Vorteilsangebot „Sicherer Online-Shop“ zum European Cyber Security Month

Sensible Kundendaten im E-Commerce-Bereich und technische Infrastruktur, die für kriminelle Zwecke missbraucht werden kann, machen Online Shops zu beliebten Angriffszielen für Hacker. Schützen Sie sich und Ihre Kunden mit unserem Vorteilsangebot im Rahmen des diesjährigen European Cyber Security Month (ECSM).

Cyberkriminelle haben viele Motive

Heute werden mehr Einkäufe über das Internet getätigt, als je zuvor. Dabei übermitteln Verbraucher bei jeder aufgegebenen Bestellung sensible Daten, wie Kreditkarteninformationen, Namen, Anschrift und Geburtsdaten, an den Online-Händler. Diese digital gespeicherten Daten sind für Cyberkriminelle aus zahlreichen Gründen eine äußerst attraktive Beute: Für gestohlene Daten gibt es im Darknet einen florierenden Absatzmarkt, auf dem Hacker die Daten ohne große Schwierigkeiten an andere Nutzer verkaufen. Mit den gestohlenen Daten können im Internet dann unter falschem Namen beispielsweise Einkäufe getätigt oder Kredite aufgenommen werden. Auch der Online Shop selbst ist ein attraktives Ziel krimineller Angriffe. So können Hacker den Shop manipulieren und beispielsweie Preise verändern, oder ihn vollständig lahmlegen – entweder, um dem Betreiber direkt zu schaden oder eine Lösegeldsumme von ihm zu erpressen. Durch eine erfolgreiche Infiltration Ihrer IT-Systeme können diese zudem zur Durchführung illegaler Aktivitäten missbraucht werden.

Große Angriffsfläche - große Gefahr

Online Shops sind zu jeder Zeit über das Internet für jeden erreichbar. In der Regel erfordert ihr Betrieb außerdem das Zusammenspiel unterschiedlicher Systeme, wie Webserver, Datenbanken, Webanwendungen, mobile Anwendungen und Schnittstellen zwischen all diesen Systemen. All diese Ebenen können jeweils zahlreiche sicherheitsrelevante Schwachstellen aufweisen, die von Angreifern ausgenutzt werden können. Dazu gehören beispielsweise fehlende Softwareupdates oder Fehlkonfigurationen. Technische Angriffsmethoden, wie SQL Injections oder Cross Site Scripting, sind darüber hinaus öffentlich bekannt und für kriminelle Hacker verhältnismäßig einfach auszuführen.

Schützen Sie sich effizient vor Angriffen

Die vielfältigen Angriffsflächen machen einen wirksamen Schutz gegen kriminelle Angreifer für Online Shops wichtiger denn je. Neben einer Härtung Ihrer Systeme durch eine sichere Konfiguration sollten Sie Ihr Patch-Management, Ihre Software und deren Entwicklung sowie weitere Aspekte der IT-Sicherheit von unabhängigen Experten regelmäßig überprüfen lassen. Nur so können Sie zuverlässig einschätzen, wie gut Sie gegen Cyberkriminelle gerüstet sind und wie Sie Ihren Schutz noch verbessern können. International geltende, verbindliche Sicherheitsstandards, wie die EU-DSGVO oder der PCI DSS schreiben deshalb regelmäßige Prüfungen vor.

Vorteilsangebot „Sicherer Online-Shop“ zum European Cyber Security Month

Mit unserem Vorteilsangebot „Sicherer Online Shop“ schützen Sie Ihr E-Commerce-Geschäft sowie Ihre Kunden- und Unternehmensdaten wirksam vor Hackerangriffen und erfüllen zugleich regulatorische Anforderungen beispielsweise aus der EU-DSGVO und dem PCI DSS. Das Angebot umfasst eine technische Sicherheitsanalyse Ihrer im Internet erreichbaren IT-Systeme sowie Ihres Online Shops (der Webapplikation).

Unsere Sicherheitsexperten überprüfen hierbei zuverlässig und effizient mittels automatisierter Testverfahren die System- und Applikationsebene auf Schwachstellen. Anhand von konkreten Maßnahmenempfehlungen können Sie identifizierte Schwachstellen schnell und einfach schließen, bevor sie von Hackern oder Kriminellen ausgenutzt werden und damit ein echter Schaden entstehen würde.

Schutz auf Systemebene durch PCI Security Scans

Um die Sicherheit Ihrer IT-Systeme zu überprüfen, führen unsere Sicherheitsexperten einen PCI Security Scan (ASV-Scan) durch. Die Sicherheitsüberprüfung erfolgt für maximal drei IP-Adressen. Dabei werden Ihre aus dem Internet erreichbaren IT-Systeme umfangreich auf Schwachstellen untersucht. Eine Gefährdung des ordnungsgemäßen Betriebs ist nahezu ausgeschlossen. Sollte der Scan PCI-relevante Findings ergeben, erhalten Sie eine unbegrenzte Anzahl kostenfreier Re-Scans – bis Ihr Scanergebnis die Anforderungen des PCI DSS erfüllt.

Schutz auf Anwendungsebene durch Web Application Security Scans

Die Sicherheit Ihres Online Shops (der Webapplikation) überprüfen unsere Sicherheitsexperten mittels eines Web Application Security Scans. Die Sicherheitsüberprüfung erfolgt für maximal eine URL mit einem Port und einer Benutzerrolle. Grundlage der Überprüfung bilden die OWASP Top 10, der international führende Standard für die Sicherheit von Webapplikationen.

Ziel der Überprüfung ist es festzustellen, ob die Webapplikation sicher ist und keine Schwachstellen oder Verwundbarkeiten besitzt. Hierzu gehören beispielsweise das Auslesen von Kundenkonten und gültigen Benutzerdaten, die böswillige Veränderung von Artikelpreisen, Erstellung und Einlösung von manipulierten Gutscheincodes oder das Tätigen von Bestellungen - entweder kostenlos oder im Namen anderer Kunden.

more security. usd

Unser Angebot für Ihren Online Shop

Ablauf der Sicherheitsüberprüfung

1: Planung

In der Planungsphase werden die zu scannenden IP-Adressen der IT-Systeme sowie die notwendigen Informationen zu dem Online Shop (URL, Port und Benutzerrolle) mit Ihnen abgestimmt. Darüber hinaus wird mit Ihnen ein Zeitfenster für die Durchführung der Scans abgestimmt. Notwendige Maßnahmen zur Vorbereitung des Scans werden vorab mit Ihnen besprochen.

2: Scan

Mit einem normierten, international anerkannten Verfahren werden Ihre aus dem Internet erreichbaren IT-Systeme bzw. Webapplikationen automatisiert auf Schwachstellen überprüft. Erkannte Schwachstellen werden nicht ausgenutzt.

3: Review

Die Ergebnisse der automatisierten Sicherheitsüberprüfung werden von einem erfahrenen Sicherheitsexperten überprüft. Bei der Bewertung der Schwachstellen orientieren wir uns an internationalen und renommierten Sicherheitsstandards.

4: Bericht

Sie erhalten einen umfassenden Bericht bestehend aus einer Executive Summary und einem Technical Report. Die Kritikalität von Schwachstellen und deren Eintrittsrisiken werden bewertet sowie Maßnahmenempfehlungen zur Korrektur identifizierter Schwachstellen gegeben. Sie haben so die Möglichkeit, ggf. vorhandene Probleme schnell und einfach zu korrigieren und sich effizient vor Hackern zu schützen.

Ihr persönliches Zertifikat

Erfüllt Ihre Sicherheitsüberprüfung die hohen Sicherheitsanforderungen der Kreditkartenindustrie (PCI DSS), bestätigen wir Ihnen dies gerne in einem persönlichen Zertifikat. So können Sie gegenüber Kunden und Partnern Ihren Anspruch an Sicherheit demonstrieren.

Vorteilsangebot: Sicherer Online Shop

PCI Security Scan (ASV-Scan) von bis zu drei IP-Adressen	+	**Web Application Security Scan** von einer URL mit einem Port sowie einer Benutzerrolle

680,– Euro* (statt 844,- Euro)

*Preis versteht sich zzgl. der gesetzlich geltenden MwSt. Der exklusive Rabatt von 164,- EUR ist ausschließlich im Rahmen des European Cyber Security Month, vom 15.09.-15.11.2021 gültig.

more security. usd

Vorteilsangebot „Sicherer Online-Shop“ zum European Cyber Security Month

Bestellung per Fax an +49 6102 8631-99 oder per E-Mail an bestellung@usd.de

☐ Hiermit bestelle ich das Vorteilsangebot „Sicherer Online-Shop“ der usd AG für 680,- Euro*.

Anrede _____

Vorname / Nachname _____

E-Mail-Adresse _____

Telefonnr. _____

Firma _____

Straße / Hausnr. _____

PLZ / Stadt _____

Land _____

Ort, Datum _____ Unterschrift _____

Firmenstempel

*Alle Preise verstehen sich zzgl. der gesetzlich geltenden MwSt. Die Leistung wird von der usd AG mit Beauftragung in Rechnung gestellt. Das Zahlungsziel beträgt 14 Tage nach Eingang der Rechnung. Nach Beauftragung nimmt die usd AG Kontakt zu Ihnen auf, um gemeinsam die Planungsparameter abzustimmen. Die Sonderaktion hat Gültigkeit vom 15.09.-15.11.2021. Danach gelten die normalen Preise ohne Vergünstigung.

usd AG
Frankfurter Straße 233, Haus C1
63263 Neu-Isenburg

Telefon: +49 6102 8631-190
E-Mail: vertrieb@usd.de
www.usd.de