sosafe

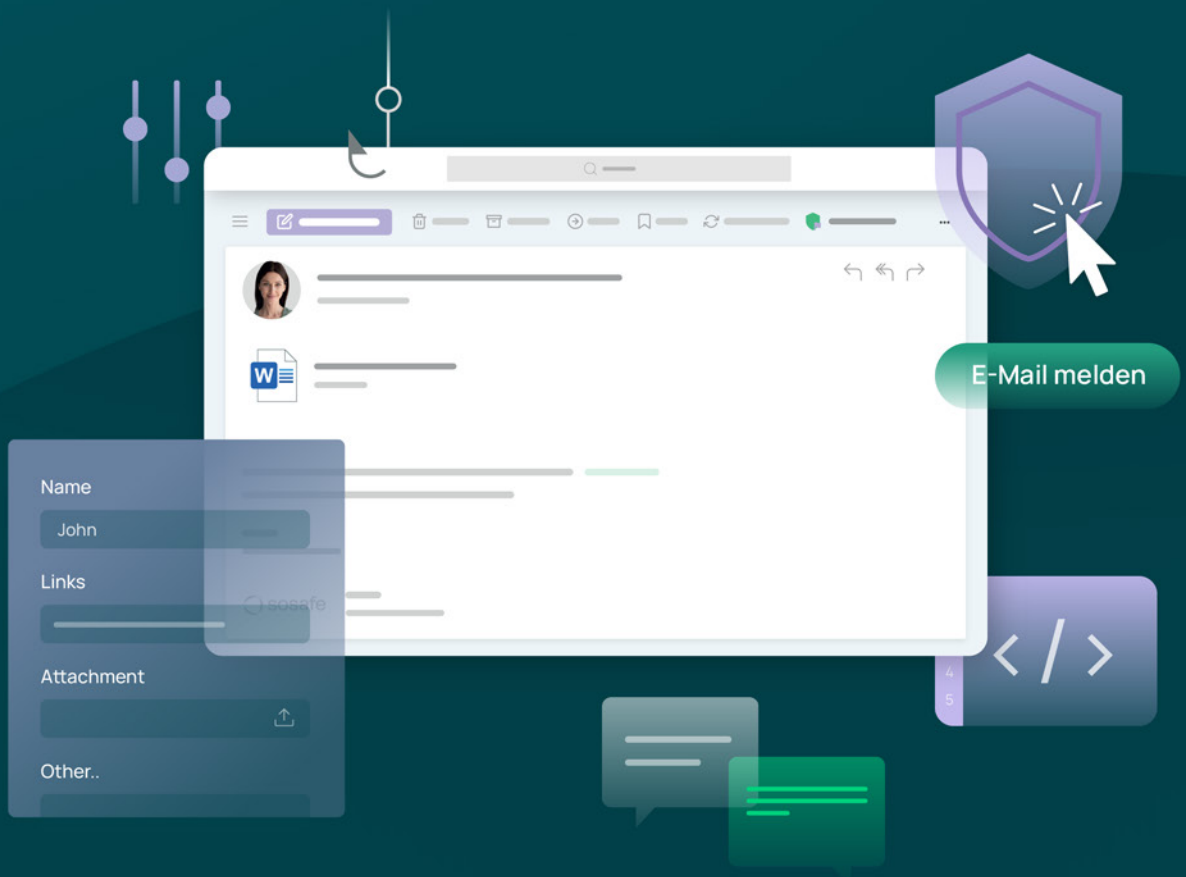
www.sosafe-awareness.com/de

GUIDE

Best Practices Phishing-Simulationen

10 Dos and Don’ts für nachhaltige Security Awareness in Ihrer Organisation

Inklusive praktischer Checkliste!



Inhaltsangabe

Cyberangriffe: Die stetig wachsende Gefahr aus dem Netz

Die Anzahl, das Ausmaß und die Komplexität von Cyberangriffen auf sowohl Privatpersonen als auch Organisationen ist in den letzten Jahren kontinuierlich gestiegen.

Im Risk Barometer der Allianz-Versicherung rangiert Cybercrime seit Jahren auf den ersten Plätzen der größten Geschäftsrisiken weltweit. Die Schätzungen des Schadens belaufen sich dabei auf jährlich mehrere Billionen US-Dollar. Denn erfolgreiche Cyberangriffe gehen für Organisationen nicht nur mit Imageverlusten einher. Vielmehr kommt es oft zu kostspieligen Betriebsausfällen oder hohen Lösegeldforderungen bei Angriffen mit Erpressungssoftware, sogenannter Ransomware.

9 von 10 Cyberangriffen starten dabei beim Faktor Mensch, und Phishing steht nach wie vor besonders weit oben auf der Liste der beliebtesten Angriffstaktiken. Insbesondere komplexe Social-Engineering-Methoden wie Spear Phishing und Dynamite Phishing treten immer häufiger auf (siehe Infobox S. 7). Dabei nutzen die Cyberkriminellen psychologische Taktiken und manipulieren die Emotionen der Empfängerinnen und Empfänger, um ihr Ziel durchzusetzen.

Über infizierte Systeme sammelte so zum Beispiel der Trojaner und „König der Schadsoftware“ Emotet, trotz kurzzeitiger Zerschlagung im Jahr 2021, vorhandene Mailverläufe, um auf Basis dieser automatisiert weitere Phishing-Mails zu erzeugen und zu verteilen. Die meisten klassischen Spamfilter können die vorgetäuschten, schädlichen Mail-Konversationen allerdings nicht zielsicher identifizieren. Die Phishing-Mails landen in den Postfächern der Mitarbeitenden – und das Übel nimmt seinen Lauf.

INFOBOX

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 erbeuteten Kriminelle mit der „Advance Fee“-Masche des sogenannten „Spanischen Gefangenen“ hohe Summen. 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 Engineerings 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 1990er Jahren 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 Cyberkriminelle ihre Opfer immer gezielter angreifen und hinters Licht führen.

Der Mensch als entscheidender Faktor im Kampf gegen Phishing

Organisationen sollten deshalb nun besonders wachsam sein und ihre Mitarbeitenden für die lauernden Gefahren aus dem Netz sensibilisieren. Geschulte und aufmerksame Mitarbeitende können frühzeitig auf Cyberrisiken reagieren und so fatale Vorfälle im Unternehmen verhindern.

Auch verschiedene, internationale Compliance-Frameworks, wie die ISO/IEC 27001 oder die europäische Datenschutz-Grundverordnung (EU-DSGVO), fordern eine kontinuierliche Schulung der Mitarbeitenden zu Informationssicherheit – im Falle der ISO/IEC 27001 auch eine Form von simulierten Social-Engineering-Angriffen. Ebenso geben immer mehr branchenspezifische Regularien, wie etwa die Bankaufsichtliche Anforderungen an die IT (BAIT) für das Finanzwesen, ähnliche Empfehlungen.

Um die höchsten Lernerfolge zu erzielen, sollten Organisationen dabei nicht nur Schulungen, etwa in Form von E-Learnings und interaktiven Lernplattformen, in Erwägung ziehen. In Kombination mit verhaltensschulenden Maßnahmen wie Phishing-Simulationen erhöhen Organisationen die Security Awareness und senken so menschliche Risiken in der Informationssicherheit effektiv und nachhaltig

INFOBOX

Social Engineering – Die beliebtesten Taktiken der Cyberkriminellen

Phishing: Phishing ist eine Betrugsmasche, bei der persönliche Daten des Opfers über eine E-Mail „abgefischt" und für kriminelle Zwecke missbraucht werden. Die Opfer erhalten eine Nachricht, in der ihr Vertrauen missbraucht wird. Anschließend geben sie unwissentlich Zugangsdaten in fremde Hände. Die Masche verfolgt immer boshafte Absichten: Den Opfern sollen persönliche oder finanzielle Schäden zugefügt werden. Gleichzeitig steht die persönliche Bereicherung der Cyberkriminellen im Fokus der Attacken.

Vishing: Vishing (kurz für Voice Phishing) ist eine Form des Phishings über das Telefon, bei der das Opfer dazu verleitet wird, persönliche Daten herauszugeben. Gerade in Zeiten hybrider Arbeitsmodelle hat diese Masche an Relevanz gewonnen, denn im Zweifelsfall können die Opfer schwieriger mit Kolleginnen und Kollegen Rücksprache halten, um den Anruf zu verifizieren.

Smishing: Smishing (kurz für SMS-Phishing) ist eine Phishing-Angriffstaktik per SMS oder Textnachricht. In der SMS werden die Opfer meist dazu aufgerufen, einem Link zu folgen. Durch diesen Klick werden Schad- oder Spionagesoftware verbreitet und persönliche Daten abgegriffen.

Spear Phishing: Im Vergleich zum „normalen" Phishing zielen Spear-Phishing-Attacken auf eine eng begrenzte Nutzergruppe, über die die Täter im Vorhinein genaueste Informationen eingeholt haben. Das macht sie besonders gefährlich, denn die persönlichen Informationen lassen die Angriffe extrem legitim erscheinen. Eine der bekanntesten Formen des Spear-Phishings ist der CEO-Fraud, bei denen sich die Cyberkriminellen als Führungskräfte ausgeben und so Geschäftsprozesse beeinflussen.

Dynamite Phishing: Dynamite Phishing ist eine besonders gefährliche Art von Spear-Phishing. Der Begriff wurde durch das Schadprogramm Emotet geprägt, welches auf dem Gerät des Opfers zunächst unentdeckt Informationen über dessen E-Mail-Verkehr sammelt. Bei dieser oft Monate andauernden Spionage wird auch der Inhalt der E-Mails abgegriffen. Hierdurch können nach einer gewissen Zeit weitere Phishing-Mails erstellt werden, die sehr gut an die normale Kommunikation des Opfers angepasst und dadurch für die Empfängerinnen und Empfänger kaum noch als schadhaft zu erkennen sind. Anders als beim normalen Spear Phishing werden die E-Mails beim Dynamite Phishing automatisiert erstellt und in großer Anzahl verschickt.

10 Dos and Don'ts für Ihre Phishing-Simulation

Phishing-Simulationen stellen Cyberangriffe realitätsnah nach, um Mitarbeitende für die Gefahren solcher Attacken zu sensibilisieren. Bei einer Phishing-Simulation werden Phishing-Mails verschickt, die vermeintlich sensible Daten abfangen sollen. 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. Die Simulation öffnet den Mitarbeitenden die Augen für die Gefahren von Phishing und hilft ihnen, sicheres Verhalten anzutrainieren.

Bei der Umsetzung solcher Phishing-Simulationen gibt es jedoch einige Fallstricke. Sie wurden in der Vergangenheit oftmals als reines Test-Tool genutzt, um personenscharf zu ermitteln, welche Mitarbeitenden ein „Sicherheitsrisiko" darstellen. Ein solches Vorgehen führt verständlicherweise zu Frustration bei den teilnehmenden Personen. Statt die Mitarbeitenden als Risiko für die Informationssicherheit einer Organisation einzuordnen, sollte eine Phishing-Simulation deshalb immer von der gegenteiligen Annahme getrieben sein: Der Mensch stellt mit einem Bewusstsein für Cyberrisiken und durch einen umsichtigen Umgang mit den Gefahren eine zusätzliche, sicherheitsrelevante Barriere dar. Und kann eine Organisation so vor kostspieligen Angriffen schützen.

Mit den folgenden Tipps und Best Practices gestalten Sie Ihre Phishing-Simulation effektiv, fördern das sichere Verhalten Ihrer Mitarbeitenden und etablieren eine schützende Sicherheitskultur in Ihrem Unternehmen:

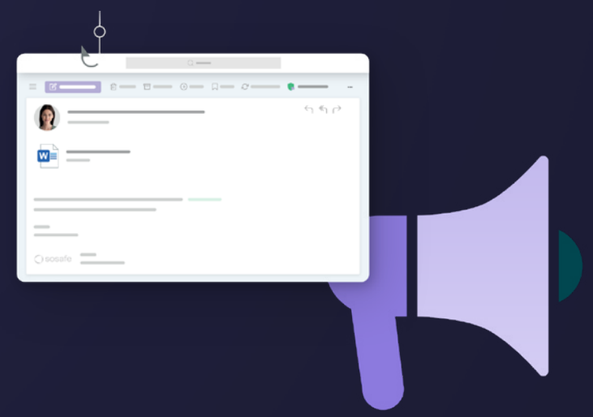
1.

Technisch überprüfen statt im Live-Betrieb anpassen

Konventionelle technische Filter können unter Umständen nicht erkennen, dass es sich bei einer simulierten Phishing-Mail um eine harmlose Schulungsmaßnahme handelt. Um sicherzustellen, dass die Nachrichten im Postfach der Mitarbeitenden 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. Tragen Sie in Absprache mit Ihrem Simulationsanbieter alle relevanten Informationen zusammen und passen Sie die entsprechenden Systeme an. Der Dienstleister selbst sollte dabei größten Wert auf Datensicherheit legen und Sie individuell dazu beraten, wie Sie beim Whitelisting allen Sicherheitsstandards nachkommen.

Statt einfach mit der Simulation zu starten, sollte diese kontinuierlich getestet werden. Durch Testversände ausgewählter Phishing-Mails, welche die Bandbreite der Simulation widerspiegeln, stellen Sie sicher, dass später im Live-Betrieb alles korrekt funktioniert. Hier lohnt es sich auch, die IT oder das Helpdesk mit ins Boot zu holen. Die Kolleginnen und Kollegen können nicht nur die entsprechenden Vorkehrungen treffen, sondern sind auch auf etwaige Rückfragen der Mitarbeitenden während der Simulation vorbereitet. Das trägt maßgeblich zu einem störungsfreien und effektiven Ablauf bei.

2.



Ankündigen statt überraschen

Das A und O einer jeden lernorientierten Phishing-Simulation ist die Kommunikation – vor, während und nach der Maßnahme. Nicht nur IT und Helpdesk, auch die Geschäftsführung sowie ggf. der Betriebsrat und die Personalabteilung sollten mit in die Planung und Durchführung einbezogen werden.

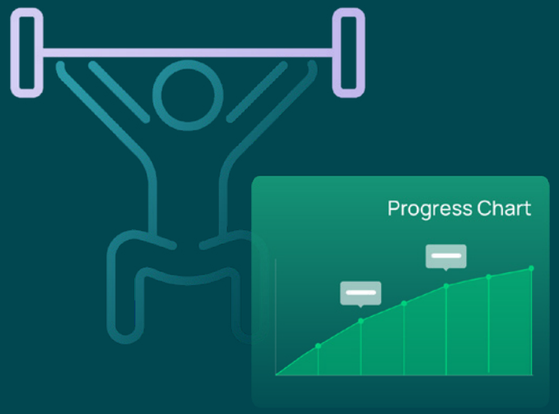
Entscheidend bleibt aber letztlich vor allem, die Empfängerinnen und Empfänger frühzeitig zu informieren. Das ist in gleich mehrfacher Hinsicht sinnvoll: Zum einen vermeiden Sie so Verunsicherung. Stellen Sie die Simulation als Lernmaßnahme vor, die den Mitarbeitenden Wissen vermittelt, das sie auch im privaten Kontext nutzen können. Zum anderen erhöht eine frühzeitige Ankündigung der Phishing-Simulation die Motivation der Nutzenden. Ist ihnen bewusst, dass die Simulation zu einer stärkeren Sicherheitskultur führt und die Organisation vor Angriffen schützt, setzen sie sich aktiver mit den Lerninhalten auseinander.

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 Mitarbeitenden handelt. Oder gestalten Sie die Awareness-Maßnahme als „freundlichen Wettbewerb" unter den Kolleginnen und Kollegen.

Inhalte der Ankündigung können sein:

Hintergrund:	Wieso führen Sie die Simulation durch und welche Effekte erhoffen Sie sich?
Umfang:	Was können die Mitarbeitenden erwarten? Geben Sie den Teilnehmenden einen Eindruck vom Umfang der Maßnahme, ohne eine konkrete Anzahl an Mails anzukündigen.
Startzeitpunkt:	Wann wird die Simulation beginnen? Geben Sie auch hier einen Zeitraum statt eines konkreten Datums an.
Ablauf:	Wie wird die Simulation ablaufen und was ist von den Mitarbeitenden gefragt?
Kommunikation:	Wen können die Mitarbeitenden bei Rückfragen zur Simulation ansprechen?
Ziel:	Wieso sollten die Mitarbeitenden die Simulation nicht als Test, sondern als Lernmöglichkeit wahrnehmen?

3.



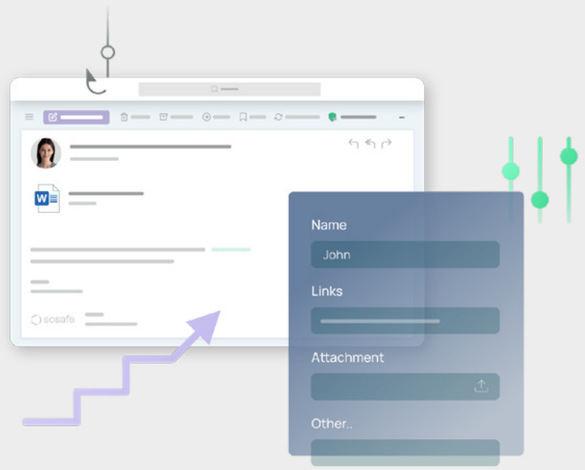
Trainieren statt testen

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, Mitarbeitende manchmal sogar mit ihrem Verhalten konfrontiert oder gar personelle Konsequenzen gezogen. Schuldzuweisungen wirken sich allerdings negativ auf die Lernbereitschaft und Motivation der Mitarbeitenden aus.

Effektiver und nachhaltiger ist es, Simulationen anonym durchzuführen, das heißt ohne die Erfassung und Verarbeitung individueller Verhaltensdaten. Bereits in der Ankündigung einer Simulation sollte den Nutzenden deutlich werden, dass es sich bei der Maßnahme nicht um einen Test handelt. Die Nutzerinnen und Nutzer sollten sich nicht überwacht fühlen, sondern die Möglichkeit haben, in ihrem eigenen Lerntempo und nach bestem Gewissen die Phishing-Simulation zu durchlaufen. Indem Sie den Mitarbeitenden ihre Rolle als „menschliche Firewall“ bewusst machen, steigern Sie die Effektivität der Schulungsmaßnahme.

In spezifischen Fällen entscheiden sich Organisationen trotz allem für personenscharfe Simulationen, zum Beispiel, weil sie sicherstellen möchten oder müssen, dass Personengruppen, die mit besonders sensiblen Daten arbeiten, ausreichend geschult sind. Die erhobenen Verhaltensdaten machen den Wissensstand einzelner Personen leicht nachvollziehbar. In dem Fall sollten Sie allerdings dafür sorgen, dass diese Art von Kontrolle ausschließlich dem Lernerfolg der Mitarbeitenden dient und nicht dem Abstrafen unsicheren Verhaltens. Nutzen Sie die erhobenen Daten etwa dazu, einzelne Mitarbeitende beim Lernen positiv zu bestärken und ihnen mehr oder weniger Lerninhalte zur Verfügung zu stellen, sodass sie potenzielle Cyberangriffe effektiv abzuwehren lernen. Begleiten Sie die Maßnahme intensiv durch transparente Kommunikation und stellen so sicher, dass die Teilnehmenden sich nicht kontrolliert fühlen.

4.



Individualisieren statt verallgemeinern

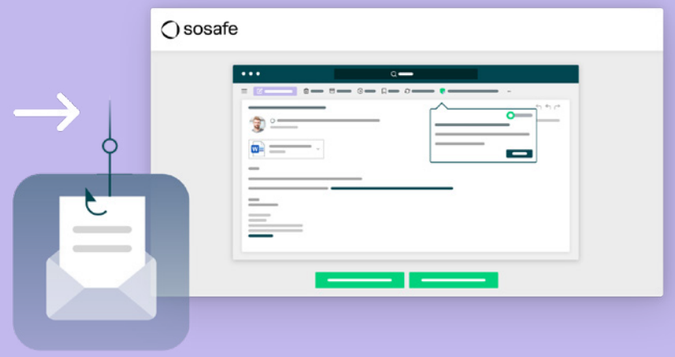
Damit die Mitarbeitenden sich nicht bloßgestellt fühlen, sollten Sie die Phishing-Simulation an die jeweiligen Kenntnisse und Anforderungen der Nutzenden anpassen. Sind sämtliche simulierten Phishing-Mails zu leicht als solche zu erkennen, sinkt zwangsläufig die Motivation der Nutzenden. Sie fühlen sich gerüstet für echte Angriffe, obwohl diese oftmals auf ausgeklügelten, psychologischen Taktiken basieren. Aber auch ausschließlich schwierig zu erkennende Simulationsmails wirken sich negativ auf die Motivation der Nutzenden aus. Im schlimmsten Fall fühlen sie sich hintergangen und in die Falle gelockt – das gilt es in jedem Fall zu vermeiden.

Ausgewogenheit ist hier der Schlüsselpunkt: Mischen Sie in der Simulation leichtere mit herausfordernden Mails, um den Nutzenden regelmäßig Erfolgserlebnisse zu ermöglichen. Damit wird außerdem das reale Phishing-Spektrum widergespiegelt. So vermeiden Sie Frustrationen seitens der Nutzenden, die von Ihnen erhobenen Statistiken zur Simulation bilden die aktuelle Gefahrenlage realitätsgetreu ab und der Lernaspekt steht weiterhin im Fokus der Maßnahme.

Schneiden Sie die Phishing-Simulation außerdem inhaltlich – ähnlich zum Spear Phishing – auf die empfangenden Personen zu, zum Beispiel:

- **Persönliche Anrede**
- **Unternehmensspezifische E-Mail-Signaturen**
- **Zielgruppenrelevante Themen**
- **Inhaltliches Aufgreifen bekannter Abläufe**
- **Nutzung besonders erfolgreicher psychologischer Maschen**
- **Realitätsnahes Design**
- **Funktion und Abteilungszugehörigkeit**
- **Sprachliche Aspekte**

5.



Lernmoment statt Schockmoment

Begleiten Sie die Phishing-Simulation mit passenden Lerninhalten, zum Beispiel in Form von E-Learnings. Hier sollten die Nutzenden Informationen dazu erhalten, wie sie sich im Arbeitsalltag sicher verhalten. 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 Empfängerinnen und 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.

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 Mitarbeitenden abzuschrecken, regen die Lerninhalte so dazu an, beim nächsten Mal vorsichtiger zu sein und schulen damit die Aufmerksamkeit.

6.

Meldekette statt Meldechaos

Wie reagiert man am besten, wenn man eine Phishing-Mail erhält? Im Falle eines Cyberangriffs zählt jede Minute. Deshalb sollten Ihre Mitarbeitenden diese Frage jederzeit beantworten können. Etablieren Sie noch vor dem Start Ihrer Simulation eine Meldekette, damit die Empfängerinnen und 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 auch laut ISO/IEC 27001 sollte es bei einem Notfall einen klar definierten und strukturierten Ablauf geben.

Es bietet sich etwa an, den Nutzenden 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 Mitarbeitenden beim bewussten Umgang mit IT-Sicherheitsrisiken den Rücken. Eine optimierte Form einer solchen Meldekette sind in das Mailprogramm integrierte Meldebuttons, wie sie auf der SoSafe-Plattform zum Einsatz kommen.

Eine solche Ergänzung bringt zahlreiche Vorteile mit sich:

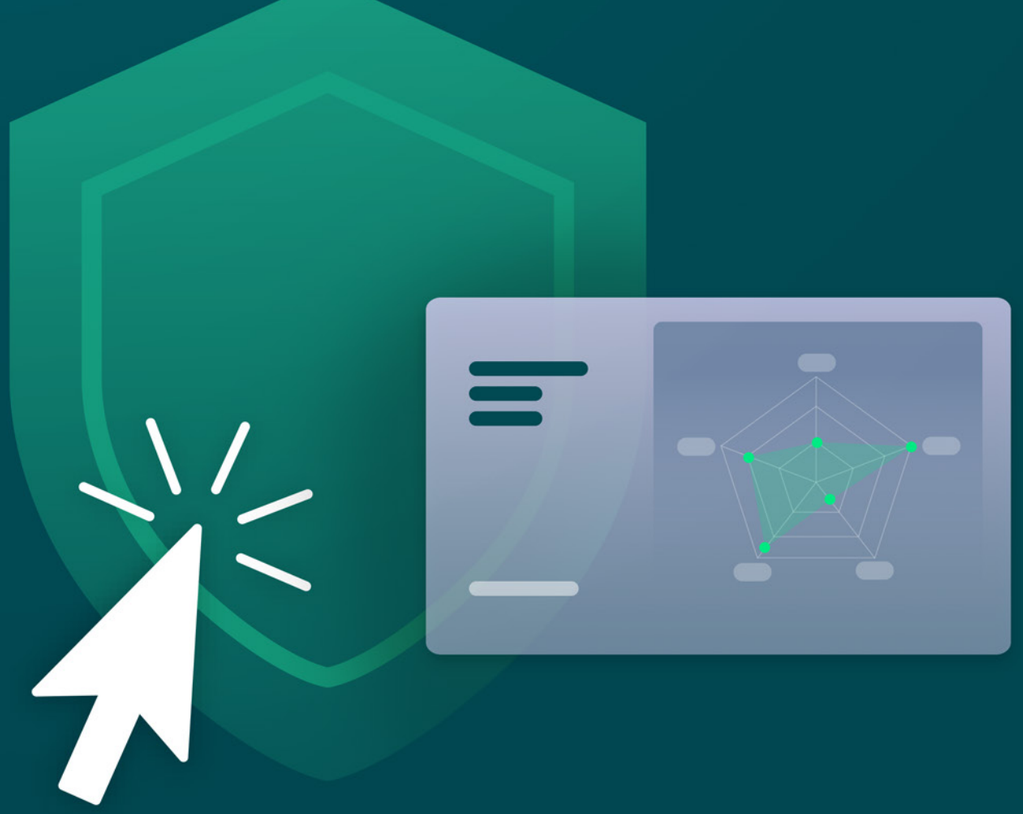
- **Die Melderate verbessert sich.**
- **Das Ticketaufkommen kann besser kontrolliert werden, da simulierte Mails nicht an das Helpdesk weitergeleitet werden.**
- **Die Mitarbeitenden werden während des Lernprozesses durch den Button positiv bestärkt.**

INFOBOX

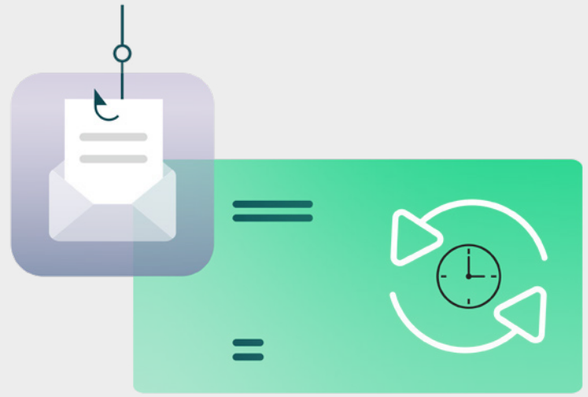
Nachhaltig erhöhte Melderaten dank intelligentem Reporting

Dass Mitarbeitende Phishing-Mails treffsicher erkennen, ist der erste Schritt hin zu einer sicheren Organisation. Noch wichtiger ist im Fall der Fälle allerdings eine schnelle Reaktion, sodass die IT entsprechende Maßnahmen einleiten und potenzielle Angriffe auf andere Mitarbeitende verhindern kann. Ein aussagekräftiger Messwert sind hier beispielsweise die Melderaten in Phishing-Simulationen.

Ergebnisse aus der SoSafe Awareness-Plattform zeigen, dass mithilfe des Phishing Report Buttons die Melderaten nachhaltig gesteigert werden. Die Integration direkt in das Mail-Programm der Organisation ermöglicht Mitarbeitenden vermeintlich gefährliche Mails unumständlich an die IT zu melden. So meldet jede und jeder Mitarbeitende im Schnitt jede zweite Phishing-Mail direkt über den Button.



7.



Kontinuierlich statt punktuell

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 zeigen, dass über einen größeren Zeitraum verteilte Lernmaßnahmen sicheres Verhalten nachhaltiger fördern als punktuelle. So wird die Cyber Security Awareness der Nutzenden über wiederholte Stupser im Alltag durch die Phishing-Simulation laufend geschult. Dieses sogenannte „Nudging" regt dabei zur stetigen Auseinandersetzung mit dem Thema Phishing an.

INFOBOX

Verteiltes Lernen als Schlüssel zum Lernerfolg

Schon seit Mitte des letzten Jahrhunderts ist bekannt, dass kontinuierliches Lernen die Vergessenskurve abflacht. Auch Daten aus der SoSafe Awareness-Plattform zeigen, dass schon nach kurzer Zeit die Klickraten auf Phishing-Mails wieder um fast ein Drittel steigen, wenn die Mitarbeitenden nicht regelmäßig mit Lerninhalten interagieren.

Um Cyber-Security-Wissen zu vermitteln, sollten Organisationen daher auf lernpsychologisch fundierte Ansätze zurückgreifen. Hochmodularisierte Trainings und stetige Anstupser zum Lernen, sogenannte „Nudges", lassen die Vergessenskurve abflachen – und minimieren dadurch menschliche Risiken langfristig. Ergebnisse aus der SoSafe Awareness-Plattform zeigen, dass durch Nudging die Engagement-Rate kontinuierlich um 30 Prozent, in der Einführungsphase sogar um bis zu 90 Prozent, erhöht wird. So prägen sich Mitarbeitende Wissen effektiv und nachhaltig ein

8.

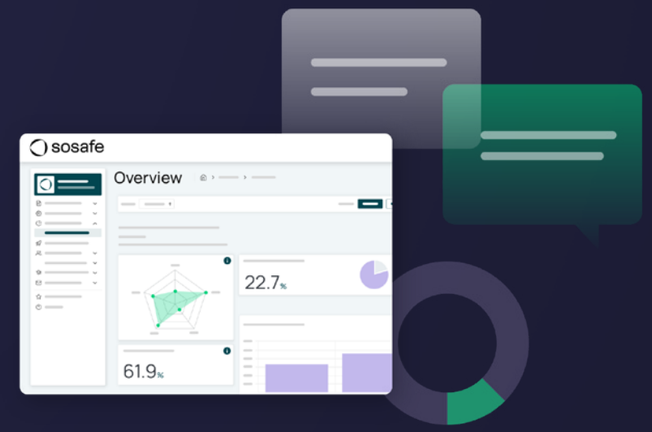
Randomisiert statt synchron

Auch die Randomisierung der simulierten Phishing-Mails ist für den Erfolg der Simulation relevant. Wird allen Empfängerinnen und 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. Nicht nur die Nutzenden 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 korrelieren Klick- oder Reporting-Raten 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 Mitarbeitenden herauszusenden und damit die Meldekette in Gang zu setzen, wird durch einen randomisierten Versand der Arbeitsaufwand für die IT über den gesamten Simulationszeitraum verteilt.

9.



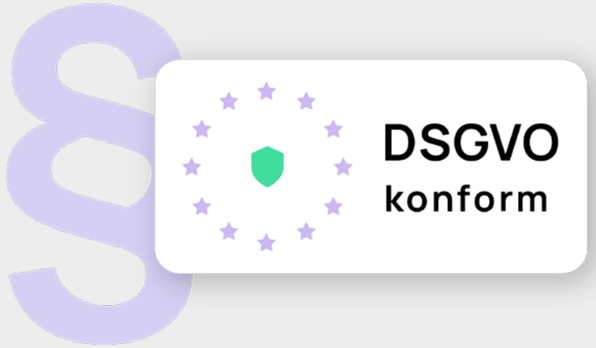
Rückmelden statt alleinlassen

Wie die vorangegangenen 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 Nutzenden zu kommunizieren. Das hilft den Mitarbeitenden 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 Sie anschauliches Feedback geben, zum Beispiel:

- → **Auf welche psychologischen Tricks sind die Mitarbeitenden am ehesten hereingefallen?**
- → **Welche KPIs sind besonders hoch oder niedrig – und was bedeutet das für die Mitarbeitenden und den Umgang mit Gefahren?**
- → **Wie erfolgreich haben Sie in Ihrer Organisation durch die Phishing-Simulation bereits Risiken reduzieren können?**

Legen Sie dabei Wert auf eine verständliche Formulierung der Ergebnisse. Technische und wissenschaftliche KPIs sagen den meisten Mitarbeitenden recht wenig – Klickraten und Interaktionsraten sind dagegen greifbar. Auch hier können Sie wieder den Lernaspekt betonen. Geben Sie positives statt negativem Feedback und fokussieren Sie sich auf Werte, die den Lernerfolg der Mitarbeitenden widerspiegeln. Viele Anbieter stellen entsprechende Kommunikationsvorschläge bereit, die Sie dabei unterstützen, die Erfolge an Ihre Mitarbeitenden zu vermitteln.

10.



DSGVO-konform statt rechtlich bedenklich

Interview: Datenschutz bei Phishing-Simulationen: DSGVO, Privacy Shield und Co. Interview mit Benedikt Woltering, Rechtsanwalt und Legal Advisor bei SoSafe

Sind Phishing-Simulationen datenschutzrechtlich unbedenklich?

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 persönlichen Daten der Mitarbeitenden 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 Daten der Mitarbeitenden 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 beispielsweise noch ausschließlich dem Zweck der Beschäftigung und einer erhöhten IT-Sicherheit? Hier gilt es, ein vernünftiges Maß zu finden und für die Mitarbeitenden invasive Vorgehensweisen wie Social Media Crawling zu vermeiden. Gleichzeitig sollten die Nutzenden keine direkten Konsequenzen zu fürchten haben. Deshalb die klare Empfehlung: Phishing-Simulationen anonym auswerten und keine personenscharfen Kontrollen durchführen. Außerdem sollten Unternehmen auf Anbieter setzen, die Daten ausschließlich in der EU verarbeiten.

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

Es besteht nach wie vor das Missverständnis, dass es ausreiche, Daten auf einer dedizierten EU-Cloud zu verarbeiten. Aber sitzen rechtliche Entitäten beispielsweise in den USA, können die dortigen Behörden jederzeit die Herausgabe von Daten erzwingen. Damit ergibt sich automatisch ein Compliance-Problem, insbesondere bei sensiblen Verhaltensdaten, die beispielsweise bei Phishing-Simulationen erhoben werden. Die Lösung ist dabei so einfach wie auch konsequent – entscheiden Sie sich für einen Dienstleister mit sämtlichen Gesellschaften innerhalb der EU, dessen Server sich ebenfalls in der EU befinden.

Zusammenfassung

Menschliche Risiken mit Phishing-Simulationen nachhaltig minimieren

Systematisch geplante und durchgeführte Phishing-Simulationen steigern nachhaltig das Bewusstsein für Informationssicherheit und stärken so die Resilienz von Organisationen gegenüber Cyberangriffen. Der Faktor Mensch und sein Bedürfnis zu lernen sollten dabei immer im Mittelpunkt stehen. Wie die vorgestellten Best Practices zeigen, sollten Organisationen dafür auf verschiedenen Ebenen Vorkehrungen treffen.

Haken Sie diese Best Practices ab und etablieren eine starke Sicherheitskultur in Ihrer Organisation, um sich effektiv und nachhaltig vor den zunehmenden Cyberrisiken zu schützen.

Checkliste

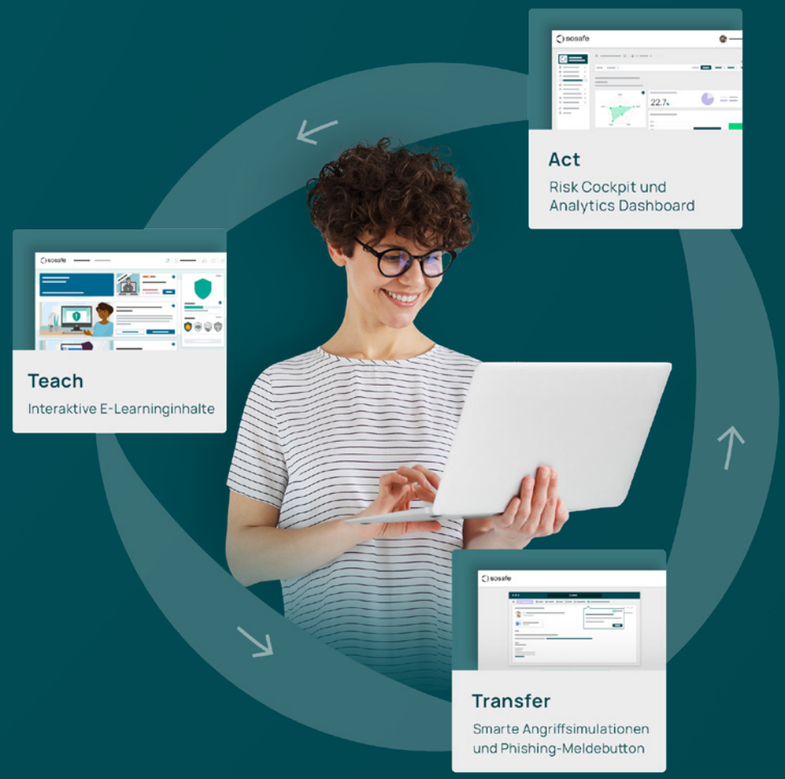
Lernorientierte Phishing-Simulationen

- [ ] Ich habe die technischen Weichen für die Phishing-Simulation gestellt, Whitelists aktualisiert, und ausreichend getestet, dass die Simulationsmails ankommen und richtig dargestellt werden.
- [ ] Alle Mitarbeitenden wissen darüber Bescheid, dass sie eine Phishing-Simulation durchlaufen werden und diese der Schulung ihrer Awareness dient.
- [ ] Ich habe sichergestellt, dass die Phishing-Simulation die Mitarbeitenden nicht bloßstellt, sondern sie zum Lernen motiviert.
- [ ] Die Simulationsmails werden individuell an die Empfängerinnen und Empfänger sowie deren Kontext (zum Beispiel ihre Abteilung) angepasst.
- [ ] Neben der Phishing-Simulation erhalten die Mitarbeitenden Lerninhalte, die ihr Wissen vertiefen und sicheres Verhalten schulen.
- [ ] Die Mitarbeitenden wissen, wie und an wen sie potenziell gefährliche Mails melden, sodass die IT im Zweifel schnell reagieren kann.
- [ ] Ich habe die Simulation auf lange Sicht geplant, damit auch die Lernerfolge und die Minimierung der Risiken fortlaufend sichergestellt werden.
- [ ] Die Phishing-Mails werden randomisiert versendet, damit sich keine Sättigungseffekte einstellen.
- [ ] Ich kommuniziere regelmäßig mit den Mitarbeitenden und teile Ergebnisse, um sie durch Feedback weiter zu motivieren.

Sie haben alle 10 Boxen abgehakt?
Dann steht der Stärkung Ihrer Sicherheitskultur über eine Phishing-Simulation nichts mehr im Wege.

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