Schwachstellen und Sicherheitsgrundlagen – Lücken im Sicherheitssystem könnten Sie 2017 teuer zu stehen kommen

Bedrohungsprognosebericht des Fujitsu Security Operations Centre

shapingtomorrow withyou

FUJITSU

Inhalt

Einleitung

» In der Welt der Cybersicherheit ist das Zurückblicken genauso wichtig wie das Vorausschauen. Wir müssen die gelernten Lektionen der Vergangenheit Revue passieren lassen, um uns auf die Bedrohungen der Zukunft vorzubereiten.

In diesem Sinne schaut dieser Bericht auf unsere Vorhersagen für 2016 zurück und darauf, wie genau sie mit den tatsächlichen Ereignissen übereingestimmt haben. Darüber hinaus möchten wir auch einige Gedanken zu dem vorausschicken, was uns 2017 erwartet.

Ich hoffe daher, dass Ihrem Unternehmen dieser Bericht nicht nur als brauchbarer Rückblick dient, sondern auch einen Ausblick darauf bieten wird, was noch kommt, damit Ihr Geschäft weiterhin ausreichend geschützt ist.«

Rob Norris
Head of Enterprise Cyber Security, EMEIA

Wie zutreffend waren unsere Vorhersagen für 2016?

Wir haben prognostiziert, dass die Anzahl der schwerwiegenden DDoS-Angriffe aufgrund der weiteren Zunahme des Internets der Dinge (IoT) steigen würde. Einige große Konzerne waren 2016 von DDoS-Angriffen über IoT-Botnetze betroffen, die auch digitale Videorekorder (DVR) und Videoüberwachungskameras einschlossen. Die Angriffe haben Dynamisches DNS in Mitleidenschaft gezogen, wodurch die Verbindung zu Online-Diensten wie Spotify, Twitter, GitHub, PayPal, u. a. im Oktober unterbrochen wurde. KrebsOnSecurity* wurde ebenfalls Opfer einer der größten Angriffe, die bislang verzeichnet wurden.
Wir haben auch angedeutet, dass Angriffe auf Web-Apps zunehmen würden und leider waren viele dieser Angriffe weiterhin erfolgreich, wie die SQL-Injection-Angriffe Anfang des Jahres 2016, denen das russische Social Media-Unternehmen VK und die Qatar National Bank zum Opfer fielen.

Ziel der Angriffe sind nach wie vor wichtige Unternehmensdaten. Universitäten und Anwaltskanzleien waren 2016 beliebte Angriffsziele, wobei die zwei Haupttaktiken im Diebstahl von Daten oder der Verwendung von Ransomware bestanden. Die Universität von Calgary räumte ein, dass sie 20.000 US-Dollar bezahlt hat, um von Ransomware befallene Dateien zu entschlüsseln.

Wir prognostizierten auch einen Anstieg der Biometrie. Fujitsu entwickelt weiterhin einige der weltweit führenden Biometrie-Technologien und viele Anbieter suchen jetzt nach Wegen, um Ihre Hardware-Anwendungen zu verbessern. Apple verwendete einige Zeit die Fingerabdruckbiometrie für sein iPhone und führte dieses Verfahren 2016 letztendlich auch für seine Macbooks ein, kurz nachdem das US National Institute of Standards and Technology (NIST) angekündigt hatte, dass es SMS als Alternativmethode der Zwei-Faktor-Authentifizierung nicht länger unterstützen würde.

Auch sagten wir voraus, dass Flash-Player als Opfer von Angreifern, die mit Exploit-Kits arbeiten, weiterhin im Rampenlicht stehen würde. Unsere Annahmen über diese Anwendung waren korrekt, denn die wichtigsten Browser entfernten Flash als Standardeinstellung während YouTube standardmäßig zu HTML5 wechselte.

Außerdem sollten wir auch Recht behalten, dass persönliche Daten zunehmend im Zentrum von Cyberangriffen stehen würden. Die UK National Lottery war eines der Opfer solcher Angriffe. 26.500 Spielerkonten wurden gehackt und es wurde auf Informationen wie Geburtstage und Kartendetails zugegriffen.

Wir sind fest davon überzeugt, dass sich Unternehmen auch 2017 für weitere Herausforderungen beim Thema Cybersicherheit wappnen müssen. Auf den folgenden Seiten werden unsere Top-10-Prognosen vorgestellt.

* Brian Krebs ist ein renomierter amerikanischer Journalist und Experte zum Thema Security und Cyberkriminaltät mit einem täglichen blog auf der Website KrebsOnSecurity.com

Fujitsu's Top-10-Cybersicherheitsprognosen für 2017

1

Viele Unternehmen werden weiterhin eine Sicherheitslücke haben

Wir sind davon ausgegangen, dass die Angriffe auch 2017 erfolgreich sein werden, da Unternehmen die Sicherheitslücke, die dadurch entsteht, dass Angriffe über verschlüsselte Kanäle aufgrund der fehlenden Kapazitäten von SSL-Inspektionen nicht als solche erkannt werden, immer noch nicht geschlossen haben. 2016 erlebten wir auch einen großen Anstieg von Angriffen gegen Unternehmen, die Microsoft PowerShell verwenden.
PowerShell ist ein Framework und eine Skriptsprache, die standardmäßig auf allen Windows-Computern installiert ist. Dieses Programm wird von Angreifern verwendet, da viele Unternehmen nicht ausreichend vor dem schädlichen Gebrauch der Anwendung geschützt sind. Da sie bereits Teil des Windows-Systems ist, ist es für Angreifer leichter, sie als Teil ihres Angriffszyklus zu verwenden und schwer für diejenigen, die mit dem Schutz des Netzwerks betraut sind, die böswillige Nutzung festzustellen, sofern überhaupt eine Überwachung stattfindet. Tools wie PowerShell Empire, die häufig auch bei Penetrationstests verwendet werden, werden auch von Angreifern benutzt, um die Umgehung des Perimeters zu erleichtern, Hintertüren zu schaffen und das Netzwerk dann seitlich zu umgehen. Unternehmen werden ihre Überwachungskapazitäten und Protokollierungsstufen überdenken und herausfinden müssen, welche guten Skripts in ihren Netzwerken verwendet werden, um auf diese Weise in der Lage zu sein, Hacker-Angriffe nach Möglichkeit festzustellen.

2

Künstliche Intelligenz wird die Art der Analyse in Security Operations Centers (SOCs) ändern.

Da Unternehmen bestrebt sind, künstliche Intelligenz (KI) und maschinelle Lernfähigkeit zu verwenden, wird sich die Art und Weise, wie Unternehmen Sicherheitsvorfälle analysieren, 2017 verändern. Das Cybersicherheitsprinzip „what good looks like" steht seit Langem im Raum. Das Maschinenlernen ist eine Ausweitung des Konzepts, das sich Algorithmen bedient, um zu bestimmen, wie gutes Verhalten aussehen sollte, wie z.B. also bestimmte Systemaufrufe gemacht oder nicht gemacht werden sollten oder wie bestimmte Dateitypen zusammengesetzt werden, sodass alle Abweichungen davon als verdächtig klassifiziert werden sollte. Die Überwachung der Kernnetzwerke auf der Suche nach abweichendem Verhalten, wie z. B. große Transaktionen oder erste Versuche, Zugriff zu einer Datenbank zu erlangen, bedeuten eine Veränderung in der Herangehensweise der Security Operations Centres, die einen intelligenzbasierten Ansatz verfolgen müssen. Sie werden nicht länger auf erkannte bösartige Zugriffe mit einer Antivirus- oder Intrusion Detection-Warnmeldung reagieren oder diese filtern, sondern sie werden eine Alarmfunktion entwickeln müssen, die, basierend auf einem Maschinenlernalgorithmus, anzeigt, dass etwas Ungewöhnliches passiert ist. Ein weiterer Bereich, auf den wir uns 2017 konzentrieren müssen, ist die Tatsache, dass Angreifer sich derselben KI bedienen, wenn sie versuchen, Netzwerke und Sicherheitskontrollen zu Fall zu bringen.

3

Kriminelle werden es weiterhin auf Kernbankenanwendungen abgesehen haben.

Die Kernbankenanwendungen sind bereits 2016 Ziel dieser Angriffe geworden. Bei den größten Zugeständnissen internationaler Bankinstitute kam es zum direkten Diebstahl von Millionen von Dollar aufgrund von Schwachstellen im globalen SWIFT-Zahlungsnetzwerk. Beim größten Diebstahl handelt es sich um 81 Millionen US-Dollar, die aus einer Bank in Bangladesch entwendet wurden. Wir konnten auch eine Zunahme von Banking-Trojanern beobachten, die „Backoffice-Anwendungen" angegriffen und den Kriminellen auf diese Weise die Möglichkeit gegeben haben, Legacy-Technologien zu missbrauchen, um Finanzmittel direkt von den Banken zu stehlen. Wir sehen auch 2017 ein erhebliches Risiko für den Bankensektor. SWIFT hat 16 vorgeschriebene Kontrollen eingeführt und wird 2018 ihre Einhaltung bei den Banken überprüfen. Dennoch bietet das immer noch ein Gelegenheitsfenster für Cyberkriminelle. Wissenschaftler haben Ende 2016 den Odinaff-Trojaner entdeckt, der auf SWIFT abzielte, und für dieses Jahr werden neue Angriffsvarianten und -methoden erwartet.

4

Angreifer werden den Fokus vor allem auf den Mobilfunkmarkt richten.

Die verbesserte Sicherheit bei neuen Betriebssystemen und die zunehmende Verwendung von Smart-Geräten für persönliche und Geschäftsdaten machen mobile Plattformen 2017 zu einem noch beliebteren Angriffsziel. Viele Unternehmen machen jetzt ein Upgrade der Microsoft-Legacysysteme, die wegen ihrer Sicherheitslücken schon oft angegriffen wurden. Sie nutzen nun die Vorteile der verbesserten Sicherheitsfunktionen des in Windows 10 integrierten Edge-Browsers und der verbesserten Server-Betriebssysteme. Da Google Chrome seit Dezember 2016 HTML5 als Standardversion verwendet, werden kleine Apps, wie Adobe Flash, die auch oft angegriffen werden, vor allem von Exploit-Kits, jetzt auch aus den Unternehmensnetzwerken und Browseranbietern entfernt.

Einzelpersonen haben heutzutage mehrere Smart-Geräte, von denen viele dank moderner Speicherkapazitäten enorme Mengen an persönlichen und geschäftlichen Daten enthalten. Angreifer werden daher innovative Angriffsmethoden gegen mobile Plattformen mit mobiler Ransomware entwickeln, bei denen dann Zahlungen für die Rückgabe oder Entschlüsselung persönlicher Fotos verlangt werden. Das Mobile-Device-Management muss durch verlässliche Sicherheitskontrollen, vor allem für geschäftlich genutzte Geräte, ergänzt werden.

Hackers werden Smart Cities angreifen.

5

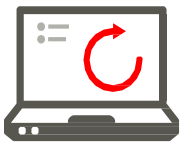
Da die Zahl der Internet-der-Dinge-Geräte exponentiell ansteigt, werden wir uns Sicherheitsfragen stellen müssen, an die wir bisher noch gar nicht gedacht hatten. Als ein Architekt die intelligenten Autobahnschilder entwarf, hat er nicht damit gerechnet, dass Hacktivists sie angreifen würden, um auf ihnen politisch motivierte Botschaften anstatt Warnhinweise für Autofahrer anzuzeigen. Dasselbe gilt für die IoT-Hersteller, die Hunderttausende von Videoüberwachungs-, DVR-Kameras und SoHo-Routern gebaut haben, aus denen jetzt das „Mirai"-Botnetz des IoT besteht.

Aus Mirai können wir einige Lektionen lernen, wie zum Beispiel das Vermeiden von fest programmierten Standard-Passwörtern. Viele der für intelligente, angeschlossene Geräte konzipierten Protokolle werden jedoch ihre eigenen potentiellen Schwachstellen und Anfälligkeiten haben, wie wir bei den Zyxel-Routern gesehen haben. 2017 wird es mehr von diesen Schwachstellen geben.

Angreifer haben diese Schwachstellen bereits zu ihrem Vorteil ausgenutzt, und während die Vorstellung, dass Ransomware eine ganze Stadt mit intelligenten, angeschlossenen Lichtern lahmlegt, vor 12 Monaten noch unwahrscheinlich und undurchführbar schien, so haben die jüngsten Ereignisse diese Wahrnehmung verändert.

Dabei geht es nicht nur um die potentiellen Schwachstellen von Smart-Geräten, sondern diese Plattformen müssen auch überwacht werden. Der Steuerungsorganisation dieser Kontroll-Plattformen kommt eine zentrale Bedeutung zu. Das schließt auch die Sicherheitskontrollen der Lieferkette mit ein, die für die Lieferung und Steuerung jedes einzelnen Teils dieser Smart City verantwortlich sind, die jetzt ans Netz geht. Wenn nur ein Glied der Lieferkette versagen muss, um die Plattform zu beeinträchtigen, die die Smart-Geräte steuert, dann können wir wohl mehr von solchen Angriffen erwarten. Angreifer werden vielleicht nicht versuchen, Schwachstellen in angeschlossenen Städten auszunutzen, aber sie könnten versuchen, Ransomware in einem kritischen Teil der Infrastruktur zu installieren.

6



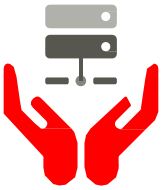
Widerstandsfähigkeit und Wiederherstellbarkeit werden danach die Geschäftsfaktoren sein, die den Unterschied machen.

Cyberangriffe sind mittlerweile so mächtig, dass sie auch die sichersten Unternehmen treffen könnten. 2017 stellt sich nur eine Frage – wie schnell lassen sie sich wiederherstellen?

Eine schnelle und vollständige Wiederherstellung erzeugt Sympathie und Respekt der Märkte, wohingegen eine schlechte Wiederherstellung Kritik und Rechtsstreitigkeiten nach sich zieht.

Ende November wurde die San Francisco Municipal Transportation Authority Opfer eines großen Ransomware-Angriffs. Dank eines verlässlichen Backup-Prozesses konnten aber die meisten Funktionen innerhalb eines Tages wiederhergestellt werden.

Nächstes Jahr werden wir die Unternehmen, die die Herausforderung ernst nehmen, an ihrer koordinierten Herangehensweise erkennen, die Schutz, Erkennung und Reaktion vereint.



7

Datenwiederherstellung wird für alle Unternehmen ein zentrales Anliegen sein, nicht nur für die mit hohem Datenaufkommen.

2017 wird es mehr Investoren, Gesellschafter und Behörden geben, die sichergehen wollen, dass vertrauliche Daten sorgfältig geschützt werden. Das wird auch im Rahmen der Datenschutz-Grundverordnung ganz besonders wichtig sein. Spezielle Data Loss Prevention (DLP)-Tools funktionieren gut, wenn sie richtig verwendet werden. Viele Unternehmen verfolgen bei DLP allerdings eine unsystematische Herangehensweise oder gehen davon aus, dass es schon ausreicht, ein DLP-Tool zu verwenden.

Unternehmen müssen die Risiken genau unter die Lupe nehmen, die wichtigsten Daten identifizieren, die geschützt werden müssen, und ihre Netzwerke sorgfältig überwachen. Sie werden auch die sensiblen Daten Dritter genauso sorgfältig schützen müssen wie ihre eigenen.

8

Globale Kunden werden die Überprüfung der Datensicherheit ihrer Lieferketten verlangen.

Die meisten Unternehmen wissen, dass ihre sensiblen Daten nicht nur intern gespeichert werden, sondern auch in ihrer Lieferkette. Oft besteht jedoch ein großer Unterschied zwischen dem, was Unternehmen von ihren Lieferanten erwarten, und dem, wozu die Lieferanten vertraglich verpflichtet sind.

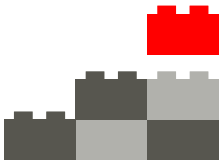
Mit steigendem Bewusstsein der Cyberrisiken suchen internationale Unternehmen nach klaren Beweisen für verlässliche Datensicherheit über professionelle Beratungsdienstleistungen. Sie umfassen Anwaltskanzleien, Buchhaltungsfirmen und Unternehmensberater. Die größten Kunden sind wegen ihrer einflussreichen Position in der Lage, verlässliche Datensicherheit zur Bedingung für die Zusammenarbeit mit diesen Beratern zu machen. Dieser Trend scheint sich auch 2017 und darüber hinaus fortzusetzen.

9

In Vorstandssitzungen wird die IT-Sicherheit zum Routinethema werden.

Mit so vielen Cyberangriffen gegen die wichtigsten Unternehmen können auch die technikfeindlichsten Geschäftsführer diese Angelegenheit nicht mehr ausschließlich der IT-Abteilung überlassen. 2017 wird das Jahr sein, in dem die Vorstände verstehen werden, wie unzureichende IT-Sicherheit Ihren Unternehmen schaden könnte.

Unternehmen müssen leitende IT-Angestellte schulen, um die Anforderungen des Vorstands zu verstehen und um IT-Angelegenheiten in einer Sprache zu erörtern, die verstanden wird.



10

Schlechte IT-Praktiken werden immer noch die am leichtesten vermeidbaren Schäden verursachen.

In den meisten Fällen werden die Cybersicherheitsprobleme von Unternehmen nicht durch neue Cyberangriffstechniken oder böswillige Insider verursacht. Eine erstaunlich große Zahl von Unternehmen machen die einfachsten – und dennoch überlebenswichtigen – Hausaufgaben nicht, um die Risiken zu reduzieren.

Sie haben keine effektive Methode, um Sicherheitslücken zu schließen, oder eine geeignete Bedrohungsanalyse. Sie haben kein Zutrittsverwaltungssystem, das nur die aktuellen Nutzer realitätsgetreu abbildet. Sie verwenden nicht das Zugangsprinzip der geringsten Rechte und handeln nicht nach den Ratschlägen, die sich aus Penetrationstests ergeben haben. Auf diese Weise sind sie unnötig anfällig für Datenverlust, Datendiebstahl oder die externe Störung ihrer Systeme.

Leider wird das 2017 genauso weitergehen, was bedeutet, dass die Vorfälle, die im kommenden Jahr Schlagzeilen machen werden, allesamt vermeidbar wären.

Es wird Angriffe geben. Sind Sie vorbereitet?

2017 wird es regelmäßig zu größer angelegten Sicherheitsverletzungen kommen. Davon werden Unternehmen aller wichtigen Geschäftssparten auf der ganzen Welt betroffen sein. Das schließt auch gut etablierte Mega-Unternehmen, große Regierungen und allseits bekannte Namen nicht aus. Manche werden Pech haben. Aber viele andere werden Opfer von Angriffen werden, die mit ein bisschen mehr Sorgfalt und Aufmerksamkeit hätten vermieden werden können.

Bitte besuchen Sie die Website www.fujitsu.com/de/security-services, ummehr darüber zu erfahren, wie Sie Ihr Unternehmen schützen können, und wie Fujitsu Sie dabei unterstützen kann, die sich ständig verändernden Bedrohungen der Cybersicherheitslandschaft besser unter Kontrolle zu haben.

shaping tomorrow with you

FUJITSU

FUJITSU

Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Strasse 8, 80807 München, Deutschland
Telefon: 00800 37210000*
Email: cic@ts.fujitsu.com
Web: www.fujitsu.com/de/security-services
20.03.2017 CEMEA&I DE

*verfügbar und kostenfrei aus allen Netzen in D/A/CH