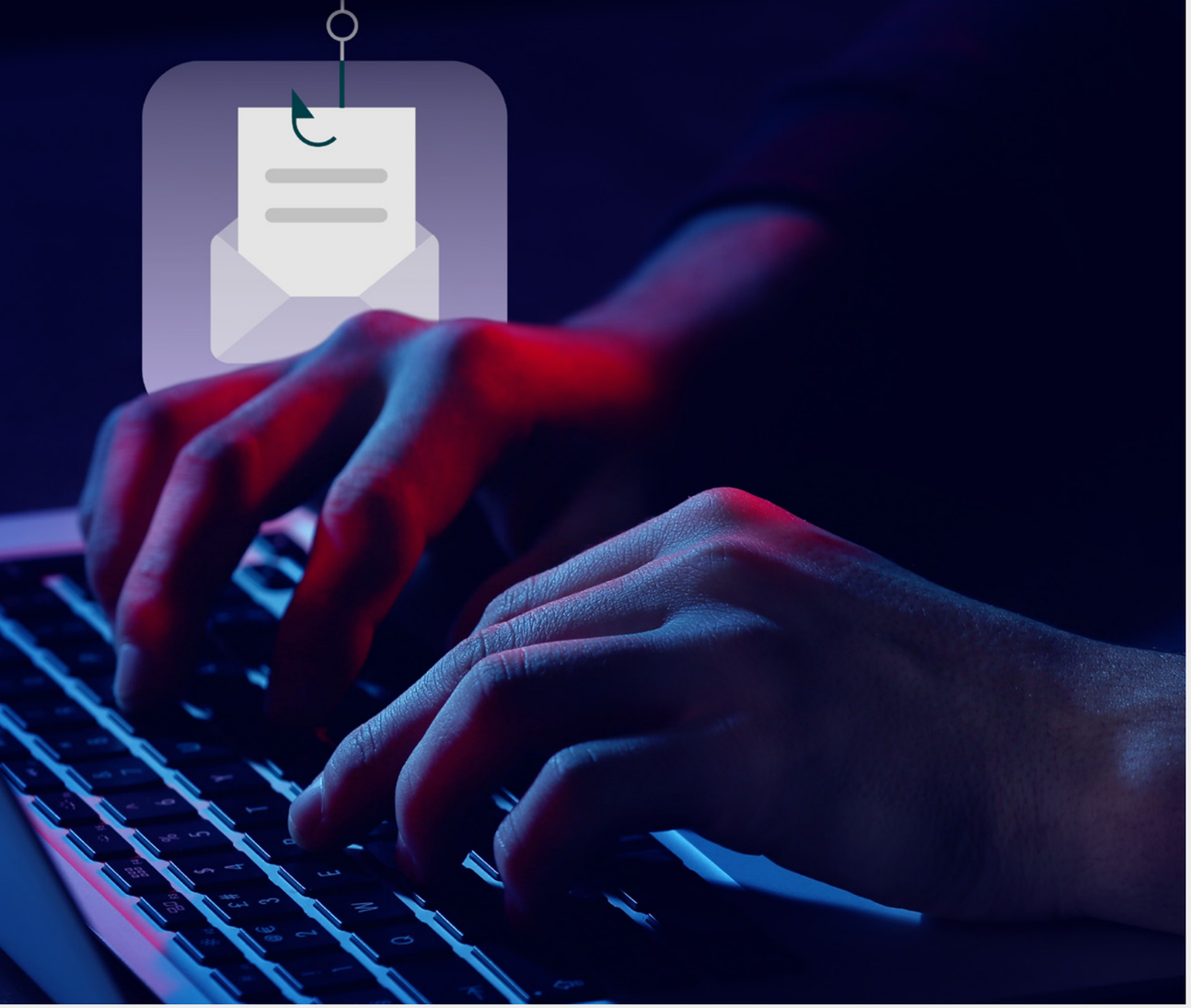
sosafe

Die Top 5 Cybercrime-Trends 2022

Aktuelle Cybercrime-Trends und wie Sie sich vor Ihnen schützen



01 Trendy Phishing: Anlassbezogene Angriffswellen

Cyberkriminelle setzen weiterhin auf bekanntes Werkzeug: In Phishing-Mails manipulieren sie die Gefühle ihrer Opfer, um an vertrauliche Daten zu gelangen und diese anschließend für ihre Zwecke zu nutzen. Dabei bleiben die Angreifenden stets im Trend: Sie greifen immer schneller aktuelle Themen und gesellschaftliche Entwicklungen in ihren trügerischen Nachrichten auf. Solche anlassbezogenen Phishing-Mails wecken oftmals Angst und Unsicherheit in den Opfern, wodurch sie eher auf schädliche Inhalte klicken – und die Cyberkriminellen zielsicher Daten erhaschen.

Bei der Auswahl der Anlässe und Themen für ihre Phishing-Nachrichten haben sie keine Skrupel. Schon die Corona-Pandemie bot den Kriminellen optimale Ausgangschancen: Bereits wenige Wochen nachdem die COVID-19 Omicron-Variante weltweit bekannt wurde, griff ein erster Phishing-Betrug in Großbritannien das Thema auf.[1] Auch der Angriffskrieg Russlands auf die Ukraine sorgte für einen beispiellosen Anstieg an Cybercrime-Aktivitäten, darunter insbesondere Phishing. So wurden in den Sozialen Medien und über Phishing-Mails etwa gefälschte Spendenaufrufe verbreitet.[2] Bei einer besonders perfiden Masche wurden Links geteilt, die vermeintlich DDoS-Angriffe auf russische Server und Dienste unterstützen sollten. Über die Klicks schleusten Cyberkriminelle stattdessen aber Viren und Trojaner in die Systeme von Privatpersonen.[3] Gleichzeitig meldete Google's Forschungsteam Phishing-Angriffe von russischer Seite auf die Systeme osteuropäischer Staaten sowie US-basierte NGOs. Auch hier sollten vertrauliche Zugangsdaten für Spionagezwecke oder zum Verbreiten von Malware abgegriffen werden.[4] Damit wird Phishing zu einer Waffe in der hybriden Kriegsführung.

In Kombination mit neuen technologischen Möglichkeiten (siehe Trend 4) steht Organisationen weltweit eine Generation höchst innovativer und erfolgreicher Phishing-Versuche bevor. Künstliche Intelligenz wird diese auch in Masse wesentlich präziser und personalisierter machen – und dementsprechend erfolgreicher.

Praxistipp

Beim Phishing setzen Cyberkriminelle darauf, dass sich ihre Opfer emotional manipulieren lassen. Die beste Methode, um Ihre Organisation zu schützen ist deshalb, Unsicherheiten zu vermeiden, indem Sie Ihre Mitarbeitenden sensibilisieren. So lassen sie sich nicht auf die Gefühle von Druck, Angst oder auch Neugier im Zusammenhang mit den trügerischen Mails ein. Setzen Sie auf Cyber Security Awareness Training, das stets aktuelle Informationen (auch zu neuen Angriffsmaschen) enthält und Phishing-Simulationen, die eine Bandbreite verschiedener Angriffsszenarien enthalten. So helfen Sie Ihren Mitarbeitenden, Phishing-Mails zu erkennen und abzuwehren – so aktuell und perfide diese auch sein mögen.

1 The Independent (2021). Scam warning over fake omicron testing text messages.
2 Zeit Online (2022). Wie können wir helfen?
3 SoSafe (2022). SoSafe warnt vor Social-Engineering-Angriffen im Kontext des Angriffskrieges auf die Ukraine.
4 ZDNet (2022). Google: Multiple hacking groups are using the war in Ukraine as a lure in phishing attempts.

02 Supply-Chain-Attacken: Explosive Kettenreaktionen

Schon 2021 ist die Anzahl an Lieferkettenangriffen, sogenannten Supply-Chain-Angriffen, um 51 Prozent angestiegen.[5] Und auch 2022 zeichnet sich dieser Trend weiter ab. Der Grund dafür scheint logisch: Cyberkriminelle erhöhen so ihre Erfolgschancen über das Partner- und Lieferantennetzwerk ihrer Opfer. Denn schon eine einzige Sicherheitslücke in der Lieferkette (zum Beispiel in der Software, die ein Partner oder Lieferant nutzt) reicht unter Umständen aus, um das gesamte Netzwerk zu kompromittieren – eine explosive Angriffstaktik, die im Falle eines Incidents weitreichende Folgen nach sich ziehen kann.

Gruppen wie REvil, BlackMatter oder DarkSide machten zuletzt beispielsweise mit groß angelegten Angriffen auf die HR-Plattform Kronos, das Ölpipelinesystem Colonial Pipeline und den Fleischproduzenten JBS von sich zu hören. Unterdes attackierte die chinesische Cyber-Spionagegruppe APT27 – auch bekannt als LuckyMouse oder EmissaryPanda – vermehrt kleinere Unternehmen. Über die Lieferkette wurden anschließend weitere Opfer angegriffen, darunter insbesondere Organisationen aus dem Bereich Pharma und Technologie.[6]

Besonders eindrücklich zeigte der Ransomware-Angriff auf den IT-Dienstleister Kaseya das Ausmaß der komplexen Angriffsmethoden: Über ein vermeintliches Software-Update gelangten die Täter nicht nur in die Systeme von Kaseya, sondern konnten die infizierte Software darüber hinaus auch auf die Informationstechnik ihrer Kunden und der gesamten Lieferkette verbreiten. Von diesem sogenannten „Software-Supply-Chain-Angriff“ waren weltweit schätzungsweise 1.500 Unternehmen, unter anderem in den USA, Deutschland und den Niederlanden, betroffen.[7] Auch die Angriffe auf SolarWinds und die Log4J-Schwachstelle lassen sich diese Software-Lieferkettenangriffen zuordnen – und zeigen deutlich, welche weitreichenden Wellen solche Vorfälle schlagen können.[8]

5 TechRepublic (2022). Supply chain cyberattacks jumped 51% in 2021.
6 Bleeping Computer (2022). German government warns of APT27 hackers backdooring business networks.
7 The Washington Post (2021). Ransomware attack struck between 800 and 1,500 businesses, says company at center of hack.
8 Forrester (2021). Log4j, Open Source Maintenance, Andy Why SBOMs Are Critical Now.
9 Gartner (2021). The Top 8 Cybersecurity Predictions for 2021-2022.

Praxistipp

Neben dem Stärken der Sicherheitskultur in Ihrer eigenen Organisation sollten Sie auch bei der Auswahl Ihrer Partner Wert auf Informations- und Datensicherheit legen. Ist Ihr Partnernetzwerk sicherheitstechnisch gut aufgestellt, verringert sich die Gefahr, dass Ihre Organisation Opfer eines Lieferkettenangriffs wird. Dazu bietet es sich beispielsweise an, (Software-)Zertifizierungen oder die Erfüllung von Regularien wie der EU-DSGVO zu überprüfen und sicherzustellen. Laut Gartner werden schon 2025 fast zwei Drittel aller Organisationen Cyberrisiken als Faktor nutzen, um zu entscheiden, mit wem sie eine Geschäftsbeziehung eingehen.[9]

03 Multiple Extortion: Mehrfachangriffe multiplizieren Schadensrisiko

Nicht ohne Grund spricht die ENISA zurzeit von der „goldenen Ära für Ransomware“. Die Anzahl der Angriffe mit Erpressungssoftware hat sich 2021 im Vergleich zum Vorjahr mehr als verdoppelt.[10] Bei dieser Angriffsart schleusen Cyberkriminelle Schadsoftware in Unternehmenssysteme ein und verschlüsseln sensible Daten, die sie nur nach Zahlung eines Lösegelds (engl. „ransom“) freigeben. Dabei suchen sie entweder den Weg über den Faktor Mensch, zum Beispiel über Phishing-Mails. Oder aber sie nutzen technische Methoden wie Brute Force, um Daten abzufischen. Beide Methoden führen immer häufiger zu Erfolg: Angriffe mit horrenden Erpressungssummen dominieren auch 2022 die Nachrichtenspalten weltweit.

Einfache Erpressungen und rein technische Angriffe gehören dabei aber der Vergangenheit an. Cyberkriminelle setzen längst auf ausgeklügelte und psychologisch versierte Erpressungstaktiken – und knüpfen weitere Angriffe an sie an. Bei diesen sogenannten Mehrfacherpressungen (Multiple Extortions) setzen die Cyberkriminellen zusätzlich zum initialen Raub und zur Verschlüsselung von sensiblen Daten (sowie der Drohung, diese bei Nicht-Zahlung zu veröffentlichen) beispielweise auf DDoS-Attacken, Crypto-Mining oder auch Botnetze. So legen die Angreifenden etwa mithilfe von DDoS-Attacken die Webseiten ihrer Opfer lahm, bis diese sich ihren Forderungen fügen.

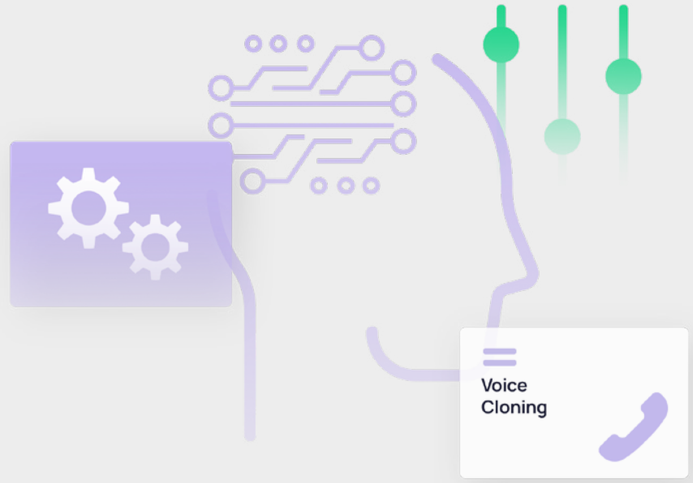
Im April 2021 griff die Ransomware-Gruppe REvil den Computerhersteller Quanta Computer an. Als das Unternehmen der Lösegeldforderung nicht nachging, versuchten es die Angreifenden bei Apple – einem Auftraggeber von Quanta Computer – und drohten damit, die zuvor beim Hersteller gestohlenen Daten zum neuesten MacBook Pro zu veröffentlichen. Es blieb unklar, ob die Lösegeldforderung von 50 Millionen US-Dollar von Apple gezahlt wurde.[11] Mitte 2022 attackierte die Gruppe ALPHV/Black Cat ein Luxusspa

[10] European Union Agency for Cybersecurity (ENISA) (2021). ENISA Threat Landscape 2021.
[11] ComputerBase (2021). Quanta: Angreifer stehlen Baupläne des nächsten MacBook Pro.
[12] Krebs on Security (2022). Ransomware Group Debuts Searchable Victim Data.

in den USA und veröffentlichte anschließend persönliche Daten von mehr als 4.000 Besucherinnen und Besuchern des Spas. Die Daten waren anschließend mit Suchoption frei verfügbar auf einer Website – eine tückische Methode, um das Opfer der Ransomware zur Überweisung des Lösegelds zu zwingen.[12] Neben dem Schaden für die Wiederherstellung der Systeme und das Lösegeld selbst, müssen Organisationen in Folge eines solchen Angriffs deshalb oft auch mit irreparablen Image-Schäden rechnen.

Praxistipp

Die Angriffstaktiken der Cyberkriminellen erweitern sich stetig. Halten Sie aus diesem Grund zum einen Ihre technischen Schutzmaßnahmen aktuell und sichern Sie Ihre Tools gegen Angriffe ab. Erstellen Sie außerdem regelmäßige Backups. Halten Sie zugleich aber auch Ihre Sensibilisierungsprogramme stets auf dem Laufenden. Auch bei Ransomware-Angriffen ist das erste Einstiegstor in vielen Fällen der Faktor Mensch – oft eine Phishing-Mail. Stärken Sie Ihre Sicherheitskultur und sorgen Sie dafür, dass Sie für den Angriffsfall eine Incident Response geplant haben, um Schäden zu minimieren.



04 Deepfakes: Harmlose Spielerei oder gefährlicher Betrug?

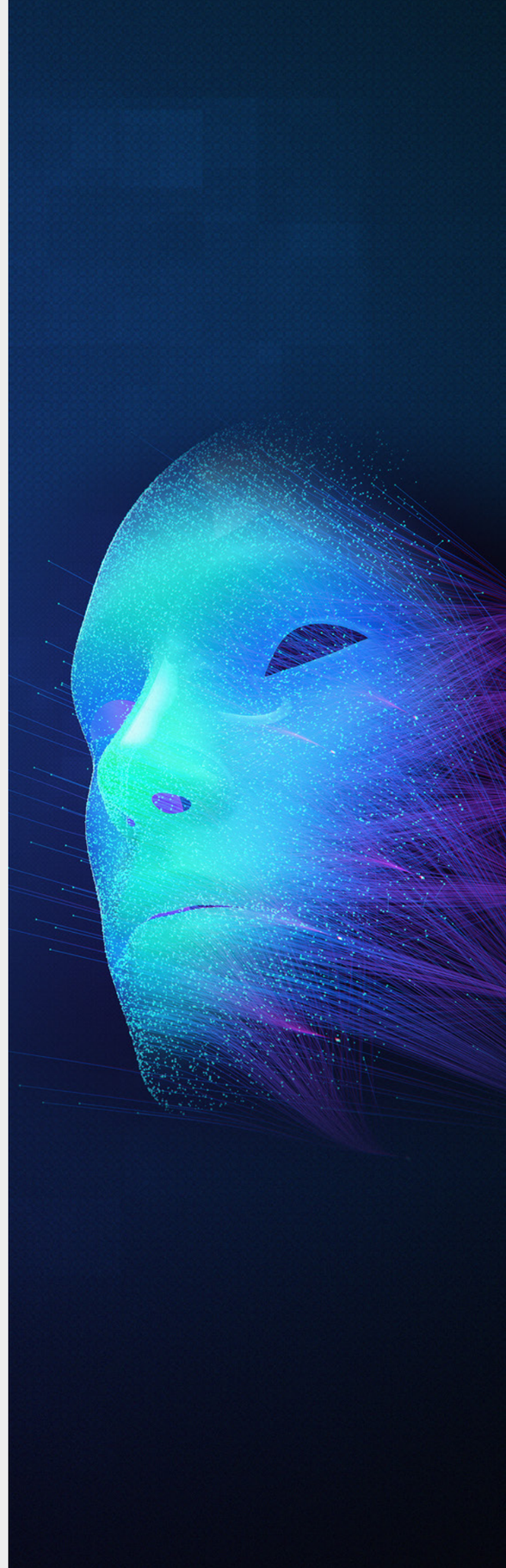
Künstliche Intelligenz (KI) ist für uns mittlerweile ein fast alltäglicher Begleiter – von Sprachassistenten wie Siri und Alexa über intelligente Automatisierungstool bis hin zum Smart Home. Doch auch Cyberkriminelle haben schnell erkannt, dass sie diese Technologien für Social Engineering und Phishing nutzen und ihre Gewinne so maximieren können.

Voice Phishing (Vishing) wird bereits erfolgreich mit Deepfake-Technologien kombiniert und dazu genutzt, Phishing-Mails zu legitimieren. Beim sogenannten „Voice Cloning" imitieren die Angreifenden die Stimme eines Vorgesetzten künstlich und bringen Mitarbeitende anschließend über einen Anruf dazu, sensible Informationen freizugeben oder Überweisungen zu tätigen. Kriminellen war es so bereits 2020 gelungen, eine Bank in Hongkong um 35 Millionen Dollar zu bestehlen.[13]

Die zunehmende Qualität bei gleichzeitig geringer werdendem Erstellungsaufwand von Deepfakes versprechen Cyberkriminellen in Zukunft noch glaubhaftere und damit erfolgreichere Angriffe. Eindrücklich zeigen das etliche Pop-Culture-Beispiele und die FaceApp, mit der Laien einfach gefälschte Audio-Video-Inhalte erstellen können. Viele der Deepfakes sind mit bloßem Auge kaum noch von ihren realen Vorbildern zu unterscheiden. Zum anderen sorgten zuletzt auch Cyberangriffe auf Basis der Deepfake-Technologie für Aufruhe und Verwunderung. So wurde Berlins Bürgermeisterin Franziska Giffey von einem scheinbar durch Künstliche Intelligenz manipulierten Vitali Klitschko zum Ukraine-Krieg in einer Videokonferenz kontaktiert. Wie sich wenig später herausstellte, handelte es sich hier zwar vermutlich lediglich um einen „Cheapfake", bei dem manipuliertes Audiomaterial über bereits existentes Videomaterial gelegt wird. Aber der Angriff zeigte deutlich, wie Deepfakes zu gefährlicher Desinformation und Manipulation führen können.[14]

Praxistipp

Obwohl bereits verschiedene Forschungsgruppen an der Entwicklung eines KI-basierten Screening-Tools arbeiten, um Deepfakes zu erkennen, reichen rein technische Schutzmaßnahmen im Kampf gegen die sich stetig verbessernde Technologie noch nicht aus. Gleichzeitig werden Deepfakes durch ihre Verbreitung in der Popkultur oft als harmlos abgestempelt. Treffen Sie in Ihrer Organisation daher KI-assistierte, menschliche Schutzvorkehrungen und schaffen Sie Awareness für die Gefahren. Rüsten Sie Ihre Mitarbeitenden mit den richtigen Tools aus, sodass Sie schädliche Inhalte schnell erkennen und im Zweifelsfall melden können.



[13] Forbes (2021). Fraudsters Cloned Company Director's Voice in $35 Million Bank Heist, Police Find.
[14] ZDF (2022). Videokonferenz mit Giffey: Falscher Klitschko doch kein Deepfake?

15 Engels, Barbara (2021). Cybersicherheit. 52,5 Mrd. Euro Schaden durch Angriffe im Homeoffice. IW-Kurzbericht, Nr. 54, Köln.

16 ZDNet (2021). Everyone is burned out. That's becoming a security nightmare.

17 Bloomberg (2021). Hackers Breached Colonial Pipeline Using Compromised Password.

05 Hybrides Arbeiten: Informationssicherheit in den Händen der Mitarbeitenden

Seit Beginn der COVID-19-Pandemie steigt die Zahl der Organisationen, die auf mobiles oder hybrides Arbeiten setzen, rasant an. Dabei sehen sie sich auch einem erhöhten Risiko von Cyberangriffen ausgesetzt. 75 Prozent der für den Human Risk Review 2022 Befragten bestätigen, dass mobile Arbeitsmodelle eine Rolle in der Verschärfung der Bedrohungslage gespielt haben.

Die Gefahr ist aus verschiedenen Gründen erhöht:

- **Fehlende technische Absicherung**

  Zurzeit sichern lediglich 38 Prozent der deutschen Organisationen Geschäftshandys oder Laptops mit einer Verbindung zum Firmennetzwerk ab.[15]

- **Neue Angriffskanäle**

  Neue Kollaborationstools wie Microsoft Teams oder auch Mobiltelefone, die im Remote-Work-Setting häufiger genutzt werden, bieten neue Angriffsflächen.

- **Unsicherheit**

  Von Pandemie und Homeoffice erschöpft, setzen sich Mitarbeitende wesentlich weniger mit Sicherheitsrichtlinien auseinander – und sind so fehleranfälliger.[16]

Die Folgen veranschaulicht beispielsweise der folgenreiche Ransomware-Angriff auf Colonial Pipeline im April 2021: Ein unvorsichtig genutztes Passwort fiel in die Hände der Cyberkriminellen und ermöglichte den Remote-Zugriff auf den VPN-Account eines Mitarbeitenden und zahlreiche interne Systeme und Daten. Die Folgen: Eine wochenlange Versorgungsunterbrechung mit Benzin an der US-amerikanischen Ostküste.[17]

Praxistipp

Wechseln Ihre Mitarbeitenden ins Homeoffice, übergeben Sie ihnen einen Großteil der Kontrolle über die Informationssicherheit ihrer Systeme. Stellen Sie sicher, dass Ihr Team weiß, worauf es ankommt. Versetzen Sie Ihre Mitarbeitenden in Trainingssituationen, die ihrer persönlichen Arbeitssituation entsprechen. Kontextbasierte Sensibilisierungsmaßnahmen wie personalisierte Phishing-Simulationen minimieren das Risiko, gezielten Cyberangriffen zum Opfer zu fallen.

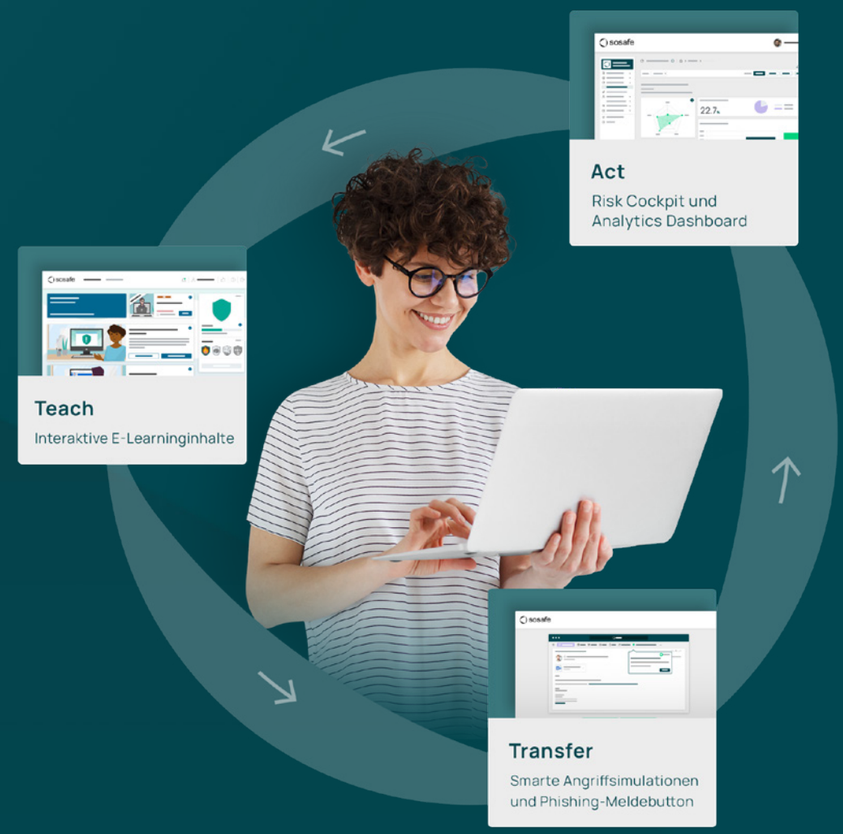
Der Human Risk Review 2022

Mehr zum Thema Cybercrime-Trends und zur aktuellen Cyber-Bedrohungslage finden Sie im Human Risk Review 2022.

Hier lesen →

Über SoSafe

SoSafe hilft Organisationen, ihre Sicherheitskultur aufzubauen und Cyberrisiken zu minimieren. Die psychologisch fundierte und DSGVO-konforme Awareness-Plattform setzt auf personalisierte Lerninhalte und intelligente Angriffssimulationen. Mitarbeitende lernen so, sich aktiv vor Online-Bedrohungen zu schützen. Die Plattform ist einfach implementier- und skalierbar; umfassende Analysen messen den ROI und zeigen Schwachstellen auf. Damit fördert SoSafe das sichere Verhalten aller Mitarbeitenden.



SoSafe GmbH
Lichtstraße 25a
50825 Köln

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