SPECTRUM Hinweise

Unabhängiger KANZLEI Systempartner

Oktober 2024

Schützen Sie sich vor Cyberkriminalität

HAUFE berichtete im Oktober 2024: *„Es ist eine grausige Vorstellung - unbemerkt haben sich Fremde Zugang zum Kanzleinetzwerk verschafft und über viele Wochen akribisch Buchhaltungsbelege, Jahresabschlüsse und Mandantendaten digital gesammelt und auf eigenen Servern gespeichert. Dann ging bei der Kanzlei eine E-Mail ein: „Wir haben ihre Mandantendaten. Zahlen Sie 100.000 Euro in Bitcoin auf dieses Bitcoin Wallet, sonst werden die Daten veröffentlicht“.*

Ein solcher Fall kann sehr teuer werden, auch wenn nicht gezahlt wird. Die Systeme wiederherzustellen beziehungsweise neu aufzusetzen, ist nicht nur kostspielig, sondern vor allem zeitaufwendig.

> **Cyberattacken nehmen rasant zu: Laut einer aktuellen BITKOM-Studie sind 8 von 10 Unternehmen in Deutschland von Datendiebstahl, Spionage oder Sabotage schon betroffen worden und der angerichtete Schaden soll in den vergangenen zwölf Monaten fast 270 Milliarden Euro betragen haben.**

Haufe meldet: *„Steuerkanzleien stehen in einem besonderen Vertrauensverhältnis zu Mandantinnen und Mandanten und bearbeiten in der Regel hochsensible Daten. Sie sind daher ein attraktives Ziel für Cyberkriminelle. Nicht nur das Mandantenvertrauen kann durch Cyberattacken zerstört werden, Angreifer könnten auch Folgeangriffe auf die Betroffenen ausüben. Letztlich besteht neben hohen finanziellen Kosten auch Gefahr, dass die Reputation der Kanzlei so stark beschädigt wird, dass der Angriff sogar das Weiterbestehen der Kanzlei gefährdet“.*

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) berichtet, dass Phishing-E-Mails bis vor einigen Jahren meistens noch dadurch auffielen, dass die Anrede unpersönlich ("Sehr geehrter Kunde…") oder der Nachrichtentext in schlechtem Deutsch verfasst war. Heute gehen Kriminelle professioneller vor und setzen zur Erstellung der Phishing-Mails sogar KI ein. Tippfehler oder seltsame Umlaute im Text sind nur noch selten ein eindeutiger Hinweis auf einen Phishing-Versuch. Auch bei gut formuliertem Text sollte man deshalb wachsam sein.

Wenn Sie als SPECTRUM-ASP-Kunde Microsoft-365 einsetzen, durchlaufen alle E-Mails das SPECTRUM-NET-Sicherheitssystem mit 5 kaskadierten Virenscannern und nachgeschaltet die Microsoft-365-Filter- und Überwachungssysteme – mehr geht eigentlich nicht mehr. Leider erkennen die E-Mail-Filtersysteme selten die Phishing-Mails, da die Kriminellen die Phishing-Mails laufend verändern und dadurch nicht erkannt werden. Beim falschen Klick auf Phishing-Mails haben zwar die SPECTRUM-Proxy und -Firewall-Systeme meistens Schlimmeres verhindert, aber die Gefahr für große Schäden ist hoch.

Phishing-E-Mails können Kanzleien, Unternehmen oder Organisationen jeder Größe und Art treffen.

Hinweis: Seien Sie vorsichtig beim Öffnen von E-Mails, sensibilisieren Sie laufend Ihre Mitarbeiter - auch gefakte Mails von bekannten Absendern können Phishing-Mails sein.

Wenn Sie also eine E-Mail erhalten, auf die **mindestens eines der folgenden Merkmale** zutrifft, sollten Sie misstrauisch werden. Denn dann handelt es sich mit hoher Wahrscheinlichkeit um eine Phishing-Mail:

- Der Text der Mail gibt dringenden Handlungsbedarf vor, etwa: "Wenn Sie Ihre Daten nicht umgehend aktualisieren, dann gehen sie unwiederbringlich verloren …".
- Drohungen kommen zum Einsatz: „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren …".
- Sie werden aufgefordert, vertrauliche Daten wie die PIN für die Microsoft-Zweifaktor-Autorisierung, Ihren Online-Bankzugang oder eine Kreditkartennummer einzugeben.
- Die E-Mail enthält Links oder Formulare.
- Die Mail scheint zwar von einer bekannten Person oder Organisation zu stammen, jedoch kommt Ihnen das Anliegen des Absenders ungewöhnlich vor.
- Selbst wenn Sie von Ihrem besten Freund, Ihrem bekannten Geschäftspartner eine E-Mail oder eine Nachricht erhalten haben, sollten Sie immer daran denken, dass dieser Freund/Geschäftspartner hereingelegt oder gehackt worden sein könnte.

Fragen Sie lieber einmal zu viel beim Absender nach, ob die E-Mail tatsächlich von ihm stammt, bevor Sie auf Links in Phishing-Mails klicken.

Sie könnten in eine Massenkampagne geraten (bei der E-Mails wahllos an Millionen von Posteingängen gesendet werden), oder dies könnte dann der erste Schritt eines gezielten Angriffs auf Ihre Kanzlei, Ihr Unternehmen oder einen bestimmten Mitarbeiter sein.

In Steuerberater-Kanzleien führen speziell Personal-/Bewerbungs-Mails zu solchen Phishing-Attacken – seien Sie hier besonders vorsichtig.

Es werden leider immer auch Mails mit Word- oder Excel-Dateien im Anhang an Kanzleien oder Unternehmen verschickt (auch angebliche Bewerbungsunterlagen). Öffnen Sie die nicht (!), fordern Sie den Absender auf, Ihnen die Anhänge ausschließlich im PDF-Format zuzuleiten. Brauchen Sie die Datei im Word- oder Excel-Format, dann nutzen Sie sichere Datendrehscheiben wie den SPECTRUM-WEB-Tresor.

Bei einer Phishing-Mail im HTML-Format verbirgt sich hinter dem angezeigten Absender oft eine andere E-Mail-Adresse. Ob dem so ist, können Sie auf verschiedene Weise feststellen: Wenn Sie Ihre E-Mails mit einem Browser verwalten, werfen Sie einen Blick auf den sogenannten Quelltext der HTML-Mail. In einem gängigen E-Mail-Programm können Sie den Cursor einfach mit der Maus über die Absenderzeile führen, aber ohne darauf zu klicken. Dann sehen Sie, ob in der Absenderzeile eine andere Adresse eingebettet ist.

Generell sollten Sie jeden Link in E-Mails und sozialen Netzen vor dem Aufruf sorgsam prüfen. Viele Verdachtsmomente sind auch für Laien leicht erkennbar. Stutzig sollten Sie zum Beispiel werden, wenn die Internetadresse zwar den Namen der jeweiligen Institution enthält, aber in Verbindung mit ungewöhnlichen Zahlen oder Zeichenkombinationen besteht.

Hier ein Warnhinweis vom BSI:

Kommt es tatsächlich zu Angriffen aus dem Cyberraum, so sind die Auswirkungen für Unternehmen und Organisationen bisweilen meist dramatisch:

- Falls bei einem Cyberangriff personenbezogene Daten betroffen sind, muss eine Kanzlei oder ein Unternehmen die zuständige Datenschutzaufsichtsbehörde nach Artikel 33 der EU-Datenschutzgrundverordnung EU-DSGVO umgehend darüber informieren.
- Die EU-DSGVO schreibt dafür ein Zeitfenster von 72 Stunden vor.
- Hier reicht schon das Bekanntwerden der E-Mail-Adressen von Mandanten/Kunden aus, denn diese gelten als personenbezogene Daten und dann müssen unverzüglich alle Betroffenen informiert werden.
- Kontaktieren Sie immer umgehend ihren Datenschutzbeauftragten.

Seien Sie bitte aufmerksam und sensibilisieren Sie laufend Ihre Mitarbeiter !

Steigern Sie aktiv die Cyberkompetenz und schärfen Sie das Urteilsvermögen Ihrer Mitarbeiter, um Phishing-Angriffe zu verhindern und Cyber-Risiken mindern.