Angebotsdschungel: Cyber Week steht vor der Tür

Bereit für den ultimativen Shopping-Wahn? Wenn, dann aber richtig, denn der „Black Friday" und der „Cyber Monday" sind für Cyberkriminelle ein Paradies. Bei Sonderverkäufen und anziehenden Angeboten greifen viele online zu und werden dabei Opfer von Cyberkriminellen. Wir geben Ihnen einige Tipps zum sicheren Shopping im Netz.

Alle Jahre wieder nutzen Cyberkriminelle solche Anlässe für verschiedenste Angriffe. Phishing-Angriffe durch gefakten Mails zu Sonderangeboten zählen dabei zu den Häufigsten. Mithilfe gefälschter E-Mails, die in Layout und Texten oft kaum von richtigen Mailings zu unterscheiden sind, gelangt man auf falsche, präparierte Webseiten. Diese Phishing-Kampagnen verbreiten vermehrt Arten von Malware, einschließlich Ransomware. Laut einer Webroot Studie generieren Hacker mitunter 46.000 Phishing-Webseiten pro Tag.

Auch beim Online-Shopping kann man schnell auf diverse Tricks hereinfallen. Gefälschte Webseiten tauchen auf, die in PDF- oder Bild-Dokumenten infizierte Dateien enthalten. Auch Werbebanner, die dann zu entsprechend manipulierten Webseiten führen, wirken auf den ersten Blick verlockend. Experten gehen davon aus, dass 1 Prozent aller Werbebanner im Internet unter die Kategorie Malvertising fallen und so ahnungslose Nutzer auf eine Seite leiten, die beim Aufruf Schadcode auf das Gerät des Nutzers herunterlädt. In einigen Fällen wird dieses Malvertising genutzt und sucht nach Schwachstellen, um nach der Infizierung eine Ransomware nachzuladen. Darüber hinaus können auf diesem Weg Viren, Spyware und Trojaner auf das Gerät geladen und dann für weitere Attacken verwendet werden.

Und auch Apps sind nicht immer sicher, denn auch bösartige Apps werden programmiert und in App-Stores unter einschlägigen Suchbegriffen beworben. Wie auf Online-Seiten kann so Ransomware auf das Tablet oder Smartphone übertragen oder gleich das gesamte Gerät, mit dem das Opfer online einkauft, in Beschlag genommen werden.

Das Ziel bleibt immer eines: Kriminelle wollen an möglichst viele Informationen des Users kommen, vor allem an Andressen, Passwörter oder Kontonummern.

WIE SIE SICH SCHÜTZEN KÖNNEN

Um beruhigt online zu shoppen sollte jedes Gerät mehrfach geschützt werden. Dazu sollte

- eine fortschrittliche Sicherheitslösung, die präventiv vor Gefahren schützt implementiert werden
- eine moderne und stets aktualisierte Antivirus-Software heruntergeladen werden
- eine Lösung, die vor infizierten Webseiten warnt und das Herunterladen von Schadcode verhindert auf dem Gerät sein
- das Gerät mit einer Lösung, die durch Social Engineering initiierte Attacken abwehrt ausgestattet sein
- ein Werbeblocker aktiviert sein.
- Des Weiteren sollten Sie sicherstellen, dass Ihr Betriebssystem, alle Browser und Plug-Ins immer auf dem aktuellsten Stand sind
- Und: klicken Sie niemals auf Links oder Dateianhänge in E-Mails von unbekannten Absendern.
- Auch Unternehmen sollten ihre Mitarbeiter laufend für die Sicherheit sensibilisieren, um möglichen Gefahren aus dem Weg zu gehen und um damit Schaden vorzubeugen.

Wenn Internetbenutzer und Unternehmen präventive IT-Sicherheitslösungen einsetzen und die genannten Sicherheitsregeln beachten, können bereits viele Phishing- und andere Attacken verhindert werden. Einem unbeschwerten Online-Shopping-Genuss steht dann nichts mehr im Weg.

Una giungla di offerte: la Cyber Week è dietro l'angolo

Pronti per la mania dello shopping estremo? Se è il caso, allora fatelo bene, perché il " Black Friday" e il " Cyber Monday" sono un paradiso per i cybercriminali. Durante le vendite speciali e le offerte interessanti, molti comprano online e diventano vittime dei cybercriminali. Vi diamo alcuni consigli per uno shopping sicuro in rete.

Ogni anno i cybercriminali utilizzano queste occasioni per diversi attacchi. Gli attacchi di phishing tramite mail false su offerte speciali sono tra i più comuni. Con l'aiuto di e-mail false, spesso difficilmente distinguibili dai veri mailing nel layout e nel testo, si può arrivare a siti web falsi e preparati. Queste campagne di phishing diffondono sempre più tipi di malware, compreso il ransomware. Secondo uno studio Webroot, gli hacker generano fino a 46.000 siti web di phishing al giorno.

Lo shopping online è un'altra area in cui ci si può facilmente imbattere in diversi trucchi. Appaiono siti web falsificati che contengono file infetti sotto forma di documenti PDF o immagini. Anche i banner pubblicitari, che poi conducono a siti web manipolati, sembrano a prima vista allettanti. Gli esperti ipotizzano che l'1% di tutti i banner pubblicitari su Internet rientri nella categoria del malvertising e quindi conducano gli utenti ignari a una pagina che, quando viene visitata, scarica codici dannosi sul dispositivo dell'utente. In alcuni casi, questa malware viene utilizzata per cercare i punti deboli di un dispositivo e per scaricare poi il ransomware. Virus, spyware e trojan possono essere scaricati sul dispositivo in questo modo e quindi utilizzati per ulteriori attacchi.

Inoltre vengono programmate e pubblicizzate negli app store con termini di ricerca pertinenti molte app dannose. Come sui siti online, il ransomware può essere trasferito sul tablet o sullo smartphone o può, in casi estremi, controllare l'intero dispositivo con cui la vittima effettua acquisti online.

L'obiettivo rimane sempre lo stesso: i criminali vogliono ottenere quante più informazioni possibili sull'utente, in particolare indirizzi, password o numeri di conto.

COME PROTEGGERSI

Per fare acquisti online in tutta tranquillità, ogni dispositivo dovrebbe essere protetto più volte. Pertanto si consiglia di

- implementare una soluzione di sicurezza avanzata che fornisce una protezione preventiva contro i pericoli
- scaricare un software antivirus moderno e costantemente aggiornato
- avvalersi di una soluzione che mette in guardia dalle pagine web infette e impedisce il download di codici dannosi sul dispositivo-
- Il dispositivo deve essere dotato di una soluzione che respinga gli attacchi avviati dal social engineering e
- deve essere attivato un blocco per la pubblicità.
- Inoltre, è necessario assicurarsi che il sistema operativo, tutti i browser e i plug-in siano sempre aggiornati.
- E: non cliccate mai su link o allegati di file nelle e-mail di mittenti sconosciuti.
- Le aziende dovrebbero inoltre sensibilizzare costantemente i propri dipendenti alla sicurezza per evitare possibili pericoli e quindi prevenire danni.

Se gli utenti di Internet e le aziende utilizzano soluzioni preventive di sicurezza e rispettano le regole di sicurezza sopra menzionate, è già possibile prevenire molti attacchi di phishing e altri attacchi. A questo punto nulla ostacola il piacere dello shopping online senza pensieri.