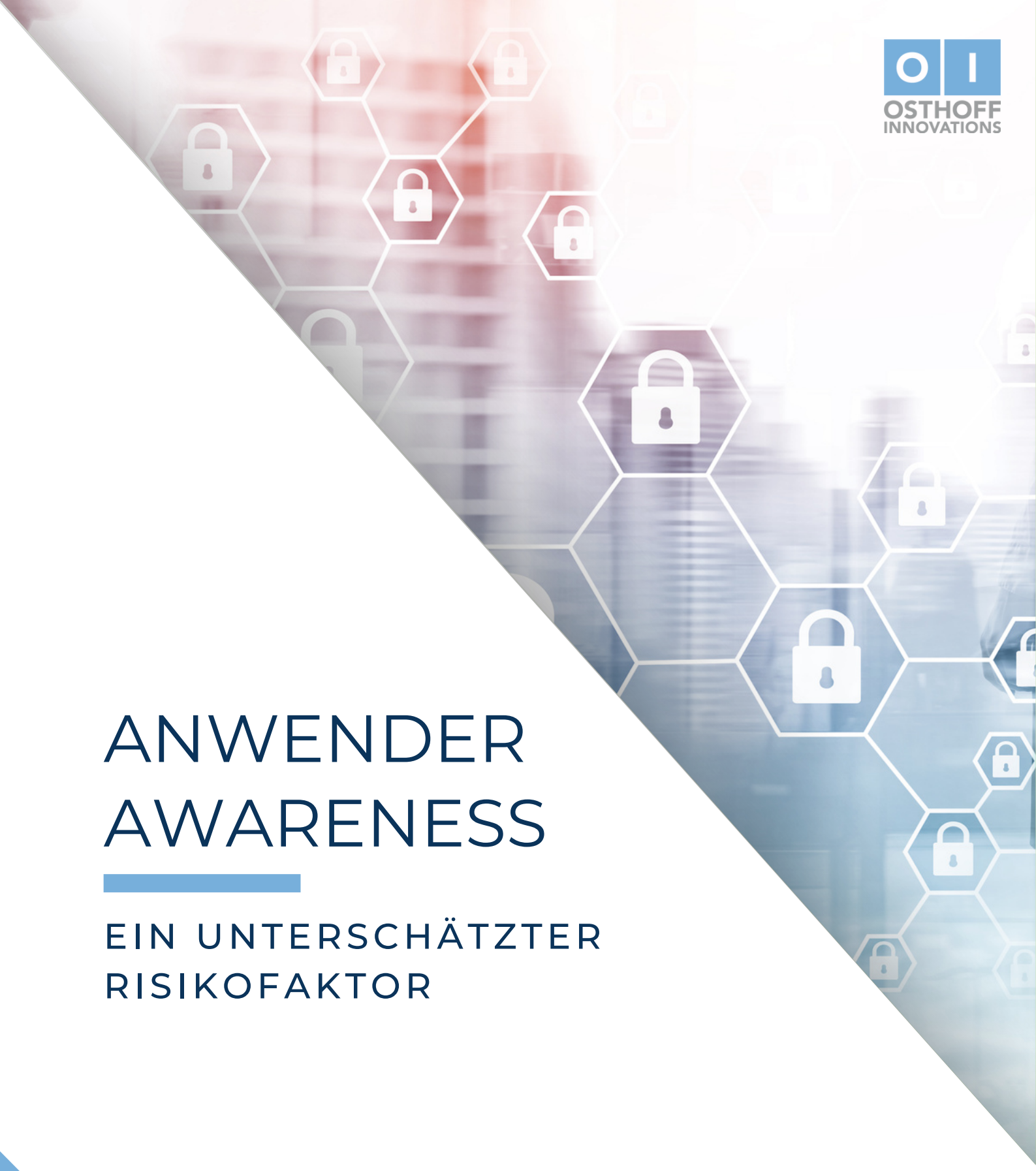

ANWENDER AWARENESS

EIN UNTERSCHÄTZTER RISIKOFAKTOR

Osthoff innovations
www.osthoff.net - info@osthoff.net
Lautenschlager Str. 23A, 70173 Stuttgart

Inhaltsverzeichnis

OSTHOFF INNOVATIONS

Einleitung

In der heutigen digitalen Welt sind wir ständig mit neuen Technologien und Anwendungen konfrontiert, die unser Leben erleichtern und bereichern. Doch gleichzeitig stellen diese Entwicklungen auch neue Risiken und Herausforderungen für unsere Sicherheit und Privatsphäre dar.

Während Cyberkriminalität und Hackerangriffe weiter zunehmen, ist es für Unternehmen essentiell, ihre IT-Sicherheit stetig zu verbessern. Die Anwender-Awareness ist dabei ein oft unterschätzter Faktor, da trotz aller technischen Schutzmechanismen nicht selten Unvorsichtigkeit seitens der Mitarbeiter das Unternehmen anfällig für Angriffe machen. Dabei lassen sich 95% aller Cybersicherheitsvorfälle auf menschliches Fehlverhalten zurückzuführen.

Anwender Awareness beschreibt die Sensibilisierung von Mitarbeitern hinsichtlich IT-Sicherheit, Cybersecurity und Datenschutz. Geschärftes Bewusstsein und regelmäßiges Training verhindern prophylaktisch Schäden an kritischer Unternehmensinfrastruktur und Datendiebstahl, der von vertraulichen Mitarbeiterinformationen bis zu Zugangsdaten firmeneigener Bankkonten reichen kann.

Ein bewusster Umgang mit Technologien und Anwendungen, welcher durch verschiedene Schulungen und Maßnahmen erlernt und etabliert werden kann, trägt also dazu bei, Sicherheitsrisiken zu minimieren und die Nutzung von Computer-Systemen effektiver zu gestalten. Weiteres erfahren Sie in diesem White Paper.

Herausforderungen

Es gibt verschiedene Herausforderungen, die im Zusammenhang mit der Anwender Awareness auftreten und gemeistert werden wollen.

Mangelndes Bewusstsein für Bedrohungen und Risiken führt zu Unkenntnis bei Mitarbeitern über verschiedene Angriffsarten wie Phishing oder Ransomware. Dadurch können Sicherheits-lücken unentdeckt bleiben und interne Daten gefährdet werden.

Des Weiteren resultiert die nachlässige Verwendung von Passwörtern und unsichere Datenverwaltung oft aus unzureichenden Schulungen der Anwender, die nicht über aktuelle Sicherheitspraktiken informiert sind. Im Optimalfall sollten sie regelmäßig und über einen längeren Zeitraum im korrekten Verhalten geschult werden. Studien zeigen, dass durch diese Kontinuität ein besseres Verständnis und ein adäquater Umgang mit auffälligen Situationen erreicht wird.

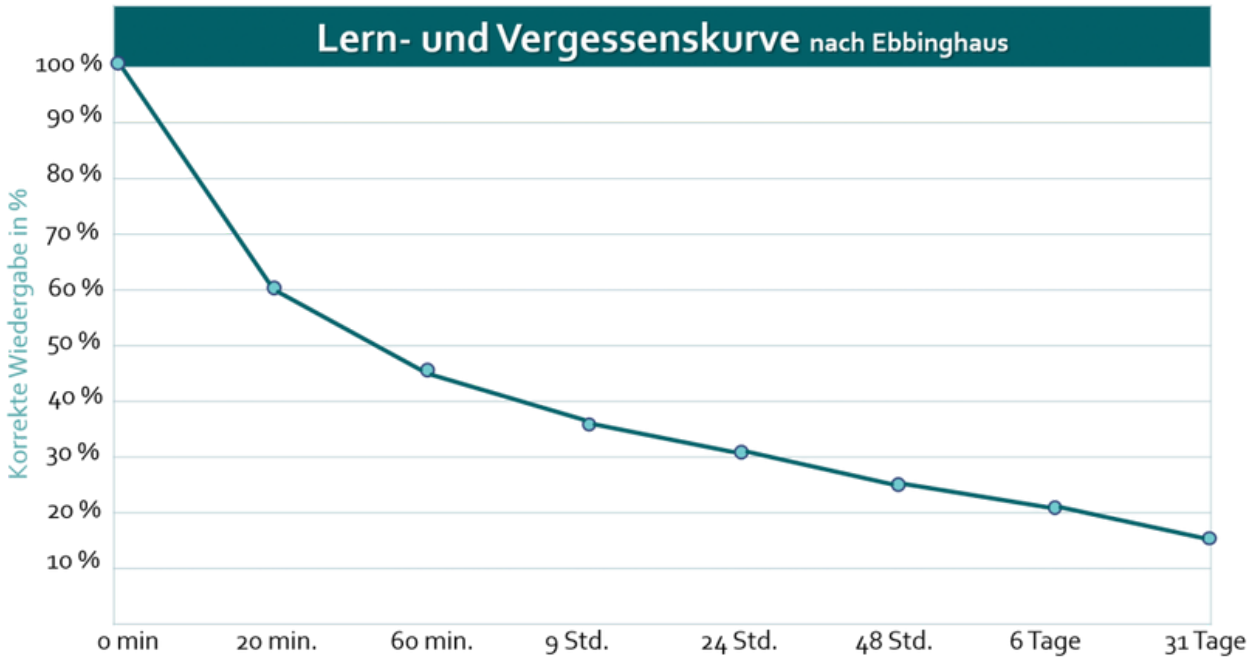

Abbildung 1: Lern- und Vergessenskurve nach Ebbinghaus (Quelle: https://q-five.com/einmal-gelernt-und-schon-wieder-vergessen)

Best-Practices zur Verbesserung der Anwender Awareness

Um die Anwender Awareness zu verbessern, gibt es verschiedene bewährte Praktiken, die Unternehmen verwenden können.

Die gängigste Methode sind Schulungen und Trainings zu neuen Bedrohungen und Technologien, inklusive Übung zum Umgang mit Phishing-Mails und anderen Vorkommnissen. Zudem ist es wichtig, dass Anwender über Strategien und Variationen von Cyberangriffen informiert sind.

Strategisches Training über Monate zu den verschiedenen Phishing-Mails reduziert die Anfälligkeit, erhöht das Bewusstsein und die Sicherheit von Mitarbeitern. Das Resultat sind weniger Malware, Virenvorfälle und Betrug bei Unternehmen.

13 Sofort-Tipps für ihr Unternehmen

1. Verdächtige Absender

Überprüfen Sie bei verdächtigen Mails zunächst den Absender. Seriöse Firmenadressen enden meist auf @firma. Phishing-Adressen können zwar einen Teil davon in der Absendeadresse enthalten, fallen aber oft durch einen Zusatz in der Mail-Adresse auf.

2. Checken Sie E-Mails auf Anhänge

Generell sollten Sie bei E-Mails mit Anhang von Ihnen unbekannten Absendern vorsichtig sein und sie im Zweifelsfall einfach löschen. Überprüfen Sie einen Anhang ganz genau, bevor Sie ihn öffnen. Es können sich versteckte Programme darin befinden, die automatisch ausgeführt werden und Daten ausspähen, ohne dass Sie es bemerken.

3. Drohungen & Fristen

Enthält die E-Mail Drohungen und setzt Ihnen enge Fristen (z. B. „Überweisen Sie bis zum nächsten Dienstag 50 Euro, sonst sperren wir Ihren Account.“), handelt es sich in der Regel um einen Betrugsversuch. Kriminelle erbeuten so nicht nur Ihre Daten, sondern auch Ihr Geld.

4. Eingabe persönlicher Daten

Sind Sie doch einem Link gefolgt, seien Sie ausgesprochen vorsichtig, wenn Sie zur Eingabe persönlicher Daten aufgefordert werden (z. B. PIN, Bankverbindung, Kreditkartennummer). Ihre Bank oder auch Online-Shops werden Sie nie per E-Mail zur Eingabe auffordern, wichtige Informationen gibt es in der Regel per Briefpost. Achten Sie aber in jedem Fall darauf, ob die Website verschlüsselt ist. Das erkennen Sie am „https://“ in der Adresszeile.

5. Zwei-Faktor-Authentifizierung

Steigern Sie die Sicherheit durch Kombination zweier Authentifizierungsmethoden, möglichst aus zwei unterschiedlichen Kategorien, z.B. SIM-Karte (Besitz) und PIN (Wissen).

6. Passwörter regelmäßig ändern

Ändern Sie Ihre Passwörter regelmäßig und verwenden Sie starke Passwörter. Nein, 12345678 ist kein starkes Passwort. Verwenden Sie am besten für jeden Account neue Anmeldedaten.

7. Seien Sie vorsichtig bei öffentlichem WLAN

Vermeiden Sie die Verwendung von öffentlichem WLAN für vertrauliche Transaktionen.

8. Technische Voraussetzungen

Stellen Sie sicher, dass Ihr Computer und Ihre Software auf dem neuesten Stand sind und dass Sie eine Antivirensoftware verwenden.

9. Keine unerwarteten E-Mails öffnen

Öffnen Sie keine unerwarteten E-Mails von unbekannten Absendern oder E-Mails mit Betreffzeilen, die zu gut klingen, um wahr zu sein.

10. Nicht nur im Notfall: Phishing-Verdacht melden

Melden Sie verdächtige E-Mails immer an Ihren IT-Verantwortlichen, Ihren IT-Support oder an eine offizielle Stelle wie das Bundesamt für Sicherheit in der Informationstechnik (BSI).

11. Verlinkungen und URLs überprüfen

Sie können ganz einfach herausfinden, ob eine verdächtige E-Mail versteckte Links enthält: Fahren Sie mit der Maus über Text und Bilder. Der Zeiger verwandelt sich in eine Hand und die verlinkte URL wird in einem gelben Kasten eingeblendet. Sind die Links gut versteckt, sollten Sie sie nicht anklicken. Ein genauer Blick lohnt sich immer: Enthält der Link Schreibfehler (z. B. paypall.com statt paypal.com) oder ist er der Webadresse eines Ihnen bekannten Anbieters sehr ähnlich (z. B. sparkasse-nuernberg.com statt sparkasse-nuernberg.de), ist das ein Hinweis auf einen Phishing-Versuch.

12. Immer gesicherte Netzwerke nutzen

Verwenden Sie nur gesicherte Netzwerke bzw. Webseiten und stellen Sie sicher, dass Ihre Verbindung verschlüsselt ist.

13. Wie verhält es sich mit der Sprache?

Ihre Bank oder auch Shopping-Portale versenden E-Mails in aller Regel mit einer persönlichen Anrede und in korrektem Deutsch. Sie sollten also stutzig werden, wenn Sie als „Sehr geehrte/r Nutzer/in“ angesprochen werden, die E-Mail auf Englisch oder in grammatikalisch nicht korrekter Sprache verfasst ist. Ziemlich sicher waren hier Betrüger am Werk.


Leistung aus Leidenschaft.

Deutsche Bank

Sehr geehrte Kundin, sehr geehrter Kunde,

Der technische Dienst der Bank fuhrt die planmassige Aktualisierung der Software durch Fur die Aktualisierung der Kundendatenbank ist es notig, Ihre Bankdaten erneut zu bestatigen. Dafuer mussen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfullen angeboten wird.

https://meine.deutsche-bank.de/mod/WebObjects/dbpbc.woa/407/wo/confirm.asp

Diese Anweisung wird an allen Bankkunden gesandt und ist zum Erfullen erforderlich.

Wir bitten um Verstandnis und bedanken uns fur die Zusammenarbeit

Abbildung 3: Phishing Mail (Quelle: https://de.wikipedia.org/wiki/Phishing)

Erfolgs-Metriken zur Bewertung der Anwender Awareness

Um die Wirksamkeit von Anwender-Awareness-Programmen zu bewerten gibt es Erfolgs-Metriken. Eine davon ist die Anzahl der erfolgreichen Phishing-Tests zu analysieren, welche zeigen, wie gut Anwender in der Lage sind, verdächtige E-Mails zu erkennen. Unternehmen können auch die Anzahl der gemeldeten Sicherheitsvorfälle und die allgemeine Sicherheitslage im Unternehmen überwachen, um die Effektivität ihrer Anwender-Awareness-Praktiken zu beurteilen.

Abbildung 4: IT-Sicherheit messbar machen (Quelle: https://www.presse-blog.com/2022/04/27/it-sicherheit-messbar-machen-it-seal-erhaelt-patent-fuer-den-esi/)

Angriffe

Es gibt unterschiedliche Arten von Phishing-Angriffen, auf die man vorbereitet sein muss. In den letzten Jahren hat sich ihre Anzahl und die der gefährlichen Webseiten signifikant erhöht. Je nach Motivation und Können der Angreifer sind diese unterschiedlich aufwendig und ebenso verschieden schwer zu erkennen. Die wichtigsten Arten sind im Folgenden aufgelistet.

E-Mail-Phishing

Angreifer verschicken gefälschte E-Mails, die vorgeben von einer vertrauenswürdigen Quelle zu kommen, um vertrauliche Informationen wie Benutzernamen, Passwörter oder Kreditkarteninformationen zu erlangen.

Eine andere Möglichkeit ist, dass der Angreifer sich als Mitglied des Unternehmens ausgibt, um an vertrauliche Informationen zu gelangen. Diese Phishing-Mails sind nicht direkt auf den Empfänger angepasst.

Spear Phishing

Bei diesem gezielten Angriff werden speziell Personen im Unternehmen ins Visier genommen. Dazu werden Informationen über die Zielpersonen gesammelt, um die E-Mail authentischer erscheinen zu lassen. Beispiele sind E-Mails, die auf vorherige Konversationen mit einem gehackten Geschäftspartner oder Kollegen aufbauen. Andere Möglichkeiten sind E-Mails zu Themen, die das Opfer gerade bearbeitet, sowie Überweisungsaufforderungen die angeblich vom Geschäftsführer kommen.

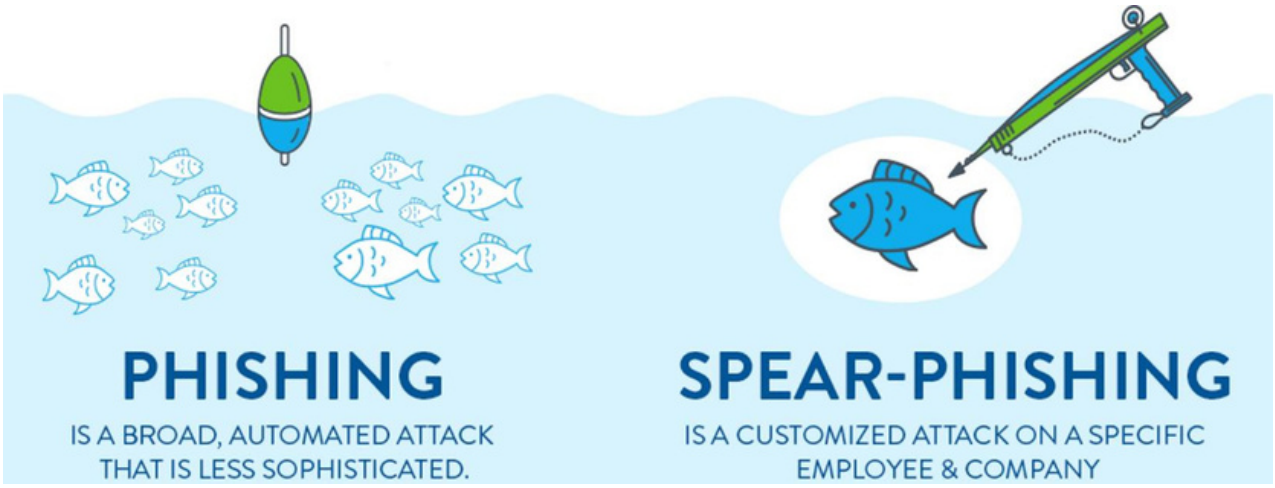

Abbildung 5: Unterschied zwischen Phishing und Spear Phishing (Quelle: https://www.reliancebank.com.au/SpearPhishing)

Phishing über Social Media

Der Angreifer nutzt Social-Media-Plattformen wie Facebook, LinkedIn oder Twitter, um gefälschte Profile zu erstellen und so an vertrauliche Informationen zu gelangen.

Spoofing

Spoofing ist eine Angriffstechnik bei der Kriminelle in Computer oder Netzwerke eindringen, indem sie eine vertrauenswürdige Identität durch eine gefälschten Absenderadresse vortäuschen.

Vishing

Hierbei handelt es sich um eine Phishing-Technik, bei der der Angreifer das Opfer telefonisch kontaktiert und sich als eine vertrauenswürdige Person oder Organisation ausgibt. Der Anruf dient dazu, persönliche Informationen zu sammeln oder einen weiteren Angriff vorzubereiten.

Pharming

Hierbei handelt es sich um eine Phishing-Technik, bei der der Angreifer das Opfer telefonisch kontaktiert und sich als eine vertrauenswürdige Person oder Organisation ausgibt. Der Anruf dient dazu, persönliche Informationen zu sammeln oder einen weiteren Angriff vorzubereiten.

Verweise zu Webseiten

Die Webseiten, auf die in Mails verwiesen werden, sind meist perfekte Nachahmungen der korrekten Webseiten, inklusive Logo, Farbgebung und Schriftarten, sodass sie täuschend echt aussehen.

Weiteres

Social-Engineering-Angriffe

Ein wichtiger Faktor bei Phishing-Mails ist das Social Engineering. Hierbei werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um die Opfer dazu zu bringen, selbstständig Daten preiszugeben, Schutzmaßnahen zu umgehen oder Schadprogramme auf ihrem System zu installieren.

Selbstständiges Erkennen

Es gibt verschiedene Möglichkeiten, wodurch Angriffe auffällig werden können. Mitarbeiter sollten darüber informiert werden, wie diese Kennzeichen aussehen. Zu den Merkmalen gehören zum Beispiel, dass es um Geld oder besondere Daten geht, es besonders dringend ist, einen bedrohlichen Unterton hat oder es Unstimmigkeiten in der Mail gibt.

Abbildung 6: 6 Punkte, um eine Phishing-Mail zu erkennen (Quelle: https://www.ines-it.de/news/phishing-mails-erkennen-und wie-sie-mit-phishing-trainings-die-awareness-erhoehen/)

Folgen

Sobald es den Kriminellen gelungen ist, in das System vorzudringen, können verschiedene Angriffe folgen. Eine Möglichkeit ist das Einsetzten von Ransomware. Bei diesem Angriff wird bösartige Software auf den Systemen installiert, die dann Daten verschlüsselt und nur gegen Zahlung eines Lösegeldes wieder freigibt.

Eine andere häufig eingesetzte Methode ist der Einsatz von Malware. Dabei wird schädlicher Code auf den Systemen installiert, um entweder Daten zu stehlen oder das System zu beeinträchtigen.

Des Weiteren können Viren innerhalb ihres Systems geschleust werden. Diese können dann kritische Systemdateien löschen und damit das Betriebssystem schädigen, das Netzwerk mit einer DDoS-Attacke überfluten und somit überlasten oder sich auf andere Art und Weise negativ auf die Systemleistung auswirken.

Fragen?

Melden Sie sich jederzeit, wenn Sie Fragen zu Ihrer IT-Sicherheit haben. Auf unserer Webseite finden Sie weitere Informationen und Soforthilfemaßnahmen, um Sicherheitslücken in Ihrem Unternehmen zu vermeiden. Auf der nächsten Seite finden Sie außerdem unsere effektivste Lösung gegen Phishing.

90% aller Hacking-Angriffe sind auf menschliche Fehler zurückzuführen

Schützen Sie Ihre Firma - Schulen Sie Ihr Team

Unser spezielles Phishing Training ermöglicht es Ihren Mitarbeitern, im Arbeitsalltag festzustellen, wie die verschiedenen Angriffe aussehen können und zu lernen, wie auf diese reagiert werden soll. Hierfür stellen wir Ihnen auf Ihre Bedürfnisse individuell zugeschnittene Lerninhalte zur Verfügung.

So werden Ihren Mitarbeitern über mehrere Monate Phishing Mails verschiedener Arten und Komplexitäten zugesendet. Durch die langfristige und regelmäßige Übung werden die Angestellten Sicherheit im Umgang mit diesen E-Mails gewinnen und weniger Fehleranfällig sein.

Übersicht

- Bis zu 3 Phishingsimulationen pro Nutzer/Monat
- KI-gesteuert: das Anforderungslevel wird an das Fehlverhalten angepasst
- Zentraler Zugriff auf alle Lerninhalte
- Interaktive Trainingseinheiten
- Gamification: Leistungsansporn und Spaß
- Auswertung der individuellen Phishing Simulation

Unsere Leistungen

Einrichtung & Setup

Auswertung der Fail-Trigger

Jahresgespräche & Notfallhilfe

Anpassungen & Verbesserungen

Quellenverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (o. D.): Betrug durch gefälschte Telefon- nummern und E-Mail-Adressen, [online] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Gefaelschte-Absenderadressen/gefaelschte-absenderadressen_node.html [abgerufen am 28.03.2023].

Bundesamt für Sicherheit in der Informationstechnik (o. D.): Phishing & Smishing auf dem Vormarsch, [online] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html [abgerufen am 28.03.2023].

Bundesamt für Sicherheit in der Informationstechnik (o. D.): Social Engineering, [online] https://www.bsi.bund.de/dok/11312692 [abgerufen am 28.03.2023].

Dr. Hesse, Carsten (2015): Methoden des Social Engineering, [online] https://www.allianz-fuer- cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/partner/150420_Partnerbeitrag_Riskworkers.pdf?__blob=publicationFile&v=1 [abgerufen am 28.03.2023].

Dr. Horch, Dietmar (2023): Lern- und Vergessenskurve nach Ebbinghaus, [online] https://q- five.com/einmal-und-schon-wieder-vergessen [abgerufen am 28.03.2023].

Dr. Schmerl, Sebastian (2021): Sechs Herausforderungen für Security-Awareness Kampagnen, [online] https://www.it-daily.net/it-sicherheit/cloud-security/sechs-herausforderungen-fuer-security-awareness-kampagnen [abgerufen am 28.03.2023].

Easydmarc (2022): 12 Arten von Phishing-Angriffen und wie man sie erkennt, [online] https://easydmarc.com/blog/de/12-arten-von-phishing-angriffen-und-wie-man-sie-erkennt/ [abgerufen am 29.03.2023].

F-Secure (o. D.): Was ist die 2 Faktor-Authentifizierung?, [online] https://www.f-secure.com/de/articles/what-is-two-factor-authentication [abgerufen am 05.04.2023].

Forum Verlag Herkert GmbH (2021): Security Awareness: Definition, Maßnahmen und Tipps zur Umsetzung https://www.forum-verlag.com/blog-di/security-Awareness [abgerufen am 05.04.2023].

HvS-Consulting AG (o. D.): Security Awareness Training, [online] https://www.is- fox.com/de/know-how/security-awareness-training-im-uberblick/ [abgerufen am 29.03.2023].

INES-IT (o. D.): 6 Punkte, an denen Sie eine Phishing-Mail erkennen, [online] https://www.ines- it.de/news/phishing-mails-erkennen-und-wie-sie-mit-phishing-trainings-die-awareness-erhoehen/[angerufen am 29.03.2023].

IT-Seal (2022): IT-Sicherheit messbar machen: IT-Seal erhält Patent für den ESI, [online] https://www.presse-blog.com/2022/04/27/it-sicherheit-messbar-machen-it-seal-erhaelt-patent-fuer-den-esi/[abgerufen am 28.03.2023].

Kanyo, Mate (2019): Lerninhalte durch optimale Wiederholung behalten, [online] https://www.bildungsblog.ch/lerninhalte-durch-optimale-wiederholung-behalten/#:~:text=Durch%20regelm%C3%A4ssiges%20Wiederholen%20von%20Lerninhalten,485%2D487 [abgerufen am 28.03.2023].

Proofpoint (o. D.): Was ist Security Awareness Training?, [online] https://www.proofpoint.com/de/threat-reference/security-awareness-training [abgerufen am 28.03.2023].

OSTHOFF INNOVATIONS

Reliance-Bank (o. D.) Unterschied Phishing und Spear-Phishing, [online] https://www.reliancebank.com.au/SpearPhishing [abgerufen am 29.03.2023].

Wiercks, Frank (2022): Phishing mit E-Mails erkennen und Angriffe abwehren, [online] https://www.trialog-magazin.de/personal-und-fuehrung/mitarbeiter-ausbildung/phishing-mail-bedeutung-und-beispiele/ [abgerufen am 29.03.2023].

OSTHOFF INNOVATIONS

Osthoff innovations
Kai Osthoff

Lautenschlager Straße 23A
70173 Stuttgart

+49 7114 009 5300
info@osthoff.net