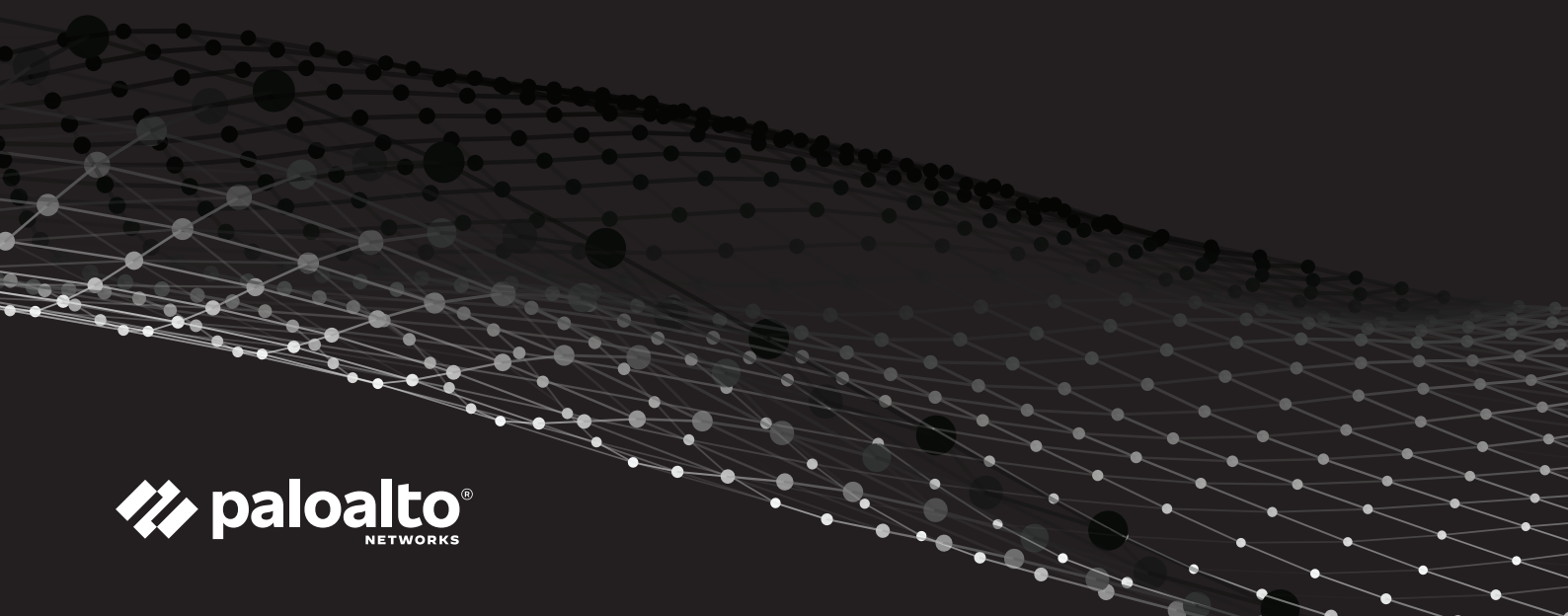
IoT Threat Report 2020 der Unit 42



Inhaltsverzeichnis

Zusammenfassung 3

01 IoT-Sicherheit heute 4

Unternehmen ohne geeignete Tools für IoT-Übersicht und -Sicherheit 5

Eine Zeitbombe für Unternehmen 6

Das Gesundheitswesen ist in einem kritischen Zustand 7

Grundregeln zur Netzwerksegmentierung werden nicht befolgt 8

Fallbeispiel: Conficker im Gesundheitswesen 9

02 Die gefährlichsten Bedrohungen für IoT-Geräte 10

Die Top 3: Exploits, Passwortangriffe und IoT-Würmer 11

Ungepatchte Geräte, veraltete Protokolle:
beste Voraussetzungen für die Ausbreitung im Netzwerk 12

Neue Bedrohungen nehmen IoT-Umgebungen ins Visier 13

Fallbeispiel: Kryptojacking im Einsatz 14

03 Schlussfolgerung und Empfehlungen 15

Maßnahmen, mit denen Sie Ihr Risiko senken 16

Maßnahme 1: Verschaffen Sie sich einen Überblick
über die IoT-Geräte im Netzwerk und damit über Ihr Risiko. 16

Maßnahme 2: Spielen Sie auch bei Druckern und
anderen leicht patchbaren Geräten Patches ein. 16

Maßnahme 3: Teilen Sie IoT-Geräte auf verschiedene VLANs auf 17

Maßnahme 4: Ermöglichen Sie eine aktive Überwachung 18

Perfektionieren Sie Ihre IoT-Strategie 19

Best Practice 1: Gehen Sie die Aufgabe ganzheitlich an und
koordinieren Sie den gesamten Lebenszyklus der IoT-Geräte. 19

Best Practice 2: Weiten Sie die Sicherheitsmaßnahmen
durch Produktintegrationen auf alle IoT-Geräte aus. 20

Über uns 21

Palo Alto Networks 21

Unit 42 21

Methodik 22

Zusammenfassung

Laut einem Gartner-Bericht aus dem Jahr 2019 sollte die Zahl der aktiv genutzten IoT-Geräte bis zum Jahresende 2019 auf 4,8 Milliarden – und damit 21,5 Prozent mehr als im Vorjahr – steigen. Das Internet der Dinge (Internet of Things, IoT) eröffnet allen Branchen die Chance, innovative neue Verfahren und Services einzuführen, ist gleichzeitig aber auch ein Einfallstor für neuartige Sicherheitsrisiken. Um sich einen Überblick über die aktuelle Bedrohungslage für IoT-Geräte zu verschaffen, haben die Threat-Intelligence-Fachleute unserer Unit 42 mit der IoT-Sicherheitslösung Zingbox® von Palo Alto Networks Sicherheitsvorfälle aus den Jahren 2018 und 2019 auf 1,2 Millionen IoT-Geräten ausgewertet. Diese Geräte befanden sich an mehreren tausend Standorten von IT-Unternehmen und Gesundheitseinrichtungen in den USA. Die Auswertung zeigt, dass das Sicherheitsniveau von IoT-Geräten sinkt. Dadurch sind Unternehmen Risiken ausgesetzt, sowohl durch neue, speziell auf IoT-Ressourcen abzielende Malware als auch durch ältere Angriffstaktiken, die für IT-Teams eigentlich schon längst erledigt waren. Dieser Bericht gibt einen detaillierten Überblick über die Bedrohungslage für die IoT-Welt, besonders gefährdete IoT-Geräte sowie die wichtigsten Bedrohungen und enthält praxistaugliche Schritte, mit denen Sie Ihr IoT-Risiko direkt senken können.

IoT-Geräte sind unverschlüsselt und ungesichert

98 Prozent des Datenverkehrs von IoT-Geräten sind unverschlüsselt, und das bedeutet, dass personenbezogene und vertrauliche Daten im Netzwerk ungeschützt sind. Angreifer, die die erste Verteidigungslinie (meist durch Phishingangriffe) überwunden und eine Verbindung zu ihrem Command-and-Control-Server hergestellt haben, können den unverschlüsselten Datenverkehr im Netzwerk direkt mitlesen, personenbezogene und vertrauliche Daten ausschleusen und im Darknet zu Geld machen.

57 Prozent der IoT-Geräte sind anfällig für mittelschwere und schwere Angriffe und damit leichte Beute für Angreifer. Da der Patchstatus von IoT-Geräten meist zu wünschen übrig lässt, haben Angreifer leichtes Spiel mit Exploits von altbekannten Schwachstellen oder können sich sogar mit Standardpasswörtern anmelden.

IoMT-Geräte mit veralteter Software

Im „Internet of Medical Things“ (IoMT) laufen 83 Prozent der Bildgebungsgeräte auf nicht unterstützten Betriebssystemen – eine gewaltige Steigerung um 56 Prozent gegenüber 2018. Das liegt daran, dass in der Zwischenzeit der Support für das Betriebssystem Windows® 7 eingestellt wurde. Dieses abnehmende Sicherheitsniveau öffnet neuartigen Angriffsformen Tür und Tor, etwa Kryptojacking (2017 noch 0 Prozent, 2019 schon 5 Prozent), und ruft auch längst vergessene Bedrohungen wieder auf den Plan, etwa den Wurm Conficker, gegen den IT-Teams ihre Systeme längst geschützt hatten.

Die IoMT-Systeme mit den größten Sicherheitslücken sind Bildgebungssysteme, die im klinischen Arbeitsablauf eine zentrale Rolle spielen. Sie sind von 51 Prozent der Bedrohungen in Gesundheitseinrichtungen betroffen. Das schränkt die Versorgungsqualität ein und ermöglicht Angreifern, die Patientendaten zu stehlen, die auf diesen Geräten gespeichert sind.

Lückenhafte Netzwerk-„Hygiene“ im Gesundheitswesen

72 Prozent der VLANs im Gesundheitswesen bestehen aus IoT- und IT-Geräten, sodass Schadsoftware von Benutzergeräten auf mangelhaft geschützte IoT-Geräte im selben Netzwerk überspringen kann. Stolze 41 Prozent der Angriffe nutzen Schwachstellen von Geräten aus: Angriffe, die von der IT ausgehen, scannen die ins Netzwerk eingebundenen Geräte auf der Suche nach bekannten Schwachstellen. Wir beobachten eine Verschiebung des Angriffsspektrums: Statt IoT-Botnets, die Denial-of-Service-Angriffe starten, zielen heute ausgefeiltere Angriffe auf Patientenidentitäten, Unternehmensdaten und Lösegeld durch Ransomware.

IoT-Cyberattacken nehmen veraltete Protokolle ins Visier

Es entstehen neuartige Bedrohungen speziell für IoT-Geräte, die etwa Command-and-Control-Kommunikationskanäle (C2) oder wurmartige Mechanismen zur Weiterverbreitung nutzen. Angreifer haben die Verwundbarkeit von Protokollen, die wie DICOM seit Jahrzehnten eingesetzt werden, erkannt und können auf diesem Weg unverzichtbare Funktionen in den Einrichtungen beeinträchtigen.

01

IoT-Sicherheit heute

Das IoT wächst schnell ...

Ende 2019 gab es geschätzt 4,8 Milliarden IoT-Geräte, **21,5 Prozent** mehr als Ende 2018.[1]

Die meisten dieser neuen IoT-Geräte sind natürlich mit Netzwerken oder dem Internet verbunden.

Heute stellen IoT-Geräte in einem durchschnittlichen Unternehmen mehr als **30 Prozent** aller Endpunkte in Netzwerken dar (Mobilgeräte nicht mitgerechnet).

... und hat ein riesiges Sicherheitsproblem

98 Prozent des IoT-Datenverkehrs sind unverschlüsselt, und das bedeutet, dass personenbezogene und vertrauliche Daten im Netzwerk ungeschützt sind.

57 Prozent der IoT-Geräte sind anfällig für mittelschwere und schwere Angriffe und damit leichte Beute für Angreifer.

83 Prozent der Bildgebungsgeräte nutzen nicht unterstützte Betriebssysteme – eine gewaltige Steigerung von 56 Prozent gegenüber 2018, die vor allem auf den Ablauf der Unterstützung für Windows 7 zurückzuführen ist.

Schlagzeilenträchtige Cyberangriffe auf IoT-Geräte zwingen ganze Branchen, sich mit den IoT-Risiken auseinanderzusetzen und sie in den Griff zu bekommen, um ihr Kerngeschäft zu schützen. Das Gesundheitswesen beispielsweise ist Risiken ausgesetzt, die alle bisherigen Erwartungen übersteigen. Einige IoT-Schwachstellen bringen Menschenleben in Gefahr, andere dagegen zielen auf zentrale Unternehmensfunktionen ab oder schleusen vertrauliche Daten nach außen.

Lesen Sie weiter, um mehr über die Sicherheitslage im Internet der Dinge zu erfahren.

1. „Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020“, Gartner, 29. August 2019, https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io.

Unternehmen ohne geeignete Tools für IoT-Übersicht und -Sicherheit

Unternehmen kennen die Risiken für ihre IoT-Geräte und -Anwendungen nicht – und das stellt sie vor eine große Herausforderung. Die Hauptursache dafür ist der fehlende Überblick über Geräte und Inventar.

Mangelnde IoT-Transparenz in IT-Abteilungen

IoT-Geräte lassen sich zwar mit in die Jahre gekommenen statischen Inventarprogrammen durch das Setzen eines Häkchens erfassen, aber das ist alles andere als ein wirksames Sicherheitsmanagement. Die Identifizierung von Geräten über klassische IT-Eigenschaften wie IP-Adresse und Betriebssystem funktioniert für das IoT nicht. Nur wenn der genaue Gerätetyp bekannt ist, kann ein Unternehmen sachgerecht planen: Netzwerkanforderungen, Bereitstellungstaktik, optimierte Sicherheitsstrategie, Betriebsplanung. Sicherheitssysteme können das Verhalten identifizierter Geräte im Kontext der Arbeitsabläufe erfassen und sind nicht mehr darauf angewiesen, lediglich unbekannte Gerätetypen mit dynamischen und wechselnden IP-Adressen zu beobachten.

Kein IoT-Support in klassischen Sicherheitssystemen

Systeme zum Schutz von Endpunkten wurden für Computer, Tablets und Smartphones konzipiert und arbeiten mit Agenten. IoT-Geräte allerdings verwenden oft benutzerspezifische oder veraltete Betriebssysteme ohne Unterstützung für Agenten. Für Cybersicherheitssysteme sind IoT-Geräte daher unbekannte Endpunkte – sie kennen weder den genauen Typ des Geräts noch sein Risikoprofil oder sein erwartetes Verhalten.

Netzwerkbasierte Systeme für die Cybersicherheit können zwar mit dem Netzwerk verbundene Endpunkte erkennen, sind aber nur selten in der Lage, IoT-Geräte korrekt zu identifizieren, zu überwachen und zu schützen.

Nebeneinander von IT und OT mit organisatorischen und personellen Herausforderungen

In den meisten Unternehmen werden Informationstechnologie (IT) und Betriebstechnologie (OT) von unterschiedlichen Teams betreut, die mit jeweils eigenen Prozessen und Tools arbeiten. Die IT-Teams kümmern sich um IT-Ressourcen wie Computer, Netzwerktechnik und Drucker, die OT-Teams betreuen die Ressourcen, die nicht zur IT gehören, etwa Medizintechnik und Sicherheitskameras.

Diese Teams sind in unterschiedliche Hierarchien eingebunden und verfolgen daher verschiedene Strategien für die Gerätesicherheit. Oft sind die IT-Teams hier wegen der rasanten Entwicklung bei den Betriebssystemen von PCs und Servern und durch ihre eigenen Sicherheitsinitiativen moderner aufgestellt als die Medizintechnik.

So kennen sich die Medizintechniker zwar mit der Funktionsweise und Wartung ihrer Geräte aus, aber nicht mit den Betriebssystemen, die auf diesen Geräten laufen. Oft nutzen diese ins Netzwerk eingebundenen medizinischen Geräte (etwa digitale Röntgengeräte) veraltete Betriebssysteme mit bekannten Schwachstellen und stellen daher ein hohes Risiko für die Beschäftigten, Patienten, Computersysteme und letztlich auch für den Geschäftsbetrieb der Einrichtung dar.

Eine Zeitbombe für Unternehmen

Alles, was kein Desktop-Computer, Laptop oder Smartphone ist, ist ein IoT-Gerät. Das können ganz alltägliche Bürogeräte sein: IP-Telefone, Drucker usw. Diese Geräte sind mit dem Netzwerk verbunden, sind allesamt Ziele für Angreifer und werden vom IT-Team oft nicht ausreichend gewartet.

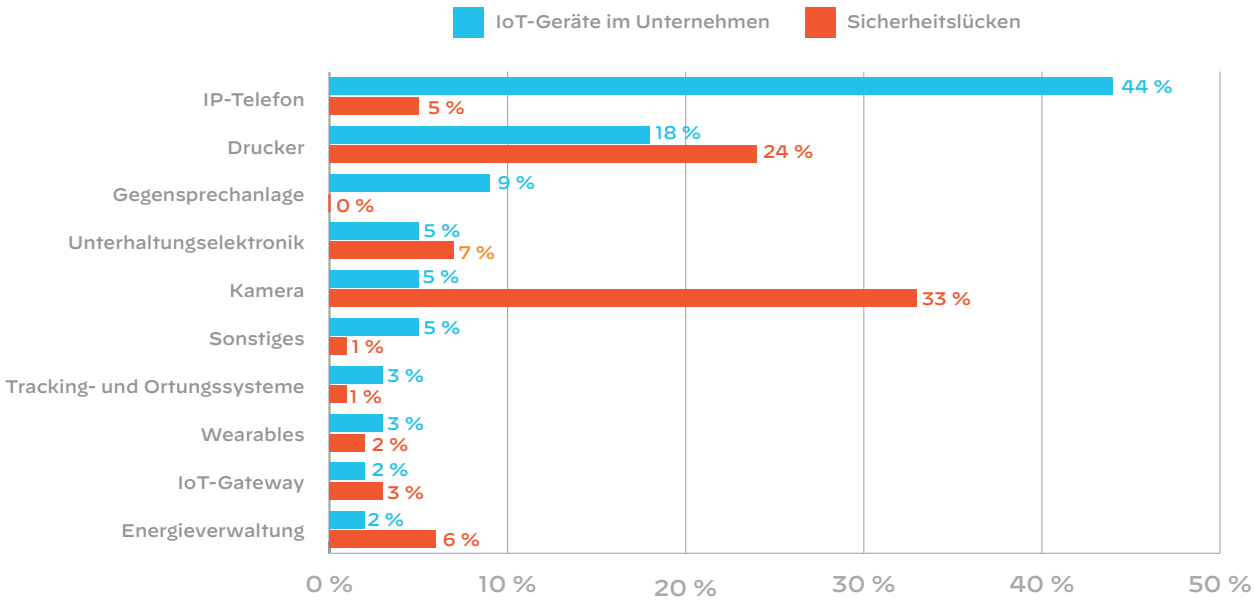
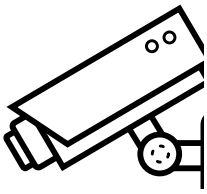


Abbildung 1: 5 Prozent aller Sicherheitslücken entfallen auf IP-Telefone.

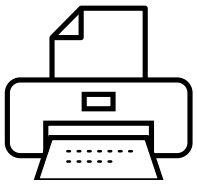
Gute Noten für IP-Telefone: Sie machen zwar 44 Prozent aller IoT-Geräte in Unternehmen aus, sind aber nur für 5 Prozent aller Sicherheitslücken verantwortlich. IP-Telefone finden sich in Unternehmen aller Branchen und wurden für Unternehmensansprüche hinsichtlich der Zuverlässigkeit und Sicherheit entwickelt.

Sicherheitskameras machen nur 5 Prozent aller IoT-Geräte in Unternehmen aus, sind aber für 33 Prozent aller Sicherheitslücken verantwortlich. Das liegt daran, dass viele Kameras für den Privatbereich konzipiert wurden, wo die Benutzerfreundlichkeit Vorrang vor der Sicherheit hat.



Wie können Angreifer Sicherheitskameras ausnutzen?
2016 starteten Jugendliche den weltumspannenden Mirai-Angriff, der über 600.000 Überwachungskameras befiel, um große Teile des Internets nach offenen Telnet-Schnittstellen abzusuchen und sich dort mit Standardpasswörtern anzumelden.

Drucker stellen 18 Prozent aller IoT-Geräte und verursachen 24 Prozent aller Sicherheitsprobleme. Drucker sind grundsätzlich mit weniger Sicherheitsmaßnahmen ausgestattet, und Schwachstellen in Browserschnittstellen machen sie oft zu idealen Einfallstoren für Cyberattacken.



Wie gefährlich ist ein gekaperter Drucker? Er kann:

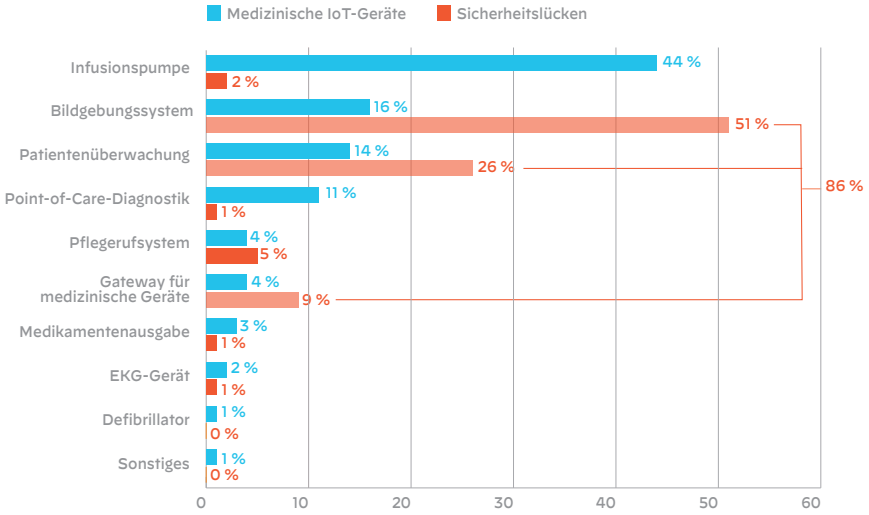
- Zugriff auf Druckprotokolle gewähren
- ein Ausgangspunkt für die Infektion anderer Computer im Netzwerk sein
- im Rahmen eines DDoS-Angriffs genutzt werden

Das Gesundheitswesen ist in einem kritischen Zustand

2019 stellte eine Gartner-Untersuchung fest, dass 40 Prozent der IT-Verantwortlichen im Gesundheitswesen für 2020 planen, neue oder zusätzliche Budgets für Cybersicherheitstools auszugeben[2]. Bis es soweit ist, befinden sich medizintechnische Geräte jedoch in einem kritischen Zustand.

Medizinische Geräte mit veralteten Betriebssystemen
Weil IoT-Geräte im Gesundheitswesen sehr lange eingesetzt werden, finden sich hier besonders häufig veraltete und oft sogar nicht mehr unterstützte Betriebssysteme. Diese Geräte werden weder von der IT-Abteilung gewartet noch von den Herstellern des Betriebssystems unterstützt.

Fehlende Sicherheitsfunktionen
Die Medizintechniker, die für medizinische Geräte verantwortlich sind, haben oft nicht die erforderlichen IT-Kenntnisse und -Ressourcen. So fehlt es an Vorgaben für Passwörter, der sicheren Speicherung von Passwörtern und dem zuverlässigen Einspielen aktueller Patches.



Die gute Nachricht: Die US-Behörde NCCoE (National Cybersecurity Center of Excellence) hat 2019 ein Projekt zur Sicherheit von IoT-Geräten im Gesundheitswesen fertiggestellt. Ziel war, Richtlinien sowie eine Referenzarchitektur zur Sicherung von PACS-Systemen bereitzustellen sowie Beispiellösungen zu entwickeln, die kommerzielle und Open-Source-Produkte für die Cybersicherheit nutzen.

Abbildung 2: Sicherheitslücken bei medizinischen Geräten

Bildgebungssysteme sind extrem anfällig

Bildgebungssysteme nutzen mit Windows, Linux und Unix unterschiedliche Betriebssysteme. Bei Redaktionsschluss liefen 83 Prozent aller Systeme zur medizinischen Bildgebung unter nicht länger unterstützten Betriebssystemen mit bekannten Schwachstellen und ohne aktuelle Sicherheitsupdates oder Patches. Dies ist eine gewaltige Steigerung um 56 Prozent gegenüber 2018, da in der Zwischenzeit der Support für Windows 7 eingestellt wurde.

Neue Angriffe nutzen Schwachstellen in den Betriebssystemen von medizinischen IoT-Geräten aus. Bildgebungssysteme sind besonders anfällig für diese Art von Angriffen, weil sie aufgrund ihrer langen Lebensdauer oft noch lange nach dem offiziellen Ende der Unterstützung für ihr Betriebssystem weiter genutzt werden.

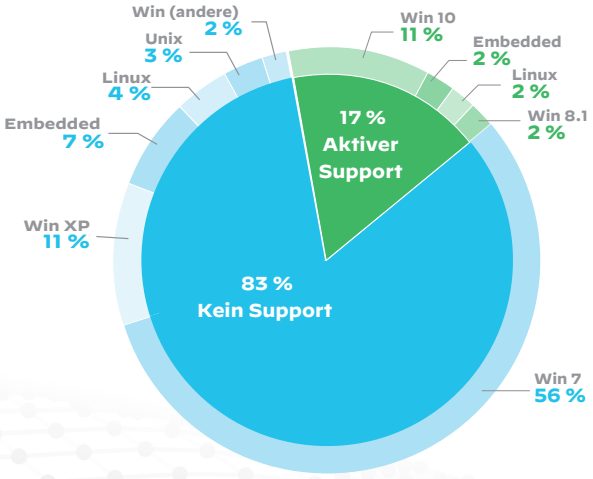


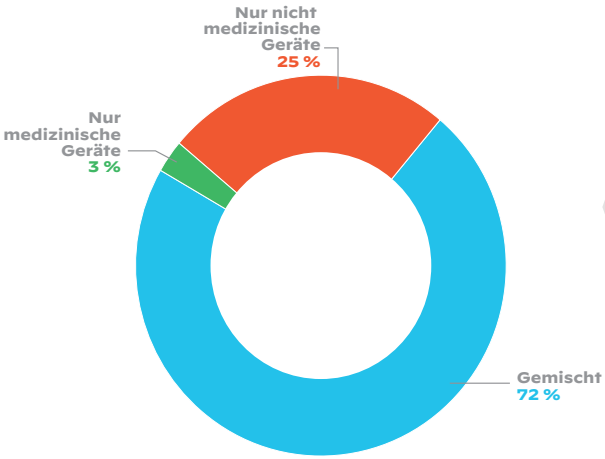
Abbildung 3: Sicherheitsvorgaben für intelligente Geräte

Fortschritt: Ein neues Gesetzesvorhaben des US-Kongresses soll die Sicherheit intelligenter Geräte regulieren. Laut dem „IoT Cybersecurity Act“ von 2019 soll das US-Normungsinstitut NIST Normen für die sichere Entwicklung von IoT-Geräten sowie für die Geräteverwaltung, Patches und das Konfigurationsmanagement erarbeiten.

2. „2019 Top Actions for Healthcare Provider CIOs: Summary and Retrospective View“, Gartner, 26. Februar 2019, https://www.gartner.com/en/documents/3903067/2019-top-actions-for-healthcare-provider-cios-summary-an.

Grundregeln zur Netzwerksegmentierung werden nicht befolgt

Die einfachste Maßnahme zur Vermeidung von Risiken durch IoT-Geräte ist die Netzwerksegmentierung. Dennoch enthalten lediglich 3 Prozent aller segmentierten Netzwerke und VLANs in den von uns untersuchten Gesundheitseinrichtungen ausschließlich medizintechnische IoT-Geräte. 25 Prozent enthielten nur IP-Telefone, Drucker und andere nicht medizinische IoT-Geräte.



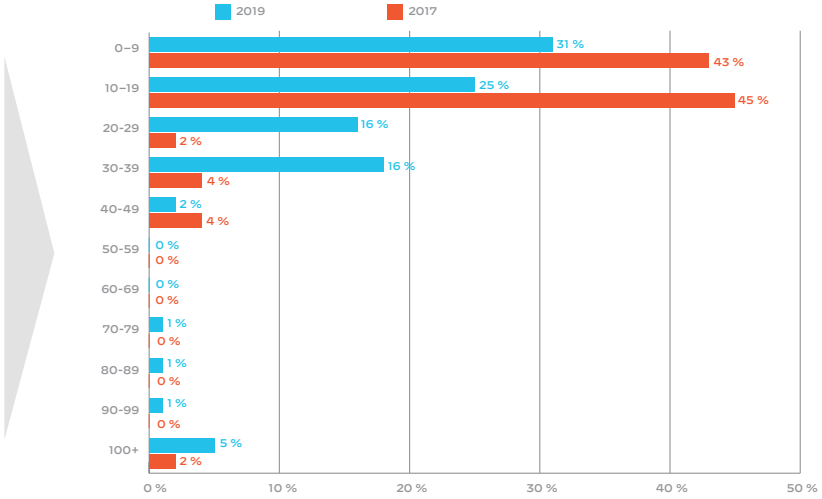
72 Prozent der VLANs im Gesundheitswesen enthalten einen Mix aus medizinischen IoT-Geräten, IoT-Bürogeräten und IT-Geräten. Das erleichtert Angreifern die Ausbreitung im Netzwerk. So können Angreifer von einem infizierten Laptop mühelos zu Überwachungskameras und DICOM-Viewern im selben Netzwerk gelangen. Gesundheitseinrichtungen sollten derart anfällige Systeme dieses Jahr unbedingt besser schützen.

Abbilding 4: **VLANs mit verschiedenartigen IoT-Geräten**

Das ist schon dreimal besser als 2017.

Zwar gibt es noch immer eine Menge zu tun, aber wir stellen fest, dass die Netzwerksegmentierung sich allmählich durchsetzt:

- 2017 hatten nur 12 Prozent aller Krankenhäuser mehr als 20 VLANs.
- 2019 waren es schon 44 Prozent.



Abbilding 5: **Mehr als dreimal so viel VLANs in Krankenhäusern**

Netzwerksegmentierung ist nicht genug: Mikrosegmentierung ist optimal

Dieser Trend ist zwar erfreulich, aber die Netzwerksegmentierung allein reicht nicht. So wäre es beispielsweise nicht verantwortungsvoll, lebenswichtige Geräte zur Herzfrequenzmessung im selben Netzwerk zu betreiben wie Bildgebungssysteme. Eine Mikrosegmentierung hingegen, die sich an Geräteprofilen und zahlreichen weiteren Faktoren wie Gerätetyp und -funktion, Kritikalität und Bedrohungsniveau orientiert, ist eine Isolierungsstrategie, die die möglichen Folgen einer Infektionsausbreitung deutlich begrenzt.

FALLBEISPIEL: Conficker im Gesundheitswesen

Zingbox, die Sicherheitslösung für IoT-Geräte von Palo Alto Networks, warnte die Sicherheitsverantwortlichen eines Krankenhauses, als der Wurm Conficker in seinem Netzwerk festgestellt wurde. Das betroffene Gerät war ein Mammografiesystem. An den folgenden Tagen identifizierte Zingbox ein weiteres Mammografiegerät, einen DICOM-Viewer, ein digitales Radiologiesystem und einige weitere Geräte mit Conficker-Verhaltensmerkmalen als infiziert.

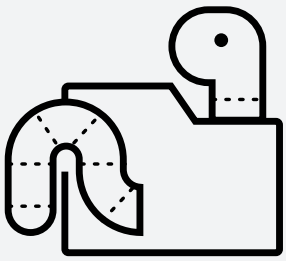
Daraufhin schaltete das Krankenhauspersonal diese Geräte aus, solange sie nicht in Verwendung waren. Zur Bestätigung der Infektion trennte das Personal eines der infizierten Mammografiegeräte und den DICOM-Viewer vom Netzwerk und spielte frische Software-Images auf. Nur wenige Stunden, nachdem die Geräte wieder online waren, hatte Conficker sie erneut infiziert.

Eine genauere Untersuchung ergab, dass die Software-Images zwar die Malware entfernt hatten, die Images aber veraltet waren: Die aktuellen Sicherheitspatches waren darin nicht enthalten, sodass die Geräte anfällig für eine Conficker-Infektion blieben. Da sich Conficker im Netzwerk von Gerät zu Gerät ausbreitet, war es nur eine Frage der Zeit, bis die Infektion von einem anderen Gerät zurück auf die neu aufgesetzten Geräte gelangte.

Nun nahm das Krankenhaus alle infizierten Geräte offline, spielte neue Images auf, installierte die aktuellen Patches und stellte die Geräte eines nach dem anderen wieder online. Dabei wurden die Geräte auf auffälliges Verhalten überwacht. Es dauerte eine Woche, bis wieder alle Geräte im Netzwerk waren. Sie zeigten keine weiteren Anzeichen einer Infektion mit Conficker.

Das ist ein typisches Beispiel für die Herausforderungen, denen sich viele Unternehmen heute gegenübersehen. Ohne Echtzeit-Einblick in das Verhalten von IoT-Geräten und ohne ausreichendes Know-how zur Cybersicherheit sind sie schlecht aufgestellt, um schnell auf Bedrohungen zu reagieren, die Ausbreitung einer Infektion einzudämmen und die Ursache zu beseitigen. In einigen Unternehmen sind die betroffenen Geräte unverzichtbar für den Betrieb. Es ist also extrem schwierig oder sogar unmöglich, diese Geräte zur Fehlerbehebung vom Netz zu nehmen und saubere Images aufzuspielen, ohne den gesamten Betrieb zu beeinträchtigen. So kommt es, dass viele Unternehmen in einer Endlosschleife gefangen sind, bei der sie lediglich die Symptome bekämpfen und hoffen, dass alles gut gehen wird.

Conficker ist zurück!



Conficker, auch unter den Namen Downup und Kido unterwegs, ist ein Wurm, der Systeme mit Microsoft Windows befällt. Bei seinem ersten Auftreten im November 2008 nutzte er Schwachstellen aus und versuchte, mit Wörterbuchangriffen Administratorpasswörter zu knacken, um sich auszubreiten und ein Botnet aufzubauen. 2009 hatte er bereits in über 190 Ländern geschätzte 15 Millionen Computer in Behörden, Unternehmen und Privathaushalten befallen. Als IT-Fachleute und Anbieter von Antivirensoftware endlich wirksame Gegenmittel hatten, konnten sie die Zahl der infizierten Rechner auf 1,7 Millionen im Jahr 2011 und 400.000 im Jahr 2015 senken.

Inzwischen ist Conficker längst vom Radar der IT-Abteilungen verschwunden, taucht aber seit Kurzem wieder auf medizintechnischen Geräten auf, die veraltete oder nicht mehr unterstützte Windows-Versionen verwenden. Als dieser Bericht verfasst wurde, hatten fast 20 Prozent der Zingbox-Nutzer aus dem Gesundheitswesen schon mindestens eine Infektion mit Conficker hinter sich.

02

Die gefährlichsten Bedrohungen für IoT-Geräte

Bedrohungen werden permanent weiterentwickelt, um IoT-Geräte mit neuen Strategien anzugreifen. Dazu werden beispielsweise Command-and-Control-Kommunikationskanäle (C2) oder wurmartige Mechanismen zur Weiterverbreitung genutzt.

Dieser Trend wird durch die unzureichende Sicherheit von Geräten und Netzwerken begünstigt.

- 72 Prozent der VLANs im Gesundheitswesen bestehen aus IoT- und IT-Geräten, sodass Schadsoftware von Benutzergeräten auf mangelhaft geschützte IoT-Geräte im selben Netzwerk überspringen kann.
- 41 Prozent der Angriffe nutzen Schwachstellen von Geräten aus: Angriffe, die von der IT ausgehen, scannen die ins Netzwerk eingebundenen Geräte auf der Suche nach bekannten Schwachstellen.
- Angriffe auf jahrzehntealte OT-Protokolle wie DICOM sind der Ausgangspunkt für gravierende Einschränkungen zentraler Geschäftsfunktionen und für die weitere Ausbreitung der Schadsoftware im gesamten Unternehmen.

Zwischen dem Sicherheitsniveau der OT- und der IT-Welt klafft eine Lücke, die das Unternehmen verwundbar macht für Angriffe, die man seit mehr als einem Jahrzehnt überwunden glaubte.

Lesen Sie weiter, um mehr über unsere Erkenntnisse zu den wichtigsten Bedrohungen und Angriffsformen zu erfahren.

der VLANs im Gesundheitswesen enthalten sowohl IoT- als auch IT-Geräte.

der Angriffe nutzen Geräteschwachstellen aus.

Die Top 3: Exploits, Passwortangriffe und IoT-Würmer

1. Exploits nutzen Geräteschwach-stellen aus

Die unzureichende Sicherheit von IoT-Geräten macht sie zwar zu leichten Angriffszielen, doch die Geräte selbst dienen in der Regel nur als Sprungbrett für die weitere Ausbreitung auf andere Systeme im Netzwerk.

In den Netzwerken laufen dann Scans des Netzwerks, von IP-Adressen, Ports und Schwachstellen – auf der Suche nach anderen Geräten und Systemen für die nächsten Ausbreitungsschritte.

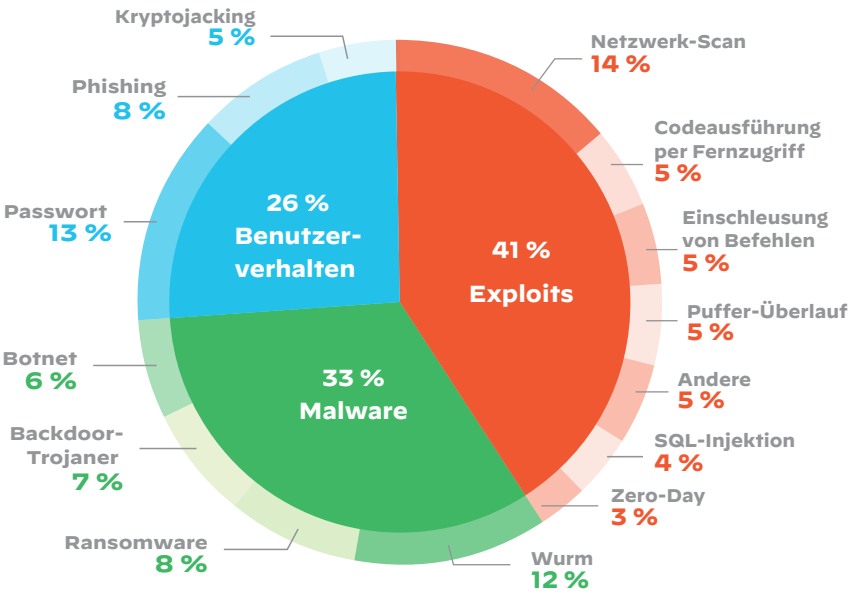


Abbildung 6: Aufschlüsselung der wichtigsten IoT-Bedrohungen

2. Passwortangriffe

Vom Hersteller vergebene Standardpasswörter und ein mangelndes Sicherheitsbewusstsein bei Passwörtern zählen nach wie vor zu den Hauptursachen für IoT-Angriffe mit geknackten Passwörtern. Das kalifornische Gesetz SB-327 verbietet bereits die Nutzung der voreingestellten Anmeldedaten bei IoT-Geräten; wir gehen davon aus, dass dieses Beispiel Schule macht.

Auch abweichende Praktiken innerhalb des Unternehmens ermöglichen Angriffe über Passwörter. Oft entsprechen die vom OT-Personal festgelegten Passwörter nicht den strengeren Vorschriften der IT für Passwörter und ihre Verwaltung. Das ist nur ein Beispiel für die unterschiedliche Handhabung der Cybersicherheit in OT- und IT-Teams.

3. IoT-Würmer statt IoT-Botnets

Derzeit lässt sich bei den Beweggründen der Angreifer eine Verschiebung beobachten: Es geht ihnen immer weniger darum, Botnets für DDoS-Angriffe durch IoT-Geräte einzurichten, sondern zunehmend darum, wurmartige Malware im Netzwerk zu verbreiten, sodass sie Schadcode ausführen und zahlreiche neuartige Angriffe durchführen können.

WLAN-Router im Fadenkreuz

Unsere Unit 42 hat eine Gafgyt-Variante gefunden, die über 32.000 möglicherweise ungeschützte WLAN-Router in kleinen Unternehmen und Privathaushalten angreift, um einen Botnet-Angriff auf Spieleserver im Internet zu führen.

WLAN-Router gehören heute zu den häufigsten IoT-Geräten in Unternehmen. Sie sind beliebte „Rekruten“ für IoT-Botnets, denn dadurch kann nicht nur das zur Arbeit benötigte Netzwerk beeinträchtigt, sondern auch die Reputation der IP-Adressen der betroffenen Unternehmen geschädigt werden.

Ungepatchte Geräte, veraltete Protokolle: beste Voraussetzungen für die Ausbreitung im Netzwerk

Schlechter Patchstatus

IoT-Exploits sind eine große Herausforderung für Sicherheitsteams, da sie oft veraltete Betriebssysteme angreifen, für die es keine Sicherheitsupdates mehr gibt. Wir haben festgestellt, dass 83 Prozent der medizinischen Bildgebungssysteme Betriebssysteme nutzen, die nicht mehr vom Hersteller unterstützt werden. Und das bedeutet, dass alte und längst bekannte Exploits für diese Systeme noch eine große Gefahr darstellen.

Ältere OT-Protokolle sind leichte Ziele

Wir haben Schwachstellen in älteren OT-Protokollen gefunden. Ursprünglich wurden diese Protokolle für den Betrieb hinter einer Firewall konzipiert, in einer Umgebung ohne nennenswerte Aktivitäten von anderen Systemen oder Benutzern. Heute nutzen allerdings immer mehr Einrichtungen und Unternehmen Clouds, sodass die Netzwerkgrenzen verschwimmen und diese jahrzehntealten Protokolle nicht mehr von dem geschäftigen Betrieb des restlichen Netzwerks abgeschottet sind.

Beispiel: Ein gehacktes Alt-Protokoll

Wir haben eine Sicherheitslücke in einem DICOM-Protokoll gefunden. Die Angreifer konnten den Header eines DICOM-Pakets so modifizieren, dass das vom Gerät erfasste Bild durch eine ausführbare Datei ersetzt wurde. Beim Speichern des „Bildes“ gelangte die Malware auf ein Netzwerklaufwerk. Wenn ein anderes DICOM-Gerät das vermeintliche Bild öffnete, führte der DICOM-Viewer stattdessen die Malware aus. Da mit DICOM-Bildern oft auch Patientendaten gespeichert werden, durften die Speicherorte der Bilder aus Datenschutzgründen nicht von Antivirensoftware untersucht werden – so wurde diese Malware durch die Sicherheitsvorgaben geschützt.

Ausbreitung im Netzwerk

Ausgangspunkt für die Ausbreitung von Schadcode im Netzwerk sind oft erfolgreiche Phishingangriffe auf IoT-Systeme im selben Netzwerk, durch die Schwachstellen dann per Fernzugriff ausgenutzt werden. 57 Prozent der IoT-Geräte sind anfällig für mittelschwere und schwere Angriffe und damit leichte Beute für Angreifer.

Kein Schutz vor zweistufigen Angriffen über Backdoors

Bei einer Schadcode-Infektion installierte Backdoors oder „Hintertüren“ werden oft nicht bemerkt oder nicht vollständig deaktiviert, sodass die Angreifer sie als Einfallstor für zahlreiche weitere Angriffe nutzen können. So wird derzeit beispielsweise die Ransomware WannaCry durch Backdoors in Unternehmensnetzwerke eingeschleust, die bei früheren Angriffen mit der Malware DoublePulsar installiert wurden.

Angesichts der Tatsache, dass die Anzahl nicht mehr patchbarer Geräte, zum Beispiel mit Windows 7, steigt, gehen wir nicht davon aus, dass sich dieser Trend abschwächen wird, solange sich nicht mehr Unternehmen auf die Best Practices in dieser Sache besinnen.

Neue Bedrohungen nehmen IoT-Umgebungen ins Visier

Peer-zu-Peer-Spezialisten

Bedrohungen, die auf IoT-Umgebungen abzielen, setzen für ihre Command-and-Control-Aktivitäten zunehmend auf dezentralisierte Peer-zu-Peer-Kommunikation, sodass die infizierten Geräte, die von einem Netzknoten über eine Serververbindung gesteuert werden, miteinander über das lokale Netzwerk kommunizieren. So können die Angreifer die Verbindungen nach draußen begrenzen und die infizierten Geräte ganz ohne Internetzugang steuern.

Über Schwachstellen in IoT-Geräten mit Cloud-Verbindung (etwa Sicherheitskameras mit Fernübertragung) können Angreifer Firewalls umgehen und in private Netzwerke eindringen.

Der Kampf um den Host

Wir beobachten zunehmend, dass Malware versucht, andere Malware von befallenen IoT-Geräten zu entfernen, um sie für sich allein zu haben. Vermutlich stehen Hardwarebeschränkungen hinter diesem Trend, denn die Gerätehersteller reduzieren die Hardwarekapazitäten ihrer speziell angefertigten Platinen auf ein Minimum, um den Energieverbrauch und die Preise zu senken.

Bekannter IoT-Malware-Code dient als Grundlage für neue Varianten

Letztes Jahr ist der Quellcode für das IoT-Botnet Mirai bekannt geworden – und in der Folge entstanden zahlreiche neue Mirai-Varianten. Die Programmierung dieser Varianten lässt sich mit der Open-Source-Szene vergleichen, wo Entwickler die Arbeit von anderen als Grundlage für eigene Projekte nehmen.

Aus Mirai ist mittlerweile ein richtiges Framework geworden, an das Entwickler neue Exploits als neue Varianten anfügen können.

Ransomware WannaCry breitet sich in unsegmentierten Netzwerken aus

Netzwerke unserer Kunden aus dem Gesundheitswesen, in denen wir WannaCry finden, sind immer gemischte Netzwerke mit PCs, Scannern, Geräten für die nuklearmedizinische Bildgebung usw. WannaCry ist sehr stark darauf ausgelegt, sich selbst weiterzuverbreiten, und bedeutet daher eine große Infektionsgefahr für andere Geräte in den IoT- und IT-Umgebungen.

Botnet-Angriffe mit Mirai

Die Malware Mirai übernimmt die Kontrolle über Netzwerkgeräte mit Linux, macht sie zu ferngesteuerten Bots und gliedert sie in Botnets ein, um sie für groß angelegte, netzwerkbasierte Angriffe zu missbrauchen. Mirai befällt hauptsächlich Onlinegeräte für den privaten Gebrauch, zum Beispiel IP-Kameras und Router.

Am 12. Oktober 2016 legte ein massiver DDoS-Angriff durch ein Mirai-Botnet einen Großteil des Internets entlang der Ostküste der USA lahm. Zunächst befürchteten die Behörden, dass hinter diesem Angriff ein anderer Staat stehen könnte.

FALLBEISPIEL: Kryptojacking im Einsatz

Immer häufiger wird Malware zum Kryptojacking eingesetzt: Sie verbirgt sich auf dem befallenen Gerät und nutzt seine Ressourcen zum „Schürfen“ von Kryptowährungen wie Bitcoins. Wie bei den meisten Angriffen durch Schadcode geht es hier um Geld. Im Unterschied zu anderer Schadsoftware soll die Malware hier allerdings vor den Nutzern verborgen bleiben. Kryptojacking belastet die CPU und das Netzwerk stark und belegt Ressourcen, die eigentlich lebensrettenden medizinischen Systemen vorbehalten sind.

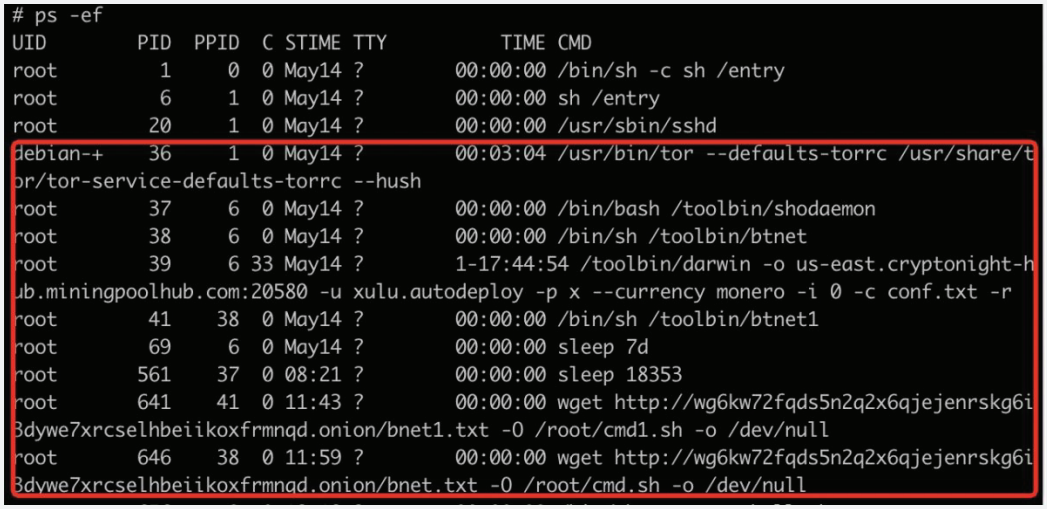


Abbildung 7: Kryptojacking beeinträchtigt lebensrettende medizinische Systeme

Zingbox machte einen Kunden, der an dieser Untersuchung teilnahm, darauf aufmerksam, dass ein Kryptojacking-Code zwischen einem Speichergerät der IT und einem OT-Gerät im internen Netzwerk übertragen wurde. Das IT-Team wollte das Gerät außer Betrieb nehmen, aber das OT-Team war aus Gründen der Produktionssicherheit nicht damit einverstanden. Während die IT-Fachleute auf die Erlaubnis warteten, das Gerät vom Netz zu nehmen, untersuchten sie das Speichergerät, während Zingbox den Datenverkehr im Netzwerk weiter auf verdächtige Aktivitäten überwachte.

Am nächsten Tag wurde wieder Kryptojacking-Code im Netzwerk identifiziert. Weitere Untersuchungen identifizierten als Quelle einen Server, der hunderte virtuelle Maschinen (VM) im OT-Netzwerk hostete, sodass die VM, von der das Problem ausging, schwierig zu finden war. Die fortlaufende Überwachung des Datenverkehrs zeigte, dass zweimal wöchentlich Datenübertragungen stattfanden. Dank dieser Regelmäßigkeit konnte das IT-Team ermitteln, welcher Prozess und welche VM das Problem verursachten. Beide wurden anschließend vom VM-Host entfernt.

03

Schlussfolgerung und Empfehlungen

CSOs können ihr IoT-Risiko mit Sofortmaßnahmen unmittelbar senken …

CSOs können das Risiko einer IoT-basierten Attacke mit einigen sofort umsetzbaren Maßnahmen mindern. Die folgende Liste ist keinesfalls vollständig, verhindert aber einen Großteil der IoT-Bedrohungen:

1. Verschaffen Sie sich einen Überblick über die IoT-Geräte im Netzwerk – und damit über Ihr Risiko.
2. Spielen Sie auch bei Druckern und anderen leicht patchbaren Geräten Patches ein.
3. Teilen Sie IoT-Geräte auf verschiedene VLANs auf.
4. Ermöglichen Sie eine aktive Überwachung.

… und das Unternehmen mit einer wirkungsvollen IoT-Strategie langfristig schützen.

Um Risiken zu kennen und ihnen vorzubeugen, benötigen Unternehmen eine wirksame Strategie für die IoT-Sicherheit. Unser Forschungsteam hat zwei weitere Prinzipien ausgewählt, die in jeder IoT-Strategie enthalten sein sollten:

1. Gehen Sie die Aufgabe ganzheitlich an und koordinieren Sie den gesamten Lebenszyklus der IoT-Geräte.
2. Weiten Sie die Sicherheitsmaßnahmen durch Produktintegrationen auf alle IoT-Geräte aus.

Maßnahmen, mit denen Sie Ihr Risiko senken

Maßnahme 1: Verschaffen Sie sich einen Überblick über die IoT-Geräte im Netzwerk – und damit über Ihr Risiko.

Mit speziell für IoT-Geräte entwickelten Sicherheitslösungen können Unternehmen IoT-Geräte im Netzwerk erkennen und identifizieren. Nach unseren Forschungsergebnissen sind in einem durchschnittlichen Unternehmen 30 Prozent aller mit dem Netzwerk verbundenen Geräte (Smartphones ausgenommen) IoT-Geräte. Obwohl das eine große Zahl an Geräten ist, haben viele Unternehmen diese Geräte gar nicht im Blick und kümmern sich daher weder um ihre Sicherheitsausstattung noch um ihr Risikoprofil.

Mit intelligenten Geräte-Scans und Geräteprofilen können sich IT-Sicherheitsteams einen Überblick über die IoT-Geräte im Netzwerk verschaffen, über ihre Risikoprofile und ihr Verhalten bei der Interaktion mit anderen Netzwerkgeräten. Modernste Lösungen für die IoT-Sicherheit wie etwa Zingbox arbeiten mit maschinellem Lernen, um selbst zuvor unbekannte IoT-Geräte zu identifizieren und das Netzwerkverhalten von Schadsoftware am Muster zu erkennen, bevor tatsächlich ein Schaden entsteht.

Es ist wichtig, die Verbindungsprofile von IoT-Geräten zu kennen. IoT-Geräte mit direktem Internetzugang haben oft ein höheres Risiko, weil sich Exploits durch den Internetzugang schneller verbreiten können, als wenn ihnen nur Geräte im LAN zur Verfügung stehen. Und trotzdem haben auch IoT-Geräte, die nur im LAN vernetzt sind, ein erhöhtes Risiko: Sie wurden in der Annahme entwickelt, dass sie sicher hinter einer Firewall betrieben werden. Deshalb finden sich auf diesen Geräten öfter als bei SaaS-Ressourcen mit Internetzugang unverschlüsselt übertragene Daten, offene Ports und schwache Zugangsbeschränkungen. In gemischten Netzwerken sowohl für Benutzer als auch für derartige Geräte besteht das Risiko, dass IoT-Geräte von Benutzergeräten aus infiziert werden.

Wenn aber die IT diese Geräte kennt und sich ihres Risikoprofils bewusst ist, kann sie an Gegenmaßnahmen arbeiten.

Maßnahme 2: Spielen Sie auch bei Druckern und anderen leicht patchbaren Geräten Patches ein.

Unsere Untersuchungen zeigen, dass Drucker und Sicherheitskameras die häufigsten und gleichzeitig die für Angriffe anfälligsten Geräte in Unternehmensnetzwerken sind. Im Gesundheitswesen belegen Systeme zur Bildgebung und zur Patientenüberwachung die Spitzenplätze.

Wir empfehlen, nach der Inventarisierung der IoT-Geräte den Sicherheitszustand der zwei oder drei häufigsten Gerätetypen im Netzwerk zu prüfen und in Abstimmung mit den Herstellern eine Strategie zum Patchmanagement als Teil zukünftiger Routinearbeiten auszuarbeiten.

Maßnahme 3: Teilen Sie IoT-Geräte auf verschiedene VLANs auf.

Die Segmentierung von Netzwerken ist in den meisten Unternehmen gang und gäbe. Ihre Einrichtung ist zwar aufwendig, lohnt sich aber angesichts der Vorteile für die Sicherheit im gesamten Unternehmen. Ein ordentlich segmentiertes Netzwerk schränkt die Ausbreitung von Exploits im Netzwerk ein, verkleinert mögliche Angriffsflächen und minimiert die Konsequenzen eines Angriffs. Unternehmen können Netzwerksegmente auf der Grundlage von VLAN-Konfigurationen und Firewallrichtlinien konfigurieren. Der Zugang zu anderen Segmenten und die Nord-Süd-Kommunikation sollten strengstens durch die Netzwerkgrenzen, Switch-ACLs und Firewallrichtlinien überwacht werden. Damit entstehen streng voneinander getrennte Netzwerkabschnitte oder Sicherheitszonen mit jeweils eigenen IoT- oder IT-Ressourcen, die abhängig von ihrer Bedeutung für die Sicherheit und das Unternehmen geschützt werden.

Laut unseren Untersuchungen verwenden

72 Prozent

der VLANs im Gesundheitswesen keine sachgerechten Netzwerkpraktiken.

2019 gab es mehr als

dreimal

so viele VLANs als noch zwei Jahre zuvor.

Wir haben jedoch festgestellt, dass nur

3 Prozent

der VLANs im Gesundheitswesen ausschließlich IoMT-Geräte enthalten.

Intelligente Mikrosegmentierung anhand des Geräteprofils

Die Segmentierung von OT, IoT-Bürogeräten und IT-Ressourcen ist erst der Anfang. Unternehmen sollten auch eine Segmentierung anhand von Geräteeigenschaften und -profilen erwägen.

In der Praxis sind die besten Kriterien für die Segmentierung von Unternehmensnetzwerken der Gerätetyp, das Gefährdungspotenzial, Nutzungsprofile und andere Geräteeigenschaften.

Gartner hat 2018 in einem Bericht prognostiziert, dass innerhalb der nächsten zwei Jahre über 60 Prozent der IoT-Geräte in Unternehmensinfrastrukturen virtuell segmentiert sein würden.[3] Zwar steigt die Zahl der nach IoT/IT segmentierten Netzwerke, aber um die Vorteile einer Mikrosegmentierung voll auszuschöpfen, müssen Unternehmen Lösungen einsetzen, die Gerätetypen und ihr charakteristisches Netzwerkverhalten identifizieren können.

Ein Beispiel aus dem Gesundheitswesen

In einer typischen Einrichtung des Gesundheitswesens gibt es kritische medizinische IoT-Systeme, allgemeine nicht medizinische IoT-Geräte und IT-Geräte. In einem auf Sicherheit konzipierten Netzwerk befinden sich die kritischen medizinischen IoT-Systeme in isolierten Netzwerksegmenten.

Parallel zur Segmentierung anhand ihrer Identität können die IoT-Geräte zusätzlich nach Sicherheitsebene segmentiert werden, um beispielsweise Geräte mit Agenten für Endpunktsicherheit von Geräten ohne solche Agenten oder Geräte mit veralteten Betriebssystemen von solchen mit aktuellen Patches zu trennen. Auch die Bereitstellung von IoT-Geräten mit unterschiedlichen Sicherheitsfunktionen sollte sich an einem sorgfältig ausgearbeiteten Segmentierungsschema orientieren.

Für eine profilbasierte Mikrosegmentierung müssen die Einrichtungen zuverlässige Verfahren zur Geräteidentifizierung mit fortlaufender Echtzeit-Geräteanalyse einsetzen. So beziehen sie in ihre Maßnahmen auch die sich ständig ändernde Situation bei Geräteschwachstellen, Risiken und andere Eigenschaften ein, die die Sicherheit ihrer IoT-Geräte beeinflussen.

3. „Predicts 2019: IoT Will Drive Profound Changes to Your Core Business Applications and IT Infrastructure“, Gartner, 13. Dezember 2018, https://www.gartner.com/en/documents/3895863/predicts-2019-iot-will-drive-profound-changes-to-your-co.

Maßnahme 4: Ermöglichen Sie eine aktive Überwachung.

Um Angriffe zuverlässig aufzudecken, muss eine Überwachungslösung skalierbar und permanent aktiv sein, alle Schwachstellen ermitteln und das Verhalten aller Geräte im Netzwerk analysieren können – und das alles in Echtzeit. Sicherheitslösungen für IoT-Geräte arbeiten in der Regel mit maschinellem Lernen und laufen in einer hoch skalierbaren Cloud-Architektur, damit sie lernen, Profile erstellen und die Sicherheitsteams bei Auffälligkeiten benachrichtigen können.

Im Gesundheitswesen sollte die Medizintechnik mit der IT zusammenarbeiten, um Richtlinien für Best Practices für die sichere Verwaltung medizinischer IoT-Geräte zu definieren. Da immer mehr Geräte mit nicht mehr unterstützten Betriebssystemen arbeiten, müssen Einrichtungen des Gesundheitswesens dafür sorgen, diese Empfehlungen so bald wie möglich anzuwenden, um die Verwaltung und die Sicherheit ihrer medizinischen IoT-Ressourcen zu unterstützen.

Wir haben das Risiko für 1,2 Millionen IoT-Geräte in Unternehmen und Gesundheitseinrichtungen untersucht (siehe Abbildung 8). Ganze 57 Prozent der IoT-Geräte sind anfällig für mittelschwere und schwere Angriffe und damit leichte Beute für Angreifer.

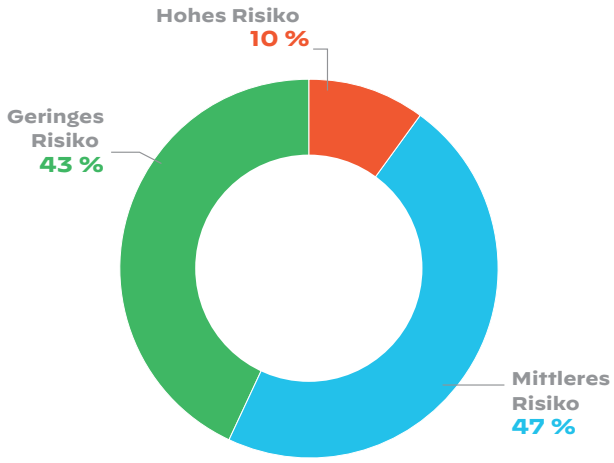


Abbildung 8: Risikoverteilung über 1,2 Millionen Geräte

Best Practices beim Risikomanagement für IoT-Geräte

Das „Common Vulnerability Scoring System“ (CVSS) ist ein in der Branche etabliertes System, das dem Schweregrad der Geräteschwachstellen einen Zahlenwert zuweist. An diesem Zahlenwert können Unternehmen ihr Risikoniveau ablesen und dementsprechend ihr Schwachstellenmanagement bewerten und priorisieren:

Hohes Risiko

Bei Geräten mit hohem Risiko ist oft sofortiges Handeln erforderlich. Solche Dringlichkeit besteht, wenn Sicherheitslücken festgestellt werden oder kritische Patches fehlen, ohne die die Geräte äußerst anfällig für Angriffe sind. Ein hohes Risiko besteht meist bei einem CVSS-Wert von 9 bis 10.

Mittleres Risiko

Die meisten IoT-Geräte fallen in diese Kategorie. Sie werden nicht sorgfältig gewartet, haben oft nicht den neuesten Patch, haben einen schwachen Passwortschutz und verwenden nicht mehr unterstützte Betriebssysteme. Außerdem laufen darauf oft nicht zugelassene Anwendungen, und wenn ein Webbrowser installiert ist, könnte dieser Verbindungen zu riskanten oder schädlichen Websites herstellen. Ein mittleres Risiko besteht meist bei CVSS-Werten zwischen 4 und 8,9.

Niedriges Risiko

Ein niedriges Risiko besteht bei Geräten, für die weder Echtzeit-Sicherheitswarnungen noch Anzeichen für Verstöße gegen die Unternehmensrichtlinien vorliegen. Wenn auf einem solchen Gerät Schwachstellen vorhanden sind, liegt der CVSS-Wert in der Regel unter 4.

Perfektionieren Sie Ihre IoT-Strategie

Best Practice 1: Gehen Sie die Aufgabe ganzheitlich an und koordinieren Sie den gesamten Lebenszyklus der IoT-Geräte.

Den gesamten Lebenszyklus von IoT-Geräten zu begleiten, ist eine neue Herausforderung für Unternehmen. Zu einer ganzheitlichen Herangehensweise gehören sechs Schritte:

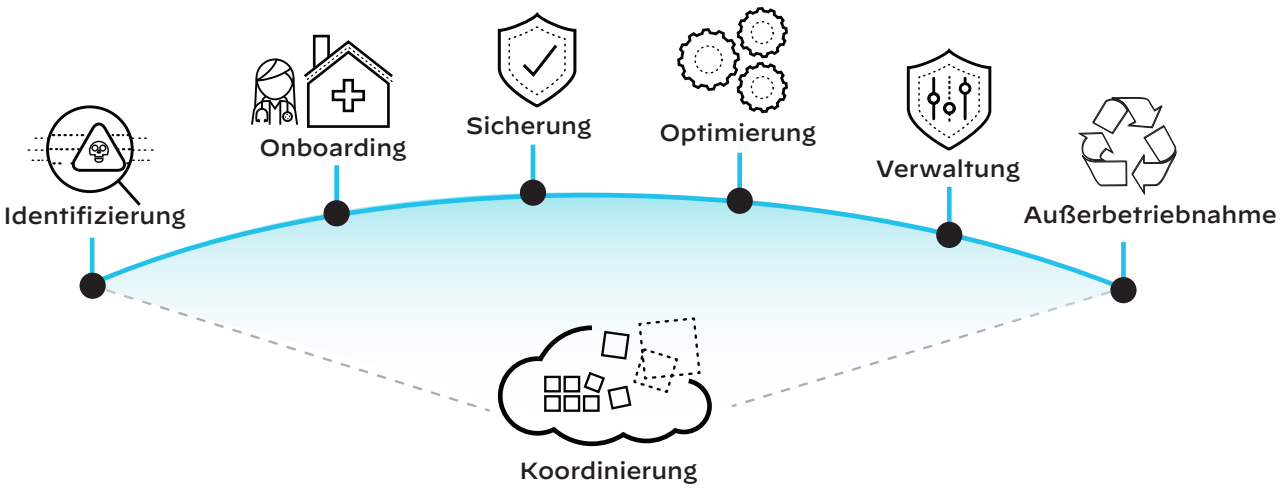


Abbildung 9: Der IoT-Lebenszyklus

1. **Identifizierung:** Lassen Sie sich immer benachrichtigen, sobald ein neues Gerät mit dem Netzwerk verbunden wird. Identifizieren Sie das Gerät, seine Kategorie, sein Risikoprofil und seine Nutzungsdaten.
2. **Onboarding:** lDie meisten Netzwerke sind so eingerichtet, dass das Onboarding von IT-Geräten dynamisch über die Netzwerkzugriffskontrolle (Network Access Control, NAC) abläuft. Für IoT-Ressourcen steht diese Funktion jedoch nicht unbedingt zur Verfügung, und das manuelle Onboarding von IoT-Geräten ist nicht einfach. Heute gibt es verschiedene Lösungen für die IoT-Sicherheit, die NAC und Next-Generation-Firewalls integrieren, sodass beim Onboarding und bei der Netzwerksegmentierung die Identität eines Geräts, sein Zweck und sein Risikoprofil berücksichtigt werden.
3. **Sicherung:** Ohne Schutz sind IoT-Geräte mit Internetverbindung ein hohes Risiko für jedes Unternehmen. Herkömmliche EDR-Lösungen (Endpoint Detection and Response) können diese Ressourcen nicht schützen, da sie mit Softwareagenten arbeiten. IoT-Sicherheitslösungen überwachen die identifizierten IoT-Geräte in Echtzeit anhand des Datenverkehrs im Netzwerk. Über Benachrichtigungen und Produktintegrationen ermöglichen sie die Sicherung oder die Quarantäne von Geräten.
4. **Optimierung:** Bei kostspieligen IoT-Ressourcen wie etwa Bildgebungssystemen in Krankenhäusern liefern ausführliche Statistiken zur Gerätenutzung wichtige Kenndaten für die Kapitalplanung und die Ressourcenoptimierung.
5. **Verwaltung:** Unternehmen benötigen für den Umgang mit dem Risiko durch IoT-Geräte zwingend Überwachung, Berichte und Warnmeldungen in Echtzeit.
6. **Außerbetriebnahme:** In vielen Fällen sind auf den Geräten personenbezogene und vertrauliche Daten gespeichert, für die bestimmte Complianceanforderungen gelten. Die Außerbetriebnahme solcher Ressourcen muss sorgfältig geplant und durch Audits begleitet werden.

Best Practice 2: Weiten Sie die Sicherheitsmaßnahmen durch Produktintegrationen auf alle IoT-Geräte aus.

IT-Netzwerke in Unternehmen sind mit modernsten Systemen für die IT-Sicherheit ausgestattet, darunter Next-Generation-Firewalls, NAC und SOAR-Lösungen (Security Orchestration, Automation and Response). Allerdings wurden die meisten dieser Produkte für die Überwachung und Steuerung von Servern, Laptops und Mobilgeräten konzipiert – IoT-Geräte fallen vollkommen aus ihrem Blickfeld, weil diese Geräte oft mit speziellen oder veralteten Betriebssystemversionen arbeiten und keine Agenten oder andere Funktionen des IT-Managements unterstützen.

Ohne Kontextinformationen ordnen Sicherheitslösungen IoT-Geräte oft falsch ein. Die richtige Klassifizierung von IoT-Geräten gewährleistet, dass sie ausschließlich Zugriff auf benötigte Ressourcen erhalten und den richtigen Netzwerksegmenten zugewiesen werden. Das senkt das Bedrohungsrisiko für andere Ressourcen und Netzwerke. IoT-Sicherheitsprodukte liefern den benötigten Kontext, sodass die IT diese Informationen über Produktintegrationen an die eingesetzten Sicherheitslösungen weiterleiten kann.

Folgende Produktkategorien kommen für eine Integration in Frage:

- Systeme zum Asset-Management und zum computergestützten Instandhaltungsmanagement (CMMS)
- SIEM-Lösungen (Security Information and Event Management)
- Sicherheitsorchestrierung, -automatisierung und -reaktion (SOAR)
- Next-Generation-Firewalls (NGFW)
- Netzwerkzugriffskontrolle (NAC)
- Lösungen zum WLAN-/Netzwerkmanagement

Über uns

Palo Alto Networks

In allen Branchen gibt es mittlerweile Milliarden von Onlinegeräten. Doch leider geht das Versprechen von Innovation und digitalem Wandel einher mit vielfältigen Problemen: Transparenz, Onboarding, Sicherheitslücken, Betriebsunterbrechungen, geschäftliche Nachteile, laufendes Management, Compliance und selbst Upgrades und die Außerbetriebnahme dieser Geräte sind betroffen. Um genau diese Probleme zu lösen, wurde Zingbox gegründet. Das Unternehmen wurde im September 2019 von Palo Alto Networks übernommen.

Wir bei Palo Alto Networks wissen, dass ein völlig neuer Ansatz für die Handhabung und Koordinierung aller Phasen des Lebenszyklus von IoT-Geräten erforderlich ist, damit Sie uneingeschränkt von sämtlichen Vorteilen dieser Geräte profitieren können. Wir wissen, wie wichtig traditionelle Best Practices der IT sind und welchen geschäftlichen Nutzen die OT haben kann. Damit das IoT wie gewünscht funktioniert, braucht es die einzigartige Kombination aus IT und OT, die wir bieten. Unsere Lösung ist schlank, cloudgestützt, arbeitet ohne Clients und ist einzigartig. Doch diese Merkmale sind nicht einfach nur die Vorteile unserer Lösung – sie sind die Prinzipien, die ihr zugrunde liegen.

Unit 42

Unit 42, das weltweit agierende Bedrohungsanalyse-Team von Palo Alto Networks, ist eine anerkannte Instanz für Cyberbedrohungen und wird häufig von Unternehmen und Regierungsbehörden auf der ganzen Welt zurate gezogen. Unsere Analysten sind spezialisiert auf die Suche nach und die Erfassung von noch unbekannten Bedrohungen sowie die Code-Analyse für das komplette Reverse-Engineering von Malware. Dieses Know-how ist die Grundlage für unsere erstklassigen und fundierten Untersuchungen der Tools, Vorgehensweisen und Verfahren, mit denen Hacker Unternehmen angreifen. Wir wollen, wo immer möglich, den Kontext liefern und genau erklären, wie ein Angriff abgelaufen ist, wer dahinter steht und warum. Diese Einblicke in Bedrohungen ermöglichen Unternehmen in aller Welt, sich wirkungsvoll zu verteidigen.

Methodik

Dieser Bericht zu IoT-Bedrohungen wurde vom Zingbox-Team in Zusammenarbeit mit Unit 42 erstellt. Die Daten in diesem Bericht stammen aus einer zweijährigen Auswertung von hunderten Kunden und über 1,2 Millionen IoT-Geräten in den Jahren 2018 und 2019. Die Daten wurden von Zingbox-Installationen an mehreren tausend Standorten von Unternehmen und Gesundheitseinrichtungen in den USA gesammelt. Diese beiden Firmenkategorien sind repräsentativ für die IoT-Nutzung in kritischen Infrastrukturen und geschäftskritischen Anwendungen. Unser Bericht verwendet Daten aus echten Installationen:

Analysierte Geräte:

1.272.000

Analysierte Netzwerksitzungen:

73,2 Milliarden

Analysierte Gerätetypen:

8.355

Oval Tower, De Entrée 99-197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de

2020-unit42-iot-threat-report-030620-de