Halloween-Saison: Keeper Security warnt vor Phishing-Angriffen

Nicht täuschen lassen, denn Cyberkriminelle haben gruselige Tricks auf Lager.

München, 26. Oktober 2023 – Findet man im Handel und an Ständen die orangenen Kürbisse, ist sie auch schon da: die Halloween-Saison. Kürbisse schnitzen, Süßes oder Saures geben, Kostüme planen, Süßigkeiten für die Kinder besorgen und natürlich Gruselfilme ansehen. Eine der gruseligsten Bedrohungen ist allerdings wenig witzig, weder für Privatpersonen noch für Unternehmen. Denn jetzt ist auch Hochsaison für Cyberkriminelle und ihre Phishing-Betrügereien. Ähnlich wie verkleidete Kinder, die an Halloween an die Tür kommen und um Süßigkeiten bitten, maskieren sich Cyberkriminelle, um Menschen dazu zu bringen, Informationen wie Benutzernamen und Passwörter und vieles mehr preiszugeben. Keeper Security gibt Tipps, um zu verhindern, dass man von Cyberkriminellen heimgesucht wird.

Es ist wichtig, wachsam zu sein. Und es ist wichtig, die verräterischen Zeichen von Phishing-Angriffen der Bösewichter zu erkennen, um zu verhindern, dass man ihnen zum Opfer fällt. Die Cyberhexen verwenden häufig die folgenden Zutaten für ihren Phishing-Trank:

Elixier 1: Auffordernde und dringliche Sprache: Phishing-Versuche enthalten oft eine Sprache, die ein Gefühl der Dringlichkeit vermittelt. Damit wollen Cyberkriminelle erreichen, dass das Opfer so schnell wie möglich handelt und keine Zeit für Zweifel an der Übermittlung der persönlichen Daten aufkommen.

Elixier 2: Unstimmigkeiten bei E-Mail-Adressen und Domänennamen: Ein weiteres Indiz ist, wenn bei einer E-Mail, die angeblich von einem Chef, einem Mitarbeiter, einem Freund oder einem Unternehmen stammt, die E-Mail-Adresse oder der Domänennamen nicht mit der Person übereinstimmen, die sie vorgibt zu sein. Oft sind es kleine Details in der E-Mail- oder Webadresse, die den feinen Unterschied machen, etwa ein o anstelle einer 0 oder .com anstelle von .net.

Elixier 3: Das Ersuchen um persönliche Informationen: Die plötzliche Aufforderung zur Angabe persönlicher Daten ist ebenfalls ein häufiges Anzeichen für Phishing-Versuche. E-Mails, Textnachrichten oder Anrufe von einer unbekannten Nummer mit der Behauptung ein bekanntes Unternehmen oder eine bekannte Person zu sein, sollten kritisch geprüft werden, bevor man persönliche Daten preisgibt - vor allem, wenn man das Gespräch nicht initiiert hat.

Elixier 4: Rechtschreibfehler und grammatikalische Fehler: Ein weiteres häufiges Anzeichen für einen Phishing-Versuch sind Rechtschreib- und Grammatikfehler in der Nachricht – auch wenn diese durch den Einsatz von KI seitens der Cyberkriminellen weniger werden. Bevor Unternehmen E-Mails an Kunden verschicken, werden diese mehrfach überprüft, um sicherzustellen, dass sie keine Fehler enthalten. Bei einer E-Mail mit offensichtlichen Fehlern, deren Verfasser sich als Unternehmen oder Privatperson ausgibt, ist die Chance eines betrügerischen Phishing-Versuchs hoch.

So wird der böse Zauber abgewehrt
Leider haben böswillige Akteure genauso viel Spaß an Cyberkriminalität wie Kinder an Kostümen und Süßigkeiten. Aber es gibt ein paar wirkungsvolle Maßnahmen, um Konten, Finanzdaten, sensible Dokumente und Identitäten vor den Heimsuchungen der Hacker zu schützen.

Gegenzauber 1: Innehalten und nachdenken, bevor man klickt: Wenn unaufgefordert Links und Anhänge per E-Mail, Textnachricht oder über andere Nachrichtenplattformen ankommen, sollten diese nicht arglos angeklickt werden. Diese Links und Anhänge können Malware enthalten, die vertraulichen Daten stehlen oder ausspionieren. Wer sich nicht sicher ist, kann mit der Maus über den Link fahren, um die vollständige Website-Adresse zu sehen. Wahlweise können auch Sicherheits-Checker wie der Google Transparency Report für mehr Sicherheit sorgen.

Gegenzauber 2: Verwenden eines Passwort-Managers: Ein Passwort-Manager hilft beim Erstellen, Verwalten und sicheren Speichern von Passwörtern und bietet eine integrierte Warnung vor Phishing-Seiten. Ein Passwort-Manager speichert die Webadresse mit den Anmeldedaten. Wenn die Daten also nicht automatisch ausgefüllt werden, bedeutet das, dass man sich nicht auf der echten Website befindet.

Gegenzauber 3: Verwenden eins E-Mail-Scanners: Ein E-Mail-Scanner ist ein Tool, das E-Mail-Anhänge auf potenzielle Malware überprüft. Die Investition in einen E-Mail-Scanner hilft, sich vor Phishing-Versuchen zu schützen, indem er gefährliche Anhänge identifiziert.

Gegenzauber 4: Aktivieren der Multi-Faktor-Authentifizierung: Konten sollten nicht nur mit sicheren Passwörtern geschützt sein, sondern nach Möglichkeit auch über eine Multi-Faktor-Authentifizierung (MFA). MFA erfordert, dass der Benutzer eine oder mehrere Formen der Authentifizierung zusätzlich zu seinem Benutzernamen und Passwort angibt. Selbst wenn man auf einen Phishing-Versuch hereinfällt und die Anmeldedaten für ein Konto preisgegeben werden, Verhindert die MFA, dass ein Cyberkrimineller auf das Konto zugreifen kann.

Gegenzauber 5: Im Zweifel mit dem Unternehmen oder der Person in Verbindung setzen: Wenn man eine E-Mail, eine Textnachricht oder einen Anruf erhält und Zweifel bezüglich der Echtheit und Legitimität bestehen, sollte die Person oder das Unternehmen direkt über eine andere Kommunikationsmethode kontaktiert werden. Wenn diese sagen, dass die Nachricht nicht von ihnen stammt, wurde ein Phishing-Angriff erfolgreich vermieden.

Über Keeper Security Inc.
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie mehr unter KeeperSecurity.com.

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de