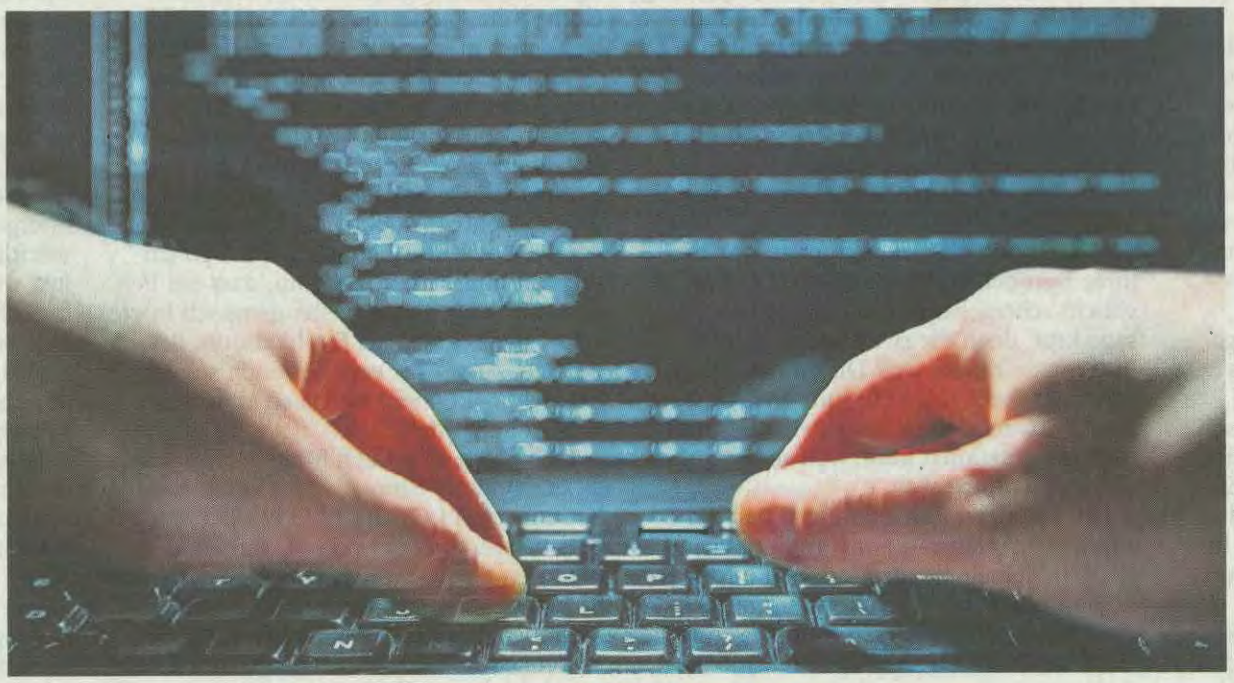
Vorbeugen ist besser als heilen

KEEP YOUR SPACE SAFE Bee Secure startet Kampagne im Kampf gegen Phishing

André Feller

Bei einem Phishing-Angriff versuchen Hacker an vertrauliche Informationen und Passwörter einzelner Internetuser zu gelangen. Ihre Opfer fallen meistens auf E-Mails herein, die jenen einer Bank, eines Bezahldienstes oder hierzulande dem Authentifizierungsdienst Luxtrust ähnlich sind. Unter dem Motto „Vorbeugen ist besser als heilen" hat Bee Secure eine neue aufklärende Kampagne „Keep your space safe" ins Leben gerufen.

Am Dienstagabend sollte eigentlich im Kulturzentrum „Schéiss" in Luxemburg-Stadt eine öffentliche Informationsveranstaltung zum Thema Bankdatenklau stattfinden. Diese wurde jedoch mangels vorheriger Anmeldungen kurzerhand abgesagt. Das *Tageblatt* möchte den Lesern dennoch dieses wichtige Thema nicht vorenthalten und unterhielt sich mit Jeff Kaufmann von Bee Secure.



Getty Images/iStockphoto

Anhand von vorgetäuschten Webseiten können Hacker an private Informationen wie Passwörter oder Kontonummern gelangen

Phishing ist eine der häufigsten Arten der sogenannten Cyberkriminalität. Kriminelle nutzten die digitalen Medien, sei es in Form von E-Mails, Social-Media-Benachrichtigungen oder SMS, um an Passwörter, Kreditkartendaten oder jene vom Luxtrust-Konto zu kommen, sagt Jeff Kaufmann.

Die häufigste Form des Phishing beginnt meist mit einer elektronischen Nachricht, in der dem Adressaten vorgegaukelt wird, er müsse sich aus Sicherheitsgründen im Webbanking einloggen. Klickt man auf den Link, so gelangt man auf eine Webseite, die jene der Hausbank täuschend echt ähnelt. Wenn der Bankkunde seine Zugangsdaten mitsamt der seehsstelligen Token-Nummer eingibt, erscheint oftmals eine Fehlermeldung. Der Kunde glaubt, sich geirrt zu haben, und gibt die Daten ein zweites Mal ein, also auch eine neue Zahlenkombination aus dem Token. Je nachdem, wie raffiniert die Hacker sich anlegen, wird der Kunde nach einem zweiten scheinbar „erfolglosen" Einloggen auf die echte Loginseite seiner Bank weitergeleitet. Dieses Manöver diene der Täuschung, so Kaufmann. Über die vorgetäuschten Webseiten haben die Hacker alle Zugangscode mitsamt jenen des Tokens abgegriffen. Nun haben die Kriminellen ein leichtes Spiel. Mit dem ersten Token-Code gelangen sie ins Webbanking, mit dem zweiten Code können sie eine Überweisung „genehmigen". Das Opfer merkte dann einige Stunden später, dass von seinem Bankkonto eine hohe Summe abgebucht wurde, erklärt Kaufmann.

Dubiose Benachrichtigungen löschen

Vorbeugen kann man Phishing-Attacken eigentlich recht einfach. Solche dubiosen Benachrichtigungen kann man gleich löschen, denn keine Bank und auch kein Bezahldienst wie PayPal fordern ihre Kunden auf, sich im Kundenportal einzuloggen. Wenn man dennoch den Link öffnet, so erkennt man in der URL-Zeile, dass die übliche Adresse nach dem Muster „bank.lu" abweicht, entweder dureh dubiose Endungen oder durch vertauschte Buchstaben. Mann solle sicherheitshalber auf die mobile App von Luxtrust setzen. Denn eine Hackerseite sei nicht in der Lage, die Authentifizierungsmethode übers Mobiltelefon zu aktivieren, präzisiert der Experte.

Weitere Machenschaft sind vermeintliche E-Mails oder SMS eines Paketdienstes. In der Nachricht wird der „Kunde" aufgefordert, eine geringe Gebühr zum Begleichen des Portos oder einer Steuer zu begleichen, bevor das Paket zugestellt werden soll. Bei dieser Art von Attacke versuchen die Hacker an die Daten der Kreditkarten zu kommen. Dass viele Leute auf diese Nachrichten hereinfallen, liege angesichts des Versandhandels quasi auf der Hand, so Kaufmann. Auch hier gilt der gleiche Grundsatz wie bei der Bank: Kein Paketdienst fordert einen Kunden auf, eine Gebühr mittels eines Links zu bezahlen. Im Zweifelsfalle solle man sich telefonisch mit dem Paketdienst in Verbindung setzen, rät Kaufmann.

Ähnlich gestalten sich Nachrichten, die vorgaukeln, durch das Bezahlen eines geringen Beitrags könne man schnelles Geld im ETF-Handel oder mit Kryptowährungen machen. Beim Anlagebetrug ist das Geld vom eigenen Konto oder der Kreditkarte schnell weg, die Webseite nach ein paar Stunden nicht mehr erreichbar.

Genauso gefährlich wie oben genannte Methoden sind jene eines E-Mail-Anhangs. Entweder versuchen Hacker über ein auszufüllendes Formular an Daten zu kommen oder sie schleusen Schadsoftware ein, sogenannte Trojaner, die Daten am Rechner abgreifen. Noch dreister ist die sogenannte Ransomware, die die Daten auf dem heimischen PC verschlüsselt. Nur wenn man eine hohe Summe zahle, würden die Daten wieder entschlüsselt werden.

Ratschläge gegen Cyberkriminalität

Wurde man Opfer einer Phishing-Attacke, so solle man als Erstes sofort die Bank oder das Kreditkarteninstitut benachrichtigen und alle Karten und Kontos einfrieren. Ebenfalls sollte man die Helpline von Bee Secure anrufen, hier erhält das Opfer weitere Tipps zur Vorgehensweise.

Die Bank kann versuchen, die kriminelle Transaktion zu stornieren bzw. den Betrag zurückzubuchen. Dies gelinge aber nicht immer, unterstreicht Kaufmann.

Hacker zielen nicht nur auf das Bankkonto ab. Auch Amazon, PayPal, soziale Medien oder die Konten von Spielkonsolen sind im Visier der Kriminellen. Viele User hinterlegen bei solchen Dienstleistern ihre Bezahldaten, verknüpfen diese mit anderen Webseiten. So haben Hacker ein Leichtes, über diesen Weg an Daten zu kommen und beispielsweise Kosten für eine vermeintliche App oder geschaltete Werbung abzubuchen.

Die Ratschläge gegen derlei Cyberkriminalität dürften allgemein bekannt sein. Jeff Kaufmann wiederholt sie gerne:

- Passwörter niemals in einer Cloud speichern;
- Wenn man eine digitale Passwortverwaltung nutze, dann nur eine spezialisierte und sichere Software;
- Zwei-Faktor-Authentifizierung für alle wichtigen Konten;
- Passwörter nie doppelt verwenden;
- Verzicht auf Anmeldungen via „Google-Konto" oder „Facebook-Konto";
- Backups von eigenen Daten anlegen;
- keine Links in E-Mail-Nachrichten, SMS oder Messengerdiensten öffnen;
- immer daran denken: Keine Bank fordert den Kunden per E-Mail oder Telefon dazu auf, seine Daten preiszugeben;
- Zugang zum Webbanking über die App am Mobiltelefon oder die Webanwendung im Browser;
- Statt des Luxtrust-Token empfiehlt sich die Nutzung der mobilen App;
- Regelmäßig neue Passwörter definieren;
- unter https://haveibeenpwned.com/ kann man selbst prüfen, ob die eigene E-Mail-Adresse gestohlen wurde.

Die neue Informationskampagne erklärt unter bee-secure.lu/kyss anhand von Videos und Lifehacks, wie man sich vor dem Betrug schützt und Geräte sicher einrichtet.