SICHERN IHRES GUTEN RUFS

Ein Leitfaden für den Einzelhandel

Inhaltsverzeichnis

Als Einzelhändler haben Sie wahrscheinlich ganz bestimmte KPIs (Key Performance Indicator; Leistungskennzahlen), nach denen Sie die Leistung Ihres Geschäfts beurteilen. Ob Ihr Schwerpunkt dabei die Optimierung der Bestandsverwaltung oder die Verbesserung der Kundenzufriedenheit ist– in jedem Fall sehen Sie sich die Daten wohl regelmäßig genauer an, um die Leistung Ihres Unternehmens beurteilen und letztlich verbessern zu können.

Verbraucher haben ihre eigenen Kennzahlen für die Bewertung Ihres Geschäfts – und sie scheuen sich nicht, sie zu benutzen! Mit dem Aufkommen von Social Media und Vernetzungs-Tools wie Facebook, LinkedIn, Yelp und vielen anderen sind Verbraucher nun im 21. Jahrhundert nur einen Katzensprung, oder besser einen Mausklick, von einer Fünf-Sterne-Bewertung oder einem Kommentar entfernt, durch den Ihr Ruf auf Wochen und Monate hinaus Schaden nehmen kann. Während die Besucherzahlen durch eine positive Bewertung überraschend stark in die Höhe schnellen können, ist eine negative oder weniger gute Bewertung unter Umständen sogar existenzgefährdend.

Als würden die Kundenrezensionen allein nicht ausreichen, gibt auch die Netzwerksicherheit ständig Anlass zur Sorge, denn sowohl KMUs als auch Konzerne von der Größe Walmarts sind nach wie vor die Hauptziele von Internetkriminellen. Alle Einzelhandelsunternehmen verarbeiten personenbezogene Daten (Personally Identifiable Information; PII), und diese Daten sind hochinteressant für Kriminelle, die das schnelle Geld suchen und ständig nach neueren, besseren und schnelleren Möglichkeiten Ausschau halten, wie sie in Ihr Netzwerk einbrechen und an diese Daten herankommen können. Wir alle haben die Schlagzeilen gesehen und erlebt, welche Auswirkungen eine Datensicherheitsverletzung auf den Ruf eines Einzelhändlers haben kann. Doch trotz heftigster Gegenreaktionen – die Sicherheitsverletzungen gehen weiter.

Die Sicherheit Ihres Unternehmensnetzwerks zu gewährleisten, ist sicherlich keine leichte Aufgabe, aber eine, der Sie sich stellen müssen, um den Ruf Ihres Unternehmens abzusichern. In diesem eBook sehen wir uns die Markttreiber an, die die Sicherheitsanstrengungen im Einzelhandel forcieren, gehen auf die zu bewältigenden Herausforderungen ein und, was sicherlich am wichtigsten ist, untersuchen die höchst realen Lösungen, nach denen jeder Einzelhändler praktisch nur zu greifen braucht.

NEGATIVE PUBLICITY NACH EINER SICHERHEITSVERLETZUNG

87 %

der Verbraucher würden Unternehmen, bei denen eine ***Datensicherheitsverletzung festgestellt*** wurde, **KONSEQUENT MEIDEN.**[1]

COMPLIANCE

4 von **5**

Unternehmen fallen bei einer turnusmäßigen Überprüfung der Einhaltung des **PCI DSS** durch.[2]

KONTINUITÄT DES GESCHÄFTSBETRIEBS

POS-Ausfallzeiten kosten den Einzelhandel **im Durchschnitt schätzungsweise**

4.700 $

PRO MINUTE[4]

WLAN-VERBINDUNG

42 %

der Einzelhändler geben an, **dass WLAN-Technologie im Laden** das **größte Sicherheitsrisiko darstellt.**[5]

1. CyberSecurity Institute, „How Does a Data Breach Affect Your Business' Reputation?" (Welche Auswirkungen hat eine Datensicherheitsverletzung auf den Ruf Ihres Unternehmens?)
2. Paments Cards & Mobile, „4 von 5 Unternehmen sind nicht PCI-konform"
3. PRWeb, „The Real Cost of Downtime to Retailers" (Die effektiven Kosten von Ausfallzeiten im Einzelhandel)
4. Level 3, „Einzelhändler: Diese Liste besser zweimal prüfen"

POS-EINDRINGVERSUCHE

Ähnlich wie ein klassischer Anzug oder die Lieblingsjeans ihre Besitzer über Jahre begleiten, sind Point-of-Sale-Eindringversuche seit jeher quasi das Steckenpferd von Cyberkriminellen: Ein verbreiteter Angriffsweg für Eindringlinge, die jede Gelegenheit nutzen, sich auf Kosten anderer zu bereichern. Bei diesen Einbrüchen platzieren Hacker Schadsoftware in einem ahnungslosen POS-System, um Daten von Zahlungskarten zu erlangen, während diese im temporären Speicher abgelegt sind. Über eine Remoteverbindung bringt der Hacker dann alle Kartendaten an sich, die er zu fassen bekommt. Einige besonders clevere Kriminelle entwickeln ihre Schadsoftware selbst, während andere sich schlicht und einfach aus dem reichhaltigen Angebot von Schadsoftware bedienen, das sie im Untergrund-Internet bzw. „Darknet" finden.

„Und was passiert dann?" werden Sie fragen. Was genau machen diese Ganoven mit möglicherweise hunderttausenden von Kartennummern? Nun, sobald er die Kartennummern in Händen hat, setzt der Kartendieb eine ausgeklügelte Maschinerie in Gang: Wie ein Rädchen im Getriebe führt jeder der Mittäter einen speziellen Auftrag aus, und alle natürlich gegen entsprechende Bezahlung. Es gibt jemanden, der die Kartennummern kauft und verkauft, jemanden, der die gefälschten Karten herstellt, Rekrutierer, die Leute anwerben, die mit den gefälschten Karten etwas kaufen sollen, und dann die Leute, die diese Einkäufe tatsächlich erledigen. Und da gibt es natürlich auch noch unsere ahnungslosen Verbraucher, die unwissentlich ihr Bankkonto preisgegeben haben, als sie eigentlich nur ein Sandwich kaufen wollten.

Zwei-Faktor Authentifizierung

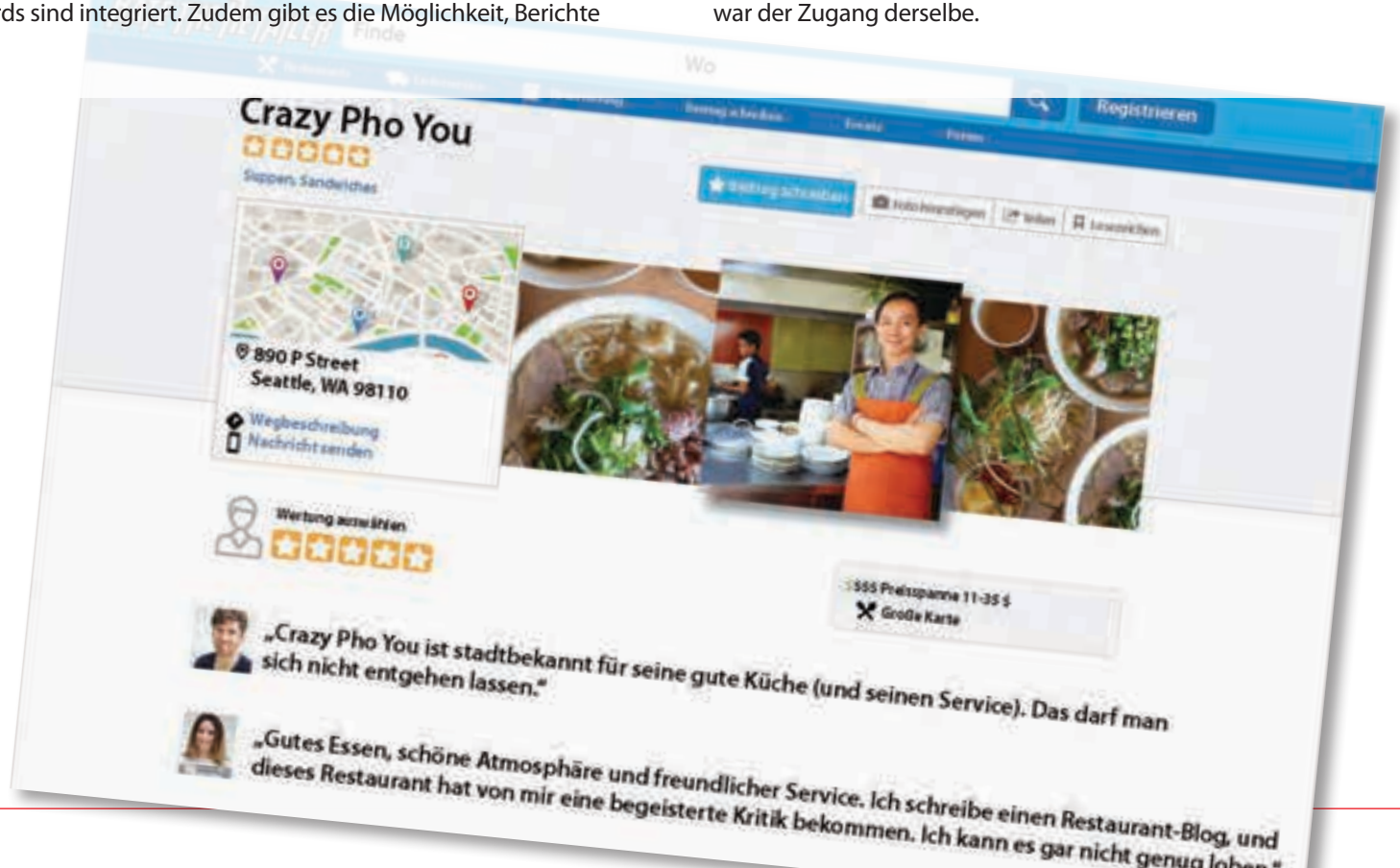
Wir müssen zur Kenntnis nehmen, dass die Ein-Faktor-Authentifizierung nicht mehr ausreicht. Sie können die Sicherheit in Ihren Verkaufsstellen drastisch verbessern, indem Sie einfach nur eine Zwei-Faktor-Authentifizierung einführen (das kann eine mobile App oder auch ein Hardware-Token sein). Achten Sie darauf, dass Ihre Verkäufer beim Betreten Ihrer POS-Umgebung eine strenge Authentifizierung durchlaufen, und überwachen Sie die Anmeldevorgänge genau.

Transparenz

Erkundigen Sie sich, welche Möglichkeiten es gibt, Ihre POS-Umgebung zu überwachen. Dimension, eine cloudfähige Visualisierungslösung, die zum Lieferumfang der UTM Firewall-Plattform von WatchGuard gehört, stellt Tools für Datenvisualisierung und Reporting bereit, mit denen sich Bedrohungen für die Netzwerksicherheit sowie Probleme und Trends eindeutig identifizieren lassen. Mehr als 100 umfangreiche Berichte und Dashboards sind integriert. Zudem gibt es die Möglichkeit, Berichte nach Plan zu erstellen und per E-Mail an bestimmte Personen zu senden.

Segmentierung

Stellen Sie Ihr POS-System nicht im selben Netzwerk bereit wie den Pausenraum-PC Ihrer Mitarbeiter, in dem jemand das Internet nach ulkigen Katzenbildern durchforstet. Das ist ein absolutes No-Go. Alle WatchGuard-Firewalls unterstützen die Netzwerksegmentierung, die eine klare Trennung zwischen POS-Umgebung und Unternehmens-LAN schafft. Ein abschreckendes Beispiel: Bei dem Hackerangriff auf den Großhändler Target, der weltweit Aufsehen erregte, wurden eigentlich die Kundendaten eines HLK-Unternehmens gestohlen, das an Standorten von Target für die Kontrolle des Energieverbrauchs und die Temperatursteuerung zuständig war. Diese Firma wollte und brauchte auch nicht auf die POS-Systeme von Target zuzugreifen, aber da das Netzwerk nicht segmentiert war, war der Zugang derselbe.



POS-EINDRINGVERSUCHE

SKIMMING VON ZAHLUNGSKARTEN

Während Hacker sich bei dem Versuch, in POS-Systeme einzudringen, durch die Hintertür anschleichen, um an personenbezogene Daten zu kommen, nehmen sie beim Skimming die Eingangstür und bringen den Schlüsseldienst gleich mit. Für das Skimming von Zahlungskarten installiert ein Datendieb physische Skimming-Hardware auf einem Gerät, das die auf dem Magnetstreifen einer Zahlungskarte aufgebrachten Daten liest. Das kann ein Geldautomat oder auch die Halterung eines POS-Terminals in Ihrem Geschäft sein. Vielleicht fragen Sie sich: „Warum sieht das keiner, bevor es zu spät ist?“ Nun, die fraglichen Skimmer – häufig Lochkameras für die Erfassung von PIN-Codes – sind winzig klein und sehr detailgenau gebaut. Sie müssten sich in Ihrer Umgebung schon ständig mit der Lupe umsehen, um einen Skimmer erkennen zu können, bevor er aktiv geworden ist.

Mitarbeiter schulen

Zeigen Sie Ihren Mitarbeitern, wie sie feststellen können, ob eine Manipulation stattgefunden hat, und machen Sie diese Kontrollen zum festen Bestandteil der Arbeitsabläufe.

Physische Sicherheit verstärken

Manipulationssichere Terminals kaufen. Manipulationssichere Funktionen machen es Hackern schwer, die Daten von Karteninhabern zu erlangen, indem sie versuchen, auf elektronische Komponenten von PIN-Pads oder Terminals zuzugreifen.

Manipulationen erkennbar machen

Alles, was Sie tun können, damit Manipulationen mit bloßem Auge besser erkennbar sind, ist eine schon gute Sache. Zwei Dinge, mit denen Sie beginnen können, sind beispielsweise die Kontrolle von Überwachungsvideos oder das Anbringen von Aufklebern auf den Türen Ihrer Terminals.

BEREITSTELLEN EINES SICHEREN WLAN-ZUGANGS

BEREITSTELLEN EINES SICHEREN WLAN-ZUGANGS

WLAN ist heutzutage nicht mehr nur „nice to have“, sondern eine absolute Notwendigkeit. Die Bereitstellung eines WLAN-Zugangs führt nicht nur zu einer längeren Verweildauer im Laden, sondern kann überdies ein entscheidender Faktor sein, der Ihren Gast überhaupt erst zu einem Besuch veranlasst.

Aber Kunden wollen nicht einfach nur einen WLAN-Zugang, sondern es muss unbedingt ein WLAN-Zugang mit höchster Geschwindigkeit und bester Signalstärke sein. Signalstärke und Übertragungsgeschwindigkeit haben einen enormen Einfluss auf die Zufriedenheit des Kunden. Somit sind 802.11ac-Geschwindigkeiten und reichlich Bandbreite für einen optimalen Empfang im gesamten Laden unverzichtbar. Die Zeiten, in denen man einen potenziellen Gast mit dem Schild für „kostenloses (aber äußerst langsames) WLAN“ anlocken konnte, sind lange vorbei.

Während sich die Frage, WLAN bereitstellen oder nicht, heute praktisch nicht mehr stellt, kann die Absicherung dieses Netzwerks eine knifflige Angelegenheit werden. So sehr Ihre Gäste den offenen Zugang zu einem WLAN auch schätzen werden, er bietet gleichzeitig Internetkriminellen einen bequemen Angriffsvektor. Ein Trick sind beispielsweise Rogue-APs. Dabei platziert ein Angreifer seinen bösartigen AP in unmittelbarer Nähe Ihres Ladens und kaschiert ihn mit einer scheinbar vertrauenswürdigen IP-Adresse. Sobald Ihre arglosen Gäste oder Mitarbeiter dann in das Netzwerk gehen, kann der Angreifer seine Absichten in die Tat umsetzen und beispielsweise Kundendaten stehlen oder die Geräte mit einer Schadsoftware infizieren, die ausgeführt wird, wenn der Benutzer sich bei einem geschützten Netzwerk (also Ihrem Unternehmens-LAN) anmeldet.

BEREITSTELLEN EINES SICHEREN WLAN-ZUGANGS

Hohe (aber immer noch sichere) Verbindungsgeschwindigkeiten

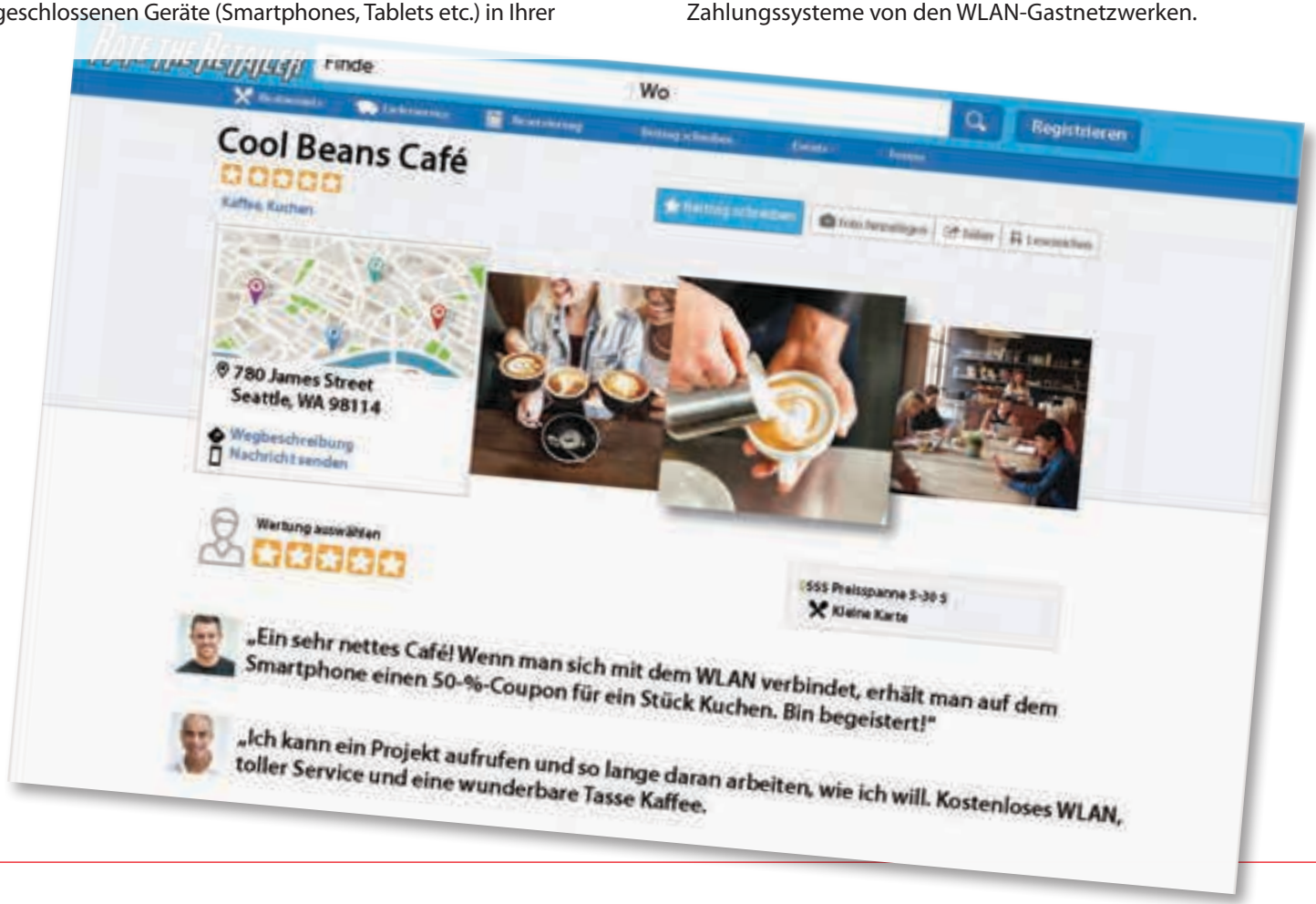
Die Modelle AP125, AP325 und AP420 eignen sich hervorragend für Innenbereiche von Einzelhandelsumgebungen. Hingegen ist der robuste AP327X ideal für Außenbereiche, um in Einkaufszentren, auf Märkten, an Touristenattraktionen und darüber hinaus für eine sichere WLAN-Verbindung zu sorgen.

Bedrohungsschutz im WLAN

Wenn Sie Ihren Kunden einen WLAN-Zugang anbieten wollen, ohne Internet-Hackern Tür und Tor für den Zugriff auf sensible Daten zu öffnen, dann brauchen Sie eine WIPS-Lösung (Wireless Intrusion Prevention System). WatchGuard WIPS hat die patentierte Marker-Packet-Technologie, die zuverlässig alle Wireless Access Points und angeschlossenen Geräte (Smartphones, Tablets etc.) in Ihrer WLAN-Umgebung erkennt und als autorisiert, extern oder nicht autorisiert klassifiziert und damit sicherstellt, dass NUR inakzeptable Verbindungen sofort beendet werden, ohne benachbarte WLAN-Netzwerke auf illegale Weise zu stören. Sie laufen also nicht Gefahr, versehentlich den WLAN-Zugang der Schule auf der anderen Straßenseite zu schließen, weil Ihr WIPS deren AP nicht erkannt hat.

Zentrale Verwaltung

Mehrere Systeme mit verschiedenen Tools zu verwalten, ist schlicht unpraktisch. Wichtig ist also ein konsolidiertes Management drahtloser und kabelgebundene Systeme auf einer Plattform. Die von WatchGuard angebotenen Optionen für eine zentrale Verwaltung vereinfachen die Bereitstellung und die Trennung der Zahlungssysteme von den WLAN-Gastnetzwerken.



EINHALTEN DER PCI DSS-COMPLIANCE

EINHALTEN DER PCI DSS-COMPLIANCE

Auf der Liste Ihrer bevorzugten Freizeitbeschäftigungen rangiert das Erreichen und Beibehalten der PCI DSS-Compliance (Payment Card Industry Data Security Standard) wahrscheinlich irgendwo in der Nähe von leidigen Putzaufgaben wie dem Entfernen von festgeklebtem Kaugummi. Wer wollte Ihnen das übel nehmen? Dies sind strikte Standards, die jedes Jahr strenger werden. Wenn die Bedrohungen größer werden, müssen die PCI-Standards nachziehen. Das macht es für viele Geschäftsinhaber schwierig, die immer längere Liste der sich ständig verändernden Anforderungen zu erfüllen. Eine 2016 vom Merchant Acquirers' Committee durchgeführte Umfrage hat ergeben, dass die PCI-Compliance bei KMUs mit gerade einmal 39 Prozent am niedrigsten ist. Das hat schwerwiegende Folgen: Bei Nichterreichen der PCI-Standards muss Ihre Händlerbank eine monatliche Strafe (in Höhe von 5.000 bis 100.000 $ pro Monat) zahlen, die sie sicherlich an Sie weitergeben wird. Außerdem wird die Händlerbank voraussichtlich entweder die Geschäftsbeziehung beenden oder die Transaktionsgebühren deutlich erhöhen.
Man kann also mit Sicherheit sagen, dass die Beibehaltung der PCI-Zertifizierung zwar eine schwierige Angelegenheit ist, eine Geschäftstätigkeit ohne diese Zertifizierung jedoch exponentiell höhere Herausforderungen stellt.

EINHALTEN DER PCI DSS-COMPLIANCE

Perimeterschutz durch Firewalls

Investieren Sie in eine UTM-Lösung, die eine gestaffelte, mehrstufige Verteidigungslinie (Defense in Depth) bietet. Stellen Sie sich das so vor: Angenommen, Sie wollen etwas Wertvolles vor den Blicken und dem Zugriff anderer schützen. Sie legen es in einen Safe. Sie stellen den Safe in einen Schrank und diesen Schrank in einen Raum. Der Raum befindet sich in einem Haus und um das Haus herum verläuft ein Zaun. Das sind Ihre Sicherheitsebenen, und genau die braucht auch Ihr Netzwerk.

Konfigurieren Sie richtig

Die ordnungsgemäße Konfiguration Ihrer Firewall ist von entscheidender Bedeutung und eine der wichtigsten Anforderungen des PCI DSS-Standards. Zudem sollte diese Konfiguration regelmäßig geprüft werden, damit nicht im Laufe der Zeit ungeschützte Löcher entstehen. „Einrichten und vergessen" ist hier nicht angebracht.

Mit WatchGuard wird diese Konfiguration dank Weboberfläche und Standardregeln denkbar einfach. Aber wenn Konfigurationen so gar nicht Ihre Sache sind, dann sollten Sie sie einem qualifizierten Technologiepartner überlassen. Sie zahlen eine monatliche Gebühr und geben die Konfiguration und Verwaltung der Firewall in die Hände eines Dienstleisters.

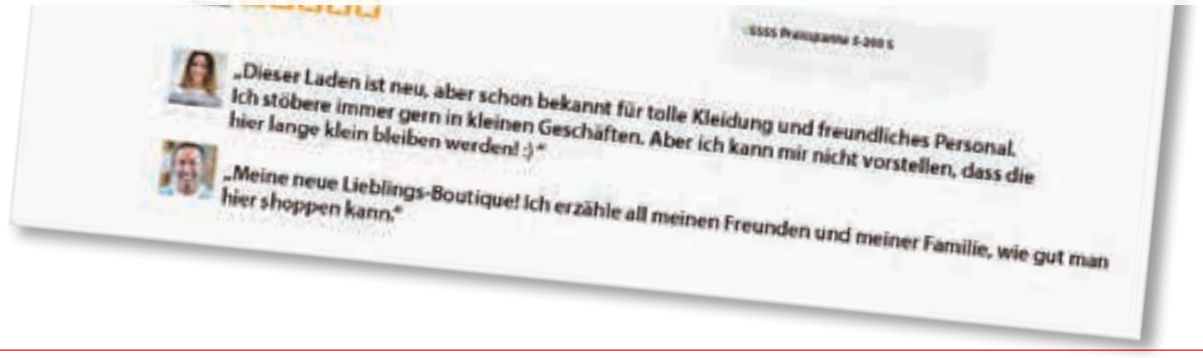
Implementieren Sie Multifaktor-Authentifizierung

Kontrollorgane wenden immer strengere Vorschriften für die Einführung von MFA (Multifaktor-Authentifizierung) in Einzelhandelsumgebungen an. So ist MFA gemäß Anforderung 8.3 der PCI DSS-Version 3.2, die 2018 umgesetzt wurde, für den Zugriff ohne Konsole auf Computer und Systeme, die Daten von Kartenlesegeräten verarbeiten, sowie für den Fernzugriff auf die Kartenleser-Umgebung verpflichtend. Mit der Anforderung 8.3 wurde der Begriff „Multifaktor-Authentifizierung" in PCI DSS eingeführt. Dieser ersetzt den zuvor verwendeten Begriff „Zwei-Faktor-Authentifizierung" (2FA). Durch diese begriffliche Änderung wurde die Authentifizierung mit zwei Faktoren zur Mindestanforderung.

Die MFA-Lösung von WatchGuard – AuthPoint™ – geht über die herkömmliche Zwei-Faktor-Authentifizierung hinaus, indem innovative Methoden der Benutzeridentifizierung eingesetzt werden, wie beispielsweise bei unserem Ansatz, die DNA des Mobilgeräts zu überprüfen. Unser umfangreiches Ökosystem aus Integrationen von Drittanbietern, bedeutet einen durchgängig starken Schutz für das gesamte Netzwerk, VPNs, Cloud-Anwendungen usw. – wo auch immer Bedarf besteht.

Wenn Sie Daten von Karteninhabern speichern müssen, dann sichern Sie sie

Die Verarbeitung der Daten von Karteninhabern ist eine Sache für sich, aber wenn diese Daten auch gespeichert werden sollen, sind zusätzliche Anforderungen zu erfüllen und Standards einzuhalten. Das Beste und Einfachste, was Sie für die PCI-Zertifizierung tun können, ist der komplette Verzicht auf die Speicherung von Daten – sofern das überhaupt möglich ist. Doch wenn Daten von Karteninhabern unbedingt gespeichert werden müssen, dann sorgen Sie dafür, dass alle diese Daten sicher verschlüsselt werden. Gewähren Sie nur den Personen in Ihrem Unternehmen Zugriff auf diese Datenbank, die diese Daten wirklich brauchen, und weisen Sie jedem von ihnen seine eigenen, eindeutigen Anmeldedaten zu.



Wenn es Ihnen um geschäftliches Wachstum geht, muss Netzwerksicherheit für Sie Priorität haben. Hier treffen die intuitiven Lösungen von WatchGuard Technologies zum Schutz von POS und WLAN sowie zur Einhaltung von Compliance einen wichtigen Nerv. Damit sind Sie in der Lage, nicht nur Ihre Netzwerke, sondern auch Ihren Geschäftserfolg und Ihren guten Ruf abzusichern.

Globale Hauptgeschäftsstelle USA
Tel: +1.206.613.6600
E-Mail: sales@watchguard.com

Hauptgeschäftsstelle Central Europe
Tel: +49 (700) 9222 9333
E-Mail: sgermanysales@watchguard.com

Hauptgeschäftsstelle APAC-Ozeanien Singapur
Tel: +65.6536.7717
E-Mail: inquiry.sea@watchguard.com

WatchGuard