sosafe

Cybercrime-Trends 2023

Aktuelle Bedrohungen und wie Sie Ihre Organisation schützen

Inhalt

Cyberkriminelle liegen im Rennen um Innovationen vorne

Der technologische Fortschritt läuft auf Hochtouren. Das Gefährliche: So wird auch Cyberkriminalität immer verbreiteter – und leichter zugänglich. Umso wichtiger ist es heute, auf potenzielle Angriffe vorbereitet zu sein. Die Innovationskraft der Cyberkriminellen kennt keine Grenzen und dasselbe gilt für ihre Taktiken: von neuartigen Angriffen basierend auf künstlicher Intelligenz, über digitale Supply-Chain-Attacken und Ransomware-as-a-Service, bis hin zu Multi-Channel-Phishing. Wenn technische Sicherheitsmaßnahmen an diesen Trends scheitern, kommt es mehr denn je auf die Wachsamkeit der Mitarbeitenden und eine starke Sicherheitskultur an, um die Angriffe frühzeitig abwehren zu können.

Die beste Methode, um Sicherheitsrisiken zu minimieren, ist deshalb stets über die neuesten Angriffsmaschen informiert zu sein. Erfahren Sie mehr über die acht größten Cybercrime-Trends 2023 – inklusive nützlicher Praxistipps, wie Organisationen ihre Informationssicherheit steigern können.

01

Die Ära der Künstlichen Intelligenz: automatisierte Cybercrime-Innovationen

Künstliche Intelligenz (KI) ist für uns mittlerweile ein alltäglicher Begleiter. Doch auch Cyberkriminelle haben längst erkannt, dass sie diese Technologien für Social Engineering nutzen und ihre Gewinne so maximieren können.

Eine der ersten KI-basierten Methoden, die Cyberkriminelle bei ihren Vishing-Angriffen anwendeten, waren Deepfake-Technologien, insbesondere Voice Cloning. Dabei machten sie Mitarbeitende mithilfe von Stimmmanipulationen glauben, sie sprächen mit Mitgliedern ihres eigenen Teams. Schon 2019 nutzten Angreifende bei einem Angriff KI-Software, um den Vorstand eines deutschen Unternehmens zu imitieren. Mit dessen Stimme forderten sie beim CEO einer britischen Tochtergesellschaft telefonisch eine Überweisung in Höhe von 220.000 € an.[1] Kriminelle nutzen derartige KI-basierte Anrufe auch in Kombination mit anderen Methoden. Indem Angreifende ihre Opfer beispielsweise per Anruf über eine E-Mail informieren, die sie in Kürze erhalten werden, ziehen die Opfer aufgrund des vorherigen Anrufs nicht mehr in Betracht, dass es sich dabei um eine betrügerische oder sogar schadhafte Mail handeln könnte. So werden also deutlich weniger Phishing-Mails als Bedrohung identifiziert, was die Erfolgsquote der Cyberkriminellen gefährlich ansteigen lässt. Als wäre die Lage noch nicht gefährlich genug, kündigte Microsoft für dieses Jahr die Einführung von VALL-E an. Das neue Text-to-Speech-Modell soll schon mit einer dreisekündigen Sprachvorlage Stimmen perfekt imitieren – und wird damit die Bedrohungslage rund um Voice Cloning weiter intensivieren.[2]

Das Manipulieren von Stimmen ist jedoch nur eine Seite der Medaille. Auch gefälschtes Videomaterial nutzten Cyberkriminelle bereits zu ihrem Vorteil: Die inszenierte Kapitulation vonseiten des ukrainischen Präsidenten Selenskyj sorgte Anfang 2022 für großes Aufsehen und veranschaulichte nur zu deutlich, welche Wellen Deepfakes schlagen können.[3] Ebenso sorgte ein vermeintlicher Deepfake in Deutschland für Aufruhr, als Berlins Bürgermeisterin Franziska Giffey von Kiews Bürgermeister Vitali Klitschko per Videokonferenz über den Ukraine-Krieg kontaktiert wurde. Erst nach 15 Minuten in der Videokonferenz stellte sich heraus, dass es sich dabei vermutlich um einen sogenannten „Cheapfake" handelte, bei dem manipuliertes Audiomaterial über bereits existentes Videomaterial gelegt wurde. Doch auch dieser Angriff zeigte eindrucksvoll, wie Deepfakes zu gefährlicher Desinformation und Manipulation führen können.[4]

Da die Qualität der Deepfakes rasant zunimmt, ist dieses Jahr mit noch glaubwürdigeren und erfolgreicheren Social-Engineering-Angriffen dieser Art zu rechnen. Rechtsexpertinnen und -experten und Sicherheitsverantwortliche sind gleichermaßen besorgt, dass Deepfakes zu weiteren folgenschweren Zwecken missbraucht werden. So könnten sie die Glaubwürdigkeit von Überwachungsvideos, Body-Cams und anderem Beweismaterial abschwächen sowie für Cyberbullying, Erpressungen, Börsenmanipulation und zur Intensivierung der politischen Instabilität eingesetzt werden.[5]

Deepfakes und andere KI-basierte Methoden, wie automatisiertes Password-Guessing und CAPTCHA-Breaking, sind erst der Anfang einer neuen Cybercrime-Ära. Denn KI trägt dazu bei, dass Cyberattacken im Minutentakt ausgereifter und weitreichender werden, während manche Organisationen gerade erst damit beginnen, ihre Abwehr in diesem Bereich aufzubauen. Das beste Beispiel ist wohl die generative KI, mit der schädliche E-Mails erstellt werden können, die jeden Spamfilter durchbrechen.

In einer Studie fand ein Forschungsteam der Singapurer Government Technology Agency schon 2021 heraus, dass mithilfe von generativer KI überzeugende Spear-Phishing-Mails erstellt werden können. Auf die künstlich generierten Mails wurde dabei sogar häufiger geklickt als auf die vom Menschen erstellten Gegenstücke.[6] Das Tool, das bei dieser Studie genutzt wurde, war kein geringeres als die Vorgängerversion von ChatGPT, das inzwischen öffentlich zugänglich ist.

Die Veröffentlichung von ChatGPT Ende 2022 stellte Cybersicherheitsverantwortliche damit vor ganz neue Herausforderungen. Forschende befürchten, dass solche generativen KI-Lösungen zur Demokratisierung der Cyberkriminalität führen könnten – cyberkriminelle Taktiken durch diese Tools also der breiten Masse zugänglich gemacht werden.[7] Denn obwohl die Nutzungsrichtlinien es verbieten und versuchen es zu unterbinden, kann jede Person in nur wenigen Schritten mit ChatGPT schädlichen Code oder überzeugende Phishing-Mails erstellen – ohne technische Vorkenntnisse. Das Tool, das zurzeit noch frei zugänglich ist, soll außerdem in der Lage sein, ausgeklügelte polymorphe Malware zu erstellen, die traditionelle Sicherheitsmechanismen einfach umgeht.[8]

Auch Ransomware-Angriffe werden voraussichtlich häufiger zum Erfolg führen, wenn Hacker neue Schwachstellen und leichte Opfer dank künstlicher Intelligenz automatisiert und gezielt aufspüren können. Da KI in rasantem Tempo lernt, menschliches Verhalten realitätsnah zu imitieren, wird sie bald in der Lage sein, biometrische Systeme zu durchbrechen oder gar menschliche Verhaltensweisen zu imitieren. Das könnte zur Folge haben, dass gestohlene Accounts von Behavioral-Security-Systemen nicht mehr erkannt werden.[9]

Auch Sicherheitsexpertinnen und -experten profitieren natürlich von künstlicher Intelligenz, zum Beispiel beim Prüfen von Code oder bei der Threat Intelligence. Dennoch hat der technologische Fortschritt in diesem Bereich die Cyber-Bedrohungslage deutlich verschärft. Worauf es jetzt ankommt, ist, wer diese Technologie in Zukunft effektiver zu nutzen weiß: Sicherheitsteams oder Cyberkriminelle.

PRAXISTIPPS

Wie bei jeder neuartigen Betrugsmasche gilt auch hier: Der beste Schutz liegt in der Prävention. Sicherheitsteams sollten ihre technischen und organisatorischen Schutzmaßnahmen kontinuierlich hinterfragen und aktualisieren, um mit der Innovationskraft der Cyberkriminellen Schritt zu halten.

KI-basierte Threat Intelligence Tools und Risk Assessments sind eine Möglichkeit, das Risiko mithilfe technischer Lösungen bereits zu reduzieren.

Gleichzeitig gilt es, Mitarbeitende über aktuelle Angriffstaktiken aufzuklären, ihre Awareness dafür zu steigern und ihnen Tools bereitzustellen, die ihnen helfen, Angriffe zu erkennen, zu melden und abzuwehren.

Dasselbe gilt für Sicherheitsteams: Durch regelmäßige Trainings können sie Sicherheitsrisiken kontinuierlich reduzieren und schnell reagieren, sollte es trotz aller Schutzmaßnahmen zu einem Angriff kommen.

1 GameStar Tech (2019). Deepfake Voice: Betrüger imitieren Stimme eines CEO und erbeuten 243.000 US-Dollar.
2 ZDNet (2023). VALL-E: AI-Modell für Text-to-Speech von Microsoft simuliert Stimmen.
3 Golem (2022). Meta löscht gefälschtes Selenskyj-Video.
4 Deutschland sicher im Netz (2022). Deep oder Cheap Fake? - Franziska Giffey spricht mit falschem Vitali Klitschko.
5 Heise Online (2022). Europol: Deepfakes werden bei Kriminellen ein immer beliebteres Werkzeug.
6 Wired (2021). AI Wrote Better Phishing Emails Than Humans in a Recent Test.
7 ZDNet (2023). Wie ChatGPT Cyberkriminelle unterstützen kann.
8 ZDNet (2023). ChatGPT wird zum Schreiben von Malware eingesetzt.
9 BSI (2022). Deepfakes - Gefahren und Gegenmaßnahmen.

02

Dauerbrenner Phishing: weiterhin die bevorzugte Angriffsmethode

Cyberkriminelle werden auch 2023 auf die emotionale Manipulation ihrer Opfer setzen – mit dem Ziel, an vertrauliche Daten zu gelangen. Seit einigen Jahren spielen die Angreifenden immer gekonnter mit menschlichen Verhaltensmustern. Indem sie ein Gefühl von Vertrauen, Autorität, Knappheit oder Dringlichkeit bei ihren Opfern hervorrufen, verleiten sie sie dazu, auf schädliche Inhalte zu klicken und/oder sensible Daten preiszugeben.

Obwohl solche Social-Engineering-Taktiken, wie Business Email Compromise (BEC) oder Romance Scams, Kriminellen schon heute Milliardenbeträge einbringen, feilen sie weiterhin an ihren Methoden. Eine der neuesten Betrugsmaschen ist das sogenannte „Pig Butchering". Dabei werden Personen per Textnachricht, Social Media oder über eine Dating- oder Kommunikationsplattform kontaktiert. Falls das Opfer nach einer einfachen Begrüßung antwortet, versuchen die Scammer eine freundschaftliche Beziehung aufzubauen. Später versuchen sie ihr Opfer dann davon zu überzeugen, in Krypto zu investieren, indem sie über die hohen Geldsummen, die sie angeblich selbst durch Kryptowährung verdient haben, prahlen. Zu diesem Zweck setzen sie schädliche Online-Plattformen auf oder imitieren Plattformen legitimer Institutionen. Um das Vertrauen ihrer Opfer zu gewinnen, bieten sie ihnen sogar an, ihren vermeintlichen neuen „Freund" per Videoanruf kennenzulernen oder lassen einen kleineren Betrag von der jeweiligen Plattform als Rückversicherung einziehen. In San Francisco verlor 2022 ein 52-Jähriger eine Summe von 1 Million US-Dollar durch einen solchen Pig-Butchering-Scam, bei dem sich die Betrüger als ehemaliger Kollege ausgaben.[10] Die insgesamt 271.000 Wörter lange Unterhaltung zwischen Täter und Opfer verdeutlicht, wie weit Cyberkriminelle bei ihren Social-Engineering-Taktiken gehen, um ihr Ziel zu erreichen. 2023 ist damit zu rechnen, dass sie sich mit neuen Betrugsmaschen verstärkt die Sorgen der Menschen zur wirtschaftlichen und umweltpolitischen Lage zunutze machen.

In unserem beruflichen Alltag könnte sich ein solcher Angriff etwa als Fake-Profil auf LinkedIn bemerkbar machen oder auch als Einladung zu einem Zoom-Meeting von einem vermeintlichen Kollegen, als gefälschte E-Mail mit verborgener Malware oder als WhatsApp-Nachricht vom „internen IT-Manager", der um Zugriff auf interne Netzwerke bittet. Egal, über welchen Kanal der Angriff erfolgt – jede dieser Maschen stellt ein enormes Sicherheitsrisiko für Organisationen dar. Und alle genannten Szenarien sind echte Beispiele aus der Cybercrime-Landschaft, mit der wir uns heute im (Arbeits-)Alltag konfrontiert sehen. Erst kürzlich führte ein Social-Engineering-Angriff auf Anbieter von Marketingautomatisierungen Mailchimp zu einer Datenschutzverletzung – es war der zweite Angriff dieser Art, dem das Unternehmen in weniger als einem Jahr zum Opfer fiel. Dabei gelangten die Hacker durch Social-Engineering-Taktiken an die Anmeldedaten von Mailchimp-Mitarbeitenden, verschafften sich Zugang zu einem der Tools, die im Kundenkontakt genutzt wurden, und griffen auf diese Weise auf ausgewählte Mailchimp-Konten zu.[11] In einem anderen Fall organisierten die Betrüger sogar einen Zoom-Call mit ihrem Opfer, dem sie während des Calls über den Chat einen schädlichen Link schickten.[12]

Wie bereits aus dem vorherigen Trend deutlich wurde, haben generative KI-Lösungen wie ChatGPT, die menschliches Verhalten imitieren, das Potenzial, zu einem der mächtigsten Phishing- und Social-Engineering-Tools des Jahrhunderts zu werden. Während wir heute Phishing-Mails oft noch anhand von Rechtschreibfehlern oder anderen stilistischen oder formatbedingten Merkmalen erkennen können, wird das Erstellen fehlerfreier Betrugsmails in Zukunft immer einfacher. ChatGPT bietet Cyberkriminellen sogar die Möglichkeit, verschiedene Variationen gleichzeitig zu erstellen, indem sie dem Tool Anweisungen wie „E-Mail soll dringend aussehen“ oder „E-Mail mit hoher Wahrscheinlichkeit, dass auf den Link geklickt wird“ geben.[13]

Da bei 82 Prozent der Datenlecks der Faktor Mensch eine zentrale Rolle spielt, ist es unerlässlich, die aktuellen Trends sowie die Innovationen der Cyberkriminellen im Blick zu behalten. Nur so können sich Organisationen auf die beispiellose Anzahl an Social-Engineering-Angriffen vorbereiten, die uns 2023 über unsere E-Mail-Postfächer, Kommunikationstools und die sozialen Medien erreichen werden.

PRAXISTIPPS

Über die erforderlichen Sicherheitsmaßnahmen wie Firewalls und ETDR-Tools hinaus wird eine starke Sicherheitskultur für Organisationen immer bedeutender, um sich vor Phishing-Attacken zu schützen.

Sie sollten den Mitarbeitenden die Bedeutung von Informationssicherheit allgemein klar machen, aber auch über verschiedene Cyberangriffstaktiken und Meldewege bei verdächtigen Aktivitäten auf ihren Geräten aufklären – und sie gleichzeitig zur Einhaltung der entsprechenden Vorschriften motivieren.

Die gute Nachricht ist, dass es effektive Lösungen gibt, die Organisationen dabei unterstützen – von Awareness-Training und Lernplattformen bis hin zu Angriffssimulationen.

10 Forbes (2022). How One Man Lost $1 Million To A Crypto 'Super Scam' Called Pig Butchering.
11 Netzwoche (2023). Hacker stehlen Daten von über 100 Mailchimp-Kunden.
12 ZDNet (2023). Phishing attacks are getting scarily sophisticated. Here's what to watch out for.
13 CIO Magazine (2023). So erleichtert ChatGPT Hackern die Arbeit.

03

Geopolitische Krisen: globale Konflikte als Angriffsvorteil

Cyberkriminelle manipulieren die Gefühle ihrer Opfer ohne Skrupel und greifen in ihren trügerischen Nachrichten oft aktuelle Themen oder gesellschaftliche Entwicklungen auf. Anlassbezogene Phishing-Mails wecken oftmals Angst und Unsicherheit bei den Opfern, sodass sie eher auf schädliche Inhalte klicken oder sensible Daten preisgeben. Schon die Corona-Pandemie bot den Kriminellen optimale Ausgangschancen: Bereits wenige Wochen nachdem die COVID-19 Omicron-Variante weltweit bekannt wurde, griff ein großflächiger Phishing-Betrug in Großbritannien das Thema auf. Dabei wurde in Textnachrichten und E-Mails auf die Verfügbarkeit von COVID-Tests aufmerksam gemacht, um an persönliche Daten der Opfer zu gelangen. Sogar das Branding des National Health Service (NHS) wurde dabei verwendet.[14]

Selbst vor geopolitischen Krisen machen Cyberkriminelle keinen Halt. So sorgte beispielsweise der Angriffskrieg Russlands auf die Ukraine für einen beispiellosen Anstieg an Cybercrime-Aktivitäten, insbesondere auf Unternehmen in den direkt betroffenen Ländern, aber auch weltweit. So nahm eine russische Hackergruppe mehrere US-basierte NGOs, das Militär mehrerer osteuropäischer Länder sowie ein NATO Centre of Excellence ins Visier. Die Angreifenden wollten so vertrauliche Zugangsdaten für Spionagezwecke oder zum Verbreiten von Malware abgreifen.[15]

Doch das sind längst nicht die einzigen Ereignisse, die unsere Gesellschaft in den letzten Jahren erschütterten. Nach Jahrzehnten der fortschreitenden Globalisierung, steht die Welt heute vor einem neuen Megatrend: Deglobalisierung.

Während es 2008 bereits die ersten Anzeichen dafür gab, nahm diese Entwicklung in jüngster Zeit an Fahrt auf – angetrieben durch den strategischen Wettbewerb zwischen den USA und China, der sich in bilateralem Handel, Investitionsströmen und in der Technologie zeigte.[16] Während sich die Lage zwischen den Vereinigten Staaten und China durch Ereignisse wie die Corona-Pandemie und die Taiwan-Krise weiter anspannt[17], zeigt sich die steigende Unbeständigkeit bereits in instabilen Lieferketten, steigender Inflation, demografischem Wandel und sogar in einer Lebensmittel- und Energiekrise.

Angesichts dieser globalen Ereignisse sind Geopolitik und Cybersicherheit heute untrennbar miteinander verschweißt. Bei einer Reihe von DDoS-Angriffen im vergangenen Jahr wurden mehrere Webseiten offizieller Institutionen von Taiwan vom Netz genommen. Da die Angriffe im Zeitraum des Besuchs der US-Politikerin Nancy Pelosi stattfanden, wurden Bedenken über Chinas Beteiligung laut.[18] Doch Cyberkriminelle zielen mit ihren anlassbezogenen Betrugsmaschen nicht nur auf öffentliche Einrichtungen, sondern auch auf private Organisationen weltweit ab. In der zweiten Jahreshälfte 2021 geriet China ins Kreuzfeuer für eine Reihe von Cyberattacken, die auf Handelsgeheimnisse, Unternehmensdaten und Impfstudien abzielten.[19] Im Fokus dieser Attacken standen vor allem die USA, Großbritannien und andere globale Verbündete. Diese hatten zuvor der chinesischen Regierung vorgeworfen, an dem Hackerangriff auf Microsoft Exchange Server beteiligt gewesen zu sein.[20]

14 The Independent (2021). Scam warning over fake omicron testing text messages.
15 ZDNet (2022). Google: Multiple hacking groups are using the war in Ukraine as a lure in phishing attempts.
16 Deutschlandfunk (2023). Wie sich weltweite Handelsströme verändern könnten.
17 Reuters (2022). U.S.-China relationship bleeds by a thousand cuts.
18 Tagesspiegel (2022). Vor Besuch von Nancy Pelosi: Hacker legen Webseite der taiwanischen Präsidentin lahm.
19 Zeit Online (2021). USA und Verbündete werfen China "bösartige Cyberaktivitäten" vor.
20 Süddeutsche Zeitung (2021). Hacker unterwegs im Auftrag der Partei.

In Anbetracht der Tatsache, dass DDoS- und andere Cyberangriffe schon jetzt verstärkt Teil geopolitischer Proteste und Betrugsfälle sind, besteht kein Zweifel, dass Cyberkriminelle in Zukunft vermehrt auf besonders geschwächte Regionen und Branchen abzielen werden. Eines steht fest: Technologie und IT werden als politische Waffe instrumentalisiert. Öffentliche wie auch private Organisationen in Ländern mit angespannter geopolitischer Lage sollten das zum Anlass nehmen, eine holistische Sicherheitsstrategie einzuführen, um ihre Cyberrisiken zu reduzieren.

PRAXISTIPPS

Für Organisationen bzw. uns als Einzelpersonen liegen geopolitische Konflikte größtenteils außerhalb unseres Einflussbereichs.

Was wir jedoch tun können, ist uns auf neue Herausforderungen im Bereich Informationssicherheit vorzubereiten, um im Ernstfall effektiv auf sie reagieren zu können.

Während sich regulatorische Anforderungen verschärfen, gilt es für Organisationen, ihre Sicherheitsmaßnahmen zu stärken, ihr derzeitiges Setup zu überdenken und bestehende Schwachstellen zu schließen.

Angesichts der zunehmenden Vielfältigkeit und Häufigkeit von Cyberangriffen, hängt die Widerstandsfähigkeit von Organisationen maßgeblich davon ab, wie gut sie auf verschiedene Bedrohungsszenarien vorbereitet sind.

Dabei darf auch die Lieferkette nicht außer Acht gelassen werden. Es liegt im Interesse der Organisationen, ihre kritischen Prozesse zu bestimmen, die dafür erforderlichen Ressourcen zu identifizieren und einen Business-Continuity-Plan aufzustellen. So kann bei Ausfall eines Zulieferers die Fortsetzung des Geschäftsbetriebs sichergestellt werden.

Stets über die neuesten Entwicklungen der Bedrohungslage im Bilde zu sein und Incident-Response- und Recovery-Pläne kontinuierlich anzupassen, kann im Ernstfall den entscheidenden Unterschied machen.

Cybersicherheit ist längst politisch – Ansporn genug für Unternehmen, das Thema auf die Führungsebene zu bringen und ihm die Aufmerksamkeit und Ressourcen zukommen zu lassen, die es verdient.

INTERVIEW

„IT-Sicherheit ist eine Reise und ein Prozess – ein permanentes Anpassen“

Ulrich Irnich
CIO und Modernization Garage Director
Vodafone Deutschland

Ulrich Irnich gestaltet seit 2020 bei Vodafone als CIO die kundenzentrierte IT-Ausrichtung. Außerdem verantwortet er die globale Modernisation Garage, um die BSS-Modernisierung bei Vodafone voranzutreiben. Zuvor war er als CIO bei Unitymedia für die agile Transformation von IT und Business verantwortlich. Er transformierte das Unternehmen von einer projektorientierten zu einer produktzentrierten Organisation. Mit seiner umfassenden Erfahrung in der Telekommunikationsbranche bringt er tiefe Einblicke in das Geschäft und die digitale Transformation mit.

Jedes Unternehmen wird früher oder später von einem Cyberangriff getroffen. Darüber gesprochen wird aber noch recht wenig. Muss das Thema Ihrer Meinung nach normalisiert werden?

Ja. Aber leider gibt es noch wenig Offenheit dahingehend. Für Unternehmen hat das vermeintlich eher mit einem Schuldeingeständnis, Schwäche und Peinlichkeit zu tun. Dabei sind Hacktivisten in diesem Bereich sehr aktiv, damit alle aus den Erfahrungen lernen können. Wir haben zuletzt auf unserer Vodafone Elevation Tour versucht, Gespräche zu erfolgreichen Cyberangriffen anzukurbeln, aber die Reaktionen waren zunächst verhalten. Betroffene Unternehmen haben sich erst geöffnet, als auch Speaker auf der Bühne offen Angriffe thematisiert haben. Auch wir haben über den erfolgreichen Cyberangriff auf Vodafone Portugal gesprochen, der dieses Jahr durch die Medien gegangen ist, und unsere Learnings geteilt.

Die Angriffe, die wir zurzeit im Kontext geopolitischer Krisen und Kriege sehen, sind nur die Spitze des Eisbergs. Wie nehmen Sie das wahr?

Security-Vorfälle haben im Kontext des Krieges auf die Ukraine zugenommen – das stimmt. Aber es waren auch vorher schon immense Gefahren da, von denen viele nicht so viel mitbekommen haben. Wenn man schaut, welche Unternehmen beispielsweise von Ransomware-Angriffen getroffen werden, kann man sagen: Eigentlich jedes. Dieses Flächengeschäft steigt immer weiter an, weil die Geschäftsmodelle für Cyberkriminelle attraktiver werden.

Geht mit der zunehmenden Professionalisierung von Cyberkriminalität auch eine Veränderung der Angriffstaktiken einher?

Auch die Taktiken werden professioneller. Früher konnte man Phishing-Mails auf den ersten Blick erkennen. Mittlerweile gibt es zum einen komplexere Taktiken, aber auch mehr Kanäle und Daten, die für Angriffe genutzt werden können. Ein kompromittiertes Konto reicht beispielsweise aus, um auf verschiedensten Plattformen Schaden zu verursachen. Nichtsdestotrotz ist der größte Teil der Angriffe weiterhin ein standardisiertes Geschäft. Es werden erst einmal flächenmäßig kleinere „Bomben" abgeworfen, um zu verstehen: Wo lohnt es sich anzugreifen? Quasi als Return-On-Investment-Betrachtung vor dem eigentlichen Angriff.

Wo sehen Sie derzeit die größten Gefahren für Unternehmen?

Das sind zum einen wie schon erwähnt Ransomware-Angriffe. Aber auch Social Engineering und Brute-Force-Attacken, Advanced Persistent Threats und von innen kommende Angriffe.

Vodafone hat schon 2013 einen großen Ransomware-Angriff erlebt. Haben sich die Erpressungsmethoden seither verändert – sowohl bei Ihnen als Konzern als auch bei Ihren Geschäftskunden?

Das Gefährliche ist: Du kannst heute als Cyberkrimineller mit Kundendaten einen wesentlich höheren Return-On-Invest erzielen als noch vor wenigen Jahren. Die Daten werden auf dem Schwarzmarkt zu horrenden Summen gehandelt. Wir sehen bei unseren Geschäftskunden bei solchen Angriffen zwar weiterhin eine Dominanz einfacher Verschlüsselung von Daten.

Bei uns als Konzern aus der kritischen Infrastruktur (KRITIS) geht es den Angreifern aber vielmehr um die Kundendaten und was mit ihnen im Nachhinein passiert. Als KRITIS-Provider hast du ein höheres Vertrauensgut, das du verlieren kannst.

Wie geht man mit einem Ransomware-Angriff aus Ihrer Sicht am besten um? Zahlen oder nicht zahlen?

Das kommt drauf an. In vielen Fällen hat man keine Wahl. Linus Neumann, Hacker und IT-Security-Consultant bei Security Research Labs, hat einmal gesagt: „Kein Backup, kein Mitleid." Ein vernünftiger Incident-Response-Plan spielt also eine entscheidende Rolle. Mein direkter Reflex ist erstmal nicht zu zahlen und darauf zu setzen, im Ernstfall Daten wiederherstellen zu können. Neben Prevention, Detection und Forensik ist die Wiederherstellung einer der wesentlichen Schritte in der ganzen Kette. Was ich Geschäftsführern rate: Kenne deine geschäftskritischen Prozesse. Je schneller die nach einem Angriff wieder laufen, desto geringer das Risiko. Denn: Je mehr Fragezeichen da sind, desto länger dauert die Wiederherstellung. Und das kann nach ein paar Wochen für viele Unternehmen schon existenzbedrohend sein.

Haben Sie das Gefühl, dass aufgrund der aktuellen Bedrohungslage im C-Level mehr Interesse an Informationssicherheit da ist?

Wir führen regelmäßig mit unserem Executives Ransomware-Simulationen durch – mit allem, was für uns in Krisensituationen dazu gehört: Gespräche mit Geschäftspartnern, Verhandlungen, Presse. Sobald man so eine Krisensituation simuliert, gibt das einen Stressmoment und der sorgt dafür, dass die Führungskräfte eine andere Einstellung zum Thema bekommen. Es hilft also ungemein, immer wieder zu sensibilisieren.

Die Kontinuität ist dabei entscheidend. Denn, wenn alles funktioniert und die Awareness nicht mehr so präsent ist, weil es keine Vorfälle gibt – dann ist das genau der Moment, in dem Kriminelle zuschlagen. Sie warten nur auf solche Schwachstellen.

Die Frage ist schon längst nicht mehr, ob du als Unternehmen gehackt wirst, sondern wann – und eben, wie gut du vorbereitet bist. Man muss von Anfang an verstehen, welche Risiken, auch Haftungsrisiken für die Geschäftsführung, mit einem Angriff einhergehen.

Und besonders wichtig: Auch klarzumachen, dass es nicht alleinige Aufgabe der IT Security ist, das Unternehmen zu schützen. Sicherheit ist ein Gemeinschaftsprodukt.

Welche Metriken nutzen Sie denn, um die Relevanz von Informationssicherheit in der Führungsebene als Thema zu platzieren?

Was sehr deutlich verstanden wird, sind die Gefahren beziehungsweise Konsequenzen von Angriffen und das Risikoprofil des Unternehmens. Wir gehen unsere Top-Risiken jährlich durch und bewerten diese gemeinsam. Risiken verstehen Geschäftsleute immer – das übersetzt sich ja auch in monetären Schaden. Die Hauptfragen sind dabei: Wie groß ist das Schadenspotenzial und wie wahrscheinlich ist der Ernstfall?

Bei beidem steht Cyber ganz oben auf der Liste. Das größte technische Risiko für die weltweite Wirtschaft ist zurzeit Cybercrime.

Security braucht Investments. Aber: Wenn die Maßnahmen erfolgreich sind, gibt es keinen sichtbaren Benefit. Sind die Budgets mit der Erkenntnis, dass Cyberkriminalität das Top-Risiko schlechthin ist, größer geworden?

Bei uns ist IT Security längst nicht mehr diskutabel – wir haben da schon eine signifikante Größe erreicht, auch aufgrund unseres Reifegrades. Als KRITIS-Provider sind wir da in der Pflicht.

Wie sieht das bei Ihren Geschäftskunden aus?

Bei den Unternehmen, die selbst Attacken erlebt haben, ist das Thema natürlich sehr viel präsenter. Gerade, wenn man sich den Mittelstand anschaut, gibt es aber noch viel an Awareness zu tun.

Früher wurde immer von der „Schwachstelle" Mensch gesprochen. Das ist aus Sicht der Psychologie nicht besonders motivierend. Was sind Ihre Erkenntnisse in Bezug auf den Aufbau einer Sicherheitskultur?

Erst einmal sollte man das rhetorisch umdrehen. Der Mensch ist nicht die größte Schwachstelle, sondern das größte Asset, das wir in der Informationssicherheit haben.

Und dann ist es vor allem wichtig, Wissen zu teilen und darüber zu sprechen, damit man gemeinsam Lernerfahrungen machen kann.

Wie ist das bei Vodafone? Wie wird der Faktor Mensch dort in der Informationssicherheit gesehen?

Für uns bei Vodafone ist es wichtig, die Menschen achtsam und resilient zu machen. Jemand, der mental stark ist, kann Negatives gut abwehren. Wir versuchen also das Positive zu fördern. Das gilt nicht nur für Cyber.

> „Wir haben verschiedene Ebenen in unserer Verteidigungsstrategie – und jeder Mitarbeiter ist Teil davon."

Außerdem haben wir verschiedene "lines of defense" - also verschiedene Ebenen in unserer Verteidigungsstrategie – und jeder Mitarbeiter ist Teil davon. Dazu zählen einerseits Pflichttrainings. Unseren Reifegrad messen wir mit einer Cyber Security Baseline. Unternehmensweit gibt es verschiedene Kontrollpunkte, die wir überprüfen und auf einer Skala beurteilen. Das ist Arbeit und fühlt sich manchmal etwas hart an. Die Leute beschweren sich, ständig etwas machen zu müssen. Die Beschwerden werden aber relativ schnell über die Konsequenzen von potenziellen Angriffen abgemindert.

Wie schaffen Sie es, die Awareness unter den Mitarbeitenden langfristig aufrecht zu erhalten?

Das ist tatsächlich ein Thema, auf das wir uns konzentrieren. Oft werden wir als zu "mature", der Reifegrad unserer Sicherheitskultur als zu hoch angesehen und das führt zu Nachlässigkeit im Arbeitsalltag. Wir bekommen gerade bei Awareness-Trainings oft Fragen: Was ist, wenn ich gut bin? Warum muss ich gut bleiben? Können wir nicht ein paar Schrauben losdrehen?

Aber gerade Infiltrierungen und Social-Engineering-Angriffe sind ja eine der Hauptgefahrenzonen. Das muss also langfristig verankert werden.

Welche Trends sehen Sie auf uns zukommen?

Wir sind in einem glorreichen Zeitalter, wo sich verschiedenste Ströme kreuzen und potenzieren: Unendliche Bandbreiten, Rechenleistungen für sehr wenig Geld, Daten, die explodieren. Da tun sich wahnsinnige Möglichkeiten auf.

Wenn man sich das Metaverse anschaut: Wie stellt man bei Avataren sicher, dass es sich um echte Partner handelt? Hier sei nur das Stichwort Deepfake einmal erwähnt. Die digitale Identität wird ein großes Thema werden.

Nächstes Thema ist die Blockchain. Technologieseitig werden wir nochmal einen Entwicklungsschritt machen müssen – die Prozesse sind derzeit noch zu rechenintensiv.

Außerdem werden neue Geschäftsmodelle im Metaverse entstehen. Zahlungswege werden sich verändern: NFTs, Krypto, … – konventionelle Banken wird das zum Wanken bringen.

Man kann sagen: Der Zusammenschluss aus digitaler und analoger Welt wird mehr Einfluss nehmen und die Angriffsflächen werden größer, denn die Geschäftsmodelle für digitale Angreifer multiplizieren sich somit.

Wir haben schon 2018 vor Deepfake-Taktiken wie Voice Cloning gewarnt. Wie schätzen Sie das Gefahrenpotenzial von Künstlicher Intelligenz ein?

Natürlich werden sich daraus neue Gefahren entwickeln. Wenn du dein Wissen mithilfe von Technologie systematisierst, kannst du es als Waffe nutzen. Technologie bietet viel – aber eben auch viel auf der dunklen Seite. Dass wir zurzeit trotz neuer Tools wie ChatGPT noch nicht viele KI-erstellte Phishing-Mails in der „freien Wildbahn" entdecken, hat eher damit zu tun, dass die Tore auch ohne diese Technologie noch zu einfach zu öffnen sind. Aber da gerade alle Instanzen dabei sind, Sicherheitsstufen zu erhöhen, wird das mit Sicherheit früher oder später kommen. IT-Sicherheit ist eine Reise und ein Prozess – ein permanentes Anpassen. Auch an solche neuen Technologien.

Wie kann man die Mitarbeitenden denn konkret dabei unterstützen?

Wir haben beispielsweise einen Button in unser E-Mail-Programm integriert, damit sie verdächtige Nachrichten direkt melden können. Und natürlich haben wir auch technische Vorkehrungen getroffen, damit im Fall der Fälle möglichst wenig schiefgehen kann.

Gleichzeitig feiern wir gemeinsam Erfolge und verleihen Spirit-Awards: Das sind Personen, die uns als Organisation sicherer machen. Unser Rezept ist also, Stärken zu stärken. Abstrafungen wirken nur kurzfristig. Heute geht es um Engagement – darum, dass die Leute auch wirklich mitmachen und mitwirken möchten.

Als Abschluss: Was sehen Sie in den nächsten 12 Monaten auf uns zukommen?

Fangen wir mit dem Positiven an: Viele neue Möglichkeiten in der digitalen Welt, mit denen wir auch globale Fragen lösen können. Neue Ansätze zum Beispiel zur Bekämpfung des Klimawandels.

Auf der negativen Seite sehe ich aber, dass die Intensität von Attacken und deren Schaden zunehmen. Darauf müssen wir uns einstellen – und die Menschen aktiv darauf vorbereiten.

> Der Mensch ist in der IT-Sicherheit nicht die größte Schwachstelle, sondern das größte Asset.“

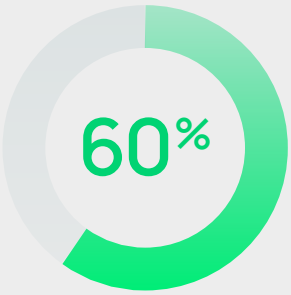
04

Burnout in Security-Teams: Cyberkriminelle hatten es nie leichter

Unmotivierte Mitarbeitende wirken sich zweifellos negativ auf die Gesamtproduktivität eines Unternehmens aus. Derzeit gibt es jedoch ein noch größeres Problem, das Unternehmen anfälliger für Cyberangriffe machen könnte: die zunehmende Erschöpfung bei Mitarbeitenden insbesondere bei IT- und Security-Expertinnen und -Experten.

Noch nie waren Sicherheitsverantwortliche so starkem Stress wie heute ausgesetzt – in einer Zeit, in der sich die Cyber-Bedrohungslage immer weiter zuspitzt. In den vergangenen Jahren standen Security-Teams durch die COVID-Pandemie, die geopolitische Lage und Remote Work verstärkt unter Druck. Durch hybrides Arbeiten öffneten sich neue Sicherheitslücken, die sich Hacker zielsicher zunutze machten: ungesicherte Verbindungen, die Nutzung privater Geräte für die Arbeit und der vermehrte Gebrauch von Kollaborationstools wie Microsoft Teams und Slack. Im Kampf gegen die Bedrohung nahmen die Expertinnen und Experten eine extrem hohe Arbeitsbelastung in Kauf: Laut dem Chartered Institute of Information Security (CIISEC) arbeiteten 12 Prozent der Mitarbeitenden zwischen 51 und 70 Stunden pro Woche.[21]

Als Folge treiben Erschöpfung und Burnout viele Sicherheitsbeauftragte bis zur Kündigung. Eine Studie der Information Systems Audit and Control Association (ISACA) ergab, dass 2022 60 Prozent der Organisationen damit zu kämpfen hatten, qualifiziertes Cybersicherheitspersonal in ihren Teams zu halten. Extremer Stress bei der Arbeit war einer der fünf häufigsten Gründe für ihre Kündigung.[22] Der Mangel an Arbeitskräften in der Security-Branche generell, der sich auf 3,5 Millionen Personen beläuft, macht die Lage nicht besser – ganz im Gegenteil.[23] Das Ergebnis sind unterbesetzte Informationssicherheitsteams, die nur schwer mit dem Anstieg an Cyberangriffen mithalten können.



der Organisationen hatten 2022 Schwierigkeiten qualifiziertes Cybersicherheits-personal zu halten

In Anbetracht der aktuellen Bedrohungslage ist es somit von enormer Wichtigkeit, den Sicherheitsteams die nötigen Ressourcen und Budgets zuzuweisen. Aus dem Bericht des CIISEC ging zudem hervor, dass 2021 lediglich 64 Prozent der Organisationen ihr Budget für Sicherheitsbelange erhöhten – während 17 Prozent es nicht erhöhten und 9 Prozent es sogar reduzierten. Von den Organisationen, die ihr Budget erhöhten, wiesen jedoch nur 9 Prozent ausreichende Mittel zu, um dem beispiellosen Ausmaß an Bedrohungen die Stirn zu bieten. Der Vergleich zu den Vorjahren zeigt, dass auch die Anzahl der Unternehmen, die ihr Budget ausreichend erhöhten, sich verringerte. Kurz gesagt: Viele Organisationen stehen der zugespitzten Cyber-Bedrohungslage ohne die nötigen Ressourcen gegenüber.

Stress, fehlende Motivation und unzureichende Budgets bilden die optimalen Voraussetzungen für Cyberkriminelle. Sie nutzen die Erschöpfung der Sicherheitsverantwortlichen zu ihrem Vorteil. Denn in dieser Situation übersehen diese leichter kleine Details und können Probleme weniger effizient lösen.[24] Außerdem übersehen überlastete Mitarbeitende eher die Anzeichen eines Angriffs oder machen sogar Fehler, die Schwachstellen für Hacker schaffen, zum Beispiel, wenn sie es versäumen, Software zu aktualisieren.[25] Auch Cyberkriminelle sind sich dieser Schwächen bewusst und greifen gezielt Organisationen an, deren Sicherheitsteam eher schwach aufgestellt ist.

PRAXISTIPPS

Unternehmen sollten die Erschöpfung ihrer Security-Teams unbedingt ernstnehmen, denn andernfalls können Cyberkriminelle diese zu ihrem Vorteil ausnutzen.

Erschöpfung und Antriebslosigkeit können langfristig mit den richtigen Maßnahmen überwunden werden: durch entsprechende Budgets, Karrierepläne zur Bindung der Mitarbeitenden und indem unterbesetzte Teams und Überstunden vermieden werden.

Viele Sicherheitsteams empfinden es darüber hinaus als zusätzliche Belastung, dass sie innerhalb der Organisation als eine Art Störfaktor empfunden werden, der Prozesse verlangsamt – zum Beispiel indem sie die Rechte für Softwaredownloads der Mitarbeitenden auf ihren Arbeitsgeräten einschränken. Es sollte deshalb das Anliegen und Ziel der obersten Führungsebene sein, klar zu kommunizieren, wie wichtig die Arbeit des Security-Teams sowie kontinuierliches Awareness-Training für die Sicherheit der Organisation sind.

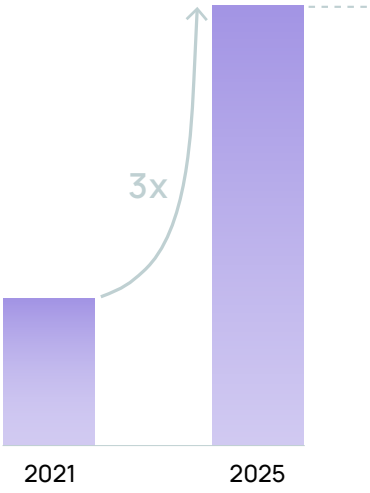
Es ist höchste Zeit, in die Ausbildung und das Training der Cybersicherheitsexpertinnen und -experten von morgen zu investieren. Denn sie sind es, die in einer immer komplexeren Bedrohungslage für unsere Sicherheit sorgen werden.

21 Chartered Institute of Information Security (2022). The security profession 2021/2022.
22 ISACA (2022). State of cybersecurity 2022: cyber workforce challenges.
23 t3n (2022). Sicherheitsexperten: IT-Fachkräftemangel führt künftig zu schweren Cyberangriffen.
24 Security Magazine (2023). One of the biggest threats of a cybersecurity team? Employee burnout.
25 Bleeping Computer (2023). IT Burnout may be Putting Your Organization at Risk.

05

Digitale Supply-Chain-Attacken: wir sind alle voneinander abhängig

Der erschütternde Anstieg von Lieferkettenangriffen 2022 war lediglich ein Vorbote für das, was uns 2023 bevorsteht. Denn dieser Trend wird neue Ausmaße annehmen und sich insbesondere auf digitale Lieferketten auswirken. Laut Gartner werden bis 2025 45 Prozent aller Organisationen weltweit Angriffe auf ihre digitale Lieferkette erlitten haben – dreimal so viele Organisationen wie noch 2021.[26]



45%

aller Organisationen werden bis 2025 Angriffe auf ihre digitale Lieferkette erlitten haben

Die Ereignisse der vergangenen zwei Jahre haben uns schonungslos vor Augen geführt, wie sehr unsere eigene Sicherheit auch von den Maßnahmen anderer abhängt. Cyberkriminelle erhöhen ihre Erfolgschancen über das Partner- und Lieferantennetzwerk ihrer Opfer, aber auch über Open-Source-Technologien. Indem sie eine einzige Sicherheitslücke in der Lieferkette ausnutzen, infiltrieren sie die Systeme oder infizieren unter Umständen das gesamte Netzwerk mit Schadsoftware.

Besonders eindrücklich zeigte dies der Cyberangriff auf FourB S.p.A., einen Partner von Vodafone. Bei der resultierenden Datenschutzverletzung wurden sensible Daten und Kontaktinformationen von tausenden Kunden freigegeben.[27]

Der Zwischenfall bei Vodafone ist aber kein Einzelfall und auch 2023 kam es bereits zu den ersten Datenlecks, die auf Schwachstellen in Partnernetzwerken zurückzuführen waren. So gab Nissan North America im Januar bekannt, dass es bei einem ihrer Softwareentwickler zu einer Datenschutzverletzung kam, bei der vollständige Namen und Geburtsdaten von tausenden Nissan-Kunden gestohlen wurden.[28]

Da diese Attacken nicht nur einzelne Unternehmen, sondern die gesamte Lieferkette ins Visier nehmen, sind neben größeren Organisationen wie Vodafone oder Nissan gleichzeitig auch lokale Unternehmen mit geringeren Ressourcen betroffen, die sich nur schwer von einem solchen Angriff erholen. Erst kürzlich musste Royal Mail, der nationale Postdienst des Vereinigten Königreichs, seinen internationalen Exportdienst aufgrund eines Ransomware-Angriffs vorübergehend einstellen. Dadurch wurden internationale Lieferungen um mehrere Tage verzögert, was für viele Kleinunternehmende erhebliche finanzielle Verluste bedeutete.[29]

Open-Source-Software gehört ebenfalls zu einem der Hauptziele von Hackern, was die Plattform Codecov bereits am eigenen Leib erfahren musste. Über eine Schwachstelle in der Docker-Bilderstellung von Codecov verschafften sich Hacker Zugriff auf Kundendaten.[30] Auch die im Dezember 2021 aufgedeckte Log4j-Schwachstelle zeigt deutlich, welche weitreichenden Wellen solche Vorfälle schlagen können. Schätzungen zufolge wurde Log4j in etwa 36.000 Programmen verwendet – die Log4j-Sicherheitslücke wird also so lange Folgen nach sich ziehen, bis alle Anwendungen ausnahmslos aktualisiert wurden.[31]

Diese Entwicklungen bilden in Kombination mit unterbesetzten Security-Teams den perfekten Nährboden für Cyberkriminelle. Und die Angriffsfläche vergrößert sich weiter, da viele Organisationen ihre Sicherheitsbelange auslagern müssen. Letztlich bringt die Nutzung von (Sicherheits-)Software immer ein gewisses Risiko mit sich, wie der Incident bei LastPass im August 2022 zeigte.[32] Da die Nutzung aber auch viele Vorteile mit sich bringt und/oder in bestimmten Fällen aufgrund der allgemeinen Situation sogar unumgänglich ist, liegt es nun bei Organisationen, ihre Sicherheitsstrategie zu stärken, um der komplexen Softwarelandschaft gerecht zu werden.

PRAXISTIPPS

Bevor Unternehmen neue Geschäftsbeziehungen mit Dienstleistern oder Zulieferern eingehen, sollten sie sich zur Reduzierung ihres eigenen Risikos gründlich über deren Sicherheitslevel und Compliance informieren.

Dazu bietet es sich beispielsweise an, (Software-)Zertifizierungen oder die Erfüllung von Regularien wie der EU-DSGVO und anderen Normen wie der ISO/IEC 27001 zu überprüfen und sicherzustellen. Unabhängige Bewertungen und Audits des potenziellen Partnerunternehmens sowie seiner Kunden, aber auch der Blick auf aktuelle Zwischenfälle können weiteren Aufschluss über die Eignung als Partner bieten.

Für ein sicheres Partnernetzwerk ist es im nächsten Schritt ratsam, sich auf die Rechte der Zulieferer bzw. Dienstleister sowie auf Reaktions- und Meldepläne im Falle eines Angriffs zu einigen.

Des Weiteren kann der Remote-Zugriff überwacht, eingeschränkt oder durch zusätzliche Schutzstufen wie Multifaktor-Authentifizierung gestärkt werden.

Entscheidend ist die regelmäßige Überprüfung der Prozesse: Sind die Partner sicherheitstechnisch gut aufgestellt? Gab es Veränderungen in der Geschäftsbeziehung, die sich auf die Sicherheit auswirken? Letztendlich ist Ihre eigene Sicherheitskultur nur so stark wie die Ihrer Partner und Zulieferer.

26 Gartner (2022). Gartner Identifies Top Security and Risk Management Trends for 2022.
27 Bleeping Computer (2022). Vodafone Italy discloses data breach after reseller hacked.
28 Cybernews (2023). Nissan data breach exposed clients' full names and dates of birth.
29 DER SPIEGEL Netzwelt (2023). Britische Post kämpft nach Hackerangriff mit massiven Problemen.
30 Inside IT (2021). Codecov-Breach: So schlimm wie Solarwinds?
31 IT Daily (2022). Die Log4j-Sicherheitslücke und der Umgang mit den Folgen.
32 IT Daily (2023). Der LastPass-Vorfall: Bequemlichkeit versus Sicherheit.

06

Ransomware-as-a-Service: Online-Erpressung per Knopfdruck

Schon seit Ende der 1980er-Jahre gehören Erpressungssoftware und Verschlüsselungstrojaner zu den häufigsten Cyber-Angriffstaktiken, gleichermaßen gefürchtet von Unternehmen wie auch von Privatpersonen. In den vergangenen Jahren professionalisierte sich die Methode weiter: Mit einem beispiellosen Anstieg von Ransomware-as-a-Service (RaaS) diversifizieren Cyberkriminelle nun ihr Geschäftsmodell.

Um einen Ransomware-Angriff durchzuführen, brauchen Angreifende heutzutage keine IT- oder Hacking-Kenntnisse mehr – eine kurze Suche im Darkweb und eine schnelle Kryptozahlung reichen aus. Die Geschäftsstruktur von RaaS ist ähnlich zu gewöhnlichen Software-as-a-Service-Anbietern. Oft bieten die Gruppen Abonnementmodelle und sogar einen Kundendienst (wie die Conti-Leaks eindrucksvoll veranschaulichten[33]) und ermöglichen somit jeder beliebigen Person, Ransomware-Angriffe im großen Stil auszuführen. Damit hat sich die Anzahl der möglichen Cyberkriminellen um ein Vielfaches multipliziert.

Die Folgen sind gleichermaßen beeindruckend wie auch angsteinflößend: Zwischen 2021 und 2022 hat die Menge an Ransomware um 13 Prozent zugenommen – mehr als in den vorherigen fünf Jahren insgesamt.[34] 2022 wurden 71 Prozent aller Organisationen Opfer eines Ransomware-Angriffs.[35] Das zerstörerische Ausmaß für die Wirtschaft macht eine neue IBM-Studie deutlich, laut der ein erfolgreicher Ransomware-Angriff Unternehmen durchschnittlich 4,54 Millionen US-Dollar kostet – das Lösegeld selbst noch nicht einberechnet.[36]

4,54 Millionen

US-dollar kostet Unternehmen ein erfolgreicher Ransomware-Angriff durchschnittlich – das Lösegeld nicht einberechnet

Organisationen weltweit wurden bereits zur Zielscheibe von RaaS-basierten Angriffen. Die Folgen veranschaulicht beispielsweise der Angriff der Ransomware-Gruppe DarkSide auf Colonial Pipeline im Jahr 2021[37], der zu einer wochenlangen Versorgungsunterbrechung mit Benzin an der US-amerikanischen Ostküste führte. Später stellte sich heraus, dass ein unsicheres Passwort und fehlende Multifaktor-Authentifizierung den Cyberkriminellen Zugriff auf zahlreiche interne Systeme und Daten ermöglicht hatten.[38]

Auch die Gruppe REvil führte viele ihrer Angriffe mittels eines RaaS-Modells durch. Von ihrer Supply-Chain-Attacke auf den Softwareanbieter Kaseya waren 2021 tausende von Unternehmen betroffen. Für Schlagzeilen sorgten auch die Cyberangriff durch REvil auf den US-Versicherer CNA Financial und den brasilianischen Fleischproduzenten JBS, die mit 40 Millionen US-Dollar und 11 Millionen US-Dollar zwei der bislang höchsten bekannten Lösegeldsummen zahlten. Die Hackergruppe REvil wurde zwar Anfang 2022 zerschlagen. Es wird jedoch vermutet, dass sie bereits unter anderen Namen wieder aktiv ist.[39]

Der neue Hauptakteur im RaaS-Geschäft ist wohl LockBit. Im Sommer 2022 geriet der Autoteilezulieferer Continental ins Visier der Gruppierung. Neben einer Lösegeldforderung stahl und verschlüsselte LockBit sensible Daten und bot diese im Darknet zu einem Preis von rund 50 Millionen US-Dollar an, nachdem das Unternehmen die Zahlung verweigert hatte. Diese Art von Mehrfacherpressung wird bei RaaS-Angriffen immer häufiger und zwingt viele Organisationen aufgrund mangelnder Alternativen letztendlich zur Zahlung des Lösegelds. Zur gleichen Zeit sorgte die LockBit-Gruppe für Aufsehen, als sie mit dem Aufruf „Make ransomware great again!" ein Bug-Bounty-Programm in ihrer Cyber-Community auflegte. Durch das Anpreisen von Belohnungen lagerten sie die Suche nach Schwachstellen bei ihren Opfern effektiv aus und vervielfachten so ihre Erfolgschancen.[40]

Mit großmaschigen Angriffen per Tastendruck, dem Boom von Mehrfacherpressungen und der steigenden Vernetzung von Lieferketten, ist Ransomware eine extrem profitable Spielwiese für Cyberkriminelle weltweit. Jetzt ist der richtige Zeitpunkt für Organisationen, in ihre Sicherheit zu investieren, denn die jüngsten Entwicklungen sind scheinbar erst der Anfang einer regelrechten Ransomware-Epidemie.

PRAXISTIPPS

Ransomware-Angriffe zu vermeiden ist ein Großprojekt. Es scheint nahezu sicher, dass jede Organisation früher oder später ins Visier der Cyberkriminellen gerät. Aus diesem Grund sollten sich Sicherheitsmaßnahmen nicht nur auf die Vorbeugung, sondern auch auf die Eindämmung der Folgen bei einem Angriff fokussieren.

Als ersten Schritt sollten Organisationen ihre Software regelmäßig aktualisieren, Schwachstellen mittels Patches schließen und sicherstellen, dass zuverlässige Endpoint-Protection- sowie Threat-Detection-Tools im Einsatz sind.

Die sparsame Vergabe von Admin-Rechten, die Überprüfung und Implementierung effektiver Passwortrichtlinien und wirksames Access Management auf Serverlevel: Diese Strategien können das Ausmaß eines Angriffs eindämmen, da sie Angreifende davon abhalten, Ransomware in gesamte Systeme einzuschleusen.

Da viele der Angriffe mit einer Form von Social Engineering beginnen, kann auch Awareness-Training das Risiko für Ransomware-Vorfälle effektiv reduzieren.

Die beste Methode, sich vor der Zahlung des Lösegelds zu schützen, sind regelmäßige Back-ups der Daten und ein Incident Response Plan, der im Falle eines Angriffs schnelles Handeln ermöglicht.

33 ZDNet (2022). Conti-Ransomware zielt auf Europa.
34 Verizon (2022). 2022 Data Breach Investigations Report.
35 Statista (2022). Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2022.
36 IBM (2022). Kosten eines Datenschutzverstoßes 2022.
37 Datensicherheit (2021). Ransomware-Angriff: Kraftstoffversorgung über Colonial Pipeline unterbrochen.
38 Security Insider (2022). Ransomware früh erkennen und stoppen.
39 CSO Online (2022). Ist REvil zurück?
40 Golem (2022). Ransomware-Gruppe startet Bug-Bounty-Programm.

07

Multi-Channel-Phishing: E-Mail-Sicherheit ist nicht mehr genug

Die Zeiten, in denen E-Mail der einzige Kanal war, über den Hacker versuchten, unsere persönlichen (Anmelde-)Daten abzugreifen und größere Datenlecks auszulösen, sind vorbei. Mit der neuen Vielschichtigkeit der Phishing-Angriffe nutzen Cyberkriminelle auch immer neue Plattformen, über die sie an sensible Daten von Privatpersonen und Unternehmen gelangen – oft greifen sie sogar über mehrere Plattformen gleichzeitig an.

Ein wichtiger Kanal sind dabei die sozialen Medien, was die kürzliche Malware-Angriffswelle über die „Invisible Body"-Challenge auf TikTok bestätigte. Bei der Challenge wurden User dazu aufgefordert, nackt zu posieren, während ein Filter den Körper der Person unsichtbar machte. Hacker sahen ihre Chance, die Neugierde der Menschen auszunutzen, und boten Software an, die die Körper wieder sichtbar machen sollte. Über einen Discord-Server teilten sie Links zu einer Malware namens WASP Stealer an die interessierten User. Auf diese Weise gelangten sie an sensible Daten, wie Passwörter und Kreditkartendaten tausender Menschen.[41]

Solche Taktiken wenden Cyberkriminelle nicht nur in Apps wie Telegram oder Discord an, sondern auch auf professionelleren Plattformen, wie LinkedIn, Slack und Microsoft Teams. Durch Remote Work ist die Grenze zwischen der privaten und beruflichen Nutzung von Geräten immer mehr verschwommen. Umso einfacher wird es für Eindringlinge, über diese Kanäle an Unternehmenslogins und andere sensible Daten zu gelangen. Ein aktuelles Beispiel dafür ist der Angriff auf Uber, bei dem einer der Mitarbeitenden dazu gebracht wurde, eine Multifaktor-Authentifizierung durchzuführen.

Über WhatsApp gaben sich die Hacker als Kolleginnen und Kollegen aus der IT-Abteilung aus und forderten ihr Opfer auf, ihnen Zugriff auf interne Netzwerke zu gewähren.[42]

Auch auf LinkedIn versuchten Cyberkriminelle zuletzt, Mitarbeitende – aber vor allem auch Jobsuchende – hinters Licht zu führen. Sie brachten sie dazu, auf Phishing-Mails zu klicken oder boten ihnen Stellenausschreibungen im Austausch gegen eine Vorabzahlung oder ihre Bankdaten.[43] Darüber hinaus ist LinkedIn das ideale Netzwerk, um Informationen für Spear-Phishing-Attacken zu sammeln. Angreifende können über die Neueinstellungen eines Unternehmens erfahren und sich den neuen Mitarbeitenden gegenüber als Vorgesetzte ausgeben. So bringen sie sie dazu, auf Links zu klicken und ihre Login-Daten auf gefakten Webseiten einzugeben.[44]

Auch andere professionelle Plattformen machen sich Hacker zunutze. Der Videospieleentwickler Rockstar Games wurde Opfer eines Angriffs, bei dem Bildmaterial der frühen Entwicklungsstufen des Videospiels Grand Theft Auto 6 (GTA6) an die Öffentlichkeit geriet. Dabei drangen die Hacker in den Slack-Kanal des Unternehmens ein und erlangten so Zugriff auf große Mengen an Aufnahmen und andere Informationen, darunter auch der Quellcode von GTA5 und GTA6. Als sie 90 Videos mit etwa 50 Minuten Filmmaterial veröffentlichten, drohten sie gleichzeitig, auch den Quellcode öffentlich zugänglich zu machen, wenn Rockstar nicht eine beachtliche Summe Geld zahlen würde.[45]

41 Bitdefender (2022). Angreifer missbrauchen TikTok-Challenge, um Nutzerdaten zu erbeuten.
42 Infopoint Security (2022). Ransomware-Attacken auf Uber und Rockstar – ist MFA nicht sicher genug?
43 Netzwoche (2022). Betrüger missbrauchen fürs Phishing am häufigsten das Linkedin-Logo.
44 ZDNet (2022). Phishing-Betrug per LinkedIn nimmt seit Anfang Februar um 232 Prozent zu.
45 Gamestar (2022). GTA 6: Der Hacker soll angeblich erst 16 und kein Unbekannter sein.
46 IT Daily (2020). Betrugsfälle bei Browser-Benachrichtigungen werden immer populärer.

Phishing lauert uns heute also nahezu überall auf – selbst in scheinbar harmlosen Browser-Benachrichtigungen. Skrupellosen Tätern können sie als Zugangspunkt zu unseren Geräten dienen oder auch als Werkzeug, um an Anmeldedaten und sensible Informationen zu gelangen. Ein Beispiel sind Browser-Benachrichtigungen, die Nutzende vor einem angeblichen Virus auf ihrem Computer warnen und sie auffordern, darauf zu klicken, um den Virus zu löschen. Das Gefühl der Dringlichkeit und Angst bringt die Opfer dazu, Schadsoftware herunterzuladen oder ihre Anmeldedaten einzugeben.[46]

Während Hacker immer neue Kanäle wie die sozialen Medien oder Messaging-Apps nutzen, um in unsere Geräte einzudringen, wird es zunehmend schwierig, Cyberangriffe zu erkennen und zu vermeiden. In der Realität von heute vergeht kaum noch Zeit zwischen der Einführung eines neuen Kommunikationskanals und seiner Ausnutzung durch Cyberkriminelle.

PRAXISTIPPS

Mit dem Faktor Mensch im Fadenkreuz von Social-Engineering-Angriffen sollte der nächste logische Schritt für Organisationen sein, die Security Awareness der Mitarbeitenden über alle Kanäle hinweg zu fördern. Die Angestellten sollten ein wichtiger Bestandteil des ISMS sein, um so die Sicherheitskultur ganzheitlich zu stärken.

Als Asset Owner ihrer Mobilgeräte und der von ihnen angeforderten Software sind sie für das Erfüllen der Sicherheitsmaßnahmen verantwortlich. Darüber hinaus können kontextbasierte Threat-Detection-Tools auf den verschiedenen Kanälen Mitarbeitenden dabei helfen, mögliche Angriffe zu erkennen und zu melden.

Da ein Großteil der Phishing-Attacken auf Zero-Day-Schwachstellen abzielen, besteht die effektivste Methode zum Schutz der Organisation in der Stärkung des Faktors Mensch, also in der Befähigung der Mitarbeitenden.

08

Multi-Faktor-Authentifizierung versagt: nicht so sicher wie gedacht?

Viele Jahre lang haben sich Organisationen auf Multi-Faktor-Authentifizierung (MFA) als effektive Schutzmaßnahme vor Sicherheitsvorfällen verlassen. Zwar ist MFA weiterhin eine große Hürde für illegale Eindringlinge. Aber jüngste Vorfälle lassen vermuten, dass die Zuverlässigkeit der Maßnahme allein überschätzt wurde.

Multi-Faktor-Authentifizierung gibt es in verschiedenen Formen. Die beliebteste besteht aus Pop-up-Benachrichtigungen auf dem Mobiltelefon, die User zur Autorisierung der jeweiligen Aktivität auffordern. Cyberkriminelle haben jedoch einen Weg gefunden, diese Authentifizierungsmethode mittels Social-Engineering-Strategien wie MFA Fatigue oder MFA Push Spam zu sabotieren. Dabei überfluten sie ihre Opfer so lange mit Pop-up-Benachrichtigungen, bis sie sie aus Versehen oder einfach aus Ermüdung bestätigen. Ähnlich wie im vorherigen Trend, nehmen die Hacker daraufhin über einen anderen Kanal Kontakt zu ihrem Opfer auf, geben sich als IT-Support aus und fordern das Opfer zu einer Bestätigung auf. Genau diese Methode steckte auch hinter den jüngsten groß angelegten Datenschutzverstößen bei Uber, Microsoft und Cisco.[47]

Eine weitere Strategie, um MFA zu sabotieren, ist die Attacker-in-the-Middle (AiTM) Methode, die wie ein gewöhnlicher Phishing-Angriff aussieht, aber etwas komplexer ist. Üblicherweise beginnt sie mit einer Phishing-Mail, von der aus der User auf eine Fake-Login-Seite geleitet wird. Zwischen der echten und der Fake-Webseite steht ein Proxy, der es den Angreifenden ermöglicht, den Sitzungscookie zu speichern, der nach der Eingabe der Login-Daten und des MFA-Passworts generiert wird. Die Hacker nutzen daraufhin diese Cookies in ihren eigenen Browsern, um sich automatisch im Konto des Opfers anzumelden, ohne den Authentifizierungsvorgang erneut durchlaufen zu müssen. Mit dieser Methode in Kombination mit Spear Phishing drangen Hacker kürzlich in verschiedenste Microsoft-365-Konten von Führungspersonen in großen Konzernen ein und lenkten Transaktionen auf ihre eigenen Bankkonten um.[48]

Auch bei der Supply-Chain-Attacke auf SolarWinds haben Angreifende versucht, MFA als Angriffsvektor zu nutzen. Der Angriff wurde erkannt, als jemand versuchte, bei der Autorisierung ein zweites Mobiltelefon zu registrieren.[49] Bedauerlicherweise sind MFA-Angriffe über das Mobiltelefon nicht immer leicht zu identifizieren. Bei einem Hackerangriff 2021 mittels sogenanntem SIM-Swapping leerten Cyberkriminelle die Krypto-Wallets ihrer Opfer, indem sie Telekommunikationsanbieter dazu brachten, Telefonnummern ihrer Kundinnen und Kunden neuen SIM-Karten zuzuweisen. Daraufhin erhielten die Betrüger SMS zur Multi-Faktor-Authentifizierung auf einer neuen SIM-Karte und verschafften sich so Zugriff auf die Krypto-Konten ihrer Opfer.[50]

Schadsoftware kann auch zur Überlistung der MFA bei Man-in-the-Endpoint-Angriffen zum Einsatz kommen. Bei dieser Methode wird Malware auf dem Gerät des Opfers installiert, über die die Hacker betrügerische Sitzungen im Hintergrund – nur für sie selbst sichtbar – ausführen können, sobald der User die MFA abschließt. Diese betrügerischen Sitzungen können die Angreifenden zu ihren perfiden Zwecken nutzen, zum Beispiel indem sie Gehaltszahlungen auf ihr eigenes Bankkonto umleiten. Bei einer weiteren Betrugsmasche bauen die Kriminellen Passwortgeneratoren in Authentifizierungssystemen nach, die auf einem einmaligen Code basieren. Diese Taktik setzt ein hohes Level an technischen Fertigkeiten voraus, denn sie erfordert das Reverse Engineering des Algorithmus und des Ausgangswerts des Generators, um die Kontrolle darüber zu übernehmen.

Ist das geschafft, können die Kriminellen jedoch Zugangscodes an User schicken und auf diese Weise die MFA umgehen.[51]

Multi-Faktor-Authentifizierung ist also inzwischen zum Angriffsvektor in großangelegten Datendiebstählen geworden. Sie mag zwar eine starke Sicherheitsmaßnahme sein. Doch wie viel Sicherheit MFA wirklich bietet, hängt letztlich von ihrer Implementierung sowie von dem Umfang der ergänzenden Sicherheitsmaßnahmen ab.

PRAXISTIPPS

Damit die Informationssicherheit von Organisationen wirklich von dem zusätzlichen Schutz durch MFA profitiert, ist ein genauerer Blick auf interne organisatorische Prozesse sowie die Awareness der Mitarbeitenden unumgänglich.

Aus technischer Sicht wird das Risiko bereits reduziert, indem MFA zusammen mit Number Matching genutzt wird oder indem die Anzahl der Versuche bzw. der Zeitraum, in dem eine Authentifizierungsanfrage angenommen werden kann, eingeschränkt wird.

Zudem sollten Organisationen sicherstellen, dass verwaiste Konten gelöscht und Zugriffsrechte regelmäßig überprüft werden, wobei das Least-Privilege-Prinzip für den Systemzugriff gelten sollte. Manche Expertinnen und Experten empfehlen sogar, zu Phishing-resistenten MFA-Methoden zu wechseln, wie zum Beispiel zur Nutzung physischer Token, oder aber MFA vollständig zu vermeiden und stattdessen für so viele Accounts wie möglich Single Sign-On zu nutzen.

Auf organisatorischer Ebene können Unternehmen von Awareness-Training für ihre Mitarbeitenden profitieren. Nutzende, die in einem Verdachtsfall schnell reagieren und einen Angriff effektiv abwehren können, sind für die Sicherheit von Organisationen von größter Wichtigkeit – auch und vor allem, wenn es darum geht, MFA-Betrug und MFA Fatigue zu vermeiden.

47 Golem (2022). Hackergruppe umgeht 2FA mit einfachem Trick.
48 Heise Online (2022). Office-Nutzer im Visier: Phishing-Kampagne umgeht Multi-Faktor-Authentifizierung.
49 Security Insider (2022). Wie Hacker MFA nutzen, um Unternehmen anzugreifen.
50 Heise Online (2022). 68 Millionen US-Dollar im Jahr 2021 durch SIM-Swapping ergaunert.
51 Computerwoche (2022). Zwei-Faktor-Authentifizierung mit Tücken.

Stärken Sie Ihre Sicherheitskultur – einfach und effektiv

Mit seiner Awareness-Plattform hilft SoSafe Organisationen, ihre Sicherheitskultur zu stärken und menschliche Risikofaktoren zu minimieren. Die Plattform bietet motivierende Lernerfahrungen und smarte Angriffssimulationen, die Mitarbeitende dazu befähigen, Cyberbedrohungen zu erkennen und aktiv abzuwehren – alles basierend auf verhaltenspsychologischen Erkenntnissen, die das Lernen spannender und effektiver gestalten. Anhand umfassender Analytics werden Verhaltensänderungen gemessen und Schwachstellen aufgedeckt, sodass Cyberbedrohungen proaktiv vorgebeugt werden kann. Die SoSafe Plattform ist im Handumdrehen eingerichtet und wächst mit Ihrem Unternehmen, um so sicheres Verhalten bei den Mitarbeitenden nachhaltig zu festigen.

TEACH

Motivierendes Micro-Learning

Eine verhaltenspsychologisch fundierte E-Learning-Plattform, mit der Lernen Spaß macht. Dynamische und wirkungsvolle Lernerfahrungen auf verschiedenen Kanälen helfen Ihnen, Ihre Abwehr gegen Cyberbedrohungen zu stärken, volle Compliance zu erzielen und mühelos sichere Verhaltensweisen aufzubauen.

- Storybasierte Micro-Lerninhalte mit Gamification-Elementen motivieren und fördern nachhaltig sichere Verhaltensweisen
- Ausgewählte, strukturierte Inhalte, die sich einfach skalieren lassen
- Benutzerfreundliche Customization- und Content-Management-Optionen, auf Ihr Unternehmen abgestimmt

TRANSFER

Smarte Angriffssimulationen

Zielgerichtete Phishing-Simulationen, um sichere Verhaltensweisen bei Ihren Mitarbeitenden zu fördern. Mit regelmäßigen, automatisierten Spear-Phishing-Simulationen befähigen Sie Ihre Mitarbeitenden, Cyberattacken zu erkennen und Security Awareness zu einem festen Bestandteil ihres Arbeitsalltags zu machen. Reduzieren Sie Ihr Cyberrisiko und Ihre Reaktionszeit im Falle eines Angriffs.

- Personalisierbare, realistische Simulationen von Cyberangriffen
- Kontextbasierte Lernseiten, die sichere Verhaltensweisen des Teams festigen
- Unmittelbares Reporting mit nur einem Klick dank Phishing-Meldebutton

ACT

Strategisches Risk Monitoring

Behalten Sie menschliche Risikofaktoren mit unserer Lösung immer im Blick und schützen Sie Ihre Organisation vor kostspieligen Sicherheitsvorfällen. Mit umfangreichen Daten und verhaltenspsychologisch fundierten Insights können Sie mögliche Schwachstellen beheben. Sie erhalten zudem ein ganzheitliches Bild über das Verhalten Ihrer Mitarbeitenden und den Erfolg Ihres Security-Awareness-Programms und können dadurch fundierte strategische Entscheidungen treffen.

- Aufschlussreiche Insights durch kontextuelle Daten, wie technische KPIs und verhaltensbasierte Kennzahlen
- Branchenspezifische Benchmarks und Handlungsempfehlungen für den Ernstfall
- Auf Audits nach ISO/IEC 27001 ausgelegt und 100 % DSGVO-konform

SoSafe GmbH
Lichtstraße 25a
50825 Köln

info@sosafe.de
www.sosafe-awareness.com/de
+49 221 65083800