SONICWALL®

WIE RANSOMWARE IHR UNTERNEHMEN LAHMLEGEN KANN

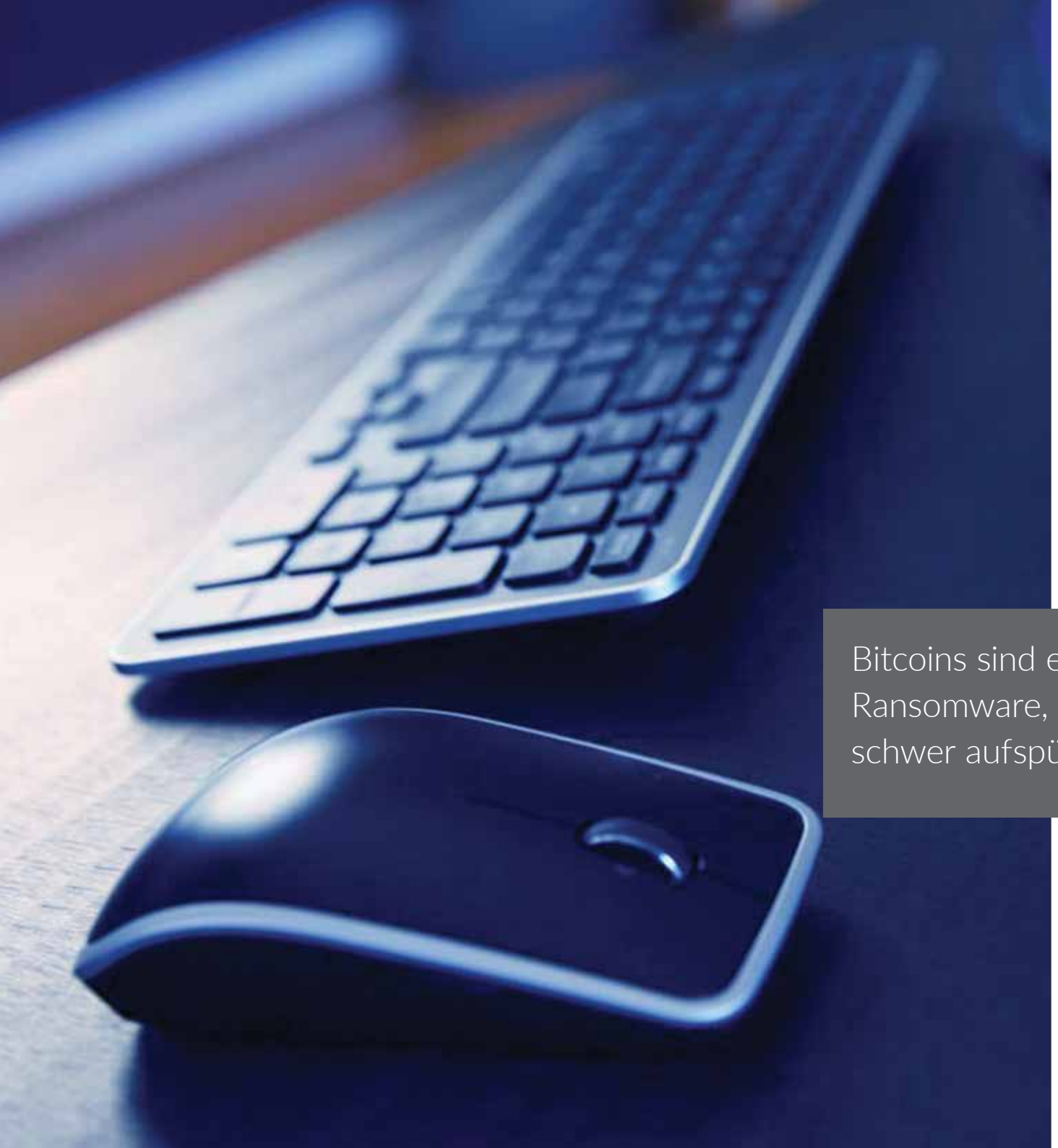
Was sind Ransomware-Angriffe und wie funktionieren sie?

Einleitung

Ransomware ist eine Form von Malware, die den Zugriff auf Daten oder Systeme blockiert. Um die Sperrung aufzuheben, verlangt der Angreifer ein Lösegeld. Zwar gibt es Ransomware schon seit vielen Jahren, doch sie tritt immer häufiger in Erscheinung und wird auch immer profitabler. Bekannte Beispiele für Ransomware sind etwa CryptoLocker, CryptoWall oder RSA4096.

Dem FBI zufolge wurden schon allein in den ersten drei Monaten von 2016[1] in den USA mehr als 209 Millionen $ Lösegeld bezahlt – im Vorjahr waren es im Vergleich dazu 25 Millionen $ über einen Zeitraum von zwölf Monaten.

1 http://sd18.senate.ca.gov/news/4122016-bill-outlawing-ransomware-passes-senate-committee



So funktioniert Ransomware

Es gibt viele Möglichkeiten, wie Ransomware in ein System gelangen kann. Letzten Endes ist es aber immer so, dass das Opfer eine böswillige Anwendung herunterlädt und installiert. Sobald sich die App auf dem Gerät befindet, verbreitet sie sich im ganzen System und verschlüsselt Dateien auf der Festplatte oder sperrt einfach das System selbst. Manchmal blockiert sie den Zugriff auf das System, indem sie Bilder oder einen Text auf dem Bildschirm erscheinen lässt. Damit soll der Benutzer dazu gebracht werden, dem Malwarebetreiber ein Lösegeld für den Chiffrierschlüssel zu zahlen, um die Dateien bzw. das System zu entsperren.

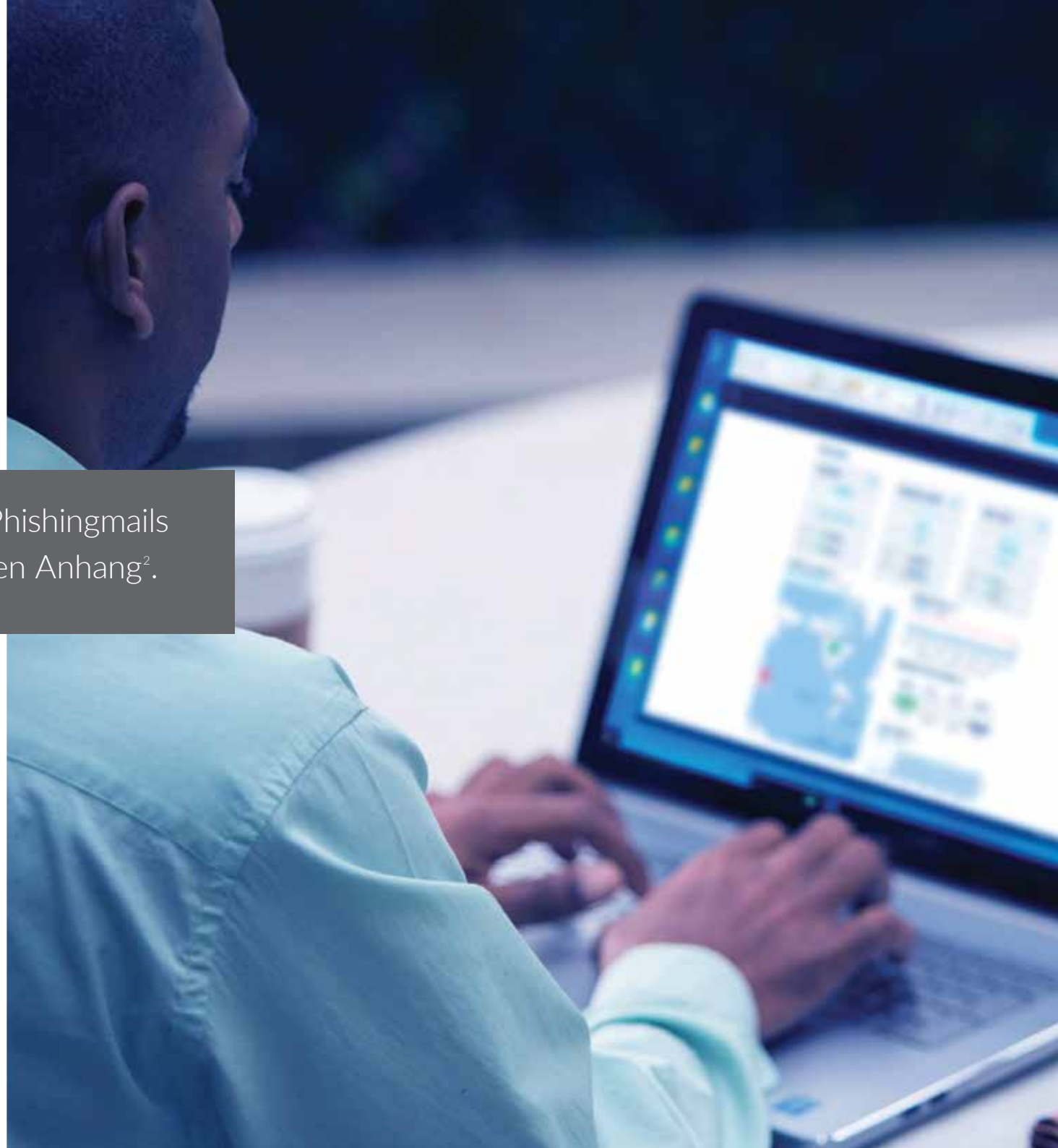
Bitcoins sind eine beliebte Zahlungsform bei Ransomware, da sich die digitale Währung nur schwer aufspüren lässt.

SONICWALL®

Phishingmails

Eine der gängigsten Verbreitungsmethoden für Ransomware sind Phishingmails. Diese Art von E-Mail versucht, den Empfänger dazu zu bringen, eine E-Mail zu öffnen und auf einen Website-Link zu klicken. Die Site kann dann nach vertraulichen Informationen fragen oder Malware wie eben Ransomware enthalten, die auf das System des Opfers geladen wird.

23 Prozent der Empfänger öffnen Phishingmails und 11 Prozent klicken sogar auf den Anhang[2].

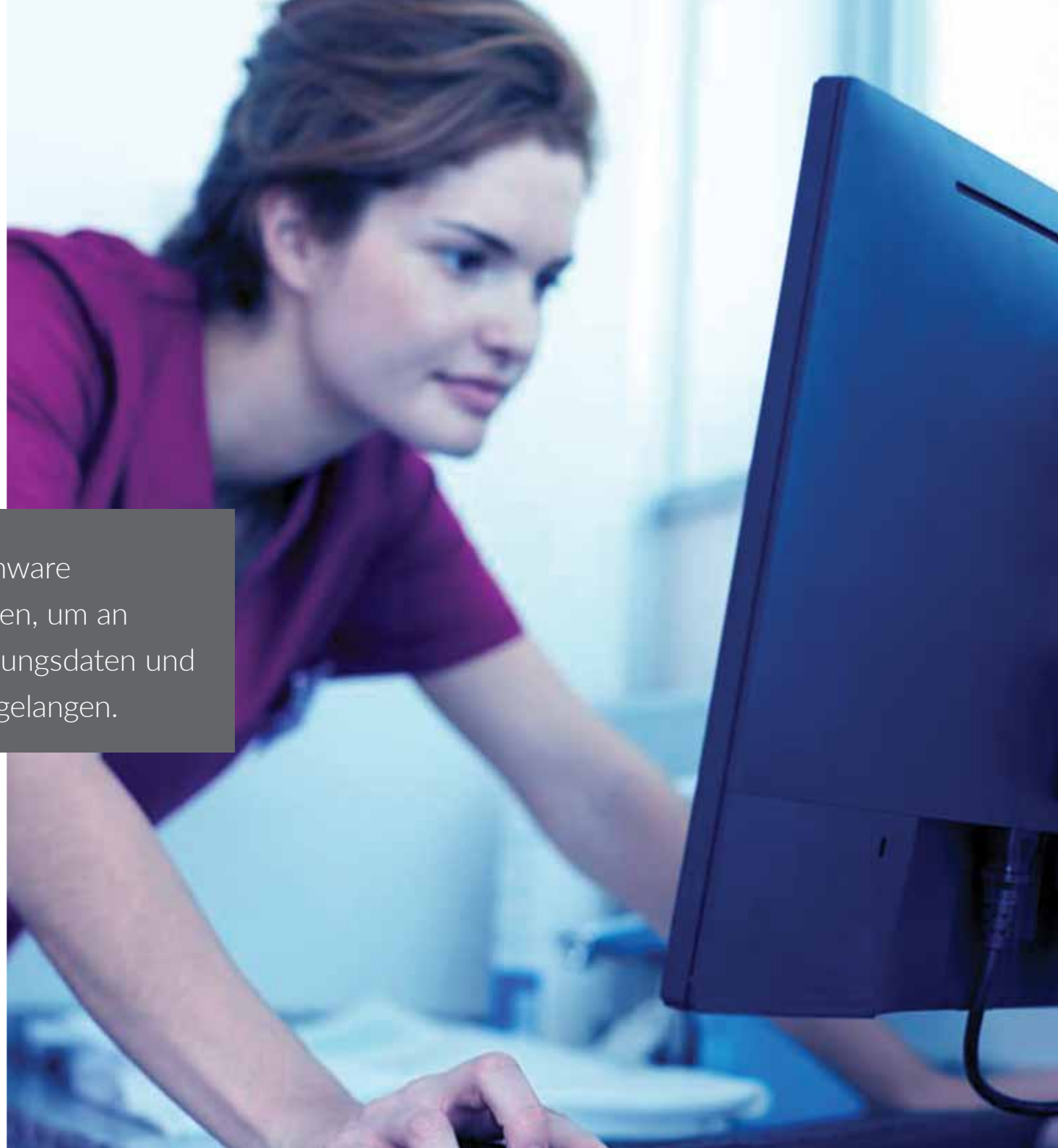


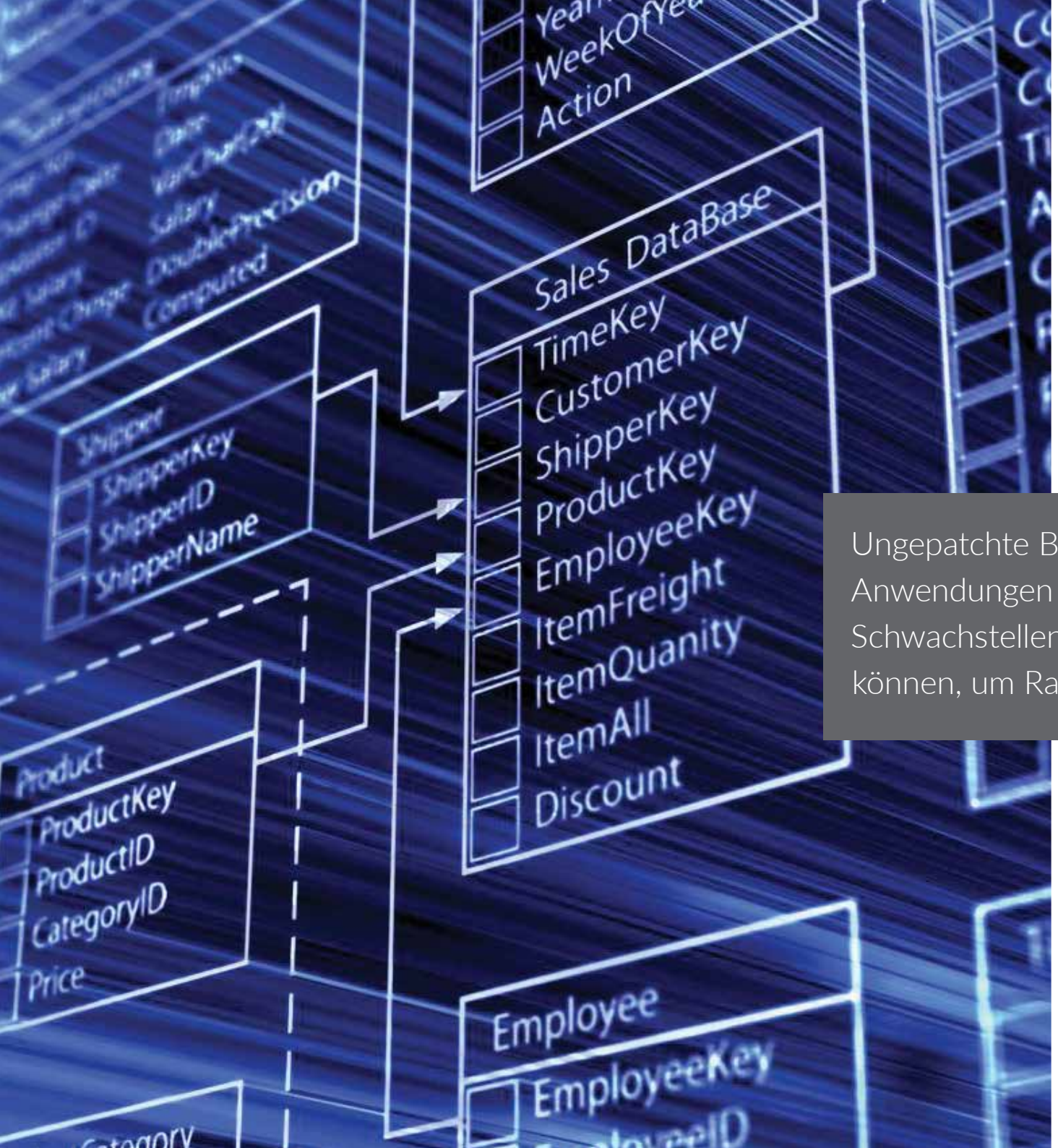
2 2015 Verizon Data Breach Investigation Report

Malvertisement

„Malvertising“ – vom englischen Begriff „malicious advertising“, also schädliche Werbung – ist eine weitere beliebte Methode zur Verbreitung von Ransomware mittels Onlinewerbung. Der Angreifer infiltriert ein Werbenetzwerk – manchmal gibt er sich als Werbetreibender oder Agentur aus – und schleust mit Malware infizierte Werbung in seriöse Websites ein. Nichts ahnende Besucher auf der Website müssen nicht einmal auf die Werbung klicken, damit ihr System infiziert wird.

Neben der Einschleusung von Ransomware können „Malverts“ auch genutzt werden, um an Kreditkartennummern, Sozialversicherungsdaten und weitere vertrauliche Kundendaten zu gelangen.



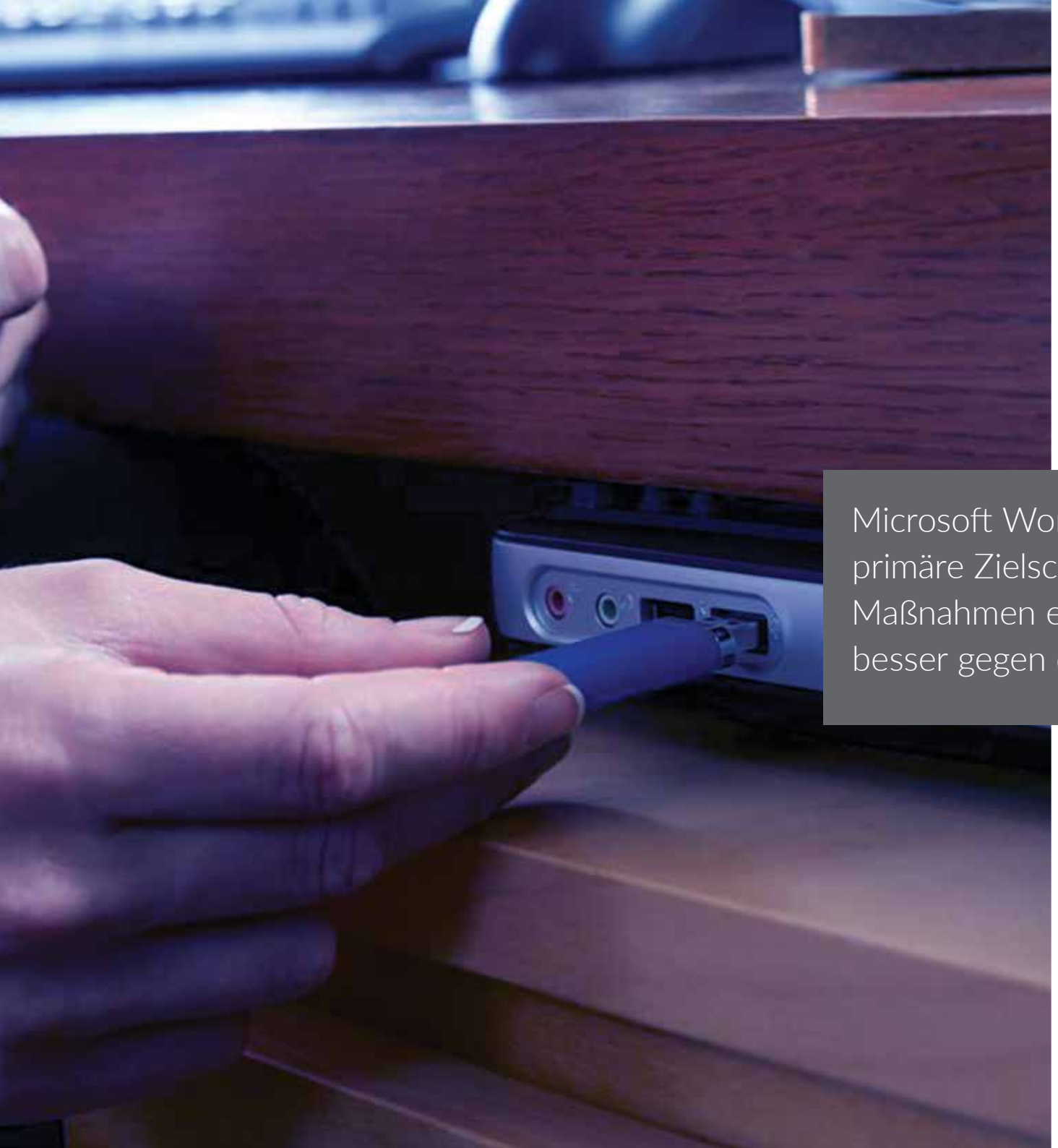


Ausnutzung ungepatchter Systeme und Anwendungen

Viele Angriffe basieren auf bekannten Schwachstellen in Betriebssystemen, Browsern und gängigen Apps. Cyberkriminelle machen sich diese Schwachstellen zunutze und richten ihre Ransomware-Angriffe gezielt gegen Systeme, die nicht über die neuesten Software-Patches verfügen.

Ungepatchte Betriebssysteme, Browser und Anwendungen enthalten möglicherweise Schwachstellen, die Cyberkriminelle nutzen können, um Ransomware-Angriffe durchzuführen.

SONICWALL®



Externe Geräte

Externe Geräte wie etwa USB-Sticks werden für die Speicherung und Übertragung von Dateien genutzt. Dabei werden sie oft von Cyberkriminellen missbraucht, um Ransomware über viele verschiedene Systeme hinweg zu verbreiten. Einige dieser Dateien enthalten Makros, ein ausgeklügeltes Feature, das Hacker nutzen, um Ransomware beim Öffnen der Datei auszuführen.

Microsoft Word, Excel und PowerPoint sind primäre Zielscheiben, obwohl Microsoft bereits Maßnahmen eingeleitet hat, um Office 2016 besser gegen diese Bedrohung abzuschirmen.

SONICWALL®

Warum man mit traditionellen Methoden Ransomware-Angriffe nicht verhindern kann

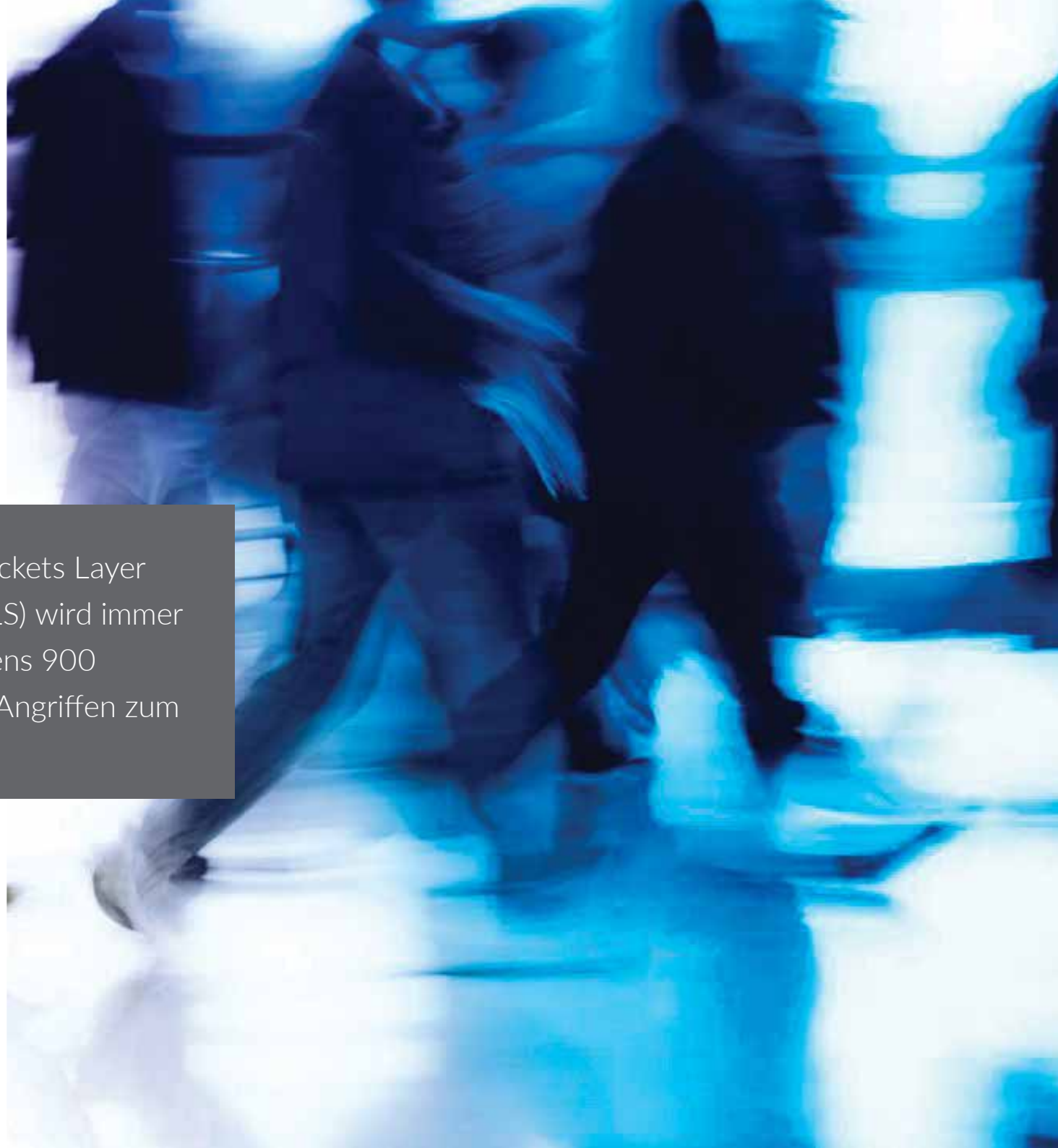
Viele traditionelle Sicherheitskontrollen sind nicht in der Lage, Ransomware zu entdecken, wenn sie nur nach ungewöhnlichem Verhalten und gängigen Hinweisen auf Kompromittierung Ausschau halten. Sobald sich die Ransomware auf einem System befindet, verhält sie sich wie eine Sicherheitsanwendung, die den Zugriff auf andere Systeme oder Programme verweigern kann. In der Regel bleiben die zugrunde liegenden Dateien und Systeme unberührt, wobei nur der Zugriff auf die Oberfläche eingeschränkt wird.

In Kombination mit Social Engineering ist Ransomware eine äußerst effektive Angriffsvariante.

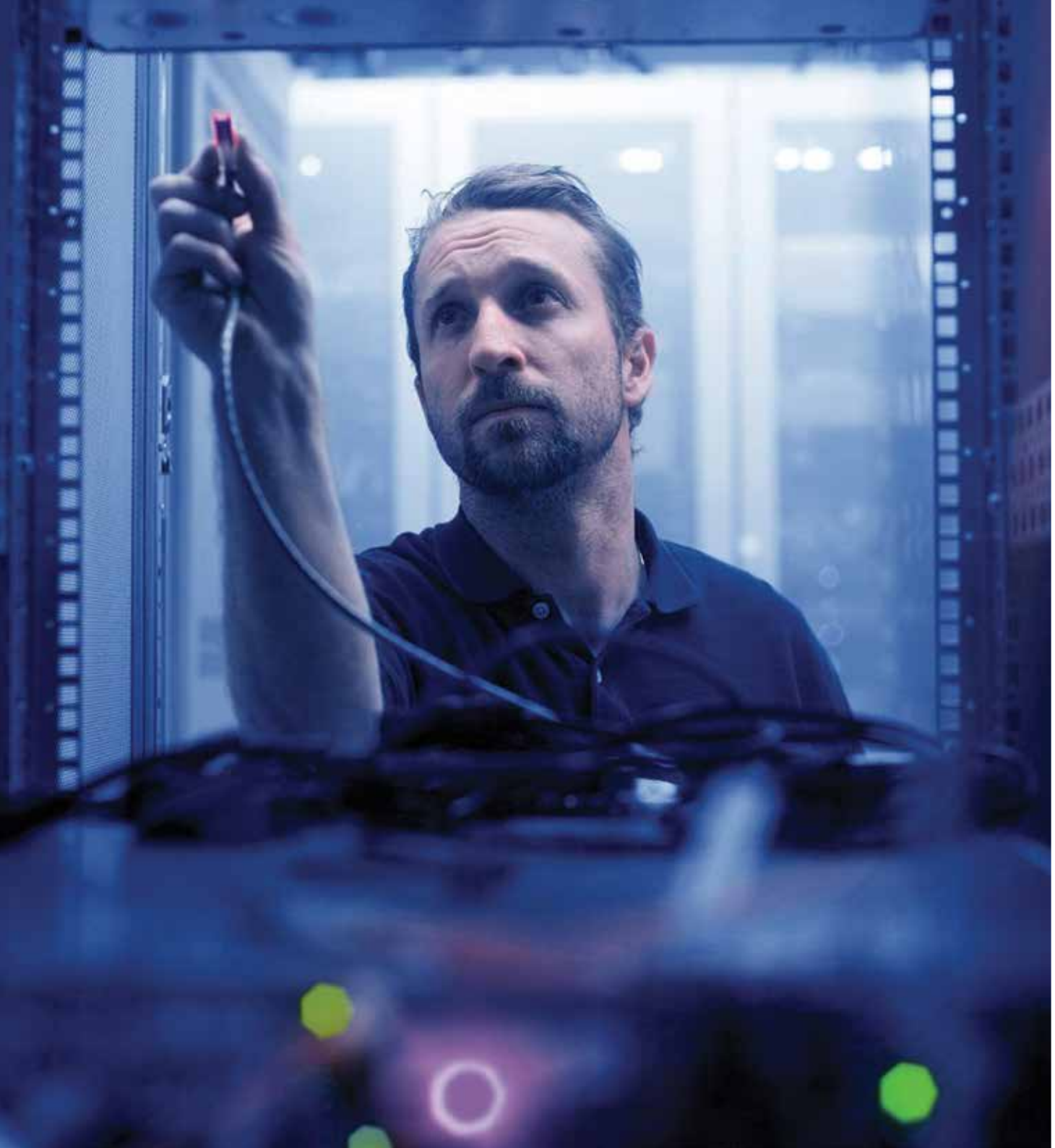
Versteckte Ransomware

Ransomware bleibt häufig auch von Firewalls unerkannt, die keinen SSL-verschlüsselten Webverkehr entschlüsseln und prüfen können. Veraltete Netzwerksicherheitslösungen sind gewöhnlich nicht in der Lage, SSL-/TLS-verschlüsselten Verkehr zu prüfen, oder haben eine so schwache Performance, dass sie bei einer Durchführung der Prüfung unbrauchbar werden. Immer mehr Cyberkriminelle haben gelernt, wie sie Malware in verschlüsseltem Verkehr verstecken können.

Die Verschlüsselung mittels Secure Sockets Layer bzw. Transport Layer Security (SSL/TLS) wird immer beliebter, sodass allein 2015[3] mindestens 900 Millionen Nutzer unbemerkt Hacking-Angriffen zum Opfer gefallen sind.



3 2016 SonicWall Annual Threat Report



Fazit

Mit SonicWall können Sie alle Identitäten effizient verwalten und sämtliche Datenpakete genau durchleuchten, um die Sicherheit in Ihrer Organisation zu verbessern. Egal wo sich Ihre Daten befinden, wir schützen sie überall und nutzen weltweit vernetzte Informationen, um Sie gegen eine Vielzahl an Bedrohungen wie Ransomware zu wappnen.

Besuchen Sie die SonicWall-Webseite für Netzwerksicherheitsprodukte.

SONICWALL®

Über uns

Seit über 25 Jahren ist SonicWall als zuverlässiger Sicherheitspartner bekannt. Von Access Security über Netzwerksicherheit bis zu Email Security: Wir haben unser Produktportfolio kontinuierlich weiterentwickelt, damit unsere Kunden Innovationen realisieren, Prozesse beschleunigen und wachsen können. Mit über einer Million Sicherheitsgeräte in nahezu 200 Ländern und Regionen weltweit bietet SonicWall seinen Kunden alles, was sie brauchen, um für die Zukunft gerüstet zu sein.

Wenden Sie sich bei Fragen zu den Nutzungsmöglichkeiten dieses Materials an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Informationen zu regionalen und internationalen Niederlassungen finden Sie auf unserer Website.
www.sonicwall.com

Ebook-NS-Ransomware-EU-IMAG-29223 -D1

SONICWALL®