neueste Bedrohungsdaten einbezieht.
- Gehen Sie davon aus, dass Anwender früher oder später auf eine Bedrohung klicken werden. Angreifer finden immer neue Möglichkeiten, den Faktor Mensch auszunutzen. Suchen Sie nach einer Lösung, die Bedrohungen mithilfe zusätzlicher Sicherheitsebenen für Ihre anfälligsten Anwender neutralisiert.
- Isolieren Sie riskante Websites und URLs. Halten Sie riskante Webinhalte von Ihrer Umgebung fern, Web-Isolierungstechnologie ist ein wichtiger Schutz vor riskanten URLs. Außerdem können Sie auf diese Weise das private Surfverhalten sowie die Webmail-Services Ihrer Anwender isolieren.

Angriffe

Cyberangriffe lassen sich nicht vermeiden. Es ist jedoch möglich, sie mit den richtigen Ansätzen, Tools und Richtlinien unter Kontrolle zu bringen.

- Errichten Sie eine zuverlässige Abwehr zum Schutz vor E-Mail-Betrug. E-Mail-Betrug lässt sich häufig nur schwer erkennen. Investieren Sie daher in eine Lösung, die E-Mails basierend auf benutzerdefinierten Quarantäne- und Blockierungsrichtlinien verwaltet. Ihre Lösung sollte externe ebenso wie interne E-Mails analysieren, da Angreifer möglicherweise kompromittierte Konten missbrauchen, um Anwender in Ihrem Unternehmen zu täuschen.
- Schützen Sie Cloud-Konten vor Übernahmen und schädlichen Apps.
- Arbeiten Sie mit einem Anbieter für Bedrohungsdaten zusammen. Für kleinere, gezielte Angriffe benötigen Sie erweiterte Bedrohungsinformationen. Implementieren Sie eine Lösung, die mithilfe von statischen und dynamischen Techniken Angriffs-Tools, -Taktiken und -Ziele aufdeckt und daraus Erkenntnisse zieht.

Berechtigungen

Alle Cyberangreifer haben es auf Daten, Systeme und anderen Ressourcen abgesehen. Je mehr Berechtigungen das Opfer besitzt, desto umfangreicher die Zugriffsmöglichkeiten der Angreifer – und desto größer ist der potenzielle Schaden.

- Stellen Sie ein System zur Abwehr von Insider-Bedrohungen bereit, mit dem Sie böswillige, fahrlässige und kompromittierte Anwender verhindern, erkennen und kontrollieren können. Dies ist das häufigste Szenario für Berechtigungsmissbrauch, auf das möglichst in Echtzeit reagiert werden sollte.
- Nutzen Sie Tools für die schnelle Reaktion auf potenziellen Berechtigungsmissbrauch, mit denen Sie herausfinden können, was vor, während und nach dem Zwischenfall geschehen ist und welche Absichten der Anwender hatte – ohne die üblichen False Positives.
- Setzen Sie Sicherheitsrichtlinien durch und nutzen Sie dazu bei Bedarf Anwenderschulungen, Echtzeit-Erinnerungen und Blockierungen.

WEITERE INFORMATIONEN

Möchten Sie mehr darüber erfahren, wie Sie mit Proofpoint Einblicke in Ihre Schwachstellen sowie Ihre Risiken durch Angriffe und Anwenderberechtigungen erhalten und sie mit einer personenzentrierten Cybersicherheitsstrategie minimieren können? Dann besuchen Sie **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

0400-008-01-01 05/22