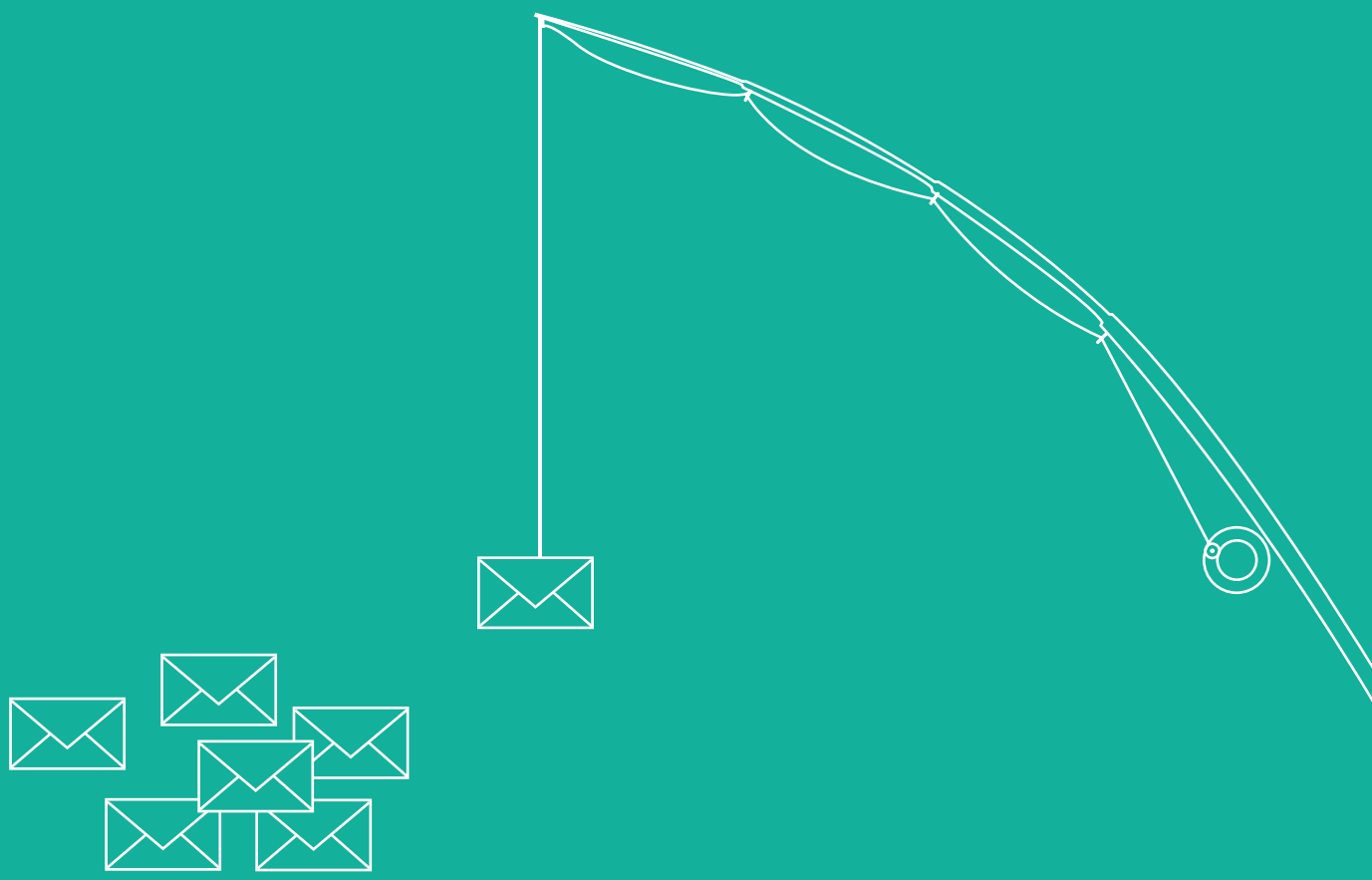


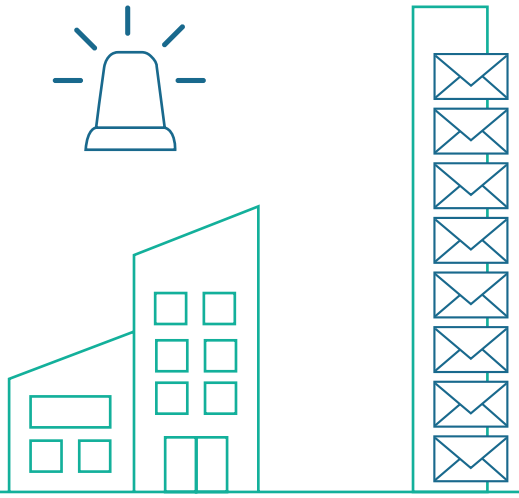
Best Practices Phishing-Simulationen

Dos and Don’ts für nachhaltiges Awareness-Building in Unternehmen

SoSafe
Cyber Security Awareness

Inhaltsverzeichnis

Warum Unternehmen ihre Mitarbeiter für Phishing-Angriffe sensibilisieren sollten



Etwa 92% aller Angriffe auf Unternehmen beginnen mit einer Phishing-Mail.

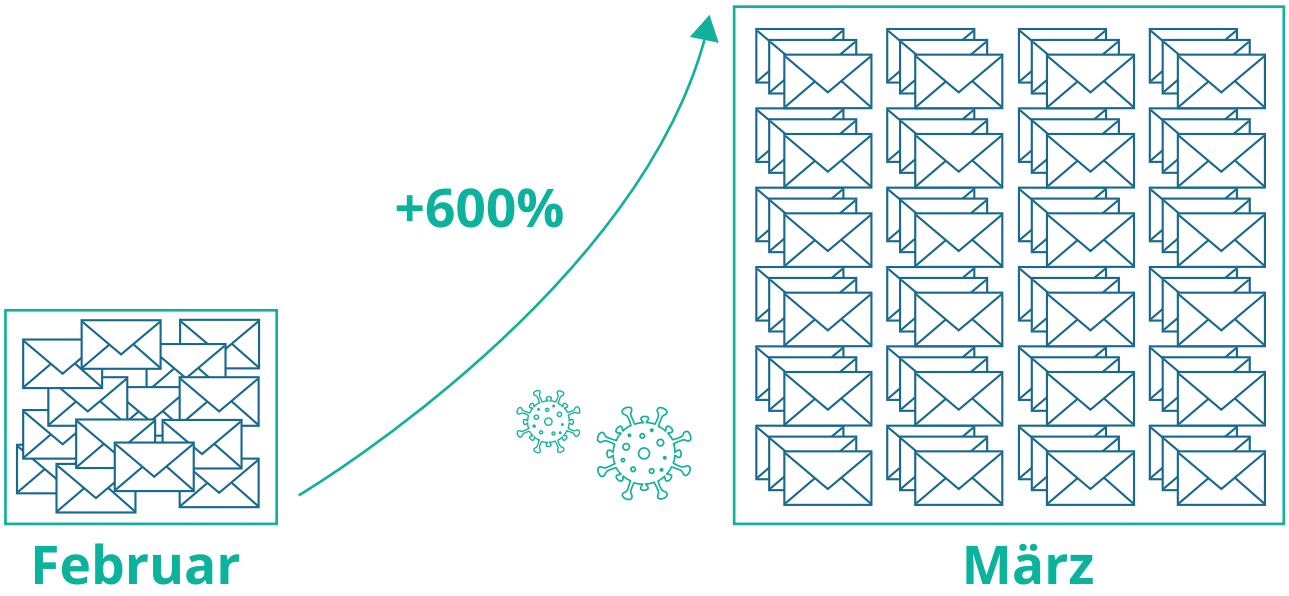
Die Anzahl der Cyberangriffe auf sowohl Privatpersonen als auch Unternehmen ist in den letzten Jahren kontinuierlich gestiegen. In einer aktuellen Bitkom-Studie zum Wirtschaftsschutz berichten knapp drei Viertel der Unternehmen von einer starken Zunahme der Cyberangriffe über die letzten zwei Jahre, 82% gehen von einem weiteren Anstieg in den nächsten zwei Jahren aus.[1] Den Schätzungen des BKA zufolge könnte sich der Schaden der Cyberkriminalität auf mehr als 100 Milliarden Euro jährlich belaufen.[2]

Besonders weit oben auf der Liste der beliebtesten Angriffstaktiken der Hacker steht dabei nach wie vor Phishing. So beginnen über 90% der Angriffe auf Unternehmen mit einer Phishing-Mail.[3] Als Reaktion auf die Coronakrise stieg allein zwischen Februar und März 2020 die Anzahl der versendeten Phishing-Mails nochmals um fast 600% – die Hacker nutzten die Verunsicherung in der Wirtschaft gezielt für ihre Zwecke aus.[4]

Unternehmen sind dabei besonders gefährdet: sie müssen mit schweren wirtschaftlichen Schäden rechnen, wenn sie Opfer von Cyberkriminellen werden. So sind temporäre Betriebsausfälle oder hohe Lösegeldzahlungen potenzielle Folgen eines Phishing-Angriffs. Im Allianz Risk Barometer 2020 schätzen Unternehmen weltweit deshalb erstmals Cybervorfälle als das größte Risiko für ihr Geschäft ein.[5]

[1] Bitkom (2020). Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt.
[2] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2019). Die Lage der IT-Sicherheit in Deutschland 2019.
[3] Verizon (2020). Data Breach Investigation Report 2020.
[4] Europäische Agentur für Cybersicherheit (ENISA) (2020). Understanding and dealing with phishing during the covid-19 pandemic.
[5] Allianz (2020). Allianz Risk Barometer 2020: Cyber steigt zum weltweiten Top-Risiko für Unternehmen auf.

Als Reaktion auf die Coronakrise stieg zwischen Februar und März 2020 die Anzahl der versendeten Phishing-Mails nochmals um fast 600%.



Deshalb sind Spam-Filter allein nicht ausreichend

Obwohl technische Barrieren wie Spam-Filter und Virenschutzprogramme bereits einen Teil der schädlichen E-Mails und Malware abfangen, reichen sie in Zeiten von „Spear Phishing“ (siehe Infobox auf S. 5) längst nicht mehr aus, um umfassend vor Cyberangriffen zu schützen.

So schaffte es laut Avanan’s Global Phish Report 2019 immer noch ein Viertel aller Phishing-Mails durch Microsofts Advanced Threat Protection Filter und landete damit in den Postfächern der Nutzer.[6]

Gleichzeitig werden die Angriffe der Hacker immer raffinierter und komplexe Angriffstaktiken wie „Dynamite Phishing“ häufiger. Über infizierte Systeme sammelte so zum Beispiel der Trojaner Emotet in den vergangenen Jahren vorhandene Mailverläufe, um auf Basis dieser automatisiert weitere Phishing-Mails zu erzeugen und zu verteilen. Die meisten klassischen Spam-Filter sind mit solch einer Vorgehensweise überfordert und können die Angriffe nicht zielsicher identifizieren.

[6] Avanan (2020). 2019 Global Phish Report.

Spear-Phishing und Social Media Crawling

Beim Spear-Phishing täuschen Cyberkriminelle ihre Opfer zielgerichtet mit der Absicht, finanzielle oder persönliche Schäden zu verursachen. Im Vergleich zum „normalen" Phishing zielen die Attacken beim Spear-Phishing auf eine eng begrenzte Nutzergruppe, über die die Täter im Vorhinein genaueste Informationen eingeholt haben.

Eine der bekanntesten Formen des Spear-Phishings ist der CEO-Fraud, bei denen sich die Hacker als Geschäftsführer oder andere Angestellte in führenden Positionen ausgeben und so Geschäftsprozesse beeinflussen. Beim Automobilzulieferer Leoni konnten die Cyberkriminellen 2016 so knapp 40 Millionen Euro erbeuten.[7] Nützliche Informationen für ihre Zwecke finden die Hacker an verschiedensten Quellen – von Social-Media-Profilen und beruflichen Netzwerken über die Firmenwebsite bis hin zum persönlichen Austausch auf Messen oder mit Lieferanten und Kunden. Beim Teilen von unternehmensinternen, aber auch privaten Informationen im Netz ist also jederzeit Vorsicht geboten.

Phishing-Simulationen sollten mit Hinblick auf die Häufigkeit der Taktik natürlich auch Spear-Phishing-Angriffe abbilden. Vorsicht ist allerdings geboten, wenn es um die Anreicherung der simulierten Phishing-Mails mit Social-Media-Daten oder anderen Individual-Daten der Mitarbeiter geht. Die Simulation mag so Phishing zwar noch einen kleinen Schritt realitätsgetreuer widerspiegeln, aus datenschutzrechtlicher Sicht ist die Nutzung und Anreicherung persönlicher Daten (auch, wenn sie im öffentlichen Raum zugänglich sind) allerdings höchst problematisch. Denn die Mitarbeiter haben Ihnen als Arbeitgeber hierzu nicht explizit ihr Einverständnis gegeben.

[7] Handelsblatt (2017). Betrugsmasche „CEO Fraud": Abgezockt vom falschen Chef.

Der Faktor Mensch bei der IT-Sicherheit

Für Unternehmen heißt es deshalb besonders wachsam zu sein und die Mitarbeiter für die lauernden Gefahren aus dem Netz zu sensibilisieren. Für Phishing-Angriffe nutzen Cyberkriminelle immer häufiger gezielt psychologische Taktiken und manipulieren die Emotionen der Empfänger, um ihr Ziel durchzusetzen.

Beim Social Engineering (siehe Infobox auf S. 7) setzen die Hacker etwa auf das Erzeugen von Druck, das Wecken von Neugier oder das Auslösen von Angst, damit die Empfänger der Phishing-Mails mit diesen interagieren und ihre Daten preisgeben.

Geschulte Mitarbeiter, die bewusst mit solchen IT-Sicherheitsrisiken umzugehen wissen, können aber frühzeitig reagieren und so fatale Vorfälle im Unternehmen abwehren. Nicht zuletzt deshalb fordern verschiedene Compliance-Frameworks, wie die ISO 27001 oder auch die DSGVO, eine kontinuierliche Schulung der Mitarbeiter in IT-Sicherheitsthemen – im Falle der ISO 27001 auch eine Form von simulierten Social-Engineering-Angriffen. Neben Informationskampagnen rund um Cyber Security sowie Mitarbeitertrainings, etwa in Form von digitalen und interaktiven Lernplattformen, bieten sich daher insbesondere Phishing-Simulationen für ein kontinuierliches Awareness-Building in Unternehmen an.

Für Phishing-Angriffe nutzen Cyberkriminelle immer häufiger gezielt psychologische Taktiken und manipulieren die Emotionen der Empfänger, um ihr Ziel durchzusetzen.

Social Engineering im Wandel der Zeit

Social Engineering – die emotionale Manipulation von Personen zum Hervorrufen bestimmter Verhaltensweisen – ist bei weitem kein neues Phänomen.

Bereits im 17. Jahrhundert konnten Betrüger mit der „Advance-Fee"-Masche des sogenannten „Spanischen Gefangenen" hohe Summen erbeuten. Unter dem Vorwand in einem spanischen Gefängnis einzusitzen, den Ort eines vergrabenen Schatzes zu kennen und diesen bei ihrer Befreiung preiszugeben, verschickten sie Briefe an wohlhabende Personen. Diese liehen den vermeintlichen Gefangenen schließlich Geld, um ihnen eine Flucht zu ermöglichen und sich selbst an dem Schatz zu bereichern. Statt eines Schatzes erwartete sie aber die bittere Erkenntnis, dass sie einem ausgeklügelten Betrug zum Opfer gefallen waren.

Das Prinzip des Social Engineering hat sich bis heute kaum verändert, lediglich die Kanäle sind andere – E-Mails, SMS, Privatnachrichten in sozialen Netzwerken und Telefonate ersetzen die Briefe von früher. Mit der Popularisierung des Internets wurden in den 90ern Cyberkriminelle auf die Methodik aufmerksam.

Beim Phishing nutzen sie seither die menschlichen Emotionen gezielt für ihre Zwecke aus und kommen über psychologische Manipulation an ihr Ziel. Dabei werden die Taktiken raffinierter: Mit der zunehmenden Menge an Daten, die öffentlich im Netz verfügbar sind, können Hacker ihre Opfer immer gezielter angreifen und hinters Licht führen.

Phishing-Simulationen: Probe für den Ernstfall

Im Zuge von Phishing-Simulationen werden Cyberangriffe nachgestellt und vorgetäuscht, um Mitarbeiter für die Gefahren solcher Attacken zu sensibilisieren. Bei der Umsetzung dieser Simulationen gibt es jedoch einige Fallstricke. In der Vergangenheit wurden sie oftmals als reines Test-Tool genutzt, um personenscharf zu ermitteln, welche Mitarbeiter ein „Sicherheitsrisiko" darstellen. Ein solches Vorgehen führt verständlicherweise zu Frustration bei den Empfängern – nicht nur, aber vor allem dann, wenn die E-Mails ohne Ankündigung im Postfach landen. Der eigentliche Sinn und Zweck der Simulation als Lehr- und Lernmittel wird so verfehlt. Die Empfänger fühlen sich bloßgestellt und verlieren das Interesse an echter Phishing-Prävention.

Bei Phishing-Simulationen sollte deshalb vielmehr das Lernen am Objekt im Mittelpunkt stehen. Um dies zu gewährleisten, muss die Simulation im Vorfeld transparent kommuniziert werden. Darüber hinaus sollte sie von Lerneinheiten begleitet werden. Direkt nach dem Klick auf eine simulierte Phishing-Mail erhalten die Mitarbeiter im besten Fall eine differenzierte Aufklärung (einen sogenannten „Teachable Moment"), indem sie beispielsweise durch die entsprechende E-Mail geführt werden und ihnen erläutert wird, an welchen Punkten sie den Angriff hätten erkennen können. Sie erfahren so unmittelbar, in welchen Formen Phishing auftritt und das, ohne ein echtes Sicherheitsrisiko einzugehen.

Das Bewusstsein der Empfänger für derartige IT-Sicherheitsrisiken wird so gestärkt und die Handlungsfähigkeit im Fall eines tatsächlichen Angriffs gesichert. Statt die Mitarbeiter also als Risiko für die IT-Sicherheit eines Unternehmens einzuordnen, sollte eine Phishing-Simulation von der gegenteiligen Annahme getrieben sein: Der Mensch kann mit einem Bewusstsein für IT-Risiken und durch den adäquaten Umgang mit diesen eine zusätzliche, sicherheitsrelevante Barriere darstellen.

Statt die Mitarbeiter also als Risiko für die IT-Sicherheit eines Unternehmens einzuordnen, sollte eine Phishing-Simulation von der gegenteiligen Annahme getrieben sein: Der Mensch kann mit einem Bewusstsein für IT-Risiken und für den Umgang mit diesen eine zusätzliche, sicherheitsrelevante Barriere darstellen.

Best Practices Phishing-Simulation

Phishing-Simulationen sind folglich trotz ihres umstrittenen Einsatzes in der Vergangenheit beliebte und notwendige Tools, um die Cyber Security Awareness von Mitarbeitern auf moderne Art und Weise zu erhöhen. Denn bei richtiger und systematischer Durchführung können sie nachhaltig die Klick- und Interaktionsraten mit Phishing-Mails senken und so Unternehmen vor fatalen (finanziellen) Schäden bewahren.

Es gilt jedoch, die bereits angedeuteten Stolpersteine aus dem Weg zu räumen, damit eine Simulation den gewünschten Effekt erzielt. Mit den folgenden Tipps gestalten Sie Ihre Phishing-Simulation effektiv und etablieren eine schützende Sicherheitskultur in Ihrem Unternehmen.

1 Die technischen Weichen für die Phishing-Simulation stellen

Bei einer Phishing-Simulation werden spiegelbildlich zu echten Hackerangriffen Phishing-Mails verschickt, die darauf abzielen, Nutzerdaten abzufangen. So enthalten Sie etwa fingierte Anhänge oder Links, die zu Webseiten mit gefälschten Login-Masken führen.

Der einzige Unterschied: Von den simulierten Mails geht natürlich kein Sicherheitsrisiko aus. Konventionelle technische Filter können unter Umständen jedoch nicht erkennen, dass es sich bei einer simulierten Phishing-Mail um eine harmlose Schulungsmaßnahme handelt.

Um sicherzustellen, dass die Nachrichten im Postfach der Empfänger landen, ist es deshalb unausweichlich, die IT-Systeme auf die Phishing-Simulation vorzubereiten. So muss etwa die IP-Adresse der verwendeten Mailserver auf die Whitelist der entsprechenden IT-Sicherheitssysteme gesetzt werden. In Absprache mit Ihrem Simulations-Anbieter sollten dazu alle relevanten Informationen zur Phishing-Simulation zusammengetragen und die relevanten, anzupassenden Systeme identifiziert werden. Der Dienstleister sollte selbst größten Wert auf Datensicherheit (im Sinne der DSGVO) legen und Sie individuell dazu beraten, wie Sie beim Whitelisting allen Sicherheitsstandards nachkommen. Bei in Deutschland oder der EU gehosteten Lösungen werden diese Ansprüche in den meisten Fällen erfüllt (siehe Interview auf S. 13).

Durch Testversände ausgewählter Phishing-Mails, welche die Bandbreite der Simulation widerspiegeln, stellen Sie anschließend sicher, dass diese ankommen und korrekt dargestellt werden. Gerade bei der technischen Vorbereitung einer Phishing-Simulation lohnt es sich – falls die Kampagne nicht ohnehin von der Abteilung aus gesteuert wird – die IT und das Helpdesk mit ins Boot zu holen. Als erste Ansprechpartner rund um IT-Sicherheitsfragen können die Kollegen nicht nur die entsprechenden Vorkehrungen treffen, sondern sind auch auf etwaige Rückfragen der Mitarbeiter während der Simulation vorbereitet. Das trägt maßgeblich zu einem stabilen und effektiven Ablauf bei.

2 Die Phishing-Simulation ankündigen

Das A und O einer jeden lernorientierten Phishing-Simulation ist die Kommunikation – vor, während und nach der Maßnahme.

Nicht nur IT, Helpdesk sowie Betriebs- oder Personalrat sollten dementsprechend mit in die Planung und Durchführung miteinbezogen werden, sondern auch die Empfänger der simulierten Phishing-Mails müssen frühzeitig informiert werden.

Das ist in gleich mehrfacher Hinsicht sinnvoll: Zum einen kann so etwaige Verunsicherung vermieden werden. Die Simulation wird auf positive Weise als Lernmaßnahme positioniert, die den Mitarbeitern Wissen vermittelt, das sie auch im privaten Kontext nutzen können. Zum anderen kann eine frühzeitige Ankündigung der Phishing-Simulation die Motivation der Mitarbeiter erhöhen. Ist ihnen bewusst, dass die Simulation im Sinne einer besseren Sicherheitskultur und zum Schutz vor sicherheitsrelevanten Angriffen durchgeführt wird, sind sie eher dazu bereit, sich mit den Lerninhalten auseinanderzusetzen. Stellen Sie deshalb die anstehende Phishing-Simulation einige Wochen vor dem Startschuss, beispielsweise in einer Rundmail, vor und machen deutlich, dass es sich hier um eine Lernmöglichkeit für die Mitarbeiter handelt.

Gehen Sie dabei etwa auf folgende Aspekte ein:

- Simulation als Schulung und Lernmöglichkeit
- Umfang und Zeitraum der Simulation
- Ablauf der Simulation
- Anonymität der Simulation (siehe Abschnitt 3)
- Ansprechpartner für Rückfragen zur Simulation

Daten aus SoSafe-Simulationen zeigen, dass eine solche Ankündigung etwa zwei bis drei Wochen vor dem Start der Simulation die erhobenen Daten – beispielsweise Klick- und Interaktionsraten – nicht signifikant verfälscht. Ein konkretes Startdatum sollte hier allerdings nicht genannt werden. Das könnte implizieren, dass die Mitarbeiter erst ab dem genannten Zeitpunkt aufmerksam sein müssen. Wie aktuelle Statistiken zu Phishing verdeutlichen, ist es aber wichtiger denn je, jederzeit bewusst mit dem Risiko eines potenziellen Angriffs umzugehen.

---

3 Die Anonymität und den Lernaspekt der Phishing-Simulation hervorheben

Als Tool des klassischen Penetration-Testings stand bei Phishing-Simulationen in der Vergangenheit häufig das Identifizieren von Sicherheitslücken im Vordergrund.

Die Simulationen wurden daher teilweise auf personenscharfer Ebene durchgeführt, Mitarbeiter manchmal sogar mit ihrem Verhalten konfrontiert oder – gerade im angelsächsischen Raum – gar personelle Konsequenzen gezogen. Schuldzuweisungen und Bloßstellungen wirken sich allerdings negativ auf die Lernbereitschaft und Motivation der Mitarbeiter aus.

Effektiver und nachhaltiger ist es daher, Simulationen anonym durchzuführen, d.h. ohne die Erfassung und Verarbeitung individueller Verhaltensdaten. Bereits in der Ankündigung einer Simulation sollte den Nutzern verdeutlicht werden, dass es sich bei der Maßnahme keineswegs um einen Test handelt. Die Nutzer sollten sich nicht überwacht fühlen, sondern die Möglichkeit haben, in ihrem eigenen Lerntempo und nach bestem Gewissen die Phishing-Simulation zu durchlaufen. Vermitteln Sie, dass diese nicht mit einem Test gleichzusetzen ist. Vielmehr handelt es sich um eine Möglichkeit, die einzelnen Mitarbeiter und das ganze Unternehmen vor schädlichen Cybervorfällen zu schützen. Indem Sie den Mitarbeitern ihre Rolle als „menschliche Firewall“ bewusst machen, steigern Sie die Effektivität der Schulungsmaßnahme.

In Bezug auf die zu vermeidende Bloßstellung ist es außerdem wichtig, die Phishing-Simulation an die jeweiligen Kenntnisse und Anforderungen der Nutzerbasis anzupassen. Sind sämtliche simulierten Phishing-Mails zu leicht als solche zu erkennen, sinkt zwangsläufig die Motivation der Nutzer. Sie fühlen sich gerüstet für echte Angriffe, obwohl diese oftmals auf ausgeklügelten, psychologischen Taktiken basieren.

Aber auch ausschließlich schwierig zu erkennende Simulationen wirken sich negativ auf die Motivation der Nutzer aus. Im schlimmsten Fall fühlen sie sich hintergangen und in die Falle gelockt – das gilt es in jedem Fall zu vermeiden.

Vermitteln Sie, dass die Phishing-Simulation nicht mit einem Test gleichzusetzen ist. Vielmehr handelt es sich dabei um eine Möglichkeit, die einzelnen Mitarbeiter und das ganze Unternehmen vor schädlichen Cybervorfällen zu schützen.

Ausgewogenheit ist hier der Schlüsselpunkt: Mischen Sie in der Simulation leichte mit herausfordernden Mails, um den Nutzern regelmäßig Erfolgserlebnisse zu ermöglichen. Damit wird außerdem das reale Phishing-Spektrum widergespiegelt – nicht alle Phishing-Mails sind zwangsläufig Spear-Phishing-Attacken, gleichzeitig sind nicht alle Phishing-Mails komplett unpersönlich gehalten. Indem Sie also eine sinnvoll durchmischte Simulation anbieten, vermeiden Sie Frustrationen seitens der Nutzer, die von Ihnen erhobenen Statistiken zur Simulation sind realitätsnah und der Lernaspekt steht weiterhin im Fokus der Maßnahme.

Interview:
Datenschutz bei Phishing-Simulationen: DSGVO, Privacy Shield und Co.

Interview mit Benedikt Woltering, Rechtsanwalt und Legal Advisor bei der SoSafe GmbH

Sind Phishing-Simulationen datenschutzrechtlich unbedenklich?

Ja und nein. Grundsätzlich sind Phishing-Simulationen natürlich ein Thema für den Datenschutz, denn im Zuge der Maßnahme werden üblicherweise personenbezogene Daten verarbeitet. Viele Anbieter reichern die simulierten Phishing-Mails zum Beispiel mit Mitarbeiterdaten an, um echte Hackerangriffe realitätsnah widerzuspiegeln. Solange diese Daten in angemessenem Umfang und nur „zum Zwecke des Beschäftigungsverhältnisses" (§ 26 BDSG) – etwa um die IT-Sicherheit zu stärken – genutzt werden, sind die Simulationen aus datenschutzrechtlicher Sicht aber unbedenklich.

Eine DSGVO-konforme Phishing-Simulation – wie sieht die aus?

Im Sinne der DSGVO sind die Mitarbeiterdaten in jedem Fall zu schützen. Phishing-Simulationen werden zwar realistischer je mehr Daten eingebunden werden, man begibt sich so aber schnell in eine rechtliche Grauzone. In welchem Ausmaß dient die Nutzung der Daten noch ausschließlich dem Zweck der Beschäftigung und einer erhöhten IT-Sicherheit? Hier gilt es, ein vernünftiges Maß zu finden und für die Mitarbeiter invasive Vorgehensweisen wie Social Media Crawling zu vermeiden.

Gleichzeitig sollten die Nutzer keine direkten Konsequenzen zu fürchten haben. Deshalb die klare Empfehlung: Phishing-Simulationen anonym auswerten und keine personenscharfen Kontrollen durchführen. Außerdem sollten Unternehmen auf Anbieter aus der EU setzen.

Wieso ist es so wichtig, einen Anbieter aus der EU zu wählen?

Die DSGVO verbietet die Verarbeitung und Speicherung von Daten an Orten, an denen nicht DSGVO-vergleichbares Datenschutzniveau herrscht. Die Aussage trifft auf viele Länder außerhalb der EU zu, so etwa die USA. Dort haben Behörden weitgehende Zugriffsrechte und EU-Bürgern steht im Zweifel kein Rechtsweg zur Durchsetzung ihrer Interessen offen.

Das Privacy Shield Abkommen, das den Datenaustausch zwischen den USA und Europa unzureichend regelte, wurde deshalb vom EuGH als rechtswidrig erklärt. Solange es keine eindeutigen Rechtsprechungen gibt, begibt man sich mit einer in den USA gehosteten Lösung so in unsichere Gewässer. Die Berliner Datenschutzbeauftragte Maja Smoltczyk hat deshalb nach dem Urteil des EuGH dazu aufgefordert, Dienstleistungen aus der EU zu nutzen, damit alle datenschutzrechtlichen Anforderungen erfüllt sind und Nutzer nicht um den Missbrauch ihrer Daten fürchten müssen.

4 Die Phishing-Simulation an die Nutzerbasis anpassen

Damit Phishing-Simulationen Wirkung zeigen, sollten sie im Idealfall auf die Gruppe der Empfänger zugeschnitten werden.

Dabei geht es sowohl um die Anpassung an individuelle Empfänger (z.B. persönliche Anrede) als auch an die Belegschaft als Ganzes (z.B. Nutzung firmenspezifischer E-Mail-Signaturen). Folgende Fragen können zum Beispiel in die Überlegungen miteinbezogen werden:

- Welche Themen sind derzeit im Unternehmen von besonderer Relevanz?
- Welche Abläufe und aktuellen Ereignisse könnten von echten Angreifern aufgegriffen werden?
- Gibt es spezielle „Maschen“, die für bestimmte Funktionen im Unternehmen, beispielsweise die Personal- oder Vertriebsabteilung, besonders gut funktionieren? Auch Führungskräfte stehen häufig ganz besonders im Fokus (siehe Infobox auf S. 5).

Auch grafische Aspekte können eine Rolle spielen:

- Sollen die Mails das Corporate Design Ihres oder eines anderen Unternehmens nachahmen?
- Werden täuschend echte Signaturen verwendet?

Cyberkriminelle nutzen oft Daten aus öffentlichen Quellen oder fangen interne Informationen ab, um Mitarbeiter damit gezielt anzugreifen. In Absprache mit Ihrem Anbieter können Sie mit Ihrer Kenntnis der Nutzerbasis dieses Verhalten nachahmen und entsprechende Simulationen erstellen. Neben der Anpassung des Schwierigkeitsgrades sollte es für einen reibungslosen Ablauf möglich sein, die Funktion des Empfängers mit in eine simulierte Phishing-Mail einfließen zu lassen oder die Sprache der E-Mails anzupassen. So werden die Nutzer eher zum Klicken animiert.

Auch thematisch gilt es, die Mails dementsprechend anzupassen. Themen und Kontexte sollten gemischt werden: Vermeintliche Mails von internen Kollegen und externen Partnern, aus dem geschäftlichen und privaten Umfeld. Denn Phishing-Mails tauchen in den unterschiedlichsten Situationen auf. Hacker greifen oft auch gesellschaftlich aktuell relevante Themen auf.[8]

So vielfältig, wie die Attacken in Erscheinung treten, sollten sie auch simuliert werden, damit die Empfänger daraus lernen und bei tatsächlich schädlichen Mails entsprechend reagieren können.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2019). Die Lage der IT-Sicherheit in Deutschland 2019.

5 Die Phishing-Simulation um Lerninhalte ergänzen

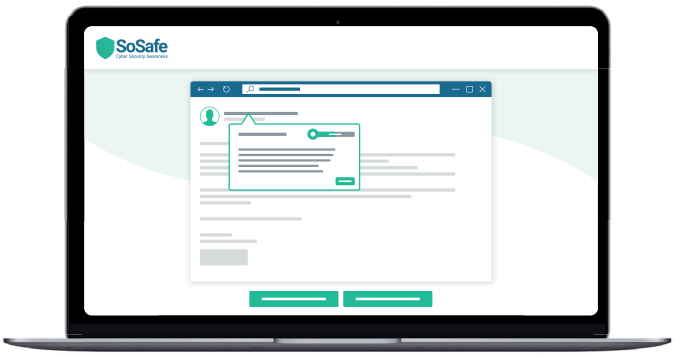
Eine Phishing-Simulation allein mag zwar typische Szenarien aufgreifen und diese den Nutzern bekannt machen. Wirklich effektiv ist die Methode als Schulungsmaßnahme aber erst dann, wenn sie von passenden Lerninhalten begleitet wird.

Um den Lernerfolg zu erhöhen, können so beispielsweise zusätzliche E-Learnings angeboten werden. Hier wird den Nutzern nahegebracht, welche Absichten Hacker verfolgen, wie Phishing-Mails funktionieren und wie sie diese erkennen können.

Gleichzeitig sollten im Idealfall gesondert auf die simulierten Phishing-Mails selbst Lerninhalte folgen. Führt ein Klick auf die simulierte Phishing-Mail ins Nichts, wissen die Empfänger möglicherweise nicht, ob diese Teil der Simulation oder ein echter Angriff ist. Der IT-Support muss mit einem erhöhten Ticketaufkommen rechnen und der erwünschte Lerneffekt verpufft.[9]

Gleiches gilt, wenn der Klick lediglich auf eine Informationsseite führt, auf der erklärt wird, dass es sich um eine simulierte Phishing-Mail gehandelt hat. Stattdessen sollten die Phishing-Mails von aufklärendem Lern-Content begleitet werden. So können im Anschluss auf einen Klick oder eine Interaktion in kleinen Kurzvideos oder „Walkthroughs“ (virtuelle Rundgänge) durch die vorgetäuschte Phishing-Mail die in dem Fall erfolgreichen Täuschungsquellen erklärt werden. Statt die Empfänger abzuschrecken, regen die Lerninhalte so dazu an, beim nächsten Mal vorsichtiger zu sein und schulen damit die Aufmerksamkeit.

Lernseiten auf der SoSafe-Awareness-Plattform regen zur Vorsicht an und vertiefen das Wissen.



[8] Neumann, Linus (2020). Hirne Hacken #36C3.

6 Eine Meldekette etablieren

Wie reagieren die Nutzer am besten, wenn sie eine fingierte Phishing-Mail als solche enttarnen?

Wie reagieren die Nutzer am besten, wenn sie eine fingierte Phishing-Mail als solche enttarnen? Etablieren Sie noch vor dem Start Ihrer Simulation eine Meldekette, damit die Empfänger der fingierten Phishing-Mails wissen, was im Fall der Fälle zu tun ist. Diese Meldekette sollte möglichst unmittelbar sein und natürlich auch über die Simulation hinaus funktionieren. Denn laut ISO-Richtlinien sollte es bei einem Notfall einen klar definierten und strukturierten Ablauf geben.

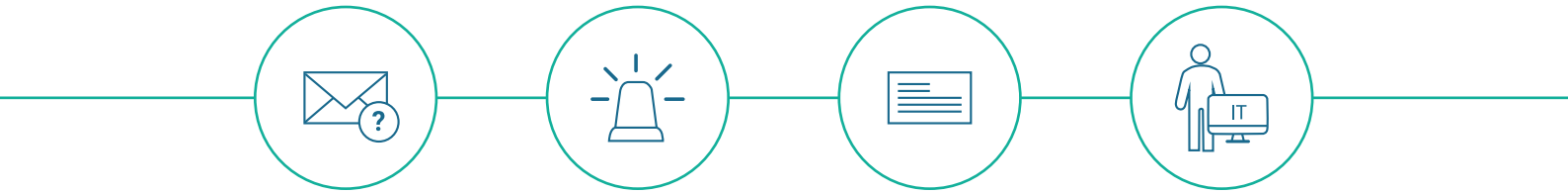
Es bietet sich etwa an, den Nutzern zu vermitteln, dass sie sich bei Verdachtsfällen unverzüglich an den IT-Support Ihres Unternehmens wenden sollten. Dabei sollten keine falschen Hemmungen entstehen: Vorsicht ist besser als Nachsicht, Prävention besser als Schadensbehebung. Etablieren Sie durch transparente Kommunikation vor, während und nach der Simulation eine Sicherheitskultur in Ihrem Unternehmen und stärken den Mitarbeitern beim bewussten Umgang mit IT-Sicherheitsrisiken den Rücken.

Eine optimierte Form einer solchen Meldekette sind in das Mailprogramm integrierte Melde-Buttons, wie sie auf der SoSafe-Plattform zum Einsatz kommen. Eine solche Ergänzung bringt zahlreiche Vorteile mit sich:

- Statistiken und Kennzahlen, wie die Melderate, verbessern sich.
- Das Ticket-Aufkommen kann besser kontrolliert werden, da simulierte Mails nicht an das Helpdesk weitergeleitet werden.
- Die Mitarbeiter werden während des Lernprozesses durch den Button positiv bestärkt.

Vorsicht ist besser als Nachsicht, Prävention besser als Schadensbehebung.

Wichtig ist in jedem Fall, dass die Mitarbeiter jederzeit wissen, wie zu handeln ist, sobald sie eine verdächtige Mail in ihrem Postfach finden – insbesondere auch dann, wenn es sich dabei nicht um eine lediglich simulierte Phishing-Mail handelt.



Etablieren Sie noch vor dem Start Ihrer Simulation eine Meldekette, damit die Empfänger der fingierten Phishing-Mails wissen, was im Fall der Fälle zu tun ist.

Der Phishing-Button von SoSafe: Als kontrollierte Melde-funktion erhöht er die Melderate und bestärkt positiv.

Case Study

dormakaba

Mit mehr als 16.000 Mitarbeitenden in über 130 Ländern ist die dormakaba-Gruppe einer der Weltmarktführer für Zutritts- und Sicherheitslösungen. Natürlich hat das Schweizer Unternehmen einen ebenso hohen Anspruch in Fragen der IT-Sicherheit. „Wir waren auf der Suche nach einer Sensibilisierungslösung gegen Phishing-Angriffe, mit der wir sämtliche Mitarbeiter erreichen – und das mit spezifischen Inhalten“, so Oliver Severin, Deputy Vice President IT Governance.

Das SoSafe-Expertenteam – bestehend aus Sicherheitsspezialisten, Psychologen und Didaktikern – erstellte entsprechende Phishing-Angriffe mit dazugehörigen Lernseiten. Berücksichtigt wurden nicht nur aktuellste Angriffsszenarien „aus der freien Wildbahn“, sondern auch mögliche künftige Attacken. „Ich war überrascht, wie schlank der Prozess dabei war. Das Team von SoSafe hat uns die meisten Schritte abgenommen und bei der Implementierung optimal unterstützt“, berichtet Christoph Bergs, Global IT Communication & Training Manager bei dormakaba.

Nach einer kurzen Baselining-Phase zur Erhebung robuster KPIs wurde der Großteil der Mails nach einem zufälligen Muster über das Jahr verteilt ausgespielt. Bereits kurz nach der Initialphase konnten substanzielle Sensibilisierungs-Effekte erzielt und nach-gewiesen werden – das Reporting-Dashboard des SoSafe-Enterprise-Paketes erlaubt dabei komplexe Schnitte. So konnten die organisationsweiten Klickraten schon während der Initialphase um mehr als zwei Drittel reduziert werden, Tendenz fallend. Gleich-zeitig erhöhte sich die Melderate verdächtiger Mails. Die Mitarbei-ter werden so zum aktiven Bestandteil der IT-Sicherheitsstrategie.

7 Kontinuierlich und randomisiert simulieren

Eine Phishing-Simulation sollte immer auf kontinuierlicher Basis laufen, denn nur so können die Lernerfolge nachhaltig und langfristig gesichert werden.

Eine Phishing-Simulation sollte immer auf kontinuierlicher Basis laufen, denn nur so können die Lernerfolge nachhaltig und langfristig gesichert werden. Erkenntnisse aus der Habit-Forschung legen nahe, dass über einen größeren Zeitraum verteilte Lernmaßnahmen im Sinne einer Verhaltensänderung vorteilhafter sind als punktuelle Lernmaßnahmen. So wird die Cyber Security Awareness der Empfänger über wiederholte Stupser im Alltag durch die Phishing-Simulation laufend geschult. Das aus der Verhaltensökonomie bekannte, sogenannte „Nudging" regt dabei zur stetigen Auseinandersetzung mit dem Thema „Phishing" an.

Auch die Randomisierung der simulierten Phishing-Mails ist für den Erfolg der Simulation relevant. Wird allen Empfängern zeitgleich eine identische simulierte Phishing-Mail zugesendet, verbreitet sich diese Neuigkeit unter Umständen sehr schnell im Unternehmen. Durch einen randomisierten Versand der simulierten Mails kommt es nur selten zu einem Sättigungseffekt der verwendeten Phishing-Mails und Templates. Denn dann funktioniert der Flurfunk nur eingeschränkt. Nach nur wenigen Tagen oder Wochen ist die Information des Kollegen aus dem aktiven Gedächtnis verschwunden.

Nicht nur die Nutzer profitieren von diesem Ansatz. Auch für Sie ergeben sich durch die kontinuierliche und randomisierte Simulation Vorteile:

- Die KPIs sind nach einer Baselining-Phase jederzeit, also „live", aussagekräftig. Bei punktuell ausgeführten Kampagnen korreliert die Klickrate häufig stark mit dem Schwierigkeitsgrad der jeweiligen E-Mail. Durch die Randomisierung einer größeren Auswahl von E-Mails und deren zeitlich verteilte Versendung sind die jeweiligen E-Mail-Typen zu jedem Zeitpunkt gleichermaßen in den KPIs präsent. Dadurch können Kennzahlen laufend interpretiert und letztlich auch ein solider Effekt der Maßnahme demonstriert werden.
- Die Ticketlast wird minimiert. Statt zu bestimmten Zeitpunkten die fingierten Mails an alle Mitarbeiter herauszusenden und damit die Meldekette in Gang zu setzen, wird durch einen randomisierten Versand der Arbeitsaufwand für die IT über den gesamten Simulationszeitraum verteilt.

8 Den Nutzern sinnvolle Rückmeldungen geben

Wie die vorangehenden Punkte deutlich gemacht haben, ist die frühzeitige Kommunikation über den Ablauf und die Ziele der Phishing-Simulation ein Kernbestandteil der Methode. Ebenso wichtig ist es jedoch, Zwischenstände an die Nutzer zu kommunizieren.

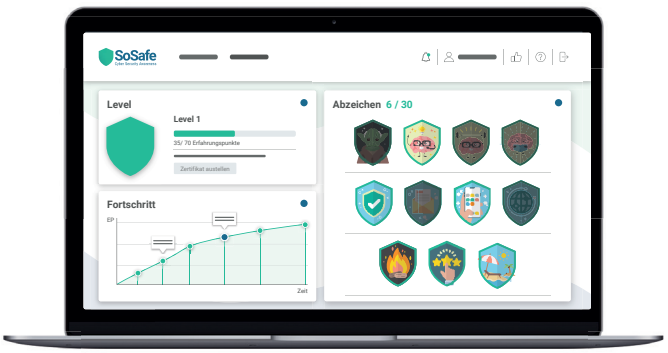
Das hilft den Mitarbeitern dabei, ihre eigene Leistung einzuschätzen und ruft Erlerntes wieder ins Gedächtnis. Auch wenn nicht auf spezifische Szenarien eingegangen werden kann, weil dadurch etwas vorweggenommen würde, sollte anschauliches Feedback gegeben werden, zum Beispiel:

- Sind die Interaktionsraten mit gefälschten Websites besonders hoch?
- Welche psychologischen Maschen funktionieren besonders gut?
- Lassen sich die Nutzer eher von Mails täuschen, die Neugier erwecken oder von solchen, die Druck erzeugen?

Legen Sie dabei Wert auf eine verständliche Formulierung der Ergebnisse. Technische und wissenschaftliche KPIs sagen den meisten Mitarbeitern recht wenig – Klickraten und Interaktionsraten sind dagegen greifbar. Auch hier können Sie wieder den Lernaspekt betonen. Geben Sie positives statt negatives Feedback: Erklären Sie den Empfängern der Phishing-Mails etwa, dass die Melderaten im Verlauf der Simulation entscheidend sind, nicht die Interaktionsraten. Denn die Nutzer sollen darin geschult werden, die Mails zu identifizieren – das Hauptaugenmerk liegt darauf, die Mitarbeiter zu einer aktiven Verteidigungslinie im Unternehmen zu machen.

Auch Gamification kann dabei eine entscheidende Rolle spielen. Wie lernpsychologische Untersuchungen zeigen, motivieren spieltypische Elemente, wie beispielsweise das Sammeln von Punkten für korrekt identifizierte und gemeldete (simulierte) Phishing-Mails, die Mitarbeiter zusätzlich.

Die Rückmeldung an die Mitarbeiter unterstützt diese zusammenfassend also dabei, die Phishing-Simulation noch spezifischer als Lern-Tool zu nutzen und ihre Awareness zu schulen.



Gamification auf der SoSafe-Awareness-Plattform: Abzeichen und Punkte sorgen für zusätzliche Motivation.

Realitätsnah lernen: Der Mehrwert von Phishing-Simulationen

Systematisch geplante und durchgeführte Phishing-Simulationen steigern nachhaltig das Bewusstsein für IT-Sicherheit und können so die Widerstandsfähigkeit von Unternehmen gegen Cyberangriffe stärken. Die Simulationen sind allerdings nur wirksam, wenn sie den Faktor Mensch und sein Bedürfnis zu lernen in den Mittelpunkt stellen und können so einen entscheidenden Beitrag zur IT-Sicherheit leisten.

Wie die vorgestellten Best Practices gezeigt haben, müssen dazu auf verschiedenen Ebenen Vorkehrungen getroffen werden. Eine durchdachte Herangehensweise an Ihre Phishing-Simulation ermöglicht Ihnen aber, eine stabile Sicherheitskultur in Ihrem Unternehmen zu etablieren und sich für die zunehmenden Cyberrisiken zu rüsten.

Bei Full- bzw. Managed-Service-Anbietern bekommen Sie alles aus einer Hand – von der Planung und Anpassung der Phishing-Mails über die Durchführung der Simulation bis hin zur Aufbereitung der Auswertung. Mit Erfahrungswerten aus der Zusammenarbeit mit anderen Unternehmen sind die Anbieter gut vorbereitet auf etwaige Rückfragen technischer und inhaltlicher Art und können Sie so optimal unterstützen.

Checkliste
Erfolgreiche Phishing-Simulation

Habe ich...

- [ ] die **technischen Vorkehrungen** für die Phishing-Simulation getroffen, z.B. ein Whitelisting für die Mailserver des Dienstleisters vorgenommen und die in den Phishingmails verwendeten Domains in die Whitelist aufgenommen,
- [ ] meinen Kollegen (und ggf. dem Betriebsrat) die Phishing-Simulation **vorgestellt** und den Start **angekündigt**,
- [ ] bei der Kommunikation die **Anonymität** und den **Lernaspekt** der Simulation hervorgehoben,
- [ ] die Simulation an die Empfänger **angepasst** oder anpassen lassen,
- [ ] dafür gesorgt, dass die Phishing-Simulation von entsprechenden **Lerninhalten** begleitet wird,
- [ ] eine **Meldekette** etabliert und die Mitarbeiter über das Vorgehen bei einem (simulierten) Phishingfall informiert,
- [ ] bei der Planung einen **kontinuierlichen und randomisierten** Versand bedacht,
- [ ] vor, während und nach der Simulation mit den Mitarbeitern **über den Zweck und die Ergebnisse der Simulation gesprochen**?

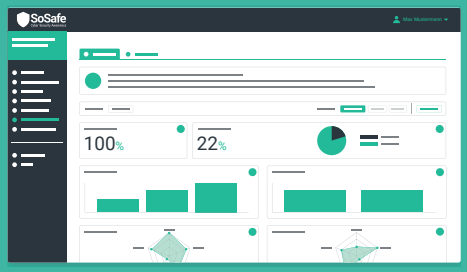
Über SoSafe

Die SoSafe GmbH mit Sitz in Köln ist ein auf IT-Sicherheit und Awareness-Building spezialisierter Anbieter digitaler Schulungslösungen. Das rund 60-köpfige Team reicht vom IT-Sicherheits-Experten bis zum Lernpsychologen.

Die Awareness-Plattform von SoSafe sensibilisiert, schult und testet Mitarbeiter im Umgang mit dem Thema IT-Sicherheit. Phishing-Simulationen und interaktive E-Learnings bringen den Mitarbeitern auf effektive und nachhaltige Art und Weise bei, worauf bei der Nutzung z.B. von E-Mails, Passwörtern oder sozialen Medien besonders zu achten ist. Der Arbeitgeber erhält ein differenziertes Reporting und kann Awareness-Building endlich messbar machen; gleichzeitig bleibt alles 100% datenschutzkonform, wodurch die Lösung auch von der Personalvertretung und v.a. den Mitarbeitern selbst durchweg positiv aufgenommen wird.

E-Learning-Plattform
- 20 interaktive Module zu IT-Security und Datenschutz
- Awareness-Videos
- Inhalt und Branding anpassbar

Phishing-Simulation
- Realistische Attacken über das Jahr verteilt
- Randomisierte Sensibilisierung
- Lernseiten mit Tipps zur Erkennung von Phishing-Mails



Unterstützende Tools
- Dashboard mit technischen und psychologischen KPIs
- Phishing-Melde-Button
- Mitarbeiter-Zertifikate

Autoren

Dr. Niklas Hellemann, Diplom-Psychologe & Managing Director
Katharina Ketels, Senior Awareness Specialist
Ann-Kathrin Krane, Marketing Manager

Kontakt

Mail: info@sosafe.de
Telefon: +49 221 6508 3800

Weitere Informationen

www.sosafe.de
www.sosafe.de/produkt
www.sosafe.de/demo

SoSafe
Cyber Security Awareness