DIE GEFAHR AUS DEM NETZ – TEIL II. VIELFÄLTIGE BEDROHUNGEN FÜR ONLINE-SHOPS

Webshops im Visier

In der Coverstory der E&W Dezemberausgabe 2021 widmeten wir uns dem Thema Cyberkriminalität. Seit Ausbruch der Corona-Pandemie sind Unternehmen – große wie kleine – vermehrt Ziele von Cyber-Angriffen. Die größten Zuwächse unter den vielfältigen Erscheinungsformen des Cybercrime verzeichnet der „Internet- und E-Commerce-Betrug", von dem sowohl Online-Shopper als auch -Betreiber betroffen sind. In dieser Ausgabe beleuchtet IT-Experte Andreas Schuster im Gespräch mit E&W die häufigsten Gefahren, denen Webshop-Betreiber ausgesetzt sind.

TEXT: Stefanie Bruckbauer | **FOTOS:** Pixabay.com, Andreas Schuster | **INFO:** www.elektro.at

Der Boom, den der Onlinehandel in den letzten Jahren erfahren hat und der durch Corona weiter befeuert wurde, hat dazu geführt, dass betrügerische Aktivitäten im Netz merklich angestiegen sind. So wurden laut einer CRIF Studie aus 2021 bereits neun von zehn Online- und Versandhändler in Deutschland, Österreich und der Schweiz Opfer von Betrug bzw. Betrugsversuchen – „ein Rekordwert im DACH-Raum", wie CRIF sagt.


© Pixabay.com

41 % der Befragten bemerkten im Vorjahr einen Anstieg betrügerischer Aktivitäten. Zu den häufigsten Betrugsformen zählen mit 76 % die Angabe falscher Namens- und / oder Adressdaten, die Angabe einer anderen Identität (75 %) sowie der Fall, dass Kunden eine Bestellung tätigen, obwohl sie wissen, die Rechnung nicht bezahlen zu können (71 %).

Viele Onlinehändler sind sich zwar des Problems von Betrug in ihrem Business bewusst, nehmen das Thema jedoch nicht aktiv in die Hand und kennen die einzelnen Gefahrenquellen – und vor allem die Gegenmaßnahmen – nicht gut genug.

DIE HÄUFIGSTEN GEFAHREN

Andreas Schuster hat sein Hobby, die IT, vor 20 Jahren zum Beruf gemacht und arbeitet seit vielen Jahren in der Crypto-Branche. Aktuell ist er als Berater für Informationssicherheit bei SEC4YOU tätig. Schuster hat im Gespräch mit E&W das Thema „E-Commerce Sicherheit für Online-Shops" beleuchtet und er sagt: „Ladengeschäfte werden heutzutage wie selbstverständlich geschützt. Man setzt Kameras oder sogar Wachpersonal ein, wertvolle Waren werden mit RFID Tags gesichert und die Kassa bzw. der Bargeldbestand werden physisch geschützt. Vergleichbare Schutzmaßnahmen müssen allerdings auch implementiert werden, wenn man einen Online-Shop betreibt." Die E-Commerce-Bedrohungen durch Cyberangriffe seien vielfältig, sagt der IT-Experte. Zu den häufigsten Gefahren, die das Online-Geschäft bedrohen, zählen:

> „Ladengeschäfte werden heutzutage wie selbstverständlich geschützt. (...) Vergleichbare Schutzmaßnahmen müssten allerdings auch implementiert werden, wenn man einen Online-Shop betreibt."
>
> Andreas Schuster

Finanzbetrug: Geschickte Hacker führen in den Online-Systemen unbefugte Warentransaktionen oder finanzielle Transaktionen aus und verwischen dann ihre Spuren. Diese Gefahr besteht seit der Einführung des Online-Handels und verursacht einen erheblichen Verlustanteil. Oft erfolgt dieser Betrug in kleinen oder sogar Micro-Transaktionen und bleibt vom Unternehmen lange unerkannt.

Oft erfolgt der Finanzbetrug auch über Warenrücksendungen und Garantieansprüche, wo Betrüger gefälschte Produkte, Diebesgut oder defekte Fremdware begutschriften lassen. Dieser Finanzbetrug entsteht auch beim gesetzlich verankerten Widerrufsrecht, wenn Kunden die Ware in der Zeitspanne intensiv abnutzen.

Spam: Auch wenn wir in der Vergangenheit gelernt haben mit Spam umzugehen, ist Spam eine hohe Gefahr für das Online-Geschäft: „Spam ist längst in den Kommentaren der Blog-Artikel und Kontakt-Formulare angekommen und dient Spammern als Einladung, infektiöse Links zu senden, die dem Unternehmen und auch seinen Kunden schaden können. Oft werden solche Nachrichten über Soziale Medien gesendet und der Angreifer wartet darauf, dass jemand in Unternehmen draufklickt", erläutert Schuster und er ergänzt: „Sollten Sie über Ihre Online-Präsenz infektiöse Links weiterverbreiten, sind Schadenersatzforderungen Dritter nicht ausgeschlossen."

Phishing: Je größer und erfolgreicher ein Online-Shop wird, desto eher steigt die Gefahr durch Phishing. Hierbei verstecken sich Angreifer hinter rechtmäßigen Unternehmen und senden E-Mail oder SMS Nachrichten an die Kunden. Dabei werden die Kunden – oft mit Zeitdruck und unter Androhung von Konsequenzen – aufgefordert, ihre vertraulichen Anmeldeinformationen sowie weitere Informationen einzugeben. Die hierzu gefälschten Webseiten sind zum Teil perfekt aufbereitet und vermitteln einen authentischen Eindruck.

Typischerweise sind die Phishing Nachrichten an die Kunden oder auch an die Mitarbeiter des Shop-Betreibers gerichtet und enthalten eine gefälschte „Sie müssen diese Aktion ausführen!"-Nachricht. Schuster sagt: „Je mehr diese Aktion der täglichen Arbeitsroutine des Zielkreises entspricht, desto eher wird der Phishing-Angriff Erfolg haben. Bedauerlicherweise lässt sich der Erfolg solcher Angriffe einfach in Prozent messen: 3 % Erfolg, wenn von 1.000 angeschriebenen E-Mailadressen 30 ihre Zugangsdaten eingeben."

Cross-Site-Scripting – XSS: Was wie eine Kleidergröße klingt, ist laut Schuster seit Jahren eine der größten Gefahren für Internetanwendungen. Bei dieser Angriffsmethode gelingt es einem Angreifer durch eine bestehende Sicherheitslücke einen Schadcode in eine vermeintlich vertrauenswürdige Umgebung einzubetten. Dadurch lassen sich Internetseiten verändern und aktive Sessions von Browsern übernehmen. Zudem können vertrauliche Daten wie Passwörter entwendet werden.

Wie der IT-Experte sagt, erreicht man einen guten Schutz gegen Cross-Site-Scripting dreistufig: „Erstens, wenn Benutzer empfangene Links kritisch prüfen (also bei Bedenken nicht anklicken!), zweitens in der technischen Absicherung der Online-Dienste mit Firewalls und Datei / Upload-Prüfung sowie drittens mit automatisierten Updates aller Online-Dienste inklusive der Online-Shop Anwendung."

SQL Injektion: Diese Angriffsmethode richtet sich gegen die Datenbank eines Online-Shops. Mit Steuerzeichen oder über versteckte Schnittstellen werden direkte Veränderungen in dieser Datenbank vorgenommen. Schuster erklärt: „Vorstellen kann man sich den Angriff über die Nutzung eines Formulars, in dem ein Kunde seine Kundendaten ändert. Das Formular wird vom Cyberangreifer so verändert, dass auch beliebige andere Daten der SQL Datenbank (z.B. Zugangsdaten weiterer Kunden oder gespeicherte Zahlungsdaten) unberechtigt verändert oder ausgelesen werden."

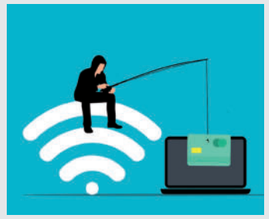
Brute-Force-Angriff: Ohne besondere Schutzmaßnahme können Angreifer mit einem Brute-Force-Angriff versuchen, die administrative Oberfläche des Online-Shops anzugreifen, indem verschiedene Passwörter ausprobiert werden. Wie Schuster erklärt, nutzen Angreifer hier Listen von häufigen Passwörtern – „das Passwortknacken wurde auf hunderte oder tausende Versuche pro Sekunde automatisiert." Schützen könne man sich durch die Nutzung eines möglichst starken, komplexen Passwortes sowie den Einsatz einer Zwei-Faktoren-Authentisierung.

Ing. Andreas Schuster ist (neben seiner Tätigkeit als Berater für Informationssicherheit bei SEC4YOU) Director Sicherheit Sensibler Systeme bei der CMG (Computer Measurement Group), einem weltweit offenen Non Profit Forum für Experten und Technologiebegeisterte aus der Kommunikations- und Informationstechnologiebranche, das den Wissenstransfer fördert. Die CMG umfasst elf Themenpanels. Eines davon beschäftigt sich mit „E-Commerce-Fraud", also Betrug im E-Commerce.

Angriff über ein Trojanisches Pferd bzw. gehacktes Endgerät: Wenn ein Angreifer es schafft, dass ein Online-Shop Administrator oder ein Kunde eine Schadsoftware herunterlädt und diese ausführt, oder es irgendwie anders schafft eines der benutzten Endgeräte zu hacken, dann hat der Cyberangreifer volle Kontrolle über alle Aktionen des Benutzers. Der IT-Experte erklärt: „Mit Leichtigkeit werden dann die Zugangsdaten aus dem Browser-Passwortspeicher oder bei der Tastatureingabe gestohlen und es können beliebige Daten am Endgerät und im Netzwerk manipuliert werden. Gerne überweisen Angreifer sich dann große Geldsummen auf Auslandskonten oder sie verschlüsseln Daten und erpressen das Unternehmen."

In der kommenden E&W erklärt Andreas Schuster eine Reihe von Maßnahmen, die eine nachhaltige Verbesserung der Sicherheit eines Online-Shops bringen sollen.

PHISING



„Phishing" zählt zu den häufigsten Cyberangriffsarten, wie eine Umfrage von Statista unter österreichischen Unternehmen ergab. Beim „Phishing" geht es darum, sich Zugangsdaten von Internetusern illegal zu „angeln" und diese zu missbrauchen.

Vorgehensweise: Der Adressat einer Mail oder SMS soll auf einen in der Nachricht enthaltenen Link klicken, der ihn auf eine z.B. als Online Shop oder Bankinstitut getarnte betrügerische Webseite leitet. Dort soll er dann seine Login-Daten eingeben, Transaktionen bestätigen oder Kreditkarteninformationen verraten. Phishing-Mails sind dabei sehr viel professioneller geworden.

Die meisten Phishing-Attacken richten sich gegen die Kunden von Banken und Zahlungsdienstleistern. Auf Platz 3 der am meisten betroffenen Branchen finden sich Online-Shops, wobei nicht nur die Kunden im Visier der Betrüger sind, sondern zunehmend auch die Webshop-Betreiber.

Um an Login-Daten zu gelangen drohen „Phisher" z.B. Marketplace-Händlern mit der Sperrung ihrer Shops, bieten Sonderkonditionen für neue Shop-Features und verbilligte Versandkontingente beim Logistikpartner an oder locken mit kostenfreien Verkaufsseminaren. Haben die Angreifer den Shop-Mitarbeiter so auf eine gefälschte Seite gelockt und sich die Zugangsdaten zum Shop verschafft, können sie Finanzdaten der Shop-Kunden ergaunern oder die Kundendatenbank für weitere Angriffe plündern. Im schlimmsten Fall übernehmen sie den ganzen Shop, indem sie die Zugangsdaten ändern und so den Shop-Betreiber aus seinem eigenen Shop aussperren.