SWISS
BUSINESS
PROTECTION

www.swissbp.ch
info@swissbp.ch
+4141 511 42 33

Cyber-Attacken am Black Friday und Cyber Monday

Für Black Friday und Cyber Monday wird mit Rabatten von bis zu 80 Prozent geworben. Schon lange vorher locken die Unternehmen mit riesigen Rabatten. Besonders in der Zeit der Corona-Pandemie versuchen viele Menschen, die vollen Innenstädte zu meiden und online einzukaufen.

Aber aufgepasst: Nicht jedes Angebot am Black Friday und Cyber Monday ist ein Schnäppchen. Auch Cyber-Kriminelle nutzen den Aktionstag für Ihre Zwecke. Die Angriffsmethoden reichen von einfachen Phishing-Attacken in Form von gefälschten Geschenkgutscheinen bis hin zu Malware und Kreditkartendatendiebstahl.

Phishing E-Mails: Cyberkriminelle wollen möglichst viele Internet-Benutzer erreichen. Daher stehen vor allem grosse Online Shops im Fokus, welche für folgende Angriffsmethoden ausgenutzt werden:

Gefälschte Geschenkgutscheine: Eine Möglichkeit um auf ein Kundenkonto zuzugreifen, führt über den Einsatz von gefälschten Geschenkgutscheinen. Der Online Benutzer erhält dabei per E-Mail einen Geschenkgutschein. Sobald er auf den Link des Gutscheins klickt, wird er auf eine Phishing-Seite weitergeleitet, welche die Anmeldeinformationen abgreift.

Gefälschte Logins: Eine der häufigsten Methoden zum Angriff auf ein Kundenkonto führt über ein vorgetäuschtes E-Mail mit einem Login-Link vom Online Shop-Kundendienst. Diese E-Mails wirken täuschend echt, insbesondere, wenn Sie soeben dort eingekauft haben. Der Link leitet auch hier auf eine Phishing-Seite weiter, welche Ihre Kundeninformationen abgreift.

Trojaner: Die gefährlichste Methode ist die Verwendung von betrügerischen E-Mails, welche im Anhang eine Bestellung oder Rechnung aufweisen. Dahinter verbirgt sich meist ein Trojaner wie beispielsweise Emotet. Sobald das Dokument im Anhang geöffnet und das Makro aktiviert wird, installiert sich ein Trojaner. Cyberkriminelle können dann im Hintergrund eines infizierten Computers Geld wegtransferieren, sobald eine E-Banking-Sitzung hergestellt wird.

Damit die obigen Täuschungen möglichst echt wirken, registrieren Cyberkriminelle bereits im Vorfeld gefälschte Web-Domains und lösen gültige Zertifikate für die Phishing-Seiten, die auf kleinen, subtilen Abweichungen der echten URL-Website basieren.

Tipp 1 – Phishing-E-Mail:

Öffnen Sie keine Anhänge mit Gutscheinen oder Sonderangeboten. Bei einem gültigen Angebot ist es nicht nötig, auf einen Link oder Anhang zu klicken. Klicken Sie nie auf Links in E-Mails. Es gibt Tausende von gefälschten Websites, die fast identisch zur echten Seite aussehen. Wenn Sie auf einer Website einkaufen möchten, die Sie häufig besuchen, geben Sie die URL manuell in Ihrem Browser ein oder speichern Sie die Webseite bei Ihren Favoriten. Besuchen Sie nur vertraute Websites. Falls Sie auch andere Seiten besuchen, empfiehlt sich die Kontrolle, ob die URL der Website mit „https://“ beginnt. Das „s“ zeigt an, dass die Webverbindung durch das SSL-Zertifikat verschlüsselt und geschützt wurde. Nutzen Sie nicht das gleiche Passwort für verschiedene Shops, sondern individuelle Passwörter.

Bleiben sie vorsichtig beim Bestellvorgang und achten sie auf Unregelmässigkeiten (lange Bestelldauer, andere Farbe der Bestellseite, anderes Logo, etc.) beim Bestellvorgang. Im Notfall sofort Internetverbindung kappen und Vorgang abbrechen.

Tipp 2 – Soziale Medien:

Cyberkriminelle nutzen am Black Friday und Cyber Monday gerne die sozialen Medien für ihre Angriffe. Beliebte Artikel werden dann zu Spotpreisen angeboten oder mit gefälschten Geschenkgutscheinen Schnäppchenjäger angelockt. Auch hier wird beim Klick auf den Link auf eine Phishing-Seite weitergeleitet. Die Cyberkriminellen werden versuchen, Dich zu einer Kartenzahlung oder Überweisung zu bewegen, um Deine persönlichen Daten abzugreifen.

Sei in sozialen Netzwerken besonders misstrauisch gegenüber Artikeln, die weit unter dem typischen Marktpreis liegen, selbst am Black Friday und Cyber Monday.

Tipp 3 – SMS Phishing:

Online Shopper erwarten Bestell- und Lieferbenachrichtigungen. Dies nutzen Cyberkriminelle aus und senden eine gefälschte SMS-Nachricht mit einem Link. Diese Links leiten dann wiederum auf eine Phishing-Seite, auf der bei Eingabe die Nutzerdaten und Passwörter abgegriffen werden.

Beim SMS Phishing ist es für die Online Shopper besonders schwierig zu erkennen, ob die empfangene Nachricht authentisch ist, da im Vergleich zu einer E-Mail nur wenige Informationen vorhanden sind. Es gibt keinen Header, mit welchem die Echtheit des Absenders überprüft werden kann oder eine kurze URL, die merkwürdig oder verdächtig vorkommen könnte.

Reagieren Sie niemals auf SMS-Nachrichten, welche Links enthalten. Klicken Sie auf keinen Fall auf die Links. Installieren Sie nur mobile Anwendungen über den offiziellen Store und niemals solche, die Ihnen über einen SMS-Link zugesandt werden.

Tipp 4 – Web-Skimming:

Web-Skimming, ist ein Cyberangriff, bei dem der Angreifer einen bösartigen Code in den Online Shop einschleust. Diese Malware zielt auf Online Shopper ab, wenn diese versuchen, eine Bestellung im Warenkorb abzuschliessen. Sobald die Zahlungsinformationen in das Online-Formular eingegeben werden, erfasst die Malware diese Daten (einschliesslich der Bankkartendaten) und überträgt sie direkt an die Cyberkriminellen. Die Folgen von solchen Angriffen können katastrophal sein. Neben dem finanziellen Schaden und der Rufschädigung, welches das Unternehmen hat, verlieren die Kunden auch das Vertrauen zum betroffenen Online Shop und kehren oft nie mehr zurück.

Zahlen Sie beim Online Shopping wenn immer möglich mit Kreditkarte und nicht mit Ihrer Debitkarte. Eine Rückerstattung aufgrund von Web-Skimming ist bei der Debitkarte nicht immer möglich. Kreditkartenherausgeber bieten dagegen einen grösseren Schutz. Aktivieren Sie den 3D-Schutz des Karten-Herausgebers so dass Sie Ihren Kauf mit der App vom Kartenherausgeber bestätigen müssen. Setzen Sie für den Kauf im Internet eine separate Kreditkarte mit einer tieferen Limite ein und zahlen Sie die Rechnungen nicht mit dem Lastschriftenverfahren. Prüfen Sie die Rechnung Ihres Kreditkartenherausgebers sorgfältig und zahlen Sie nur die korrekten Einkäufe per Rechnung. Falls Sie etwas Verdächtiges entdecken, lassen Sie die Ihre Kreditkarte sofort sperren.

www.swissbp.ch

Nehmen Sie mit uns Kontakt auf und vereinbaren Sie einen Termin. **Tel: +41 41 511 42 33** **E-Mail: risk@swissbp.ch**