IT-Defense 2018, München

Aufstand gegen IoT und Cloud

Auf der IT-Defense – der kleinen, aber feinen Jahreskonferenz des Heilbronner IT-Security-Beratungshauses Cirosec, die Ende Januar in München stattfand – stachen unter den zahlreichen spannenden Vorträgen drei besonders heraus: Mikko Hyppönen, Chef-Forscher bei F-Secure, warnte eindringlich vor Gefahren durch das IoT (Internet of Things); Security-Urgestein Marcus Ranum wetterte gegen die Cloud; und Pen-Testerin Paula Januszkiewicz demonstrierte in flottem Tempo die Angreifbarkeit Windows-basierter IT-Umgebungen.

Mikko Hyppönen, Chief Research Officer (CRO) des finnischen Online-Security-Anbieters F-Secure, zeichnete in seiner Keynote-Rede ein düsteres Bild der „nächsten Revolution" der IT: nämlich der IoT-Revolution, die dieser Tage auf die PC- und die Internet-Revolution folgt. Dank Internet-Revolution sind die Computer weltweit vernetzt, so der F-Secure-Mann, doch mit der IoT-Revolution gehe nun noch wesentlich mehr Equipment ans Netz: „Wenn etwas mit Strom läuft, geht es online."

Die Basis dafür bilden laut Hyppönen zwei Megatrends: Computer werden immer kleiner und – siehe Moore's Law – immer preiswerter. Das Problem: Heute ist uns bekannt, welche unserer Geräte online sind, künftig aber werden viele Devices ohne unser Wissen kommunizieren – und ohne dass wir es unterbinden können. „Die Hersteller wollen Daten sammeln", erklärt Hyppönen, denn schließlich habe man ihnen gesagt, Daten seien „das neue Öl". Und wenn der Chip, der Nutzungsdaten per BLE (Bluetooth Low Energy) und Co. ins Internet pumpt, nur zwei Cent koste, dann werde er eben verbaut. Solche Devices zu meiden ist laut dem Finnen langfristig keine Lösung: In fünf, zehn oder fünfzehn Jahren werde es gar keine Elektrogeräte ohne Netzanbindung mehr geben. Dies setzt die Devices dann allerdings sämtlichen Gefahren aus, die im Internet lauern: von Malware über Spionage-Tools bis hin zu Erpressung mittels Ransomware, Letzteres im Zusammenspiel mit Kryptowährungen. Eigentlich, so Hyppönen, sei die Blockchain (auf der Kryptowährungen beruhen) „eine der größten Innovationen des Jahrzehnts" und für zahlreiche Einsatzfälle nützlich. Jedoch: „Die Online-Kriminellen lieben Kryptowährungen, wie die Kriminellen in der realen Welt Bargeld lieben."

„Die Online-Kriminellen lieben Kryptowährungen, wie die Kriminellen in der realen Welt Bargeld lieben", so Mikko Hyppönen, CRO von F-Secure. Bild: Dr. Wilhelm Greiner

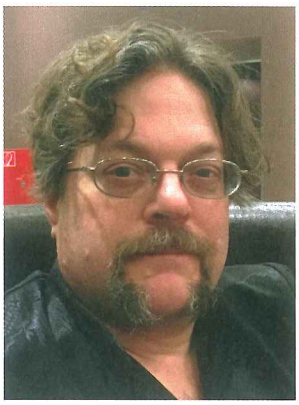
Der Security-Fachmann erläuterte, warum eine Währung wie Bitcoin, die dank Blockchain auf einem öffentlich einsehbaren Hauptbuch beruht, Anonymität für das Einsammeln von Lösegeldern bietet: „Die Russ… äh… die Kriminellen" (O-Ton Hyppönen), die hinter der Ransomware Petya stecken, haben die Lösegelder auf ein riesiges Netz von Bitcoin-Wallets verteilt und dann die Blockchain gewechselt: Nach dem Umtausch der Bitcoins in Moneros habe sich die Spur verloren.

Smart = angreifbar

„Wir verwandeln alles in smarte Geräte", resümierte Hyppönen und verwies auf eine seiner Aussagen, die man inzwischen auch als „Hypponen's Law" (ohne „ö", da englisch) kennt: „Wenn ein Gerät smart ist, dann ist es angreifbar." Als prominenten Beleg nannte er jenen Jeep Cherokee, den die beiden Hacker Miller und Valasek 2015 aus der Ferne übernahmen und dann fernsteuerten.

Hyppönen mahnte aber, sich nicht auf jene dramatische Szenarien zu konzentrieren, die der Security-Vordenker Bruce Schneier „Movie Plot Threats" (Bedrohungen wie aus einem Filmdrehbuch) nennt. Die Hauptgefahr sei nicht, dass ein Angreifer ein vernetztes Auto übernimmt und „über die Klippe steuert" – das sei für Cyberkriminelle kein valides Geschäftsmodell. Eine reale Gefahr vernetzter Fahrzeuge sei vielmehr zum Beispiel folgende: Autodiebe spüren nachts von der Straße aus mittels eines Sensors den funkbasierten Autoschlüssel des Opfers in dessen Haus auf; dann verstärken sie per Repeater dessen Funksignal, um das Fahrzeug zu öffnen und zu entführen. Das Auto werde dann mit allerlei Signalen protestieren, so Hyppönen, denn es erkenne nach wenigen Metern, dass der Schlüssel fehlt – aber den Dienst verweigern werde es nicht. Das sei für Autodiebe sehr reizvoll: Hacking erspart das Einschlagen einer Scheibe. Er riet, sich bei IoT-Gefahren stets zu vergegenwärtigen, wer tatsächlich der Gegner ist: eine kriminelle Bande, ein Wettbewerber, eine Regierungsbehörde…?

Zugleich warnte Hyppönen vor der sozialen Sprengkraft des IoT: Es werde „einen Aufstand der Menschen" gegen das Internet der Dinge geben. Damit meinte er allerdings keinen Krieg Mensch vs. Roboter wie in den Terminator-Filmen, sondern alltäglichen Protest. So berichtete er von Müllwagenfahrern, die die Füllstandsensoren „smarter" Mülltonnen demoliert hatten: Dank der Sensorik wurden die Tonnen



„Die Cloud beseitigt das Problem nicht, sie macht es nur schneller", warnt Security-Experte Marcus J. Ranum.
Bild: Dr. Wilhelm Greiner

nicht mehr regelmäßig jede Woche, sondern nur noch bei Bedarf – also seltener – geleert. Dies empfanden die Fahrer als existenzbedrohend und reagierten gewaltsam. Er forderte die Zuschauer auf, über den Tellerrand hinauszudenken: „Unser Job ist es nicht, die IT zu schützen, sondern die Gesellschaft zu schützen."

Cloud als Zeichen der Schwäche

Noch deutlichere Kritik am Status quo äußerte Security-Urgestein Marcus J. Ranum in seiner Keynote am zweiten IT-Defense-Tag. Seine Argumentation: Die Cloud ist nur deshalb eine Option, weil die Unternehmens-IT teuer und unsicher ist – und dies wiederum ist sie nur, weil man sie schlecht managt. Den Unternehmenslenkern warf er vor, nur auf's Geld zu schauen: Gemacht wird, was Einsparungen verspricht, selbst wenn es aus IT-Security-Sicht bedenklich ist, wie etwa die Public Cloud oder BYOD. Da IT-Sicherheit somit hochgradig von den Management-Kosten abhänge, sei der aktuelle Fokus auf Standards und Compliance – Stichwort: DSGVO – genau der falsche Weg: Man belaste eine Softwarelandschaft, deren Problem eh schon das Management ist, durch neue Management-Schichten und bekämpfe Komplexität mit noch mehr Komplexität. „Stattdessen sollten wir die IT vereinfachen", forderte er.

Für diese Vereinfachung sorge die Cloud nur scheinbar: „Die Cloud beseitigt das Problem nicht, sie macht es nur schneller", so Ranum. Über die großen Cloud-Provider schimpfte er: „Allein schon die Tatsache, dass sie einen (in die jeweils eigene Cloud-Umgebung, d.Red.) einsperren wollen, zeigt, dass sie keine guten Absichten haben. Es zeigt, dass sie einen in fünf bis zehn Jahren über den Tisch ziehen wollen." Doch auch an Unternehmens-IT-Organisationen teilte Ranum Ohrfeigen aus: „Sicherheit ist im Grunde eine Unterdisziplin des System- und Netzwerk-Managements. Wir (die IT-Security-Branche, d.Red.) existieren nur, weil die System- und Netzwerk-Manager versagt haben." Sein Lösungsvorschlag: der Wechsel zu zwingend vorgeschriebenen gestreamten Software-Updates; ein Whitelisting von Applikationen, Netzwerken und Speichern; sowie ein Fokus auf die aggregierten Management-Kosten.

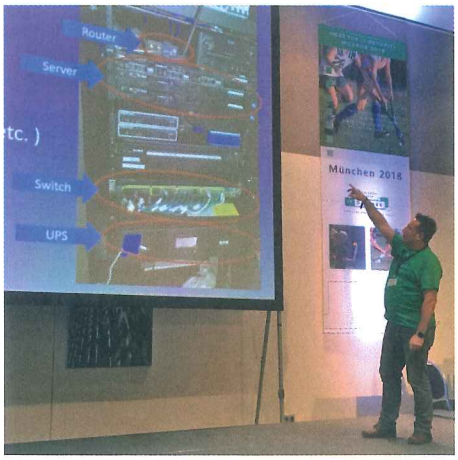
Denn um die Geschäftsführung davon zu überzeugen, statt in die Cloud in eine besser verwaltete Inhouse-IT zu investieren, müsse der IT-Leiter mittels geeigneter Metriken Vorher/Nachher-Vergleiche parat haben, zum Beispiel: „Wir hatten X Incidents pro Woche und haben die Maßnahme Y ergriffen. Dafür haben wir den Betrag X investiert, statt Y für das Incident-Management ausgeben zu müssen." Derlei Metriken seien die Grundvoraussetzung für das IT-Management und deshalb auch für IT-Sicherheit. Denn, so Ranums Fazit: „Unwissenheit ist teuer."

Angriffe im Detail

Der Reiz der IT-Defense liegt darin, dass sie den Bogen von High-Level-Keynotes (oder Gardinenpredigten wie im obigen Fall) bis hin zu technisch detaillierten Hacker-Vorträgen spannt. Die diesjährige Cirosec-Veranstaltung – mit etwas über 200 Besuchern wie immer ausgebucht – glänzte gleich mit mehreren spannenden Vorträgen.

So erklärte Sicherheitsexperte Stephan Gerling, wie man eine Millionen Euro teure Mega-Yacht hackt: Kommunikation wie die in der Seefahrt üblichen AIS-Signale (Automatic Identification System) zu fälschen ist laut Gerling „kein Hexenwerk". Im Detail schilderte er einen Angriff auf den Router eine Yacht, dessen in XML geschriebene Konfigurationsänderungen per FTP und somit unverschlüsselt übertragen wurden. User-Name und Passwort waren zudem – man errät es schon – hart codiert hinterlegt. Auf Gerlings Analyse hin wechselte der Hersteller von FTP zu SSH – behielt die hart codierte Authentifizierung aber bei. Gerlings Urteil: „Die maritime IT-Security ist noch recht am Anfang."

Der Hacker Starbug blickte auf 15 Jahre Überwindungsversuche von Biometrielösungen zurück, von der ersten Maus mit Fingerabdruckscanner über die aktuelle Gesichtsbiometrie mit 3D-Scanner und Infrarotlicht bsi zur Handvenenerkennung. Für „normale User", so Starbug, könne man Biometrie inzwischen verwenden, für Hochsicherheitsbereiche empfiehlt er sie nach wie vor nicht. Changhoon Yoon von der KAIST Universität in Korea warnte, dass SDN (Software-Defined Networking) aus Security-Sicht noch lange nicht unternehmenstauglich ist, während Co-



„Die maritime IT-Security ist noch recht am Anfang", so Yachten-Hacker Stephan Gerling.
Bild: Dr. Wilhelm Greiner

lin O'Flynn zeigte, wie leicht sich smarte Glühbirnen aus dem Hause Philipps kompromittieren lassen. Das Risiko: Die Kompromittierung kann sich Peer-to-Peer zwischen den Leuchtkörpern ausbreiten. So könnte ein Angreifer, der zehntausende ferngesteuerter Glühbirnen schnell ein-

und ausschaltet, eines Tages vielleicht sogar das Stromnetz destabilisieren.

Benjamin Kollenda und Philipp Koppe von der Ruhr-Universität Bochum erläuterten Angriffe auf Prozessor-Microcode – angesichts von Meltdown und Spectre ein brandheißes Thema. Das Grundproblem sei, dass moderne CPUs Update-fähig sind – diese Updates sich aber eben kompromittieren lassen, etwa mittels des von ihnen selbst entwickelten „Angry OS", erhältlich auf Github. Da die Software-Updates für Microkernel-Code nicht signiert sind, so die Forscher, werde jedes Update akzeptiert, sobald ein Hacker sich einmal Zugang verschafft hat. Dies ebne den Weg für Backdoors, die nur sehr schwer zu entdecken sind.

Das Highlight unter den Technikvorträgen war aber die Präsentation von Paula Januszkiewicz, CEO des Pen-Testing-Anbieters Cqure. Zunächst beschrieb sie, wie sie das Stereotyp der blonden, gutaussehenden Frau nutzt, um per Social Engineering in Unternehmen einzudringen (Tipp: immer zuletzt aus dem Fahrstuhl steigen, damit ein hilfsbereiter Herr die ID-kartengesicherte Tür aufhält). Anschließend diskutierte sie im Schnelldurchlauf die wichtigsten Bedrohungen der Unternehmens-IT. Problem Nummer eins, so die Expertin: „Wir haben einen jämmerlichen Umgang mit Passwörtern." Auch für diverse weitere Kernprobleme sind laut Januszkiewicz die Endanwender verantwortlich: Diese lassen ihre PCs unbeaufsichtigt und ungesichert zurück, nutzen unbekannte USB-Sticks (90 Prozent der Nutzer würden laut einer Umfrage einen fremden USB-Stick verwenden, wenn dieser das Unternehmenslogo trägt), sie fallen auf Phishing herein, vergessen Geräte in Taxis, nutzen fremde WLANs und geben ihre Passwörter an Dritte heraus.

Doch neben menschlichen gibt es auch technische Schwächen: So demonstrierte sie, wie man, einmal ins Unternehmensnetz eingedrungen, dank Kenntnis der Windows-Schwachstellen und passender Hacking-Tools mittels Privileg-Eskalation an die Admin-Passwörter gelangt. Laut Januszkiewicz' Angaben hat ihr Unternehmen inzwischen über 200 solcher Hacking-Tool entwickelt und auf dem Unternehmens-Blog bereitgestellt. Für das Auslesen des Admin-Passworts zum Beispiel nutze Cqure eine hauseigene Version des bekannten Hacking-Toolkits Mimikatz, die von Antivirenlösungen nicht erkannt werde.

Die Pen-Testerin riet dazu, neben Präventionsmaßnahmen wie laufender Schwachstellenermittlung und kontextbezogener Analyse auch den menschlichen Faktor zu berücksichtigen. Denn für das IT-Security-Fachpersonal seien Risiken eine Frage der Mathematik, für Endanwender aber eine Frage des Gefühls.

Diesem „menschlichen Faktor" widmete Vesselin Popov vom Psychometrics Centre der University of Cambridge einen nicht-technischen, aber ebenso spannenden Vortrag: Psychometrisches Targeting – also auf das individuelle, per AI (Artificial Intelligence) ermittelte Profil eines Anwenders ausgerichtete Information – ist, so führte der Cambridge-Mitarbeiter aus, nachweislich dazu geeignet, Entscheidungen und Aktionen der Anwender zu beeinflussen. Brisant ist dieses Thema angesichts des Umstands, dass man derzeit in den USA wie auch in Großbritannien diskutiert, in welchem Maß die Entscheidungen für Trump beziehungsweise pro EU-Austritt mittels Social-Media-Targeting beeinflusst wurden.

„Wir haben einen jämmerlichen Umgang mit Passwörtern", so Security-Auditorin und Pen-Testerin Paula Januszkiewicz. Bild: Dr. Wilhelm Greiner

Auf Facebook, so der Cambridge-Mann, könne man heute allein mittels Auswertung der Likes wesentliche Charaktereigenschaften oder auch die sexuelle Orientierung eines Nutzers eruieren. Mittels AI sei es längst möglich, die „Big Five"-Faktoren der menschlichen Psyche – Offenheit für Erfahrungen, Gewissenhaftigkeit, Extraversion (Geselligkeit), Verträglichkeit und Neurotizismus – ebenso zu ermitteln wie die Intelligenz, Lebenszufriedenheit, politische und religiöse Ansichten oder die finanzielle Risikoeinstufung eines Nutzers. AI liege dabei inzwischen sogar öfter richtig als das direkte Umfeld des Betroffenen, so der britische Forscher.

Das Psychometrics Centre will Human- und Ingenieurswissenschaften näher zusammenbringen, so Popov, um „gerechtere Entscheidungssysteme" zu schaffen. Ein verantwortungsvoller Umgang mit AI setzt laut Erkenntnissen aus Cambridge folgende Schritte voraus:

- Kontrolle: Datenverwendung nur mit Zustimmung des Anwenders,
- Transparenz: der Betroffene erfährt die Ergebnisse,
- Personalisierung: Nutzung der Daten für eine verbesserte „User Experience",
- Relevanz: Datenverwendung und Ergebnis hängen direkt zusammen (also keine unerwünschte Zweitverwendung der Daten), sowie
- Dialog mit dem Anwender, um das Verfahren zu verbessern.

Angesichts des Umstands, dass AI ebenso wenig wieder verschwinden wird wie Targeted Marketing oder politische Instrumentalisierung, sei diese Forschung heute höchst relevant, so Popov gegenüber LANline. Nötig sei eine Grassroots-Bewegung für mehr Privatsphäre und sinnvolle Nutzung der IoT-Daten. Denn Targeting ermöglicht es laut Popov nicht bloß, Marketing-Maßnahmen noch effektiver zu machen, sondern kann zum Beispiel auch helfen, Risiken durch ein optimiertes Zusammenspiel von Mensch und Maschine zu mindern. So habe die Forschung gezeigt: Die Zahl der Autounfälle sinkt, wenn die Stimme des Navigationssystems auf den Charakter des Fahrers abgestimmt ist.

Die diesjährige IT-Defense punktete durch provokant vorgetragene Thesen ebenso wie durch eine Fülle von Fakten und Erkenntnissen zum Status quo in Sachen IT-Security. Die nächste IT-Defense findet von 6. bis 8. Februar 2019 in Stuttgart statt.

Dr. Wilhelm Greiner