G DATA academy

Der Mensch im Visier von Cybercrime

SECURITY AWARENESS IN ZAHLEN 2023

Liebe Leserinnen, liebe Leser,

immer wieder höre ich von Unternehmerinnen und Unternehmern, aber auch von IT-Verantwortlichen die Aussage: „Warum sollten uns kriminelle Hacker angreifen? Wir sind doch kein lohnendes Ziel.“ Aber gerade Mittelständler sitzen da einem Trugschluss auf. Opfer einer Cyberattacke zu werden, ist keine Frage der Attraktivität eines Angriffs, sondern nur eine Frage der Zeit. Der Grad der Digitalisierung in Deutschland ist sehr hoch, auch wenn es sicherlich noch viel zu verbessern gibt. Die digitale Transformation hat längst alle Lebens- und Wirtschaftsbereiche erreicht. Sie ist dabei, wenn wir Kontakte knüpfen und pflegen, Wissen gewinnen, Termine planen, uns ausweisen, Verträge schließen, einkaufen und bezahlen. Sie unterstützt Unternehmen, wenn sie Rechnungen und Aufträge schreiben, Kunden ansprechen, Informationen speichern, Wissen managen. Daher ist die sichere Versorgung mit digitalen Dienstleistungen schon heute so existenziell wie die Versorgung mit Strom oder Wasser. Aber fast täglich führen uns Meldungen über erfolgreiche Cyberangriffe vor Augen, wie verletzlich unsere digitale Infrastruktur ist, wenn Unternehmen ihre Produktion einstellen. Ohne Telefonanlage, ohne E-Mails, ohne Warenwirtschaftssystem, ohne Online-Shop, sprich ohne funktionierende IT, stehen viele schnell am Rande einer Insolvenz.

Seit vielen Jahren bietet unser Unternehmen Sicherheitstechnologien und Dienstleistungen an, um auf digitale Gefahren vorbereitet zu sein und im Fall der Fälle bestmöglich agieren zu können. Einen Faktor, der jedoch beim Design von IT-Sicherheitskonzepten oft außer Acht gelassen wird, ist der Mensch selbst. Er nutzt digitale Technologien oft blind und ist sich vieler teils trivialer Gefahrenquellen nicht bewusst. Mit Phishing-Mails, CEO-Fraud oder Social Engineering überwinden Cyberkriminelle zu schnell technische Hürden und verschaffen sich über den Faktor Mensch Zugang zu Unternehmensnetzwerken. Unbemerkt werden so vertrauliche Daten abgegriffen, finanzielle Transaktionen manipuliert, Unternehmensnetzwerke verschlüsselt und blockiert und letztlich Lösegeldsummen erpresst. IT-Sicherheit muss heute auf mehrere Säulen verteilt werden. Unternehmen müssen ihre Belegschaft in die IT-Sicherheitsstrategie einbeziehen. Wir sprechen hier von „Human Centered Security“. Dies gelingt, wenn Unternehmen das menschliche Verhalten updaten – mit Security Awareness Trainings. Diese Schulungen stellen den Menschen und sein Verhalten in den Mittelpunkt, nicht die Technik. So lässt sich gezielt nicht nur Aufmerksamkeit im wörtlichen Sinne, sondern ein generelles Umdenken erreichen. Mitarbeitende verstehen, welchen Beitrag sie für die IT-Sicherheit des eigenen Unternehmens leisten können.

Auf den folgenden Seiten haben wir Zahlen aus der Studie „Cybersicherheit in Zahlen“ für Sie zusammengefasst, die belegen, welche Rolle Ihre Mitarbeitenden in puncto IT-Sicherheit spielen, wie Hacker unachtsames Verhalten ausnutzen und wie es um digitale Kompetenzen der Deutschen bestellt ist.

Ich wünsche Ihnen eine aufschlussreiche Lektüre.

Andreas Lüning
Vorstand und Mitgründer der G DATA CyberDefense AG

G DATA academy

INHALT

STATUS QUO DER CYBERKRIMINALITÄT

Bedrohliche Zahlen für deutsche Unternehmen

Jeden Tag landen in den Postfächern von Mitarbeitenden unzählige Mails. Einige davon sind Spam, also unerwünschte Werbung, oder – viel schlimmer – Phishing. Also Nachrichten von Cyberkriminellen mit dem Ziel, persönliche Daten wie Zugangsinformationen zum Online-Banking oder zum Firmen-Account zu kopieren, um diese zu missbrauchen. Oder um uns zum Öffnen eines Anhangs zu verleiten, der Schadsoftware enthält und auf diesen Weg den eigenen Computer oder das Firmennetzwerk kompromittiert – mit teils dramatischen Folgen. Wie groß das Problem aktuell ist, zeigen Zahlen des Internet Crime Complaint Centers des amerikanischen FBIs. Innerhalb von fünf Jahren ist die Zahl der gemeldeten Phishing-Fälle um mehr als 1.560 Prozent gestiegen. Auch andere Internet-Straftaten haben zugenommen, aber nicht in diesem Maße.

Anstieg gemeldeter Phishing-Attacken von 2016 bis 2021

Quelle: FBI, Internet Crime Complaint Center, US Department of Justice

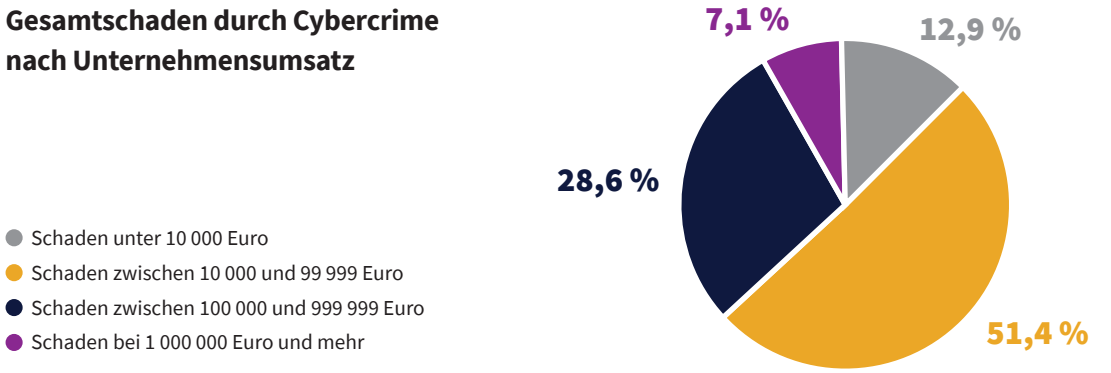
Nicht nur die Zahl der Straftaten ist um ein Vielfaches gewachsen, auch die Schäden im Zusammenhang mit Internetkriminalität steigen. Ein Ende ist noch nicht in Sicht, wie aktuelle Zahlen des Bundesamts für Sicherheit in der Informationstechnik zeigen. Innerhalb von zwei Jahren hat sich der jährliche Schaden durch Ransomware in Deutschland mehr als vervierfacht – von 5,3 Milliarden auf 24,3 Milliarden Euro. Eine wahrscheinlich eher konservative Hochrechnung, zumal nicht alle Unternehmen einen Cyberangriff melden und sich durch eine Lösegeldzahlung freikaufen. Weltweit haben Cyberkriminelle 2021 schätzungsweise 509 Milliarden Euro Profit mit Lösegeldforderungen bei Ransomware-Angriffen gemacht – das entspricht ungefähr dem Bruttoinlandsprodukt Belgiens.

Jährlicher Schaden durch Ransomware in Deutschland

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Schäden infolge eines Cyberangriffs können unterschiedliche Auswirkungen haben und hängen direkt davon ab, wie hoch das Schutzniveau im Unternehmen ist bzw. wie gut ein Unternehmen auf eine derartigen IT-Notfall vorbereitet ist. Denn je schneller ein Unternehmen wieder handlungsfähig ist, desto geringer ist die Ausfallzeit etwa beim Webshop oder in der Produktion und damit auch der wirtschaftliche Schaden. Dieser kann im schlimmsten Fall aber auch direkt zur Insolvenz führen. Eine Studie von KPMG zeigt den Gesamtschaden für deutsche Unternehmen nach Umsatzgrößen. Über die Hälfte der befragten Unternehmen hat einen Schaden zwischen 10.000 und 99.999 Euro erlitten. Und 7 % sogar über eine Million Euro.

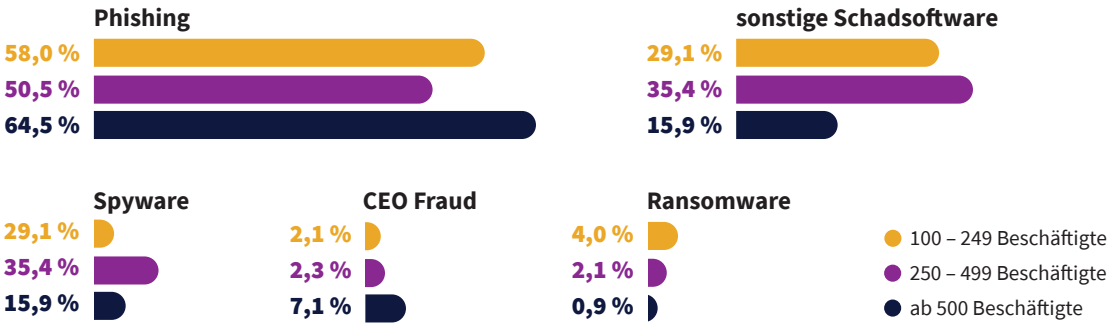
Gesamtschaden durch Cybercrime nach Unternehmensumsatz



Quelle: KPMG

Bei vielen Angriffen spielt der Mensch eine entscheidende Rolle. Mit Phishing-Attacken umgehen Cyberkriminelle Schutzmechanismen und nehmen Anwenderinnen und Anwender direkt ins Visier. Die Erklärung, warum wir Menschen immer wieder auf derartige Mails hereinfallen, ist einfach: Menschliches Verhalten lässt sich auf unterschiedliche externe Trigger zurückführen. Diese lösen verschiedene Reaktionen aus, die Menschen im Laufe der Zeit gelernt haben. Die Kriminellen setzen dabei insbesondere auf Trigger wie Gier, Neugier, Angst, Druck, Pflichtbewusstsein, Hilfsbereitschaft und Gewohnheit. Oft werden diese auch miteinander kombiniert. Wir öffnen eine erhaltene E-Mail automatisch, um sie zu lesen. Dieses Verhalten nutzen Angreifer aus: Sie zielen direkt auf Gefühle. Wer hatte nicht schon eine E-Mail in seinem Postfach, die einen Geldgewinn oder eine Erbschaft in Millionenhöhe versprach? Aber die Tricks werden immer perfider. Nachrichten von einer verspäteten Paketzustellung, die Aufforderung, das Passwort eines Social-Media-Accounts zu erneuern oder eine Mail der Hausbank mit der Bitte, eine neue App fürs Online-Banking zu installieren, sind deutlich schwieriger zu entlarven. Somit überrascht es auch nicht, dass Phishing für alle Unternehmen eine zentrale Herausforderung ist, wie die Zahlen des Kriminologischen Forschungsinstitutes Niedersachsen zeigen. Bei Cyberangriffen liegt der Anteil von Phishing-Attacken zwischen 50 und 66 % in Deutschland – je nach Unternehmensgröße.

Anteil der erlebten Cyberangriffe nach Angriffsart und Unternehmensgröße



Quelle: Kriminologisches Forschungsinstitut Niedersachsen e.V.

CYBERCRIME TRENDS FÜR 2023

Angreifer professionalisieren sich weiter

Auch in diesem und den kommenden Jahren bleibt der Mensch ein beliebtes Angriffsziel, denn die IT-Bedrohungslage wird sich 2023 weiter verschärfen. Grund dafür ist die fortschreitende Professionalisierung der Cybercrime-Szene.

Da sich der technologische Schutz gegen Schadsoftware deutlich verbessert hat und IT-Security-Unternehmen diesen stetig weiterentwickeln, verfeinern auch Cyberkriminelle ihre Angriffsmethoden. Das bedeutet, dass sie nach Schwachstellen in der Verteidigungsstrategie suchen. So werden wir wieder einmal an das schwächste Glied in der Sicherheitskette erinnert: schlecht informierte Nutzer*innen. Cyberkriminelle werden auch in Zukunft auf Social Engineering setzen, um persönliche Daten oder Informationen abzugreifen. Diese nutzen sie, um sich Zugriff auf einen Computer und/oder ein Unternehmensnetzwerk zu verschaffen oder um sich Zugangsdaten für soziale Netzwerke zu beschaffen. Jeder, der denkt, dass ihm oder ihr das nicht passieren wird, unterschätzt die Gefahr, denn die Angriffe werden immer professioneller: Anstelle von Massenattacken greifen Cyberkriminelle gezielt einzelne Personen an.

Ein aktuelles Beispiel, wie trickreich Angreifende agieren und Menschen manipulieren: Unternehmen setzen zunehmend auf Multi-Faktor-Authentifizierung (MFA), um zu verhindern, dass sich Unbefugte einfach mit Anmeldedaten in ein Netzwerk einloggen können. Zurzeit ist zu beobachten, dass Cyberkriminelle eine Social-Engineering-Technik namens „MFA Fatigue“ nutzen. Der Vorteil für Angreifende: Die Technik funktioniert ohne Malware- oder Phishing-Infrastruktur. Bei diesem Angriff führen Kriminelle ein Skript aus, um sich mit gestohlenen Log-in-Daten anzumelden. Dabei erzeugt die MFA unzählige Push-Anfragen an das Mobilgerät des Kontoinhabers oder der Kontoinhaberin. Irgendwann stimmen die Anwender*innen den Push-Nachrichten zu und die Cyberkriminellen erhalten direkten Zugriff auf das VPN und das Netzwerk. Diese Angriffsmethode kam sowohl beim Cisco- als auch beim Uber-Hack zum Einsatz.

Wie im genannten Beispiel spielen gerade Mobilgeräte/Smartphones bei Cyberattacken eine entscheidende Rolle. Angreifende nehmen vermehrt via Messenger-Dienst, wie etwa per Whatsapp oder Telegram, Kontakt zu ihren potenziellen Opfern auf. Wie real die Gefahr ist, zeigen aktuelle Betrugsversuche. Dabei haben Täter den Enkeltrick in den digitalen Raum verlagert, sozusagen als “Enkeltrick 2.0”. Täter geben sich als ein Familienmitglied in Not aus und versuchen, ihr Opfer zur Überweisung eines größeren Geldbetrags zu überreden.

SIND UNTERNEHMEN GEWAPPNET?

IT-Verantwortliche und Mitarbeitende schätzen die Lage ein

Es zeigt sich: Unternehmen müssen die IT-Sicherheit ganzheitlich durchdenken. Dabei spielen die Mitarbeitenden eine zentrale Rolle. Wenn Angestellte aufmerksam sind und beispielsweise verdächtige Mails löschen, anstatt sie zu öffnen, schützen sie nicht nur sich selbst und ihr eigenes Postfach, sondern ihren Arbeitgeber und damit auch die Arbeitsplätze der Kolleg*innen. Stellt sich also die Frage, wie kompetent wir beim Thema IT-Sicherheit sind. Die Antwort findet sich in der Arbeitnehmer*innen-Umfrage, die wir gemeinsam mit Statista und brand eins durchgeführt haben: Sie fällt ernüchternd aus und zeigt dringenden Handlungsbedarf. Nur jede*r vierte Befragte schätzt seine persönlichen IT-Sicherheitskompetenzen als groß oder sehr groß ein. Demgegenüber bescheinigen sich mehr als 33 Prozent geringes und sehr geringes Fachwissen in Bezug auf IT-Sicherheit. Auffällig ist, dass sich das Wissen um IT-Sicherheit in den Branchen stark unterscheidet und darüber hinaus von der Unternehmensgröße abhängt.

Für wie kompetent halten Mitarbeitende ihr Unternehmen beim Thema IT-Sicherheit?

Top und Flop 3 der Branchen

Bei der Unternehmensgröße gilt: In kleinen Firmen schätzt ein besonders großer Teil der Mitarbeitenden die eigene Kompetenz im Bereich IT-Sicherheit (sehr) gering ein. Bei größeren Unternehmen ist es aber auch immer noch fast jede*r vierte Angestellte.

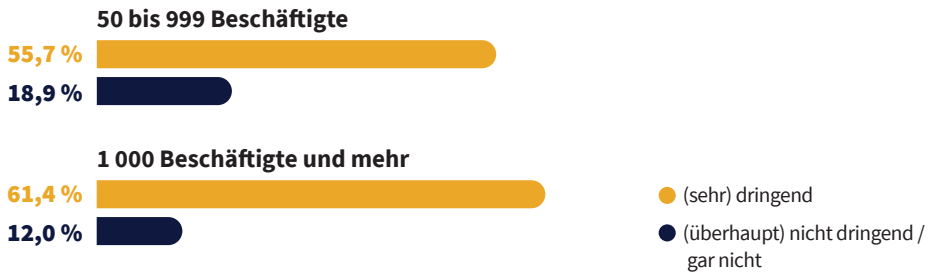
Einschätzung der Kompetenz nach Unternehmensgröße

	unter 50 Beschäftigte	50 bis 999 Beschäftigte	1 000 Beschäftigte und mehr
(sehr) große Kompetenz	22,8 %	42,6 %	33,5 %
(sehr) geringe Kompetenz	36,6 %	21,4 %	23,4 %

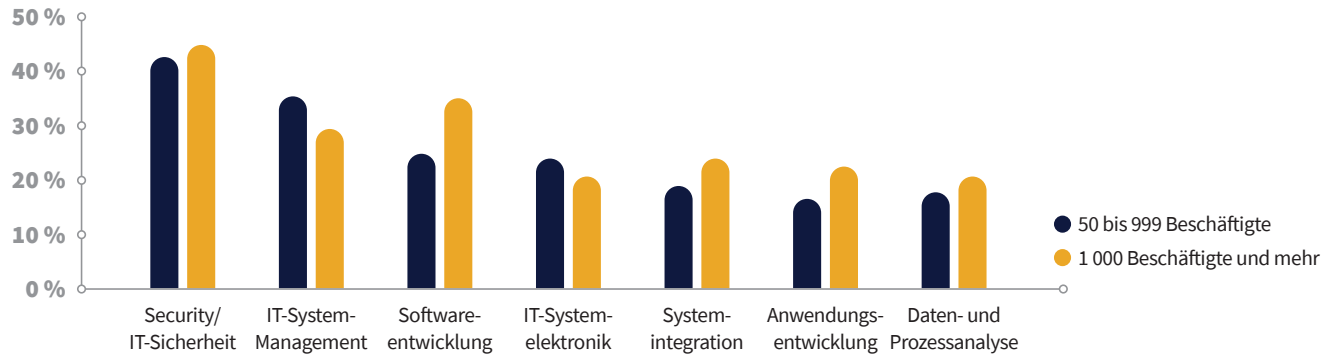
Quelle: Statista im Auftrag von G DATA

Die Ergebnisse der nächsten Umfrage machen das Bild leider nicht besser. Denn die Unsicherheit der Mitarbeitenden trifft auf einen Mangel an IT-Fachleuten, insbesondere im Bereich IT Security. Eine gefährliche Mischung. Die Antworten von Mitarbeitenden aus den Beriechen IT, Personal und Geschäftsführung zeigen, wie dringlich insbesondere große Unternehmen nach IT-Fachkräften suchen, um die Cyberrisiken einzudämmen.

Wie dringend werden IT-Fachleute gebraucht?

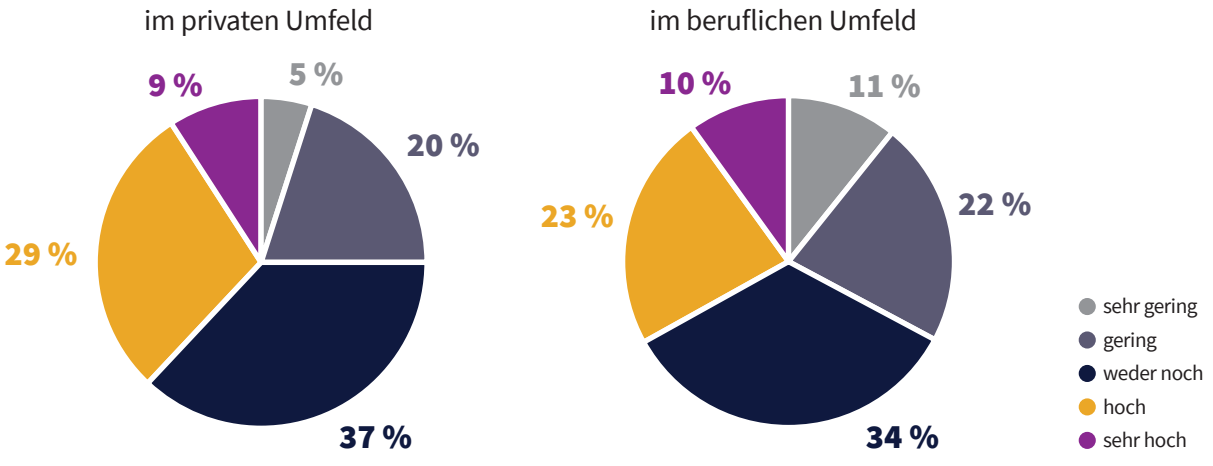


Wo ist der Bedarf an IT-Fachleuten am größten?



Mitarbeitende sind sich der bestehenden Cyberrisiken teilweise durchaus bewusst, wie folgende Grafik belegt. Im beruflichen Umfeld schätzt über ein Drittel der Befragten das Risiko als hoch oder sehr hoch ein, Cyberkriminalität zum Opfer zu fallen. Im privaten Umfeld liegt der Anteil sogar noch höher – bei 38 Prozent. Auf der anderen Seite zeigt sich aber auch, dass ein Drittel im beruflichen Umfeld das Risiko als sehr gering einschätzt.

Wie hoch schätzen Sie das Risiko ein, Opfer einer Cyberattacke zu werden?



Quelle: Statista im Auftrag von G DATA

Fehlende Expertise und unbedarfter Umgang mit Cyberbedrohungen bei steigendem Digitalisierungsdruck für alle Branchen – das alles bildet einen guten Nährboden für Cyberkriminelle und erfolgreiche Angriffe. Hinzu kommt: Zur mangelnden IT-Sicherheitskompetenz gesellt sich Leichtsinn: Mehr als 17 Prozent der Befragten schätzen sich bei der IT-Sicherheit als sehr oder eher leichtsinnig ein.

Typische Beispiele für ein derartiges Verhalten:

Mitarbeitende nutzen einfache, leicht zu merkende Passwörter, die Cyberkriminelle mittels Brute-Force-Attacke in Sekundenbruchteilen knacken.

Sie notieren ihre Passwörter auf einem Notizzettel und befestigen diesen direkt am Monitor – für jede andere Person einsehbar.

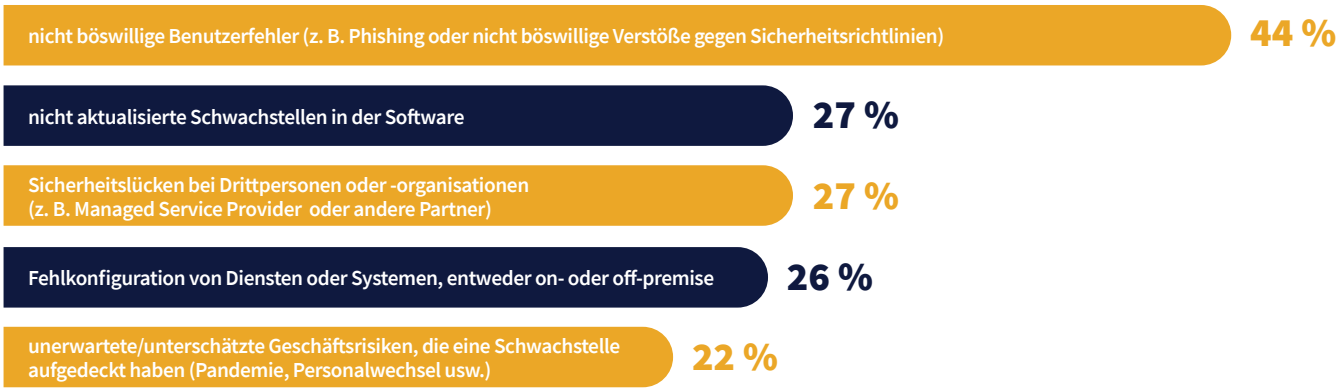
Sie nutzen ein Passwort für mehrere Services. Kopiert eine unbefugte Person diese Log-in-Informationen, hat sie Zugang zu vielen, teils persönlichen Konten.

DER MENSCH IM FOKUS VON CYBERCRIME

Was tun, wenn Technik allein nicht schützt?

Aus Sicht vieler Mitarbeitenden liegt die Verantwortung für die unternehmensweite IT-Sicherheit bei den Fachleuten, die mit teuren Systemen für Schutz sorgen. Daher denken viele Angestellte gar nicht daran, dass sie Teil eines Sicherheitskonzepts sind. Das Gegenteil ist aber der Fall, wie folgende Grafik verdeutlicht: 44 Prozent der IT-Sicherheitsvorfälle im Jahr 2021 ließen sich auf Fehler durch Nutzer*innen zurückführen. Dazu gehört auch das Öffnen von Anhängen von Phishing-Mails oder die versehentliche Weitergabe von Log-in-Daten auf gefälschten Webseiten.

Top 5 Ursachen für Sicherheitsvorfälle in Unternehmen



Quelle: Foundry

Eine Besserung ist nicht in Sicht. Im Gegenteil: Unachtsamkeit und Nichterkennen von Verdachtsfällen führen immer noch die Liste der Faktoren an, die Cyberattacken begünstigen. Der größte Zuwachs bei den Einfallstoren liegt bei unzureichend geschultem Personal (plus 35 Prozent).

SO SIEHT PHISHING IM ALLTAG AUS

5 echte Phishing-Mails

Phishing ist und bleibt im Ranking der Internet-Straftaten unangefochten die Nummer eins. Das belegt auch ein Bericht des FBI. Dort ist die Zahl der gemeldeten Straftaten im Zusammenhang mit Phishing innerhalb von fünf Jahren um mehr als 1 560 Prozent gestiegen. Ein Grund dafür: Cyberkriminelle verfeinern ihre Methoden – Phishing-Mails sind immer schwerer zu erkennen. Wie Cyberkriminelle ihre Opfer auswählen und welche Mails sie verschicken, erklärt Manuel Beelen, Head of Security Operations bei G DATA CyberDefense.

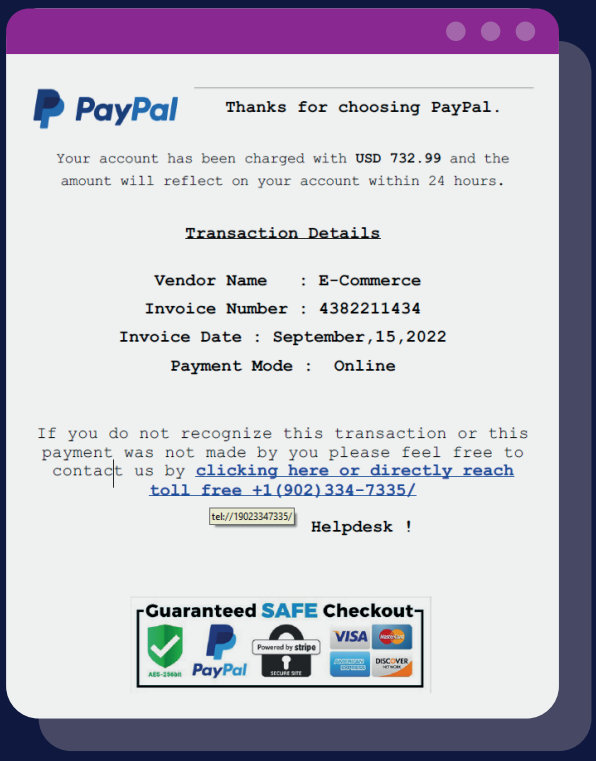
Kaum zu glauben: Eine kurze Suche bei Google reicht Kriminellen, um die passenden E-Mail-Adressen für Phishing-Kampagnen zu identifizieren. Mit wenigen Klicks finden sie wichtige Informationen, die Mitarbeitende beispielsweise im Business-Netzwerk veröffentlichen.

„In sozialen Netzwerken wollen wir ja, dass uns Freunde oder Geschäftskontakte finden“, sagt Manuel Beelen. „Für den Aufbau und die Pflege von diesen sozialen Netzwerken braucht es elementare Informationen, um auffindbar zu sein.“ Genau aus diesen Daten können Angreifende aber zusätzliche Informationen ableiten, etwa die Logik der E-Mail-Adressen eines Unternehmens. So müssen sie nicht mehr aufwendig ausprobieren, welches Format das richtige ist.

Wie täuschend echt Kampagnen zurzeit aussehen, zeigt sich anhand von aktuellen Beispielen, mit denen Kriminelle versucht haben, Mitarbeitende von G DATA auszutricksen. Beelen stellt fünf aktuelle Phishing-Mails vor, die auch Profis nicht auf den ersten Blick erkennen.

1 Phishing mal anders

Das potenzielle Opfer erhält eine Nachricht mit Anhang im PDF-Format über eine Paypal-Abbuchung. Interessanterweise enthält die Mail auch eine Kontaktmöglichkeit: eine Telefonnummer in den USA. Wer diese Nummer anruft, erreicht einen freundlichen Service-Mitarbeiter, der sogar deutsch spricht. Er erklärt, dass der oder die Anrufer*in zunächst die eigenen Paypal-Daten inklusive Passwort angeben muss, damit sie die Zahlung zurückbuchen können.



PayPal

Thanks for choosing PayPal.

Your account has been charged with USD 732.99 and the amount will reflect on your account within 24 hours.

Transaction Details

Vendor Name : E-Commerce
Invoice Number : 4382211434
Invoice Date : September,15,2022
Payment Mode : Online

If you do not recognize this transaction or this payment was not made by you please feel free to contact us by clicking here or directly reach toll free +1(902)334-7335/

tel://19023347335/

Helpdesk !

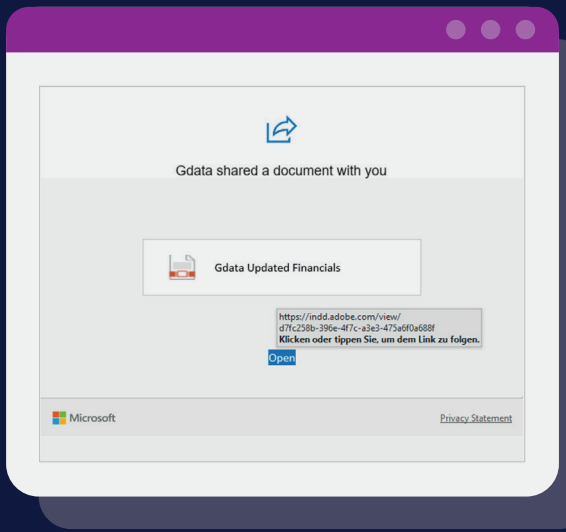
Guaranteed SAFE Checkout

2 Angriff mit Microsoft

Die Nachricht von Microsoft über ein abgelaufenes Passwort gehört zu den Klassikern der Phisher. Bei einer aktuellen Methode sieht die Phishing-Mail auf den ersten Blick plausibel aus, weil auch die Adresse beim Mouse-Over mit gdata.de anfängt. Aber dann folgen Buchstaben und Zahlen, die den eigentlichen Absender verraten, nämlich manxtrider.com. Das Fatale: So weit prüfen manche Anwender*innen die Daten nicht. Der Blick geht nur auf gdata.de, die Opfer klicken den Link an und landen auf einer gefälschten Webseite. Hier geben sie dann im guten Glauben ihre Anmeldedaten preis.

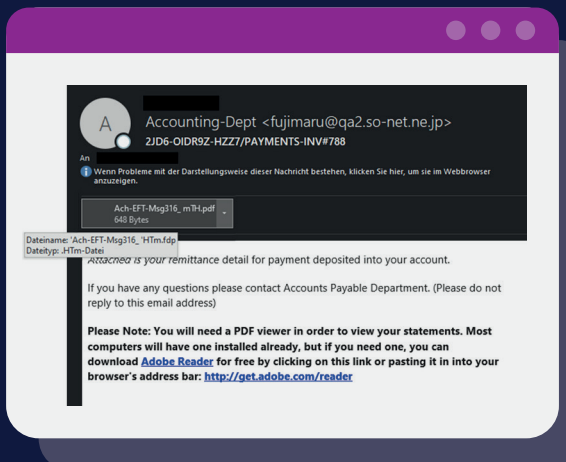
3 Mit InDesign auf Phishing-Tour

Beim dritten Beispiel steht ein Missbrauch von InDesign-Seiten im Mittelpunkt. Ein Vorteil für Cyberkriminelle: Die Webseiten lassen sich direkt bei Adobe hosten und Shortlinks schnell generieren. Somit verschicken die Angreifenden eine authentische Mail von Adobe an ihre Opfer. Wer die Nachricht genauer betrachtet, stutzt sicherlich über das Privacy Statement von Microsoft. Wer aber auf den Trick hereinfällt und den Link in der Mail anklickt, landet dann auf der Phishing-Seite. Für die Empfänger*innen ist es also sehr schwer, die Falle zu erkennen, da es sich um eine echte Adobe-Seite handelt. Das Problem: Diese lassen sich nicht blocken, weil sonst das gesamte InDesign-Framework geblockt ist.



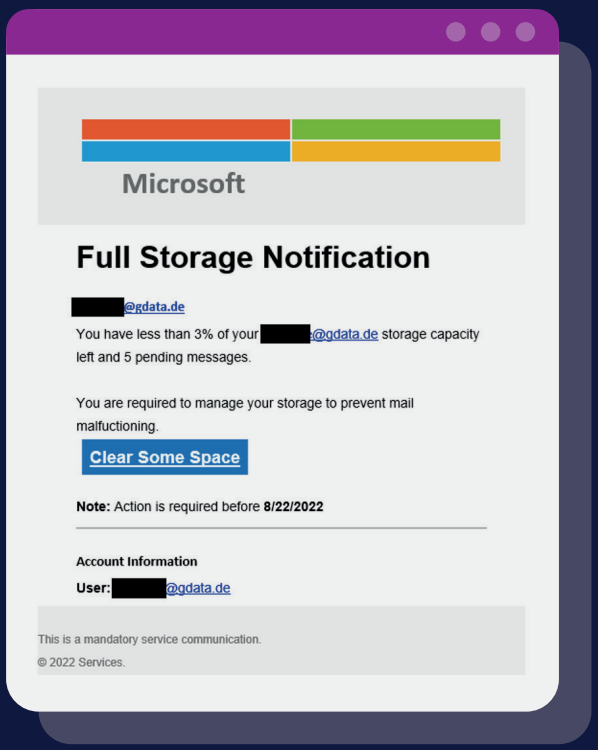
4 Phishing mal anders

Bei dieser Methode enthält eine E-Mail im Anhang ein Dokument mit der Dateiendung .pdf. Aber der Schein trügt, denn es handelt sich um eine .htm-Datei. Möglich ist das, weil sich im Windows-Dateisystem die Reihenfolge der Schriftzeichen umkehren und in die Mitte bauen lässt. So wird aus ”Dateiname_fdp.htm” dann “Dateiname_mth.pdf”. Wer die Datei öffnet, landet direkt im Browser mit einer Weiterleitung auf eine Phishing-Seite.



5 Angriff mit E-Mail-Software

Ebenfalls ein Klassiker aus dem Phishing-Baukasten: Eine Information über knapp werdenden Speicherplatz, direkt verknüpft mit einem – natürlich falschen – Link, um mehr Speicher freizuschalten. Die Taktik: Die Angreifenden bauen Druck auf, um ihr Opfer zu einer schnellen und unüberlegten Handlung zu zwingen.
Bei diesem Angriff setzen die kriminellen Hacker einen legalen Mailservice namens Contactmonkey ein. Eine valide E-Mail-Software, die viele Unternehmen für den Versand von Werbe-Mails nutzen. Allerdings ist die Absender-Adresse direkt mit einer anderen Adresse verknüpft. Auch hier müssen Nutzer*innen schon genauer hinschauen, um den Betrug zu erkennen.



„Das Problem moderner Phishing-Mails ist, dass diese keine Malware direkt enthalten“, sagt Manuel Beelen. „Solche Angriffsversuche lassen sich extrem schwer verteidigen. Das ist auch für IT-Profis wie Admins eine große Herausforderung.“ Geschickte Fälschungen lassen sich nicht einfach mit Sicherheitslösungen wegfiltern, ohne dass auch echte Mails davon betroffen wären. Hinzu kommt: Die Landingpages der Cyberkriminellen sind Original-Kopien echter Seiten, sodass normale Anwender*innen den Unterschied nicht merken und in die Falle tappen. Sie geben ihre Credentials ein, die Daten sind weg und Angreifende können diese problemlos nutzen.

Gute Schutzlösungen wie die von G DATA CyberDefense blocken falsche Phishing-Seiten und schützen auf diesem Weg die Nutzer*innen. Aber Technologien alleine wehren keine gut gemachten Phishing-Angriffe ab. Es braucht auch Mitarbeitende, die wissen, wie trickreich Angreifende agieren. Denn dann schauen sie bei verdächtigen Mails genauer hin und verhindern Angriffe, wenn sie die Mail löschen, nicht den Anhang öffnen oder dem Link folgen. Das Bewusstsein der Belegschaft lässt sich gezielt mittels Security Awareness Trainings verbessern. Hier lernen Angestellte, wie Phisher vorgehen und welche psychologischen Tricks sie anwenden, um ihre Opfer hereinzulegen.

SICHERES VERHALTEN LERNEN UND FÖRDERN

Mit Security Awareness Trainings

Security Awareness Trainings der G DATA academy

Auf unserer interaktiven Lernplattform erfahren Mitarbeitende in spannenden Online-Kursen, wie sie sich und Unternehmen vor Angriffen im digitalen Alltag schützen. Wie erkenne ich Schadsoftware? Was passiert, wenn ich aus Versehen auf einen falschen Link klicke? Worauf sollte ich im Homeoffice achten? Das und noch viel mehr lernen Ihre Beschäftigten in abwechslungsreichen Übungen.

- Komplettpaket aus Lernplattform und -inhalten
- Auch als White-Label-Lösung oder Content-Stream verfügbar
- Optional: Vertiefungstrainings speziell zu Phishing

Phishing Simulation

Mithilfe unserer Phishing Simulation schaffen Sie einen sicheren Rahmen, um Ihre Mitarbeitenden im echten Arbeitsalltag für Phishing zu sensibilisieren. Wir senden vorgetäuschte Phishing-Mails direkt in die Postfächer Ihres Teams. Sie erhalten einen nachvollziehbaren Bericht mit Kennzahlen, wie oft potenziell gefährliche Anhänge geöffnet oder Daten herausgegeben wurden. So wird das Sicherheitsbewusstsein messbar.

Das G DATA Awareness Game

Gamifizierte Lernmethoden haben nachweislich einen hohen Effekt: Nutzende können sich später an bis zu 90 Prozent mehr Inhalte erinnern als bei traditionellen Lernmethoden (Quelle: American Federation of Scientists). In unserem ca. 20-minütigen Awareness Game „Im Netz des Social Engineers“ schlüpfen Ihre Beschäftigten in die Rolle eines Detectives – des besten, wenn es um Cybercrime geht. Hier gilt es aufzuklären: Warum sind alle Rechner bei Meyer Maschinenbau durch Ransomware verschlüsselt? Und was hat Mitarbeiter Paul damit zu tun? Nach dem Spielen weiß Ihr Team genau, was Social Engineering ist und wie es Ransomware sofort erkennt.

G DATA academy

MACHEN SIE IHRE MITARBEITENDEN ZUR STÄRKSTEN VERTEIDIGUNG.

Testen Sie unsere Security Awareness Trainings und sehen Sie wie Stories und spielerische Ansätze Lernenden helfen, Cyberangriffe zu verhindern.

Jetzt testen:
gdata.de/awareness-training