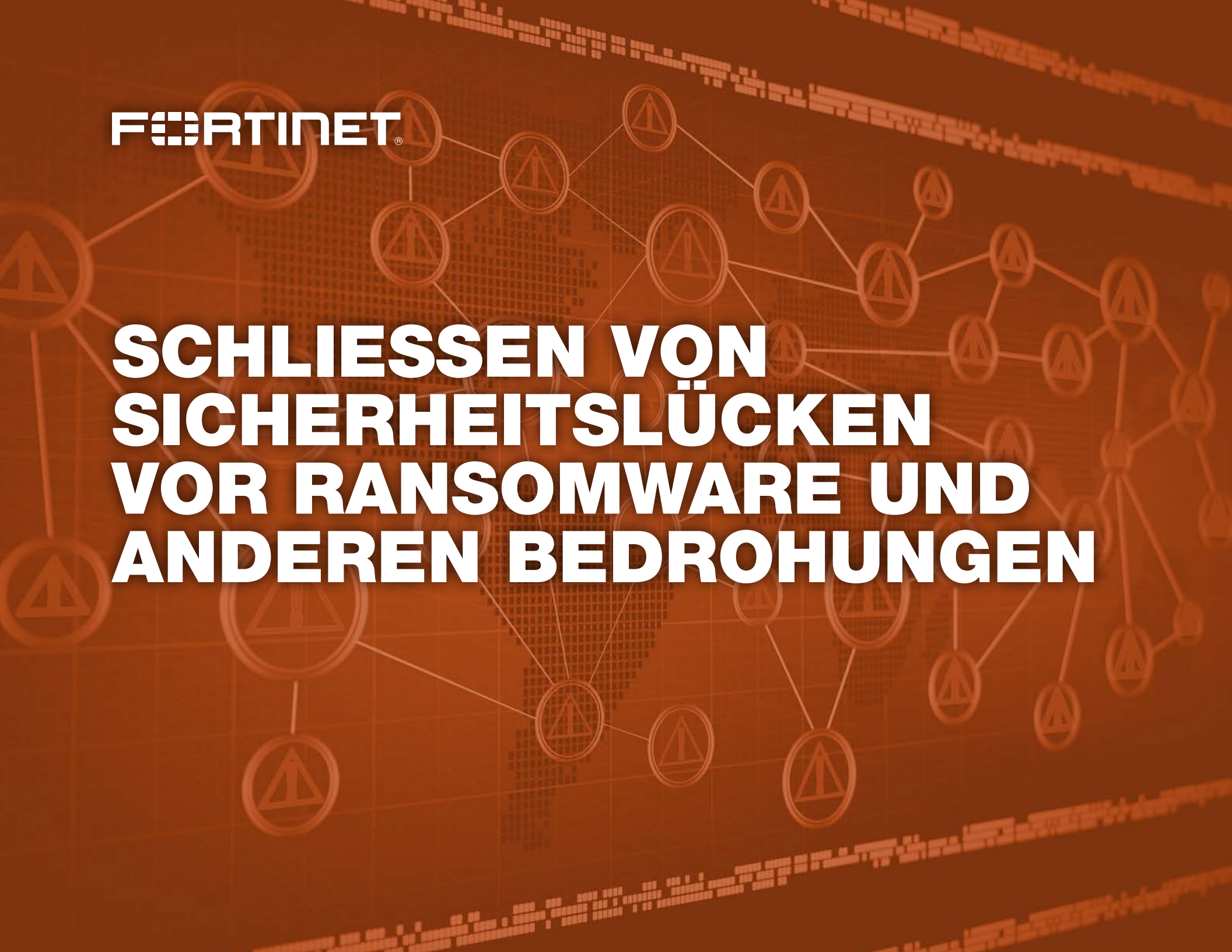


SCHLIESSEN VON SICHERHEITSLÜCKEN VOR RANSOMWARE UND ANDEREN BEDROHUNGEN

INHALT

EINLEITUNG

Es wird von Tag zu Tag schwieriger, ein Unternehmen vor Ransomware und anderen Cyber-Bedrohungen zu schützen. Vor nicht allzu langer Zeit hatten Netzwerke noch eine gut definierte Außengrenze, die es zu schützen galt. Die zunehmende Ausbreitung des Internet der Dinge (IoT), mobile Geräte und BYOD sowie der Übergang zu öffentlichen und privaten Cloud-Services haben zur Schaffung einer wesentlich vielfältigeren und dynamischeren Angriffsfläche geführt.

Doch damit nicht genug. Die heutige Bedrohungslandschaft entwickelt sich sowohl, was das Volumen angeht, als auch hinsichtlich der Komplexität der Angriffe immer weiter. Cyber-Kriminalität hat sich zu einem „Big Business“ mit spektakulären jährlichen Umsätzen entwickelt. Nur ein Beispiel: Ransomware präsentierte sich 2016 explosionsartig auf dem Markt und schaffte es regelmäßig in die Top-5 der wöchentlichen Malware-Liste der FortiGuard Labs und kostete Unternehmen geschätzte 850 Millionen USD an Lösegeldzahlungen. Und diese Zahl enthält nicht einmal die zusätzlichen Kosten der damit verbundenen Ausfallzeiten oder der Auswirkungen der negativen Schlagzeilen auf die betroffene Marke. Großen Anteil an dieser explosionsartigen Verbreitung hat der hohe Entwicklungsstand des Ökosystems der Cyber-Kriminalität, wie durch die Zunahme der Ransomware-as-a-Service- und Ransomware-Partner-Programme belegt wird.[1] Unternehmen müssen angemessene Schutzmechanismen für die gesamte Angriffsfläche sicherstellen.

[1] http://blog.fortinet.com/2017/02/16/ransomware-as-a-service-rampant-in-the-underground-black-market

01 E-MAIL-ANGRIFFE

Spam ist heutzutage Ihre kleinste Sorge, was Ihren Posteingang angeht. Von Phishing-Betrügereien über Malware-Anhänge und Links bis hin zu einer stetig zunehmenden Welle von Ransomware-Angriffen – E-Mails sind schon seit geraumer Zeit ein beliebter Angriffsvektor von Cyber-Kriminellen. Sie werden zudem häufig als erste Stufe für komplexe Bedrohungen genutzt. Branchenquellen schätzen, dass 66 % der Malware, die zu Incidents führt, per E-Mail installiert wird, und 97 % der Ransomware im Jahr 2016 auf diese Weise übertragen wurden.

Während E-Mail-Sicherheit gesättigt und gereift ist, stellen Analysten fest, dass eines der vorrangigen Kriterien zur Differenzierung sicherer E-Mail-Gateways die Fähigkeit des Schutzes vor komplexen und gezielten Bedrohungen ist. Falls Sie Ihre Sicherheitsmaßnahmen in diesem Bereich in den vergangenen 12 bis 18 Monaten nicht überprüft haben, wäre es sicher sinnvoll, sie genauer unter die Lupe zu nehmen. Zusätzlich zu gezielten Angriffen und ausgeklügeltem Social Engineering von Bedrohungen, die Geschäfts-E-Mails gefährden, gibt es eine Vielzahl von immer neuen Verschleierungstaktiken (wie zum Beispiel verschlüsselte

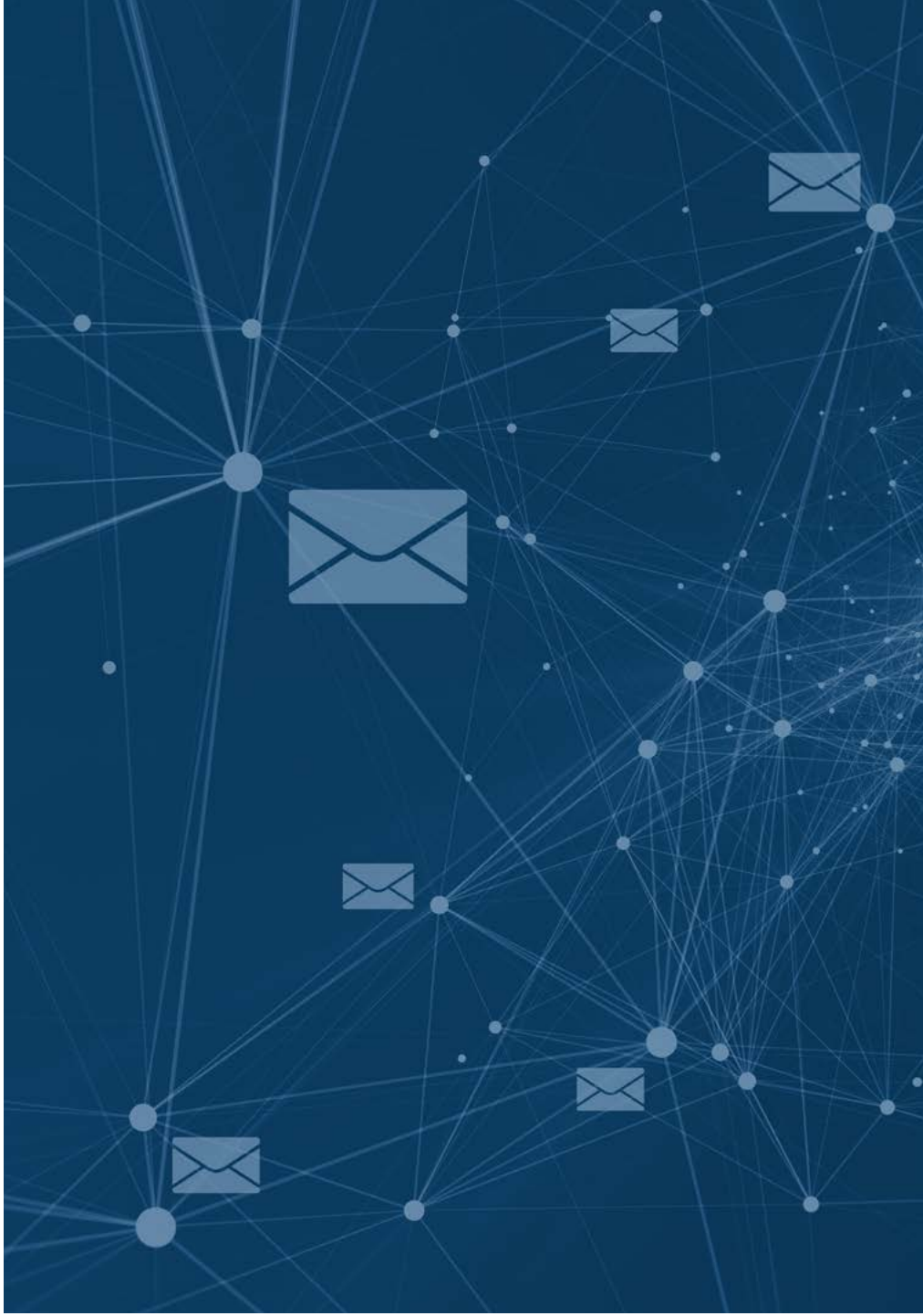
Schadensroutinen, die einen Entschlüsselungscode erfordern). Sicherheitsteams müssen gewährleisten, dass ihre E-Mail-Sicherheit routinemäßig aktualisiert wird, um den jeweils neuesten Techniken von Cyber-Kriminellen entgegenzutreten.

Erschwerend kommt hinzu, dass sich diese Bedrohungen sehr schnell weiterentwickeln. Eine Prüfung muss daher in der Lage sein, sowohl bekannte als auch Zero-Day-Infektionen zu erkennen. Neuere Technologien wie die Sandbox-Analyse werden hinzugefügt, um E-Mail-Gateways zu sichern und herkömmliche Verteidigungstechniken zu unterstützen.

Da E-Mails zu einem unerlässlichen und universellen Kommunikationsinstrument geworden sind, muss ihr Schutz für alle Unternehmen höchste Priorität haben – unabhängig von Größe oder Branche.

***Wussten Sie schon, dass...**

- **97 %** der Phishing-E-Mails nun **Ransomware übertragen?**
- E-Mails 2016 laut Verizon das Übertragungswerkzeug für **zwei Drittel der installierten Malware waren**?
- ein **einzelner Klick** zum größten Datendiebstahl der Geschichte führte?[2]



[2] http://thehackernews.com/2017/03/yahoo-data-breach-hack.html

02 WEBBASIERTE EXPLOITS (NETZWERK/INTERNET)

Aufgrund funktionaler Notwendigkeiten sind Unternehmensnetzwerke zu komplexen Ungetümen geworden. Die heutigen Netzwerke sind dank Trends wie immer größeren Mobilitätsanforderungen, der Verbreitung von IoT-Geräten und der Einführung von privaten/öffentlichen Cloud-Services (z. B. Amazon Web Services und Microsoft Azure) größer und zunehmend grenzenlos. Die ständig wachsende Ausbreitung und Komplexität dieser Infrastrukturen macht es immer schwerer, sie gegen Angriffe von außen zu verteidigen.

SaaS-basierte INFEKTIONEN

In einer kürzlich durchgeführten Umfrage haben IT-Experten Web-Anwendungen genannt, bei denen sie bereits Infektionen durch Ransomware gesehen haben:

- Dropbox – 70 %
- Microsoft Office 365 – 29 %
- Google Apps – 12 %
- Box – 6 %
- Salesforce – 3 %

Bei einer expandierenden, zunehmend durchlässigen und potenziell überwindbaren Netzwerkgrenze stellt sich die Aufgabe, die Netzwerksicherheit so zu gestalten, dass sie einem derartigen dynamischen und sich ständig ändernden Perimeter folgen kann. Und da Cyber-Kriminelle die webbasierten Exploits zur Installation von Malware, einschließlich Ransomware, kontinuierlich ändern, ist eine starke Bedrohungsabwehr gegen diesen Angriffsvektor unentbehrlich. Neben der E-Mail sind Drive-by-Downloads über das Internet eine häufig genutzte Methode zur Verbreitung von Ransomware, wie von FortiGuard Labs berichtet wird.[3] Die Verwendung des Internets zum Hosten von Malware erlaubt es Angreifern, ihre Schadensroutinen im Handumdrehen zu ändern.

[3] https://blog.fortinet.com/2016/04/06/10-steps-for-protecting-yourself-from-ransomware

Moderne Unternehmen müssen tiefergehende Überprüfungen einsetzen – wie zum Beispiel Firewalls der nächsten Generation, Netzwerk-Sandboxes und noch ausgeklügeltere Tools wie Netzwerk-Verhaltensanalysen und Täuschungsinfrastruktur. Zusammen mit E-Mail können starke Schutzmechanismen für das Internet 99 % der Malware daran hindern, in das Netzwerk zu gelangen. Dabei ist jedoch zu beachten, dass durch zusätzliche Schutzmethoden die Netzwerksicherheit auch komplexer und zunehmend schwieriger zu koordinieren und zu verwalten ist.

***Wussten Sie schon, dass...**

- durchschnittlich **zwei Drittel** des gesamten Datenverkehrs im Netzwerk **verschlüsselt sind**?
- die Netzwerkebene laut Verizon **3 der 5 wichtigsten Vektoren** für Cyber-Kriminalität umfasst?
- **87 %** der CIOs der Meinung sind, dass SSL-Verschlüsselung ihr Unternehmen einem größeren Risiko aussetzt?
- das durchschnittliche Unternehmen **30 unterschiedliche Cloud-Dienste nutzt**?

03 UNGESCHÜTZTE WEB-ANWENDUNGEN

Ungeschützte Web-Anwendungen sind der einfachste Zugangspunkt für Hacker, da sie gegenüber verschiedenen Arten von Angriffen anfällig sind. Die Verwendung von Websites, webbasierten Anwendungen und Infrastruktur-Tools (sowohl lokal als auch als IaaS-Formular) sind gut dokumentierte Schwachstellen, die in der Vergangenheit zu Datendiebstählen geführt haben. Angreifer nutzen diese Schwachstellen (über XSS, SQL-Injection usw.) aus, um Zugang zu Netzwerken zu erhalten.

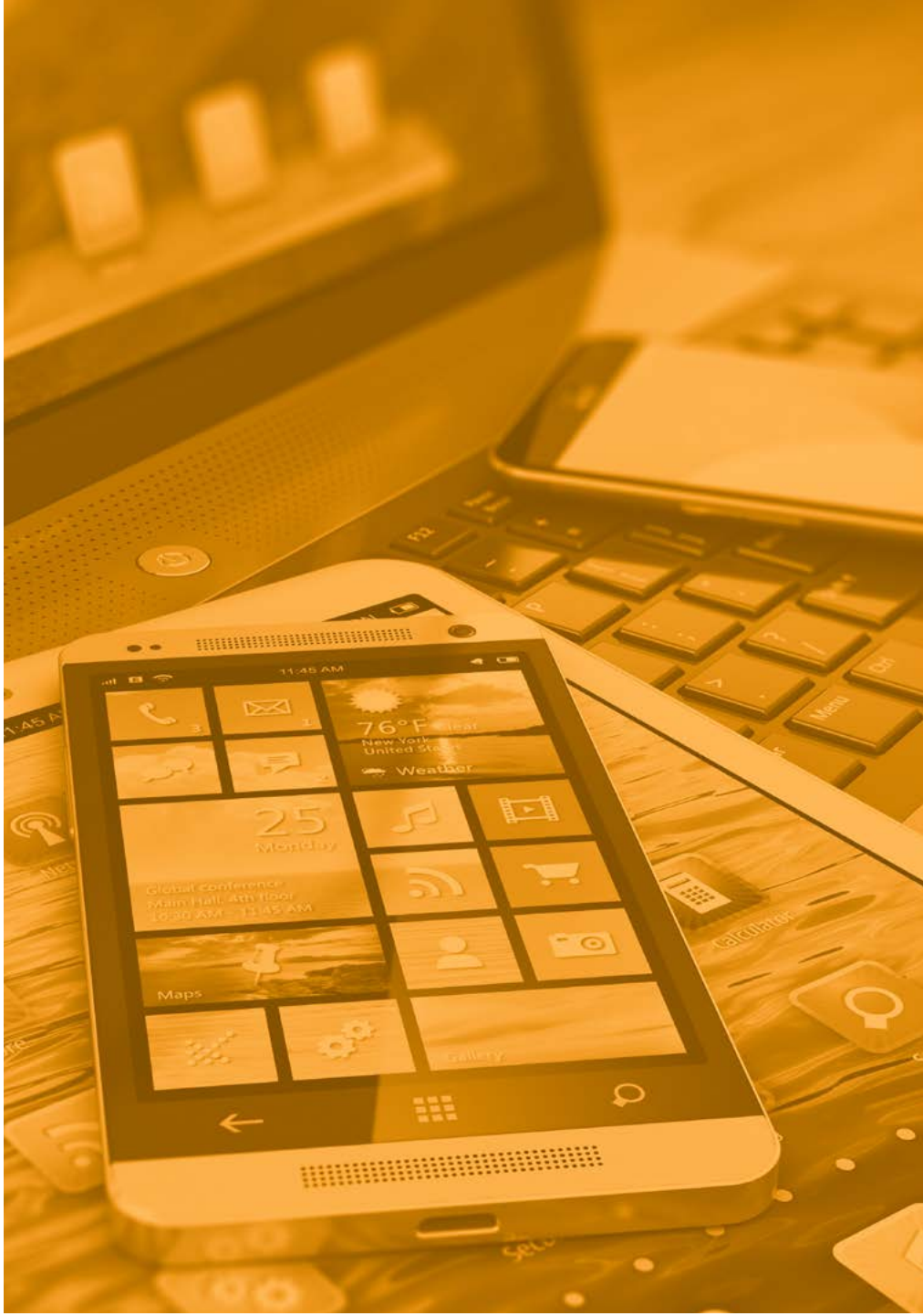
Das Jahr 2017 begann mit der FortiGuard Labs-Veröffentlichung von bedeutenden Schwachstellen in einem weit verbreiteten Open Source-Code, der u. a. von WordPress, Drupal und Joomla verwendet wird.[4] Darauf folgte die Veröffentlichung von Schwachstellen in der Apache-Internet-Infrastruktur und anderen. Cyber-Kriminelle können die anfällige Internet-Infrastruktur für viele Zwecke nutzen, wie etwa, um Zugang zum Netzwerk zu erhalten und sich darin zu bewegen, oder um Informationen aus Backend-Datenbanken zu stehlen. 2016 gab es außerdem Fälle, bei denen Websites zum Zwecke von Lösegeldforderungen verschlüsselt wurden.[5]

[4] http://blog.fortinet.com/2017/01/05/analysis-of-phpmailer-remote-code-execution-vulnerability-cve-2016-10033
[5] http://sensorstechforum.com/drupal-ransomware-uses-sql-injection-lock-drupal-websites/

Unternehmen mit umfassenden oder kritischen webbasierten Systemen – insbesondere solche, die öffentlich genutzt werden – sollten diesen Angriffsvektor mittels Web Application Firewall und Network-Sandbox schließen und zudem während der Entwicklung strenge Code-Prüfungen durchführen. Dies gilt für alle E-Commerce-Unternehmen, Behörden (z. B. Finanzämter) und Personaldienstleister.

***Wussten Sie schon, dass...**

- Angriffe auf Web-Anwendungen die **vorrangige Quelle** für Datendiebstähle sind?[6]
- eine Reihe von Angriffs-Incidents sowohl in **Apache als auch in WordPress** Schwachstellen enthüllt haben?
- die **Finanz- und IT-Branche sowie öffentliche Behörden** 2016 besonders hart von Angriffen auf Web-Anwendungen getroffen wurden?



[6] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

04 SCHWACHSTELLEN AM ENDGERÄT

Cyber-Kriminelle versuchen ständig, Schwächen in der Angriffsfläche eines Unternehmens zu finden und auszunutzen. Das eigentliche Ziel sind jedoch Endgeräte, da auf ihnen Daten gespeichert werden. Für ihre Absicherungist daher, zusätzlich zu den Schutzmaßnahmen für alle anderen Angriffsvektoren, eine letzte Verteidigungslinie erforderlich.

Endbenutzer können selbst die Quelle einer Reihe von Endgerät-Schwachstellen sein, die nur schwer zu verteidigen sind. Personen lassen sich häufig von raffinierter Social-Engineering-Malware täuschen. Derartige Angriffe ändern ihre Taktiken ständig, um einen kurzen Moment der Fehleinschätzung oder einen falschen Klick auszunutzen.

Die Vielzahl von unterschiedlichen Geräten, die Endbenutzer mit dem Netzwerk verbinden, birgt auch Sicherheitsprobleme. Die meisten Mitarbeiter brauchen sowohl innerhalb als auch außerhalb des Betriebs Zugriff auf das Unternehmensnetzwerk. Datenschutzrichtlinien des Unternehmens müssen jedoch zu jeder Zeit durchgesetzt werden, um diese Endgeräte so sicher wie möglich zu machen.

Der Schutz Ihrer Endgeräte vor komplexen Bedrohungen auf unzähligen Geräten kann eine große Herausforderung darstellen:

- Endgeräte, die Daten speichern, werden nicht immer korrekt identifiziert und gesichert.

- Kritische Endgerätsysteme bleiben häufig aus Gründen der Verfügbarkeit unbehelligt – zum Nachteil der Sicherheit.
- Eine abnehmende Anzahl von Endbenutzergeräten entspricht aufgrund von BYOD, der Beschäftigung von externen Mitarbeitern usw. dem Unternehmensstandard.
- Die schiere Anzahl von verbundenen Geräten, die alle geschützt werden müssen, kann erdrückend sein.
- Die meisten Geräte sind gelegentlich ungeschützt, wenn außerhalb des Unternehmensnetzwerks auf das öffentliche Internet zugegriffen wird.

So schwierig es auch sein kann, dies ist die letzte und in einigen Fällen auch die einzige Verteidigungslinie, und genau deshalb sind moderne Schutzmaßnahmen unerlässlich.

***Wussten Sie schon, dass...**

- 2016 **850 Mio. US-Dollar** Lösegeld gezahlt wurden, um verschlüsselte Systeme wiederherzustellen?
- Ransomware **30–50 Tsd.** Geräte pro Monat infiziert?
- Unternehmen durchschnittlich **vier aktive Malware-Schadprogramme/Bots haben**?

FAZIT

Wie Gartner vor Kurzem feststellte: „Alle Unternehmen müssen jetzt davon ausgehen, dass sie kontinuierlich gefährdet sind.“[7] Und die oben beschriebenen Daten zu Ransomware, Lösegeldforderungen/-zahlungen und anderen Incidents belegen klar, warum. Unternehmen sollten daher ihre Schutz-, Erkennungs- und Abwehrmechanismen im Rahmen ihrer breiteren Sicherheitsstrategie aktiv verbessern.

Der effektive Schutz Ihres Unternehmens beginnt mit der Abdeckung all dieser unterschiedlichen Angriffsvektoren durch koordinierte Advanced Threat Protection (ATP). Die Schutzmechanismen müssen in der Lage sein, Datenverkehr, Objekte und Benutzeraktivität auf dem Endgerät (einschließlich IoT) zu prüfen und auf äußere und zentrale Netzwerkschichten bis hin zu Anwendungen und zur Public Cloud zuzugreifen – ohne dabei Geschäftsabläufe zu verlangsamen. Die Schutzmechanismen müssen die gesamte Angriffsfläche abdecken.

[7] http://www.gartner.com/smarterwithgartner/security-at-the-speed-of-digital-business/

Außerdem ist es unerlässlich, leistungsstarke Sicherheitskomponenten einzusetzen, die globale Bedrohungsdaten (die von einem Forschungslabor außerhalb des Unternehmens erkannt werden) sowie lokale Sicherheitsdaten (dazu, was in Echtzeit innerhalb des Unternehmens passiert) teilen. Dies ermöglicht es ihnen, als ein einheitliches, kohärentes System zu arbeiten.

Wenn Komponenten unabhängig voneinander agieren, entstehen Lücken, durch die Cyber-Kriminelle eindringen, und isolierte Bereiche, die Antwort- und Abwehrzeiten verlangsamen. Die Automatisierung aller bereitgestellten Komponenten bildet die stärkste und einheitlichste Verteidigung.

Das Implementieren einer nahtlosen, konsistenten End-to-End-Sicherheitsstrategie für Advanced Threat Protection, selbst über Komponenten verschiedener Hersteller hinweg, stellt den erfolgversprechendsten Ansatz gegen komplexe Bedrohungen dar, die die gesamte Angriffsfläche moderner Unternehmen abdecken.

FORTINET®

www.fortinet.com