DIE GEFAHR AUS DEM NETZ – TEIL III. SCHUTZMASSNAHMEN FÜR ONLINE-SHOPS

Hack me if you can!

In den letzten zwei E&W-Ausgaben widmeten wir uns dem Thema Cyberkriminalität. Seit Ausbruch der Corona-Pandemie sind immer mehr Unternehmen Ziele von Cyber-Angriffen. Vor allem der „Internet- und E-Commerce-Betrug" boomt. In dieser Ausgabe beleuchtet IT-Experte Andreas Schuster im Gespräch mit E&W eine Reihe von Maßnahmen, die Webshop-Betreiber ergreifen können, um ihren Onlineshop zu schützen.

TEXT: Stefanie Bruckbauer | **FOTOS:** A. Schuster | **INFO:** www.elektro.at

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. In der letzten Ausgabe ging es um die vielfältigen möglichen Bedrohungen für Webshops. Nun spricht er darüber, mit welchen Maßnahmen man einen Onlineshop gegen Angriffe schützen kann.

MASSNAHMEN

Schuster sagt: „Grundsätzlich haben sichere Online-Shops Gemeinsamkeiten: Sie verlassen sich nicht auf externe Schutzmethoden oder Security-Plugins und sie sparen nicht an einer robusten Hardwareausstattung." Der IT-Experte führt eine Reihe von Maßnahmen an, die eine nachhaltige Verbesserung der Sicherheit eines Online-Shops bringen können.

Eine bewährte eCommerce Plattform

Bei der Auswahl des Shop-Systems sollte man sich nicht von Marketingversprechen leiten lassen, sondern eine bewährte Plattform wählen, die regelmäßig aktualisiert wird und erstklassige Sicherheit bietet. Bekannte und bewährte Plattformen sind laut Schuster z.B. Shopify, Magento Commerce, 3DCart, WooCommerce, Prestashop. Quelloffene Lösungen werden oft von einer großen Community gepflegt und die Sicherheit wird dadurch regelmäßig geprüft.

> „Sofern Kreditkartendaten in der Datenbank eines Online-Shops gespeichert werden, ist dies eine große Verantwortung, die der Shop-Betreiber trägt. Für einen Hacker sind diese Kreditkartendaten nämlich ein gefundenes Fressen.
>
> Andreas Schuster

„Schützen Sie Ihren Server und Ihre Admin Zugänge"

Schuster erläutert: „Fast alle E-Commerce-Lösungen sind mit Benutzernamen und Passwort geschützt. Im Zuge der Installation wird ein Standard-Passwort angelegt, dass alle Hacker nur zu gut kennen. Wenn Sie diese Zugangsdaten nicht unverzüglich ändern, riskieren Sie einen Angriff, der nicht nur Zugriff auf Ihre wertvollen Daten hat, sondern auch ein Backdoor installieren kann, um jederzeit wieder in Ihr System einzusteigen."

Neben dem Admin-Zugang des Online-Shops seien auch die administrativen Zugänge der Hosting-Provider bestmöglich zu schützen. „Über den Admin-Zugang des Hosting-Providers (z.B. 1&1, All-Inkl.com, DomainFactory, Hetzner Online, World4You, Domaintechnik, easyname, u.v.a) haben Angreifer ebenfalls vollen Zugriff auf alle Programmdateien und Online-Shop Daten und können beliebige Transaktionen erstellen bzw. manipulieren", so der IT-Experte, der rät:

„Nutzen Sie starke Passwörter und optimal auch eine Zwei-Faktoren Authentisierung für diese kritischen Zugänge. Auch lassen sich diese Zugriffe auf gewisse IP-Adressbereiche einschränken. Optimieren können Sie diesen Schutz noch mit einer automatisierten E-Mail Benachrichtigung, sobald ein Zugriff von einer unbekannten IP-Adresse erfolgt."

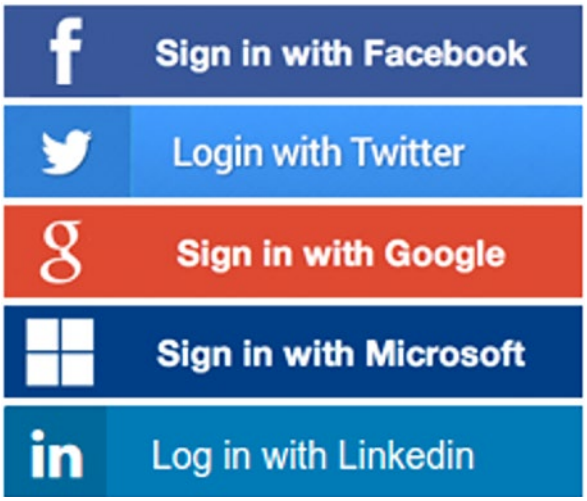
„Wechseln Sie zu HTTPS und einem gültigen SSL-Zertifikat"

„Das veraltete HTTP Protokoll hat in Online-Shops, aber auch in dahinterliegenden APIs, nichts mehr verloren", so Schuster. „Das Protokoll bietet keinen ausreichenden Schutz der übertragenen Daten und Zugangsdaten. Dies gilt übrigens auch für das veraltete FTP Protokoll, das leider immer noch häufig für den Datenaustausch verwendet wird. Obwohl Google Webseiten mit HTTP Zugriff schlecht bewertet und auch moderne Browser Warnmeldungen bei HTTP Inhalten anzeigen, gibt es immer noch viele Webseiten, die dieses unsichere Protokoll verwenden."

Geschützt werde das moderne HTTPS Protokoll durch ein gültiges SSL-Zertifikat, das in der Regel um wenig Geld über den Hosting-Provider gekauft werden kann. Schuster ergänzt: „Kleinere Shops nutzen auch gerne die kostenfreien SSL-Zertifikate des Anbieters Let's Encrypt. Prüfen können Sie Ihre Sicherheit kostenfrei mit dem SSL Labs Tool erreichbar unter https://www.ssllabs.com/."

Starke Passwörter und Social Login

Speziell die Kunden sind laut Schuster nachlässig mit ihrer Sicherheit und wählen aus Bequemlichkeit schwache Passwörter für die genutzten Online-Shops.



Ein Social Login ist eine gute Anmeldemethode für Kunden in Onlineshops. Man benötigt mit dieser Methode keine zusätzlichen Zugangsdaten, sondern kann sich bequem mit dem eigenen Facebook-, Google-, Instagram-, etc. Account anmelden.

„Auch fallen diese Zugangsdaten den Hackern durch Phishing-Angriffe in die Hände“, sagt der IT-Experte und er rät: „Stellen Sie daher die Passwortkomplexität in Ihrem Online-Shop auf hoch und erzwingen Sie so möglichst starke Zugangsdaten. Weisen Sie auch Ihre Kunden auf die Gefahren hin, sollten ihre Zugangsdaten missbraucht werden.“

Bevor man aber dazu übergeht, eine Zwei-Faktoren Authentisierung für seinen Online-Shop einzuführen, sollte man überlegen, ob ein Social Login nicht die bessere Anmeldemethode für die Kunden wäre. „Kunden benötigen mit dieser Methode keine zusätzlichen Zugangsdaten, sondern können sich bequem mit ihrem Facebook, Google, Instagram, etc. Account anmelden“, erklärt Schuster.

Ein elementarer Bestandteil eines Online-Shops ist der Zahlungsprozess. Sofern Kreditkartendaten in der Datenbank des Shops gespeichert werden, ist dies eine große Verantwortung, die der Betreiber trägt, sagt Schuster. „Für einen Hacker sind diese Kreditkartendaten ein gefundenes Fressen, gleichzeitig wird bei einem Diebstahl dieser Daten die Reputation Ihres Unternehmens nachhaltig geschädigt und nach Meldung an die Datenschutzbehörde drohen hohe Strafen sowie Schadenersatzforderungen.“

Um diese Gefahren zu vermeiden, sollten Kreditkartendaten niemals in der Datenbank gespeichert werden – „sondern nutzen Sie im Check-out Prozess einen bewährten Zahlungsdienstanbieter. Über den externen Dienstleister können Ihre Kunden eine Vielzahl an unterschiedlichen Zahlungsarten von Apple Pay, Pay Pal, Banküberweisung, Kreditkarten u.v.m. nutzen. Ihr Unternehmen erhält das Geld abzüglich einer definierten Transaktionsgebühr, aber die sichere Speicherung dieser hochvertraulichen Zahlungsdaten entfällt“, erklärt Andreas Schuster.

Firewalls und Firewall-Plugins

Sehr effizient ist laut Schuster die Nutzung von vorgelagerten Firewalls, gerne auch als Software-Firewall, und speziellen Firewall-Plugins, um eingehende Verbindungen zu kontrollieren. „Sofern Ihr Online-Shop nur Waren für den deutschsprachigen Raum anbietet, können Sie mit passenden Regeln Angreifer aus dem Ausland abweisen, aber gleichzeitig relevante Suchdienste zur Seitenindizierung erlauben. Durch diese Schutzmaßnahme wird Ihr Online-Shop auch größtenteils vor SQL Injektion und Cross-Site-Scripting (XSS) geschützt.“

E-Commerce Security Plug-in

Für viele E-Commerce Lösungen gibt es spezielle Security Plug-ins, oft in einer kostenfreien jedoch eingeschränkten Version und in einer Bezahlversion. Diese Plug-ins bieten u.a. Schutz vor bösartigen Suchdiensten, SQL Injektion, XSS und einer Vielzahl an anderen Angriffsmustern. Schuster empfiehlt: „Sehr bekannt sind Astra und WordFence, die wie andere Plug-ins auch neben dem Internetzugriff die E-Commerce Softwareversion, die Plug-ins, die Betriebssystemlücken und diverse Sicherheitskonfigurationen überwachen und aktiv Alarm schlagen. Empfehlenswert ist der Kinsta-Blog von Brian Jackson mit einer Kurzvorstellung von 17 WordPress Security Plugins: https://kinsta.com/de/blog/wordpress-security-plugins/ .“

Überwachung von auffälligen Aktivitäten

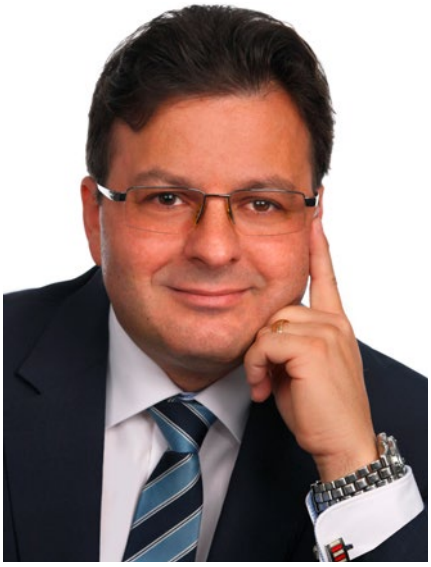
Leider oft unbemerkt gibt es täglich verdächtige Aktivitäten innerhalb des Online-Shops, die zu prüfen sind. Werden diese Aktivitäten frühzeitig erkannt, können Betrugstransaktionen verhindert werden. Dies hilft eine Menge an Problemen zu vermeiden und rettet den Verlust durch Betrug. Für diese Überwachung gibt es spezielle Software, die in Echtzeit die Aktivitäten analysiert und über fragwürdige Transaktionen benachrichtigt.

Schuster führt ein Beispiel an: „Hacker verschleiern oft ihren Standort über VPN-Netzwerke oder Jump-Hosts und greifen von unterschiedlichsten IP-Adressen auf Ihren Shop zu. Beispielsweise um 10 Uhr aus China, um 11 Uhr von einem Server aus Malaysia und um 13 Uhr aus Brasilien. Kennen Sie eine seriöse Person, die in Summe 21.000 km in drei Stunden zurücklegen kann?“

Updates, Updates, Updates

Sicherheitsschwachstellen in einem Online-Shop entstehen automatisch. Wie? „Indem jemand sie findet!“, so Schuster.

„Die Entwickler der Online-Shop Software haben die Sicherheitsschwachstellen nicht absichtlich hinein programmiert, sondern diese sind durch Programmierfehler oder fehlerhafte Bibliotheken entstanden. Jeden Monat finden Experten tausende Schwachstellen und sicherlich auch in der von Ihnen genutzten Software. Daher ist es essenziell, dass Sie die Software des Online-Shops, sowie alle Plug-ins und auch das darunter laufende Betriebssystem aktualisieren. Speziell die



Ing. Andreas Schuster ist Berater für Informationssicherheit bei SEC4YOU und Director Sicherheit Sensibler Systeme bei der CMG (Computer Measurement Group).

großen Shop-Systeme haben bereits einen automatischen Update-Mechanismus und können sich ohne Zutun auf eine neue Version aktualisieren. Sofern Sie kein großes Team für die Pflege der Software haben, nutzen Sie dieses Sicherheitsfeature.“

Vollautomatisches Backup

Datenverlust kann sowohl durch einen Hardwaredefekt, als auch durch einen Cyberangriff entstehen. Nur wenn Daten regelmäßig gesichert werden, kann ein kostspieliger Datenverlust verhindert werden. Schuster sagt: „Vertrauen Sie nicht darauf, dass der Hosting Provider Ihre Daten sichert, kümmern Sie sich selbst um eine passende Backup-Strategie. Verzichten Sie auf manuelle Backups und nutzen Sie einen automatischen Backupdienst. Backup in der Cloud ist sehr kostengünstig, es ist empfehlenswert, die Daten nicht beim eigenen Hosting Provider zu sichern, sondern eine unabhängige Lösung zu implementieren.“

Training der Mitarbeiter

Zu guter Letzt rät der IT-Experte: „Ihre Mitarbeiter müssen sich ihrer Verantwortung bewusst sein und die geltenden Gesetze und Unternehmensvorgaben einhalten, um die Daten der Kunden zu schützen. Als Verantwortlicher eines Online-Shops müssen Sie Ihr Personal sorgfältig auswählen und regelmäßig schulen.

Denken Sie auch daran, dass beim Ausscheiden eines Mitarbeiters alle administrativen Zugänge des Mitarbeiters des Online-Shop Systems sofort gesperrt werden.“ ■