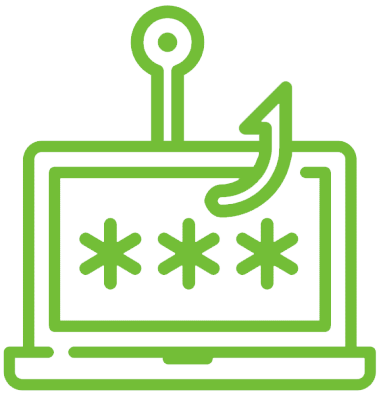
Phishing – die Gefahr lauert im Netz

TreeSolution
SECURITY AWARENESS SINCE 2005

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

Cyber-Risiken wie der Befall mit Schadprogrammen durch Phishing-Attacken haben in den letzten Jahren immer mehr zugenommen. Das zeigt auch der Allianz Risk Barometer *(1)*. Die Befragten sehen Cyber-Risiken als grösstes Risiko für das kommende Jahr.



90 %

der Datendiebstähle beginnen mit einer Phishing-E-Mail *(5)*

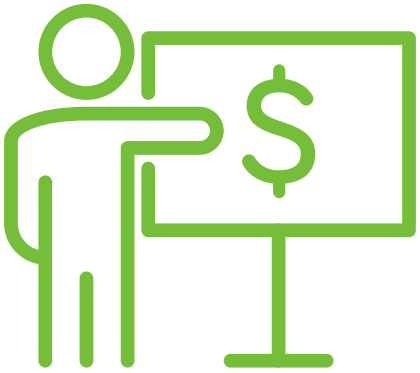
Zunehmend sind nicht nur grosse Firmen im Visier der Angreifer, sondern auch kleine und mittlere Unternehmen. In der Schweiz haben die Attacken in den letzten Wochen und Monaten stark zugenommen. Man kann fast täglich von betroffenen Unternehmen lesen. Eine Befragung von DigitalSwitzerland *(2)* unter 506 Geschäftsführenden von kleinen und mittleren Unternehmen ergab, dass im letzten Jahr 36 % Opfer eines Cyberangriffs wurden. Dies entspricht einer Steigerung von 11 % (im Vorjahr waren es 25 %). Dabei entstanden unter anderem finanzielle Schäden, Schäden am Image des Unternehmens oder ein Verlust von Kundendaten. Potential sieht die Studie bei der Steigerung der Mitarbeiterschulung. Nur 39 % der Befragten schulen ihre Mitarbeitenden regelmässig, 21 % schulen gar nicht.

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

Wird ein Unternehmen durch Phishing erfolgreich mit Schadprogrammen infiziert, kann die Produktion zwischen einem Tag und mehreren Wochen still stehen, bis der Schaden behoben ist. Auch dauert es teilweise Monate, bis betroffene Unternehmen realisieren, dass sie Opfer eines Cyberangriffs wurden.

Die häufigsten Angriffe mit Schadprogrammen erfolgen über Phishing-E-Mails. Weshalb? Weil der Mensch eine der erfolgreichsten Einflugschneisen für Angriffe darstellt. Die Hacker setzen auf die Unwissenheit, Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit ihrer Opfer. Eine Eine Phishing-E-Mail zu erstellen ist einfach und kostengünstig und kann per Knopfdruck an Tausende von Personen gleichzeitig versendet werden. Und bei jedem solchen Angriff fallen dutzende, wenn nicht gar hunderte Personen darauf rein.

Spam-Filter können oft nicht alle Phishing-E-Mails rechtzeitig erkennen. Daher ist es wichtig, dass alle Mitarbeitende geschult sind und Phishing selbst erkennen und so zum Schutz des Unternehmens beitragen.



14.8 Millionen Dollar

haben Unternehmen im Jahr 2021 im Durchschnitt aufgrund von erfolgreichen Phishing-Attacken verloren. ***(5)***

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

Was genau ist Phishing?

Heutzutage ist jeder von uns, egal ob Privatperson oder Mitarbeitende/r, potenzielles Ziel von Hackerangriffen und somit von Phishing. Wahrscheinlich haben auch Sie schon mal eine Phishing-E-Mail erhalten.

Die Angreifer werden immer professioneller und daher wird es auch immer schwieriger, Phishing-E-Mails zu erkennen. Es ist sehr wichtig, dass man bei E-Mails kritisch ist.

Mit Phishing-E-Mails, Instant Messaging, persönlichen Nachrichten oder Internetseiten versuchen Angreifer an die Daten ihrer Opfer zu gelangen. Besonders beliebt sind Zugangsdaten wie Passwörter, Benutzernamen oder Kontoinformationen. Mithilfe von Links und verseuchten Internetseiten kann auch Ransomware auf einem PC oder Firmennetzwerk eingeschleust werden

Hat ein Hacker einmal Zugang zu Nutzerkonten oder Netzwerken erlangt, so können Kunden- oder Geschäftsdaten ausgespäht oder gestohlen werden. Geldüberweisungen können getätigt oder Systeme manipuliert oder gar betriebsunfähig gemacht werden. Oft folgen auf einen ersten Angriff noch weitere Angriffe, was zu grossen finanziellen Verlusten und Imageschäden führen kann. In schwerwiegenden Fällen führt es bis zum Konkurs.

Mehr als

2 Millionen Phishing-Internetseiten

wurden 2020 durch Google entdeckt. Das entspricht einem Anstieg von ca. 20 % gegenüber dem Vorjahr. *(6)*

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

Die verschiedenen Formen von Phishing

Gefälschte Internetseiten, E-Mails und Kurznachrichten

Mit täuschend echt aussehenden E-Mails oder Internetseiten wollen Angreifer ihre Opfer dazu bewegen, ihre persönlichen Daten in einem gefälschten Internetformular oder in einer E-Mail anzugeben. Die Nachrichten enthalten oft Links, die auf gefälschte Internetseiten führen und zur Dateneingabe auffordern. Dies kann z. B. eine gefälschte Login-Seite Ihrer Bank oder von Ihrem Arbeitgeber sein.

Schadprogramme in Dateianhängen oder auf Internetseiten

Per E-Mail werden die Opfer dazu verleitet, einen verseuchten Anhang zu öffnen oder eine verseuchte Internetseite zu besuchen. Der Anhang oder die Internetseite installiert anschliessend automatisch und vom Nutzer unbemerkt eine Schadsoftware unbemerkt eine Schadsoftware auf dem PC. Dadurch erhalten Cyberkriminelle direkten Zugriff auf das Gerät oder das Netzwerk des Opfers und dessen Daten.

Spear Phishing

Spear Phishing-Nachrichten sind gezielt auf das Opfer abgestimmt. Vor einem Angriff informieren sich die Cyberkriminellen im Internet, z. B. auf LinkedIn oder Facebook, über ihre Opfer. Die erlangten Informationen verwenden sie in der Phishingnachricht und erhöhen damit die Glaubwürdigkeit. Dadurch steigt die Wahrscheinlichkeit, dass das Opfer auf die Nachricht hereinfällt und seine Daten angibt. Diese Art von Phishing erfordert mehr Zeit von den Cyberkriminellen und richtet sich oft an Personen aus der Finanzabteilung, dem HR, dem höheren Management oder der Produkteentwicklung. Aber auch einflussreiche oder angesehene Persönlichkeiten aus der Politik, dem Showbusiness oder der Wirtschaft sind beliebte Opfer. Aber Achtung, auch der «Otto-Normalverbraucher» kann zu einem solchen Ziel werden!

CEO Fraud

Beim CEO Fraud werden E-Mails vom «CEO» an Personen mit Entscheidungskompetenz im Finanzbereich versendet, z. B. jemand aus der Finanzabteilung oder der persönlichen Assistenz. Der vermeintliche «CEO» fordert diese Personen auf, dringend Geld an eine bestimmte Adresse zu überweisen, da z. B. sonst ein Geschäft nicht abgeschlossen werden kann. Ist das Geld einmal überwiesen, hat das Unternehmen kaum eine Chance, dieses zurückzubekommen.

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

PHISHING ERKENNEN

1. Merkwürdiger Absender

Ist Ihnen der Absender nicht bekannt? Sie hatten mit dieser E-Mail-Adresse noch nie Kontakt? Dann sollten Sie misstrauisch sein!

Das gilt auch, wenn der Absender, also der E-Mailheader bzw. die E-Mail-Adresse nicht zum hinterlegten Internet-Link passt (Beispiel: *mailto:no_reply@europcar.ch* / Internetseite: *www.europcart.ch*).

Absenderadressen werden leicht gefälscht, diese enthalten dann oft kleine Fehler oder eine andere URL (zum Beispiel *.net* statt *.com*).

Ein weiteres Zeichen ist eine persönliche Absenderadresse (z. B. *@gmail.com* oder *@outlook.com*), auch wenn die Nachricht vorgibt, von einem Unternehmen zu sein.

Betreff: **Wichtige Nachricht**

Von: IT Support Center <mailer@itsup-center.net> 1
Datum: Freitag, 25. Marsch 2022 07:23
Anhang: Wichtig_Readme.zip 2

Lieber User, 3

Wir schliessen alle unbenutzte und inaktiven Computer-Account, Sie müssen Ihre Account verifizieren 4 indem Sie sich innerhalb der nächsten 24 Stunden 5 an unserem Verifizierungs-System anmelden 6 um die Sperrung Ihres Accounts zu verhindern HIER KLICKEN 7 für die Verifizierung. Bitte ignorieren Sie diese Nachricht wenn Sie Ihren Account schon verifiziert haben.

Thanks 8
IT Support Center 9

2. Unübliche oder dubiose E-Mailanhänge

E-Mailanhänge können PCs und Netzwerke mit Schadprogrammen infizieren. Daher sollten dubiose Anhänge nicht geöffnet werden. Fragen Sie im Zweifelsfall beim Absender nach.

Wichtig: Antworten Sie dafür nicht in der Nachricht, sondern wählen Sie einen anderen Kommunikationskanal wie z. B. das Telefon. Wenn Sie unsicher sind, öffnen Sie den Anhang besser nicht.

Achten Sie bei der Nutzung von Windows darauf, dass im Windows Explorer im Register «Ansicht» die Auswahl «Dateinamenerweiterungen» aktiviert ist. Ist diese Einstellung deaktiviert, erkennt man den Dateityp nicht auf Anhieb. Es besteht somit die Gefahr, dass man manipulierte Erweiterungen wie bspw. *«Dokumentenname.pdf.exe»* nicht erkennt und eine Datei mit einem Schadprogramm öffnet.

3. Unpersönliche Ansprache

Eine unpersönliche Anrede, wie z. B. *«Sehr geehrter Kunde»*, kann ein Hinweis auf Phishing sein. Aber Vorsicht: Cyberkriminelle können sich über soziale Netzwerke oder Suchmaschinen über ihre Opfer informieren und sie so gezielt anschreiben (das sogenannte «Spear Phishing»).

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

4. Grammatik- und Orthografie-Fehler

Fehlerhaftes Deutsch, Zeichensatzfehler, fehlende Buchstaben oder Umlaute, Grammatik- und Orthografie-Fehler, Buchstaben aus anderen Alphabeten (z. B. kyrillische Buchstaben). Achtung: Buchstaben aus einem anderen Alphabet sind oft sehr schwer zu erkennen.

5. Aufforderung zum dringenden Handlungsbedarf

Wenn Sie aufgefordert werden, innerhalb einer kurzen Frist zu handeln, oft verbunden mit einer Drohung (z. B. der Sperrung von Kreditkarten oder Online-Zugängen), kann dies auf Phishing hinweisen. Prüfen Sie daher genau, ob die Aufforderung wirklich berechtigt ist. Oft ist eine Einladung auch «zu schön, um wahr zu sein».

6. Eingabe von Daten

Wenn Sie aufgefordert werden, persönliche Daten, wie Passwort, PIN oder TAN einzugeben, sollten Sie aufpassen. Merken Sie sich: Kein seriöses Unternehmen fordert ihre Kunden auf, über einen beigefügten Link oder ein angehängtes Formular ihre Benutzerdaten zu ändern. Wenn doch, dann ohne direkten Link auf die Login-Seite. Passen Sie Benutzerdaten immer über die von Ihnen gespeicherte Internetseite an. Beantworten Sie niemals E-Mails, in denen nach Benutzernamen, Passwörtern oder Kontoinformationen usw. gefragt wird.

7. Gefälschte Links

Die Nachricht enthält eine oder mehrere Links, welche auf eine Adresse verweisen, die nicht zum Adressbereich des Absenders gehört. (BEISPIEL Absender: *info@ebay.net* Link: *http://www.paypal.com-verfy-transactionid-7961312693567631367.login.ebay-buyerprotection.net*).

Überprüfen Sie zudem, dass keine Sonderzeichen (z. B. aus dem kyrillischen Zeichensatz, Leerschläge, etc.) in der URL enthalten sind. Um eine URL zu prüfen, fahren Sie mit der Maus über den Link. In einem Pop-up-Fenster erscheint der ausgeschriebene Link. Wenn das nicht funktioniert, müssen Sie dies in den Einstellungen aktivieren. Überlegen Sie sich gut, ob Sie den Link besuchen müssen oder nicht und klicken Sie nicht einfach aus Neugierde drauf.

8. Fremde Sprachen bzw. Sprachenmix

Normalerweise ist die Kommunikation in der Sprache des Empfängers. Manchmal, wie in der Beispiel-E-Mail im Bild, werden mehrere Sprachen vermischt. Einerseits ist dies verdächtig, andererseits wirkt es nicht sehr seriös, wenn ein Unternehmen zum Beispiel mit *«Thanks»* in einer deutschen E-Mail abschliesst.

9. Verwendung unüblicher Bezeichnungen

Wenn für Abteilungen, Produkte oder Dienste unübliche oder unbekannte Bezeichnungen verwendet werden, sollten Sie aufhorchen und vorsichtig sein. Prüfen Sie im Intranet, ob diese Bezeichnung innerhalb des Unternehmens verwendet wird. Falls nicht, die E-Mail melden und löschen.

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

Richtig Handeln bei Verdacht auf Phishing

Wenn Sie eine E-Mail erhalten, welche Ihnen verdächtig erscheint oder Sie diese deutlich als Phishing erkennen, melden Sie sich immer unverzüglich bei Ihrem IT Service Desk. Verwenden Sie dafür die in Ihrem Unternehmen gängige Methode (z. B. durch Weiterleiten der E-Mail an den IT Service Desk oder das Melden über eine bestimmte Schaltfläche im E-Mail-Programm).

Nur durch Ihre Mithilfe können Phishing-Angriffe frühzeitig erkannt und die nötigen Gegenmassnahmen ergriffen werden. Es ist daher wichtig, solche E-Mails sofort zu melden, nicht zu beantworten oder auf darin enthaltene Links oder Anhänge zu klicken. Der technische Schutz der IT-Infrastruktur in einem Unternehmen ist in der Regel gegeben, so dass hier kaum noch Hacker-Angriffe zu verzeichnen sind. Über die Mitarbeitenden, also die Nutzer der IT-Infrastruktur, können Hacker jedoch immer noch sehr erfolgreich an Geld, Daten und Informationen gelangen und Lösegeld erpressen. Aus diesem Grund ist es so wichtig, dass auch die Menschen, welche die IT-Infrastruktur nutzen, wissen, wie sie sich sicher verhalten. Insbesondere im Umgang mit Phishing. Schulen Sie Ihre Mitarbeitenden in den Themen der Informationssicherheit und vermindern Sie so das Risiko eines erfolgreichen Hackerangriffs.

Möchten Sie regelmässig über spannende Themen, Tipps und Tricks aus dem Bereich Informationssicherheit und Security Awareness informiert werden? Bleiben Sie auf dem Laufenden und abonnieren Sie unseren Newsletter. Hier geht es zum Anmeldeformular: https://www.treesolution.com/news

Haben Sie Fragen zu unseren Produkten und Services? Vereinbaren Sie jetzt ein kostenloses Beratungsgespräch. Hier geht es zur Anmeldung: https://treesolution.link/downloads/beratung

TreeSolution
SECURITY AWARENESS SINCE 2005

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

Quellen:

1. Allianz Risk Barometer 2022
   https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
2. Digital Switzerland 2021: Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU.
   https://digitalswitzerland.com/sub-programm/digitalswitzerland-studies/
3. Sophos 2021: Phishing Insights 2021.
   https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-phishing-insights-2021-report.pdf
4. Verizon: 2021 Data Breach Investigations Report (DBIR).
   https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf
5. Ponemon Institute. Cost of Phishing study 2021
   https://www.proofpoint.com/us/resources/analyst-reports/ponemon-cost-of-phishing-study
6. Forbes 2020:
   https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/

TreeSolution Security Awareness AG
+41 58 510 98 00
info@treesolution.com
www.treesolution.com

TREESOLUTION
SECURITY AWARENESS SINCE 2005