Südtiroler
Wirtschaftszeitung
Wochenblatt für Wirtschaft und Politik
Data: 29/11/2019 | **Pagina:** 8
Categoria: Raiffeisen-Geldorganisation Print & Web

Vorweihnachtliches Hacking

WARNUNG – Wenn mit dem „Black Friday" und dem „Cyber Monday" die **Schnäppchenwochen** der Vorweihnachtszeit eingeläutet werden, beginnt auch für **Cyberkriminelle die Hochsaison.**

Bozen – Cyber-Kriminelle nützen das Weihnachtsgeschäft aus, um mit Phishing-Angriffen Adressen, Passwörter und Kontonummern von unachtsamen Nutzern zu stehlen. Denn in der Vorweihnachtszeit sind die Mailfächer voll mit Post über Sonderverkäufe und Angebote – und diese bieten die perfekte Tarnung für Phishing-Mails. Vor allem Online-Shopper sind gefährdet, auf diverse Tricks hereinzufallen: Gefälschte Webseiten, die infizierte Dateien enthalten – vorzugsweise PDF- oder Bild-Dateien – lauern überall. Auf bekannten Online-Shopping-Seiten schalten Cyberkriminelle darüber hinaus Werbeanzeigen, die dann zu entsprechend präparierten Webseiten führen. Das perfide an Malvertising ist, dass es auf Seiten eingeblendet wird, die oft besucht werden, und dass es täuschend echt nach echter Werbung aussieht.

Experten gehen davon aus, dass ein Prozent aller Werbebanner im Internet unter die Kategorie Malvertising fallen, also ahnungslose Nutzer auf eine Seite leiten, die beim Aufruf Schadcode auf das Gerät des Nutzers herunterlädt.

Wer über sein Smartphone oder Tablet einkauft und dafür Apps benutzt, ist ebenfalls nicht davor gefeit, ein Opfer von Betrügern zu werden, denn auch bösartige Apps werden programmiert. Diese Apps werden damit angepriesen, dass sie Sonderangebote enthalten oder auf günstige Restposten hinweisen. Cyberkriminelle wollen mit diesen Tricks an Kreditkarteninformationen kommen oder aber gleich das Gerät, mit dem das Opfer online einkauft, in Beschlag nehmen.

Wie man sich schützen kann

Nicht nur Private sollten sich dieser Gefahren bewusst sein. Auch Unternehmen sollten ihre Mitarbeiter laufend in Sachen Onlinekriminalität bzw. Cyber-Sicherheit sensibilisieren, um möglichen Gefahren aus dem Weg zu gehen und um damit Schaden vorzubeugen.

„Wenn Internetbenutzer und Unternehmen präventive IT-Sicherheitslösungen einsetzen und einige Sicherheitsregeln beachten, können schon viele Phishing- und andere Attacken verhindert werden", betont Martin Galler, Privacy-&-Data-Security-Experte des Südtiroler IT-Unternehmens Konverto. In diesem Sinne empfiehlt Galler, jedes Gerät mehrfach zu schützen. Zu den Maßnahmen, die ergriffen werden sollten, gehören:

- fortschrittliche Sicherheitslösung, die präventiv vor Gefahren schützt,
- eine moderne und stets aktualisierte Antiviren-Software,
- eine Lösung, die vor infizierten Webseiten warnt und das Herunterladen von Schadcode verhindert sowie durch Social Engineering initiierte Attacken abwehrt,
- ein Werbeblocker,
- Betriebssystem, alle Browser und Plug-ins sollten immer auf dem aktuellsten Stand sein,
- Und „last but not least": niemals auf Links oder Dateianhänge in E-Mails von unbekannten Absendern klicken!