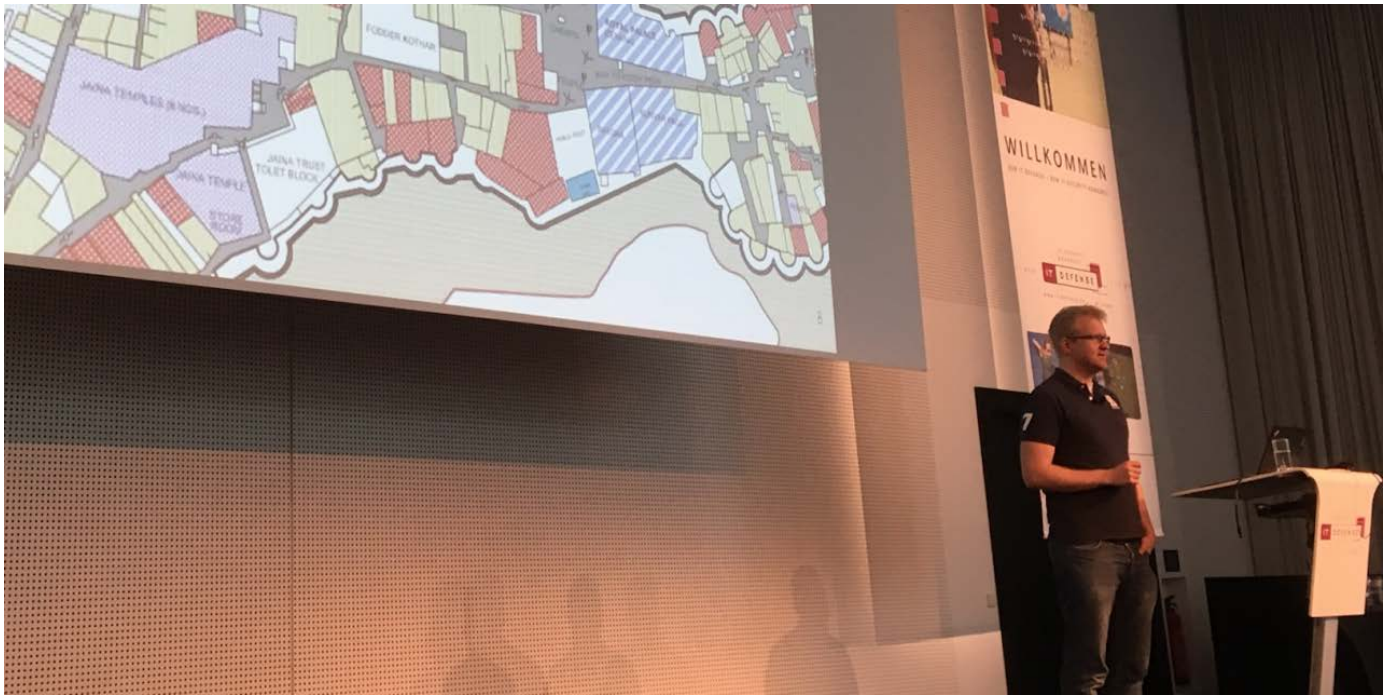
IT-Defense, Berlin

Ein Schutzwall für das Internet

21. Februar 2017 | Von Dr. Wilhelm Greiner.
Schlagwörter: Cirosec, Hacking, IT-Defense, Konferenz



Die vom Beratungshaus Cirosec ausgerichtete Sicherheitskonferenz IT-Defense fand im Februar dieses Jahres zum 15. Mal statt, Veranstaltungsort war diesmal Berlin. Das Spektrum der Vorträge, die Cirosec den 200 Besuchern präsentierte, reichte von der Angreifbarkeit von Windows über Social-Media-basierte Angriffe, Trends in der Exploit-Entwicklung und das Gefährdungspotenzial des Quanten-Computings bis hin zur Frage, unter welchen Bedingungen eine sichere, vertrauenswürdige IT-Landschaft möglich sein könnte.

Der unter dem Pseudonym „Halvar Flake“ bekannte White-Hat-Hacker Thomas Dullien, heute für Google tätig, präsentierte auf der IT-Defense spannende Überlegungen zu einem fundamentalen Problem: Wie könnte eine Architektur für ein

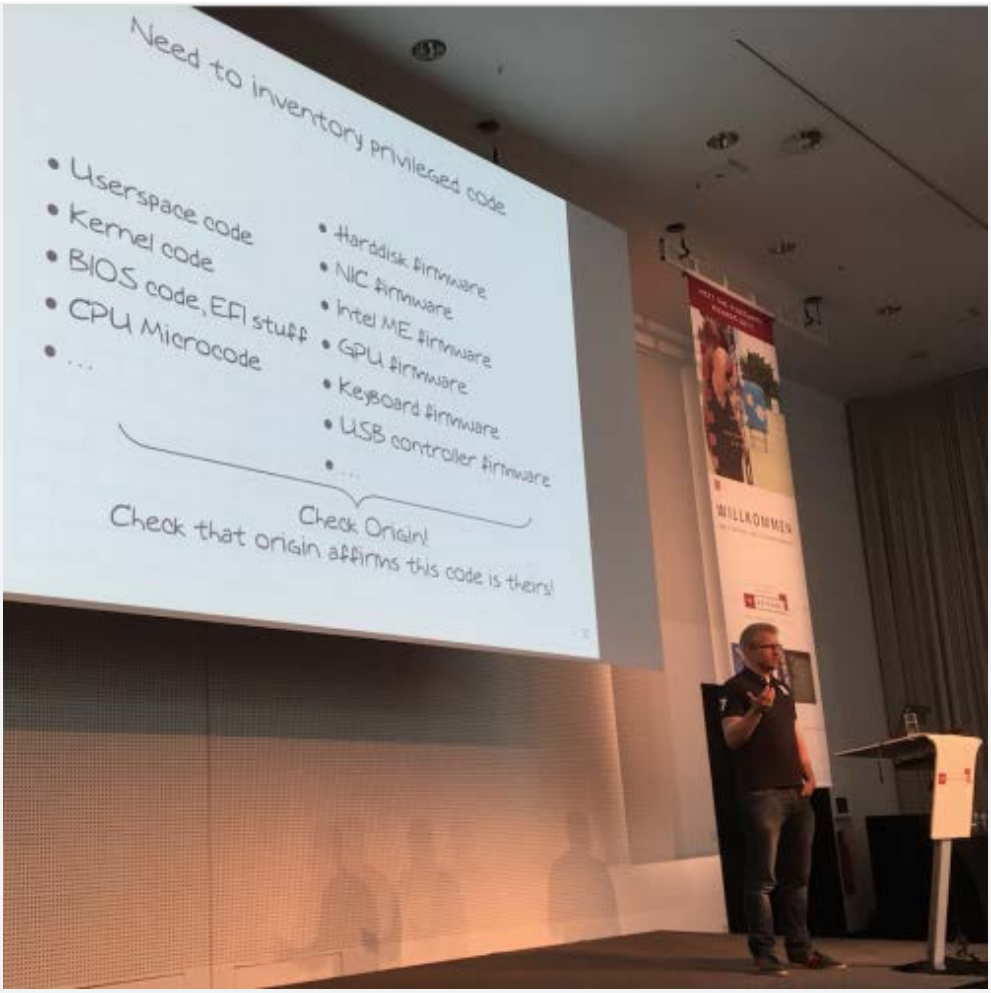
Internet aussehen, sodass man es verteidigen kann? „Der Angreifer bewegt sich immer in dem Netz, das der Verteidiger designt hat“, so Dullien. Wie man im mittelalterlichen Burgenbau enge Ecken und Gassen einzogen habe, damit Angreifer mit dem Rammbock nicht um die Kurve kamen, sei es nun Aufgabe des Verteidigers, sein Netzwerk auf Verteidigung auszulegen.

Die Kernfrage laute daher: „Wie kann man IT-Systeme so umbauen, dass man sie überhaupt verteidigen könnte?“ Anders als in der analogen Welt könne man Besitz in der digitalen Welt schließlich nicht mehr mit Kontrolle gleichsetzen: „Wir haben überhaupt keine Kontrolle darüber, was mit den Geräten (im Internet der Dinge, d.Red.) passiert“, so Dullien. Der Bezug von Software gleiche einem „Schuhkauf, bei dem man jemandem den Hausschlüssel überlassen muss, damit er die neuen Schuhe in den Schuhschrank stellen kann.“

Man müsse also die Geräte so redesignen, dass sich etablieren lässt, wer überhaupt Kontrolle über das Gerät hat. Das Problem dabei: Jedes Gerät ist heute, so Dullien, ein „Netzwerk von Computern“ – ohne standardisierten Weg, Firmware von Geräten auslesen. Ist Firmware kompromittiert, könne man dies nicht nachweisen. Nötig sei daher ein standardisiertes, nicht aktualisierbares Ausleseverfahren inklusive einer Codesignatur, die beweist, dass der ausgelesen Code tatsächlich vom Hersteller stammt.

Öffentliches Hauptbuch für Firmware

Doch Codesignaturen sind laut Dullien in ihrer derzeitigen Form nicht ausreichend vertrauenswürdig. Notwendig sei ein Überblick über die Codesignaturen mittels einer verteilten, transparenten Buchführung („Distributed Ledger“) – also Verfahren, wie man sie von SSL oder digitalen Währungen her kennt. Statt des heute üblichen Wirrwarrs an Vertrauensbeziehungen zwischen PC- und Komponentenherstellern forderte Dullien einen auditierbaren Pfad für Quellcode im Quellcode-Repository mit signierter Versionierung und einem öffentlichen Hauptbuch für Code („Public Code Ledger“), das auch Hashes der Codequellen umfasst. Dazu wiederum brauche man ein generisches „Recht auf Reverse Engineering“.



Thomas Dullien, auch bekannt als Halvar Flake, beschrieb die Voraussetzungen für ein vertrauenswürdiges und damit zu verteidigendes Internet. Bild: Dr. Wilhelm Greiner

Dieses Vorgehen wäre laut Thomas Dullien technisch möglich und auch gar nicht so teuer (unter einem Dollar pro Gerät, sofern gleich beim Design berücksichtigt); doch angesichts des stark zersplitterten IT-Markts hätten selbst die großen Hersteller weder das Budget noch die Macht, ein solches Konzept durchzusetzen. Selbst Google habe nicht genügend Gewicht, um bei Intel ein Umdenken anzustoßen. Am ehesten, so Dullien, sei Apple mit seiner vertikal integrierten Produktion in der Lage, ein solches Verfahren zu verwirklichen. Doch Apples geschlosses System widerspreche der Idee eines öffentlichen Hauptbuchs. Sein Fazit: Verteidiger müssten ihre Netzwerke „verteidigbar“ machen – doch leider hat kein Verteidiger auf Hardwareebene genug Marktmacht, um das durchzusetzen. Der nötige Druck, so Dullien, könne damit nur vom Gesetzgeber kommen (wofür er wenig Sympathie hegte) oder zum Beispiel über Versicherungsanbieter, nach dem Motto: „Wir reduzieren deine Prämie, wenn deine Hardware nachweislich signierten Code nutzt.“

Zielscheibe Windows

Der finnische White-Hat-Hacker Sami Laiho befasste sich in seinem Vortrag mit dem Hacking von Windows-Systemen und der grundlegenden Frage, warum Windows-

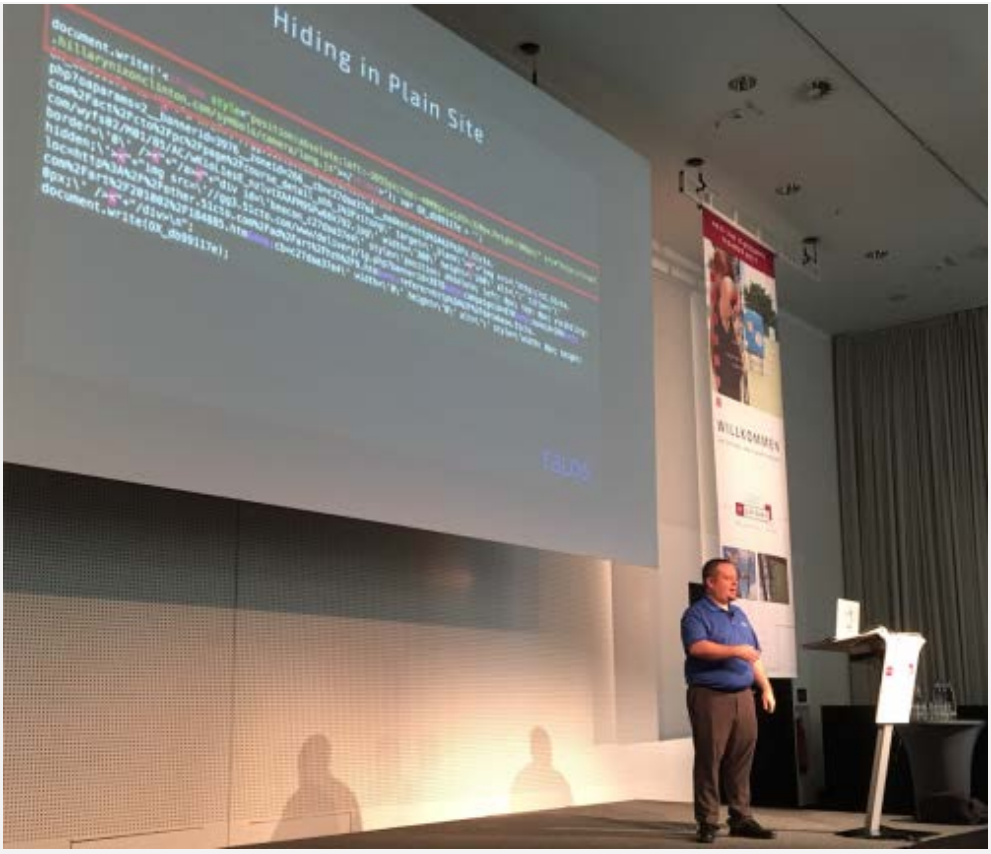
Systeme dafür anfällig sind. Basis seines „Conceptual Hackings“ ist dabei laut seiner Aussage schlicht die gründliche Kenntnis der Windows Internals. Er demonstrierte, dass man sich mit fünf schnellen Tastendrücken Root-Zugriff auf einen ungeschützten Windows-Rechner verschaffen kann, und wie man sich dann mittels Administratorprivilegien die Beschränkungen der Gruppenrichtlinien überwindet.

Auch ein Windows-10-Upgrade ist laut Laiho ein „ernsthaftes Sicherheitsrisiko“, reiche doch die Tastenkombination Shift-F10 zur rechten Zeit während des Bootens, um auch hier Root-Rechte zu erhalten. Sein Rat an die IT-Fachleute lautete deshalb, niemals unbeaufsichtigte Windows-10-Upgrades zuzulassen. Auch solle man sich als Domänenadministrator nie auf einem kompromittierten Client einloggen. Er empfahl zudem den Einsatz von Applocker, um die Installation unerwünschter Apps mit Adminrechten zu unterbinden.

Generationswechsel bei Exploit Kits

Nick Biasini, Sicherheitsforscher bei Cisco Talos, gab einen faszinierenden Einblick in den jüngst erfolgten „Generationswechsel“ bei Malware: 2016 war laut Biasini eine „goldene Ära“ für Exploit Kits, vor allem dank der Millionengewinne, die mittels Ransomware zu erzielen waren (und sind). Der „König“ der Exploit Kits war Angler vor Konkurrenten wie Nuclear und Neutrino – bis im Juni 2016 eine russische Hackerbande verhaftet wurde, die hinter Angler und dem Banktrojaner Lurk steckte. Wenig später wurde auch Nuclear eingestellt, auch Neutrino verlor an Relevanz.

Seitdem, so Biasini, geben die Exploit Kits Rig/Rig-V sowie Sundown den Ton an. Rig dominiere dabei die Aktivitäten, Rig-V allerdings sei die ausgefeiltere Variante. So verstecke Rig-V die URLs zu den Malware-Web-Seiten viel besser und prüfe zudem, ob die Malware-Payload von einer der führenden Antiviren-Engines entdeckt wurde. An Sundown hingegen ließ Biasini kein gutes Haar: Angler sei sehr durchdacht designt gewesen, mit einer genau auf das Ziel abgestimmten Payload und schneller Entwicklung neuer Exploits, zum Beispiel nach jedem Adobe-Update; demgegenüber bewege sich Sundown lediglich auf Script-Kiddie-Niveau und bewerfe das Opfer mit allem, was vorrätig ist. „Die neuen Exploits“, so Biasini, „lernen gerade das Krabbeln, während Angler schon am Sprinten war.“



Nick Biasini verglich die derzeit populärsten Exploit Kits mit ihrem Vorgänger Angler – und sie schnitten alles andere als gut ab. Bild: Dr. Wilhelm Greiner

Derzeit verlassen sich Exploit Kits laut dem Talos-Mann stark auf Schwächen in Microsoft Silverlight und Adobe Flash. Diese Angriffsfläche schwinde aber allmählich: Silverlight werde nicht mehr weiterentwickelt, dem oft kritisierten Flash drohe das gleiche Schicksal, und selbst das beliebte Angriffsziel Internet Explorer habe deutlich Marktanteile an Googles Sandbox-bewährten Browser Chrome verloren. Cyberkriminelle konzentrierten sich deshalb zunehmend auf Südamerika und Asien, so Biasini, wo Windows 7 nach wie vor verbreitet sei. In Asien finde man zudem viel Softwarepiraterie und damit große Zurückhaltung, den offiziellen Update-Weg zu gehen – und dies in einem Markt mit über 48 Prozent der Internet-Nutzer.

Als weiteren wichtigen Angriffsvektor beschrieb Biasini Mobilgeräte und hier – wenig überraschend – insbesondere Android-Devices. Schließlich sei Android das mit großem Abstand verbreitetste Mobile-OS, und es bestehe eine „fürchterliche Fragmentierung“: Über 30 Prozent der User nutzten noch Android 4.4 oder älter. Biasini warnte vor Angriffsszenarien, bei denen Ransomware auf Mobilgeräten mit Click-Fraud kombiniert wird: Selbst wenn man nach Zahlung eines Lösegelds wieder Zugriff auf sein Mobilgerät und dessen Daten erlangt hat, gehe im Hintergrund der Klickbetrug als „Low and Slow“-Angriff unbemerkt weiter.

Spear-Phishing im Eigenbau

Für hohen Unterhaltungswert sorgen der auf Red-Teaming spezialisierte Jayson E.

Street und der britische Hacker Adam Laurie. Street zeigte, wie man sich – ganz offiziell, ohne eine einzige Firewall-Regel zu unterlaufen – über Social Media und WHOIS-Einträge der Unternehmens-Websites alle Informationen beschaffen kann, die man für einen Spear-Phishing-Angriff benötigt. Für das Versenden des Phishing-Links empfahl er die Fußzeile „Sent from a mobile device“: Hier, so Street, nähmen es die Empfänger nicht so genau, wenn Orthografie oder Sprachgebrauch vom Erwarteten abweichen. Den Verteidigern riet er: „Baut ein U-Boot, keine Mauer!“ Gemeint war: Honeypots mit automatischen Alerts als Frühwarnmechanismus. Zudem, so Street, sollten Unternehmen „vermittelbare Momente“ für die Mitarbeiter schaffen – bevor echte Angreifer dies übernehmen.

Jayson E. Street skizzierte, wie man sich aus öffentlichen Quellen alle Informationen für einen Spear-Phishing-Angriff besorgt. Bild: Dr. Wilhelm Greiner

Adam Laurie von Aperture Labs präsentierte anhand von allerlei Video-Clips und Marketing-Material die Fülle „smarter“ – und damit angreifbarer – Gadgets, mit denen die Industrie das Verbrauchervolk beglücken will. Die Angebote reichten – zum Amüsement des Publikums – vom „smarten“ Cocktail Shaker und Kochtopf über Socken, Handschuhe und Büstenhalter bis hin zu Whiskeyflaschen und Vibratoren: „Die Frauen wollen uns durch Roboter ersetzen“, warnte ein vorgeblich schockierter

Laurie, der beim Bild eines „smarten“ Toilettensitzes samt zugehöriger App lakonisch feststellte: „Ich will gar nicht wissen, über was sich meine Toilette und mein Telefon unterhalten.“ Das Internet der Dinge – das neben solchen obskuren Neuheiten auch Schwergewichte wie Amazon Echo und Google Nest hervorgebracht hat – sei problematisch, da zahlreiche der über Zigbee, Bluetooth und WLAN vernetzten Dinge „auf gefährliche Weise ungeschützt“ sind, so Laurie.

Auf der IT-Defense gab es zudem eine Reihe spannender Vorträge zu Forschungsthemen. So diskutierte Jaya Baloo, CISO von KPN Telekom, die Fortschritte bei Quantencomputern. Sie beschrieb den Wettbewerb im Bereich der Quantenkryptografie als neues „Manhattan Project“, somit als Wettlauf wie beim Bau der ersten Atombombe: Wer zuerst ans Ziel gelangt, kann potenziell die gesamte bestehende Ordnung kippen. Dan Guido von Trail of Bits berichtete über die Fortschritte beim Fuzzing für die Verbesserung von Code durch automatisierte Identifikation von Bugs, und Prof. Christof Paar von der Ruhr Universität Bochum referierte über Ansätze, wie Angreifer Trojaner auf Hardwareebene einbringen können. Auf diese Weise könnten Angreifer wie etwa Regierungsorganisationen zum Beispiel eine PIN-Verifizierung schwächen, warnte er.

Die nächste IT-Defense findet vom 31. Januar bis 2. Februar 2018 in München statt. Weitere Informationen finden sich unter www.it-defense.de.

Dr. Wilhelm Greiner ist Stellv. Chefredakteur der LANline.