



McAfee Labs Bedrohungsprognosen für 2017

November 2016



McAfee Labs stellt die wichtigsten Bedrohungen vor, die im nächsten Jahr erwartet werden.

Über McAfee Labs

McAfee Labs ist eine der weltweit führenden Quellen für Bedrohungsforschung sowie -daten und ein Vordenker in Bezug auf Cyber-Sicherheit. Dank der Daten von Millionen Sensoren für alle wichtigen Bedrohungsvektoren (Dateien, Web, Nachrichten und Netzwerke) bietet McAfee Labs Echtzeit-Bedrohungsdaten, wichtige Analysen und Expertenwissen für besseren Schutz und Risikominimierung.

McAfee ist jetzt ein Geschäftsbereich von Intel Security.

www.mcafee.com/de/mcafee-labs.aspx



McAfee Labs folgen

Einführung

Willkommen beim McAfee-Bericht zu den Bedrohungsprognosen für 2017. Wir haben den Bericht in zwei Bereiche aufgeteilt. Im ersten Teil gehen wir genauer auf drei wichtige Bereiche ein.

- Das erste Thema dieses Berichts sind schwer zu bewältigende Sicherheitsherausforderungen im Bereich der Cyber-Sicherheit sowie die ersten Bemühungen der Sicherheitsbranche, diese Herausforderungen anzugehen. Hierfür haben wir verschiedenste Vordenker bei Intel Security zusammengebracht, die sich über die ihrer Meinung nach größten Herausforderungen austauschten. Anschließend haben wir diese Herausforderungen gruppiert und abstrahiert. In diesem Artikel gehen wir auf die sechs größten Herausforderungen ein.
- In unserem nächsten Artikel sehen wir uns Cloud-Bedrohungen näher an. Elf Vordenker von Intel Security geben eine gemeinsame Prognose zu Cloud-Bedrohungen und entsprechenden Reaktionen in der Rechtsprechung sowie der Sicherheitsbranche in den nächsten zwei bis vier Jahren ab. Mit welchen Bedrohungen und Kompromittierungen rechnen wir? Wie werden sich geopolitische Fragen, Gesetzgebung und Regulierungsmaßnahmen auf diese Umgebung auswirken? Und welche Reaktionen sollten wir von den Anbietern von Cloud-Diensten und Sicherheitsprodukten erwarten?

- Unser letzter Schwerpunktartikel befasst sich mit Bedrohungen für das Internet der Dinge. Ebenso wie beim Artikel zu Cloud-Bedrohungen geben zehn Intel Security-Vordenker Prognosen zu Bedrohungen und Kompromittierungen, Gesetzen und Ländergrenzen sowie den Reaktionen der Anbieter ab.

Im zweiten Abschnitt formulieren wir konkrete Prognosen zu Bedrohungsaktivitäten im Jahr 2017. Unsere Vorhersagen für das nächste Jahr decken verschiedenste Bedrohungen ab, darunter Ransomware, Schwachstellen aller Art, die Nutzung von Bedrohungsdaten zur Verbesserung der Abwehr sowie Angriffe auf Mobilgeräte.

Der Bericht widmet sich unter anderem folgenden Themen:

- Wir sagen voraus, dass Ransomware Mitte des nächsten Jahres ihren Höhepunkt erreichen und danach langsam zurückgehen wird.
- Wir erläutern, warum der Austausch von Bedrohungsdaten 2017 große Fortschritte machen wird.
- Sie erfahren, warum die Branchen für physische und Cyber-Sicherheit enger zusammenarbeiten werden.
- Wir sagen voraus, dass Hacktivisten Privatsphäreprobleme für Verbraucher aufdecken werden, und erläutern, wie Gesetzgeber und Unternehmen reagieren dürften.
- Wir erklären, warum es beim Stilllegen von Cyber-Kriminellen mehr Zusammenarbeit zwischen Sicherheitsanbietern und Strafverfolgungsbehörden geben wird.
- Wir zeigen detailliert auf, warum Schwachstellen in den häufigsten Apps im Jahr 2017 weiterhin Probleme bereiten werden.
- Wir erläutern, wie der Umfang gefälschter Produkt-Rezensionen, „Likes“, Werbung, Sicherheitswarnungen usw. weiter zunehmen und das Vertrauen in das Internet verringern wird.
- Sie erfahren, warum Social-Engineering-Angriffe mit Machine Learning verbessert werden.

Wir hoffen, dass diese Themen wertvolle Informationen liefern, mit denen Sie Ihre kurzfristigen Pläne und langfristigen Strategien optimaler gestalten können.

Über unsere Threat-Report-Umfragen erhalten wir auch weiterhin wertvolle Rückmeldungen von unseren Lesern. Wenn Sie uns Ihre Meinung zu diesem Bericht zu Bedrohungsprognosen mitteilen möchten, klicken Sie bitte [hier](#), um eine kurze Umfrage auszufüllen, die Sie nur fünf Minuten kosten wird.

Ich wünsche Ihnen und Ihrer Familie eine schöne Weihnachtszeit.

Vincent Weafer, Vice President, McAfee Labs

Diesen Bericht teilen



Inhalt

Bedrohungsprognosen von McAfee Labs für 2017

Diese Vordenker waren an der Vorbereitung und Erstellung dieses Berichts beteiligt:

Jonathan Anderson
Yuriy Bulygin
Peter Bury
Torry Campbell
David Coffey
Carric Dooley
Brian Dye
Lynda Grindstaff
Barbara Kay
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Shishir Singh
Martin Stecher
Jamie Tischart
Ramnath Venugopalan
Lori Wigle
Candace Worley

Diese Bedrohungsprognosen für 2017 wurden recherchiert und verfasst von:

Christiaan Beek
Yuriy Bulygin
Douglas Frosst
Paula Greve
Jeannette Jarvis
Eric Peterson
Matthew Rosenquist
Fernando Ruiz
Craig Schmugar
Rick Simon
Bruce Snell
Dan Sommer
Bing Sun
Adam Wosotowsky

Schwer zu bewältigende Sicherheits Herausforderungen	5
Cloud – Bedrohungen, Vorschriften und die Reaktionen der Anbieter	11
IoT – Bedrohungen, Vorschriften und die Reaktionen der Anbieter	21
Prognosen für 2017	29
Ransomware geht in der zweiten Hälfte des Jahres 2017 zurück	30
Schwachstellen-Exploits unter Windows gehen zurück und legen auf anderen Plattformen zu	32
Hardware- und Firmware-Bedrohungen ein immer größeres Ziel für raffinierte Angreifer	35
„Dronejacking“ führt zu Bedrohungen am Himmel	37
Bedrohungen für Mobilgeräte umfassen Ransomware, Remote-Zugriffs-Tools und kompromittierte App-Märkte	39
IoT-Malware öffnet eine Hintertür ins Haus	40
Machine Learning beschleunigt Social-Engineering-Angriffe	42
Rasante Zunahme bei gefälschter Werbung und gekauften „Likes“ zerstört Vertrauen	44
Eskalation der Werbekriege fördert die Malware-Übertragung	49
Hacktivistinnen legen Datenschutzprobleme offen	50
Stilllegungen durch Strafverfolgungsbehörden werfen Cyber-Kriminalität zurück	52
Der Austausch von Bedrohungsdaten macht hervorragende Fortschritte	52
Cyber-Spionage: Sicherheitsbranche und Strafverfolgungsbehörden vereinen ihre Kräfte	54
Die Branchen für physische und Cyber-Sicherheit vereinen ihre Kräfte	55



Schwer zu bewältigende Sicherheitsherausforderungen

Feedback teilen



Schwer zu bewältigende Sicherheitsherausforderungen

McAfee Labs

Im Bereich der Sicherheit digitaler Informationen mangelt es nicht an Herausforderungen. Inkrementelle Veränderungen durch unsere Gegner lösen endlose Aktualisierungen und Patches aus. Große Software-Veröffentlichungen bringen nicht nur wichtige neue Funktionen, sondern auch unerwartete Schwachstellen mit sich. Auf die Erkennung neuer Exploits folgen dringende Benachrichtigungen und Fehlerkorrekturen.

Große, schwer zu lösende Probleme sind solche, die Grundlagenforschung, neue Produktkategorien, enormen Entwicklungszeitbedarf sowie -aufwand, ständiges Augenmerk und oft auch die Zusammenarbeit mehrerer Branchenteilnehmer erfordern. In diesem Artikel erörtern wir sechs dieser Herausforderungen.

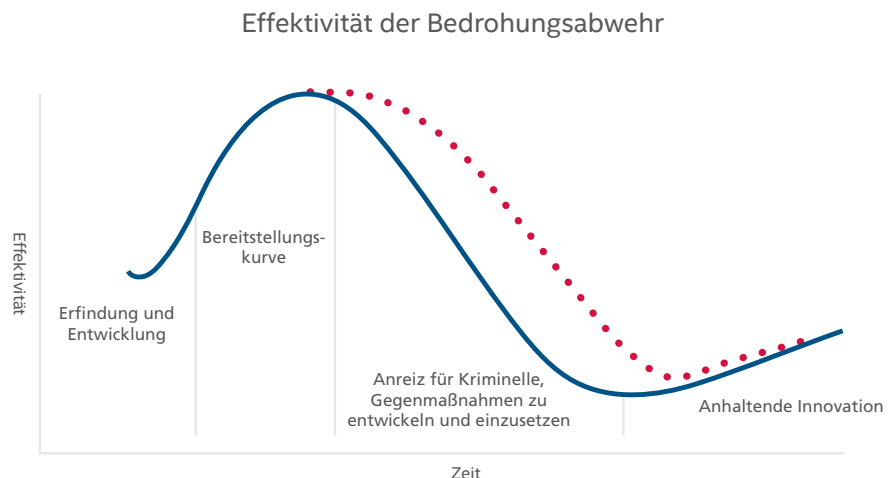
Dann sind da noch die großen, schwer zu lösenden Probleme. Dabei handelt es sich um die allgemeinen Probleme, die sich nicht mit Patches oder Software-Aktualisierungen aus der Welt schaffen lassen. Die Lösung dieser Probleme erfordert Grundlagenforschung, neue Produktkategorien, enormen Entwicklungszeitbedarf sowie -aufwand, ständiges Augenmerk und oft auch die Zusammenarbeit mehrerer Branchenteilnehmer.

In den letzten Jahren sind die herkömmlichen Schutzmethoden für digitale Informationen der zunehmenden Nutzung von Cloud-Diensten, der Aufweichung der Grenze zwischen internen und externen Netzwerken sowie der unglaublichen Flut neuer Geräte kaum noch gewachsen. In diesem Artikel werden sechs große Herausforderungen für die Sicherheitsbranche sowie Beispiele für entsprechende Maßnahmen der Branche besprochen.

Effektivität der Bedrohungsabwehr

Angriffe und Abwehrmaßnahmen befinden sich in einem ständigen Tanz aus Anpassung und Weiterentwicklung. Das folgende Diagramm veranschaulicht die typische Entwicklung einer Abwehrmaßnahme im Zeitverlauf. Die Effektivität neu entwickelter Techniken nimmt schnell zu, bis sie reif für die Bereitstellung sind. Nach der Bereitstellung wird die Effektivität durch den umfassenden Einsatz in realen Szenarien, Feedback an das Entwicklungsteam und die Integration in andere Abwehrmaßnahmen weiter verbessert. Dies setzt sich fort, bis ein Maß erreicht ist, das bei den Gegnern eine Reaktion auslöst. In dieser Phase finden Angreifer Wege, diese Abwehrmaßnahmen zu umgehen und durch Entwickeln von Gegenmaßnahmen deren Wert zu mindern.

Die Effektivität neu entwickelter Techniken nimmt schnell zu. Dies setzt sich fort, bis ein Maß erreicht ist, das bei den Gegnern eine Reaktion auslöst. Angreifer finden Wege zur Umgehung dieser Abwehrmaßnahmen und entwickeln Gegenmaßnahmen, um deren Wert zu mindern. Wir müssen die Effektivität der Bedrohungsabwehr verbessern, indem wir die Kurve nach oben und nach rechts verlagern.



Diesen Bericht teilen



Die Herausforderung für die Sicherheitsbranche besteht darin, den Kreislauf der Bedrohungsabwehreffektivität zu verbessern, indem sie die Kurve nach oben und nach rechts zu der gepunkteten roten Linie hin verlagern. Mit den folgenden Aktionen kann dieser Kreislauf beeinflusst werden:

- Verringern der Asymmetrie der Informationen zwischen uns und den Gegnern
- Erhöhen der Kosten oder Verringern der Bereicherungsmöglichkeiten von Angriffen
- Verbessern der Transparenz von Sicherheitsabläufen
- Identifizieren der Ausnutzung legitimer Tools und Anmeldeinformationen
- Schützen dezentralisierter Daten
- Agentenloses Erkennen und Schützen

Verringern der Asymmetrie der Informationen

Die Gegner verfügen über mehr Informationen zu unseren Abwehrmaßnahmen, als uns über ihre Angriffe vorliegen. Angriffe auf Sicherheitsmaßnahmen können gefahrlos getestet werden. Die meisten Tests bemerken wir nicht, sodass wir aus ihnen nichts lernen können. Wir müssen Wege finden, Angreifer an diesen Tests zu hindern, ihre Experimente zu erkennen, aus ihnen zu lernen und sie nach Möglichkeit in die Irre zu führen.

Die Gegner verfügen über mehr Informationen zu unseren Abwehrmaßnahmen, als uns über ihre Angriffe vorliegen. Diese Asymmetrie beeinflusst die Effektivitätskurve der Bedrohungsabwehr. Angriffe auf Sicherheitsmaßnahmen können gefahrlos getestet werden, sei es in mit unserer gesamten Produktpalette ausgestatteten Laboren oder in der Praxis anhand von bereitgestellten Systemen. Sie können uns testen, und wir bemerken es meistens nicht, sodass wir aus ihnen nichts lernen können. Können wir die Kurve zu unseren Gunsten verlagern, indem wir Wege finden, Angreifer an diesen Tests zu hindern, ihre Experimente zu erkennen, aus ihnen zu lernen und sie nach Möglichkeit in die Irre zu führen?

Diese Tests durch Angreifer zu verhindern, ist äußerst schwierig und möglicherweise nicht machbar. Ein wichtiger erster Schritt im Hinblick auf diese Asymmetrie ist der intensivere Austausch von Informationen zu Angriffen. Wenn wir Angriffsinformationen austauschen und zusammenführen, verstehen wir besser, auf welche Weise Angreifer nach Schwachstellen in unseren Algorithmen suchen. Dadurch können wir unsere Abwehrmaßnahmen schneller anpassen und verbessern.

Viel lernen können wir auch aus den zahlreicheren und detaillierteren Telemetriedaten, z. B. aus Cloud-Umgebungen, virtuellen Maschinen und IoT-Geräten. Wir lernen, die Datenwissenschaft auf diese Informationen anzuwenden, um Angriffsmuster besser erkennen und Angriffsindikatoren schneller entwickeln zu können. Außerdem erhalten wir die Möglichkeit, die Berechenbarkeit unserer Abwehrmaßnahmen zu ändern und damit den Gegnern das Identifizieren konkreter Schwachstellen zu erschweren. Dazu müssen verschiedene Abwehrschichten in Echtzeit koordiniert werden, damit Angriffe oder Tests, die eine Schicht durchdringen, von einer anderen gestoppt werden.

Erhöhen der Kosten oder Verringern der Bereicherungsmöglichkeiten von Angriffen

Die Untersuchung und strafrechtliche Verfolgung von Cyber-Kriminalität steht im umgekehrten Verhältnis zur Schwere der Verbrechen. Wir müssen die Wirtschaftlichkeit des Angriffsprozesses ändern, die Erfolgsrate von Angriffen verringern und die Ergreifungswahrscheinlichkeit für die Täter erhöhen, damit die Ziele weniger interessant werden.

Bei den meisten Cyber-Angriffen ist Geld das Hauptmotiv. Können wir die Kosten von Angriffen erhöhen oder ihre Rentabilität verringern? Wenn wir die Wirtschaftlichkeit des Angriffsprozesses ändern, die Erfolgsrate von Angriffen verringern und die Ergreifungswahrscheinlichkeit für die Täter erhöhen, werden die Ziele weniger interessant. Wir haben Strafverfolgungsdaten analysiert und sind zu dem Schluss gekommen, dass die Untersuchung und strafrechtliche Verfolgung von Cyber-Kriminalität im umgekehrten Verhältnis zur Schwere der Verbrechen steht. Bei physischen Verbrechen konzentriert sich die strafrechtliche Verfolgung vor allem auf die schwersten Verbrechen. Bei der Cyber-Kriminalität sind groß angelegte Angriffe schwer zu untersuchen und strafrechtlich zu verfolgen, da oft mehrere Rechtssysteme beteiligt und häufig mehr Kenntnisse

Diesen Bericht teilen



sowie Ressourcen erforderlich sind. Dadurch fällt es den Angreifern leichter, sich der Erkennung und der strafrechtlichen Verfolgung zu entziehen. Eine mögliche Reaktion besteht darin, die Angreifer zu täuschen, sodass sie mehr Zeit für einen bestimmten Angriff aufwenden und dadurch leichter ausfindig zu machen, zu identifizieren, zu ergreifen und strafrechtlich zu verfolgen sind.

Anbieter von Sicherheitsprodukten arbeiten inzwischen intensiver mit den Strafverfolgungsbehörden zusammen. Wir sammeln explizit Informationen, die den Gesetzesvollzug und die strafrechtliche Verfolgung unterstützen können. Inzwischen haben Sicherheitsunternehmen den Markt betreten, die sich auf Täuschungsmaßnahmen konzentrieren sowie sogenannte Honeypots einrichten, um Gegner anzulocken und sie so von wertvolleren Zielen abzulenken. Ähnlich wie bisherige Methoden der Strafverfolgungsbehörden, bei denen gekennzeichnete Geldscheine, Fahrzeugortung sowie andere Maßnahmen zur Verfolgung und Wiedererlangung eingesetzt wurden, nutzt Cyber-Sicherheit verstärkt digitale Köder, alarmgesicherte Dateien und andere nicht entfernbare Markierungen zum Auffinden von Angreifern.

Verbessern der Transparenz

Wir haben begrenzte Kontrolle über Informationsressourcen, und das Ausmaß dieser Kontrolle nimmt aufgrund der enormen Steigerung der Anzahl sowie Speicherorte der Ressourcen ab. Wir müssen Unternehmen dabei unterstützen, ihre Sicherheitstransparenz zu verbessern.

Zu oft erfahren Unternehmen erst nach einer Kompromittierung, wie gut ihre Ressourcen geschützt sind. Schatten-IT, alle Arten von Clouds und der Trend zu „Bring Your Own Device“ verschleiern die Effektivität der Sicherheitsabläufe weiter. Seit Jahrzehnten jagen Unternehmen dem Heiligen Gral der Identifizierung und Kontrolle über alle Unternehmensressourcen nach. In Wirklichkeit haben wir begrenzte Kontrolle über Informationsressourcen, und das Ausmaß dieser Kontrolle nimmt aufgrund der enormen Steigerung der Anzahl sowie Speicherorte der Ressourcen ab. Praktisch kein Unternehmen kann von sich sagen, die Speicherorte von Informationsressourcen sowie die Kontrolle über diese voll im Griff zu haben. Daher müssen wir Unternehmen dabei unterstützen, ihre Sicherheitstransparenz zu verbessern.

Die Sicherheitsabläufe in Unternehmen sowie die Anbieter von Sicherheitsprodukten verlagern ihren Schwerpunkt von IT-Ressourcen auf Datenressourcen und von „pseudoabsoluten“ Verteidigungsmaßnahmen auf durch Informationen gestützte Risikoverwaltung. Wir haben Tools, die Daten identifizieren und klassifizieren, ihre Verwendung überwachen, entsprechende Richtlinien anwenden oder bei Bedarf die Übertragung blockieren können. Mit diesen Tools können Unternehmen ihr Risikoprofil effektiver quantifizieren, kritische Lücken erkennen und Ressourcen gezielt einsetzen. Gute Unternehmen vergleichen Standardstatistiken mit dem Vormonat, ähnlich wie in der Buchhaltung. Bessere Unternehmen erstellen zu Vergleichszwecken regionale, nationale und branchenweite Benchmarks, ähnlich wie Investoren. Viele allgemeine Sicherheitskennzahlen bieten jedoch wenig praktischen Nutzen. Wir glauben, dass erheblich mehr notwendig ist, um nahezu in Echtzeit handeln zu können, wenn in einer geschützten Umgebung bedrohliche Aktivitäten beobachtet werden.

Identifizieren der Ausnutzung von Legitimität

Viele Angriffe beginnen mit der Verwendung gestohlener Anmeldeinformationen. Der Unterschied zwischen der Verwendung eines legitimen Tools zu einem legitimen Zweck und einer verdächtigen Aktivität ist sehr schwer zu erkennen. Wir benötigen ein Modell, bei dem die Legitimität jeder Transaktion getestet wird.

Viele Angriffe beginnen mit der Verwendung gestohlener Anmeldeinformationen, gefolgt von der Verwendung legitimer Verwaltung-Tools, die das Zielsystem ausforschen und Daten exfiltrieren. Herkömmliche Methoden zur Erkennung unzulässiger Aktivitäten durch Suchen nach böswilligen oder verdächtigen Objekten auf der Grundlage einer Dateisignatur oder anderer Kriterien eignen sich für dieses Szenario nicht. Die Objekte sind als harmlos bekannt, werden aber zu böswilligen Zwecken verwendet. Daher bleibt uns nur, den Zweck einer Aktion zu ermitteln. Handelt es sich um eine normale Anmeldung oder um einen Angriff? Wird Verschlüsselung für Datensicherheit oder zur Exfiltration genutzt? Wird eine bestimmte PowerShell-Sitzung von einem Administrator verwendet oder dient sie zur Ausspähung?

Diesen Bericht teilen



Der Unterschied zwischen der Verwendung eines legitimen Tools zu einem legitimen Zweck und einer verdächtigen Aktivität ist sehr schwer zu erkennen. Als einzige Methode steht uns hier die Verhaltensanalyse zur Verfügung, die in Bezug auf die Cyber-Sicherheit noch in den Kinderschuhen steckt. Damit ist ein guter Anfang gemacht. Wir müssen jedoch außerdem zu einem Modell übergehen, bei dem die Legitimität jeder Transaktion getestet wird, nicht nur die von Dateien und Anmeldeinformationen. Wir müssen Aktionen sowie Datenübertragungen analysieren und versuchen, die Absicht externer Akteure ebenso wie nicht autorisierter Insider zu ermitteln. Für diesen Schritt müssen wir sehr viel mehr über den Kontext der Aktivität wissen.

Eine kontrovers diskutierte Möglichkeit ist die Entwicklung von Benutzerreputation und prädiktiven Analysen. Bei diesem Konzept wird die Wahrscheinlichkeit bewertet, dass ein bestimmtes Konto kompromittiert, gestohlen oder für Aktivitäten nicht autorisierter Insider verwendet wird. Durch Erfassen des Benutzerverhaltens im jeweiligen Kontext, von der Tendenz zur Wiederverwendung von Kennwörtern auf verschiedenen Systemen bis zur Tätigkeitsbeschreibung und der typischen Arbeitszeit, können wir jede Aktion mit einem Satz erwarteter legitimer Aktivitäten vergleichen und diejenigen kennzeichnen, die eine bestimmte Risikostufe überschreiten. Hier handelt es sich um einen sensiblen Bereich. Bevor diese Technik allgemein eingesetzt wird, sind wichtige Fragen in Bezug auf Privatsphäre, Ethik und Gesetzmäßigkeit zu beantworten.

Schützen dezentralisierter Daten

Daten werden über die Unternehmensperipherie hinaus übertragen und dadurch deutlich anfälliger für unbeabsichtigte Kompromittierungen und gezielte Angriffe. Sie werden nicht nur in Clouds und auf persönliche Geräte, sondern auch an Partner, Lieferanten sowie Kunden übertragen. Wir müssen die Daten bei der Übertragung ebenso wie am Ziel besser schützen.

Daten werden über die Unternehmensperipherie hinaus übertragen und dadurch deutlich anfälliger für unbeabsichtigte Kompromittierungen und gezielte Angriffe. Sie werden in Clouds und auf persönliche Geräte sowie an Partner, Lieferanten sowie Kunden übertragen. Wie können wir die Daten bei der Übertragung ebenso wie am Ziel schützen? Weniger als 20 Prozent der Unternehmensdaten werden in diesem erweiterten Ökosystem übertragen, und doch sind 70 Prozent der Datenverluste mit dieser Übertragung verbunden. Einige versuchen heute, derartige Datenübertragungen zu schützen, indem sie Verschlüsselung verwenden und die Entschlüsselungsschlüssel in einer separaten E-Mail senden, um die Verantwortung für den Schutz an die nächste Person in der Kette weiterzureichen. Dadurch entsteht jedoch nur ein sehr kleiner Vertrauensbereich. Wir müssen herausfinden, wie wir diesen ausweiten und gleichzeitig besser kontrollieren können.

Systeme für Datenklassifizierung und Schutz vor Datenverlust stellen erste Bemühungen dar, den Vertrauensbereich zu verwalten und auf dezentralisierte Daten auszuweiten. Der nächste Schritt ist Sicherheit, die bei der Datenübertragung erhalten bleibt und dauerhafte Richtlinien erzwingt. Wir müssen in der Lage sein, die Daten bei der nächsten Verwendung zu schützen, ähnlich wie bei DRM-Mechanismen (Digital Rights Management).

Agentenloses Erkennen und Schützen

In Zukunft wird es oft nicht möglich sein, zu Schutzzwecken Agenten auf Geräten zu platzieren. Wir müssen andere Schutzmethoden finden.

In der Vergangenheit basierte unsere Stärke im Sicherheitsbereich zum großen Teil darauf, dass auf dem zu schützenden Gerät ein Agent ausgeführt wird. In Zukunft wird dies oft nicht möglich sein. Es gibt IoT-Geräte mit sehr wenig Speicher oder Rechenkapazität, aus Sicherheitsgründen geschlossener Betriebssysteme, eine rasant wachsende Zahl von Betriebssystemen sowie Gerätetypen, mit denen die Forschung und Entwicklung der Anbieter von Sicherheitsprodukten nicht Schritt halten kann, sowie Komponenten mit langem Lebenszyklus, die nicht so leicht aktualisiert werden können (z. B. in Branchen wie der Automobilbranche und kritische Infrastrukturen). Die Zukunft der Cyber-Sicherheit und die Lösung für die meisten dieser großen, schwer zu lösenden Probleme muss sich in einer agentenlosen Sicherheitswelt abspielen.

Diesen Bericht teilen





Schwer zu bewältigende Sicherheitsherausforderungen

Die Entwicklung hin zu agentenloser Sicherheit ist bereits im Gange, wobei erste Lösungen das Problem aus mehreren Richtungen angehen. Chip-Designer verbessern die Sicherheit auf Hardware-Ebene, den Speicherschutz und vertrauenswürdige Ausführungsumgebungen. Verhaltensanalyseprodukte beobachten die Aktivitäten von außen und sind bereit, Geräte, die verdächtige oder anomale Aktionen ausführen, zu isolieren sowie zu untersuchen. Irgendwo muss die Verarbeitung und Analyse stattfinden, jedoch werden wir anstelle dedizierter Agenten zunehmend flexible Datenverarbeitungsressourcen nutzen. Es gibt bereits verteilte Erzwingungspunkte, die die Erzwingung in einem Gerätenetzwerk verteilen, wobei mehrere Punkte in Echtzeit über ihre Erkennungs- und Schutzaktionen kommunizieren sowie zusammenarbeiten.

Fazit

Die Steigerung unserer Bedrohungsabwehreffektivität in der gesamten Sicherheitsbranche wird entscheidend sein, wenn wir den Gegnern einen Schritt voraus bleiben wollen. Wichtig ist, dass mehrere Branchenteilnehmer zusammenarbeiten, um allgemeine Probleme zu lösen, die sich nicht einfach mit Patches oder Software-Aktualisierungen aus der Welt schaffen lassen. Wir müssen unter Branchenführern Informationen intensiver austauschen, damit wir nicht nur mehr und detailliertere Telemetriedaten erhalten, sondern auch Täuschungstechniken unterstützen. Indem wir verstärkt prädiktive Analysen nutzen, die Sicherheitstransparenz für Unternehmensressourcen sowie dezentralisierte Daten verbessern und die Verwendung dedizierter Agenten reduzieren, können wir unsere Effektivität im Kreislauf der Bedrohungsabwehr steigern.



Cloud – Bedrohungen, Vorschriften und die Reaktionen der Anbieter

Feedback teilen



Cloud – Bedrohungen, Vorschriften und die Reaktionen der Anbieter

Sie können zwar die Arbeit auslagern, aber nicht das Risiko.

Elf Vordenker von Intel geben eine gemeinsame Prognose zu Cloud-Bedrohungen und entsprechenden Reaktionen in den nächsten zwei bis vier Jahren ab.

Beitragende:

Yuriy Bulygin
Peter Bury
David Coffey
Carric Dooley
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Shishir Singh
Jamie Tischart
Candace Worley



In diesem Artikel beantworten wir folgende Fragen:

- Mit welchen Cloud-Bedrohungen und -Kompromittierungen rechnen wir?
- Wie werden sich geopolitische Fragen, Gesetzgebung und Regulierungsmaßnahmen auf die Cloud-Umgebung auswirken?
- Welche Reaktionen sollten wir von den Anbietern von Cloud-Diensten und Sicherheitsprodukten erwarten?

Cloud-Dienstanbieter schaffen Vertrauen und gewinnen so Kunden. Als Folge dessen werden immer mehr sensible Daten und geschäftskritische Prozesse in öffentliche sowie hybride Clouds verlagert. Aber auch Angreifer werden sich an diesen neuen Trend anpassen und weiter nach den einfachsten Möglichkeiten suchen, ihre Bemühungen zu Geld machen oder ihre Ziele zu erreichen. Unser Fokus liegt auf der Entwicklung der Cloud-Sicherheit während der nächsten zwei bis vier Jahre. Mit welchen Bedrohungen und Kompromittierungen rechnen wir? Wie werden sich geopolitische Fragen, Gesetzgebung und Regulierungsmaßnahmen auf diese Umgebung auswirken? Und welche Reaktionen sollten wir von den Anbietern von Cloud-Diensten und Sicherheitsprodukten erwarten?

Bedrohungen und Kompromittierungen

Cloud-Dienste vermehren und entwickeln sich weiterhin rasant, wodurch sowohl Unternehmen als auch Kriminelle und staatliche Stellen nicht nur neue Möglichkeiten erhalten, sondern auch mit neuen Bedrohungen konfrontiert werden. Aus unseren Diskussionen haben sich die folgenden elf Vorhersagen als die wichtigsten und wahrscheinlichsten Ergebnisse für die nächsten zwei bis vier Jahre herauskristallisiert:

Das Vertrauen in die Cloud wird zunehmen und zur Speicherung sensiblerer Daten sowie umfangreicherer Verarbeitung in der Cloud führen – und damit zu einem größeren Interesse an Angriffen auf die Cloud.

Die erste Vorhersage ist zwar einfach, bildet aber die Grundlage für alle unsere anderen Prognosen zu Cloud-Bedrohungen. Während der letzten Jahre hat der Wechsel zu Cloud-Anwendungen, -Prozessen sowie -Speichern zugenommen, und wir rechnen damit, dass dieser Trend weiter anhält. Die Cloud-Dienstanbieter sind erheblich besser geworden und werden auch weiterhin ihre Sicherheitskontrollen sowie Absicherungen für Kunden optimieren. Sofern keine schwerwiegenden Kompromittierungen oder Ausfälle auftreten, die zahlreiche Unternehmen, Länder oder Wirtschaftsbereiche betreffen, wird das Vertrauen in die Cloud weiter steigen. Als Folge dessen werden Unternehmen aller Branchen sowie Größen Prozesse sowie Daten zunehmend in Clouds verlagern – und viele Unternehmen werden dann vollständig von Clouds abhängen. Aber auch die Angriffe werden sich anpassen, und es wird neue Bedrohungen sowie Kompromittierungen geben.

Unternehmen werden auch weiterhin die wertvollsten Daten in ihren vertrauenswürdigen Rechenzentren und Netzwerken aufbewahren.

Trotz des Wechsels in die Cloud werden die meisten Unternehmen nicht alle ihre privaten Prozess- und Speicherfunktionen auslagern, sondern geistiges Eigentum sowie einige Daten, die für das Unternehmen besonders wichtig sind, in eigenen Speichersystemen behalten. Ironischerweise sind öffentliche Clouds meist sicherer als private Clouds, da sie oft von größeren Sicherheitsteams betreut werden, in denen umfassendere Kenntnisse – vom Chip bis zu den Anwendungen – gebündelt sind. Wenn Unternehmen eine private Cloud aufbauen, müssen sie sicher sein, dass sie alle Schichten von Anwendungen bis zu Betriebssystemen und von der Hardware bis zu den Hypervisoren absichern können. Da die Grenzen heutzutage weniger klar definiert sind, ist es für Unternehmen zunehmend schwierig, die wichtigsten Daten zu schützen. Die stärkere Nutzung von Cloud-Diensten wird dies zusätzlich erschweren, wodurch Unternehmen und ihre Cloud-Dienstanbieter klarer festlegen müssen, welche Inhalte wohin übertragen werden dürfen und welche Art von Schutz dafür notwendig ist.

Diesen Bericht teilen



In Cloud-Angeboten werden auch weiterhin der Wunsch nach hoher Geschwindigkeit und Effizienz sowie geringen Kosten auf der einen und das Verlangen nach Kontrolle, Transparenz sowie Sicherheit auf der anderen Seite im Widerspruch zueinander stehen. Anbieter und deren Kunden werden auf unterschiedliche Weise versuchen, das Gleichgewicht zwischen beiden Seiten zu halten.

Auch in Zukunft werden antiquierte Authentifizierung und die zugehörigen Kontrollsysteme das schwächste Glied bei der Cloud-Schutztechnologie sein. Wir erwarten eine Zunahme bei gezieltem Diebstahl von Anmeldeinformationen sowie Brute-Force-Angriffen auf Administratorkonten.

In Cloud-Angeboten werden auch weiterhin der Wunsch nach hoher Geschwindigkeit und Effizienz sowie geringen Kosten auf der einen und das Verlangen nach Kontrolle, Transparenz sowie Sicherheit auf der anderen Seite im Widerspruch zueinander stehen.

Für Unternehmen, die sich noch nicht vollständig für die Cloud entschieden haben, ist der Sicherheitsaspekt der Haupthinderungsgrund für eine stärkere Nutzung. (Dennoch arbeiten diese Unternehmen bereits mit der Cloud, da viele ihrer Mitarbeiter Dateien in Diensten wie Google, Dropbox, iCloud und OneDrive oder anderen Diensten speichern.) Hingegen liegt für Unternehmen, die den Wechsel in die Cloud bereits vollzogen haben, [die Sicherheit bei den Hinderungsgründen lediglich auf Platz zwei oder drei](#) – hinter zuverlässiger Verfügbarkeit und finanzieller Kontrolle. Dieser Konflikt wird sich auch in den Cloud-Angeboten widerspiegeln, da Dienstanbieter zwischen dem Wunsch nach hoher Geschwindigkeit und Effizienz sowie niedrigen Kosten auf der einen und dem Verlangen nach Kontrolle, Transparenz sowie Sicherheit auf der anderen Seite abwägen müssen. Anbieter werden auf unterschiedliche Weise versuchen, das Gleichgewicht zwischen beiden Seiten zu halten. Das äußert sich letztlich in den Preisen und Nutzungsbedingungen, bei denen Unternehmen zwischen den Optionen wählen können, die ihren Risikoprofilen am besten entsprechen. Auch wenn es sich bei Cloud-Diensten heute überwiegend um virtualisierte Speicher, Server und Anwendungen handelt, gehen wir davon aus, dass die Dienste in den nächsten vier Jahren zunehmend differenzierter werden. In diesem Zusammenhang wird die Cloud immer stärker ein ereignisbasierter Container und immer weniger ein Server-basierter Code. Container werden jedoch eine wesentlich kürzere durchschnittliche Lebensdauer als virtuelle Maschinen haben, die mit Code und Daten arbeiten, die anschließend verschwinden. Dieser Trend hin zu höherer Geschwindigkeit und Effizienz wird nicht nur den Druck auf das Sicherheitsteam, sondern auch die Widersprüche bei Sicherheitsmaßnahmen drastisch erhöhen.

Auch in Zukunft werden antiquierte Authentifizierung und die zugehörigen Kontrollsysteme das schwächste Glied bei der Cloud-Schutztechnologie sein. Viele Angriffe werden sich zuerst auf den Diebstahl von Anmeldeinformationen konzentrieren.

Kennwörter und die Personen, die diese Kennwörter erstellen und nutzen, werden auch auf absehbare Zeit der größte Schwachpunkt bei den meisten Technologien bleiben. Die Cloud-Authentifizierung bildet da keine Ausnahme, vielmehr stellt sie für Diebe ein noch viel lohnenderes Ziel dar. Die oftmals sehr gedulden und raffinierten Angreifer werden soziale Netzwerke, zuvor gestohlene Kennwörter und andere personenbezogene Daten auswerten, um dann Anmeldeinformationen – insbesondere von Cloud-Administratoren – zu stehlen. Bereits jetzt, aber auch in Zukunft, kommen dafür gezielte Phishing-Angriffe, fingierte Einstellungskampagnen und andere Techniken zum Einsatz. Unternehmensinterne Authentifizierungssysteme, wie Active Directory, können nur in begrenztem Maße mit den Authentifizierungssystemen der Cloud-Dienstleister zusammenarbeiten. Durch die Verbreitung von Cloud-Anwendungen und -Diensten sowie der Tendenz von Nutzern, für jeden Cloud-Dienst das gleiche oder ein ähnliches Kennwort zu verwenden, wird dieses Problem weiter verstärkt. Stellen Sie sich also auf eine Zunahme bei gezieltem Diebstahl von Anmeldeinformationen sowie Brute-Force-Angriffen auf Administratorkonten ein, und beobachten Sie die Aktivität der Administratorkonten genau.

Angriffe werden aus allen Richtungen kommen und sowohl horizontale als auch vertikale Angriffsvektoren nutzen.

Wie bereits auf der Black Hat-Konferenz und anderen Sicherheitskonferenzen angesprochen, untersuchen Cyber-Kriminelle auch weiterhin neue Angriffsvektoren, um diese dann erfolgreich auszunutzen. In herkömmlichen Systemen und Netzwerken gehen die meisten Angriffe vertikal vor. Sie versuchen, sich nach oben oder unten durch die Ebenen zu bewegen, um ihre Berechtigungen auszuweiten, eine Schwachstelle auszunutzen oder Zugriff auf Daten bzw. Anwendungen zu erhalten. Zusätzlich zu dieser Strategie werden Kriminelle bei Cloud-Angriffen auch horizontale Angriffsmöglichkeiten nutzen. Dabei versuchen sie, sich von einer virtuellen Maschine, einem Container oder einem anderen Cloud-Element zum nächsten zu bewegen sowie zwischen Diensten oder sogar Unternehmen hin und her zu springen. Angreifer nutzen die gesamte Bandbreite der Clouds und deren größere Angriffsflächen, um breit gefächert nach Schwachstellen zu suchen und dann mehrere Unternehmen beim gleichen Cloud-Dienstanbieter zu treffen oder böswillige Prozesse zu starten, mit denen sie einen Ausgangspunkt für fortlaufende Überwachung und Exfiltration haben.

Lücken in der Absicherung zwischen Dienstebenen sowie uneinheitliche Einstellungen oder Kontrollen sind das zweitschwächste Glied in der Sicherheitskette. Angreifer werden diese Lücken und Inkonsistenzen erfolgreich ausnutzen.

Lücken in der Absicherung zwischen Dienstebenen sowie uneinheitliche Einstellungen oder Kontrollen sind das zweitschwächste Glied in der Sicherheitskette. Angreifer werden diese Lücken und Inkonsistenzen erfolgreich ausnutzen.

Es gibt viele verschiedene Arten von Cloud-Diensten – die Palette der Anbieter reicht von Infrastrukturen bis hin zu Anwendungen. Unternehmen wissen nicht immer ganz genau, wie die Zuständigkeiten zwischen ihnen und ihren Cloud-Anbietern aufgeteilt sind, was zu potenziell ausnutzbaren Sicherheitslücken führt. Diese Lücken entstehen nicht durch Technologie-, sondern durch Prozessfehler. Zwar kennen Unternehmen die Aufgaben, die durchgeführt werden müssen, und besitzen auch die erforderlichen Werkzeuge dafür, aber oftmals nehmen sie an, dass sich die Gegenseite darum kümmert. Darüber hinaus stützen sich Unternehmen, die mehrere Cloud-Dienstanbieter nutzen, aufgrund unterschiedlicher oder uneinheitlicher Kontrollen oder Terminologien bei den einzelnen Anbietern möglicherweise auf unterschiedliche Sicherheitsmaßnahmen. Zum Teil ist das eine Folge der zahlreichen von Cloud-Dienstanbietern eingesetzten Sicherheitsstandards, die neben der Konsistenz auch die direkte Vergleichbarkeit erschweren. Diese Prozessfehler und Inkonsistenzen bei den Sicherheitskontrollen werden so lange einen fruchtbaren Boden für Cyber-Kriminelle bereiten, bis die Prozesse besser verstanden werden und sich die Standards für Cloud-Sicherheitskontrollen weiterentwickelt haben.

Bei der Verlagerung von IT-Prozessen und Daten in die Cloud werden Transparenz sowie Kontrolle auch weiterhin zu den Hauptproblemen der Unternehmen gehören.

Beim Cloud Computing können Prozesse und Daten nach Bedarf verschoben werden. Daraus ergeben sich einerseits enorme Vorteile – aber auch potenziell schwerwiegende Sicherheits- oder Datenschutzprobleme. Wir haben bereits von Fällen gehört, in denen Mitarbeiter dafür bezahlt wurden, dass sie ihre Kennwörter preisgeben. Wenn nicht bekannt ist oder nicht kontrolliert werden kann, wo Daten gespeichert sind oder welche Prozesse ausgeführt werden, wird das bei jedem Unternehmen zu Problemen führen. Ganz egal, ob Unternehmen Daten zur Einhaltung nationaler Datenschutzvorschriften innerhalb des Landes behalten, aufgrund von Sicherheitsbedenken die Ausführung von Prozessen in bestimmten Cloud-Umgebungen verhindern, die Speicherung sowie Verarbeitung sensibler Daten bzw. von geistigem Eigentum auf den Standort beschränken oder einfach nur die Muster ihrer Cloud-Nutzung verstehen wollen: Die Möglichkeiten zur Visualisierung und Beschränkung der Bewegungen innerhalb und zwischen Clouds liegt weit hinter dem tatsächlichen Bedarf dafür zurück. Der Einsatz legaler Mittel (z. B. Apps, Anmeldedaten) für möglicherweise illegale Zwecke macht einen Wechsel hin zu kontextbasierten Verhaltensanalysen notwendig. Wir rechnen damit, dass diese Transparenz- und Kontrollprobleme auch für die absehbare Zukunft bestehen bleiben.

Diesen Bericht teilen





Angreifer – einschließlich gemieteter Angreifer – nutzen Cloud-Umgebungen wegen ihres Umfangs, ihrer Geschwindigkeit und ihrer Anonymität.

Leider gibt es keine einfache Möglichkeit, Cloud-Ressourcen vor der Ausnutzung durch Angreifer zu schützen. Natürlich werden einmal aufgedeckte Sicherheitslücken geschlossen, doch das kann Monate dauern. In der Zwischenzeit nutzen Angreifer die Cloud-Ressourcen für massive Brute-Force-Angriffe, komplexe Angriffe mit mehreren Vektoren sowie flexible Angriffe, die zwischen Standorten und Ländern wechseln, um der Strafverfolgung zu entgehen. Cloud-Datenspeicherdienste bilden ein regelrechtes Lager mit gestohlenen Daten, das nach nützlichen Verbindungen und Korrelationen durchsucht werden kann. Durch die wiederholte Änderung von Konten, IP-Adressen, Dienststandorten, kurzlebigen Containern sowie anderen Cloud-Merkmalen können die Kriminellen ihre Identitäten länger geheim halten und sind noch schwerer aufzuspüren. Das wird sich auch in den nächsten zwei bis vier Jahren nicht ändern.

„Denial-of-Service-Angriffe mit Lösegeldforderung“ werden zu einer häufig genutzten Angriffsform gegen Cloud-Dienstanbieter und Cloud-basierte Unternehmen.

Die Tatsache, dass eine Cloud von vielen Mandaten genutzt wird, macht Denial-of-Service-Angriffe auf Cloud-Dienstanbieter noch reizvoller. Die meisten Diensteanbieter können herkömmliche Denial-of-Service-Angriffe ganz gut abwehren. Trotzdem werden Angreifer auch weiterhin nach ausnutzbaren Schwachstellen Ausschau halten. Sobald solche Schwachstellen gefunden sind, lassen Angriffe nicht lange auf sich warten. Wenn ein Unternehmen seine gesamten Prozesse und Daten in die Cloud verlagert hat, gibt es zahlreiche Schnittstellen zwischen dem Unternehmen und der Cloud, die angegriffen werden können, um das Unternehmen effektiv außer Gefecht zu setzen. Zu diesen Schnittstellen gehören die Internetverbindung, DNS-Dienste und andere Infrastrukturkomponenten. Um ein von der Cloud abhängiges Unternehmen außer Gefecht zu setzen, muss nicht unbedingt der Cloud-Dienstanbieter direkt gestört werden. Stattdessen reicht es, wenn Angreifer den Zugang zur Cloud unterbrechen und das Unternehmen dann in Geiselschaft nehmen.

Mit Ausnahme der Kompromittierungen, die auf schwachen Anmeldeinformationen beruhen, wird die Zahl erfolgreicher Datenkompromittierungen in öffentlichen Clouds zwar weiterhin niedrig bleiben, diese Vorfälle werden aber einen zunehmend stärkeren Einfluss haben.

Cloud-Dienstanbieter haben oft ein größeres Team an Cloud-Sicherheitsexperten als die Kunden, die ihre Dienste nutzen. Deshalb gehen wir davon aus, dass die Zahl der erfolgreichen Cloud-Datenkompromittierungen weiterhin niedrig bleibt. Die einzige Ausnahme davon sind Kompromittierungen, die aus dem Diebstahl von Anmeldeinformationen resultieren. Wenn jedoch ein Angreifer durch eine Kompromittierung Zugang zu großen Datenspeichern mehrerer Kunden erlangen kann, sind die potenziellen Konsequenzen einer Cloud-Datenkompromittierung erheblich. Ob der Cloud-Dienstanbieter oder die betroffenen Unternehmen mehr von der Kompromittierung betroffen sind, hängt dann wahrscheinlich davon ab, wer nachweislich alle angemessenen Anstrengungen in seinem Zuständigkeitsbereich unternommen hat.

Die zunehmende Zahl und Vielfalt an IoT-Geräten (Internet der Dinge) wird einige Cloud-Sicherheitsmodelle sprengen, wodurch es zu erfolgreichen Angriffen über diese Geräte kommen kann.

Meist erfordert die Authentifizierung eine Interaktion zwischen einer Person und einem Gerät oder zwischen zwei Geräten. Da immer mehr IoT-Geräte sowie Dienste online gehen, kommunizieren diese Geräte mit mehreren anderen IoT-Geräten und entscheiden mit Gerätegeschwindigkeit darüber, wem sie vertrauen. Die Sicherheitsstrukturen, vertrauenswürdigen Stellen und Kontrollen über diese Art der Kommunikation sind sehr mangelhaft, was zu ausnutzbaren Lecks und Schwachstellen führen kann. Beim Versuch der Cloud-Dienstanbieter,

die aktuellen Modelle an diese neue Umgebung anzupassen, wird sich deren Latenz und Komplexität erhöhen. Das ist der perfekte Nährboden für Sicherheitsprobleme. Uns sind bereits Fälle bekannt, bei denen Unternehmensnetzwerke erfolgreich über unsichere IoT-Geräte kompromittiert wurden, und Clouds sind der nächste Punkt auf der Liste.

Gesetze und Ländergrenzen

Cloud-Bedrohungen und -Kompromittierungen werden Auslöser für politische Reaktionen sowie Regulierungsmaßnahmen sein. Die Geschwindigkeit des technologischen Fortschritts wird effektive Gesetze behindern und umgekehrt. Unterschiedliche oder sogar widersprüchliche Vorschriften in verschiedenen Ländern werden die Lage für Verbraucher, Unternehmen und Cloud-Dienstanbieter erschweren.

Gesetze können nicht mit technologischen Neuerungen Schritt halten. Cloud-Dienstanbieter, ihre Kunden sowie die sich entwickelnde Cyber-Versicherungsbranche müssen über Jahre mit Gerichtsverfahren rechnen, bevor sich ein angemessenes Verhalten fest etabliert hat.

Gesetze können nicht mit technologischen Neuerungen Schritt halten. Vorschriften werden Formulierungen wie „Sorgfaltspflicht“ und „angemessene Anstrengungen“ enthalten, über die sich Cloud-Dienstanbieter und ihre Kunden in Gerichtsverfahren auseinandersetzen müssen.

Es ist hinreichend bekannt, dass Gesetze nicht mit technologischen Neuerungen Schritt halten können. Gesetze zu Datensicherung und Verbraucherdatenschutz in der Cloud bilden da keine Ausnahme. In Bezug auf Cloud-Datensicherheit werden Rechtssysteme auf Formulierungen wie „Sorgfaltspflicht“ oder „angemessene Anstrengungen“ setzen, um Gesetze zu verabschieden, die effektiv und nicht sofort wieder überholt sind. Allerdings wird es einige Zeit dauern und viele Gerichtsverfahren kosten, bis diese Bedingungen ausreichend detailliert durch gerichtliche Präzedenzfälle definiert sind. Oft gibt es keine einfachen Ja-oder-Nein-Tests, die auf Cyber-Sicherheit für Systeme und Daten angewendet werden können. Dies gilt besonders für die Cloud, in der mehrere Akteure gemeinsam für den Schutz sorgen. In der Zwischenzeit müssen Cloud-Dienstanbieter, ihre Kunden und die sich entwickelnde Cyber-Versicherungsbranche über Jahre mit Gerichtsverfahren rechnen, in denen sie als Kläger und/oder Angeklagte darüber verhandeln müssen, ob ihre Anstrengungen „angemessen“ waren. Da auch die öffentliche Meinung eine Rolle spielt, versuchen Unternehmen, deren Cloud kompromittiert wurde, nachzuweisen, dass sie alles in ihrer Macht stehende unternommen haben, um ihre Kunden zu schützen.

Die Datenbewegung in und aus rechtlichen Zuständigkeitsbereichen wird auch weiterhin eine Herausforderung darstellen. Zudem verzögern Gesetze zum Verbraucherschutz den Wechsel in die Cloud.

In ihren Bemühungen, die Privatsphäre der Verbraucher zu schützen, werden politische Gremien Gesetze verabschieden, nach denen Unternehmen selbst erfasste personenbezogene Daten innerhalb der Grenzen des Landes speichern müssen, in dem die zu den Daten gehörigen Bürger leben. Das ist nicht nur für Unternehmen eine Herausforderung, die ihre Daten identifizieren sowie klassifizieren müssen, sondern auch für Cloud-Dienstanbieter, die immer differenziertere Kontrollen für Daten- und Prozessbewegungen anbieten müssen. Was passiert beispielsweise mit den vertraglichen Vereinbarungen, wenn ein in einem Land ansässiges großes Cloud-Rechenzentrum Opfer eines Angriffs ist, sich das nächstgelegene Backup-Rechenzentrum jedoch in einem anderen Land befindet? Wie werden international agierende Unternehmen Kunden-, Verkaufs- und Produktdaten so trennen, dass Kontrollen entsprechend diesen neuen Gesetzen angewendet werden können? Diese und ähnliche Herausforderungen werden den Wechsel in die Cloud verzögern, da Unternehmen entweder gezwungen sind, in einigen Ländern eigene Rechenzentren einzurichten, oder sich aus Kostengründen gegen eine Geschäftstätigkeit in diesen Ländern entscheiden müssen.

Einige Rechtssysteme erlegen Cloud-Diensteanbietern und ihren Geschäftspartnern Mindestbetriebsanforderungen, Zertifizierungen und/oder Audits auf.

Was passiert mit den Daten, wenn ein Cloud-Diensteanbieter in Konkurs geht? Wie sind Unternehmen und Verbraucher vor Kriminellen oder staatlichen Stellen geschützt, die böswillige Cloud-Dienste entwickeln, um primär Daten zu erfassen? Welche rechtlichen Bestimmungen gibt es zwischen einem Cloud-Diensteanbieter und seinen Subunternehmern oder Geschäftspartnern? In einer anderen wahrscheinlichen Reaktion erlegen politische Gremien den in ihren Ländern agierenden Cloud-Diensteanbietern Mindestbetriebsanforderungen auf und fordern unabhängige Zertifizierungen oder Audits. Die Definition der Bedingungen und Beziehungsstufen ist eine enorme Herausforderung, die heftige Diskussionen in der Branche auslösen wird. Doch ungeachtet der Gesetze wird der Hauptdiensteanbieter – und nicht die Subunternehmer oder die Partner – das Risiko sowie die größten Konsequenzen einer Datenkompromittierung tragen.

Reaktionen der Anbieter

Bedrohungen, Kompromittierungen und Gesetze werden Cloud-Anbieter sowie Anbieter von Sicherheitsprodukten zu Reaktionen in Bezug auf ihre Technologien und Dienste veranlassen. Um Lücken zu schließen und Inkonsistenzen zu reduzieren, werden Authentifizierungssysteme optimiert, Kontrollen für Unternehmen entwickelt sowie Sicherheitsfunktionen automatisiert. Außerdem wird die Erkennung durch den Austausch von Bedrohungsdaten erheblich verbessert. Dies sind unsere zehn wichtigsten Erwartungen bezüglich der Reaktionen auf Cloud-Bedrohungen in den nächsten zwei bis vier Jahren:

Kennwörter müssen durch sicherere Authentifizierungssysteme ersetzt werden, die den Anmeldevorgang aber nicht allzu sehr beeinträchtigen dürfen. Sowohl biometrische Merkmale als auch mehrstufige Authentifizierung sowie Verhaltensanalysen werden dafür sorgen, dass die „Schaltzentrale“ der Cloud-Diensteanbieter und ihrer Kunden geschützt ist.

Sowohl biometrische Merkmale als auch mehrstufige Authentifizierung sowie Verhaltensanalysen werden dafür sorgen, dass die „Schaltzentrale“ der Cloud-Diensteanbieter und ihrer Kunden geschützt ist.

Kennwörter müssen durch sicherere Authentifizierungssysteme ersetzt werden, die den Anmeldevorgang aber nicht allzu sehr beeinträchtigen dürfen. Kurzfristig erwarten wir eine zunehmende Nutzung der mehrstufigen Authentifizierung mittels Mobiltelefonen oder Frage-Antwort-Systemen. Diese neue Art der Authentifizierung wird zuerst von Administratoren eingesetzt werden, da gestohlene Administrator-Anmeldeinformationen die massivsten Auswirkungen haben. Zudem gehen wir davon aus, dass teilweise Verhaltensanalysen genutzt werden, um ungewöhnliche Aktivitäten bei Kontoanmeldungen zu erkennen. Langfristig erwarten wir eine verstärkte Nutzung biometrischer Merkmale in einer Art und Weise, die von Benutzern als bequem und benutzerfreundlich empfunden wird. Sobald die Implementierung neuer Erkennungstechnologien kommerziell rentabel ist, werden Fingerabdrücke durch andere eindeutige Faktoren wie Gesichtszüge, Herzschlag oder Netzhaut ersetzt oder erweitert.

Transparenz sowie Kontrollen auf Unternehmensebene werden die Verwaltung der Datenverlagerung in die Cloud durch Schatten-IT unterstützen und die Komplexität sowie das Volumen der in der Cloud durchgeführten Aktivitäten koordinieren.

Über Cloud-Diensteanbieter werden Abteilungen oder Geschäftsbereiche die Möglichkeit haben, Workloads ganz ohne Beteiligung des IT-Teams in die Cloud zu verschieben. Das führt dazu, dass die Sicherheits- oder IT-Teams in vielen Unternehmen gar nicht wissen, wenn Daten oder Prozesse durch diese Akteure in die Cloud verschoben werden und dadurch das gesamte Unternehmen gefährdet wird. Deshalb werden die Dienst- und Sicherheitsanbieter aufgefordert, Tools zur Verbesserung der Datentransparenz und -kontrolle zu entwickeln. Wir erwarten, dass die Tools zur Verhinderung von Datenkompromittierungen und Koordinierung von Richtlinien zunehmend für den Einsatz in der Cloud geeignet sein werden. Der nächste Schritt sind dann Cloud-fähige Erweiterungen, mit denen Sicherheitskontrollen und -richtlinien direkt beim Cloud-Diensteanbieter angewendet werden können.

Diesen Bericht teilen



Sicherheitsbewertung, Authentifizierung, Risiko-vermeidung sowie Cloud-Audits sind nur einige der Bereiche, in denen die Arbeit von Sicherheitsexperten durch Automatisierung ergänzt und der Fachkräftemangel ausgeglichen werden kann.

Durch Automatisierungen im Sicherheitsbereich werden die Folgen des Fachkräftemangels ausgeglichen.

Der Mangel an Sicherheitsexperten wird für Cloud-Dienstanbieter eine Gefahr und gleichzeitig eine Chance sein. Damit jedoch aus der Gefahr eine Chance wird, müssen Kenntnisse und Erfahrungen im Bereich Sicherheit in automatisierte Tools sowie Bots integriert werden. Diese vereinfachen die Kontrolle der Cloud-Sicherheit, sodass eine größere Personengruppe ihre Schutzmaßnahmen effektiv einrichten und überwachen kann. Sicherheitsbewertung, Authentifizierung, Risikovermeidung sowie Cloud-Audits sind nur einige der Bereiche, in denen die Arbeit von Sicherheitsexperten durch Automatisierung ergänzt, Kontexterkenntnis hinzugefügt und der Funktionsumfang auf die Leiter der Geschäftsbereiche ausgedehnt werden kann.

Anbieter für Cloud-Zugangssicherheit werden sich weiterentwickeln und neben besseren Schutzmaßnahmen auch mehr Transparenz sowie Kontrolle bieten.

Die Erkennung und Anwendung von Richtlinien sowie die Authentifizierung bei Cloud-Diensten werden beim Schutz von Unternehmen weiterhin eine wichtige Rolle spielen. Ein Anbieter für Cloud-Zugangssicherheit (Cloud Access Security Broker, CASB) kann zwar bei der Einführung und Durchsetzung von Richtlinien helfen, aber nicht das Hauptproblem der Authentifizierung lösen. Am wertvollsten sind nach wie vor die Daten. Während sich CASBs weiterentwickeln und mit anderen Sicherheitssystemen vernetzen oder mit ihnen gemeinsam entscheiden werden, welche Daten in der Cloud wie gesichert werden müssen, rücken die Daten immer stärker in den Fokus.

Der bessere Schutz gespeicherter und gerade übertragener Daten wird zunehmend zum Wettbewerbsvorteil einiger Cloud-Dienstanbieter.

Einige grundlegende Cloud-Dienste wie der Speicher- oder Prozessorverleih sind inzwischen standardisiert. Um sich von Wettbewerbern abzuheben, werden manche Cloud-Dienstanbieter zusätzlichen Schutz für Daten anbieten, die in ihren Systemen gespeichert, von ihnen verarbeitet oder darin übertragen werden. Dabei werden diese Premiumdienste nicht nur Verschlüsselung, sondern auch Integritätsprüfungen, Echtzeitüberwachung sowie modernste Techniken zum Schutz vor Datenkompromittierung umfassen, um langfristig einen Wettbewerbsvorteil zu bieten.

Die Auditierung und Transparenz der Abläufe bei Cloud-Dienstanbietern wird zum Standard.

Sei es aufgrund von Kundenforderungen, Wettbewerbsdruck oder Branchenvorschriften – bei den meisten Cloud-Dienstanbietern werden Echtzeit-Auditierung und -Transparenz innerhalb der nächsten vier Jahre zum Standardangebot gehören. Damit wird aus dem Differenzierungsmerkmal, dem Kunden immer genau den Speicherort seiner Daten nennen zu können, schnell eine Standardkomponente bei Cloud-Diensten. Statische Audits und historische Übersichten reichen nicht mehr aus, um wertvollen Daten und Workflows ausreichenden Schutz zu bieten.

Anbieter von Sicherheitslösungen werden sich zunehmend auf maschinelles Lernen stützen, um Angriffe vorhersagen und abwehren zu können, bevor sie Schaden anrichten.

Sicherheitslösungen zum Schutz der Cloud-Infrastruktur werden immer wichtiger, da Angreifer durch die Kompromittierung der Infrastruktur direkten Zugang zu den Anwendungen und Daten zahlreicher Kunden erhalten. Solche Ereignisse werden in überwältigender Zahl auftreten, weshalb wir die ständige Weiterentwicklung hochentwickelter, automatisierter Tools erwarten, mit denen Zwischenfälle schnell diagnostiziert und behoben werden können. Aufbauend darauf und durch den Einsatz von maschinellem Lernen sowie Big-Data-Analysen werden Sicherheitslösungen prädiktiv und präskriptiv. Sie erkennen neue Bedrohungen und wehren Angriffe ab, lange bevor Systeme kompromittiert werden.

Sicherheitslösungen werden prädiktiv und präskriptiv. Sie erkennen neue Bedrohungen und wehren Angriffe ab, lange bevor Systeme kompromittiert werden.

Diesen Bericht teilen



Zwischen Unternehmen und Cloud-Anbietern wird es einen stärkeren Austausch von Bedrohungsdaten geben, was eine bessere Identifizierung von Angriffen und kürzere Reaktionszeiten zur Folge haben wird.

Unter den Cloud-Dienstanbietern werden sich Unternehmen für den Bedrohungsdatenaustausch bilden, was eine bessere Identifizierung von Angriffen und kürzere Reaktionszeiten zur Folge haben wird.

Auch heute noch erkennen einige Unternehmen und Cloud-Dienstanbieter nicht die Vorteile, die sich aus dem Austausch von Bedrohungsdaten ergeben. Aufgrund von Vorschriften oder aggressiven Angriffen wird dieser Austausch zwischen Unternehmen und Cloud-Dienstanbietern innerhalb der nächsten Jahre jedoch stärker zunehmen und die Vorteile deutlicher machen. Denn auch wenn es manchmal unangenehm ist, über versuchte oder erfolgreiche Angriffe zu sprechen, werden Unternehmen erkennen, dass die Vorteile eines Echtzeit-Datenaustauschs die Nachteile bei weitem überwiegen.

Die Technik- und Absicherungsstandards bei Cloud-Sicherheit werden weiter gestärkt.

Die [Cloud Security Alliance](#) und andere Gruppen haben Standards, Leitlinien, Zertifizierungen sowie empfohlene Vorgehensweise für die Verwaltung von Cloud-Diensten entwickelt. Dabei lag ihr Schwerpunkt bisher auf der Entwicklung von Standards und Anleitungen, mit denen Kunden ein höheres Maß an Transparenz erhalten. Cloud-Sicherheitsstandards sind zurzeit noch etwas lückenhaft, die Verantwortlichen stimmen aber zunehmend darin überein, wie wichtig der sichere Aufbau und Betrieb einer Cloud ist. Wir gehen deshalb davon aus, dass die Absicherungsstandards in den nächsten zwei bis vier Jahren besser durchdacht, stärker konsolidiert und von führenden Cloud-Dienstanbietern umgesetzt werden.

Der Markt für Cyber-Versicherungen wird wachsen. Gleichzeitig müssen sich die Beteiligten mit der Interpretation der Formulierung „angemessene Anstrengungen“ sowie damit auseinandersetzen, ob das eingetretene Ereignis versicherbar war.

Wir gehen davon aus, dass Versicherungsunternehmen Cyber-Versicherungen sowie Sicherheitsbewertungen anbieten werden, mit denen die Versicherungskosten reduziert werden können. In einigen Ländern werden Gesetze und Vorschriften eingeführt, die zusammen mit der Weiterentwicklung des Angebots von Cloud-Diensten das Vertrauen in diese Dienste weiter stärken werden. Dennoch wird die Versicherung der Cloud ein subjektives Geschäft mit vielen Ausnahmeklauseln bleiben. In dem hier veranschlagten Zeitrahmen von zwei bis vier Jahren wird es nicht möglich sein, die notwendige Infrastruktur aufzubauen und die Erfahrungen zu erlangen, mit der objektive Entscheidungen über Kosten, Ansprüche und versicherbare Ereignisse getroffen werden können.

Fazit

Das ungebremsst starke Wachstum bei der Nutzung von Cloud-Diensten bedeutet auch, dass diese Dienste zu immer wertvolleren Angriffszielen werden. Viele Unternehmen bewahren ihre sensibelsten Informationen zwar weiterhin in privaten Rechenzentren auf, doch aufgrund der hohen Anforderungen hinsichtlich Geschwindigkeit, Effizienz und Kosten werden aber immer mehr Daten aus dem vertrauenswürdigen Netzwerk in Clouds verlagert, in denen diese Vorteile genutzt werden können. Während Unternehmen lernen, wie sie ihre Abläufe Cloud-fähig gestalten können, werden Lücken bei Kontrolle, Transparenz und Sicherheit zu Datenkompromittierungen führen.

Angriffe erfolgen aus allen Richtungen – sie bewegen sich vertikal durch alle Ebenen eines Unternehmens und horizontal zwischen Unternehmen, die sich in der gleichen Cloud befinden. Auch in Zukunft werden Anmeldeinformationen und Authentifizierungssysteme die am meisten gefährdeten Angriffspunkte sein, weshalb Cyber-Kriminelle alles daran setzen werden, in den Besitz von Anmeldeinformationen zu gelangen. Insbesondere die Informationen für Administratorkonten sind lukrativ, da diese Konten den umfassendsten Zugang versprechen.

Diesen Bericht teilen



Auf Sicherheits- und Datenschutzbedenken wird die Gesetzgebung im Allgemeinen mit der Zertifizierung von Cloud-Diensteanbietern, Mindestbetriebsanforderungen sowie weiteren gesetzlichen Kontrollen reagieren. Diese Maßnahmen können sich zwischen den einzelnen Rechtssystemen erheblich unterscheiden und in einigen Fällen den Wechsel in die Cloud ausbremsen. International agierende Unternehmen müssen zum Beispiel auf Ländergrenzen achten und sorgfältig darum herum navigieren. Da Gesetze nicht mit den Neuerungen bei Cloud-Technologien und Dienstangeboten Schritt halten können, wird es insbesondere nach Kompromittierungen zu Gerichtsverfahren kommen, in denen Kläger und Angeklagte herausfinden müssen, wessen Anstrengungen „angemessen“ waren.

Cloud-Diensteanbieter werden ebenso wie Sicherheitsanbieter weiter an der Optimierung von Authentifizierungssystemen arbeiten und zunehmend die Erkennung biometrischer Merkmale als beste Lösung einbinden. Zugleich machen sich Diensteanbieter und ihre Kunden für höhere Transparenz stark, und Echtzeit-Auditierung wird zum Standard. Es wird neue Technologien geben, mit denen gespeicherte und gerade übertragene Daten besser geschützt werden können. Mit Verhaltensanalysen, Sicherheitsautomatisierungen sowie Diensten zum Austausch von Bedrohungsdaten sollen einerseits die schiere Menge an Bedrohungen sowie die enorme Geschwindigkeit bei der Entwicklung neuer Bedrohungen bewältigt und andererseits die Erkennungs- sowie Behebungsfunktionen verbessert werden. Maschinelles Lernen wird sich als neue Methode etablieren, mit der Angriffe vorhergesagt und abgewehrt werden können, bevor sie Schaden anrichten.



IoT – Bedrohungen, Vorschriften und die Reaktionen der Anbieter

Feedback teilen



IoT – Bedrohungen, Vorschriften und die Reaktionen der Anbieter

Vielsprechende Konzepte treffen auf den Wilden Westen

Zehn Vordenker von Intel geben eine gemeinsame Prognose zu IoT-Bedrohungen und entsprechenden Reaktionen in den nächsten zwei bis vier Jahren ab.

Beitragende:

Jonathan Anderson
Yuriy Bulygin
Carric Dooley
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Ramnath Venugopalan
Lori Wigle
Candace Worley



In diesem Artikel beantworten wir folgende Fragen:

- Mit welchen IoT-Bedrohungen und -Kompromittierungen rechnen wir?
- Wie werden sich geopolitische Fragen, Gesetzgebung und Regulierungsmaßnahmen auf die IoT-Umgebung auswirken?
- Welche Reaktionen sollten wir von den Entwicklern von IoT-Geräten und den Anbietern von Sicherheitsprodukten erwarten?

Die Bedrohung durch IoT-Angriffe ist real, jedoch ist noch nicht klar, welche Gelegenheiten sich Kriminellen auf der Suche nach Bereicherung bieten. Cyber-Kriminelle werden profitable Modelle finden, und Angriffe aus finanziellen Motiven werden sich ausbreiten.

Diesen Bericht teilen



Das Internet der Dinge umfasst in jeder Branche Hunderte oder Tausende von Gerätetypen. Tatsächlich muss man beim IoT nicht an Geräte, sondern an Netzwerke aus Geräten denken, die Dienste ermöglichen und anbieten. Viele dieser Dienste sind Cloud-basiert. Daher sind IoT-Bedrohungen und die Reaktionen auf diese eng mit Cloud-Bedrohungen sowie den entsprechenden Reaktionen verknüpft.

In vielen Branchen kann man sich diese Cloud-basierten Gerätenetzwerke als Interessengemeinschaften vorstellen. So ist beispielsweise eine Produktionsstätte für den Hersteller eine Interessengemeinschaft, und das Netzwerk enthält die für die Fertigung der Waren erforderlichen Geräte. In einem Krankenhaus stellen die von den Mitarbeitern benötigten medizinischen Geräte und das zugehörige Netzwerk eine Interessengemeinschaft dar.

Dabei ergeben sich verschiedenste Gelegenheiten, Daten zu entwenden, Vorgänge zu verweigern oder Schaden zu verursachen. In diesem Artikel konzentrieren wir uns auf die Entwicklung der IoT-Sicherheit in den nächsten zwei bis vier Jahren. Mit welchen Bedrohungen und Kompromittierungen rechnen wir? Wie werden sich geopolitische Fragen, Gesetzgebung und Regulierungsmaßnahmen auf diese Umgebung auswirken? Und welche Reaktionen sollten wir von den Entwicklern von IoT-Geräten und den Anbietern von Sicherheitsprodukten erwarten?

Bedrohungen und Kompromittierungen

IoT-Geräte sind aus ein oder zwei Gründen für Cyber-Kriminelle oder staatliche Akteure attraktiv: Sie sind eine potenzielle Quelle für Daten sowie Metadaten oder ein potenzieller Angriffsvektor, um Schäden zu verursachen. Aus unseren Diskussionen haben sich die folgenden zehn Vorhersagen als die wichtigsten und wahrscheinlichsten Ergebnisse für die nächsten zwei bis vier Jahre herauskristallisiert:

Die Bedrohung durch IoT-Angriffe ist real, jedoch ist noch nicht klar, welche Gelegenheiten sich Kriminellen auf der Suche nach Bereicherung bieten.

Schwachstellen und Gelegenheiten für Angriffe auf IoT-Geräte existieren bereits, jedoch sind die Möglichkeiten begrenzt, aus Angriffen Profit zu schlagen. Dies liegt daran, dass die einzelnen IoT-Geräte nicht in hinreichender Anzahl an gewinnversprechenden Stellen im Netzwerk vorhanden sind und fest umrissene Modelle für die Monetisierung von Angriffen fehlen. Bietet es sich an, IoT-Geräte in Geiselschaft zu nehmen, Daten von ihnen zu stehlen und im „Dark Web“ zu verkaufen oder mit ihrer Hilfe für ein Unternehmen Schäden wie beispielsweise großflächige Ausfälle herbeizuführen? In den nächsten vier Jahren werden Cyber-Kriminelle diese Fragen beantworten, und finanziell motivierte Angriffe werden sich ausbreiten. Interessanterweise gibt es weitaus mehr Gelegenheiten, Schäden zu verursachen, von denen bisher nur wenige genutzt wurden, möglicherweise aus Angst der potenziellen Täter vor Vergeltungsmaßnahmen.

Ransomware wird sich auf das IoT verlagern, da es sich für Kriminelle als relativ einfache Möglichkeit zur Gewinnerzielung erwiesen hat.

Ransomware wird die Hauptbedrohung darstellen.

Eine der Herausforderungen bei Bedrohungsvorhersagen ist die Verknüpfung potenzieller Motive mit tatsächlichen Gelegenheiten. Einige allgemein publik gewordene Hacks oder Schwachstellen von IoT-Geräten lassen sich nur mit großem Aufwand im großen Stil durchführen. Wir sind sicher, dass sich Ransomware auf das IoT verlagern wird, da es sich für Kriminelle als relativ einfache Möglichkeit zur Gewinnerzielung erwiesen hat. Ein oder mehrere IoT-Geräte, ihre Steuerungsebene oder ihren Cloud-Aggregationspunkt zu stören und die Geräte als Geisel zu nehmen, ist eine einfachere sowie schnellere Möglichkeit zur Gewinnerzielung als die heimliche Kompromittierung einer großen Anzahl von Geräten, um Daten abzuzapfen. Wir sehen bereits bei der Energieversorgung und im Gesundheitswesen, dass IoT-Geräte in Geiselhaft genommen werden.

Hacktivismus wird zur größten Sorge.

Obwohl Ransomware für viele Unternehmen mit IoT-Geräten und -Verbindungen zur Realität werden wird, wird Hactivismus die größte Sorge darstellen. Unserer Meinung nach geht es den meisten Kriminellen um den Profit und nicht darum, ein Unternehmen zu schädigen oder seinen Betrieb ernsthaft zu behindern. Meist jedoch versuchen die Aktivisten mit unverhältnismäßig drastischen Mitteln, die gewünschte Wirkung zu erzielen. Ob es darum geht, die Kontrolle zu übernehmen und die Ergebnisse von Wahlmaschinen zu manipulieren, Ventile an einem Staudamm zu öffnen oder Sicherheitssysteme in einer Chemieranlage außer Kraft zu setzen – das Potenzial für katastrophale Schäden ist real. In den nächsten zwei bis vier Jahren rechnen wir mit entsprechenden Versuchen von Hacktivisten, die in den meisten Fällen jedoch erfolglos bleiben werden.

Staatlich gesteuerte Angriffe auf kritische Infrastrukturen werden zwar eine ständige Sorge darstellen, aber aufgrund befürchteter physischer oder Cyber-basierter Vergeltungsmaßnahmen nur vereinzelt auftreten.

Staatlich gesteuerte Angriffe sind sozusagen der große Bruder des Hactivismus. Die Gelegenheit, die militärischen oder wirtschaftlichen Möglichkeiten eines anderen Staats zu schädigen oder zu stören, ist real, und im vergangenen Jahr haben wir bereits einige Angriffe gesehen. Diese Angriffe richteten sich in erster Linie gegen SCADA-Systeme, eine Art von IoT-Geräten. Jedoch begrenzt die Furcht vor militärischen, wirtschaftlichen oder Cyber-basierten Vergeltungsmaßnahmen durch das Opfer die Häufigkeit von staatlich gesteuerten Angriffen auf kritische Infrastrukturen.

IoT-Geräte werden schnell an die Grenzen aktueller Datenschutzgesetze stoßen, und die politischen Instanzen werden weiterhin langsam reagieren.

Durch das IoT wird die Privatsphäre der Verbraucher signifikant beeinträchtigt.

Berichte über den Tod der Privatsphäre sind bisher zwar übertrieben, aber mit dem IoT rückt ihr Ende näher. Es gibt schlicht zu viele IoT-Geräte, die alle Handlungen von Verbrauchern beobachten, belauschen, aufzeichnen, sammeln und anderweitig aufmerksam erfassen. In vielen Fällen zahlen Verbraucher für die Dienste eines Unternehmens und lassen sich kostenlos überwachen. Die Details sind zwar in den Endbenutzer-Lizenzverträgen enthalten, aber die meisten Verbraucher lesen diese nicht und haben sowieso keine Opt-Out-Möglichkeit. IoT-Geräte werden schnell an die Grenzen aktueller Datenschutzgesetze stoßen, und die politischen Instanzen werden weiterhin langsam reagieren. Die Datenschutzerwartungen werden sich auf Geräteanbieter und Dienstbetreiber auswirken, da einige Regierungen explizite Vereinbarungen, Opt-Ins und sogar eine Vergütung für die Nutzung oder Weitergabe persönlicher Daten vorschreiben werden.

Wir werden mehr Fälle sehen, in denen IoT-Geräte als Einfallstore für den Diebstahl von Daten und geistigem Eigentum, die Störung kritischer Infrastrukturen sowie andere groß angelegte Angriffe genutzt werden.

IoT-Geräte werden sich als nützliche Angriffsvektoren für Steuerungs-, Überwachungs- und Informationssysteme erweisen.

In den nächsten zwei bis vier Jahren werden wir mehr Fälle sehen, in denen IoT-Geräte als Einfallstore für den Diebstahl von Daten und geistigem Eigentum, die Störung kritischer Infrastrukturen sowie andere groß angelegte Angriffe genutzt werden. Viele neu auf den Markt kommende IoT-Geräte bieten wenig oder gar keine Sicherheit. Bereits heute haben IoT-Geräte oft ähnliche oder bekannte Schwachstellen, die nicht gepatcht oder aktualisiert werden können. In anderen Fällen werden harmlose Geräte ohne geeignete Isolierung oder Segmentierung mit dem Netzwerk verbunden und ermöglichen unbeabsichtigt den Zugriff auf vertrauenswürdige Umgebungen. Schließlich üben auch die für den Betrieb Verantwortlichen Druck aus: „Alles funktioniert. Bloß nichts ändern!“ Alle diese Elemente zusammen verwandeln IoT-Geräte in offene Tore zu vielen Arten von Systemen und Organisationen.

Die Gerätehersteller werden bei der Internetfähigkeit ihrer Produkte weiterhin Anfängerfehler machen.

Unternehmen entwickeln im Wesentlichen aus zwei Gründen internetfähige Geräte: zur Effizienzsteigerung und zur Sammlung von Daten über die Gerätenutzung. Einige dieser Unternehmen haben wenig oder gar keine Erfahrung mit Geräten mit Internetverbindung. Daher machen viele von ihnen Anfängerfehler, lernen ihre Lektionen und durchlaufen in anderer Hinsicht die Geschichte der Internetsicherheit erneut. Leider tun sie dies in einer feindlicheren Umgebung. Eine gewisse Kombination aus Kompromittierungen, Vorschriften und Lernen ist notwendig, damit konzeptionelle Sicherheit in die regulären Aktivitäten aller Unternehmen integriert wird. Diese Lernphase wird länger als vier Jahre dauern.

Die Steuerungsebene von IoT-Geräten wird ein wichtiges Ziel sein.

Wenn allgemein über IoT-Angriffe gesprochen wird, sind meist direkte Angriffe auf IoT-Geräte gemeint. Obwohl Angriffe auf Geräteebene sicherlich verbreitet sind, lassen sie sich nicht so leicht in großem Maßstab durchführen. Ein Angriff auf ein einziges autonomes Auto, vernetztes Ventil oder intelligentes Türschloss ist nicht allzu lohnenswert. Daher bevorzugen Angreifer oft die Steuerungsebene von IoT-Geräten als Ziel. Steuerungsebenen verfügen über ein gewisses Maß an privilegiertem Zugriff und ermöglichen die Überwachung von Prozessen sowie Änderung der Einstellungen für mehrere Geräte. Während sich die Sicherheitsmaßnahmen auf die IoT-Geräte selbst konzentrierten, richtete sich das Augenmerk weniger auf die Systeme, die diese Geräte steuern. Angesichts des erwarteten Maßstabs der wichtigsten IoT-Gerätebereitstellungen werden deren Steuerungsebenen komplex sein und eine sehr große Angriffsfläche bieten. Die Bemühungen von Angreifern, die aufgrund schwacher Authentifizierung oder mithilfe gestohlener Anmeldeinformationen die Integrität von Nachrichten im Steuerungsdatenstrom beeinflussen oder den Controller selbst kompromittieren können, werden sich stärker auszahlen.

Aggregationspunkte, an denen die Daten von Geräten gesammelt werden, werden ebenfalls ein wichtiges Ziel sein.

Eine weitere potenzielle Schwachstelle von IoT-Systemen ist der Aggregationspunkt, an dem Daten von mehreren IoT-Geräten gesammelt werden. Ebenso wie die Steuerungsebene ist die Kompromittierung des Aggregationspunkts ein lukratives Ziel. Warum nicht die Hauptader anzapfen, anstatt viele einzelne Geräte anzugreifen und langsam nach und nach kleine Datenmengen zu sammeln? Anstatt einzelne Autos als Geisel zu nehmen, wäre es lohnenswerter, über die Wartungssysteme eines Autohändlers dessen gesamten Fahrzeugbestand zu übernehmen. Auch hier stellen Anmeldeinformationen und Authentifizierungssysteme die Schwachstellen dar. Da sich die meisten Aggregationspunkte für IoT-Geräte in der Cloud befinden, kommen natürlich auch die mit der Cloud verbundenen Schwachstellen und Bedrohungen zum Tragen.

Aggregationspunkte, an denen die Daten von IoT-Geräten gesammelt werden, werden ein wichtiges Ziel sein. Anmeldeinformationen und Authentifizierungssysteme stellen die Schwachstellen dar.

Diesen Bericht teilen



Ransomware wird internetfähige medizinische Geräte angreifen.

Wir wissen noch nicht, warum Angreifer medizinische Geräte, auf denen Patientendaten gesammelt werden, kompromittieren, aber es geschieht, und medizinische Daten werden exfiltriert. Dies wird sich vermutlich in den nächsten zwei bis vier Jahren fortsetzen, und außerdem werden wir erfahren, warum medizinische Daten gestohlen werden. Noch beunruhigender ist, dass medizinische Geräte zum Überwachen und Steuern der von Körperfunktionen (z. B. Herzschrittmacher, Insulinpumpen und Nervenstimulatoren) internetfähig werden. Skrupellose Angreifer werden diese medizinischen Geräte als den nächsten Schritt nach Ransomware-Angriffen auf Krankenhäuser sehen. Krankenhäuser sind zum Teil deswegen erfolgreiche Ransomware-Ziele, weil sie unmittelbaren Zugriff auf Informationen benötigen. Ein Herzschrittmacher ist das ultimative Beispiel für die Notwendigkeit von unmittelbarem Zugriff. Daher suchen Angreifer nach Schwachstellen in diesen internetfähigen Geräten und werden im Erfolgsfall in der Lage sein, hohe Geldbeträge zu erpressen.

Gesetze und Ländergrenzen

IoT-Bedrohungen und -Kompromittierungen werden Auslöser für politische Reaktionen sowie Regulierungsmaßnahmen sein. Die Geschwindigkeit des technologischen Fortschritts wird effektive Gesetze behindern und umgekehrt. Unterschiedliche oder sogar widersprüchliche Vorschriften in verschiedenen Ländern werden die Lage für Verbraucher, Gerätehersteller und Dienstanbieter erschweren.

Ehre unter Dieben?

Kürzlich äußerten sich Mitglieder der Hacker-Community nach einem Ransomware-Angriff auf ein Krankenhaus in Kalifornien abschätzig über die Angreifer und bezeichneten sie als die „dümsten Hacker aller Zeiten“, weil sie sich ausgerechnet dieses Ziel ausgesucht hatten. Zudem meinten sie: „Wenn dadurch jemand gestorben oder verletzt worden wäre, wäre das einfach daneben“. So unwahrscheinlich es auch klingt: Hacker haben in der Regel ein gewisses Maß an Mitgefühl. Auch wenn manche IoT-Angriffe aus finanzieller Sicht attraktiv erscheinen, denken einige von ihnen aufgrund der Möglichkeit, Verletzungen oder Todesfälle zu verursachen, durchaus über ihr Handeln nach und begrenzen Anzahl sowie Schwere ihrer Angriffe.

Gesetze hinken hinter der IoT-Gerätetechnologie und ihrer Einführung hinterher, was zu Rechtsstreitigkeiten führt.

Dass die Gesetze nicht mit dem technologischen Wandel Schritt halten können, ist allgemein bekannt. Die Vorteile von IoT-Geräten und -Systemen (bessere Ergebnisse im Gesundheitswesen, bei der Fertigungseffizienz und im Privatbereich sowie zahlreiche andere Möglichkeiten) werden die Einführung trotz Sicherheits- und Datenschutzbedenken vorantreiben. Daher wird es zu Vorfällen kommen, die Anlass zu Rechtsstreitigkeiten, Protesten und Empörung bei den Verbrauchern geben werden. Die Gesetze werden sich aufgrund kultureller Normen und der Geschwindigkeit der Gesetzgebung von Land zu Land stark unterscheiden. Das Verfassen der Gesetze wird aufgrund konkurrierender und widersprüchlicher Interessen eine große Herausforderung für die Gesetzgeber darstellen. Einige Rechtssysteme, wie beispielsweise die EU, werden dabei eine Vorreiterrolle einnehmen, während andere so lange wie möglich zusehen und abwarten werden.

Gesetze und kulturelle Unterschiede in Bezug auf den Datenschutz werden von Land zu Land stark voneinander abweichen.

Der Datenschutz wird im Mittelpunkt der Gesetze im Zusammenhang mit verbraucherorientierten IoT-Geräten, Diensten sowie den von diesen gesammelten Daten stehen. Dies wird größtenteils auf dem Druck durch die Verbraucher beruhen und sich nach einigen großen Datendiebstählen intensivieren. Die Reaktionen werden erheblich durch kulturelle Normen

Der Datenschutz wird im Mittelpunkt der Gesetze im Zusammenhang mit verbraucherorientierten IoT-Geräten, Diensten sowie den von diesen gesammelten Daten stehen. Die Reaktionen werden durch kulturelle Normen beeinflusst werden, und der Umgang mit diesen Unterschieden wird für Unternehmen eine Herausforderung darstellen.

Diesen Bericht teilen



beeinflusst und je nach Land, Branche oder anderen Kategorien sehr unterschiedlich ausfallen. Der Umgang mit diesen Unterschieden wird für Unternehmen eine große Herausforderung darstellen und dazu führen, dass einige in bestimmten Märkten verzögert oder gar nicht aktiv werden.

Die Sicherheit von IoT-Geräten wird für Unternehmen zu einem wichtigen Kaufkriterium. Für Verbraucher spielt hingegen der Datenschutz eine wichtigere Rolle.

Zwei getrennte, jedoch verwandte Aspekte werden bei den Anbietern für IoT-Geräte und Sicherheit führen. Unternehmen werden die Sicherheit von IoT-Geräten und -Systemen als eines der wichtigsten Kaufkriterien sehen. Dies wird Funktionen wie Gerätezertifizierungen, Datenverschlüsselung, vertrauenswürdige Aktualisierungen, Hardware-basierte Sicherheit sowie vertrauenswürdige Ausführungsumgebungen fördern. Verbraucher werden beim Kauf von IoT-Geräten zunehmend den Datenschutz berücksichtigen, sich im Zweifelsfall aber weiterhin eher für den Komfort entscheiden. Diese Sichtweise wird zu verbesserter Verschlüsselung führen und möglicherweise Merkmale wie Geräteanonymität und direkte oder indirekte Vergütung für die Zustimmung zur Erfassung sowie Nutzung persönlicher Daten vorantreiben.

Reaktionen der Anbieter

Bedrohungen, Kompromittierungen und Gesetze werden Hersteller von IoT-Geräten, Dienstleister sowie Anbieter von Sicherheitsprodukten zu Reaktionen in Bezug auf ihre Technologien und Dienste veranlassen. Gerätesicherheit und Datenschutz werden verbessert, Maßnahmen zum Schutz der Benutzeridentität entwickelt, Hardware-basierte Abwehrmaßnahmen erweitert und Versicherungen auf IoT-Implementierungen ausgeweitet. Dies sind unsere sieben wichtigsten Erwartungen bezüglich der Reaktionen auf IoT-Bedrohungen in den nächsten zwei bis vier Jahren:

Wenn Sie für das Produkt nicht bezahlen, sind Sie selbst das Produkt.

Verbraucher erkennen allmählich, dass ihre Daten auf IoT-Geräten, wie beispielsweise Smartphones, wertvoll sind und dass ihnen für die Weitergabe dieser Daten eine Vergütung zusteht. Kostenlose Produkte und Dienste, die durch Datensammlung oder zielgerichtete Werbung Umsätze generieren, werden dies in den nächsten zwei bis vier Jahren deutlich offener tun. Einige werden kostenpflichtige Optionen ohne Datensammlung anbieten, während andere den Verbrauchern abhängig von der Menge der gesammelten Daten unterschiedliche Beträge zahlen werden. Dies alles setzt voraus, dass die Entwickler von IoT-Geräten und -Systemen Sicherheit sowie Datenschutz integrieren.

Neue und verbesserte Verschlüsselungsoptionen.

Als logische Folge der vorherigen Prognose wird die Möglichkeit, von IoT-Geräten generierte Daten bei der Übertragung zwischen Ursprung und Ziel zu schützen, äußerst wichtig werden, um Man-in-the-Middle-Angriffe zu verhindern. Ob Remote-Kameras, Zahlungskartenleser, Standortverfolgungsgeräte oder Überwachungssysteme in der Fertigung: Die Midstream-Erfassung von durch IoT-Geräte generierten Daten ist zurzeit zu einfach. Anbieter werden mit mehr Verschlüsselungsoptionen und längeren Schlüsseln zur Verbesserung der Sicherheit sowie Hardware-Unterstützung zur Minimierung der Leistungsauswirkungen reagieren. Diese Optionen werden wir in den nächsten vier Jahren sehen.

Ein Teil der IoT-Geräte-Hardware wird über integrierte Datenschutz- und Sicherheitsfunktionen verfügen.

Sei es aufgrund der Formfaktoren, der hohen Stückzahlen oder der fehlenden menschlichen Interaktion: Der Schutz von IoT-Geräten durch Software ist schwieriger als bei herkömmlichen IT-Geräten. Daher wird Hardware-basierte Sicherheit erheblich wichtiger sein. Beispielsweise enthalten manche Prozessoren bereits vertrauenswürdige Ausführungsumgebungen, in denen nur festgelegte Prozesse ausgeführt werden und auf Daten zugreifen dürfen. Die Entwickler von IoT-Geräten werden diese Umgebungen nutzen. In zwei bis vier Jahren werden die Hersteller von IoT-Geräten mit diesem Produktmerkmal werben, und wir werden sogar erste partitionierte oder vertrauenswürdige Apps sehen, die über die jeweiligen App-Märkte für Geräte verfügbar sein werden. Je mehr Sicherheit in die IoT-Geräte-Hardware integriert ist, desto größer ist die Wahrscheinlichkeit, dass diese eine solide Grundlage für gute Sicherheit und guten Datenschutz darstellt.

Anbieter von Sicherheitsprodukten werden Branchenstandards zum Schutz der IoT-Geräteidentität einführen und unterstützen.

Ein Ansatz für die Verbesserung des Datenschutzes besteht darin, sicherzustellen, dass Dienstanbieter nie die Identität von IoT-Geräten kennen. Die Authentifizierung sowie Überprüfung der Geräteidentität kann abstrahiert und von einem Drittanbieter bereitgestellt werden, der dann dem Dienstanbieter bestätigt, dass ein IoT-Gerät Mitglied einer vertrauenswürdigen Gruppe ist. Eine interessante Möglichkeit ist die Verwendung der Blockchain-Technologie, die Ähnlichkeit mit der von Bitcoin verwendeten Technologie hat und die Anonymität von Transaktionen gewährleistet, damit diese nicht mit einem bestimmten IoT-Gerät oder Konto verknüpft werden können. Daten können zwar dennoch gesammelt und verkauft werden, jedoch nur als aggregierter Satz und nicht personenbezogen. Wir gehen davon aus, dass sich diese Methoden innerhalb von vier Jahren schnell von proprietären Techniken zum Branchenstandard entwickeln werden.

Es werden Steuerungssysteme zur automatischen, aggregierten Verwaltung und Absicherung von IoT-Geräten entwickelt.

Es wird Steuerungssysteme für IoT-Geräte geben, um die enorme Anzahl der IoT-Geräte zu integrieren und zu schützen, die voraussichtlich bis zum Jahr 2020 online sein werden.

Die große Anzahl sowie die manchmal begrenzten Funktionen von IoT-Geräten machen es unmöglich, diese so wie herkömmliche IT-Systeme zu verwalten und zu schützen. Daher werden Steuerungssysteme zur automatischen, aggregierten Verwaltung und Absicherung von IoT-Geräten entwickelt. Zu den wichtigsten Funktionen werden autonome Geräteauthentifizierung und -überprüfung, Software- und Aktualisierungsverwaltung für IoT-Geräte sowie Datenschutz- und Sicherheitsrichtlinienverwaltung gehören. Aufgrund der Schwierigkeit, alle im Umlauf befindlichen Geräte schnell zu aktualisieren, werden zusätzliche Sicherheitsmaßnahmen zum Schutz der Geräte vor Zero-Day-Exploits erforderlich sein.

Verhaltensüberwachung für IoT-Geräte wird eingeführt.

Als Schutztechnik wird in den nächsten zwei bis vier Jahren Verhaltensüberwachung hinzukommen. Diese soll ungewöhnliche oder nicht autorisierte Aktionen auf IoT-Geräten erkennen und entsprechend reagieren. Dies wird besonders wichtig als Abwehrmaßnahme gegen Angriffe mit Zero-Day-Exploits und gestohlenen Anmeldeinformationen, bei denen herkömmliche Sicherheitsvorkehrungen machtlos sind. Wenn auf einem IoT-Gerät oder dem zugehörigen Controller ungewöhnliche Aktivitäten erkannt werden, sei es abhängig von der Uhrzeit (Warum wird diese Aktivität um 2:00 Uhr morgens angefordert?), vom Kontext anderer IoT-Geräte (Warum ist dieses Ventil geöffnet, wenn der zugehörige Prozess nicht ausgeführt wird?) oder von einer Blacklist (Die Bremse meines Autos darf niemals remote deaktiviert werden.), kann der Befehl blockiert, eine Sofortmaßnahme zur Minimierung der Bedrohung eingeleitet oder ein Mensch um Anweisungen gebeten werden.

Diesen Bericht teilen



Internetversicherungen und Risikoverwaltung für Implementierungen von IoT-Systemen werden eine größere Rolle spielen.

Schwachstellen in IoT-Geräten und -Systemen verschärfen Risiken. Während Unternehmen und Verbraucher IoT-Geräte aufgrund ihrer Vorteile weiterhin nutzen werden, versuchen Unternehmen, das Risiko einzudämmen. Zu diesem Zweck wird es entsprechende Versicherungsangebote geben. Dazu müssen Unternehmen sowie Versicherer Mindestbetriebsanforderungen im Einklang mit den sich verändernden Gesetzen und Vorschriften definieren sowie überwachen. Aufgrund der möglichen Schäden durch einen erfolgreichen IoT-Angriff werden Versicherungspolicen elementarer Bestandteil der IoT-Systemplanung werden.

Fazit

Angesichts Milliarden von IoT-Geräten, die in den nächsten Jahren online sein werden, ist die Bedrohung durch Cyber-Angriffe sehr real. Es wird jedoch eine Weile dauern, bis Kriminelle herausgefunden haben, wie sie Angriffe zu Geld machen können. Daher wird die Anzahl der erfolgreichen Angriffe auf diese Geräte wahrscheinlich klein bleiben.

Die IoT-Einführung wird die Angriffsfläche enorm vergrößern. Unzureichende Sicherheit und Anfängerfehler der IoT-Gerätehersteller werden das Problem verschärfen. Einige dieser Schwachstellen werden als anfängliche Angriffsvektoren für Steuerungs-, Überwachungs- und Informationssysteme ausgenutzt werden. Ransomware ist kurzfristig die wahrscheinlichste Bedrohung. Aggregationspunkte, an denen die Daten von IoT-Geräten gesammelt werden, werden kurzfristig ebenfalls ein wichtiges Ziel sein.

Der Verlust der Privatsphäre für Verbraucher und die als Reaktion erlassenen Gesetze werden für Schlagzeilen sorgen. Der Komfort und die Einsparungen durch IoT-Geräte werden jedoch die Nachteile aufwiegen, sodass die Einführungs-raten hoch bleiben werden. Vorschriften werden sich je nach Rechtssystem stark unterscheiden sowie dem Markt hinterherhinken, und Rechtsstreitigkeiten werden für die Zukunft des IoT-Markts eine wichtige Rolle spielen.

Anbieter werden eine Fülle von Reaktionen entwickeln, um die Einführung im Markt zu fördern und zu unterstützen. Neue Verschlüsselungsoptionen, Sicherheit und Datenschutz auf Chip-Ebene, Gerätesteuerungssysteme zur automatischen Verwaltung und Absicherung von IoT-Geräten sowie Verhaltensüberwachung für IoT-Geräte werden schnell den Online-Betrieb aufnehmen und weiterentwickelt werden.

Eine wichtige Änderung wird darin bestehen, den immanenten Wert der persönlichen Daten besser zu verstehen. Verbraucher werden Optionen für die Weitergabe der von IoT-Geräten gesammelten persönlichen Daten sowie eine Vergütung erwarten.



Prognosen für 2017

Feedback teilen



Prognosen für 2017

Ransomware geht in der zweiten Hälfte des Jahres 2017 zurück

Christiaan Beek

NO MORE RANSOM!

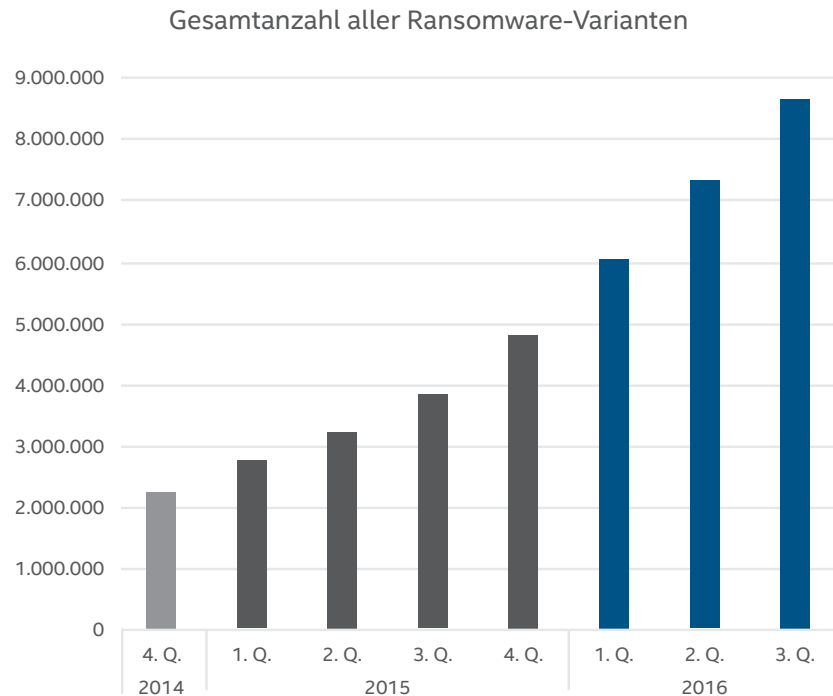
Wir sagen voraus, dass Umfang und Effektivität von Ransomware-Angriffen in der zweiten Hälfte des Jahres 2017 zurückgehen werden.

Bis dahin wird Ransomware auch weiterhin eine ernsthafte Bedrohung bleiben. Ransomware-as-a-Service, in Untergrundmärkten angebotene individualisierte Ransomware sowie kreative Ableitungen von Open-Source-Ransomware-Code werden die Sicherheitsbranche in der ersten Hälfte des Jahres beschäftigt halten. Die Auswirkung von Ransomware auf alle Branchen und Regionen wird die Sicherheitsbranche zwingen, gezielte Maßnahmen zu ergreifen. Wir sagen voraus, dass Initiativen wie die Kooperation „[No More Ransom!](#)“ (Nie mehr Lösegeld!) bis Ende 2017 die Entwicklung und Veröffentlichung von Ransomware-Schutztechnologien sowie kontinuierliche Strafverfolgungsaktionen den Umfang und die Effektivität von Ransomware-Angriffen verringern werden.

Das Konzept von Ransomware wurde erstmalig Anfang der 1990er Jahre demonstriert. Als Bitcoin eingeführt und im Jahr 2013 erstmals von der Ransomware-Familie CryptoLocker genutzt wurde, öffnete das die Tür für anonyme Lösegeldzahlungen, die die Angreifer vor der Entdeckung schützten. Die „Pioniere“ von Ransomware, wie CryptoLocker und CryptoWall, stammen aus der Welt der Banking-Trojaner und hatten umfangreiche Erfahrung darin, erfolgreiche Cyber-kriminelle Aktionen auf die Beine zu stellen. Sie machten schnell ihre Erfahrungen und konnten ihre Infrastruktur bzw. ihren Code anpassen, sobald das Geschäft schlechter lief. Diese Gruppen werden auch weiterhin im Ransomware-Geschäft bleiben und neue Profitmöglichkeiten suchen. Derzeit haben wir es mit vielen kleineren und weniger fachkundigen Gruppen zu tun, die von den Umsätzen der organisierten Gruppen angezogen werden. Wie im [Bericht zu CryptoWall Version 3](#) der Cyber Threat Alliance besprochen, können die Umsätze einer einzigen Ransomware-Familie den Betrag von 325 Millionen überschreiten. Solche Beispiele führten, wie mehrfach berichtet, zu einem enormen Anstieg an Ransomware-Familien und -Angriffen. Einzelne Kriminelle möchten an dieser sprudelnden Geldquelle ebenfalls ihren Anteil haben und hängen sich entweder als Partner an oder nutzen öffentlich verfügbaren Code. Wir rechnen damit, dass diese kleinen Initiativen im Laufe des Jahres 2017 zurückgehen, da die Sicherheitsbranche sowie internationale Strafverfolgungsbehörden zusammenarbeiten werden, um solche Akteure zu ermitteln und auszuschalten.

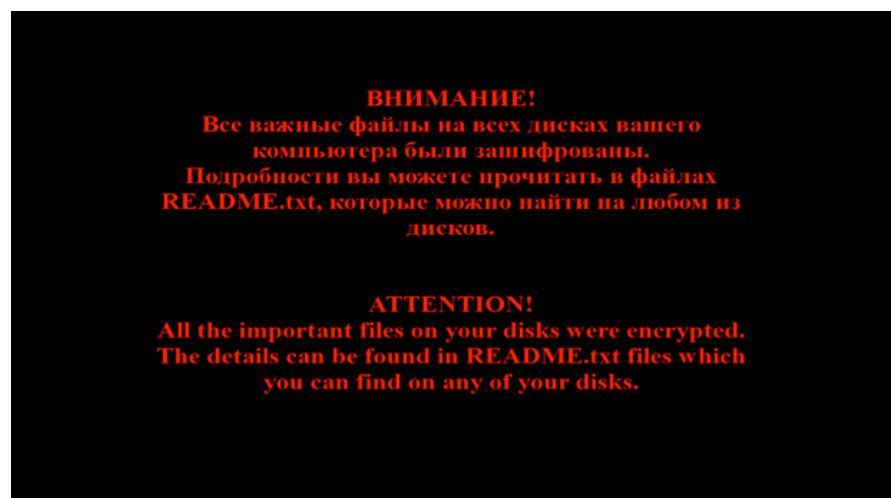
Diesen Bericht teilen





Quelle: McAfee Labs, 2016.

Zudem hat die Sicherheitsbranche damit begonnen, Tools und Funktionen zu entwickeln, die Unternehmen beim Kampf gegen Ransomware unterstützen. Während der Konferenz Black Hat USA 2016 stellte das [Intel Security Advanced Threat Research-Team](#) eine Demonstration von Ransomware-Konzeptstudien vor, die IoT-Geräte angreifen. Dazu gehörte auch eine Variante, die ein Auto-„Infotainment“-System angreift und Bremsen sowie Anlasser des Autos blockiert, bis das Lösegeld gezahlt wurde. Das Advanced Threat Research-Team konzentriert sich auf zukünftige Bedrohungen sowie auf Branchenkooperationen, um die Aufmerksamkeit für dieses Thema zu wecken und Ransomware-Bedrohungen schon zu einem frühen Zeitpunkt abzuwehren.





Bitcoin-Mixer: Unterbricht die Verbindung zwischen einer Bitcoin-Adresse, die Coins überträgt, und der Zieladresse.

Doch was ist mit virtuellen Währungen, die dem Ransomware-Wachstum Tür und Tor geöffnet haben? Wird Bitcoin überleben oder werden die Ransomware-Akteure sich anderen Zahlungsmethoden zuwenden? Selbst die Nutzung von Bitcoin-Mixern genügt nicht, um die Analyse von Transaktions-Links zu verhindern. Außerdem wurden andere Bitcoin-Dienste auf der Bitcoinconference von den Teilnehmern kritisiert, die sich über fehlendes Mixing einiger Dienste sowie die unsichere Verwendung von Supernodes beschwerten, da sich auf diese Weise die Identität aufdecken ließe. Aus diesem Grund sagen wir voraus, dass es bei Lösegeld-Zahlungsmethoden einen Wechsel hin zu virtuellen Währungen wie Monero und Zerocoin/Zerocash geben wird.

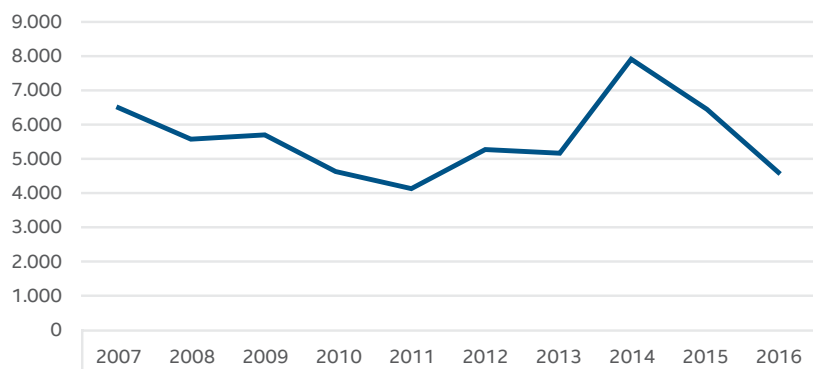
Schwachstellen-Exploits unter Windows gehen zurück und legen auf anderen Plattformen zu

Bing Sun, Haifei Li, Stanley Zhu und Debasish Mandal

Die Ausnutzung Client-seitiger Software-Schwachstellen wurde in den letzten Jahren immer schwieriger, was die Entwicklungskosten für generische und zuverlässige Exploits in die Höhe trieb. Zum erfolgreichen Eindringen in die neuesten Betriebssysteme (z. B. in einen Microsoft Edge-Browser auf dem neuesten Patch-Stand unter Windows 10 mit 64 Bit) müssen Angreifer häufig mehrere raffinierte Schwachstellen zusammen mit hochentwickelten Ausnutzungstechnologien kombinieren. Obwohl erfolgreiche Angriffe bei Hacker-Wettbewerben wie Pwn2Own 2016 demonstriert wurden, haben wir noch keine derart raffinierten Exploits im realen Einsatz registriert. Wir vermuten, dass solche Exploits nur wenigen Akteuren zur Verfügung stehen und nur bei sehr schwerwiegenden raffinierten Angriffen zum Einsatz kommen.

Neue gefundene Schwachstellen

National Vulnerability Database (US-Datenbank zu Softwareschwachstellen)



Daten für das Jahr 2016 bis zum 20. September

Diesen Bericht teilen



Wir gehen davon aus, dass Schwachstellenausnutzungen in Windows und Flash weiterhin abnehmen, während Exploits von Infrastruktur-Software und Virtualisierungs-Software zunehmen werden.

Beim Blick in den Bericht zu den [Bedrohungsprognosen von McAfee Labs für 2016](#) zeigt sich, dass viele unserer Vorhersagen zu Schwachstellen-Exploits wahr geworden sind. Basierend auf unseren Beobachtungen in diesem Jahr hoffen wir auf eine ähnliche Erfolgsrate bei unseren Schwachstellenprognosen für 2017.

- **Adobe Flash:** Dies ist immer noch das bevorzugte Ziel der meisten realen Schwachstellenausnutzungen. Flash-Zero-Day-Schwachstellen wie CVE-2016-4117 und CVE-2016-1019 waren 2016 für etwa die Hälfte aller von Sicherheitsunternehmen entdeckten Zero-Day-Angriffe verantwortlich. Im Jahr 2015 sagten wir voraus, dass die Zahl der Flash-Ausnutzungen 2016 zurückgehen würde, da im Juli 2015 eine wichtige Behebungsfunktion (Überprüfung der Cookie-Länge des Vector-Objekts) eingeführt wurde. Aus diesem Grund nahmen reale Flash-Exploits 2016 erheblich ab (bis zum aktuellen Zeitpunkt lediglich vier, während es 2015 noch elf waren). Ein neuer Flash-Exploit (die Nutzung von ByteArray und BitmapData in CVE-2015-7645) kam schon kurz nach der Einführung der Vektor-Behebung auf. Adobe fügt auch weiterhin neue Behebungsmaßnahmen zu Flash hinzu, z. B. Überprüfung der Cookie-Länge des ByteArray-Objekts, isolierter Heap, System-Heap und Speicherschutz. Obwohl keine dieser Funktionen perfekt ist und einige sogar zu neuen Problemen führten, erschweren sie Ausnutzungen doch erheblich. Daher gehen wir davon aus, dass Flash als Angriffsvektor im Jahr 2017 weiterhin zurückgehen wird. Das Finden von Flash-Schwachstellen wird schwieriger, und ihre Ausnutzung noch komplizierter.
- **Microsoft Internet Explorer und Edge:** Wie wir im Bericht zu den *Bedrohungsprognosen für 2016* vorhersagten, bleibt die Zahl der Angriffe auf Internet Explorer und Edge auch weiterhin minimal. In diesem Jahr haben wir bislang keine echten Zero-Day-Exploits für Internet Explorer im realen Einsatz erlebt. Obwohl die Exploits CVE-2016-0189 und CVE-2016-0034 über einen Browser übertragen und ausgeführt werden, handelt es sich tatsächlich um Schwachstellen des Skriptmoduls bzw. von .NET Framework. Dank einer verringerten Angriffsfläche (z. B. kein Dokumentenmodus, kein Visual Basic Script, keine Browserhilfsobjekte und ActiveX, kein Silverlight) sowie verbesserten Schutzmaßnahmen ist der Edge-Browser noch sicherer. Seit seiner Veröffentlichung gab es keine Zero-Day-Exploits für Edge im realen Einsatz. Im Allgemeinen scheinen die Schutzmaßnahmen der Microsoft-Browser sehr effektiv zu sein. Einige Schutzmaßnahmen halfen, bestimmte Schwachstellenkategorien zu beseitigen (z. B. haben Use-After-Free-Fehler seit der Einführung von isolierten Heaps und Speicherschutz erheblich abgenommen), während andere die Schwachstellenausnutzung erheblich erschweren. Der Ablaufsteuerungsschutz ist eine der wichtigsten Schutzfunktionen und verhindert, dass Exploits den Programmausführungsfluss kapern. Wir sagen voraus, dass Internet Explorer- und Edge-Ausnutzungen im Jahr 2017 vor allem auf 64-Bit-Plattformen schwieriger werden, da die Erstellung und Kontrolle spezifischer Speicher-Layouts extrem schwierig sein wird.
- **Java, PDF und Microsoft Office:** Bei den Angriffen auf Java-, PDF- und Office-Anwendungen gab es 2016 nur wenige Änderungen. Früher rechneten wir damit, dass die Ausnutzungen von Office-Schwachstellen aufgrund der riesigen Angriffsfläche und des komplexen Codes erheblich zunehmen würden. Dies ist jedoch nicht eingetreten. Das könnte daran liegen, dass Office keine Skriptsprachen unterstützt, was die Entwicklung von Exploits erschwert. Andererseits rechnen wir für das kommende Jahr mit anderen Office-basierten Bedrohungen, wie z. B. Makro-basierter Ransomware.

Diesen Bericht teilen





- **Windows-Kernel:** Obwohl einige Schutzmaßnahmen (Supervisor Mode-Ausführungsschutz, Win32k-Systemaufruf-Filterung, Verbesserungen bei der zufälligen Anordnung des Layouts des Kernel-Adressraums, im Benutzermodus durchgeführte Schriftartenverarbeitung) eingeführt wurden, spielen Kernel-Mode-Exploits immer noch eine große Rolle. Einer der Gründe dafür ist, dass sie häufig das beste Mittel zur Überwindung von Sandboxes (z. B. AppContainer) sowie zur Berechtigungs eskalation sind. Dies zeigte sich bereits bei Zero-Day-Angriffen (CVE-2016-0165/0167) und Hacker-Wettbewerben (CVE-2016-0176). Angesichts der großen Angriffsfläche sowie der im Vergleich zum Benutzermodus schwächeren Schutz- und Abwehrmaßnahmen im Kernel-Bereich gehen wir davon aus, dass Ausnutzungen des Kernel-Modus auch 2017 ein großes Thema sein werden.
- **Infrastruktur-Software:** Angriffe auf Infrastruktur-Schwachstellen werden im Jahr 2017 sehr aktiv sein. Auf der Empfehlungsliste für OpenSSL sehen wir mit jeder neuen Version viele behobene Schwachstellen. Abseits von OpenSSL finden wir kritische Schwachstellen in anderer Open-Source-Software, z. B. CVE-2015-7547 (ein Stack-basierter Buffer Overflow im DNS-Client glibc) sowie CVE-2016-5696 (eine Linux-Schwachstelle, die das Kapern von Internetdatenverkehr ermöglicht).
- **Ältere Komponenten im Vergleich zu neuen Funktionen:** Obwohl sich die meisten Malware-Autoren auf Funktionen wie das Windows-Subsystem für Linux mit 216 neuen Systemaufrufen und 700 KB Code konzentrieren, haben sich andere älteren Komponenten zugewandt. Seit der kritischen Schwachstelle GHOST (CVE-2015-0234), die seit mehr als 15 Jahren in glibc existiert und im letzten Jahr entdeckt wurde, haben Sicherheitsforscher damit begonnen, älteren Code erneut zu untersuchen. Im Jahr 2016 wurde beispielsweise ein schwerwiegender Fehler (BadTunnel) im Web Proxy Autodiscovery Protocol entdeckt. Der Fehler ist seit 20 Jahren im Code vorhanden. Da die Sicherheit wichtiger älterer Komponenten jahrelang vernachlässigt wurde, sind Sicherheitsforscher damit beschäftigt, seit langem vorhandene Schwachstellen zu beseitigen. Wir gehen davon aus, dass 2017 weitere Fehler gefunden und behoben werden.
- **Virtualisierungs-Software:** Angesichts der rasanten Durchsetzung von Cloud-Technologien ist Virtualisierungssicherheit ein heißes Thema, das große Aufmerksamkeit bei Sicherheitsforschern und Angreifern findet. Viele umfangreiche Forschungsergebnisse haben den Weg in die Öffentlichkeit gefunden. Im Juli wurde eine kritische Schwachstelle im Xen-Hypervisor behoben, die einem Gast das „Entkommen aus dem Host“ erlaubt (die „Po Tian“-Schwachstelle, CVE-2015-7835). Im September entdeckte das Intel Security Advanced Threat Research-Team die Xen-Schwachstelle XSA 188, die dem Cloud-Hosting-Service Linode den Neustart seines Xen-basierten Servers erlaubte. Kritische Fehler wurden auch in VMware dokumentiert, z. B. CVE-2016-5332, CVE-2016-2077 und CVE-2016-2079. Microsoft Hyper-V ist nicht immun: Wir registrierten mehrere CVEs, die sich auf Hyper-V bezogen (MS16-045 und MS16-046). Hinzu kommt, dass die virtualisierungs-basierte Sicherheit bzw. der virtuelle sichere Modus von Microsoft in Windows 10 ein neues Ziel ist – einige der damit zusammenhängenden Sicherheitsprobleme wurden bereits gefunden und veröffentlicht. Andererseits wurden zwar viele Schwachstellen in Virtualisierungs-Software gefunden, dennoch fehlen bei VM-Angriffen (virtuelle Maschinen) im Vergleich zu den ausgereiften Browser-Exploits immer noch systematische und universelle Ausnutzungstechniken sowie Methoden, die bestimmte Klassen von VM-Sicherheitsproblemen generisch abdecken können. Die meisten Fälle von VM-Ausbrüchen sind stark von den Schwachstellen selbst abhängig,

z. B. CVE-2015-7835, CVE-2016-3710 und CVE-2015-7504. Da VMs zu Zielen für Angreifer geworden sind, rechnen wir damit, dass es nur eine Frage der Zeit ist, bis wir systematische Exploits und hochentwickelte Angriffe auf Virtualisierungs-Software erleben werden. 2017 könnte das Jahr werden, in dem dies geschieht.

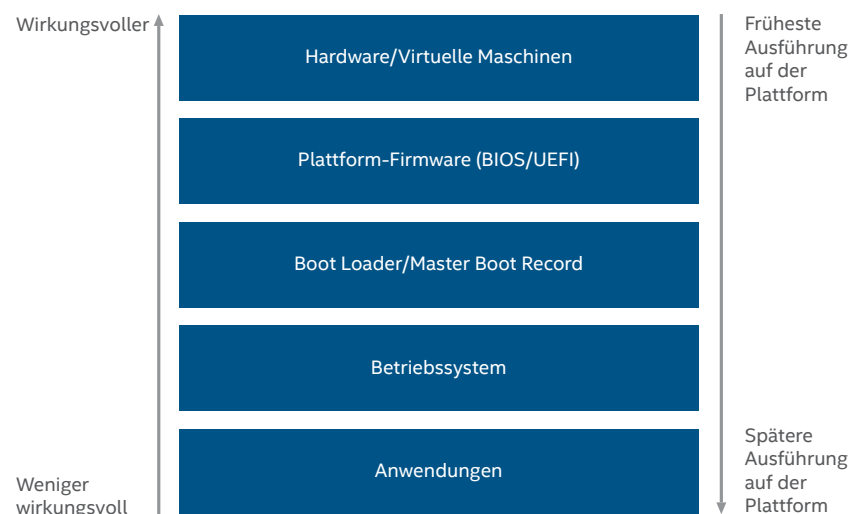
- **Sicherheitsprodukte:** Im Jahr 2016 fanden wir zahlreiche schwerwiegende Schwachstellen in Sicherheitsprodukten. Anfang des Jahres fanden Google-Forscher eine schwerwiegende Remote-Code-Ausführungsschwachstelle in FireEye-Appliances. Anschließend entdeckten Google-Forscher Schwachstellen in Produkten der meisten Malware-Schutz-Anbieter. Und im Sommer zeigten veröffentlichte Daten der Equation Group viele Exploits (einschließlich mehrerer nicht gepatchter Zero-Day-Schwachstellen), die verschiedene Firewall-Produkte angreifen. Diese Entwicklung wird sich 2017 ohne Zweifel fortsetzen.

Hardware- und Firmware-Bedrohungen ein immer größeres Ziel für raffinierte Angreifer

Yuriy Bulygin

Software, einschließlich Betriebssystemen und Anwendungen, benötigt per Definition eine Hardware-Basis. Deshalb können Hardware-Schwachstellen den Betrieb und die Sicherheit des gesamten Software-Stacks untergraben. Die Ausnutzung einer Hardware-Schwachstelle kann ein ganzes System kompromittieren und erfordert keinen Exploit des Software-Stacks. Des Weiteren können Systeme, deren Hardware erfolgreich angegriffen wurde, ohne einen Austausch der anfälligen Hardware schwer zu patchen sein. Schließlich sind die Software-basierten Sicherheitsmechanismen und Schutzmaßnahmen des Systems nicht mehr verlässlich, da sie voraussetzen, dass die Hardware nicht kompromittiert wurde.

Es gibt jedoch auch Abhilfe. Hardware ist Angriffen weniger ausgesetzt als Software-Stacks, und der Angriff auf die Hardware umfasst – im Gegensatz zu den zahlreichen Software-Schwachstellen in Software-Stacks – beinahe immer eine Schwachstelle in der Hardware-Logik. Die geringere Angriffsfläche der Hardware erhöht die Komplexität von Angriffen. Daher sehen wir sehr wenige Hardware-Schwachstellen und Vorfälle, bei denen die Hardware angegriffen oder erfolgreich ausgenutzt wird. Deshalb gilt, dass durchschnittliche Malware fast nie die Hardware angreift.



Diesen Bericht teilen



Sicherheitsforscher haben in den letzten Jahren einige Hardware-Schwachstellen entdeckt – einschließlich Schwachstellen bei Mikroprozessoren und DRAM-Technologien [1, 2, 3, 4] sowie Schwachstellen, die vom Betriebssystem unabhängige Side-Channel-Angriffe ermöglichen [1, 2, 3]. Diese können Cloud-Umgebungen beeinträchtigen, da die auf dem gleichen Server gehosteten VMs (Co-Location-VMs) angreifbar werden [1, 2, 3, 4].

Computersysteme verfügen häufig über spezialisierte Soft- und Hardware, die das System initialisiert, bootet sowie grundlegende Wartungsaufgaben durchführt. Diese spezialisierte Soft- und Hardware hat ihren eigenen Mikrokontroller- und Software-Stack, der auch als Firmware bezeichnet wird. Beispiele für diese spezialisierte Firmware sind BIOS, UEFI (Unified Extensible Firmware Interface), EFI sowie Coreboot. Zudem verfügen externe Geräte wie USB-, Festplatten- und SSD-Laufwerke, Erweiterungskarten sowie selbst Ladeadapter über ihre eigene Firmware.

Diese hat Eigenschaften, die sie zu einem interessanten Angriffsziel machen. Häufig befindet sich Firmware dauerhaft auf nichtflüchtigem Speicher wie Flash-Chips und verfügt über Vollzugriff auf die verwaltete Hardware. Zudem ist sie meist für Betriebssysteme und Sicherheits-Software unsichtbar. System-Firmware wird ausgeführt, bevor das Betriebssystem die Kontrolle übernimmt. Zudem ist Firmware selbst nur Software, sodass sie ähnliche Schwachstellen, dafür aber weniger integrierte Schutzmaßnahmen und Exploit-Sicherungen besitzt.

Bedrohungsforscher haben nachgewiesen, dass Schwachstellen in System-Firmware [1, 2, 3] Angriffe auf die Pre-Boot-Authentifizierung ermöglichen können. Dazu gehören auch Angriffe auf Systeme mit vollständiger Datenträgerverschlüsselung durch das Trusted Platform Module (z. B. Microsoft Windows BitLocker [1, 2]) oder Windows Secure Boot [1, 2, 3, 4]. Pre-Boot-Angriffe erlauben die Installation verborgener und dauerhafter Rootkits, Backdoors oder Würmer [1, 2, 3, 4, 5] und dringen in vertrauenswürdige Ausführungsumgebungen ein, die auf Virtualisierungstechnologien basieren, z. B. sicherer Kernel und isolierter Benutzermodus mit der Überwachung von Anmeldeinformationen und dem DeviceGuard in Microsoft Windows 10 [1, 2].

Abseits von System-Firmware fanden Sicherheitsforscher Firmware-Schwachstellen in USB-Geräten [1, 2, 3], Netzwerkkarten [1, 2], eingebetteten und Tastatur-Controllern [1], Baseboard Management-Controllern [1, 2, 3], LTE/3G/GSM-Baseband-Modems [1, 2], CPUs [1, 2], Akkus [1], Routern in Privathaushalten [1, 2, 3, 4], Bürodrukern [1, 2], IP-Telefonen [1], Firmware sowie sicherer Software für ARM TrustZone [1, 2, 3, 4, 5] und vielen anderen Komponenten.

Angrifer wie staatliche Stellen – unterstützte Hacker-Gruppen, Industriespionageteams und organisierte kriminelle Gruppen sind an Angriffen auf System-Firmware interessiert. Vor zwei Jahren nahm die Equation Group die Firmware von Festplatten ins Visier [1]. Im Jahr 2015 sahen wir das erste kommerzielle UEFI-Firmware-Rootkit der Gruppe Hacking Team [1]. Kürzlich zeigte ein Datenpaket der Gruppe Shadow Brokers, dass diese Organisation – der Verbindungen zur Equation Group nachgesagt werden – die Firmware von Netzwerk-Firewalls mit dauerhaften Implantaten angreift [1, 2].

Hard- und Firmware sind komplexe Ziele, doch erfolgreiche Attacken bieten den Angreifern maximale Persistenz, gute Versteckmöglichkeiten, Zugriff auf eine Vielzahl an Hardware-Ressourcen sowie die Möglichkeit zum Implantieren von Backdoors in die Software-Stacks des Systems. Wir sagen voraus, dass raffinierte Angreifer (z. B. staatliche Stellen) im Jahr 2017 auch weiterhin nach ausnutzbaren Schwachstellen in Hard- und Firmware suchen werden. Wir gehen davon aus, dass raffinierte Angreifer über die Möglichkeiten zur Ausnutzung von Systemen mit BIOS oder (U)EFI sowie Firmware auf anderen Gerätetypen wie SSD-Laufwerken, Netzwerkkarten und WLAN-Geräten verfügen.

Wir sagen voraus, dass raffinierte Angreifer im Jahr 2017 auch weiterhin nach ausnutzbaren Schwachstellen in Hard- und Firmware suchen werden. Wir gehen davon aus, dass sie über die Möglichkeiten zur Ausnutzung von Systemen mit BIOS oder (U)EFI sowie Firmware auf anderen Gerätetypen wie SSD-Laufwerken, Netzwerkkarten und WLAN-Geräten verfügen. Einige dieser raffinierten Exploits werden wahrscheinlich in gewöhnlichen Malware-Angriffen zum Einsatz kommen.

Diesen Bericht teilen



Einige dieser raffinierten Exploits werden wahrscheinlich in gewöhnlichen Malware-Angriffen zum Einsatz kommen. Im Jahr 2017 werden wir Malware erleben, die Bootkit-Komponenten nutzt, um UEFI-basierte Betriebssystem-Bootloader anzugreifen oder sogar Firmware-Rootkit-Komponenten zu installieren. Zudem wird es zu Firmware-Angriffen kommen, bei denen virtualisierungsbasierte vertrauenswürdige Ausführungsumgebungen wie VBS in Windows 10 angegriffen werden. Ebenfalls eine Rolle spielen wird Ransomware, die die ersten Stufen des Betriebssystem-Startvorgangs infizieren wird, z. B. Bootloader und Firmware.

Auf der Gegenseite werden sehr wahrscheinlich weitere kommerzielle Sicherheitstechnologien eingeführt, die die Firmware sowie andere grundlegende Systemkomponenten umfassender analysieren als bisherige Software-Stacks.

„Dronejacking“ führt zu Bedrohungen am Himmel

Bruce Snell

Drohnen sind ein immer alltäglicherer Anblick. Was als Spielzeug für Kinder und relativ preisintensives Hobby für Enthusiasten begann, ist jetzt richtig durchgestartet. Drohnen sind dabei, zu einem der wichtigsten Hilfsmittel für Lieferdienste, Strafverfolgungsbehörden, Fotografen, Landwirte, Nachrichtenmedien und viele andere zu werden. Es lässt sich kaum bestreiten, dass diese Fluggeräte für viele Arten von Unternehmen und Regierungsbehörden sehr wertvoll geworden sind. Kürzlich wurde ein Fall bekannt, bei dem eine Drohne mit einer vollständigen Hacker-Suite ausgestattet wurde und auf dem Dach eines Hauses, Unternehmens oder einer kritischen Infrastruktur landen und sich in das lokale WLAN-Netzwerk einhacken konnte.

Im Jahr 2015 wurde [auf der Konferenz DefCon mit einem Konzept-Hack demonstriert](#), wie einfach sich eine Spielzeugdrohne übernehmen lässt. Obwohl die Übernahme eines Kinderspielzeugs eher amüsant und nicht wie eine große Sache wirkt, wird das Problem angesichts der enormen Drohnenzahlen deutlich sichtbar.

- **Lieferdienste:** Sowohl Amazon als auch UPS haben Pläne bekannt gegeben, Pakete mit Drohnen zu liefern. Dies schafft ein realistisches Ziel für Kriminelle, die sich ohne viel Aufwand bereichern wollen. Lieferdrohnen werden höchstwahrscheinlich von einem dedizierten Standort gestartet, sodass die Flugmuster leicht sichtbar sind. Wenn jemand Lieferungen mittels „Dronejacking“ abfangen möchte, kann er sich einen Standort mit starkem Drohnenverkehr suchen und auf sein Ziel warten. Sobald eine Paketlieferdrohne ihn überfliegt, könnte die Drohne zum Landen gezwungen werden, sodass der Kriminelle das Paket stehlen kann. Der Fairness halber muss angemerkt werden, dass es sich bei diesen Diebstählen um eine Art Glücksspiel handeln würde: Da es keine einfache Möglichkeit gibt, an Informationen über den Paketinhalt heranzukommen, können diese Pakete praktisch alles enthalten.
- **Kameracrews:** Luftaufnahmen sind seit dem Aufkommen von Drohnen erheblich einfacher geworden. Eine schnelle Suche nach „Fotodrohnen“ führt zu Webseiten, die hochwertige und teure Ausrüstungen sowohl für Liebhaber als auch für professionelle Kameralente anbieten. Diese hochwertige Ausrüstung ist ein attraktives Ziel für das Dronejacking durch Kriminelle. Wenn der Kriminelle eine Drohne zum Landen zwingen kann, lässt sich ihre Ausrüstung verkaufen, sodass ihm das Geld buchstäblich in den Schoß fällt.

- **Persönliche Flugverbotszonen:** Bislang sind einige Fälle bekannt geworden, bei denen Menschen ihrem Ärger über die Drohnen über ihren Häusern Luft machten und entsprechende Maßnahmen ergriffen – mit Schrotflinten, geworfenen Steinen usw. Die Ausnutzung von Software-Schwachstellen in Drohnen kann dazu führen, dass jemand eine elektronische Barriere rund um ein Haus aufbaut, die zu nahe fliegende Drohnen entweder abschießt oder umleitet. Obwohl das für Menschen, denen ihre Privatsphäre wichtig ist, als Vorteil erscheinen könnte, sind Drohnen in vielen Ländern und Rechtsordnungen immer noch eine Grauzone. Diese Grauzone könnte zu einer hitzigen Debatte sowie möglicherweise zu Gerichtsverfahren führen, wenn jemand seine persönliche Flugverbotszone einführen möchte.
- **Strafverfolgung:** Immer mehr Strafverfolgungsbehörden interessieren sich zu Überwachungszwecken und für die Kontrolle größerer Menschenmengen für Drohnen. In einer so stark aufgeladenen Situation wie einer Protestkundgebung oder bei einem Amoklauf wäre eine Polizeidrohne ein verlockendes Ziel für jemanden, der sich vor den Strafverfolgungsbehörden verbergen möchte. Solche Szenen sind aus zahllosen Actionfilmen bekannt: Die Gegenspieler (oder Helden) betreiben enormen Aufwand, um Sicherheitskameras auszuschalten. Heute haben wir es nicht mehr mit wandmontierten Sicherheitskameras zu tun, sondern die Kameras sind an Drohnen befestigt. Da sich Demonstranten und Hacktivist*innen immer stärker vermischen, spricht einiges dafür, dass Protestierende mit der entsprechenden Technik es schaffen können, die Überwachungsdrohnen auszuschalten.

Doch wie werden diese Angriffe durchgeführt? Verschiedene Forscher haben festgestellt, dass viele Drohnen für Privatanwender mit offenen Ports und schwachen Authentifizierungsmethoden ausgeliefert werden, sodass eine Person mit der richtigen Ausrüstung der angegriffenen Drohne Befehle senden könnte. Bislang war das ein relativ aufwändiger manueller Prozess, doch wie die Erfahrung zeigt, werden neue Exploits früher oder später in einem einfach reproduzierbaren Format angeboten.

Die Mehrzahl der Schwachstellen in kommerziellen Drohnen lässt sich problemlos mit einer Software-Aktualisierung beheben, was natürlich einen Patch durch den Hersteller erfordert. Während bei Highend-Drohnen höchstwahrscheinlich relativ schnell mit einem Patch zu rechnen ist, werden Besitzer billiger Drohnen lange darauf warten müssen. Wie sich bei anderen IoT-Technologien gezeigt hat, suchen die Benutzer netzwerkfähiger Geräte sofort nach Möglichkeiten, diese zu hacken. Erleichtert werden diese Versuche durch die breite Einführung von IoT-Geräten (einschließlich Drohnen), die kaum oder keine Sicherheitsmaßnahmen besitzen. Der Grund dafür, dass sich Drohnen relativ einfach hacken lassen, liegt in der schnellen und einfachen Einrichtung, die häufig über unverschlüsselte Kommunikation und offene Ports abläuft.

Außerdem sagen wir voraus, dass im Jahr 2017 die ersten Drohnen-Exploit-Kits ihren Weg in die dunklen Ecken des Internets finden werden. Sobald diese Toolkits verfügbar werden, ist es nur eine Frage der Zeit, bis in den Nachrichten Meldungen über gekaperte Drohnen erscheinen. Doch selbst ohne ein Toolkit für Drohnen-Hijacking wird es zu einer Zunahme von Zwischenfällen im Zusammenhang mit Drohnen kommen.

Im Jahr 2017 wird es Meldungen über Menschen geben, die es satt haben, dass Kinder aus der Nachbarschaft ihre Drohnen über ihrem Grundstück kreisen lassen. Doch anstatt ein Luftgewehr oder eine Zwillie in die Hand zu nehmen, wird die Drohne mit einem Laptop mit angeschlossener Richtantenne und der entsprechenden Software vom Himmel geholt. Angesichts des viralen Internets werden Berichte zu solchen Vorfällen schon bald auf Facebook-Seiten auf der ganzen Welt auftauchen und Diskussionen über das Für und Wider dieser Aktionen aufwerfen – inklusive hitziger Debatten und sarkastischer Kommentare.

Im Jahr 2017 werden Drohnen mit einem Laptop mit angeschlossener Richtantenne per Software vom Himmel geholt. Wir werden auch mehr von Strafverfolgungsbehörden eingesetzte Drohnen zur Überwachung größerer Menschenmengen erleben sowie von Protestierenden per Hack ausgeschaltete Überwachungsdrohnen.

Diesen Bericht teilen



Im Laufe des Jahres 2017 werden zudem die Strafverfolgungsbehörden mehr Drohnen einsetzen, um größere Menschenmengen zu überwachen. Anfangs werden die Demonstranten versuchen, die Drohnen mit Wurfgeschossen vom Himmel zu holen, doch schon bald werden sie Hacker-Angriffe starten, um die Überwachungsdrohnen auszuschalten.

Wie werden die Gesetzgeber auf diese Vorfälle reagieren? Die US-Flugsicherheitsbehörde Federal Aviation Administration (FAA) arbeitet gerade intensiv an der Einführung von Vorschriften, die den Betrieb von Drohnen regeln. Es gibt jedoch zahlreiche Nutzungsbereiche, die geklärt werden müssen und die wahrscheinlich noch nicht einmal zur Sprache gekommen sind. Während sich die kommerzielle Luftfahrt langsam entwickelte, nimmt die kommerzielle Drohnennutzung rasant zu und bringt die Regulierer in Zugzwang.

Bedrohungen für Mobilgeräte umfassen Ransomware, Remote-Zugriffs-Tools und kompromittierte App-Märkte

Fernando Ruiz

McAfee Labs rechnet damit, dass Mobilgeräte-Malware ihr Wachstum auch im Jahr 2017 fortsetzen wird. Dabei werden Ransomware, Banking-Trojaner und Remote-Zugriffs-Tools (Remote Access Tools, RATs) zu den größten Bedrohungen zählen.

Das auf Mobilgeräte-Malware spezialisierte McAfee Labs-Forschungsteam hat vor allem im 2. und 3. Quartal 2016 eine große Zahl von Ransomware-Varianten für Mobilgeräte erfasst. Bei diesen Exemplaren handelt es sich sowohl um kleine Konzeptstudien, die den Anmeldebildschirm sperren, als auch um komplette Krypto-Malware-Pakete, die den externen Speicher kompromittieren. Eine im 2. und 3. Quartal besonders prominente Mobilgeräte-Ransomware-Familie war Android/Jisut. Diese Ransomware ändert die Sperr-PIN eines Mobilgeräts und verlangt Lösegeld per Bitcoin oder Prepaid-Karte.

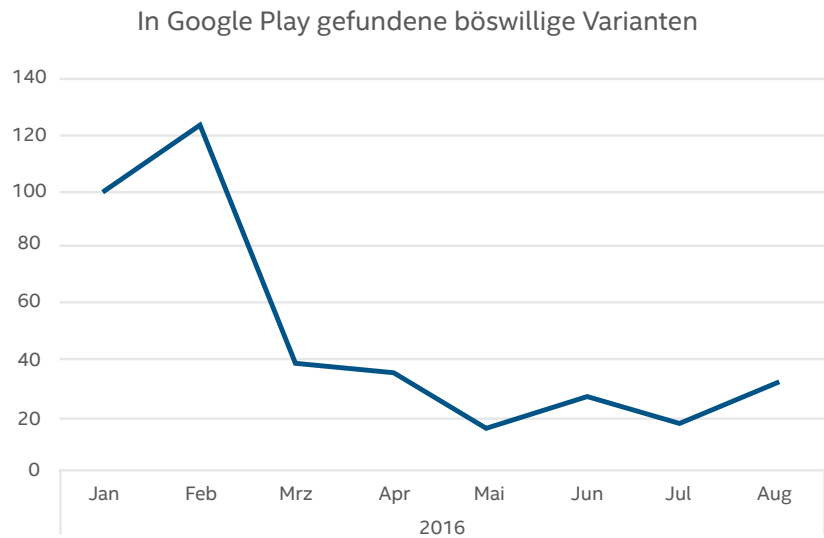
Wir gehen davon aus, dass Mobilgeräte-Ransomware ihr Wachstum im Jahr 2017 fortsetzen wird, wobei sich der Fokus der Malware-Autoren verändern wird. Da das Backup von Mobilgeräten meist über die Cloud erfolgt, hält sich der Erfolg bei direkten Lösegeldzahlungen zum Entsperrn von Geräten meist in recht engen Grenzen. Aus diesem Grund werden Mobilgeräte-Malware-Autoren Sperrungen mit anderen Angriffsformen wie dem Diebstahl von Anmeldeinformationen kombinieren. Beispielsweise stellten wir in diesem Jahr fest, dass Malware-Familien wie Android/Svpeng, die von der Sicherheitsbranche als Mobilgeräte-Ransomware identifiziert wurde, es mittlerweile auf Banking-Anmeldeinformationen abgesehen haben, um die Bankkonten der Opfer leerzuräumen. Wir rechnen damit, dass Banking-Trojaner im Jahr 2017 wieder eine Rolle spielen und dieses Mal von Ransomware-Autoren entwickelt werden. Dabei wird diese Malware Mobilgerätesperren und andere Ransomware-Funktionen mit herkömmlichen Man-in-the-Middle-Angriffen kombinieren, um primäre und sekundäre Authentifizierungsfaktoren zu stehlen, sodass Angreifer Zugriff auf Bankkonten und Kreditkarten erhalten.

Im Jahr 2016 registrierten wir eine Zunahme bei Remote-Zugriffs-Tools (RATs) für Android. Sie gaben sich als legitime Support-Hilfsprogramme aus und wurden auf Drittanbietermärkten angeboten. Mithilfe solcher RATs werden beispielsweise [Pokémon Go-Fans](#), [Terrorismosympathisanten](#) und [Sicherheitspersonal](#) bespitzelt. Die Verbreitung erfolgt über soziale Netzwerke. Aufgrund des Wachstums und der Raffinesse kommerzieller Spyware und RATs erwarten wir, dass diese Art von Malware im Jahr 2017 mehr Opfer finden wird. Verwundbare Smartphones sind eine perfekte Spionageplattform, die von jedem kontrolliert werden kann, der die Kompromittierungsmethoden beherrscht.

Wir gehen davon aus, dass im Jahr 2017 Mobilgeräte-Ransomware ihr Wachstum fortsetzen wird, wobei sich der Fokus der Malware-Autoren verändern wird. Die Angreifer werden Mobilgerätesperren mit anderen Angriffsformen wie dem Diebstahl von Anmeldeinformationen kombinieren, um Zugriff auf Bankkonten und Kreditkarten zu erlangen.

Diesen Bericht teilen





Obwohl wir und andere Quellen dazu raten, nur Apps aus vertrauenswürdigen App-Märkten herunterzuladen, ist das keine absolute Sicherheitsgarantie. Im Laufe des Jahres 2016 tauchten [mehrere Male](#) böswillige Apps in Google Play auf, die jedoch schnell wieder entfernt wurden. Wir raten Benutzern auch für 2017 dringend, Apps vor der Installation genau zu prüfen, selbst wenn sie aus vertrauenswürdigen Märkten stammen. Das Wissen darüber und die Nutzung einer effektiven Malware-Schutz-App sind unverzichtbar, um Infektionen von Smartphones zu verhindern.

Das Herunterladen von Apps aus unbekannten und nicht vertrauenswürdigen Märkten war schon immer mit größeren Gefahren verbunden, was sich auch 2017 nicht ändern wird. Dazu gehören auch die Gefahren von Apps, deren URLs in Instagram, YouTube-Videos oder Tweets erscheinen – sie alle können möglicherweise Malware oder Spyware übertragen. Die Nutzung sozialer Medien kann zu Infektionen führen, da vertraute Umgebungen Benutzer dazu verführen, Sicherheitsrisiken auf die leichte Schulter zu nehmen.

IoT-Malware öffnet eine Hintertür ins Haus

Bruce Snell

Der Markt für Verbraucherelektronik wächst auch weiterhin rasant. Ein Verbraucher-Bereich, der bis 2019 etwa 1,8 Milliarden Geräte umfassen soll, ist das Internet of Things. Dieser Markt wird umgangssprachlich als „Smart Home“ oder „Vernetztes Haus“ bezeichnet und umfasst eine Reihe etablierter Marken und Produkte sowie eine riesige Anzahl an kleineren Unternehmen, die in diesem Markt Fuß fassen wollen.

Im Business-Bereich gibt es das Konzept des „Minimum Viable Product“ (Produkt mit den Mindestanforderungen und -eigenschaften, MVP). MVP (nicht zu verwechseln mit „Most Valuable Player“) bedeutet, dass das Produkt die mindestens erforderlichen Funktionen und Eigenschaften besitzt, sodass frühzeitige Anwender ein Interesse entwickeln. Der Markt für IoT-Hausgeräte ist sehr bindungsstark, d. h. wenn ein Anwender einen intelligenten Thermostat oder ein intelligentes Beleuchtungssystem kauft, wird er anschließend auch weiter bei diesem Anbieter bleiben. Aus diesem Grund drängen zahlreiche Anbieter mit aller Macht auf diesen Markt, und speziell die Hersteller von IoT-Heimgeräten setzen meist auf den MVP-Ansatz. Viele nutzen beispielsweise Code-Bibliotheken von Drittanbietern, um die Entwicklung zu beschleunigen und die Kosten zu senken.

Diesen Bericht teilen



Diese Eile und der Einsatz von Drittanbieter-Software können zu potenziellen Sicherheitsproblemen führen. Empfehlungen bei der Code-Entwicklung besagen, dass die Entwickler den Code jeglicher Drittanbieter-Code-Bibliotheken, die in ihren Produkten enthalten sind, gründlich untersuchen sollten. Leider wird beim Versuch, schnell ein MVP auf den Markt zu werfen, der Code „zusammengestückelt“ und mit minimalen Tests implementiert, wobei die Fehlerbehebung auf die Zeit nach der Veröffentlichung verschoben wird. Wenn Entwickler unter Zeitdruck stehen, bleibt die Sicherheit leider zu oft auf der Strecke – wobei noch nicht einmal garantiert ist, dass Sicherheit überhaupt als Konzept existiert. Wir kennen eine ganze Reihe von IoT-Verbrauchergeräten, die mit riesigen Sicherheitslücken ausgeliefert wurden und bis heute keine Patches erhalten haben.

Wir werden im kommenden Jahr erleben, dass sich böswilliger Code in häufig genutzten Bibliotheken verbirgt oder direkt in Geräte im IoT-Verbraucherbereich eingebettet wird. Der Code wird sich in Elementen wie den Bibliotheken für HTML-Darstellung, Netzwerk und Kameras verbergen.

Nun spinnen wir den Faden in diesem Szenario einen Schritt weiter. Wenn sich ein Krimineller den Weg zu einer Vielzahl von Produkten erschließen will, die sich in Heimnetzwerken befinden und nur über minimale Sicherheitsmaßnahmen verfügen, ist die Platzierung einer Backdoor in IoT-Verbrauchergeräten eine perfekte Möglichkeit. Ein Beispiel dafür wurde vor einigen Jahren bekannt, als ein Samsung-Smartphone-Klon, das Star N9500, in großen Online-Marktplätzen mit in der Firmware installierter Malware verkauft wurde.

Anstatt einen bestimmten Hersteller anzugreifen und seine Code-Basis zu kompromittieren, ist es einfacher, eine „kostenlose“ Version einer weit verbreiteten Code-Bibliothek mit einer Backdoor anzubieten und diese vielen IoT-Geräteherstellern anzubieten. Wir haben unter Android bereits böswilligen Code in beliebten Code-Bibliotheken entdeckt, sodass es durchaus vorstellbar ist, dass dies auch für IoT-Geräte der Fall sein kann.

In den nächsten 12 bis 18 Monaten werden wir erleben, dass sich böswilliger Code in häufig genutzten Bibliotheken verbirgt oder direkt in Geräte im IoT-Verbraucherbereich eingebettet wird. Möglicherweise wird es auch Fälle von konspirativer Zusammenarbeit zwischen IoT-Verbrauchergeräten und Smartphone-Apps geben.

An welchen Stellen wird im Jahr 2017 böswilliger Code auftauchen? Aus Sicht des Angreifers ist die Nutzung einer Code-Bibliothek deshalb von Vorteil, weil sie häufig Direktzugriff auf wichtige Komponenten des Betriebssystems oder der Geräte-Hardware hat. Deshalb erwarten wir, böswilligen Code an folgenden Stellen zu finden:

- Bibliotheken zur HTML-Darstellung: Einige IoT-Geräte bieten Verwaltungsoberflächen, bei denen es sich lediglich um Webseiten zur Konfiguration handelt. Es bietet sich an, böswilligen Code in einer Bibliothek einzubetten, die Zugriff auf die Darstellung dieser Webseiten hat. Dadurch kann die Malware Benutzernamen und Kennwörter erfassen sowie die Malware über die Verwaltungsoberfläche steuern. Niemand vermutet eine Infektion, wenn er die intelligente Beleuchtung seines Hauses steuert!
- Netzwerkbibliotheken: Heimnetzwerke gelten allgemein als sicher. Wenn Malware in einem Heimnetzwerk Fuß fassen kann, kann sie häufig den gesamten Netzwerkverkehr analysieren, da Heimnetzwerke meist eine offene und flache Hierarchie besitzen. Dabei sucht die Malware nach Dingen wie Benutzernamen sowie Kennwörtern und sendet diese an einen externen Kontroll-Server. Da die Malware Direktzugriff auf das Netzwerk hat, bleibt dieses Verhalten meist unerkannt.
- Kamerabibliotheken: Gibt es eine bessere Möglichkeit, eine nichtsahnende Person zu überwachen, als sich in die Kamera eines Babyphons oder Heimsicherheitssystems einzuklinken? Durch das Verstecken in Sicherheitskameras kann die Malware Bilder und Videos nichtsahnender Menschen erfassen und senden, die ihren täglichen Verrichtungen nachgehen.

Diesen Bericht teilen

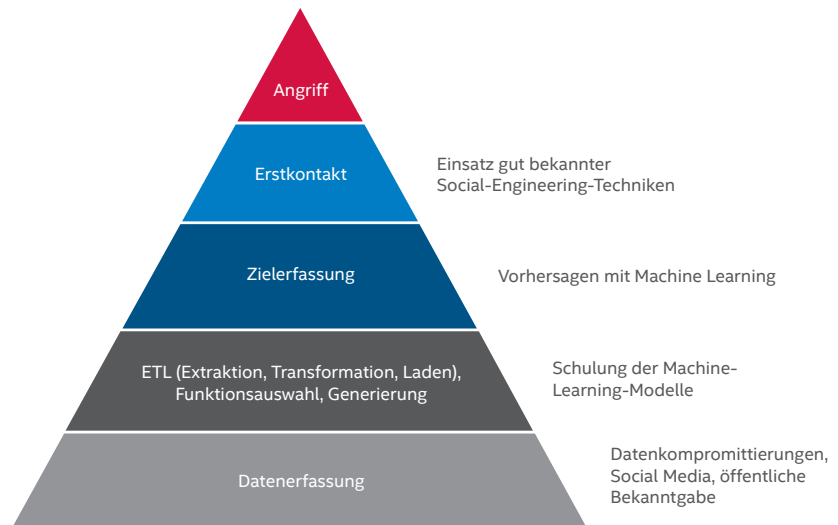


Wir sagen voraus, dass im Jahr 2017 einige IoT-Geräte mit installierten Backdoors verkauft werden. Aufgrund der Natur dieser Geräte können die Spionage und der Diebstahl persönlicher Informationen jahrelang unerkannt bleiben.

Machine Learning beschleunigt Social-Engineering-Angriffe

Eric Peterson

Durch die Nutzung von Toolkits, Dokumentationen und Lernprogrammen für Machine Learning (maschinelles Lernen) ist dessen Einsatz im Bildungs-, Geschäfts- und Forschungsbereich regelrecht explodiert. In gerade einmal einer Stunde kann ein Mensch komplexe Modelle mithilfe großer Datenbestände auf einer verteilten Architektur trainieren. Im Jahr 2016 haben Enthusiasten und professionelle Informatiker Computern beigebracht, [Shakespeare-Sonette zu schreiben](#), [Musik zu komponieren](#), [wie Picasso zu malen](#) und [den professionellen Go-Spieler Lee Sedol zu schlagen](#). Die Schulungsdauer ist kürzer geworden, und die Zugänglichkeit für jedermann – auch Cyber-Kriminelle – war noch nie so gut. Sicherheit ist ein Wettrüsten, und die Cyber-Kriminellen optimieren ihre Methoden mithilfe von Machine Learning.



Wir gehen davon aus, dass Cyber-Kriminelle ihre Opfer mit Machine Learning angreifen. Tools zur Durchführung der komplexen Analyse hinter der Zielauswahl sind frei verfügbar, und es gibt eine Vielzahl an öffentlichen Datenquellen, mit denen böswillige Machine-Learning-Algorithmen entwickelt und trainiert werden können. Wir erwarten, dass die Zugänglichkeit von Machine Learning im Jahr 2017 zur Beschleunigung und Verschärfung von Social-Engineering-Angriffen führen wird.

Eine von mehreren persistenten Bedrohungen, die wir aktuell verfolgen, wird vom US-amerikanischen FBI als Business Email Compromise-Betrug (Kompromittierung geschäftlicher E-Mails, BEC) bezeichnet. Diese Betrugsform [hat seit Anfang 2015 rapide zugenommen](#). Bei BEC-Betrug nehmen die Bedrohungsakteure einzelne Personen mit finanzbezogenen Aufgabenbereichen ins Visier. Durch geschicktes Social Engineering verleiten sie diese Menschen dazu, Gelder an ein betrügerisches Bankkonto zu überweisen. In einigen Fällen fielen die Angriffe zeitgleich mit Geschäftsreisen von Führungskräften zusammen, was die Erfolgswahrscheinlichkeit des Betrugsversuchs verbessern soll. Laut dem FBI wurden mehr als 3 Milliarden US-Dollar gestohlen, wobei die Opfer aus allen 50 US-Bundesstaaten sowie 100 Ländern in aller Welt kommen. Auch wenn bisher nicht klar ist, wie die Opfer ausgewählt wurden, ist klar, dass im Vorfeld jedes Angriffs umfangreiche Recherchen betrieben werden. Wir gehen davon aus, dass Cyber-Kriminelle die Opfer von BEC- und ähnlichen Betrugsversuchen mit Machine Learning angreifen.

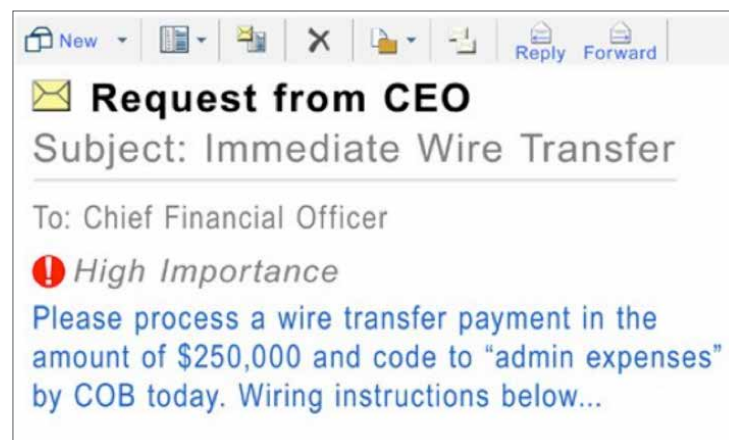
Diesen Bericht teilen





Richtig eingesetzt hat maschinelles Lernen das Potenzial, wichtige, komplexe und relevante Geschäftsprobleme zu lösen. Mithilfe von Regressionsalgorithmen lassen sich Werte vorhersagen, Clustering-Algorithmen decken Strukturen in Datenbeständen auf und Algorithmen zur Anomalieerkennung finden atypische Datenpunkte. Unter der Haube ist die Mathematik, die hinter diesen Algorithmen steckt, viel zu kompliziert, um für jedermann nutzbar zu sein. Wie jedoch moderne Malware-Toolkits wie Trillium, Zeus und Angler zeigen, können Malware-Autoren mithilfe solcher Toolkits erheblich mehr Schaden anrichten, als wenn sie sich auf ihre eigenen Fähigkeiten verlassen müssten. Machine-Learning-Tools und Bibliotheken wie Google TensorFlow, Numpy, Scikit-learn, Pandas und andere beschleunigen auf die gleiche Weise die Entwicklung auf dem Gebiet der Datenwissenschaft. Unter Sicherheitsexperten gelten Machine-Learning-Tools als Wirkbeschleuniger. Gleichzeitig wäre es fahrlässig, nicht davon auszugehen, dass Cyber-Kriminelle diese leistungsfähigen Hilfsmittel ebenfalls einsetzen.

Legitime und illegale Geschäftsmodelle haben eine Gemeinsamkeit: beide müssen Gewinn erwirtschaften. In jedem Fall optimieren die Unternehmen permanent ihr Geschäftsmodell, um bei minimalen Ausgaben ein Maximum an Einnahmen zu erzielen. Wenn wir das BEC-Angriffsmodell als Beispiel nehmen und die Verfügbarkeit von Machine-Learning-Tools zur Durchführung komplexer Datenanalysen berücksichtigen, wird das Zusammenspiel zwischen maschinellem Lernen und kriminellen Aktivitäten deutlich. Die dritte Stütze dieser Angriffsform sind Daten.



Allein im Jahr 2016 gab es 30.000 Kompromittierungen von Mitarbeitern des US-Justizministeriums, 2,2 Millionen Patientendatensätzen des 21st Century Oncology, 1,5 Millionen Verizon Enterprise Solutions-Kundendatensätzen sowie fast 150 Millionen Konten bei großen E-Mail-Anbietern wie Yahoo!, Hotmail und Gmail. Die Daten aus zahlreichen dieser Kompromittierungen wurden standardisiert und auf offenen Märkten wie leakedsource.com verkauft. Dieser Anbieter gibt an, dass seine Datenbank mehr als 2 Milliarden Datensätze umfasst. Auf der anderen Seite bietet EDGAR, die Datenbank der US Securities and Exchange Commission, Diensteanbietern Zugriff auf mehr als 21 Millionen Datensätze. Dank Informationen aus sozialen Medien, gestohlenen Datenbanken sowie in die Öffentlichkeit gelangten Unternehmensdaten haben Angreifer Zugriff auf genug Daten, um Vorhersagemodelle zu trainieren und Erfolg versprechende Ziele auszumachen.

Betrachten wir den Lebenszyklus eines BEC-Betrugsversuchs als Beispiel für einen Angriff, der von Machine Learning profitieren kann. Cyber-Kriminelle wissen, dass eine gut gestaltete E-Mail an eine Führungskraft mit finanzieller Verantwortung, die scheinbar von der Unternehmensleitung kommt und Dringlichkeit vorgibt, einige Erfolgswahrscheinlichkeit bietet. Eine Reihe von Umgebungsfaktoren, die vor der Durchführung des Angriffs erfüllt sein müssen, steigern die Chance auf einen erfolgreichen Betrug. Aus Sicht des Angreifers lassen sich wertvolle Erkenntnisse durch die Beantwortung grundlegender Fragen herleiten, was durch öffentlich verfügbare Informationen möglich ist: Gibt es Hinweise auf Spannungen oder Risse im Unternehmen? Gibt es aktuelle SEC-Meldungen zur Vorbereitung der Übernahme oder des Verkaufs des Unternehmens? Gibt es Zusammenhänge zwischen Social-Media-Beiträgen, die auf den Wechsel mehrerer Mitarbeiter von einem Unternehmen zu einem anderen hindeuten? Gab es strategische Diskussionen, die zu oder von persönlichen oder privaten Adressen geschickt wurden? Die Antworten auf jede dieser Fragen können als Funktionsvektoren für Machine-Learning-Algorithmen dargestellt werden. Mit genug Zeit und Sorgfalt kann ein Modell für die erfolgreiche Durchführung von Betrugsversuchen entwickelt werden, das die Erfolgswahrscheinlichkeit zukünftiger Angriffe berechnet.

Bedrohungsakteure haben ein erfolgreiches Angriffsmodell für den BEC-Betrug entwickelt. Tools zur Durchführung der komplexen Analyse hinter der Zielauswahl sind frei verfügbar, und es gibt eine Vielzahl an öffentlichen Datenquellen, mit denen böswillige Machine-Learning-Algorithmen entwickelt und trainiert werden können. Im Hinblick auf 2017 und die Folgejahre wären wir nicht überrascht, wenn Anbieter von Datendiebstahl sich auf „Target Acquisition as a Service“ mithilfe von Machine-Learning-Algorithmen spezialisieren. Wir erwarten, dass die Zugänglichkeit von Machine Learning im Jahr 2017 zur Beschleunigung und Verschärfung von Social-Engineering-Angriffen führen wird.

Rasante Zunahme bei gefälschter Werbung und gekauften „Likes“ zerstört Vertrauen

Craig Schmugar

Das Internet wird durch gefälschte „Likes“, Werbung, Produkt- sowie Service-Rezensionen, Online-Sicherheitswarnungen, Benachrichtigungen und vieles mehr weniger vertrauenswürdig.

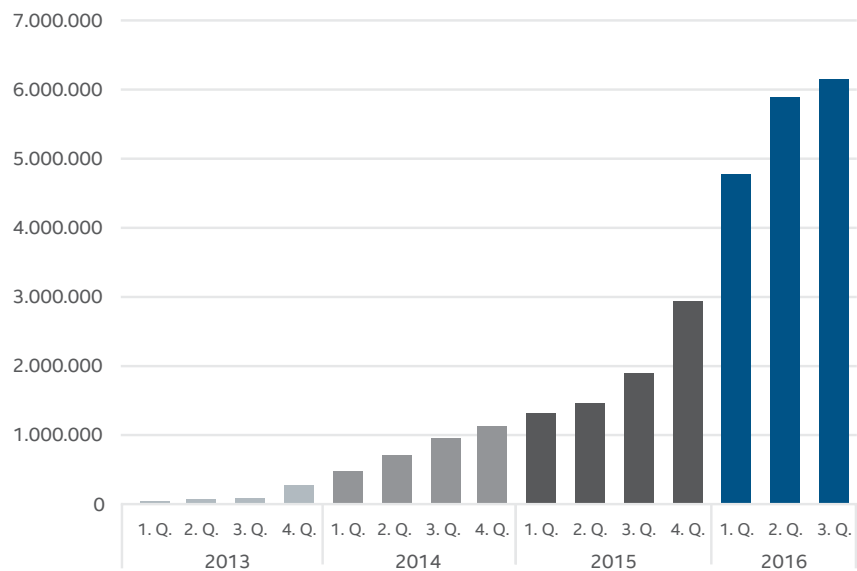
Jeder Internetnutzer wird mit Informationen bombardiert, die ihn zur Entscheidungen drängen: was soll er anklicken, was lesen, wo Geld ausgeben? Diese Entscheidungen treiben eine Online-Wirtschaft mit einem Umfang von mehreren Milliarden US-Dollar an. Angesichts dieser Summen überrascht es nicht, dass skrupellose Akteure nach Möglichkeiten suchen, andere Menschen auszunutzen. Für viele Entscheidungsträger ist die Reputation ausschlaggebend, wenn es darum geht, sichere Entscheidungen zu treffen.

Eine der beliebtesten Methoden zum Aufbau von Vertrauen ist das Feedback früherer Benutzer. Der Wert eines Facebook-„Likes“ wurde auf bis zu [200 US-Dollar](#) oder sogar noch mehr geschätzt. Aus diesem Grund erschienen Services auf der Bildfläche, die für eine Gebühr die Zahl der Likes steigern. Obwohl Facebook streng gegen solche Entitäten vorgeht, handelt es sich hierbei um ein Katz-und-Maus-Spiel, und die neueste Runde zeigt eine Investition von Malware-Autoren, um die Maus länger am Leben zu lassen. Im Gegensatz zu einer „Klickfarm“, die schlecht bezahlte Arbeitskräfte anstellt, um auf Links zu klicken, hängt sich die Faceliker-Malware an Benutzersitzungen an, sodass die Klicks legitim wirken.

Diesen Bericht teilen

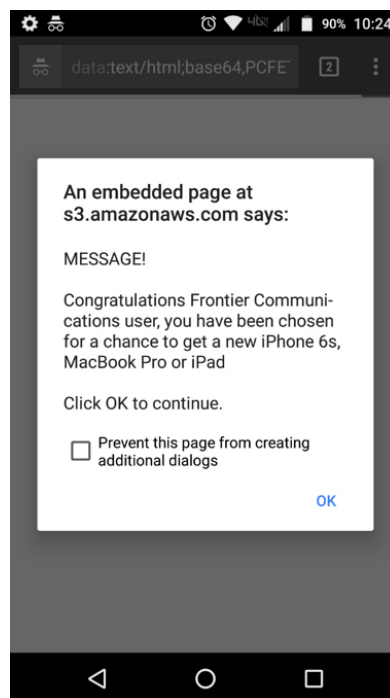


Gesamtanzahl der eindeutigen Faceliker-Malware-Varianten



Wachstum bei Faceliker-Trojaner-Varianten.

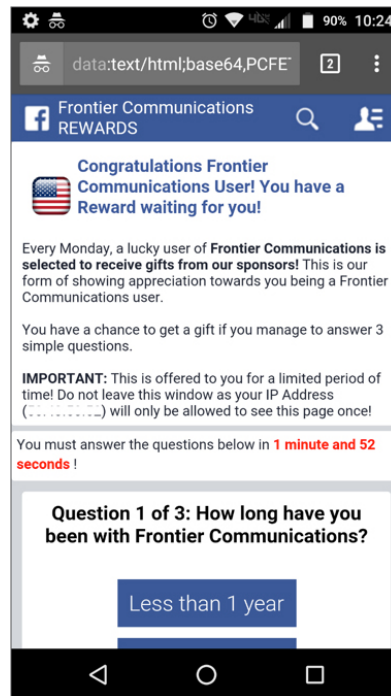
Gefälschte Werbung wird uns ebenfalls erhalten bleiben, wobei eine wachsende Zahl von Werbenetzwerken die Browser-Sitzungen von Benutzern kapert, um Malware zu übertragen, Betrugsversuche zu starten oder endlose Umfragen durchzuführen. Obwohl diese Dinge wirklich lästig sein können, wenn man von den „Hauptverkehrsstraßen“ des Internets abweicht, sind sie noch beunruhigender, wenn sie über bekannte Webseiten ausgeliefert werden.



Gefälschte Werbung, die das Telefon vibrieren lässt und von einer bekannten Webseite in Australien ausgeliefert wurde, wobei Amazon AWS die Werbung verteilte.

Diesen Bericht teilen





Eine unerwünschte Seite, die es einem Benutzer unmöglich macht, die gewünschte Webseite zu erreichen.

Wir finden regelmäßig weitere Fälle gefälschter Inhalte in Produktrezensionen auf den größten eCommerce-Webseiten. Aufgrund der derzeit rasanten Entwicklungen setzen viele Verbraucher auf übersichtliche Produkt- und Service-Empfehlungen. Es überrascht nicht, dass die Händler der Versuchung nicht widerstehen können, bei der Bewertung ihrer Produkte nachzuhelfen. Text-, Audio- und Videorezensionen werden von Menschen angeboten, die bereit sind, ihre eigenen Inhalte zu erstellen oder ein Skript vorzulesen.

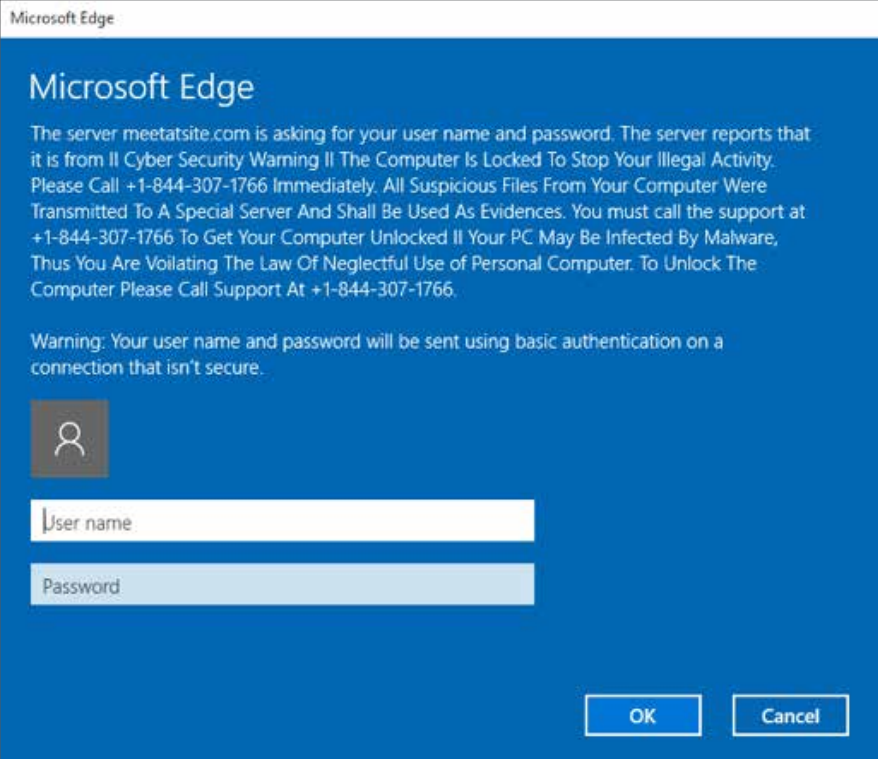
Bewaffnet mit den neuesten Machine-Learning-basierten Schutzmaßnahmen ergreifen die Branchenführer Maßnahmen gegen diese Praktik, die nicht nur gegen die Rezensenten, sondern auch gegen die Händler gerichtet ist, die von diesen Aktivitäten profitieren. Neue Drittanbieter-Webseiten wie FakeSpot und ReviewMeta bauen auf der Grundlage auf, die in den vergangenen Jahren gebildet wurde. Daher ist damit zu rechnen, dass diese Verbraucherschutzinitiativen auch im kommenden Jahr wachsen werden.

Im Jahr 2016 wurde eine Reihe fortschrittlicher Schutzmaßnahmen eingeführt, z. B. erweiterte statische und dynamische Malware-Erkennungsmöglichkeiten oder verbesserte Twitter-Bot-Erkennung. Wir erwarten, dass die Betrüger 2017 zum Gegenangriff übergehen und entweder die Angriffe auf ihre aktuellen Ziele verstärken oder den Weg des geringsten Widerstandes gehen werden. Für Malware-Autoren kann das bedeuten, dass sie „böse Zwillinge-Apps“ (Schadroutinen, die in Versionen legitimer Software eingefügt wurden) oder Kombi-Programme (einzelne Anwendungen, die als legitime Programme sowie als Malware agieren können) entwickeln. Diese Bemühungen werden für die Benutzer sowie für defensive Scanner die Grenze zwischen dem Realen und dem Gefälschten weiter verwischen.

Diesen Bericht teilen



Anfang dieses Jahres wurde eine Kooperation zwischen der US-amerikanischen Netzbehörde FCC (Federal Communications Commission) und der Sicherheitsbranche bekannt gegeben, um den so genannten „Robocalls“ ein Ende zu bereiten. Wir werden im kommenden Jahr sehen, welche Auswirkungen diese Kooperation tatsächlich hat, doch es ist damit zu rechnen, dass die interessierten Parteien ihre gefälschten Botschaften auch weiterhin an den Mann bringen werden. Eine zu erwartende Möglichkeit wird eine Zunahme bei gefälschten Online-Sicherheitswarnungen oder alternativ gefälschter Benachrichtigungs-Malware sein, z. B. falschen Windows-Installationswarnungen, die den Benutzer zu einem Anruf drängen. Diese Warnungen fallen bei nichts ahnenden Internetnutzern auf fruchtbaren Boden und führen dazu, dass naive Opfer aus Angst, den Zugriff auf ihre Systeme zu verlieren, einknicken.



Microsoft Edge

Microsoft Edge

The server meetatsite.com is asking for your user name and password. The server reports that it is from II Cyber Security Warning II The Computer Is Locked To Stop Your Illegal Activity. Please Call +1-844-307-1766 Immediately. All Suspicious Files From Your Computer Were Transmitted To A Special Server And Shall Be Used As Evidences. You must call the support at +1-844-307-1766 To Get Your Computer Unlocked II Your PC May Be Infected By Malware, Thus You Are Voilating The Law Of Neglectful Use of Personal Computer. To Unlock The Computer Please Call Support At +1-844-307-1766.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

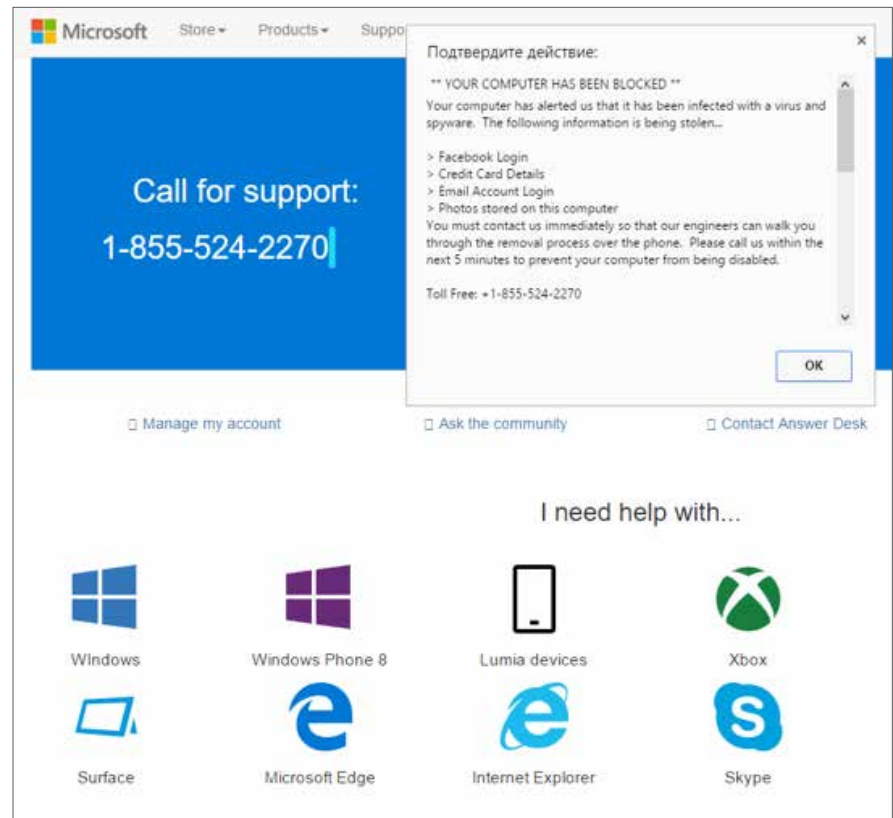


User name

Password

OK Cancel

Eine gefälschte Warnung von einer scheinbaren Microsoft-Webseite, die für einen Zugangscode zum Entsperren von Inhalten den Benutzer auffordert, den Support anzurufen.



Diese Betrugsseite füllt den gesamten Bildschirm und gibt sich als legitime Microsoft-Webseite aus. Sie spielt auch einen Warnton ab, der den Benutzer dazu drängt, eine Support-Telefonnummer anzurufen.

2016 erwies sich als das Jahr, in dem Augmented Reality dank des enormen Erfolges von Pokémon Go zum Mainstream wurde. Die Benutzer nahmen die eingefügten virtuellen Darstellungen als Bestandteil des Gesamterlebnisses wahr und entwickelten eine regelrechte Sucht nach dem Spiel. Diese Erfolgsgeschichte wird ganz sicher nicht einmalig bleiben. Wird es für uns in Zukunft in einer Welt, die das Reale und das Virtuelle zunehmend stärker vermischt, immer schwieriger, böswillige Fälschungen von erwünschter Fiktion zu unterscheiden?

Eskalation der Werbekriege fördert die Malware-Übertragung

Adam Wosotowsky

Das Katz-und-Maus-Spiel zwischen Werbetreibenden und Werbeblockern wird sich fortsetzen. Einige der Techniken von Werbetreibenden zur Umgehung aktiver Werbeblocker werden zukünftig von Malware-Verbreitern ausgenutzt, um per Drive-by-Download Malware zu verbreiten.

Sicherheitsforscher verbringen viel Zeit in gefährlichen Bereichen des Internets, in denen es viele geknackte Webseiten und Drive-by-Malware-Downloads gibt. Um sich in diesen Bereichen relativ sicher bewegen zu können, verwenden wir Sicherheits-Add-Ons für Browser, die aktive Inhalte deaktivieren, den Quell-Code der Site-Inhalte auslesen und die Bestandteile mithilfe verschiedener Server stückchenweise abrufen. Zudem arbeiten wir in virtuellen Maschinen, die zur Vermeidung lokaler Computerinfektionen neu geladen werden. Mit diesen Vorsichtsmaßnahmen wird das „Surfen im Internet“ erheblich schwieriger.

Die meisten Benutzer müssen keinen so großen Aufwand betreiben. Der durchschnittliche Benutzer interessiert sich zudem vor allem für die Benutzerfreundlichkeit seines Browsers und der besuchten Webseiten. Und dann kam die Pop-Up-Werbung. Plötzlich wurden Webseiten hinter einem Haufen neuer Browser-Fenster verborgen, die mit sinnloser Werbung blinkten und die Webseiten praktisch unbrauchbar machten. Als Reaktion darauf erhielten Browser Funktionen, mit denen sich Pop-Up-Fenster blockieren lassen. Damit begann der Werbekrieg.



**You must Disable or Remove
Adblock to visit this website.**

[Click here to go back](#)

Viele Webseiten machen sich heute die schlechte Benutzerfreundlichkeit von Webseiten Mitte der 1990er Jahre zu eigen. Das hat allerdings nichts mit Pop-Up-Fenstern zu tun. Stattdessen enthalten sie enorm ablenkende, blinkende Werbeanzeigen, direkt über dem Inhalt liegende Werbung sowie Videowerbung (mit Ton), die automatisch abgespielt wird, sobald ein Benutzer die Seite besucht (sodass dieser schnell das Browser-Fenster schließt und sich schuldbewusst nach umstehenden Personen umsieht). Wenn eine Werbung 10 MB an Werbedaten an das Mobiltelefon eines Benutzers sendet, der lediglich 50 Sätze Text lesen wollte, ist das Unternehmen zu weit gegangen.

Sicherheits-Tools, die die Ausführung aktiver Inhalte im Browser stoppen, blockieren auch solche Werbung. Werbetreibende nutzen die gleichen Methoden wie Malware-Verbreiter, um Computer zur Ausführung von beliebigem Code zu zwingen, der von der Webseite geliefert wird, damit die Werbung auch ohne Zustimmung des Benutzers ausgeführt wird.

Wenn es den Werbetreibenden nur um die Anzeige der Werbung ginge, würden sie die Werbung *direkt* über die primären Domänen der jeweiligen Webseiten bereitstellen – und die Benutzer hätte kaum eine Möglichkeit, sie zu blockieren. Leider ist das Anzeigen von Werbung nicht so wertvoll wie die Nachverfolgung der Benutzer ohne deren Zustimmung über mehrere Domänen hinweg und mit dem Ziel, Benutzerprofile zu erstellen, die wiederum verkauft und zum Hosten der Werbung bei noch mehr Kunden genutzt werden können. Diese Akteure nutzen die gleichen Techniken wie Malware-Verbreiter zur Erfassung der Telemetrie-Daten und zur Installation von Daten für die gepushten böswilligen Infektionen. Interessanterweise verwenden Werbeblocker, die Werbung beim Surfen stoppen, die gleichen Methoden wie Sicherheitsforscher beim Schutz vor Infektionen.

Diesen Bericht teilen



Der Werbekrieg zwischen Benutzern (und ihren Werbeblockern) und den Werbetreibenden, die Werbung anzeigen und Telemetriedaten zum Benutzerverhalten sammeln wollen, heizt sich immer weiter auf. [Werbetreibende setzen auf neue Methoden zur Umgehung von Werbeblockern](#), doch diese werden mit aktualisierter Werbeblockier-Software gekontert, die diese wiederum blockieren. Viele Werbeblocker analysieren webseitenübergreifende Skripts sowie andere Webseitenkomponenten, um Inhalte selektiv zu blockieren. Dies ist notwendig, da nur wenige Browser wirklich die Möglichkeit (für Entwickler) bieten, die Funktion zur Ausführung von aktivem Code vollständig zu deaktivieren. Es ist deutlich, wohin das führen wird: Mit genügend Verschleierung werden Kriminelle in der Lage sein, schützende Add-Ons zu umgehen. Werbetreibende, denen der Umsatz wichtiger ist als die Sicherheit, tun Malware-Verbreitern einen Gefallen. Im Jahr 2017 werden einige der Techniken von Werbetreibenden zur Umgehung aktiver Werbeblocker von Malware-Verbreitern ausgenutzt werden, um per Drive-by-Download Malware zu verbreiten.

Hacker legen Datenschutzprobleme offen

Paula Greve

Hacker werden die Verbraucher über ihre digitalen Spuren aufklären, indem sie einige Unternehmens-Clouds mit Kundendaten angreifen und erfolgreich kompromittieren. Anschließend legen die Hacker persönliche Daten offen, um Empörung unter Verbrauchern zu erzeugen und Maßnahmen zu erzwingen. Diese Aktionen werden so lange weitergehen, bis sie als nicht berichtenswert eingestuft werden oder die Empörung der Öffentlichkeit Änderungen in Datenschutzgesetzen und Unternehmensrichtlinien erzwingt.

Im Laufe der Jahre ist der Umfang der Daten, die zu Benutzern gesammelt werden, exponentiell gewachsen. Dank der aggregierten Daten können wir unsere Gesundheit verbessern, bei der Suche schneller unser gewünschtes Ziel erreichen, alte Freunde wiederfinden, den Funktionsumfang unserer Heimelektronik erweitern oder sogar unterwegs geschützt bleiben. Die Nützlichkeit dieser Daten wird sogar im [Leitfaden zum EU-US-Datenschutzschild](#) hervorgehoben: „Die Übermittlung personenbezogener Daten ist ein wichtiger und unverzichtbarer Bestandteil der transatlantischen Beziehungen, insbesondere in der heutigen globalen digitalen Wirtschaft“ (Seite 1). In diesem Jahr wurde die Aufmerksamkeit für die von unseren Geräten gesammelten Informationen und die Größe unserer digitalen Spur weiter gesteigert. Dazu kommen ebenso Schulungsinitiativen, in denen Kinder über die Kontrolle ihrer Daten informiert werden, wie Artikel zur Nutzung persönlicher Daten für gezielte Werbung zum Einsatz. Tatsächlich ergibt eine [TED-Suche](#) mehr als ein Dutzend Treffer zu Gesprächen über „die dunkle Seite der Daten“. Dieses aktuelle und kontroverse Thema wird im nächsten Jahr wieder Schlagzeilen machen.



Ursprünglich auf Flickr mit dem Titel „Anonymous at Scientology in Los Angeles“ (Anonymous bei Scientology in Los Angeles) veröffentlichtes Foto, von Vincent Diamante [CC BY-SA 2.0 (<http://creativecommons.org/licenses/by-sa/2.0>)], über Wikimedia Commons.

Diesen Bericht teilen





Aufgrund dieser Trends sagen wir voraus, dass Hacktivist*innen diese Gelegenheit im Jahr 2017 nutzen werden, um Benutzer*innen darin zu „schulen“, wie viele ihrer Daten sie preisgeben. Dies wird wohl über Angriffe geschehen, bei denen einige der Cloud-Datenerfassungsdienste (z. B. Suchvorgänge, Links, Verbindungen, Seitenansichten, Produktnutzung, Heartbeats) infiltriert und die kompromittierten Inhalte anschließend als „Ankündigungen öffentlicher Dienste“ öffentlich gepostet werden. Wie bisher auch werden Hacktivist*innen-Gruppen nach einem erfolgreichen Angriff in einem bestimmten Bereich ähnliche Angriffe ausführen, um ihre Botschaft zu vermitteln – und dazu mit jedem Angriff versuchen, die Aufmerksamkeit zu erhöhen. Deshalb erwarten wir, dass diese Datenkompromittierungen ausufern und die Aufmerksamkeit auf anerkannte Webseiten und Unternehmen richten werden.

Obwohl wir weltweit mit Folgen durch diese Angriffe rechnen, wird der Druck auf US-Unternehmen wahrscheinlich am größten werden. In den USA wollen Unternehmen die Kontrolle über Kundendaten behalten. So [zog Microsoft zum Beispiel mehrmals vor Gericht](#), um Benutzerdaten vor der US-Regierung zu „schützen“. Entsprechend dem neuen [EU-US-Datenschutzschild](#) können Bürger erfahren, welche Unternehmen welche Daten sammeln. Ironischerweise kann diese Liste auch von entschlossenen Hacktivist*innen verwendet werden, die europäische Bürger und die ganze Welt darüber informieren wollen, wie viele Daten US-Unternehmen über sie sammeln.

Diese Angriffe werden einige damit zusammenhängende Sicherheitsprobleme auslösen. Dazu können kompromittierte Unternehmen gehören, die mit den Folgen der Kompromittierung für die Sicherheit und das Kundenvertrauen kämpfen oder sich auf die zu erwartende Flut an Kundenbeschwerden vorbereiten müssen. Oder auch Unternehmen, die 45 Tage Zeit zum Reagieren haben und die Folgen davon zu spüren bekommen, dass Kunden, die mit der Reaktion unzufrieden sind, zahlreiche Optionen zur Verfügung stehen. Unternehmen müssen aufgrund dieser Beschwerden zusätzliche Maßnahmen ergreifen, z. B. Nachweise über die Dauer der Datenspeicherung, den echten Bedarf nach den erfassten Daten sowie darüber, ob die Erfassung der Daten, die per Opt-In, Opt-Out oder vielleicht einfach nur zufällig gesammelt wurden, dem Kunden gegenüber fair ist.

Im Rückblick auf die Folgen vergangener Datenkompromittierungen durch Cyber-kriminelle Gruppen waren die Betroffenen darüber erschrocken, wie viele Daten gesammelt wurden und wie alt einige Daten waren. Es ist schlimm genug, wenn persönliche Daten gestohlen werden, doch das Vertrauen leidet noch weiter, wenn sich zusätzlich herausstellt, dass einige der Daten veraltet sind. In den nächsten Jahren werden sich Verbraucher der gesammelten Daten stärker bewusst sein und Maßnahmen verlangen, z. B. zusätzliche Kontrolle über ihre persönlichen Informationen sowie konsistente Speicherungsrichtlinien.

Wir werden vielleicht erleben, dass Verbraucher die Unternehmen zur Einführung des „Rechts auf Vergessen“ und zur vollständigen Transparenz der erfassten Daten zwingen.

Zusammenfassend erwarten wir, dass Hacktivist*innen die Verbraucher über ihre digitalen Spuren aufklären, indem sie einige Unternehmens-Clouds angreifen und erfolgreich kompromittieren, die Kundendaten enthalten. Anschließend legen die Hacktivist*innen persönliche Daten offen, um Empörung unter Verbrauchern zu erzeugen und Maßnahmen zu erzwingen. Diese Aktionen werden so lange weitergehen, bis sie als nicht berichtenswert eingestuft werden oder die Empörung der Öffentlichkeit Änderungen in Datenschutzgesetzen und Unternehmensrichtlinien erzwingt.

Stilllegungen durch Strafverfolgungsbehörden werfen Cyber-Kriminalität zurück

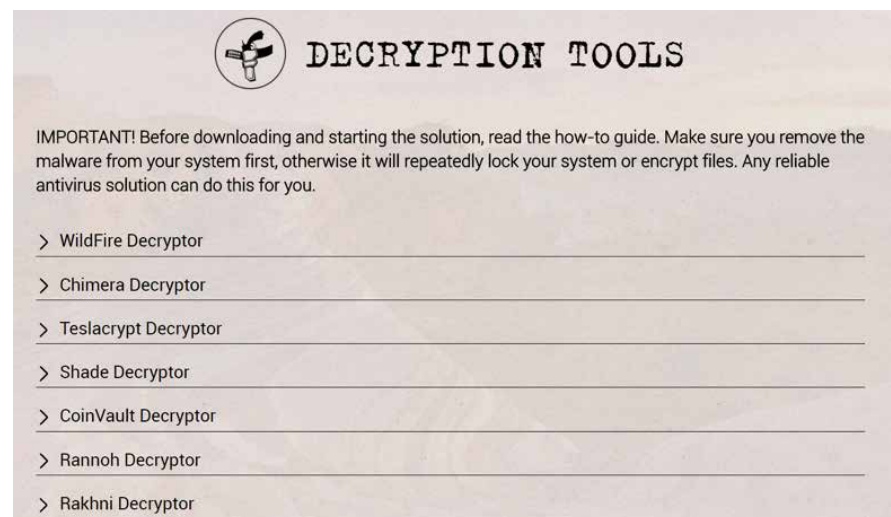
Christiaan Beek

Die Aktionen gegen Autoren verteilter Denial-of-Service-Angriffe und Botnets auf der gesamten Welt werden zunehmen, da Privatwirtschaft und Strafverfolgungsbehörden verstärkt zusammenarbeiten. Immer mehr Länder werden die Folgen der Cyber-Kriminalität für ihre Wirtschaft zu spüren bekommen und ihre Investitionen in Cyber-Abwehrmaßnahmen erhöhen.

Kürzlich gab es einige beachtliche Erfolge der Strafverfolgungsbehörden und ihrer Partner bei der Stilllegung böswilliger Webseiten und Akteure. Intel Security war bei einigen dieser Operationen beteiligt. Was ist eine Stilllegung? Hierbei handelt es sich um eine Reihe koordinierter Aktionen, bei denen Strafverfolgungsbehörden zusammen mit anderen Parteien (meist Sicherheitsanbietern) eine Cyber-kriminelle Operation beenden. Im besten Fall erfolgen dabei Verhaftungen, doch in jedem Fall werden dabei die von den Cyber-Kriminellen verwendeten Infrastrukturen gestört oder beschlagnahmt. Eine Stilllegung ist das Ergebnis von Ermittlungen, die sich über viele Monate – in einigen Fällen sogar Jahre – erstrecken.

Ein Beispiel für eine großmaßstäbliche Stilllegung durch russische Strafverfolgungsbehörden im Juni beinhaltete die Verhaftung von 50 Personen, die für eine mehrjährige Kampagne verantwortlich waren und von russischen Banken 25 Millionen US-Dollar gestohlen hatten. Eine [Videoaufzeichnung zu diesen Verhaftungen](#) finden Sie auf YouTube.

Im Jahr 2016 war Intel Security an vier Stilllegungen von Ransomware-Verbreitern beteiligt und unterstützte einige weitere Operationen, die nicht in den Nachrichten veröffentlicht wurden. Die Ransomware-Stilllegungen sind Teil des Projekts „[No More Ransom!](#)“ (Nie mehr Lösegeld!), bei dem Strafverfolgungsbehörden und IT-Sicherheitsunternehmen gemeinsam Cyber-Kriminellen das Handwerk legen, die für ihre Angriffe Ransomware einsetzen. Intel Security ist eines der Gründungsmitglieder dieses Projekts.



Im Anschluss an Stilllegungen konnten bereits zahlreiche Ransomware-Decodierer zur Verfügung gestellt werden.

Wir fühlen uns dadurch ermutigt, dass sich andere Sicherheitsunternehmen am Kampf gegen Cyber-Kriminalität beteiligen. Leider wurden durch vorzeitige Ankündigungen in diesem Jahr Monate der Forschung und einige Stilllegungen vereitelt. Durch eine Nachfrage bei den entsprechenden Strafverfolgungsbehörden hätten diese Kompromittierungen vermieden werden können. Da sich viele Sicherheitsunternehmen und Strafverfolgungsbehörden auf aller Welt am „No More Ransom!“-Projekt beteiligen möchten, sind wir der festen Überzeugung, dass wir Ransomware das Handwerk legen können.

Diesen Bericht teilen



Intel Security wird die weltweiten Strafverfolgungsbehörden auch im Jahr 2017 bei Stilllegungen unterstützen. Wir werden uns außerdem aktiv am „No More Ransom!“-Projekt sowie ähnlichen Organisationen beteiligen und unsere Erfahrung sowie Kenntnisse teilen, um der weltweiten Community zu helfen.

Die Aktionen gegen Autoren verteilter Denial-of-Service-Angriffe und Botnets auf der gesamten Welt werden zunehmen, da Privatwirtschaft und Strafverfolgungsbehörden verstärkt zusammenarbeiten. Immer mehr Länder werden die Folgen der Cyber-Kriminalität für ihre Wirtschaft zu spüren bekommen und ihre Investitionen in Cyber-Abwehrmaßnahmen erhöhen. Je schneller wir handeln, desto besser können wir reagieren und eingreifen. Privatunternehmen, die sich an gemeinsamen Operationen mit Strafverfolgungsbehörden beteiligen, sollten mit rechtlichen Folgen rechnen und sich darauf vorbereiten. Im nächsten Jahr könnten Cyber-Kriminelle erstmals versuchen, die Beziehung zwischen privaten Anbietern und Strafverfolgungsbehörden herauszufordern.

Der Austausch von Bedrohungsdaten macht hervorragende Fortschritte

Jeannette Jarvis

Durch den Austausch von Bedrohungsdaten verschiebt sich das Machtverhältnis von den Kriminellen wieder zurück zu uns, den Verteidigern. Dadurch wird der Angriffszyklus unterbrochen, und Kriminelle müssen mehr Aufwand betreiben und ihre Ressourcen sowie Techniken auf neue Taktiken ausrichten. Dieser Wechsel machte sich 2016 bezahlt, als die Gründungsmitglieder der [Cyber Threat Alliance \(CTA\)](#) bei [Forschungen zu Version 3 der CryptoWall-Kampagne](#) zusammenarbeiteten. Kurz nach der Veröffentlichung dieses Forschungsberichts wandten sich die CryptoWall-Autoren von Version 3 ab und konzentrierten ihre Bemühungen auf eine neue Kampagne (Version 4). Die CTA wird die gemeinsamen Abwehrmaßnahmen verbessern und dazu im Jahr 2017 zusammenarbeiten sowie tiefgehende Forschung betreiben. Bei dieser Forschung werden neue Angriffe und Details zu Kompromittierungsindikatoren aufgedeckt, die weitergegeben und zu den Kontrollsystemen der Mitglieder hinzugefügt werden, um weitere Angriffe zu stoppen.



Wenn der Austausch von Bedrohungsdaten so wertvoll ist, warum gibt es nicht mehr Zusammenarbeit? In der Vergangenheit mussten vor allem drei wichtige Hindernisse überwunden werden:

1. Vermeidung der unbeabsichtigten Weitergabe privater Kundeninformationen
2. Sorgen um den Verlust des Wettbewerbsvorteils
3. Bedenken in Bezug auf die öffentliche Aufmerksamkeit eines Unternehmens, das angegriffen wurde

Zum Glück verändert sich die Sicherheitsbranche, sodass diese Sorgen schwinden. So bietet zum Beispiel der [Cybersecurity Information Sharing Act](#) (US-Gesetz zur Weitergabe von Cyber-Sicherheitsinformationen) die rechtliche Grundlage für die Weitergabe von Bedrohungsdaten zwischen der US-Regierung und der Privatwirtschaft sowie innerhalb der Privatwirtschaft, wobei sich der Haftungsschutz auf die austauschenden Akteure erstreckt. In Anbetracht des neuen Haftungsschutzes bewerten US-Unternehmen ihre Richtlinien zur Datenweitergabe neu. Im Jahr 2017 wird es daher wahrscheinlich erheblich mehr Datenaustausch geben.

Es wird zum Aufbau vertrauenswürdiger ISAO-Communitys kommen. Wir werden zudem sehen, dass ISAO-Plattformen geschaffen werden, über die Unternehmen automatisch Bedrohungsdaten zu ihren Sicherheitssystemen hinzufügen können.

Diesen Bericht teilen





Zur Blockierung von Angriffen fast in Echtzeit sind automatisierte Tools und Prozesse erforderlich. Im Rahmen des [US-Präsidentiallasses 13691](#) erhielt der US-Minister für Heimatschutz den Auftrag, die Normungsorganisation [Information Sharing and Analysis Organization \(ISAO\) Standards Organization](#) zu gründen. Die ISAO Standards Organization stellt [grundlegende Leitlinien und empfohlene Vorgehensweisen](#) zum effektiven Austausch und Analysieren von Informationen bereit. Im Jahr 2017 werden viele vertrauenswürdige ISAO-Communitys für verschiedene Branchen, Regionen und verwandte Domänen aufgebaut. Wir werden zudem sehen, wie ISAO-Plattformen geschaffen werden, über die Unternehmen automatisch Bedrohungsdaten zu ihren Sicherheitssystemen hinzufügen können.

Im Zuge der Weiterentwicklung der ISAOs sowie anderer Programme zum Austausch von Bedrohungsdaten erwarten wir Verbesserungen in Bezug auf Governance und Haftbarkeit. Die Bildung der [International Association of Certified ISAOs](#) (IACI), deren Auftrag darin besteht, die Leitlinien und Zertifizierung der ISAOs zu unterstützen, wird im Jahr 2017 vollständig abgeschlossen sein. IACI wird Unternehmen weltweit bei der (Weiter-) Entwicklung der Verwaltung ihrer Programme zum Austausch von Cyber-Bedrohungsdaten zur Seite stehen.

Zur Verbesserung unserer Cyber-Abwehr muss die Branche zusammenarbeiten. Dank per Crowd-Sourcing bereitgestellter Bedrohungsdaten und gemeinsamer Analysen können leichter Zusammenhänge erkannt und ein besseres Bild der Angriffslandschaft erstellt werden. Im Jahr 2017 wird der Austausch von Bedrohungsdaten seine wichtigsten Fortschritte machen.

Cyber-Spionage: Sicherheitsbranche und Strafverfolgungsbehörden vereinen ihre Kräfte

Christiaan Beek

Aufgrund von Änderungen bei internationalen Gesetzen und Abkommen zwischen Ländern rechnen wir damit, dass bisher staatlich finanzierte Cyber-Spionage-Teams zu Informationshändlern werden, die gegen Geld „Zugang“ bereitstellen. Ihre Vorgehensweise wird sich dabei nicht ändern.

In den ersten neun Monaten des Jahres 2016 registrierte Intel Security 78 öffentliche Fälle, die wir als Cyber-Spionage oder Cyber-Krieg einstufen. Bei den meisten dieser Kampagnen interessierten sich staatliche Stellen für die politischen Ansichten oder Hintergründe der Zielentitäten, bei denen es sich um Regierungsbehörden bzw. in einigen Fällen um Einzelpersonen oder Mitglieder einer politischen Partei handelt.

Die Vorgehensweise ist hier ähnlich, und wir erwarten im Jahr 2017 keine großen Veränderungen. Jede Aktion beginnt damit, dass die Akteure eine Host-Domänen-Infrastruktur einrichten, die entweder als Kontroll-Server oder zur Übertragung von Schaddaten dient. Anschließend erfolgt ein Spearphishing-Angriff, bei dem das Ziel eine speziell präparierte E-Mail erhält. In einigen Fällen binden die Angreifer verborgenen Code in die eingebettete HTML ein, mit dem sie die zu kontrollierenden Computer nachverfolgen können und erfahren, wo die Schaddaten innerhalb des Netzwerks gelandet sind. Ab diesem Punkt setzen die Angreifer das Arsenal ihrer Tools ein, die von Anmeldedaten-Editoren, über Pass-the-hash-Angriffe bis zu benutzerdefinierten Skripts reichen. In den meisten Fällen hält ein Backdoor-Trojaner mit Remote-Zugriff im Netzwerk die Stellung. Weniger erfahrene Akteurgruppen nutzen kommerzielle, vorgefertigte Remote-Zugriffs-Tools (z. B. PlugX) und passen die Basiseinstellungen an ihre Kampagnen an.

Zwei Fälle von Cyber-Spionage machten uns in diesem Jahr besonders neugierig. Der erste Fall betraf Irongate. Forscher fanden eine komplexe Malware-Variante, die Industrieleitsysteme angreift. Einige Code-Elemente waren mit dem berühmten Stuxnet-Cyber-Wurm verwandt. Das ist eines der Risiken von Malware, die als Cyber-Waffe eingesetzt wird: Nach einem Leak taucht der Code garantiert an anderer Stelle wieder auf, und früher oder später wird jemand den Code weiter anpassen sowie die Malware-Apps weiter optimieren. Dies führt zum zweiten Fall,

Diesen Bericht teilen



Strider/Sauron, einer sehr raffinierten Malware, die auf einen modularen Ansatz und entsprechende Techniken setzt. Strider/Sauron ist eine beeindruckende Malware, die die Bezeichnung „hochentwickelte hartnäckige Bedrohung“ wahrlich verdient. Es sollte uns nicht kalt lassen, wenn solcher Code öffentlich gemacht wird, und wir müssen damit rechnen, dass staatlich finanzierte Gruppen von diesen Techniken lernen und ihre Vorgehensweise anpassen werden.

Was wird im Jahr 2017 in Bezug auf Cyber-Spionage passieren? Cyber-Spionage wird immer präsent sein – entweder im Rahmen staatlicher Spionageaktivitäten oder durch organisierte Gruppen, die es auf geistiges Eigentum abgesehen haben, um es verkaufen zu können. Aufgrund von Änderungen bei internationalen Gesetzen und Abkommen zwischen Ländern rechnen wir damit, dass bisher staatlich finanzierte Teams zu Informationshändlern werden, die gegen Geld „Zugang“ bereitstellen. Jeder verfügt über wertvolle Informationen, doch es bedarf eines kreativen Kopfes, um daraus Profit zu schlagen.

Eine weitere Prognose betrifft die Netzwerksicherheit. Der Leak der Tools, die angeblich zur Equation Group gehören, zeigt ganz deutlich das Interesse raffinierter Angreifer an der Kompromittierung von Firewalls. Erfolgreiche Angriffe auf Kern-Router der VPN-Konzentratoren ermöglichen Netzwerkzugriff und bieten eine hervorragende Möglichkeit, die Sicherheitsmaßnahmen zu unterlaufen. Im Jahr 2017 wird es mehr Forschung – und Erkennungen – zu diesem Exploit-Typ geben.

Die Branchen für physische und Cyber-Sicherheit vereinen ihre Kräfte

Matthew Rosenquist

Der Sicherheitsbranche steht ein strategischer Wandel bevor. Die Domänen der Anbieter für physische sowie Cyber-Sicherheit überschneiden sich zunehmend und erstrecken sich über die realen wie digitalen Welten. Die kontinuierliche Einführung von Technologien, die das Leben vieler Menschen und die Produktivität der Unternehmen verbessern, zwingt die Sicherheitsbranche zum Schließen der Lücke zwischen physischer und Cyber-Sicherheit. Dieses Zusammenwachsen ist ein natürlicher Nebeneffekt des gemeinsamen Zwecks beider Bereiche: des Schutzes von Menschen und Ressourcen.

Zwei Giganten, ein Ziel

Die Branchen für physische und Cyber-Sicherheit liegen weltweit bei jeweils etwa 80 Milliarden bzw. 100 Milliarden US-Dollar. Die Produkte für physische Sicherheit sind erheblich ausgereifter und stabiler, während der Markt für Cyber-Sicherheit durch mehr Unruhe sowie schnelles Wachstum geprägt ist.

Seit mehreren Jahren existieren beide Branchen weitestgehend unabhängig voneinander. Die physische Sicherheit konzentriert sich auf Videoüberwachung, Zugangskontrollsysteme (z. B. Türverriegelungen und Ausweisleser), Sperren, Sicherungssysteme sowie Tools zum Schutz wertvoller Ressourcen. Der Schwerpunkt der Cyber-Sicherheit liegt im Schutz von Computern, intelligenten Geräten, Telekommunikation, Daten, Clouds und allen Geräten mit Internetzugang. Diese Ressourcen sowie Dienste sind enorm wertvoll und müssen vor verschiedenen Bedrohungsformen geschützt werden.

Die Welt verändert sich

Da digitale Tools und Technologien eine immer größere Rolle in unserem täglichen Leben spielen, steigt auch der Bedarf nach Cyber-Sicherheit. Der Trend geht dahin, Geräte von überall zu verbinden, zu überwachen und zu kontrollieren. Computersysteme sind heute mit mehr Sensoren und Funktionen ausgestattet. Tagtäglich verwendete Geräte sind heute vernetzt und zunehmend „intelligent“. Die Bildung des Internets der Dinge führt dazu, dass bis zum Jahr 2020 voraussichtlich 200 Milliarden Geräte mit dem Internet verbunden sein werden. Viele dieser Geräte werden sich in Privathaushalten und Unternehmen befinden – bis heute der Kernmarkt für Anbieter physischer Sicherheitsprodukte. Wenn sich Ihre neue, intelligente Eingangstür für Einbrecher öffnet oder Ihr Babyphon seine Daten live ins Internet überträgt, werden Sie sich nicht sicher fühlen.

[Gartner schätzt](#), dass im Jahr 2020 bei mehr als 25 Prozent aller Angriffe auf Unternehmen IoT-Geräte eine Rolle spielen. Diese Tatsache wird die ohnehin enormen Investitionen in IoT-Sicherheit verdoppeln – von 282 Millionen US-Dollar im Jahr 2015 auf 547 Millionen US-Dollar im Jahr 2018.

Sicherheitsprodukte wie Alarmanlagen, Zugangskontrollen und Videoüberwachung geraten selbst bereits ins Visier von Cyber-Kriminellen. Die Vernetzung von Sicherheitsgeräten mit Netzwerken ermöglicht Kostenersparungen und erweitert die zur Verfügung stehenden Funktionen. Gleichzeitig wird dadurch die Angriffsfläche für Hacker vergrößert. Die Software und Firmware sowie die Daten können ausgenutzt werden.

Die zwei Märkte brauchen einander

Die Technologien, die für physische Sicherheits- und Schutzsysteme verwendet werden, benötigen dringend besseren Cyber-Schutz. Alle Geräte in IP-Netzwerken, besonders solche mit direkter Internetverbindung, benötigen Cyber-Sicherheitsfunktionen. Schätzungen gehen davon aus, dass etwa 70 Prozent der heute verkauften Videoüberwachungskameras mit Computernetzwerken verbunden sind. Das ergibt eine sehr große Anzahl anfälliger Geräte.

Zahlreiche Videoüberwachungskameras werden bereits gehackt. Mit einer einfachen Google-Suche lassen sich die Standorte von Systemen ermitteln, die Videodaten verbreiten. Eine offen verfügbare Suchmaschine, [Shodan](#), ermöglicht die Suche nach anfälligen Webcams und zeigt damit das Problem auf: Live-Feeds von Kameras aus aller Welt sind problemlos abrufbar. Feeds von [Schlafzimmern](#), [Banken](#), [Wohnzimmern](#), [Babyphonen](#), Pools, Hochschulen usw. können von jedermann angesehen werden. Diese Daten sind öffentlich verfügbar, weil die Geräte schlecht konfiguriert sind oder selbst grundlegende Sicherheitskontrollen fehlen. Gewissenhaft vorgehende Hacker sind diskreter und verwenden bessere Tools, um auf viele weitere Systeme zuzugreifen.

Das ist jedoch nur der Anfang. Je mehr physische Sicherheits- und Schutzsysteme mit dem Internet verbunden werden, desto mehr Ausnutzungen und Hijacking-Aktionen sind möglich. Kürzlich wurden [mehr als eine Million Kameras sowie digitale Videorekorder kompromittiert](#) und von einem Angreifer so konfiguriert, dass sie Teil eines Botnets wurden. Dieses Botnet griff anschließend andere mit dem Internet verbundene Systeme an. Da jedoch keine Erkennungskontrollen vorhanden waren, fand all dies statt, ohne dass die Gerätebesitzer merkten, dass sie kriminelle Aktivitäten unterstützen. Physische Sicherheitsprodukte und -dienste benötigen dringend Cyber-basierte Sicherheitskontrollen, um Cyber-Angreifer abwehren zu können.

Die Branchen für physische und Cyber-Sicherheit werden ihre Kräfte bündeln und damit beginnen, Sicherheitsprodukte vor digitalen Bedrohungen zu schützen. Sie werden voneinander profitieren und die Sicherheit der Produkte sowie Dienste der nächsten Generation verbessern.

Durch die Einführung von immer mehr digitalen Geräten und Online-Diensten sowie die zunehmende Vernetzung wird der Bedarf nach Sicherheitsfunktionen weiter steigen. Verbraucher und Unternehmen wollen ihre Privatsphäre sowie Sicherheit schützen und gleichzeitig die Vorteile erweiterter Remote-Funktionen nutzen. Die Unterscheidung zwischen physischen und Cyber-Domänen wird immer weniger relevant sowie zunehmend unmöglich werden. Verbraucher werden es nicht gutheißen, wenn die Kameraaufzeichnung aus dem eigenen Schlafzimmer von Fremden über das Internet gesteuert wird. Es wird sie nicht interessieren, ob dies aufgrund eines Software- oder Netzwerkproblems möglich ist. Stattdessen werden sie den Hersteller des Produkts, den Sicherheitsdienstleister oder den Installateur dafür verantwortlich machen. Das gleiche gilt für Geräte im Gesundheitswesen, Fahrzeuge und Industrieleitsysteme in Unternehmen. All diese Systeme müssen sowohl physisch als auch digital sicher sein.

Verbraucher und Führungskräfte werden das verlangen, was sie schon immer verlangt haben: Eine einzige Entität, die für die Probleme verantwortlich ist und diese behebt. Aktuelle Umfragen zeigen, dass sich Verbraucher der Risiken bereits bewusst werden und [im Falle einer Kompromittierung bereit sind, sich von ihrem Lieblingseinzelhändler zu trennen](#). Diese Tatsache bekam die Telekommunikationsbranche bereits schmerzlich zu spüren. Nach einer aktuellen Datenkompromittierung bei TalkTalk in Europa [wechselten 100.000 Kunden](#) zu einem anderen Anbieter. Diese veränderten Erwartungen, die durch die Verschmelzung der Technologien ausgelöst werden, werden zur aktiven Zusammenarbeit der Anbieter für physische und Cyber-Sicherheit führen.

Vorhersagen

Im Jahr 2017 werden die Branchen für physische und Cyber-Sicherheit zusammenarbeiten, um umfassendere und zuverlässigere Sicherheitslösungen zu schaffen:

1. Die Branchen für physische und Cyber-Sicherheit werden ihre Kräfte bündeln und damit beginnen, Sicherheitsprodukte vor digitalen Bedrohungen zu schützen. Beide Märkte verfolgen bereits das gleiche Ziel bei ihren Kunden. Nun werden sie voneinander profitieren und die Sicherheit der Produkte sowie Dienste der nächsten Generation verbessern.
2. Verbraucher werden verärgert sein über Cyber-Angriffe auf physische Geräte, bei denen die eigene Sicherheit und Privatsphäre unterminiert wird. Sie werden umfassende Sicherheit verlangen und andernfalls nach anderen Anbietern suchen.
3. Anbieter von Cyber-Sicherheitslösungen werden Dienste und Support für Anbieter physischer Sicherheitssysteme bereitstellen. Dazu können neue Software-Plattformen und -Architekturen gehören, die die Integration vereinfachen. Wir erwarten entsprechende Ankündigungen von großen sowie kleinen Cyber-Sicherheitsunternehmen.
4. Auf Konferenzen zu physischer Sicherheit werden Themen, Experten und Anbieter für Cyber-Sicherheit vertreten sein. Die Teilnahme an eigentlich fachfremden Fachveranstaltungen ist ein untrügliches Zeichen für die Zusammenarbeit.



Feedback. Für die zukünftige Gestaltung wünschen wir uns Ihre Rückmeldungen. Wenn Sie uns Ihre Meinung mitteilen möchten, [klicken Sie bitte hier](#), um eine kurze Umfrage zum Threat-Report auszufüllen, die Sie nur fünf Minuten kosten wird.

McAfee Labs folgen



Über Intel Security

McAfee gehört jetzt zu Intel Security. Durch die Security Connected-Strategie, einen innovativen Ansatz für Hardware-unterstützte Sicherheitslösungen sowie das Global Threat Intelligence-Netzwerk ist Intel Security voll und ganz darauf konzentriert, für die Sicherheit seiner Kunden zu sorgen. Dazu liefert Intel Security präventive, bewährte Lösungen und Dienste, mit denen Systeme, Netzwerke und Mobilgeräte von Privatanwendern und Unternehmen weltweit geschützt werden können. Intel Security verknüpft die Erfahrung und Fachkompetenz von McAfee mit der Innovation und bewährten Leistung von Intel, damit Sicherheit als essentieller Bestandteil jeder Architektur und Computerplattform eingebettet wird. Intel Security hat sich zum Ziel gesetzt, allen – Privatpersonen ebenso wie Unternehmen – die Möglichkeit zu geben, die digitale Welt sicher nutzen zu können.

www.intelsecurity.com



McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

Die hier enthaltenen Informationen werden Intel Security-Kunden ausschließlich für Fort- und Weiterbildungszwecke bereitgestellt. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern und werden wie besehen zur Verfügung gestellt, ohne Garantie oder Gewährleistung auf die Richtigkeit oder Anwendbarkeit der Informationen zu einem bestimmten Zweck oder für eine bestimmte Situation. Intel und die Intel- und McAfee-Logos sind Marken der Intel Corporation oder von McAfee, Inc. in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Copyright © 2016 Intel Corporation. 1807_0916_rp_threats-predictions-2017