Anti-Phishing-Paket: In 4 Schritten zur erfolgreichen Hacker-Abwehr

CYBERXPERTS

Inhaltsverzeichnis

Wer sind wir eigentlich und warum?

Liebe Leserin, lieber Leser,

Kompliment, dass Sie sich zum Thema Phishing und Awareness-Kampagnen informieren. Damit haben Sie einen wichtigen Schritt gemacht, Ihr Unternehmen vor Cyber-Angriffen zu schützen.

Warum das so dringlich ist, zeigen alarmierende Zahlen wie diese:

- Die schiere Anzahl an Phishing-Mails stieg im letzten Jahr um unglaubliche 29 % an.[1]
- Der Schaden durch Ransomware ist allein in Deutschland auf 24,3 Mrd. Euro angestiegen.[1]
- 45 % der Vorstände geben Cyber-Angriffe als das Hauptgeschäftsrisiko für ihr Unternehmen an.[2]
- Bei fast 9 von 10 Unternehmen in Deutschland haben Angriffe im letzten Jahr zu einem Schaden geführt.[3]
- Die Schäden für die Unternehmen stiegen auf 223,5 Mrd. Euro.[3]

Zur Versinnbildlichung der Größenordnung: 223,5 Milliarden Euro ist vergleichbar mit dem Jahres-Umsatz der gesamten Maschinenbau-Industrie in Deutschland.[4]

1 Bitkom e.V., Wirtschaftsschutzbericht 2021, 05.08.2022.

2 KPMG, Ist Cybersecurity Chefsache?, 05.07.2022, abrufbar unter: https://hub.kpmg.de/ist-cyber-security-chefsache.

3 Bitkom e.V., Wirtschaftsschutzbericht 2021, 05.08.2022.

4 Bundesministerium für Wirtschaft und Klimaschutz, Maschinen und Anlagebau, 08.07.2022, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Artikel/Branchenfokus/Industrie/branchenfokus-maschinen-und-anlagenbau.html.

Wir finden: Es reicht!

Unternehmen können sich schützen – sie müssen nur wissen, wie!

Deshalb haben wir im Jahr 2022 das Security-Awareness-Plattform CyberXperts auf den Markt gebracht. Unternehmen erstellen mit CyberXperts:

- simulierte Phishing-Kampagnen,
- komplette Trainings für Mitarbeiter zur Prävention und
- einen intuitiven 360°-Check zur Einschätzung ihres Risikoprofils.

Mit CyberXperts erreichen Unternehmen eine Rundum-Sensibilisierung der Mitarbeiter für Cyber-Angriffe jeder Art.

Auch wenn CyberXperts als Produkt und Marke neu auf dem Markt ist: Das Team hinter CyberXperts ist es nicht.

Seit über 15 Jahren veröffentlichen wir Fachinformationen zum Thema Datenschutz und Datensicherheit im renommierten Fachverlag Privacy-Xperts aus Bonn. So verfügen wir über ein breites Netzwerk an Experten, die ihr gesamtes Wissen und ihre Erfahrung für den Start von Cyber-Xperts versammelt haben.

Und tatsächlich – das Feedback der Ersttester aus der Fachwelt ist überwältigend (Namen aus Datenschutzgründen geändert):

> *„Die Plattform ist schön einfach und verständlich gestaltet. Wir haben nun schon mehrere Lösungen ausprobiert, aber wir sind mit keiner zurechtgekommen. Bei cyberyxperts.de konnte ich direkt starten und bekam eine fertige Awareness-Kampagne für meine Mitarbeiter. Mir gefällt es gut, dass ich das Experten-Wissen gut aufbereitet erhalte. Endlich verstehe ich, was ich machen soll! Durch die automatische Dokumentation spare ich mir Zeit, da ich es nicht mehr über Excel machen muss."*
>
> Frau Schmitt, öffentliche Verwaltung

> *„Die Zeit ist reif für eine Lösung wie CyberXperts. Die Bedrohungslage ist so massiv gewachsen, dass kein Unternehmen um eine professionelle Unterstützung herumkommt."*
>
> Herr Scholl, Maschinenbau

„Das Portal ist wirklich nah am Bedarf der klein- und mittelständischen Unternehmen in Deutschland entwickelt. Gut gemacht!“

Herr Weber, Handel

„Auch wenn Unternehmen glauben, für Hacker uninteressant zu sein. Jedes – ich betone: JEDES (!) Unternehmen ist inzwischen Zielscheibe, z. B. für Ransomware. Ihr Produkt ist deshalb ein Must-have für alle.“

Herr Sauer, Lebensmittelindustrie

„Ich kenne ja einige Software-Anbieter für Cybercrime-Abwehr. Ihre Lösung gefällt mir sehr gut, insbesondere dass sie so intuitiv zu bedienen ist.“

Frau Stahl, IT-Branche

Wir laden Sie ein: Informieren Sie sich doch auch einmal kostenlos und unverbindlich zu Ihren Möglichkeiten mit CyberXperts. Klicken Sie hier, um Ihr Gratis-Strategie-Beratungsgespräch zu vereinbaren.

Wir freuen uns auf Sie!

Ihr Team von CyberXperts

Andreas Hessel
Chief Information Security Officer

Naomi Meier
Senior Sales Managerin

Es geht um Gold ... viel Gold !

Executive Summary: Die Cybercrime-Welt in Zahlen & Fakten

Sie können sich Cyber-Kriminelle wie Golddiebe vorstellen.

Gold, das sind die Daten Ihres Unternehmens. Selbst kleinste Datenschnipsel sind wertvoll, und sei es nur, weil diese einen Wert für das Opfer haben und es bereit ist, für das Entschlüsseln Lösegeld zu zahlen (sogenannte Ransomware).

Eines der häufigsten Einfallstore für die Diebe ist „Phishing".

Phishing ist oft der Startpunkt für schlimme Angriffe auf Unternehmensdaten und personenbezogene Informationen von beispielsweise Beschäftigten und Kunden, aber auch Geschäftsgeheimnisse..

Und so funktioniert Phishing:

Sie erhalten eine täuschend echt aussehende E-Mail, angeblich von Behörden, Banken, Software-Programmen oder Online-Shops. Diese ist so formuliert und gestaltet, dass Sie sich unter Druck gesetzt fühlen. Um Schaden oder Ärger zu vermeiden, sollen Sie eine Datei öffnen oder sich auf einer gefälschten Website mit Ihren Benutzerdaten anmelden. Es geht etwa um eine Rechnung, einen Antrag oder einen

Fragebogen. Öffnen Sie den Anhang, wird Ransomware installiert. Diese bösartige Software (Malware) verschlüsselt im Hintergrund alle erreichbaren Daten. Nur gegen Zahlung eines „Lösegelds“ soll das Unternehmen die Informationen zur Entschlüsselung seiner Daten erhalten.

Phishing war 2021 Haupteinfallstor für Kriminelle, um Login-Daten, Banking-Informationen zu erhaschen oder Schadsoftware zu platzieren. Die erbeuteten Daten werden dann im Darknet verkauft und gehandelt.[5] Die Angriffe steigen in den letzten Jahren rasant an und sind spätestens seit der Corona-Pandemie eine außerordentliche Bedrohung für Unternehmen.

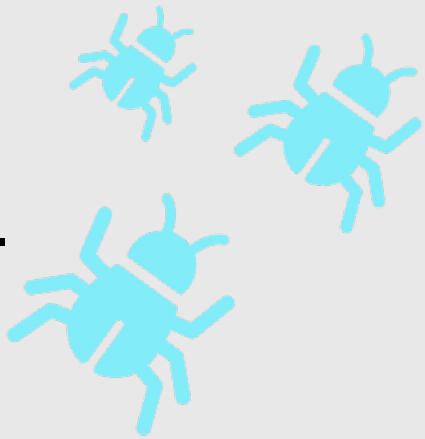
Durch die Pandemie nahm die Nutzung von digitalen Angeboten noch einmal stark zu – sowohl im privaten Bereich als auch beruflich. Cyberkriminelle nutzten diese Verlagerung in die digitale Welt in Verbindung mit den aufkommenden Ängsten und Verunsicherungen der Menschen aus, um vermehrt Angriffe zu streuen.[6]

14,8 Millionen

Meldungen über eine

Schadsoftware-Infektion

gingen 2021 beim BSI ein[7]



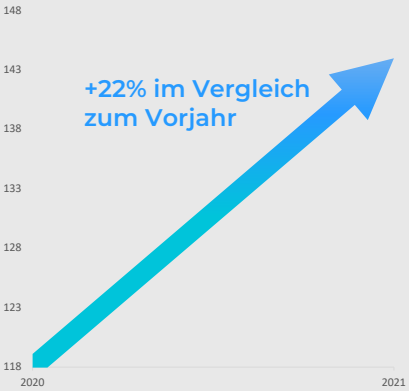
5 BKA, Bundeslagebericht Cybercrime 2021, 05.07.2022, abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

6 BKA, Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie, 12.07.2022, Abrufbar unter: file:///C:/Users/ag/Downloads/cybercrimeSonderauswertungCorona2019.pdf

7 BSI, „Die Lage der IT-Sicherheit in Deutschland 2021“, 24.08.2022, https://www.bsi.bund.de

Vom BSI geprüfte Systeme 2021[8]

Schadprogramm-Varianten 2021



144 Millionen
neue Varianten 2021[9]

8 BSI, „Die Lage der IT-Sicherheit in Deutschland 2021“, 24.08.2022, https://www.bsi.bund.de.

9 Bitkom e.V., Wirtschaftsschutzbericht 2021, 05.08.2021, https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf.

Goldenes Zeitalter für Hacker: So einfach häufen sie gigantische Vermögen an …

Ransomware ist die Hauptbedrohung 2021 im Bereich Cyberkriminalität. Im Vergleich zu den Vorjahren ist das Schadenspotential 2021 noch einmal stark angestiegen.[10]

Der entstandene weltweite Gewinn nur durch Ransomware-Zahlungen für die Hacker betrug 2021 **602 Millionen US-Dollar (!)**, wobei von einer hohen Dunkelziffer der tatsächlichen Gewinne der Cyber-Kriminellen auszugehen ist.

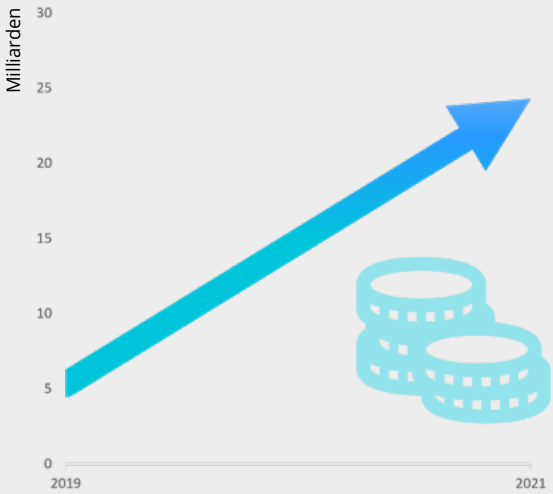
Auch die Anzahl der aktiven Ransomware-Gruppierungen hat in den letzten Jahren stetig zugenommen. Die Gruppierungen selbst sind immer nur wenige Monate aktiv und kommen dann unter einem neuen Namen zurück. So wird eine Nachverfolgung der Täter schwierig und es entsteht der Eindruck, dass viele unterschiedliche Gruppen aktiv sind. Laut Bundeskriminalamt liegt die **Aufklärungsquote für Cybercrime-Straftaten bei nur knapp unter 30 %** und ist zum Vorjahr rückläufig.[11]

Insgesamt ist 2021 ein Anstieg von Cybercrime-Delikten in Deutschland von 12,2 % zum Vorjahr zu verzeichnen. Die Anonymisierung im Netz, aufwendige und umfangreiche Ermittlungsarbeiten und Gruppierungen aus dem Ausland machen die Arbeit herausfordernd.[12]

War auch Ihr Unternehmen schon einmal von einem Cyber-Angriff betroffen? Machen Sie jetzt einen 360°-Check Ihrer Sicherheitslage mit CyberXperts. Vereinbaren Sie gerne ein persönliches Strategie-Beratungsgespräch – inklusive Live-Demo.

10 BKA, Bundeslagebericht Cybercrime 2021, 05.07.2022, abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html
11 Chainalysis, Crypto Crime Report 2022, 05.07.2022, abrufbar unter: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/
12 BKA, Bundeslagebericht Cybercrime 2021, 05.07.2022, abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.

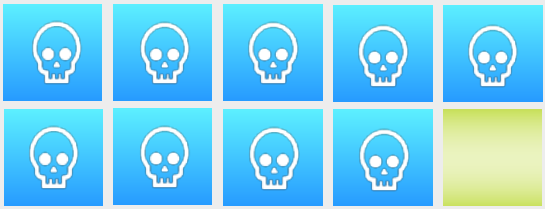
Jährlicher Schaden durch Ransomware[13]



2021:
24,3 Milliarden in Deutschland

Der Schaden hat sich innerhalb von 2 Jahren verfünffacht

2021 waren 86% der Unternehmen von Cyberangriffen betroffen[13]



13 Studie: Bitkom e.V., Wirtschaftsschutzbericht 2021, 05.08.2021, https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf.

Das Who's Who der prominenten Opfer – Das sind die Top-10 der erfolgreichsten Cyber-Attacken

Große Konzerne, Behörden und Einrichtungen der sogenannten kritischen Infrastrukturen (KRITIS) rücken immer öfter ins Visier der Cyber-Kriminellen. Doch oft sind gerade dort die Schäden auch massiv. Jeder von uns kennt die Massenaufrufe nach dem Hack von E-Mail-Providern oder Sozialen Netzwerken, seine E-Mail-Adresse auf z. B. https://haveibeenpwned.com/ zu überprüfen. Dabei ist der Höhe der Schäden nach oben keine Grenze gesetzt. Ein paar Beispiele:

Die Top 10 der schädlichsten Cyber-Attacken:

1. 2013 wurde der Internet-Dienst Yahoo Opfer einer Attacke. 3 Mrd. Nutzerkonten waren betroffen. Die Hacker stahlen Daten von circa 1 Mrd. Nutzern, dabei u. a. E-Mail-Adressen, Telefonnummern und unkenntlich gemachte Passwörter.[14]
2. Die bekannte US-Fastfood-Kette Wendys erwischte es im Jahr 2016. Mehr als 1.000 Restaurants waren betroffen und die Angreifer erbeuteten mithilfe von Malware Kreditkarteninformationen der Kunden. Die Malware wurde erst nach einiger Zeit entdeckt und richtete vermutlich schon seit Monaten Schaden im Unternehmen an.[15]
3. 2013 traf Adobe eine Attacke. Schätzungsweise 38 Millionen Kunden waren betroffen. Es wurden Daten der Opfer gestohlen, z. B. Passwörter und Nutzernamen der Adobe Programme.[16]
4. Im Mai 2021 wurde die US-Firma Colonial Pipeline angegriffen, eine der größten Ölversorger in den USA. Es kam zu Ausfällen und Versorgungsschwierigkeiten.[17]

14 SZ, Hackerangriff bei Yahoo traf alle drei Milliarden Konten, 07.07.2022, abrufbar unter: https://www.sueddeutsche.de/digital/yahoo-hackerangriff-bei-yahoo-traf-alle-drei-milliarden-konten-1.3693671.
15 BBC, Food chain Wendy's hit by massive hack, 07.07.2022, abrufbar unter: https://www.bbc.com/news/technology-36742599.
16 Welt, Adobe Hackerangriff betrifft 38 Millionen Kunden, 07.07.2022, abrufbar unter: https://www.welt.de/wirtschaft/article121368277/Adobe-Hackerattacke-betrifft-38-Millionen-Kunden.html.
17 BKA, Bundeslagebericht Cybercrime 2021, 05.07.2022, abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.

5. 30 Mio. Nutzerdaten eines US-amerikanischen Mobilfunkanbieters wurden 2021 im Darknet angeboten und für eine Preis von 6 Bitcoin, damals etwa 240.000 Euro.[18]
6. 50 Millionen Dollar bei Acer. Schon der zweite Angriff auf das Tech-Unternehmen Acer nach einer Ransomware-Attacke im März 2021, nachdem Kriminelle Server geknackt und Daten gestohlen haben. Die Kriminellen wollten 50 Millionen Dollar Lösegeld für die Daten.[19]
7. Bei einem Angriff auf Kaseya, einem US-amerikanischen IT-Dienstleister, über vermeintliche Software-Updates, gelangten die Kriminellen an Informationen und konnten Schadsoftware platzieren. Die Software verschlüsselte Daten auf den Computern, sodass diese nicht mehr einsatzbereit waren. Da Kaseya als IT-Dienstleister mehrere Kunden betreut, waren u. a. auch eine Supermarktkette in Schweden und deutsche Firmen betroffen. Das Lösegeld umfasste 70 Millionen Dollar![20]
8. Fast 2.400 Daten von Accenture wurden bei einem Hackerangriff im August 2021 veröffentlicht. Die Angreifer drohten mit weiteren Attacken und forderten Lösegeld.[21]
9. In Anhalt-Bitterfeld erlitt die Kreisverwaltung im Juli 2021 einen Angriff und der Cyber-Katastrophenfall wurde erstmals in Deutschland festgestellt. Öffentlicher Dienstleistungen mussten eingeschränkt werden und monatelang war der Normalbetrieb außer Kraft.[22]
10. Im August 2021 kam es zu einem Angriff auf ein Krankenhaus in Sachsen-Anhalt, wodurch die Kommunikation des Klinikums zusammenbrach. Auch die IT konnte nicht fehlerfrei genutzt werden. Glücklicherweise war die medizinische Versorgung der Patienten nicht betroffen.[23]

18 BKA, Bundeslagebericht Cybercrime 2021, 05.07.2022, abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.
19 ZDnet, Acer confirms second cyberattack in 2021 after ransomware incident in March, 05.07.2022, Abrufbar unter: https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/.
20 Die Zeit, Professioneller erpresst denn je, 05.07.2022, abrufbar unter: https://www.zeit.de/2021/28/hackerangriff-kaseya-ransomware-erpressungssoftware-unternehmen-it-sicherheit.
21 BSI, Newsletter Sicher Informiert vom 26.08.2021, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Newsletter/DE/BuergerCERT-Newsletter/15_Sicher-Informiert_26-08-2021.html?nn=132646#doc964748bodyText3
22 BKA, Bundeslagebericht Cybercrime 2021, 05.07.2022, abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.
23 BKA, Bundeslagebericht Cybercrime 2021, 05.07.2022, abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.

Raffiniert und skrupellos wie nie: Wieso Phisher aktuell so erfolgreich sind

Kriminelle Cyber-Gruppen nutzen aktuelle Trends, politische Ereignisse und die Grundbedürfnisse der Menschen aus, um Ihre Kampagnen erfolgreich zu machen.

Dabei wird zum Beispiel ein zeitlicher Druck aufbaut („*Ihr Konto wird nach 2 Stunden gesperrt*“) oder mit Gewinnen oder Anreizen geworben („*Wir schenken Ihnen jetzt 500 €*“).

Dabei sehen die Mails meist täuschend echt aus und sogar die Absender scheinen bekannt zu sein. Doch in Wahrheit werden diese nur verschlüsselt und dahinter stecken Kriminelle.

Aktuelle Themen als Aufhänger für eine Phishing-E-Mail

Ein Beispiel: Seit 2018 aktualisieren Unternehmen ständig ihre Datenschutzrichtlinien und weisen Nutzer häufig per E-Mail darauf hin.


Hallo [redacted]

Ihre Mithilfe ist erforderlich!

Die neuen Datenschutzgesetze verpflichten uns nun dazu, in regelmäßigen Abständen die Konten unserer Kunden zu überprüfen. Dies dient ausschließlich zu Ihrer eigenen Sicherheit, da in der Vergangenheit immer mehr Vorfälle von Benutzung verschiedener Kundenkonten durch unbefugte Personen entstanden sind.

Um daher wie gewohnt weiterhin Ihr Konto bei uns nutzen zu können, ist Ihre aktive Mitwirkung erforderlich. Dies wird vom Gesetzgeber so verlangt.

Nachdem Sie sich über den Bestätigungsbutton angemeldet haben, werden Ihnen detailiert alle weiteren notwendigen Schritte erklärt.

Bestätigen

Bei Missachtung oder Verweigerung ist ganz klar eine Schließung des Kundenkontos vorgesehen. Der Gesetzgeber fordert in so einem Fall dazu auf.

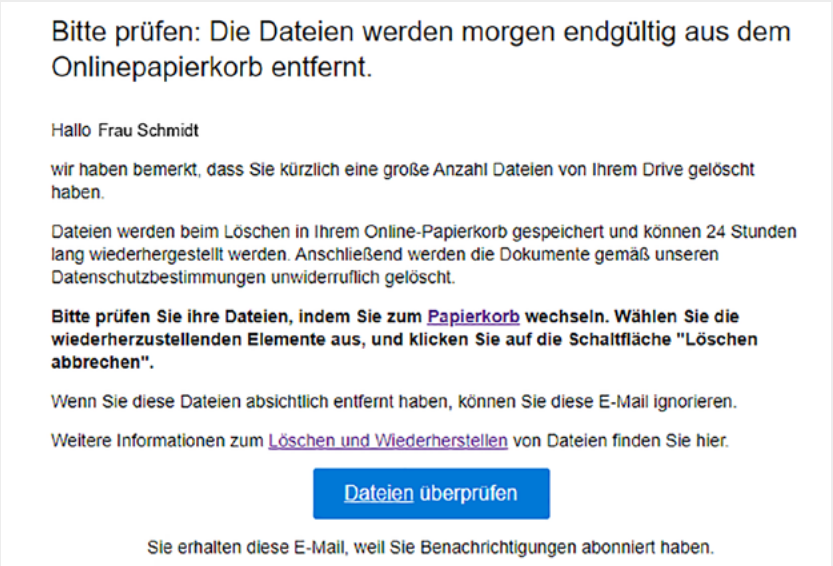
Vielen Dank im voraus für Ihre Mitwirkung und Ihr Verständnis!

Mit freundlichen Grüßen
Ihr PayPal Kundensupport

E-Mails wie diese haben eine hohe Klickerquote, denn: Der Absender ist bekannt, das Anliegen erscheint plausibel, die Dringlichkeit ist hoch. (Bildquelle: https://verbraucherzentrale.de)

Dies machen sich auch Angreifer zu Nutze: Mit gefakten E-Mails bringen sie die Leser dazu, neue Nutzungsbedingungen zu akzeptieren oder Kontodaten zu bestätigen.

So werden vermehrt E-Mails vom vermeintlichen Absender Paypal genutzt, um Opfer zu ködern. Sie sollen Ihre Daten bestätigen. Doch in Wirklichkeit verbirgt sich dahinter ein Betrug.



Bitte prüfen: Die Dateien werden morgen endgültig aus dem Onlinepapierkorb entfernt.

Hallo Frau Schmidt

wir haben bemerkt, dass Sie kürzlich eine große Anzahl Dateien von Ihrem Drive gelöscht haben.

Dateien werden beim Löschen in Ihrem Online-Papierkorb gespeichert und können 24 Stunden lang wiederhergestellt werden. Anschließend werden die Dokumente gemäß unseren Datenschutzbestimmungen unwiderruflich gelöscht.

Bitte prüfen Sie ihre Dateien, indem Sie zum Papierkorb wechseln. Wählen Sie die wiederherzustellenden Elemente aus, und klicken Sie auf die Schaltfläche "Löschen abbrechen".

Wenn Sie diese Dateien absichtlich entfernt haben, können Sie diese E-Mail ignorieren.

Weitere Informationen zum Löschen und Wiederherstellen von Dateien finden Sie hier.

Dateien überprüfen

Sie erhalten diese E-Mail, weil Sie Benachrichtigungen abonniert haben.

E-Mails, die wie hier der Standard-Kommunikation von Microsoft nachempfunden sind, lassen sich im Eifer des Gefechts kaum vom Original unterscheiden.

„Ihr Kollege Herr Schmitz hat eine Datei mit Ihnen geteilt“

Microsoft wird in vielen Unternehmen als Standard genutzt und die Kommunikationslösung Microsoft Teams ist beliebt. Auch das nutzen Angreifer aus.

So versenden sie beispielsweise Mails mit der Aufforderung, eine von einem vermeintlichen Kollegen geteilte Datei zu öffnen oder sich mit den Kontodaten einzuloggen, weil das Konto sonst gesperrt werden würde.

Auch sehr beliebt, weil einer echten E-Mail nachempfunden: *„Bitte prüfen: Die Dateien werden morgen endgültig aus dem Onlinepapierkorb entfernt.“*

Dramatische Folgen: Von lahmgelegten Krankenhäusern über Trinkwasser-Vergiftung bis hin zu Wahl-Manipulation

Von reiner Geldgier über Industriespionage bis hin zur Verfolgung politischer Ziele: Die Motivationen der Täter sind vielseitig.

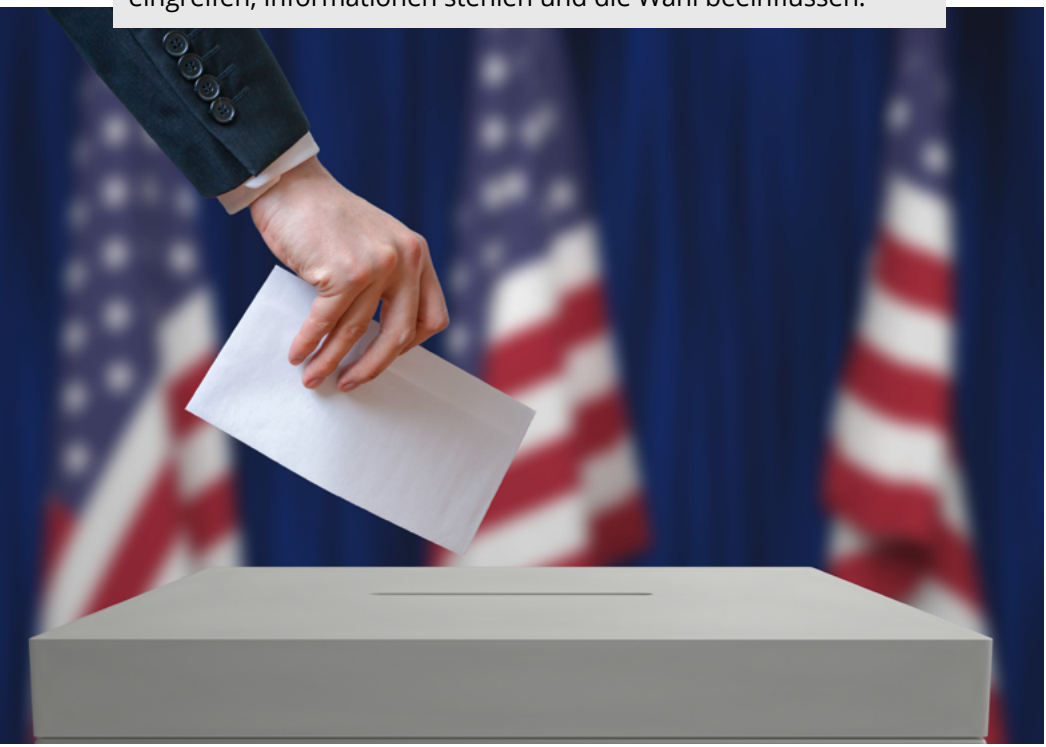
Wie dramatisch die Folgen erfolgreicher Cyber-Angriffe sein können, zeigte erst kürzlich die **Attacke auf das Klinikum Fürstenfeldbruck**. Diese begann mit einer Phishing-E-Mail und legte den Klinikbetrieb phasenweise völlig lahm – zum Glück waren Menschenleben nicht gefährdet.[24]

Auch der **Angriff auf die Trinkwasserversorgung** eines Versorgers im US-Bundesstaat Florida nahm in Kauf, Menschen zu schädigen.[25]

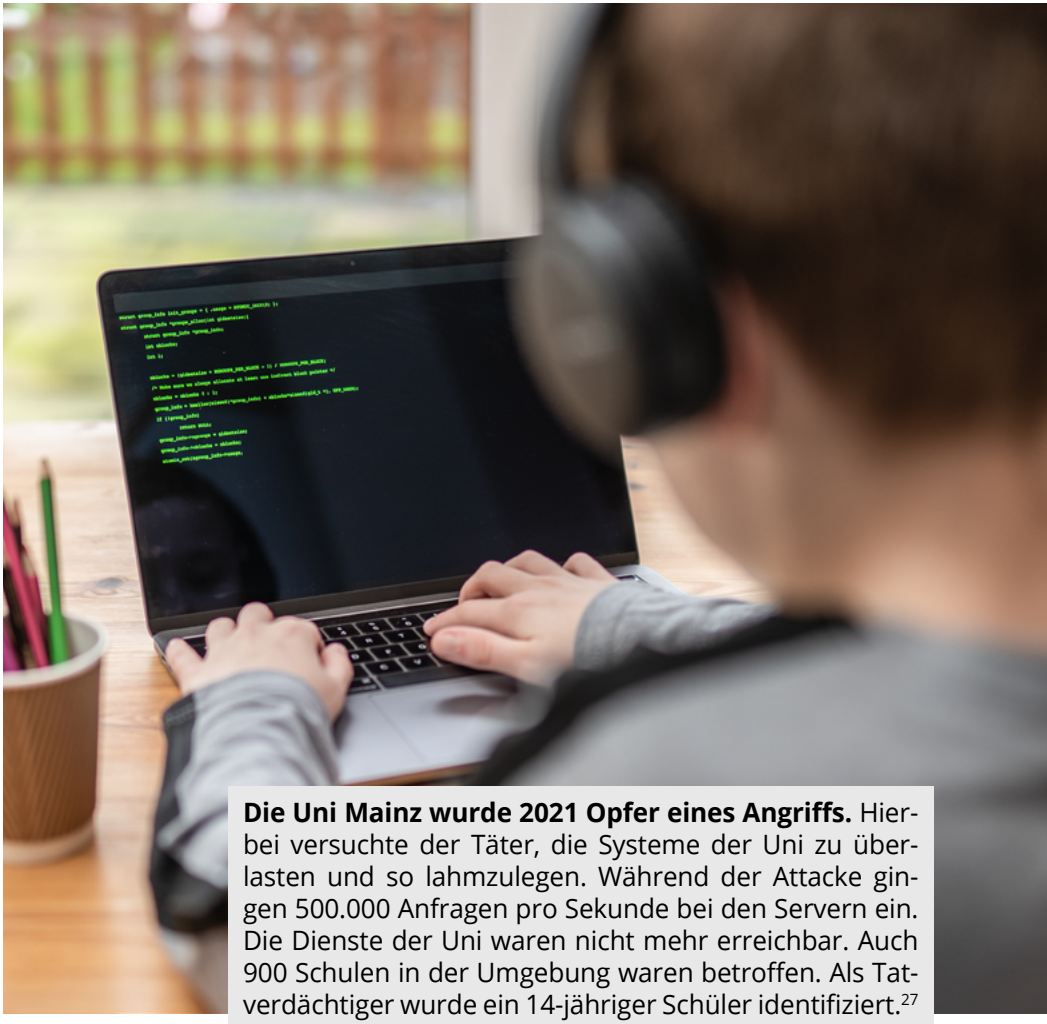
24 Heise, Fürstenfeldbruck: Malware legt Klinikums-IT komplett lahm, 06.07.2022, abrufbar unter: https://www.heise.de/newsticker/meldung/Fuerstenfeldbruck-Malware-legt-Klinikums-IT-komplett-lahm-4223573.html.

25 SZ, Wenn die Trinkwasserversorgung gehackt wird, 06.07.2022, abrufbar unter: https://www.sueddeutsche.de/digital/it-sicherheit-hacker-wasserwerk-florida-1.5205113.

Im **US-Wahlkampf** gab es den Versuch, an interne Informationen zu gelangen. So erhielten Parteikollegen der damals kandidierenden Hillary Clinton sogenannte Spear-Phishing-E-Mails mit dem Hinweis auf eine Passwortänderung. Bei einem Spear-Phishing-Angriff werden die Betroffenen im Vorfeld meist wochenlang beobachtet und es werden Informationen über die Opfer gesammelt. Dadurch sind die Angriffe noch gezielter und gefährlicher. So wollten Angreifer in diesem Fall die Postfächer der Clinton-Anhänger eingreifen, Informationen stehlen und die Wahl beeinflussen.[26]



26 SZ, Das waren die spektakulärsten Hackerangriffe, 06.07.2022, abrufbar unter: https://www.sueddeutsche.de/digital/it-sicherheit-das-waren-die-spektakulaersten-hackerangriffe-1.4960052.



Die Uni Mainz wurde 2021 Opfer eines Angriffs. Hierbei versuchte der Täter, die Systeme der Uni zu überlasten und so lahmzulegen. Während der Attacke gingen 500.000 Anfragen pro Sekunde bei den Servern ein. Die Dienste der Uni waren nicht mehr erreichbar. Auch 900 Schulen in der Umgebung waren betroffen. Als Tatverdächtiger wurde ein 14-jähriger Schüler identifiziert.[27]

27 BSI, Die Lage der IT-Sicherheit in Deutschland 2021, 06.07.2021, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

Neue Trends: Diese fiesen Methoden machen Hacker fast unbesiegbar … und führen zu Rekord-Schäden

Neben klassischen Lösegeldforderungen für verschlüsselte Daten werden Hacker immer kreativer bei der Auswahl ihrer Methoden. Auch Schweigegeld-Erpressung oder Schutzgeld-Erpressung ist im Trend.

„Double Extortion“: So wird das Opfer doppelt abgezockt

Bei Double-Extortion-Angriffen wollen die Kriminellen gleich doppelt Gewinn machen. Sind sie einmal erfolgreich an die Daten gekommen, können sie diese im Darknet versteigern. Doch damit nicht genug: Zunächst werden die Opfer aufgefordert, ein Schweigegeld zu zahlen um so eine Veröffentlichung zu verhindern. In der Regel handelt es sich hierbei um sensible Daten, Geschäftsgeheimnisse oder Innovationen. Ob diese nach einer Zahlung nicht veröffentlicht wurden, kann jedoch meist nicht nachvollzogen werden.[28]

DDoS: So einfach legen Hacker komplette Server lahm

Bei einem Distributed-Denial-of-Service-Angriff (DDoS) versuchen Angreifer die Website oder Server zu sperren, indem sie diese überlasten. Zurzeit ist auch ein kombinierter Angriff von Ransomware und DDoS beliebt, um die Opfer doppelt zu schädigen. So gelangen die Täter an die Daten des Unternehmens und sperren gleichzeitig Webpräsenzen oder Server, was eine Wiederherstellung der verlorenen Dateien erschwert.

28 BSI, Die Lage der IT-Sicherheit in Deutschland 2021, 06.07.2021, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

So laden sich Kriminelle fertige Schadprogramme aus dem Netz – und greifen SIE dann an

Wussten Sie, dass für eine erfolgreiche Phishing-Attacke nicht mehr als eine Google-Suche nötig ist? Jeder kann sich im Darknet ein „schlüsselfertiges“ Phishing-Kit kaufen.

Das geht so problemlos wie Online-Shopping. „Access-as-a-Service“ (AaaS) ist ein neues Geschäftsmodell innerhalb der Underground Economy. Hierbei werden angriffsfertige Lösungen verkauft. Die Underground Economy ist die Gesamtheit der Plattformen, die von Cyberkriminellen zum Austausch genutzt werden und ist damit Basis für viele Straftaten.

Service	Preis in US $ (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner		
▪ Desktop-Version	1.000 - 10.000 $	bei Kauf
▪ Mobile-Version	1.000 - 10.000 $	bei Kauf
RAT (Remote Administration Tool)	60 - 530 $ ca. 3.000 $	pro Monat bei Miete bei Kauf
Mining Bots	50 – 150 $	pro Monat bei Miete
Crypting	0 - 100 $ 30 - 500 $	bei Kauf von einem Crypt bei einem Wochen-Abo mit 50 Crypts pro Tag
DDoS-as-a-Service	80 - 1.500 $	pro Monat bei Miete
Bulletproof Hosting		
▪ Shared	5 - 50 $	pro Monat bei Miete
▪ Dedicated	50 - 700 $	pro Monat bei Miete
Counter-AV-Service	10 $	pro Monat und 300 Scans
Infection-on-Demand (Phishing-Services o.ä.)	Ab 100 $	pro Monat
Stealer Logs	5 -15 $ 400 – 900 $	pro Stück pro Monat für Abonnement

Fertige Hacking-Tools sind erschreckend günstig und machen den Aufwand für den Angreifer überschaubar. (Quelle: BKA, Bundeslagebild Cybercrime 2021)

Üble Folge:

Die Hürden für Internetkriminalität sind dadurch extrem niedrig geworden.

Das bedeutet: Ihre Mitarbeiter werden dadurch fast zwangsläufig über kurz oder lang mit einem Cybervorfall konfrontiert.

78 % der Unternehmen waren 2021 Opfer von Ransomware-Attacken per E-Mail.[29]

So wie im Beispiel oben mit der Login-Seite für Microsoft 365.

Der Grat zwischen einer teuren Ransomware-Infektion und einem Mitarbeiter, der sich von vornherein sagt: *„Diese E-Mail sieht verdächtig aus, also habe ich sie nicht geöffnet."* ist schmal. Doch wer garantiert, dass jeder einzelne dann genau richtig reagiert? Wie ist gewährleistet, dass solche Phishing-Versuche an Ihre IT-Abteilung gemeldet werden?

Die Mitarbeiter sind Ihre wichtigsten Verbündeten im AbwehrKampf gegen Hacker

Immer mehr Unternehmen setzen deshalb sogenannte **Awareness-Kampagnen** auf (zu Deutsch: Sensibilisierung), um zu erreichen, dass ihre Mitarbeiter – die bei Phishing ja der Schlüssel zu einer wirksamen Gefahrenabwehr sind – jederzeit richtig auf Phishing-Angriffe reagieren.

Dabei holen sie sich in der Regel professionelle Hilfe, damit die Awareness-Kampagne auch wirklich ihr Ziel erreicht.

Denn welcher IT-Manager verfügt schon über ein umfangreiches Wissen auf dem Level eines Hackers – um z. B. eine Phishing-Kampagne zu simulieren?

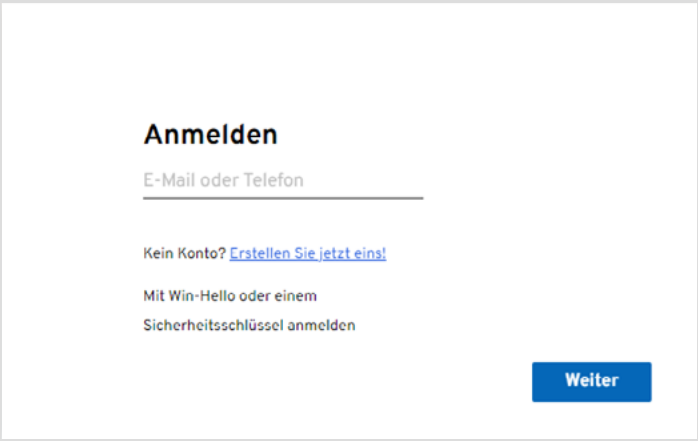
Unsere Empfehlung: Lassen Sie sich einmal professionell zu Ihrer Strategie und zum Aufsetzen einer Awareness-Kampagne mit Cyber-Xperts beraten.

Garantie: Das Erstgespräch ist **kostenlos** und nicht mit einer Kaufverpflichtung verbunden. Klicken Sie einfach hier, um Ihr unverbindliches Gespräch zu vereinbaren.

29 Proofpoint, State of the Phish Bericht 2022, 06.07.2022, Abrufbar unter: State of The Phish-Bericht 2022 | Proofpoint DE.

Was können Sie mit CyberXperts erreichen?

Mit CyberXperts eignen sich Ihre Mitarbeiter ganz bequem von zu Hause aus oder im Büro all die Kenntnisse an, mit denen sie bei verdächtigen Mails, Webseiten oder Angeboten sofort sagen: „*Halt, Stopp!*"



Mit den Spezial-Schulungen von CyberXperts erfahren Mitarbeiter, woran sie Phishing-Angriffe zuverlässig erkennen. Da Ihre Mitarbeiter an vorderster Front in der Gefahrenabwehr stehen, reduzieren Sie so die Gefahren für Ihr Unternehmen deutlich.

Alle Beschäftigten entwickeln dadurch **ein unterbewusstes Alarmsystem**, durch das sie schon kleinste Ungereimtheiten oder Abweichungen wie eine falsche URL oder E-Mail-Adresse erkennen.

Und zwar **BEVOR sie Zugangsdaten eingeben**, die sofort in die Hände von Hackern fallen.

Wieso die Methode von CyberXperts so wirksam ist?

Grund Nr. 1: Mitarbeiter nehmen gerne an Schulungen teil, wenn sie das Gefühl haben, darin etwas Nützliches zu lernen.

Natürlich hat in der Regel jeder schon einmal etwas von Phishing gehört. Aber etwas anderes ist es, wenn man selbst einmal auf eine Hacker-Masche reingefallen ist.

Deshalb steht am Anfang einer Awareness-Kampagne mit CyberXperts auch immer eine simulierte Phishing-Kampagne.

Die Mitarbeiter erleben so am eigenen Leibe, wie leicht sogar die klügsten Köpfe darauf heutzutage hereinfallen (es ist eben nicht mehr der nigerianische Prinz, der uns hier schreibt – die E-Mails sind tausendfach einfallsreicher und glaubwürdiger).

Später werden in regelmäßigen Abständen weitere Phishing-E-Mails versendet.

Grund Nr. 2: Mitarbeiter verstehen, dass sie selbst von ihrem neuen Wissen profitieren.

„Auf eine falsche E-Mail würde ich nie und nimmer hereinfallen!" – das würden zumindest die meisten von sich behaupten.

Mitarbeiter sind überrascht, wie trickreich E-Mails sein können und wie viel sie selbst dagegen tun können – auch privat. Mitarbeiter sind in der Regel dankbar, wenn sie an Cybercrime-Schulungen teilnehmen dürfen und dabei konkrete Tipps erhalten, wie sie bei der Gefahrenabwehr mithelfen können.

Fazit: Machen Sie einfach hier Ihren Termin für ein unverbindliches Stra-tegie-Beratungsgespräch aus. Es ist kostenlos und ein wichtiger Schritt hin zu mehr Sicherheit.

Fokus: So groß ist die Gefahr in Ihrer Branche

Cybercrime betrifft jeden – ob Privatperson oder Unternehmen, ob Einzelhandel oder Finanzwesen. Jede Branche steht unter der Gefahr, zu jeder Minute angegriffen zu werden. Einige Branchen haben besondere Herausforderungen zu meistern und sind extrem beliebt bei Angreifern, weil sie über Informationen oder Daten verfügen, die für Cyber-Kriminelle sehr lukrativ sein können.

Öffentliche Verwaltung: Ein gefundenes Fressen für die Angreifer

In Sassnitz haben Angreifer die komplette E-Mail-Kommunikation der Stadt lahmgelegt, weil sie das System übernahmen und darüber Phishing-E-Mails an Bürger verschickten. In Wismar wurden Strukturen der IT durch einen Ransomware-Angriff verschlüsselt. In Schwerin mussten Systeme durch Backups wiederherstellt werden, weil auch dort Server angegriffen wurden.[30]

Gerade die öffentliche Verwaltung litt schwer unter den Cyber-Attacken im Jahr 2021. Behörden verwalten riesige Mengen personenbezogener Daten wie Adressen der Bürger, Religionszugehörigkeit, Gesundheitsdaten und vieles mehr, die in höchsten Maßen schützenswert sind.

Doch gerade Behörden müssen häufig mit veralteten Systemen arbeiten und die IT-Infrastruktur ist nicht auf dem neusten Stand. Dadurch sind sie schlecht gegen Angriffe von außen geschützt.[31]

30 BKA, Bundeslagebericht Cybercrime 2021, 05.07.2022, abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.

31 Handelsblatt, Erster Cyber-Katastrophenfall in Deutschland – Landkreis lahmgelegt, 06.07.2022, abrufbar unter: https://www.handelsblatt.com/politik/deutschland/hackerangriff-erste-cyber-katastrophenfall-in-deutschland-landkreis-lahmgelegt/27409824.html.

Finanzsektor: Das Geld an der Quelle abschöpfen

Banken verwalten nicht nur unser Geld, sondern haben auch immense Mengen an sensiblen Daten über Bürger und Unternehmen inne. Auch spielen sie eine zentrale Rolle in einer funktionierenden Wirtschaft und sind daher Dreh- und Angelpunkt für viele Transaktionen. **Das macht sie für Angreifer und Kriminelle doppelt attraktiv.**

Leider hat die Finanzbranche noch ein weiteres Problem:

Die komplette IT-Infrastruktur hängt von nur wenigen IT-Dienstleistern ab oder ist in einer Cloud.

Wird dann nur einer dieser Dienstleister angegriffen, hat es verheerende Folgen für viele Banken.

Und nicht nur Banken spüren die Auswirkungen: Durch Ausfall der Technik können auch Geschäfte und Transaktionen nicht durchgeführt werden und der gesamte Finanzsektor sowie die Bürger spüren die Nachwirkungen.[32]

Im Juni 2021 hat eine Attacke 800 Volksbanken getroffen. Die Rechenzentren des IT-Dienstleister der Banken wurde mit einem DDoS-Angriff an zwei Standorten attackiert, wodurch die IT lahmgelegt wurde. Sowohl die Website als auch die Onlinebanking-Portale der Banken waren stillgelegt und Kunden konnten die Services nicht mehr nutzen.[33]

32 Bundesverband Deutscher Banken, Wie sich Deutschlands Banken gegen Cyberkriminalität rüsten, 07.07.2022, abrufbar unter: https://bankenverband.de/newsroom/reden_und_interviews/wie-sich-deutschlands-banken-gegen-cyberkriminalitat-rusten/.

33 Golem, DDos-Angriff legte Onlinebanking bei Volksbanken lahm, 07.07.2022, abrufbar unter: https://www.golem.de/news/fiducia-ddos-angriff-legt-onlinebanking-bei-volksbanken-lahm-2106-157040.html .

Hacker-Spielwiese Einzelhandel

Auch der Einzelhandel bleibt von den Cyber-Gruppierungen nicht verschont. In 2021 sind die Angriffe auf Einzelhändler um 13% gestiegen. Insbesondere das Saisongeschäft um Weihnachten herum ist ein beliebtes Ziel, um Lieferschwierigkeiten auszulösen.[34]

Auch vor den Verkaufstagen „Black Friday" und „CyberMonday" steigen die DDos-Angriffen stark an, so berichtet das BSI.[35]

Apetito, einer der führenden Hersteller von Tiefkühl-Lebensmitteln und Kantinenmahlzeiten, wurde im Juni 2022 Opfer eines weitreichenden Angriffs. Dadurch fiel die komplette IT aus, die normalerweise die Verteilung von Essen auf Kantinen, Kliniken und Seniorenheime verwaltet. Mitarbeiter mussten dieses händisch zuordnen und ausliefern.[36]

34 IT-Daily, Hacker greifen in 2021 vermehrt Einzelhändler an, 15.07.2022, Abrufbar unter: https://www.it-daily.net/it-sicherheit/cybercrime/hacker-greifen-in-2021-vermehrt-einzelhaendler-an.
35 BSI, DDoS-Entwicklungen vor Black Friday und Cyber Monday, 07.07.2022, abrufbar unter https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-269757-1032.html.

Die Firma apetito informiert transparent und professionell über den Cyberangriff. (Bildquelle: www.google.de)

36 Tagesschau, Cyberangriff legt Essensdienst Apetito lahm, 07.07.2020, Abrufbar unter: https://www.tagesschau.de/wirtschaft/unternehmen/cyberangriff-apetito-essenslieferungen-101.html.

Produktion: Lieblingsopfer von Spionen und politischen Aktivisten

Auch das produzierende Gewerbe ist betroffen. Verstärkte Digitalisierung in der Produktion und globale Vernetzung steigern das Potenzial für Cyber-Attacken.

Dabei lag der Fokus der neuen Technologien hauptsächlich auf einer höheren Performance und selten auf IT-Sicherheit.

Da die Systeme meist sehr speziell auf die Produktion zugeschnitten sind, werden sie von Spezialisten und nicht von IT-Fachkräften betrieben. Dadurch wird die Sicherheit häufiger vernachlässigt.[37]

Auch stehen die Gewerbe oft in Zusammenhang mit der Politik, sodass bei einem Angriff nicht nur finanzielle, sondern auch politische Ziele verbunden sein können.

Zwei Beispiele:

In Bayern lag die Produktion des Traktorherstellers Fendt für einige Zeit still, nachdem sich Hacker mit einer Ransomware-Attacke Zugriff auf den Mutterkonzern verschafft hatten.[38]

Ein Tochterunternehmen des weltweit größten Fleischkonzerns JBS aus Brasilien war ebenfalls Opfer eines Angriffs, was Auswirkungen auf die Produktion hatte. Insgesamt wurden Teile des Unternehmens in Nordamerika und Australien gehackt. Mehrere Betriebe mussten Ihre Arbeit stilllegen, bis die Schäden der Attacke behoben sind. Es kam auch zu Lösegeldforderungen.[39]

37 Deloitte, Global Cyber Executive Briefing, 07.07.2022, abrufbar unter: https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/Manufacturing.html.
38 SZ, Hacker legt Produktion bei Fendt lahm, 07.07.2022, abrufbar unter: https://www.sueddeutsche.de/bayern/fendt-traktor-bayern-marktoberdorf-allgaeu-hacker-1.5581239.
39 Tagesschau, Cyber-Angriff auf weltgrößten Fleischkonzern, 07.07.2022, abrufbar unter: https://www.tagesschau.de/ausland/amerika/cyber-attacke-auf-brasilianischen-fleischkonzern-101.html.


Smart Industrial Control System
Dashboard
Overview
Product report
Performance
Product Quality
Machine State
32.04%
99%
25%
67%
Fine

7 Todsünden & Co.: Diese psychologischen Faktoren nutzen Hacker gnadenlos aus

Auch wenn die klassischen 7 Todsünden eher in der Morallehre des Mittelalters populär waren und inzwischen nicht mehr als strafwürdige Sünde gesehen werden:

Sie haben als menschliche Antreiber auch heute noch 100 % Gültigkeit.

Denken Sie nur an Werbeslogans wie diese:

„Weil ICH es mir wert bin“ (Hochmut)

„Geiz ist Geil“ (Habgier)

„Für das Beste im Mann“ (Wollust)

„Das Kinn von Opa, die Augen von Papa, HIV von Mama“ (Zorn)

„Holen Sie sich was Ihnen zusteht“ (Völlerei)

„Mein Auto, mein Haus, mein Boot“ (Neid)

„Red Bull verleiht Flügel!“ (Trägheit)

Doch auch Hacker bedienen sich dieser menschlichen Bedürfnisse. Obwohl über diese Beispiele viel berichtet und aufgeklärt wurde, funktionieren sie immer noch:

Wer von uns hat nicht schon einmal das Angebot „*Kredite ohne Schufa*“ erhalten? (Gier)

Oder das Versprechen, uns eine Provision dafür zu zahlen, dass wir fremdes Geld auf unserem Konto „*zwischenparken*“ (Gier).

Viele ältere Damen erhalten E-Mails von einem „*alten Geschäftsfreund ihres verstorbenen Mannes*“, der angeblich noch ausstehende Schulden überweisen möchte (Gier).

Auch auf sehr plumpe E-Mails mit Betreffs wie „*Ihr Gewinn*“ oder „*Ihre Sparkasse informiert*“ wird zuhauf reagiert (Gier)[40].

40 Quelle: CyberXperts-Datenbank.

Die persönliche Eitelkeit (Hochmut) sprechen Phisher z. B. mit „*Ihre Erfahrungen mit unserem Produkt*“ an.

Auch das Appellieren an unsere Hilfsbereitschaft, z. B. Hilfe für die Ukraine, triggert in unserem Inneren das sehr zufriedenstellende Gefühl „*Ich bin gut.*“ (Hochmut)

Im Business-Bereich ist eine sehr erfolgreiche Phishing-Betreffzeile: „*Der Vorstand lädt Sie zu einem Teams-Chat ein.*“ (Hochmut)

Darüber hinaus sind 2 der häufigsten durch Phishing-E-Mails angesprochenen Emotionen Neugier und Angst:

Die Büchse der Pandora: Wieso Neugier immer gewinnt – und den Angreifer reich macht!

In einer im März 2016 veröffentlichten Studie „*The Pandora Effect: The Power and Peril of Curiosity*“, über die *Die Welt* berichtete[41], zeigten US-Forscher, dass Probanden eher bereit waren, Schmerzen zu ertragen als ihre Neugier unbefriedigt zu lassen.

Konkret gaben sie in einem Versuch ihren Probanden Kugelschreiber, die Elektroschocks auslösten, wenn man auf sie klickte. Eine Gruppe erhielt mehrere Stifte, wobei die Stifte mit Elektroschock entsprechend markiert waren. Die andere Gruppe erhielt Kugelschreiber gänzlich ohne Markierung – ob sie also Elektroschocks verteilen würden oder nicht, war für den Studienteilnehmer nicht ersichtlich.

Das Ergebnis: 1.000 : 0 für die Neugier

Diejenigen, die Stifte gänzlich ohne Markierung erhalten hatten, klickten viel häufiger auf die Kugelschreiber. Um ihre Neugier zu stillen, nahmen sie Elektroschocks in Kauf. Für die andere Gruppe – wo die Stifte markiert waren – bestand kaum ein Anreiz, zu klicken, da sie ja wussten, welche Stifte Elektroschocks verteilen würden und welche nicht.

41 https://www.welt.de/gesundheit/article154834405/Darum-ist-Neugier-staerker-als-Angst.html.

In einem weiteren Experiment testeten die Forscher, ob sich die Neugier zügeln ließe, wenn die Studienteilnehmer gebeten würden, vorher über ihr Verhalten nachzudenken.

Und tatsächlich: **Die Reflektion über mögliche Konsequenzen führte dazu, dass der Neugier weniger häufig nachgegeben wurde.**

Für Sie bedeuten diese Erkenntnisse:

Wenn Sie Ihre Mitarbeiter dazu bringen, sich mit dem Thema Phishing auseinanderzusetzen, haben Sie gute Chancen, dass diese im Falle eines Angriffs ihre Neugier bändigen.

Zum Beispiel wenn E-Mails mit Betreffs wie diesen im Postfach landen:[42]

„Wir steigen um!“

„Änderung der Kontaktinformation“

„Wichtige Änderungen“

„Neue Aktivität in Teams“

Tipp: Gerade weil das Triggern von Neugier so gut funktioniert, sollten Sie in einer Awareness-Kampagne dieses Thema mit besonderem Fokus behandeln – z. B. in einer simulierten Phishing-Kampagne mit genau diesem Motiv und/oder in Schulungen zu diesem Thema. Mit CyberXperts sind das nur wenige Klicks für Sie – ge-nauso wie Ihre kostenlose Reservierung eines unverbindlichen Strategie-Beratungsgesprächs.

42 Quelle: CyberXperts-Datenbank.

Der Trick mit den USB-Sticks: Dem Impuls, sie einzustecken und „mal zu schauen, was drauf ist“, kann keiner widerstehen

USB-Datenträger sind eine zentrale Schwachstelle, über die Angreifer Malware in Ihr Unternehmensnetz einschleusen können. Gerade Spionage-, aber auch Sabotageangriffe werden immer wieder erfolgreich mit USB-Datenträgern, auf denen Malware installiert wurde, durchgeführt.

Hierzu werden die USB-Datenträger in der Regel entweder über Social-Engineering-Angriffe den Opfern ausgehändigt oder einfach auf dem Firmengelände ausgelegt. In den meisten Fällen wird ein solcher USB-Stick von dem Finder aus purer Neugier in einen PC eingesteckt. Dann hat der Angreifer oftmals schon gewonnen.

Angst & Autorität – eine hochwirksame Kombination, die von Angreifern gern genutzt wird

Der Inbegriff von Autoritäts-Anmaßung mit manipulativen Absichten ist der Hauptmann von Köpenick. Er schaffte es, in einer falschen Uniform und militärischem Auftreten Zugang zur Stadtkasse zu erhalten. In Kombination mit Druck und Angst ist Autorität eine wirksame Angriffs-Strategie, die sich Hacker zur Nutze machen. Beliebte Betreffe sind:[43]

„Antwort erforderlich! (Amazon)“

„Service Unternehmensberatung“

„Mithilfe erforderlich“

„Sie haben die offizielle [Unternehmen] AG Kalender App noch nicht installiert“

Doch auch pure Angst wirkt aus Sicht der Angreifer bombastisch. Beispielsweise reagieren Menschen auf E-Mails, in der ihnen mit einem Gerichtsverfahren gedroht wird. Oder auf E-Mails, die suggerieren, dass man etwas Wichtiges verpassen könnte, also die Angst vor Nachteilen:

43 Quelle: CyberXperts Datenbank.

„Bitte um Antwort: Unerlaubte Websites besucht?“

„DRINGEND: Microsoft 365 Konto Verlängerung“

„Verpassten Anruf, 12:32 VOICEMAIL“

„Kreissparkasse: Achtung, Ihr Konto wird bald gesperrt.“

„Vorzahlung ist fällig am:“

„Abrechnungsproblem!“

„Richtlinienverstoß: Konto deaktiviert“

„Sichere deinen Zugriff“

„Dringend!“

„Wichtige Informationen zu Ihrem Passwort“

„Rechtsklage“

„Sperrung Konto“

„Ablauf Online Zugang“

„Widerherstellung Konto“

„Dringend: Falschparker“

Heutzutage meldet sich bei Ihnen kein nigerianischer Prinz ... sondern ein Social Engineer!!

Immer noch wähnen sich zu viele Menschen in Sicherheit, denn sie wissen: Auf plumpe Spam-E-Mails wie die vom nigerianischen Prinzen werden sie niemals hereinfallen.

Das mag sicherlich so sein, doch schützen wird sie diese Aufgeklärtheit heutzutage nicht mehr.

Denn der Hacker von heute geht viel raffinierter vor. Er bedient sich aus den Tiefen der psychologischen Trickkiste und triggert – häufig in mehrstufigen Angriffswellen – die gewünschten Verhaltensweisen bei seinem Opfer. Der Fachbegriff für diese ausgeklügelte Fallenstellung lautet: Social Engineering.

Ein Beispiel: Eine Dame erhält eine E-Mail ihrer Bank mit der Aufforderung, ihre Kontodaten zu bestätigen. Weil sie bereits über solche SPAM-E-Mails etwas gelesen hat, löscht sie die E-Mail. Dann erhält sie aber einen Anruf vom Kundenberater ihrer Bank, den sie namentlich kennt (dass die Stimme eine andere als sonst ist, fällt ihr nicht auf). Er versichert ihr, dass es sich um eine rechtmäßige E-Mail handelt und sendet sie ihr noch einmal zu. Zusätzlich erhält sie noch ein postalisches Schreiben. Nun ist sie 100 % überzeugt. **Die Falle schnappt zu, ihr Erspartes ist weg.**

Social Engineering funktioniert nach 2 Prinzipien:

1. Die Zielperson muss durch den Einsatz psychologischer Kniffe Vertrauen in den Absender und/oder den Inhalt der Phishing-E-Mail haben.
2. Sie muss daran glauben, dass sich eine Reaktion auf den Inhalt der E-Mail lohnen wird.

Bei CyberXperts nutzen wir beide Prinzipien, um das Testszenario zu 100 % dem echten Phishing nachzustellen:

1. Zum Einsatz kommen (Fake)-Phishing-E-Mails, die individuell zum Unternehmen passen, z. B. die eingesetzte Software.
2. Und wir nutzen Inhalte der E-Mails, die in der Praxis vorkommen und regelmäßig große Verwüstungen in Unternehmen anrichten.

Ja, ich möchte mehr darüber erfahren, wie ich mithilfe von CyberXperts täuschend echte Test-Phishing-Kampagnen aufsetze.

CEO-Fraud: Warum fallen so viele (eigentlich intelligente) Mitarbeiter auf E-Mails eines Fake-Vorstands herein?

Angenommen, der Leiter der Buchhaltung Ihrer Firma bekommt direkt vom Vorstand oder Geschäftsführer eine dringende E-Mail:

Er soll dringend eine diskrete und schnelle Überweisung für eine „wichtige Firmenübernahme“ in 6-stelliger Höhe anweisen…

Die Betrüger kommen hier durch täuschend echte E-Mails des vermeintlichen Chefs zunächst an sensible Firmendaten. Ja, selbst harmlose Presse-Meldungen über eine anstehende Firmenübernahme könnten sie nutzen, um den Kaufpreis auf ein anderes Konto „umzuleiten“.

Das Unglaubliche: Diese Masche wirkt. Und zwar so gut, dass sie immer mehr zunimmt.

Die Funktionsweise:

Die Cyber-Kriminellen kombinieren hier die „Autorität“ mit dem Faktor „Angst“, denn es geht immer um schnelle und dringende Überweisungen, die sonst ein Geschäft platzen lassen oder das Unternehmen in sonst irgendeine Art von Bredouille bringen.

Mit einer Awareness-Kampagne lassen Sie ab sofort JEDEN Phishing-Versuch an Ihrem Unternehmen abprallen!

Die Bedeutung der Mitarbeitersensibilisierung nimmt in Zeiten massiver Angriffe auf Unternehmen stetig zu. Um dieser Bedeutung gerecht zu werden, müssen Sie ausgetretene Pfade verlassen. Setzen Sie auf Bewährtes, aber reichern Sie es mit neuen Methoden an. Sie müssen darauf hinwirken, dass sich Ihr Unternehmen diesen Herausforderungen stellt und eine nachhaltige Sicherheitskultur etabliert werden kann.

Awareness-Kampagnen zielen in erster Linie darauf ab, auf unterschiedlichsten Kommunikationskanälen Mitarbeiter auf ein Thema aufmerksam zu machen und zum Handeln zu bewegen. Hierbei kommen Plakate, Flyer, Videos und Trainings zum Einsatz.

Das Geheimnis wirksamer Awareness-Kampagnen: Mitarbeiter müssen erst einmal so richtig reinfallen!

Zur Erreichung maximaler Aufmerksamkeit werden auch gezielte Attacken auf die Mitarbeiter mit gefälschten E-Mails ausgeführt.

In weiteren Szenarien geistern vermeintliche Spione durchs Unternehmen, die unachtsamen Mitarbeitern z. B. vertrauliche Informationen entwenden.

In den letzten Jahren hat sich gezeigt, dass es für den nachhaltigen Erfolg einer Awareness-Kampagne unerlässlich ist, diese bewährten aber zumeist einmaligen Maßnahmen mit längerfristigen Methoden zu unterstützen.

Damit entwickeln Ihre Mitarbeiter schon im Unterbewusstsein eine Art automatisches Alarmsystem. Und sind sensibilisiert für selbst kleine Ungereimtheiten und Abweichungen. Und zwar BEVOR sie heikle Daten eingeben!

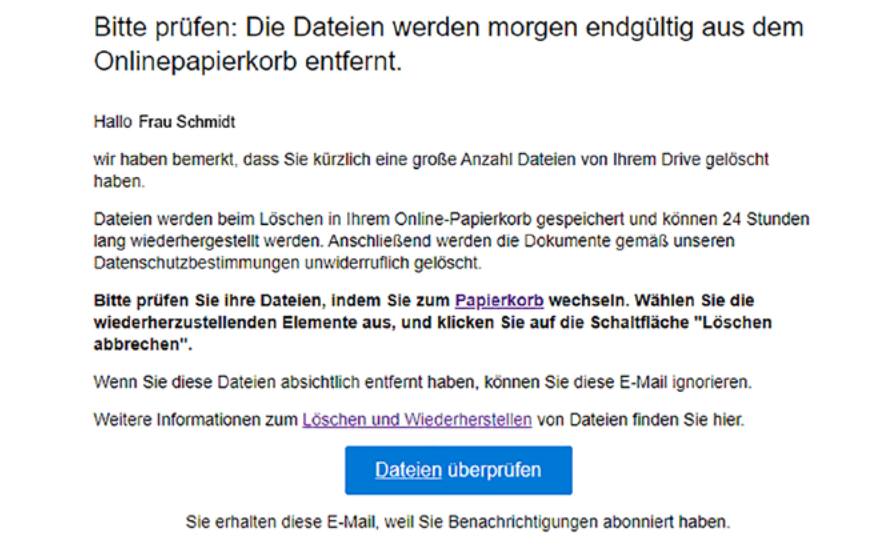
Mit der **Awareness-Kampagne von CyberXperts** eignen sich Ihre Mitarbeiter ganz bequem von zu Hause aus oder im Büro all die Kenntnisse an, mit denen sie **bei verdächtigen Mails, Webseiten oder Angeboten sofort sagen: „*Halt Stopp!*"**

Alle Beschäftigte entwickeln dadurch ein **unterbewusstes Alarmsystem**, durch das sie schon kleinste Ungereimtheiten oder Abweichungen wie eine falsche Internetadresse erkennen. Und zwar BEVOR sie Zugangsdaten eingeben, die sofort in die Hände von Hackern fallen.

Reservieren Sie einfach Ihr persönliches Strategie-Beratungsgespräch, um CyberXperts in aller Ruhe und unverbindlich einmal GRATIS auszuprobieren.

***„Die Mail sah aber täuschend echt aus!"* – Ja, genau, lieber Mitarbeiter. Deshalb hast du ja auch auf den Link darin geklickt.**

„Die Mail sah aber täuschend echt aus!"



Bitte prüfen: Die Dateien werden morgen endgültig aus dem Onlinepapierkorb entfernt.

Hallo Frau Schmidt

wir haben bemerkt, dass Sie kürzlich eine große Anzahl Dateien von Ihrem Drive gelöscht haben.

Dateien werden beim Löschen in Ihrem Online-Papierkorb gespeichert und können 24 Stunden lang wiederhergestellt werden. Anschließend werden die Dokumente gemäß unseren Datenschutzbestimmungen unwiderruflich gelöscht.

Bitte prüfen Sie ihre Dateien, indem Sie zum Papierkorb wechseln. Wählen Sie die wiederherzustellenden Elemente aus, und klicken Sie auf die Schaltfläche "Löschen abbrechen".

Wenn Sie diese Dateien absichtlich entfernt haben, können Sie diese E-Mail ignorieren.

Weitere Informationen zum Löschen und Wiederherstellen von Dateien finden Sie hier.

Dateien überprüfen

Sie erhalten diese E-Mail, weil Sie Benachrichtigungen abonniert haben.

In einem Feldversuch klickten 14,5% Prozent der Probanden auf diese E-Mail. 6,2 Prozent gaben ihre Office-Zugangsdaten ein. Wie würden Ihre Mitarbeiter auf eine solche E-Mail reagieren? – ***Stellen Sie sie doch einmal auf die Probe.*** *Hier klicken.*

Diesen oder einen ähnlichen Satz hören Sie von den meisten Phishing-Opfern.

Und das ist das Problem: Die E-Mails schauen tatsächlich täuschend echt aus, sind nur schwer von authentischen E-Mails zu unterscheiden. Mitarbeiter müssen die Hinweise genau kennen, um hier nicht in die Falle zu tappen.

Mal eben in die Firmen-Cloud einloggen – oder ein paar Dateien aus dem SharePoint herunterladen? Das kann schnell in die Hose gehen – denn die E-Mail oben ist eine perfekte Fälschung, die in Sekunden MS-Office-Zugangsdaten abfischt – und dann Cyber-Kriminelle alle Firmendaten und Geschäftsgeheimnisse lesen können wie ein offenes Buch.

Die Konsequenzen wären verheerend:

Praktisch alle sensiblen Firmendaten liegen heute in einer Cloud oder im Intranet.

Nicht nur können diese Daten an Konkurrenzfirmen oder Geheimdienste weitergeleitet werden.

Es könnte auch sein, dass die Kriminellen alle Daten verschlüsseln und nur gegen eine hohe Lösegeldzahlung wieder freigeben …

Eine Studie im letzten Jahr belegt: Fast 60% aller Unternehmen, die infiziert wurden, haben ein Lösegeld gezahlt, um an ihre Daten zurückzugewinnen! [44]

Besser, Sie machen sich von Anfang an unangreifbar. Wie das funktioniert? – Testen Sie einmal, wie widerstandsfähig Ihre Mitarbeiter gegenüber Phishing sind.

44 Proofpoint, State of the Phish Bericht 2022, 06.07.2022, Abrufbar unter: State of The Phish-Bericht 2022 | Proofpoint DE.

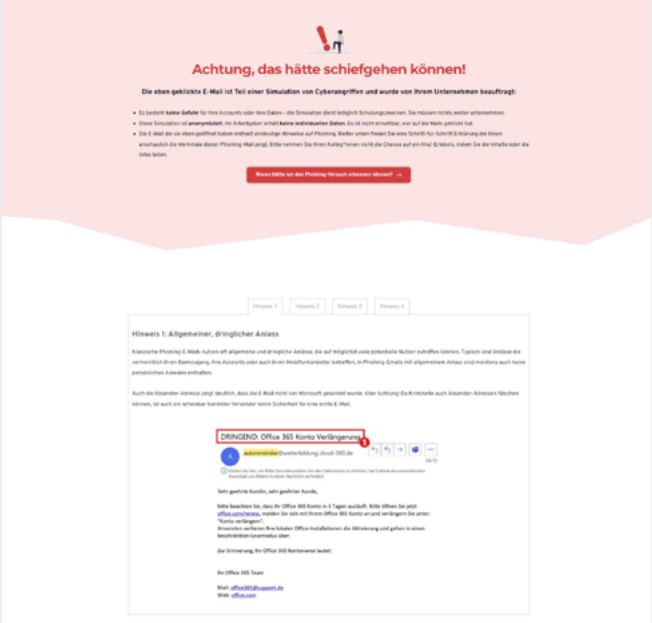
So gehen Sie vor, um die Widerstands-Kraft Ihrer Mitarbeiter gegenüber Phishing zu testen:

Schritt 1: Versenden Sie genau diese E-Mail oben einmal testweise, BEVOR ein Ernstfall eintritt. (Ganz leicht machen Sie sich das mit der Security-Awareness-Plattform CyberXperts, die solche Phishing-Tests auf Knopfdruck anbietet.)

Schritt 2: Sie messen, wie viel Prozent Ihrer Mitarbeiter geöffnet, geklickt und Daten preisgegeben haben. Natürlich erwähnen Sie niemanden öffentlich, es geht nicht um Bloßstellung.

Doch allein die unvorstellbar hohen Zahlen und das Wissen, dass man selbst darunter war, reichen in der Regel aus, um das Bewusstsein für die Gefahr zu schärfen.

Und selbst wenn ein Mitarbeiter selbst nicht geklickt hat: Jeder kann nachempfinden, wie leicht es gewesen wäre, reinzufallen. Und: Jeder Mitarbeiter wird alles dafür tun, das nächste Mal nicht unter den Opfern zu sein, die „reingefallen" sind.



Wichtig bei einer Awareness-Kampagne: Aufklären – ohne bloßzustellen.

Normalerweise ist es natürlich aufwendig, eine Test-Phishing-E-Mail so zu versenden, dass der (Fake-)Angriff plausibel erscheint.

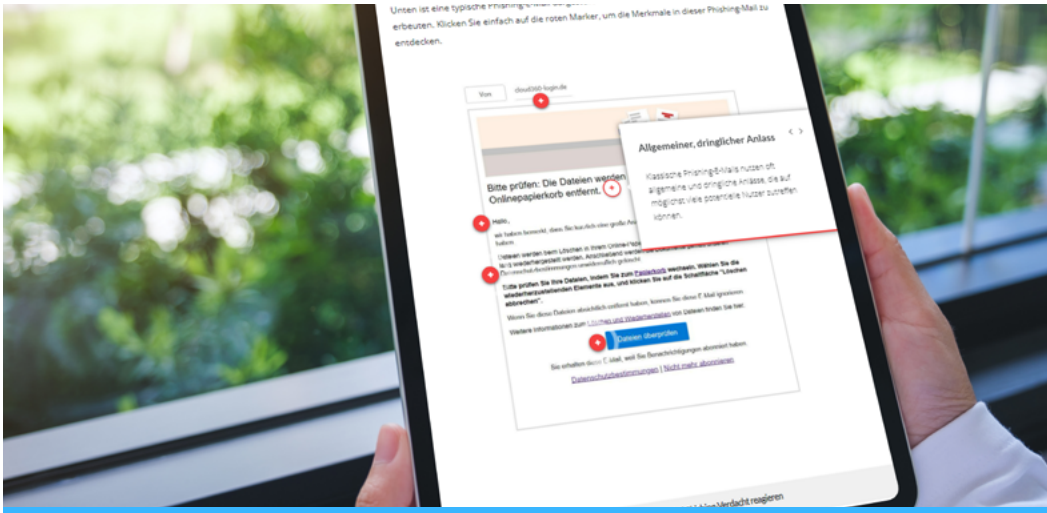
Deshalb ist unsere Security-Awareness-Plattform CyberXperts auch so gestaltet, dass die Fake-Phishing-E-Mails genauso von echten Hackern versendet worden sein könnten – mit dem Unterschied, dass es eben nur Testszenarien sind.

CyberXperts ist sehr leicht und intuitiv einzusetzen:

Machen Sie einfach ein Gespräch mit unseren Kundenbetreuern Naomi Meier aus, die Sie bei Ihrer ersten Test-Phishing-Kampagne begleitet.

Klicken Sie einfach hier, um Ihr persönliches und unverbindliches Strategie-Beratungsgespräch zu reservieren.

Naomi Meier
Senior Sales Managerin



So bauen Sie eine wirksame Awareness-Kampagne auf (Bitte keinen Schritt überspringen!)

Jeder einzelne Schritt Ihrer Awareness-Kampagne muss durchgeführt werden, um den gewünschten Effekt zu erzielen. Kein Schritt darf übersprungen werden. (Wir von CyberXperts unterstützen Sie dabei gerne. Mehr Informationen.)

Planen Sie deshalb diese Bestandteile Ihrer Kampagne ein:

Schritt 1: Mit guter Vorbereitung legen Sie den Grundstein für Ihren Erfolg

- Definieren Sie Ihre Ziele ganz klar – oder lassen Sie es gleich bleiben!
- Der Slogan: Das zentrale Element Ihrer Kampagne
- Ihr wichtigster Verbündeter: Die Geschäftsleitung

Schritt 2: Versenden Sie die (Fake-)Phishing-Mail – OHNE Ankündigung!

Schritt 3: Jetzt lösen Sie auf … und starten Ihre Sensibilisierungs-Kampagne

- Lassen Sie die Geschäftsleitung den Start der Kampagne einläuten (Management-Attention)
- Präsentieren Sie jetzt Ihre Ergebnisse: *„Leute, Ihr habt da auf einen Phishing-Link geklickt … das muss besser werden!“*
- Kampagne mit Werbeträgern (Plakate, Flyer, Intranetseite usw.)
- Zielgruppenorientierte Trainings: So erreichen Sie die Mitarbeiter
- Webbased-Training: Mit spannenden E-Learnings schaffen Sie Awareness
- 20 Minuten Training für die Führungskräfte – So werden sie zu Vorbildern und Multiplikatoren

Schritt 4: Messen Sie den Erfolg anhand dieser Kriterien

Wollen auch Sie sich Ihre nächste Awareness-Kampagne besonders einfach machen?

CyberXperts unterstützt Sie bei jedem der 4 Schritte. Unsere netten Berater zeigen Ihnen gerne, welche genialen Möglichkeiten Sie mit CyberXperts haben. Einfach hier Strategie-Beratungsgespräch ausmachen.

Andreas Hessel
Chief Information Security Officer

Naomi Meier
Senior Sales Managerin

Schritt 1: Mit guter Vorbereitung legen Sie den Grundstein für Ihren Kampagnen-Erfolg

Definieren Sie Ihre Ziele ganz klar – oder lassen Sie es gleich bleiben!

Eine Awareness-Kampagne kann nur erfolgreich sein, wenn die Ziele konkret definiert sind. Andernfalls werden Sie bei den Mitarbeitern das Gefühl von Beliebigkeit erzeugen, aber Sie werden niemanden begeistern können.

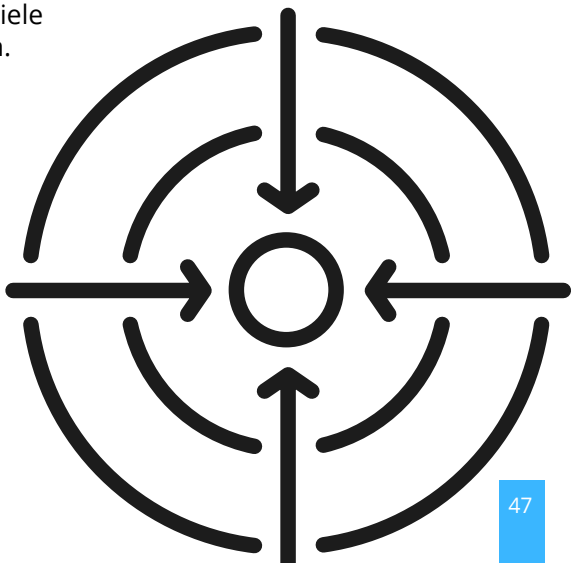
Ohne konkrete Ziele ist der Erfolg einer Awareness-Kampagne auch nicht messbar.

Konkret könnten Sie sich beispielsweise das Ziel setzen, die Mitarbeiter zu den folgenden Themen zu sensibilisieren:

- Social Engineering
- Trojaner und Ransomware
- E-Mail-Sicherheit

Sie möchten zudem den Erfolg der Awareness-Kampagne messen und dauerhaft wirksame Maßnahmen zur Etablierung einer Sicherheitskultur etablieren.

Tipp: Wir entwickeln die Ziele gerne gemeinsam mit Ihnen. Besprechen Sie Ihre Ziele einfach mit unseren CyberXperts-Kundenbetreuern. Falls Sie sich unsicher sind, welche Ziele möglich oder sinnvoll sind, beraten diese Sie gerne. Völlig unverbindlich. Hier kostenlos persönliches Gespräch reservieren.



Der Slogan: Das zentrale Element Ihrer Kampagne

Eine Awareness-Kampagne benötigt zunächst einen aussagekräftigen Slogan und, falls möglich, ein Logo.

Beide Elemente sollten so gewählt werden, dass sie zur Corporate Identity (CI) Ihres Unternehmens passen und auf Ihren Veröffentlichungen (Rundschreiben, E-Mails, Intranetseiten) verwendet werden können.

So erreichen Sie einen dauerhaften Wiedererkennungseffekt, der auch dazu führt, dass die Inhalte der Kampagne bei den Mitarbeitern in Erinnerung bleiben.

Mein Tipp: Mit einem Slogan erreichen Sie Mitarbeiter. Sie signalisieren ihnen, dass Ihr Unternehmen die Mitarbeiter wertschätzt und auf sie baut. So verhindern Sie Trotz-Reaktionen und gehen gleichzeitig gegen die Beharrlichkeit einiger Kollegen vor. Setzen Sie sich mit Ihrer Marketingabteilung in Verbindung. Die Kollegen kennen bestimmt einen Grafiker, der Ihnen zu Ihrem Slogan ein Logo entwirft.

Konkrete Beispiele zu Slogans:

„Sie sind der wichtigste Mitarbeiter der IT-Sicherheit."

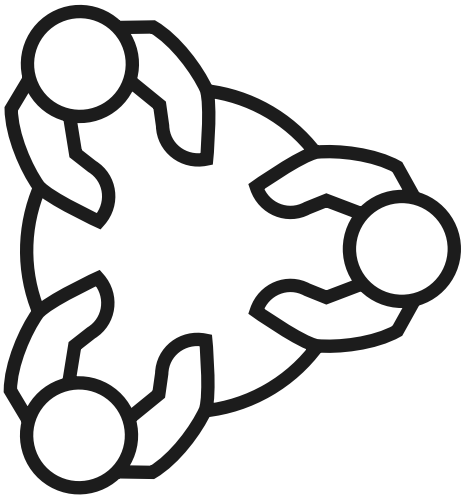
„Unsere Mitarbeiter sind unsere stärkste Firewall."

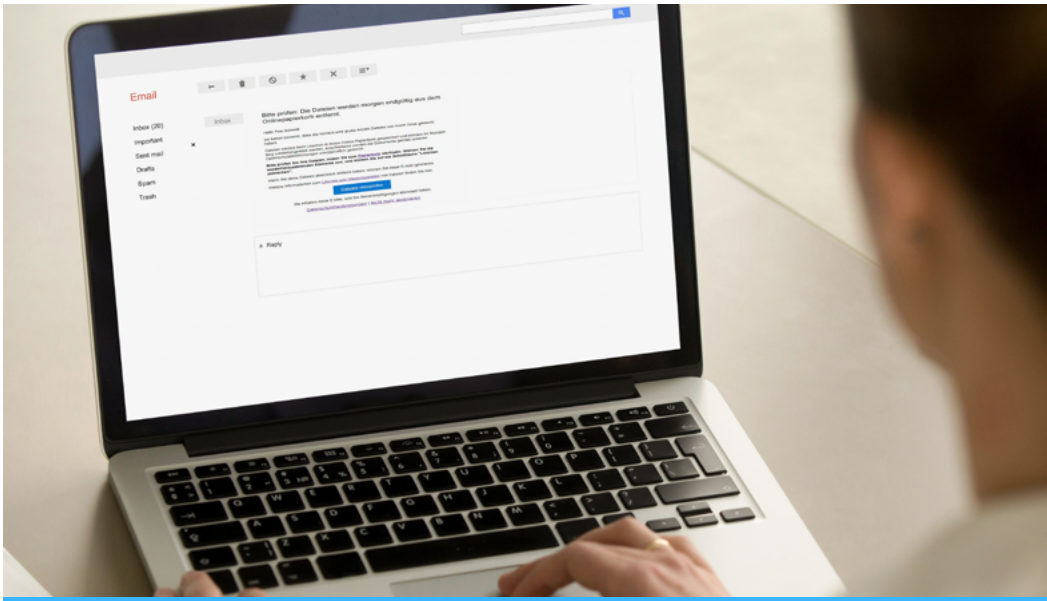
„Sie trotzen jedem Angriff. Mit SICHERHEIT."

Ihr wichtigster Verbündeter: Die Geschäftsleitung

Sie müssen bei der Planung einer Awareness-Kampagne vieles beachten. Zunächst sollten Sie sich darüber im Klaren sein, dass eine solche Kam-pagne ohne die Unterstützung der Geschäftsleitung nicht sinnvoll ist. Nur wenn Ihre Geschäftsleitung sich klar und deutlich zu den Inhalten der Awareness-Kampagne bekennt und Sie unterstützt, können Sie beginnen.

Jetzt haben Sie Ihre Geschäftsleitung davon überzeugt, dass eine Security-Awareness-Kampagne für die Sicherheit im Unternehmen unerlässlich ist. Sie haben ein Budget, mit dem Sie zumindest die beglei-tenden Maßnahmen wie Flyer, Plakate, usw. finanzieren können. Bestenfalls haben Sie noch ein Budget für externe Unterstützung durch versierte Berater.





Schritt 2: Versenden Sie eine (Fake-)-Phishing-Mail – OHNE Ankündigung!

In Ihrem Unternehmen ist von Ihren Planungen noch nichts bekannt geworden.

Das sollte auch so bleiben. Denn jetzt müssen Sie den Paukenschlag vorbereiten, mit dem Sie Ihre Kampagne starten. Damit dieser Start gelingt, müssen Sie die volle Aufmerksamkeit Ihrer Mitarbeiter haben.

Als Paukenschlag hat sich bewährt, einen Phishing-Angriff per E-Mail nachzubilden.

Achtung: Diese Kollegen müssen trotzdem VORHER informiert werden! Bevor Sie Ihren „Angriff" per E-Mail starten, müssen Sie sicherstellen, dass Datenschutzbeauftragte und IT-Sicherheitsbeauftragte an einem Strang ziehen und den Betriebsrat informieren. Die Kollegen aus der IT müssen darauf vorbereitet sein, dass Mitarbeiter beim Support nachfragen, was denn das für eine E-Mail sei usw. Den Betriebsrat müssen Sie darüber informieren, dass Sie lediglich Aufmerksamkeit für die Kampagne erreichen wollen, dass ausschließlich anonymisierte Daten gespeichert werden und keine personenbezogenen Auswertungen gemacht werden.

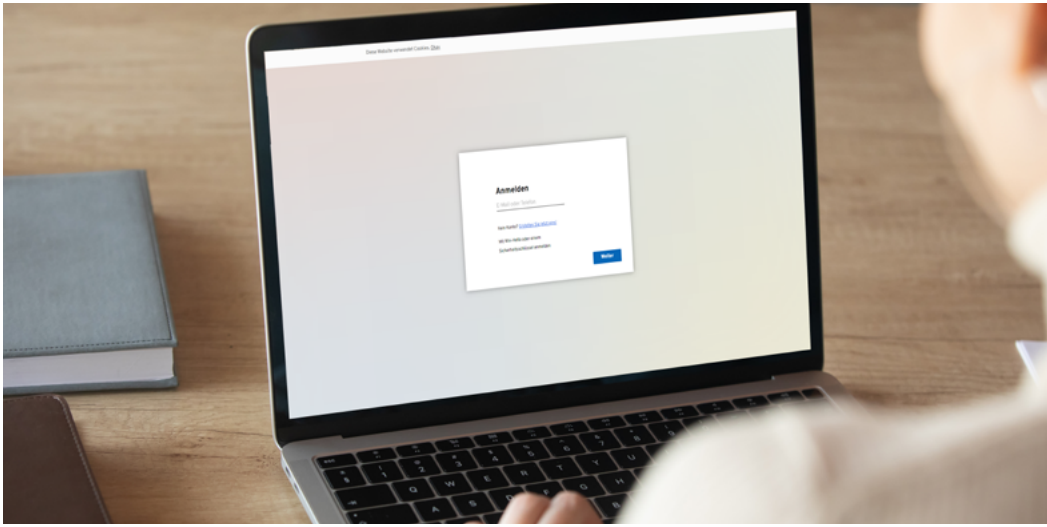
Wie Sie Ihre Phishing-Mail so richtig echt wirken lassen

Hierzu müssen Sie sich zunächst ein Szenario ausdenken, mit dem Sie die Mitarbeiter ködern können. Versuchen Sie, ein realistisches Szenario zu finden, das zu Ihrem Unternehmen passt.

Bereiten Sie z. B. eine E-Mail vor, in der Sie nachfolgendes Szenario beschreiben: Im Unternehmen sollen iPhones eingeführt werden. Die IT-Abteilung sucht nun Mitarbeiter, die bereit sind, die neuen Geräte auf Herz und Nieren zu testen. Die Testpersonen können die iPhones als Dankeschön am Ende des Tests behalten. Da nur eine begrenzte Anzahl von Testgeräten bereitsteht, werden die Teilnehmer ausgelost. Die Interessenten müssen sich auf der Internetseite des Unternehmens mit ihrem Benutzeraccount und Passwort registrieren.

Im nächsten Schritt müssen Sie eine **Internetseite bereitstellen, die das oben aufgeführte Szenario abbildet.**

Auf dieser Seite muss ein Eingabefeld für einen Benutzernamen und ein Passwort vorhanden sein. Die Anzahl der Besucher der Internetseite und die Anzahl der Mitarbeiter, welche die Anmeldung durchgeführt haben, muss gespeichert werden.

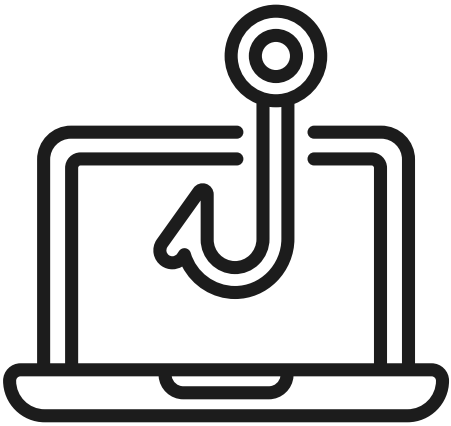


Benutzen Sie einfach diese Fix und fertige Phishing-Simulation

Wenn Sie den Aufwand der Erstellung von E-Mail und dazugehöriger Internetseite nicht leisten wollen oder können, bietet sich CyberXperts als perfekte Lösung an:

Denn CyberXperts bietet für Ihre Phishing-Simulation bereits **fertige Lösungen, die individuell auf Ihr Unternehmen abgestimmt werden. So sparen Sie sich viel Aufwand!** Wir kümmern uns um die Erstellung der Mails, Versand und Auswertung Ihrer Kampagne. Hier mehr Informationen erhalten.

Jetzt gratis Phishing-E-Mails zu Programmen wie Microsoft Teams, Outlook oder Cloud-Anbietern erstellen! Direkt hier Ihren persönlichen Beratungstermin vereinbaren.



Nur mit maximalem Schock-Effekt erzielen Sie eine Verhaltensänderung

Wenn die E-Mail sprachlich zu Ihrem Unternehmen passt und sich inhaltlich auf ein reales allgemein bekanntes Thema bezieht, werden in der Regel die meisten Mitarbeiter in die Falle tappen.

Instruieren Sie die IT: Machen Sie den Kollegen klar, dass sie den Mitarbeitern, die sich über die Hintergründe der E-Mail informieren wollen, keine direkten Auskünfte zu der Kampagne geben. Natürlich dürfen sie auch nicht bestätigen, dass die E-Mail echt ist. Am besten ist es, wenn die Kollegen des IT-Supportes einfach aussagen, dass sie die Hintergründe klären müssen, und sich dann wieder melden. Für die Statistik ist es wichtig, dass die Anzahl der Anrufer festgehalten wird. Weisen Sie darauf hin, dass keine Namen registriert werden dürfen. Nach diesen Vorbereitungen können Sie die E-Mail an alle Mitarbeiter senden.

Tipp: Werten Sie die Ergebnisse am gleichen Tag aus. Dass mit dieser E-Mail irgendetwas nicht stimmt, wird sich schnell in Ihrem Unternehmen verbreiten. Nachzügler sind daher meist informiert und verfälschen das Bild.

Schritt 3: Jetzt lösen Sie auf … und starten Ihre Sensibilisierungs-Kampagne offiziell

Lassen Sie die Geschäftsleitung den Start der Kampagne einläuten

Nach dem Versand der Phishing-E-Mail sollten Sie unmittelbar am darauffolgenden Tag mit der Kampagne starten. Lassen Sie die E-Mail der Geschäftsleitung daher auch am Vorabend versenden. In dieser E-Mail sollte die Geschäftsleitung die Kampagne kurz vorstellen, die gemeinsamen Ziele sowie die zentrale Rolle der Mitarbeiter hervorheben.

Präsentieren Sie jetzt Ihre Ergebnisse: *„Leute, Ihr habt da auf einen Phishing-Link geklickt … das muss besser werden!“*

Präsentationen zu Awareness-Kampagnen müssen zentrale Botschaften und kein Fachwissen vermitteln. Fachwissen wird in Trainingseinheiten vermittelt. Verwenden Sie daher in Ihren Präsentationen viel Bildmaterial, Comicfiguren, Videos und wenig Text.

Sie müssen die Mitarbeiter begeistern und nicht langweilen. Bewährt haben sich auch kleine Live-Hacking-Beiträge, bei denen z. B. gezeigt wird, wie schnell Passwörter gehackt werden oder wie leicht man mit einem USB-Stick Daten ausspionieren kann.

Auch das macht eine Kampagne mit CyberXperts für Sie besonders attraktiv:

CyberXperts wertet alle Phishingkampagnen auf Abteilungsebene für Sie aus und erstellt passende Grafiken, mit denen Sie Ihre Mitarbeiter überzeugen können. Spannende E-Learnings inkl. Videos unterstützen Sie bei der Präsentation in Ihrem Unternehmen. Jetzt gratis Beratungstermin für Ihre erste Phishing-Simulation vereinbaren!

Tipp: Zu den Präsentationsterminen sollten alle Mitarbeiter eingeladen werden. Wirken Sie darauf hin, dass die Geschäftsleitung vor jeder Präsentation zu den Mitarbeitern spricht und sich für die Ziele der Awareness-Kampagne stark macht. Die Anwesenheit des Managements ist für den Erfolg der Awareness-Kampagne von entscheidender Bedeutung. Das lockert die Stimmung auf und sorgt für Solidarität mit den Mitarbeitern.

Diese Inhalte sollte Ihre Präsentation haben:

- **Stellen Sie die Ergebnisse der Phishing-E-Mail dar.** Heben Sie hervor, wie viel Prozent der Mitarbeiter den Link in der Mail angeklickt haben und wie viele Mitarbeiter tatsächlich ihren Benutzernamen und ihr Passwort eingegeben haben.
- **Weisen Sie aber darauf hin, dass dieses Ergebnis normal ist.** Verdeutlichen Sie, dass es menschlich ist, seiner Neugierde nachzugeben und solchen vermeintlich attraktiven Angeboten reflexartig nachzukommen.
- **Vermeiden Sie den Oberlehrer** und weisen Sie darauf hin, dass Sie auch schon in solche Fallen getappt sind. So können Sie die Mitarbeiter sensibilisieren und in die Awareness-Kampagne mitnehmen.

Denken Sie immer daran, dass Sie gegen Beharrlichkeit und Trotz der Mitarbeiter kämpfen müssen. Da hilft es nicht, mit Fachwissen zu glänzen. Ein Lacher und ein gut gemachtes Video (das Sie z. B. bei CyberXperts finden), das die Zuschauer fesselt, sind bei weitem hilfreicher.

Zielgruppenorientierte Trainings: So erreichen Sie die Mitarbeiter

Sie haben die Mitarbeiter mit Ihrer Phishing-Mail aufgerüttelt und die Ergebnisse gezeigt. Ihre Security-Awareness-Kampagne war ein voller Erfolg. Nun gilt es, diese Aufmerksamkeit zu nutzen, um den Mitarbeitern Ihre zentralen Themen nachhaltig zu vermitteln.

Um dieses Ziel zu erreichen, führen Sie zielgruppenorientierte Trainings durch. Zielgruppen sind in der Regel „alle Mitarbeiter", „Führungskräfte" und „Geschäftsleitung".

Neben diesen primären Zielgruppen sollten Sie Trainings zu speziellen Business-Themen oder Abteilungen planen wie z. B. Personaldaten, Kundendaten, Forschungsdaten sowie Ergänzungstrainings zu Sicherheitsthemen.

CyberXperts bietet Ihnen die **perfekten Vorlagen und Trainingsmaterialien** für Ihre Schulungen. Hier gratis informieren.

Webbased Training: Mit spannenden E-Learnings schaffen Sie Awareness

Für die Zielgruppe „Alle Mitarbeiter" können Sie nur in kleinen Unternehmen Präsenztrainings anbieten. Ab einer Größenordnung von 100 Mitarbeitern ist der Einsatz eines Webbased Trainings (WBT) sinnvoller.

Tipp: Das Training muss kurzweilig und interessant sein. Die Mitarbeiter müssen das WBT aufrufen, weil es ihnen Spaß macht. Nur so können Sie vermeiden, dass das WBT als lästige Pflichtübung verstanden wird und die Lösungen für die Testfragen im Unternehmen kursieren, weil jeder das WBT schnell durchklicken will. Ein langweiliges WBT oder ein WBT, in dem mit dem erhobenen Zeigefinger gearbeitet wird, kann Ihnen die Erfolge Ihrer gesamten Security-Awareness-Kampagne zunichtemachen.

In der Regel können diese Programme auf das Corporate Design des Unternehmens angepasst werden. Sie sollten die Slogans und Logos Ihrer Awareness-Kampagne in das WBT integrieren lassen. Achten Sie bei der Auswahl eines Produktes darauf, dass dabei mit Multimedia-Inhalten (Videos, Animationen, Comicelemente, Sprache usw.) gearbeitet wird und eine Erfolgskontrolle oder ein Test integriert ist.

Sie möchte Ihre Mitarbeiter mit spannenden E-Learnings inklusive interaktiven Elementen wie Videos oder Quiz sensibilisieren? **CyberXperts bietet eine große Auswahl an Awareness-Schulungen, die Ihre Mitarbeiter mit realen Beispielen wirksam schulen.** Hier gratis und unverbindlich informieren.

Tipp: Das WBT sollte einen Pool von Fragen bereitstellen und nach einem Zufallsprinzip eine bestimmte Anzahl von Fragen für den Teilnehmer auswählen. Das WBT sollte nicht länger als eine Stunde dauern und es muss die Möglichkeit bestehen, dass der Teilnehmer das WBT an beliebigen Stellen wiederaufnehmen kann. Der Teilnehmer muss auch den Test so lange wiederholen können, bis er alle Fragen beantwortet hat. (Genau das bietet z. B. CyberXperts.)

20 Minuten Training für die Führungskräfte – So werden sie zu Vorbildern und Multiplikatoren

Führungskräfte müssen ein Bewusstsein dafür entwickeln, dass sie eine besondere Verantwortung für das Thema Sicherheit tragen. Sie müssen den Mitarbeitern ein Vorbild sein und die Mitarbeiter immer wieder dazu ermutigen, die Sicherheitsrichtlinien einzuhalten und sich bei der täglichen Arbeit die erforderliche Sensibilität und Aufmerksamkeit für die Informationssicherheit zu bewahren.

Führungskräfte müssen geschult werden, damit sie wie jeder Mitarbeiter die Sicherheitsrichtlinien einhalten, den Mitarbeitern als Vorbild dienen, in ihrem Fachbereich Verantwortung für die Informationssicherheit übernehmen, in ihrer Personalverantwortung auch den Datenschutz ernst nehmen.

Je nach Unternehmensgröße bieten sich Präsenztrainings für Führungskräfte an oder WBT mit den genannten Inhalten. In beiden Fällen sollten die Trainings nicht länger als 20 Minuten dauern. Auch bei diesem Training ist es wichtig, auf Unterhaltung zu setzen.

Schritt 4: Messen Sie den Erfolg anhand dieser Kriterien

Erfolgsmessungen machen transparent, ob Sie mit Ihren Sensibilisierungsmaßnahmen gegen Dynamik, Beharrlichkeit und Trotz der Mitarbeiter erfolgreich waren und ob in den Trainings nachhaltig Fachwissen vermittelt wurde.

Aus den Ergebnissen können Sie direkt erkennen, an welchen Themen Sie weiterarbeiten müssen.

Spätestens jetzt wird deutlich, dass Ihre Aufgabe nicht mit der Durchführung einer Phishing-Kampagne beendet ist.

Die erste Phishing-Kampagne war der erste Schritt auf Ihrem Weg zur Etablierung einer Sicherheitskultur, auf dem Sie die gemeinsamen Ziele, Interessen, Normen, Werte und Verhaltensmuster in Ihrem Unternehmen herausbilden müssen.

Die Auswertung der Phishing-E-Mail hat Ihnen sehr genau gezeigt, wie viele Mitarbeiter anfällig für solche Angriffe sind.

Wenn Sie einen solchen Angriff ein halbes Jahr nach der ersten Kampagne wiederholen, haben Sie einen deutlichen Nachweis, ob sich die Aufmerksamkeit Ihrer Mitarbeiter verbessert hat.

Ebenso liefert Ihnen das E-Learning Informationen darüber, wie viele Mitarbeiter teilgenommen haben und wie deren Testergebnisse waren. Auch hier können Sie durch regelmäßige Auswertungen erfahren, wie der Kenntnisstand Ihrer Mitarbeiter ist.

Führen Sie weitere Prüfungen durch, mit denen Sie messbare Ergebnisse erhalten.

Erstellen Sie einen Prüfungsplan, mit dem Sie den Erfolg Ihrer Maßnahmen nachweisen können.

Mit solchen Prüfungen können Sie über einen längeren Zeitraum auswerten, ob sich das Verhalten der Mitarbeiter durch Ihre Awareness-Maßnahmen ändert.

Stellen Sie Verbesserungen fest, sollten Sie diese auch kommunizieren.

Ihrer Geschäftsleitung können Sie nachweisen, dass sich die Security-Awareness-Kampagne bezahlt gemacht hat, und die Mitarbeiter können Sie für ihre Sensibilität und ihr Fachwissen loben.

Verschlechtern sich die Ergebnisse, müssen Sie themengerecht Trainings oder Sensibilisierungsmaßnahmen durchführen. So können Sie sehr genau steuern, in welchen Themenbereichen Sie aktiv Maßnahmen ergreifen müssen.

CyberXperts Prüfung	**Methode**	**Prüfungs-gegenstand**
Phishing-E-Mail	Versand gefälschter E-Mails	Sensibilität der Mitarbeiter
E-Learning	Durchführung von digitalen Lerneinheiten	Vorhandensein von Fachwissen
Sicherheitsmeldungen	Auswertung der Help-Desk-Datenbank und Anzahl der Nachfragen zu auffälligen E-Mails	Sensibilität der Mitarbeiter
E-Mail-Verschlüsselung	Auswertung von E-Mail-Protokollen	Sensibilität der Mitarbeiter

CyberXperts macht Ihnen das Messen Ihrer Awareness-Kampagne besonders leicht:

Denn es bietet Ihnen **automatische Auswertungen Ihrer Phishing-E-Mails auf Abteilungsebene.** So sehen Sie direkt, welche Abteilung Schulungsbedarf hat und wo Sicherheitslücken entstanden sind.

Passend dazu können Sie direkt unsere E-Learning-Einheiten nutzen und die Abteilungen zu den digitalen Trainings einladen. Im Anschluss erhalten Sie einen Nachweis über die Sensibilisierungsmaßnahme für Ihre Unterlagen.

Ja, ich möchte meinen persönlichen Termin für ein Strategie-Beratungsgespräch jetzt reservieren. Hier klicken.

CyberXperts – die geniale neue Lösung für Ihre nächste Awareness-Kampagne

Modul 1: Mit diesen stets aktuellen Schulungsvorlagen sensibilisieren Sie Ihre Mitarbeiter wirksam für Cyber-Fallen!

Ihre Mitarbeiter sind Ihre Human Firewall und schützen Ihr Unternehmen. Schulungslücken und fehlende Awareness sind das größte Risiko für Sie. Zeitdruck und Unvorsichtigkeit im Berufsalltag sind das Einfallstor für Angreifer.

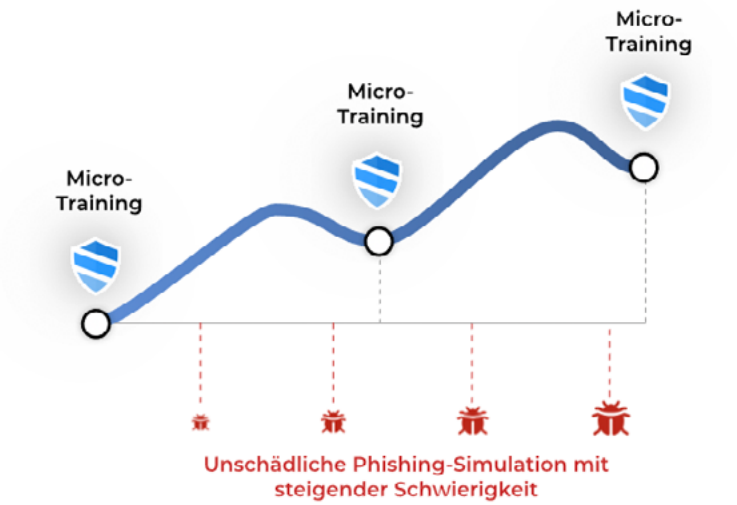
Sicher ist Ihr Unternehmen nur, wenn Awareness zur Routine wird.

Mit dem starkem Bild- und Videomaterial von CyberXperts sensibilisieren Sie Ihre Mitarbeiter wirksam und langanhaltend.

Stets aktuelle Schulungen sorgen dafür, dass Ihre Mitarbeiter bei den ständig neuen Bedrohungen immer auf dem neuesten Stand sind.

Dabei gehen wir bei CyberXperts nach diesen Prinzipien vor:

- **Positives Reinforcement:** Kontinuierliche Schulungs-Einheiten sorgen für einen nachhaltigen Lern-Effekt
- **Kein trockenes E-Learning, kein Frust:** Gamifizierung und Interaktion bringen Interesse und Motivation.
- **Echte Beispiele aus der Realität:** Reale Situationen unterstreichen die Relevanz des Themas und zeigen, wie raffiniert Cyberkriminelle vorgehen!
- **Maßgeschneidert für Ihr Unternehmen** Unser E-Learning können Sie mit Ihrem Unternehmenslogo individualisieren und an Ihre Corporate Identity anpassen.



Modul 2: Die perfekte Phishing-Simulation: So identifizieren Sie Schulungs-Potenzial und erhalten einen Nachweis für die ISO 27001

Mit simulierten Phishing-E-Mails lernen Ihre Mitarbeiter effektiv Angriffe zu erkennen und im Ernstfall richtig zu reagieren. Die automatisierten Phishing-Kampagnen von CyberXperts können Sie individuell an Ihr Unternehmen anpassen und aussteuern.

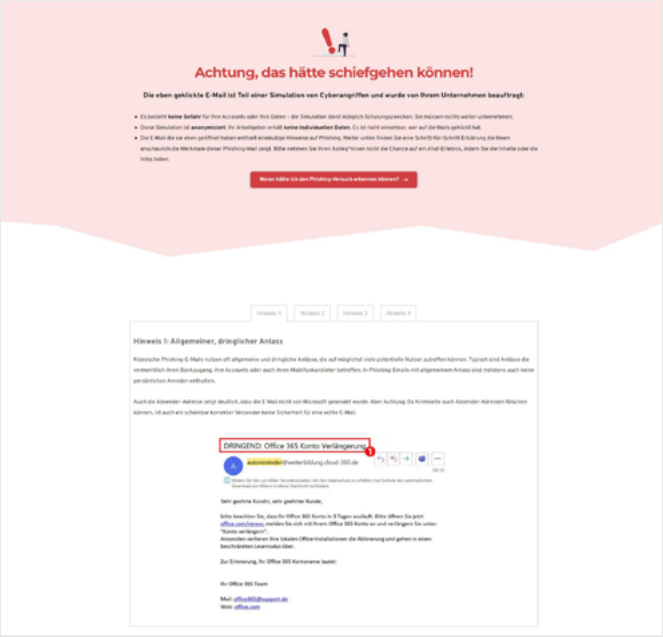
Ihre Auswertung zeigt Ihnen das Schulungspotential und kann als **Nachweis für Cyber-Versicherungen und die ISO 27001** genutzt werden.

So geht's:

Wir besprechen in einem persönlichen Gespräch mit Ihnen wie Ihre persönliche Kampagne aufgesetzt werden soll: Sie wählen, ob alle oder nur einzelne Abteilungen E-Mails erhalten und in welchem Abstand. Für eine möglichst realistische Simulation berücksichtigen wir, welche Tools und Software in Ihrem Unternehmen standardmäßig verwendet werden.

1. **Let's phish! Die Test-E-Mails gehen raus.** Nachdem Ihre Kampagne eingerichtet wurde, versenden Sie eine unangekündigte Test-Phishing-E-Mail, die Sie zum Startschuss Ihrer Kampagne machen. Danach werden in regelmäßigen Abständen simulierte Phishing-E-Mails automatisiert an Ihre Mitarbeiter versendet. Sie brauchen sich um nichts mehr zu kümmern. Falls ein Mitarbeiter klickt, erhält er einen Hinweis und kann direkt lernen, wie er eine solche Panne beim nächsten Mal vermeiden kann.
2. **Eine automatische Auswertung Ihrer Phishing-Kampagne wird für Sie generiert.** Hier erfahren Sie, wie viel Prozent Ihrer Mitarbeiter geklickt haben und in welchen Abteilungen Schulungsbedarf besteht.

Jetzt gratis Phishing-Simulation für Ihr Unternehmen durchführen: Reservieren Sie einfach hier Ihr persönliches Strategie-Gespräch!



Mit einer Phishing-Simulation sorgen Sie für einen starken Aha-Effekt bei Ihren Mitarbeitern … und einer hohen Bereitschaft dafür, sich mit dem Thema CyberSecurity auseinanderzusetzen.

Modul 3: Mit einem intuitivem 360°-Check zur Einschätzung Ihres Risikoprofils kennen Sie die Sicherheitslage Ihres Unternehmens genau

CyberXperts hilft Ihnen dabei, aktuelle Gefahren zu identifizieren und geeignete Gegenmaßnahmen umzusetzen. So haben Angreifer bei Ihrem Unternehmen keine Chance!

Mit dem CyberXperts-Dashboard sehen Sie alle Risiken auf einem Blick. Mit ausgewählten Fragen analysieren wir Ihr Risikoprofil und zeigen mögliche Szenarien.

Verständliche Schritt-für-Schritt-Maßnahmen

Sie erhalten zu jeder potenziellen Bedrohung individuelle Maßnahmen, um Ihr Unternehmen besser zu schützen. Mit einer leicht verständlichen Schritt-für-Schritt-Anleitung können Sie diese kinderleicht in Ihrem Unternehmen umsetzen.

Immer im Blick und automatische Erinnerungen

Damit Ihre IT-Sicherheit im Alltagsstress nicht in Vergessenheit gerät, erinnern wir Sie rechtzeitig daran und analysieren die aktuelle Sicherheitslage Ihres Unternehmens.

Ja, ich möchte mehr über den 360°-Check für mein Unternehmen erfahren.

Wir freuen schon auf Ihre Terminvereinbarung!

Impressum

CyberXperts

ein Unternehmensbereich der
VNR Verlag für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2-4; D-53095 Bonn

Vorstand: Richard Rentrop

Telefon: 0228 - 9 55 01 50 (Kundendienst)
Telefax: 0228 - 3 69 64 80
E-Mail: info@cyberxperts.de
Internet: https://www.cyberxperts.de

Verantwortlicher i.S.d.P.: Michael Jodda, Theodor-Heuss-Straße 2-4, 53177 Bonn

Enthält u. a. Artikel von Andreas Hessel, Andreas Würtz

Satz: BB-Design, Birken-Honigsessen

Bildnachweis: S. 1 NicoElNino, S. 7 andranik123, S. 8 eigene Erstellung (CyberXperts) S. 16 Gorodenkoff, S. 17 Goffkein, S. 18 vchalup, S. 19 Matthew, S. 25 PR Image Factory, S. 26 contrastwerkstatt, S. 27 Tiberius Gracchus, S. 28 oatawa, S. 31 panuwat, S. 32 martialred, S. 33 jacartoon, S. 34 Comauthor, s. 35 DGTL Graphics, S. 37 terovesalainen, S. 39 Monkey Business, S. 45 FarknotArchitect, S. 47 Editable Line icons, S. 49 davooda, S. 50 fizkes, S. 51 fizkes, S. 52 MacroOne Phishing, S. 55 blankstock, S. 57 Fizkes, S. 59 eigene Erstellung (CyberXperts), wo nicht anders vermerkt alle AdobeStock

Bonn, Bukarest, Manchester, Warschau