Cyber-Pandemie

Hackerangriffe im Gesundheitswesen

panda

Die Cyber-Pandemie

In keinem anderen Wirtschaftszweig steht das Wohl des Menschen mehr im Mittelpunkt als im Gesundheitswesen. Auch in Konfliktsituationen werden Patienten respektiert und bestmöglich geschützt. Deshalb ist es schwer vorstellbar, dass jemand vorhaben könnte, das öffentliche Ansehen der Gesundheitsindustrie zu beschädigen oder gar vorsätzlich gezielte Cyberattacken zu starten.

Geld regiert die Welt, ohne Rücksicht auf gesellschaftliche Schichten, Bedingungen oder Bereiche zu nehmen. Geld ist daher auch die größte Motivation für Cyberkriminelle, die im Gesundheitswesen eine wichtige Ressource für ihre kriminellen Machenschaften gefunden haben.

Der Gesundheitssektor konzentriert sich auf seine Kernaufgaben, was wahrscheinlich der Grund dafür ist, dass die IT-Sicherheit jahrelang vernachlässigt wurde. Wir sehen uns zunehmend konfrontiert mit fortschrittlichen (medizinischen) Technologien bei gleichzeitig mangelnder IT-Sicherheit und das ist äußerst beunruhigend.

Erpressersoftware ist heute eine der am weitesten verbreiteten Bedrohungen und ein Beleg dafür, dass Geld die Hauptmotivation für Cyberkriminelle ist. Ransomware ist die perfekte Waffe, um ein Opfer anzugreifen, das wertvolle Informationen besitzt und bereit ist, Lösegeld für die Rückgabe der Daten zu zahlen.

Wir haben schon verschiedene Cyberangriffe erlebt, die speziell für bestimmte Branchen entwickelt wurden. In der Tat ist in gewissen Wirtschaftszweigen, wie zum Beispiel im Finanzsektor, das Interesse eines Hackers mehr als offensichtlich, nämlich Bankkonten zu leeren.

Andere Sektoren sind vielleicht nicht direkt vom Gelddiebstahl betroffen, doch das Endziel ist immer noch sehr klar. Wie im Whitepaper „Die Hotel Hijacker“ dokumentiert, gab es seit 2015 vermehrt Cyberattacken auf Hotels. Cyberkriminelle infizierten dabei vorzugsweise POS-Terminals, weil sie es auf die Kreditkarteninformationen der Hotelkunden abgesehen hatten.

Im Gesundheitssektor ist das Motiv dagegen nicht so offensichtlich. In vielen Ländern ist es nicht üblich, dass Patienten für Dienstleistungen mit Kreditkarte bezahlen, da gesetzliche oder private Krankenversicherungen dafür aufkommen. Trotzdem werden Krankenhäuser, Kliniken, Labore und alle Arten von Gesundheitszentren immer öfter Opfer von Datendiebstahl.

Warum ist der Gesundheitssektor Ziel der Cyber-kriminellen?

Nach Angaben des Amtes für Bürgerrechte der Vereinigten Staaten **gab es 2015 etwa 253 Sicherheitslücken in Einrichtungen des Gesundheitswesens; dabei wurden 112 Millionen Datensätze gestohlen. Laut IBM erlebte diese Branche 2015 mehr Angriffe als jede andere.**

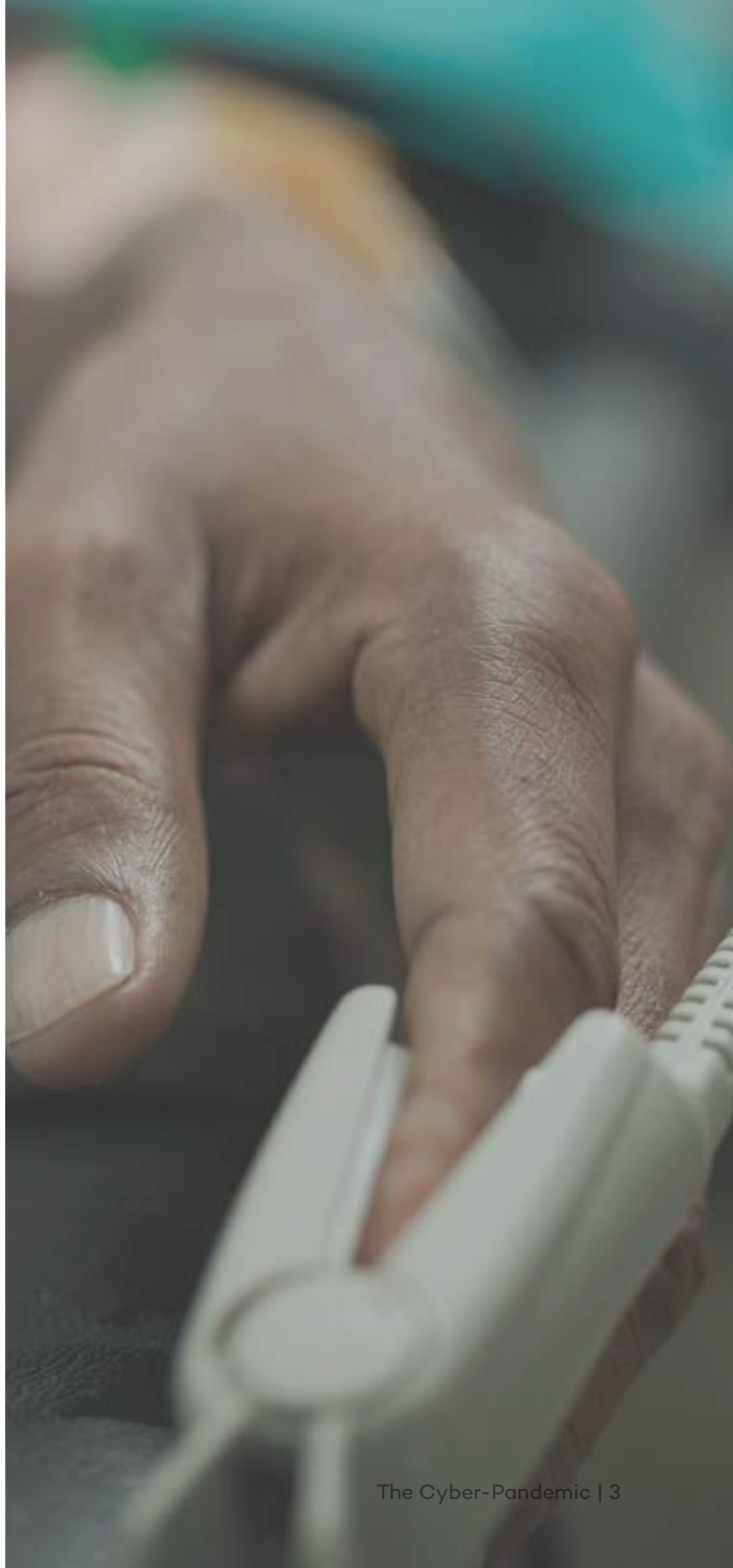
Das Gesundheitswesen befindet sich inmitten eines technologischen Umbruchs. Alle Informationen werden zunehmend elektronisch gespeichert, was zweifellos sowohl für die Patienten als auch für das Pflegepersonal von Vorteil ist. Die Daten sind in einem Netzwerk verfügbar und können im Falle von Veränderungen, beispielsweise bei Arztwechsel, problemlos abgerufen werden. Dieser Vorteil beschert der Gesundheitsindustrie jedoch auch ein ernsthaftes Sicherheitsproblem. Medizinische Daten sind sehr wertvoll und streng vertraulich, daher kann derjenige, der diese Daten kontrolliert, ein Vermögen damit machen.

In einigen Ländern kann man diese gestohlenen Informationen verkaufen. Es gibt verschiedene Unternehmen, die an dieser Art von Daten interessiert sind, von Forschungszentren bis hin zu Versicherungsunternehmen. Natürlich gibt es auch den Schwarzmarkt, auf dem Patientendaten wertvoller als Kreditkarteninformationen sein können.

Krankenakten enthalten viele persönliche Informationen, die als Generalschlüssel für zukünftige gezielte Angriffe genutzt werden könnten. Denken Sie nur an Menschen in Machtpositionen, die sehr darauf bedacht sind, ihre Privatsphäre zu schützen, und deshalb auch keine persönlichen Informationen in sozialen Netzwerken preisgeben. Selbst diejenigen, die besonders vorsichtig sind, können nicht verhindern, dass medizinische Zentren ihre Krankenakten aufbewahren. Wenn diese vertraulichen Informationen in die falschen Hände geraten, werden die persönlichen Daten nicht länger privat sein.

Ein weiteres Beispiel könnte der Zugriff auf vertrauliche Daten von pharmazeutischen Studien sein. Mitbewerber wären bereit, große Summen zu zahlen für die Chance, dem Konkurrenten ein Patent zu stehlen. Der Zugang zu den Krankenakten eines praktischen Arztes könnte genutzt werden, um unerlaubt Medikamente zu verschreiben.

Krankengeschichten, Testergebnisse, E-Mail-Adressen, Passwörter, Sozialversicherungsnummern, vertrauliche Mitarbeiter-, Patienten- und Firmendaten: **All diese Informationen sind wertvoll und werden mithilfe neuester Technologien gespeichert. Das Problem ist, dass sie mit Sicherheitssystemen geschützt werden, die meist veraltet sind.**



Erfolgreiche Angriffe im Gesundheitswesen

Amerikanisches Rotes Kreuz

Früher war der IT-Schutz einfacher. Fast alle Angriffsmethoden erforderten physischen Zugriff auf Server oder mussten zumindest innerhalb eines Unternehmens ausgeführt werden. Im Jahr 2006 stahl ein Angestellter des Amerikanischen Roten Kreuzes in St. Louis die Identitäten und Daten von drei Blutspendern. Die Folgen hätten weitaus gravierender sein können, denn dieser Angestellte hatte Zugriff auf die Daten von mehr als einer Million Spendern.

Zugriff auf mehr als eine Million Spenderdaten

Temple Street Children's University Hospital

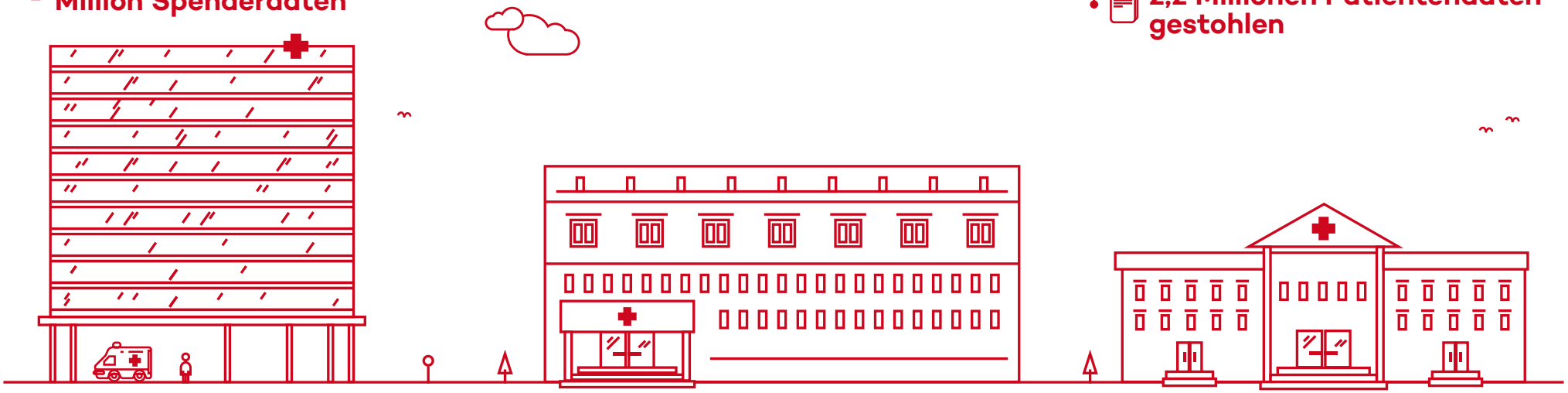
Ein Jahr später wurden zwei Server aus dem Temple Street Children's University Hospital in Irland gestohlen. Auf den Servern waren die Daten von fast einer Million Patienten gespeichert, einschließlich Namen, Geburtsdaten und Gründe für die Aufnahme.

Daten von fast 1 Million Patienten gestohlen

The University of Utah Hospitals & Clinics

2008 gab die University of Utah Hospitals & Clinics bekannt, dass die Daten von 2,2 Millionen Patienten gestohlen wurden. Die Informationen waren auf Backup-Bändern gespeichert, die der Angestellte einer vom Krankenhaus beauftragten IT-Firma in seinem Auto gelassen hatte. In diesem Fall hatte der Angestellte die Vorschriften für den Transport von Daten nicht eingehalten und so wurden die privaten Daten von Millionen Menschen kompromittiert.

2,2 Millionen Patientendaten gestohlen



Bisher haben wir nur Einzelfälle aufgezeigt und keine groß angelegten Cyberangriffe. Doch im Laufe der Jahre hat sich die Bedrohungssituation drastisch verändert. **Laut einer Studie des Ponemon Institutes haben die Angriffe im Gesundheitssektor in den vergangenen fünf Jahren um 125 Prozent zugenommen. Cyberattacken sind zur Hauptursache für Datenverlust geworden.**

Diese Situation ist besorgniserregend, insbesondere da 91 Prozent der in der Studie überprüften Unternehmen in den vergangenen zwei Jahren mindestens einen Angriff erlitten haben, der zu Datenverlust führte. 40 Prozent bestätigten sogar fünf oder mehr Fälle von Datendiebstahl im selben Zeitraum.

Anthem Insurance Company

Eine der weltweit größten Attacken im Gesundheitswesen ereignete sich im Februar 2015. Beim Angriff auf das zweitgrößte Versicherungsunternehmen in den Vereinigten Staaten, Anthem, wurden 80 Millionen Kundendatensätze gestohlen. Äußerst sensible Daten wie zum Beispiel Sozialversicherungsnummern gingen verloren.

Neben dem Datendiebstahl und dem möglichen Verkauf dieser Informationen spielen auch Ransomware-Angriffe eine wichtige Rolle im Gesundheitssektor. Einrichtungen wie Krankenhäuser, Pharma- und Versicherungsunternehmen besitzen eine so große Menge an wertvollen Informationen, dass sie besonders häufig von Ransomware-Attacken betroffen sind. Dabei hacken sich Cyberkriminelle in die digitalen Systeme der Unternehmen ein, um wichtige Daten zu „kidnappen“ und Lösegeld für deren Herausgabe zu verlangen.

Zugriff auf 80 Millionen Kundendatensätze

Hollywood Presbyterian Medical Center

Im Februar 2016 gab das Hollywood Presbyterian Medical Center in Los Angeles einen “internen Notfall” bekannt. Die Angestellten hatten keinen Zugriff mehr auf digitale Patientenakten, E-Mails und andere IT-Systeme. Infolgedessen konnten einige Patienten nicht behandelt werden und mussten an andere Krankenhäuser überwiesen werden. Die Cyberkriminellen verlangten ein Lösegeld in Höhe von 3,7 Millionen Dollar. Der Geschäftsführer des Krankenhauses einigte sich schließlich mit den Hackern auf die Zahlung von rund 17.000 Dollar, um die entwendeten Dateien zurückzuerhalten.

3,7 Millionen Dollar Lösegeld verlangt

Baltimore MedStar Health

Im März bestätigte das in Baltimore ansässige Unternehmen MedStar Health, dass einige der Krankenhaussysteme aufgrund eines Angriffes, der dem auf das Hollywood Presbyterian Medical Center glich, vom Netz genommen werden mussten.

Klinik musste auf IT-Systeme verzichten

Henderson Methodist Hospital

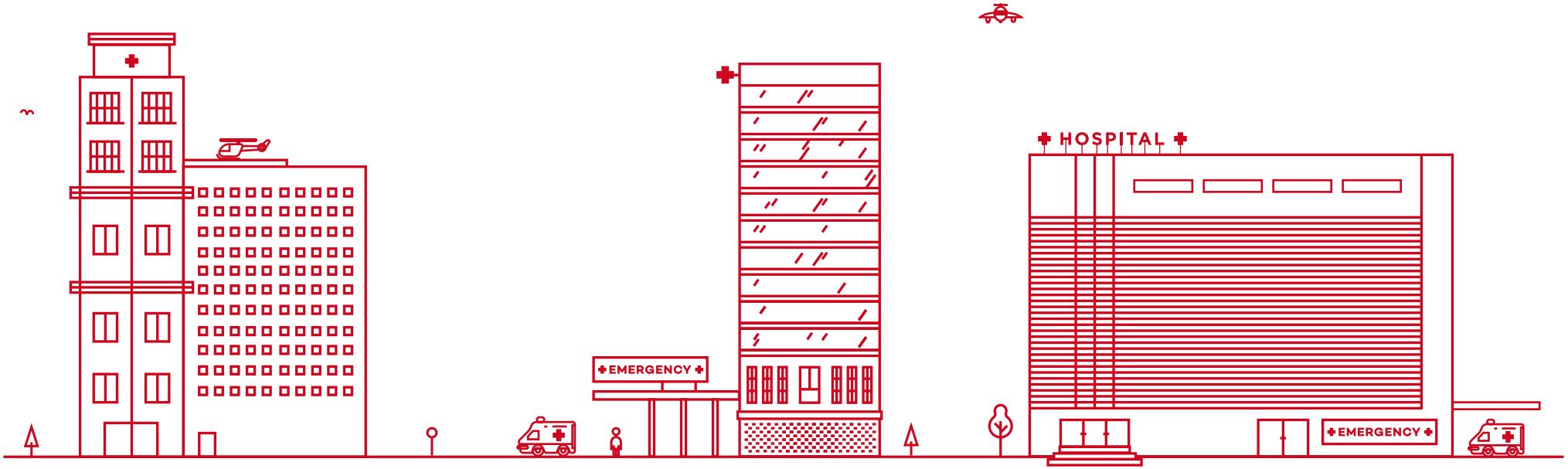
Das Methodist Hospital in Henderson, Kentucky, war ein weiteres Opfer. In diesem Fall wurde ein Lösegeld in Höhe von 17.000 US-Dollar gezahlt. Diese Zahl wurde jedoch nicht bestätigt und so wird vermutet, dass die Summe weitaus höher gewesen sein könnte.

Mehrere Tausend Dollar Lösegeld gezahlt

Prime Healthcare Management

Der große US-amerikanische Anbieter Prime Healthcare Management, Inc. wurde ebenfalls Opfer von Cyberattacken. Zwei seiner Krankenhäuser wurden von Cyberkriminellen angegriffen (Chinese Valley Medical Center und Desert Valley Hospital). Von dieser Attacke, die zu Netzwerkabschaltungen führte, waren auch viele andere Einrichtungen betroffen. In diesem Fall zahlte das Unternehmen kein Lösegeld.

Netzwerkabschaltungen in Kliniken



Deutsche Krankenhäuser betroffen

Nicht nur amerikanische Krankenhäuser sind Ziele von Hackerangriffen. Auch mindestens sechs deutsche Kliniken wurden 2015 und 2016 Opfer von Ransomware-Angriffen, wie zum Beispiel das Lukaskrankenhaus in Neuss und das Klinikum Arnsberg. Keines der Krankenhäuser zahlte das Lösegeld.

Mindestens 6 deutsche Kliniken angegriffen

Kansas Heart Hospital

Es sollte beachtet werden, dass **die Zahlung des Lösegeldes keinesfalls die Rückgabe der Daten garantiert**. Ein Beispiel dafür ist der Ransomware-Angriff auf das Kansas Heart Hospital im Mai 2016. Der Leiter des Krankenhauses entschied sich für die Zahlung des Lösegeldes. Doch die Erpresser erkannten den Wert der Daten und forderten eine zweite Zahlung für die vollständige Wiederherstellung der Daten. Das Krankenhaus beschloss, der zweiten Lösegeldforderung nicht nachzukommen.

Die Hacker verlangten eine zweite Lösegeldzahlung

Im Medizinbereich gilt das Sprichwort **“Vorbeugen ist besser als Heilen”**. Nach all den Vorfällen im Gesundheitswesen sollten die Verantwortlichen diesen eigenen Ratschlag ebenfalls befolgen.

Science Fiction wird Realität

Wie die genannten Beispiele zeigen, können Cyberangriffe ein Krankenhaus komplett lahmlegen, indem der Zugriff auf Dateien verweigert wird, Tausende von Datenprotokollen gestohlen und sensible Patienteninformationen entwendet werden.

Doch es gibt Hackerattacken, die uns alle noch viel direkter betreffen können: Nahezu alle medizinischen Geräte (Herzschrittmacher, Röntgengeräte, Infusionspumpen, Beatmungsgeräte usw.) sind heutzutage mit einem digitalen Netzwerk verbunden. Es ist durchaus möglich, dass diese medizinischen Geräte gehackt werden.

2013 offenbarte der ehemalige US-Vizepräsident Dick Cheney, dass seine Ärzte die drahtlose Kommunikation zu seinem Herzschrittmacher deaktiviert hatten, da die Möglichkeit einer Attacke per Fernzugriff bestand.

Ein Jahr zuvor demonstrierte der neuseeländische Hacker Barnaby Jack den Teilnehmern einer Sicherheitskonferenz, wie ein Herzschrittmacher aus der Ferne gehackt werden und so einen lebensbedrohlichen Stromschlag auslösen kann. Barnaby entwickelte eine Angriffsmethode, die alle Herzschrittmacher in einem 15-Meter-Radius beeinflusst.

Er zeigte ebenfalls, wie eine häufig von Diabetes-Patienten genutzte tragbare Insulinpumpe per Fernzugriff so modifiziert werden kann, dass es möglich ist, in alle Geräte im Umkreis von 90 Metern eine tödliche Dosis Insulin einzuspeisen.

Jack wollte zudem zeigen, wie man künstliche Herzen hacken kann. Doch er starb eine Woche vor seiner angekündigten Demonstration. Auf der Black Hat Conference 2013 hätte er demonstriert, wie man den Rhythmus dieser Implantate in nur wenigen Augenblicken verändern kann.

Herzschrittmacher, Insulinpumpen, Beatmungsmaschinen... medizinische Geräte, die häufig ungeschützt sind.

Ein Herzschrittmacher wurde gehackt... und konnte so einen tödlichen Stromschlag auslösen.

Insulinpumpen wurden so modifiziert... dass sie eine tödliche Dosis Insulin verabreichen können.

Auch der bekannte Hacker Billy Rios hatte es sich zur Aufgabe gemacht, Schwachstellen in medizinischen Geräten zu enthüllen. Während eines zweiwöchigen Krankenhausaufenthalts im Stanford Hospital (USA) stellte Rios fest, dass sein Bett mit einem Computer verbunden war. Es gab automatische Gurte, die seine Füße anhoben, sowie eine Infusionspumpe, die ihm täglich seine Medikamente injizierte. Ohne sein Zimmer zu verlassen, entdeckte er bis zu 16 Netzwerke und acht Wi-Fi-Hotspots.

Nach einigen Tagen Bettruhe stand er auf, um sich auf dem Flur die Beine zu vertreten. Dabei entdeckte er einen computergesteuerten Medikamentendosierer. Der für die Verteilung aller Medikamente Verantwortliche war hier also tatsächlich ein Computer, den Ärzte und Krankenschwestern mithilfe einer codierten Kennkarte steuerten. Richard hatte bereits vor dem Entdecken des Gerätes festgestellt, dass dieses System eine Schwachstelle hatte: ein in den Quellcode des Programmes eingebettetes Passwort (fest kodiertes Passwort), das anderen Personen ermöglichte, mit dem Arzneimittelspender „herumzuspielen".

Zusammen mit seinem Partner Terry McCorkle entdeckte Rios danach mehr als 300 gefährdete Geräte in rund 40 verschiedenen Unternehmen im Gesundheitswesen. Die Namen der betroffenen Firmen wurden nie veröffentlicht, doch der Hacker ist sich sicher, dass diese Schwachstellen auch heute noch existieren.

Um die Gefahren aufzuzeigen, die von diesen Sicherheitslücken ausgehen können, **demonstrierte Richard Rios, wie einfach es ist, die Medikamentenpumpen in Krankenhäusern auf der ganzen Welt per Fernzugriff zu manipulieren.** Er hackte mehrere dieser Geräte, um die Medikamentenmenge so anzuheben, dass sie tödlich war. Rios warnte davor, dass dies auf mehr als 400.000 Geräten weltweit möglich sei, solange die Schwachstellen nicht behoben werden.

Fast zeitgleich begannen mehrere Analysten bei TrapX Security in San Mateo, Kalifornien, gefährdete Geräte in über 60 Krankenhäusern aufzuspüren. Sie infizierten Hunderte von Geräten mit einem Programm, das einen Teil des ursprünglichen Betriebssystems der betreffenden Apparate ersetzte. Die infizierten Geräte blieben dabei voll funktionstüchtig, sodass niemand das Problem bemerkte.

TrapX konnte sechs Monate lang alle Aktivitäten im Netzwerk der Krankenhäuser überwachen. Sie hatten Zugriff auf Röntgengeräte, Pumpen, Blutanalysegeräte und auf die Computer, die vom medizinischen Team genutzt wurden. Auf vielen dieser Geräte waren Betriebssysteme installiert, die nicht länger vom Hersteller unterstützt werden, wie zum Beispiel Windows XP oder Windows 2000. Diese waren extrem anfällig. Die Tatsache, dass der Virenschutz der bei fast allen betroffenen Krankenhäusern die TrapX-Infektion nicht entdeckt hatte, legt nahe, dass die Geräte nicht ausreichend geschützt waren. Sie blieben infiziert, bis TrapX Security selbst Alarm schlug.

Wie hätten diese Angriffe vermieden werden können?

Cyberkriminelle hacken Unternehmen im Gesundheitswesen, um sensible Daten wie Krankengeschichten, pharmazeutische Studien oder Informationen über versicherte Personen zu stehlen. Oder sie legen mithilfe von Ransomware ganze Krankenhäuser lahm, um Geld zu erpressen.

Die Verhinderung solcher Attacken ist keine leichte Aufgabe. Wir empfehlen, eine ganze Reihe von Vorsichtsmaßnahmen zu ergreifen und dabei jeweils spezielle Ressourcen und Sicherheitsrichtlinien zu erstellen, um Geräte, Daten und Menschen bestmöglich zu schützen.

Die dringendste Empfehlung ist verhältnismäßig einfach umzusetzen, jedoch äußerst wichtig und effektiv: Verwenden Sie eine IT-Sicherheitslösung mit erweiterten Schutzfähigkeiten, die mögliche Bedrohungen erkennen und beseitigen kann.

Eines haben die meisten dieser Cyberangriffe gemeinsam: Sie nutzen die fehlende Kontrolle über die Vorgänge, die sich in den Computersystemen ereignen. Deshalb empfehlen wir Ihnen ein Sicherheitsmodell, das **alle Prozesse überwachen kann**, die auf einem Netzwerk und seinen Endgeräten laufen.

Dadurch können Sie jede Anomalie entdecken und handeln, bevor Schaden entsteht.

Darüber hinaus ist es absolut notwendig, alle Betriebssysteme und Programme stets auf dem neuesten Stand zu halten. Auf diese Weise werden mithilfe der Patches alle bekannten Sicherheitslücken geschlossen.

Panda bietet die passende Lösung

Um uns vor fortschrittlichen Bedrohungen und gezielten Angriffen zu schützen, benötigen wir ein System, das die Vertraulichkeit von Daten, den Schutz von sensiblen (Kunden-) Informationen und einzigartigem Firmenwissen gewährleistet.

Adaptive Defense 360 ist ein neu entwickeltes IT-Schutzsystem auf höchstem technischem Niveau, das erstmals Endpoint Protection (EPP) und Endpoint Detection and Response (EDR)-Fähigkeiten kombiniert.

Adaptive Defense 360 kann Malware und ungewöhnliches Verhalten erkennen, weil es alle laufenden und ausgeführten Prozesse klassifiziert. Dies können blacklist-basierte Anti-Malware-Systeme nicht.

Deshalb schützt es sowohl vor bekannter Malware als auch vor unbekannter Malware, wie Zero-Day-Bedrohungen, APTs (Advanced Persistent Threats) und direkten Angriffen.

Mit Adaptive Defense 360 wissen Sie immer, was mit jeder Ihrer Dateien und Prozesse geschieht.

Detaillierte Diagramme aller ausgeführten Aktionen geben einen klaren Überblick über alle Ereignisse, die im Netzwerk passieren. Zeitleisten und Heatmaps geben visuelle Informationen über die Herkunft der Malware-Verbindungen, wie diese ins System gelangt sind, welche Dateien sie erstellt haben oder erstellen wollten und vieles mehr.

Mit Adaptive Defense 360 lassen sich Schwachstellen leicht erkennen und beseitigen. Gleichzeitig verhindert es die Ausführung unerwünschter Prozesse (wie die Installation zusätzlicher Navigationsleisten, Adware, Add-ons usw.).

Weite Informationen unter: http://www.pandasecurity.com/germany/enterprise/solutions/adaptive-defense-360/

Adaptive Defense 360

Uneingeschränkte Transparenz, absolute Kontrolle

pandasecurity.com

panda

Weitere Informationen unter:

pandasecurity.com/germany/enterprise/solutions/adaptive-defense-360/

Rufen Sie uns an:

02065 961-200

Kontaktieren Sie uns per E-Mail:

vertrieb@de.pandasecurity.com

panda