IT-Defense: Immer Ärger mit Windows 10

Teilzeitschutz

Jörg Riether

Nachdem Microsoft auf die jüngste Kritik wegen Datenschutzmängeln in Windows 10 mit der Ankündigung neuer Features reagierte, steht erneut Ärger ins Haus: Ein Sicherheitsexperte entdeckte, dass die betriebssystemeigene Verschlüsselung BitLocker temporär versagt.

Mitte Februar trafen sich in Berlin IT-Sicherheitsexperten zur „IT Defense", die das Heilbronner Beratungsunternehmen Cirosec zum 15. Mal ausrichtete. Sami Laiho, spezialisiert auf Windows-Sicherheit, berichtete von einem fatalen Designfehler in der Windows-10-Upgrade-Systematik, den er Ende 2016 entdeckt hatte. So sei es tatsächlich derzeit Fakt, erklärte Laiho, dass Windows-10-Systeme, die mit BitLocker geschützt seien, während eines großen „Feature-Updates" die Verschlüsselung vorübergehend aussetzten. Konkret könne man ohne Weiteres während eines Feature-Updates mit der gewohnten Shift-F10-Funktion eine Kommandozeile öffnen und somit Vollzugriff auf sämtliche Daten erhalten – und zwar insbesondere auch auf via BitLocker verschlüsselte Systeme.

Es geht aber noch weiter: Selbst wenn man seitens des Herstellers die Shift-F10-Funktion unterbinden würde – es gebe trotzdem Wege. Man drücke etwa einfach beim Feature-Update direkt nach dem ersten Neustart einmal die Hardware-Reset-Taste des entsprechenden Rechners und boote von einem Installationsmedium und schon habe man wieder Vollzugriff auf die vermeintlich verschlüsselten Daten. Hier spiele es im Übrigen überhaupt keine Rolle, ob zum Zeitpunkt der Initialisierung des Feature-Updates ein Benutzer mit oder ohne administrative Rechte angemeldet gewesen sei.

Laiho erklärte den verdutzten Zuhörern, dass Microsoft nicht glücklich über seine Entdeckung sei und ihm zu verstehen gegeben habe, dass doch normalerweise niemand seinen PC unbeaufsichtigt lassen würde, wenn ein großes Update laufe. Insofern darf man an dieser Stelle sehr gespannt sein, ob Microsoft die Update-Logik und -Routinen dahingehend ändern wird, dass die Laufwerksverschlüsselung zu keinem Zeitpunkt ausgesetzt wird.

Nick Biasini, Forscher im Bereich IT-Bedrohungen, berichtete über den Status quo und die mögliche Zukunft von Exploit Kits. RIG/RIG-V sei derzeit der weltweit am weitesten verbreitete Malware-Baukasten. Als Payload komme vor allem Ransomware zum Einsatz.

Biasini prognostizierte zwei wesentliche Trends: Regionalisierung und Mobilgeräte. Zur Regionalisierung dürften die Täter ihre Aktivität in Nordamerika und Europa vermutlich reduzieren, weil in diesen Regionen viele Augen auf den Datenverkehr gerichtet seien. Attraktive Zielregionen seien zukünftig noch stärker Südamerika und Asien. Südamerika etwa sei besonders interessant für kriminelle Malware-Initiatoren, weil es dort einen spürbar verzögerten Umstieg auf Windows 10 gebe.

In Asien sei das zwar auch so, jedoch nicht, weil man schlicht später upgraden würde, sondern aufgrund von Softwarepiraterie. Letztere sei in Asien verbreitet. Ergo benutze man zuhauf keine automatischen Updates, weil zahlreiche nicht lizenzierte Software benutzt würde. Asien habe gleichzeitig mit Abstand die meisten Internetnutzer weltweit.

Über Laihos jüngste Entdeckung der fehlerhaft arbeitenden BitLocker-Verschlüsselung war Microsoft wenig erfreut.

Zu den mobilen Geräten sagte Biasini, dass die weltweite Internetnutzung mit ihnen quantitativ höher liege als die aller Desktops zusammengenommen. Somit sei dies ein attraktives Ziel, und zwar Android, um genau zu sein. Der Grund sei so traurig wie einfach – extrem viele Geräte im Umlauf enthielten sehr alte Versionen des Betriebssystems.

Aber wie verfahre man nun als Angreifer? Es gehe nämlich bei den Mobilgeräten gar nicht um Ransomware, sagte Biasini. Die Zukunft werde sich viel perfider entwickeln. Anstatt zu verschlüsseln, stehle man einfach alle Daten und teile seinem Opfer anschließend mit: Entweder du zahlst oder ich mache sämtliche Daten, Dokumente und Fotos allen Personen in deiner Kontaktliste publik.

Banking-Trojaner auf Mobilgeräten würden in Zukunft aber an Bedeutung verlieren. Neue Botnets hingegen seien die größte Gefahr. Warum nicht ein paar Millionen Geräte kontrollieren, die DDoS-Attacken fahren, Massenmails versenden oder auch Klickbetrug durchführen können, so Biasini.

Codetransparenz durch Blockchain

Reverse-Engineering-Experte Thomas Dullien wagte in seinem Vortrag den Versuch der Skizzierung eines Modells, das nötig wäre, um die Kompromittierung von Hardware und Software zuverlässig zu erkennen. Betrachtete man einmal den Status quo, so Dullien, sei es heute tragischerweise so, dass, wenn man von einem gehackten System Kenntnis erlange, die einzige sichere Maßnahme dessen vollständige Entsorgung sei. Und das hänge einfach mit fehlender Kontrolle zusammen. Die Ansicht, man habe mit dem Besitz von IT-Systemen auch die Kontrolle darüber, sei eine Illusion.

Eine mögliche Lösung könne sein, von vornherein komplette Einsicht in jedweden Code zu bekommen, und zwar bis auf die Ebene des BIOS-Codes, des CPU-Microcodes oder jeglicher Firmware. Dies könne man etwa mit einem standardisierten und nicht updatefähigen Hardwarepfad bewerkstelligen, der den Speicher auslesen und etwaige Hash-Werte idealerweise auf dem denkbar simpelsten Anzeigegerät ausgeben kann. Jetzt fehle aber noch eine verbindliche Bestätigung der Hersteller. Codesignaturen in der heutigen Form könne man nicht trauen. Überhaupt sei transitives Vertrauen grundsätzlich problematisch, denn schlussendlich finde man immer mögliche Pfade, auf denen zu vielen Beteiligten zu viel Vertrauen entgegengebracht werde.

Es erfordere vielmehr eine neue Form der Transparenz, einen, wie Dullien es nannte, „Public Distributed Ledger", also eine Art öffentliches und fälschungssicheres Notariat. Jeder müsse sofort sehen können, dass etwa CA X eben für die Firma Y ein Zertifikat Z ausgestellt hat. Oder beispielsweise Hersteller A die DLL B gerade mit dem Hash C signiert hat. Das würde natürlich, wenn man es zu Ende denkt, nur dann funktionieren, wenn dieses Notariat auch Kenntnis von jeglichem Quellcode hätte. Und selbst wenn Letzteres als unrealistisch abgeschmettert werden würde – ein generisches Recht auf Reverse Engineering sei als absolutes Minimum notwendig. Finanziell wäre so etwas machbar, es würde weniger als 1 US-Dollar pro Gerät kosten, so Dullien. Das Notariat könne man mit weniger als 1 Million US-Dollar pro Jahr realisieren. Vielmehr erfordere es aber den unbedingten Willen und ein Umdenken auf breiter Front. (ur)