IT-Defense 2018: Vernetzt wider Willen

Keine Kontrolle

Jörg Riether

Die Vernetzung von IoT-Geräten könnte in Zukunft anders und weniger freiwillig ablaufen, als wir uns dies heute vorstellen.

Die diesjährige auf IT-Sicherheit ausgerichtete Fachkonferenz IT-Defense in München war die insgesamt 16. Veranstaltung des Heilbronner Unternehmens Cirosec.

Mikko Hyppönen von F-Secure beschäftigte sich in seinem Vortrag „The Next Revolution" mit einer Voraussage, wie IoT zukünftig aussehen könnte. Der heutige Grad der Vernetzung von IoT-Geräten werde in naher Zukunft belächelt werden, so Hyppönen. In etwa 10 Jahren würden selbst die allerdümmsten und billigsten Geräte im Internet stehen. Wenn heute ein leistungsfähiger IoT-Kommunikations-Chip beispielsweise 10 Dollar koste, so würde man diesen derzeit kaum in einen 20-Dollar-Toaster einbauen. Wenn der Chip aber in ungefähr 9 bis 10 Jahren nur noch wenige Cent koste, sähe die Sache plötzlich gänzlich anders aus.

Sicher ohne WLAN?

Bei der Frage, welche erheblichen Sicherheitsprobleme diese Entwicklung bringen könnte, würden manche Aspekte selbst von vorsichtigen und kritischen Menschen derzeit noch unterschätzt.

Einige könnten nun abwiegeln und argumentieren, man könne ja einfach die IoT-Geräte in Zukunft nicht mehr ins WLAN hängen – man habe also immer die Kontrolle. Dies sei aber zu kurz gedacht, so Hyppönen. In Zukunft würden solche Geräte sicherlich nicht auf umständliche Dinge wie WLAN zurückgreifen. Warum auch, wenn man demnächst für wenige Cents eSIM auf LTE- und 5G-Netzwerken basierend nutzen könne. Die Kunden müssen also gar nicht erst gefragt werden, die Geräte würden einfach auch ohne ihr Wissen online gehen, sich anmelden und Analysedaten senden. Etwaige Analyse- und Einsatzmöglichkeiten in dieser Richtung seien drastisch – man könne an alles denken, was einen Stromanschluss besitzt, sei es ein Toaster, ein elektrisches Bett oder Leuchtmittel.

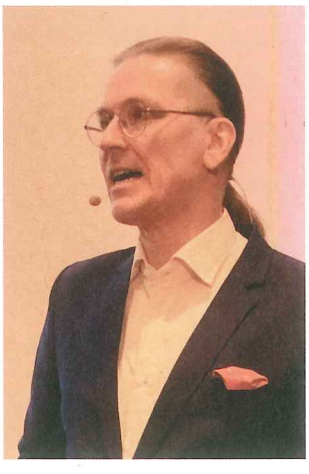
Zu wenig Beachtung

Wenn also in Zukunft so viel Engagement in Datenanalyse eingebracht wird, sollte man annehmen, dass auch in die Sicherheit von IoT erhebliche Bemühungen einfließen. Dies ist aber unwahrscheinlich, glaubt Hyppönen. Ein Teil des Problems seien sogar wir selbst. Wenn wir eine Waschmaschine kaufen, würden wir nach Dingen wie Preis und Farbe fragen. Nach etwaigen Sicherheitstechniken würden wir uns hingegen kaum erkundigen. Wenn aber der Kunde solche Dinge nicht verlange, sei es ziemlich unwahrscheinlich, dass Hersteller diese priorisieren würden.

Stephan Gerling beschäftigte sich mit der Sicherheit vernetzter Systeme auf Hochseeyachten, im Detail mit Netzwerkroutern von Locomarine. Diese Systeme seien in der Regel vom Internet aus direkt erreichbar. Gerling fand heraus, dass deren gesamtes Sicherheitsmodell von erheblichen Schwächen betroffen ist. Seine Untersuchung im Juni 2017 habe ergeben, dass via Netzwerkanalyse, zum Beispiel mittels Wireshark, ein vom Hersteller hart-vordefiniertes administratives Konto samt Passwort im Klartext über die Leitung gehe – und zwar via FTP.

Und noch schlimmer: Die in .NET geschriebene Administrationssoftware für diese Router, die man sich einfach über die Homepage des Herstellers besorgen könne, sei problemlos mit gängigen Analysetools wie ILSpy (https://github.com/icsharpcode/ILSpy#ilspy -------) lesbar zu machen. Dort seien neben den bereits via Wireshark herausgefundenen Login-Daten sogar noch weitere im Klartext zu finden gewesen. Gerling meldete im Juni 2017 seinen Fund an den Hersteller, worauf dieser etwa Mitte November einen Fix herausgebracht habe. Letzterer entpuppte sich aber nach einer erneuten Analyse durch Gerling als unwirksam.

Man habe die Administrationssoftware schlicht mit Verschleierungstechnik versehen, um eine Analyse zu erschweren, berichtete Gerling. Außerdem übertrage man etwaige Konfigurationen nun via SSH anstelle FTP. Gerling habe sich daraufhin anstelle der Windows-Version einfach die Android-Variante der Software aus dem Google Play Store besorgt. Nach dem Entpacken und Analysieren einer DLL, erneut mittels ILSpy, seien dort neue vom Hersteller fest vergebene administrative Login-Daten im Klartext auffindbar gewesen. Je nachdem, welche internen Geräte einer Yacht an diesem Netzwerk hängen, könnte eine solche Nachlässigkeit schnell zu einer Gefahr für Leib und Leben werden, so Gerling. Bedenkt man, dass vermutlich einige Yachten mit diesen Systemen gerade auf hoher See unterwegs und die Router möglicherweise verwundbar sind, sollte der Hersteller hier dringend Abhilfe schaffen und das komplette Sicherheitsmodell überarbeiten.



Mikko Hyppönen sieht zukünftig durch 5G-Pfennigware jedes noch so kleine Billiggerät vernetzt – auch ohne Zutun des Nutzers.

Neue Ideen für Angriffserkennung

Stefan Strobel von Cirosec sprach in seinem Round-Table über Angriffserkennung. Es gebe heute Tausende Ansätze und vieles habe seine Daseinsberechtigung, aber gerade zwei relativ triviale Methoden sieht Strobel derzeit als besonders zielführend. Dazu gehöre zum einen Anomalieerkennung. Dahinter verbergen sich Systeme, die auf alle Vorgänge des Normalbetriebs von Systemen und Netzwerken trainiert werden und etwaige Abweichungen melden oder automatisch tätig werden können. Damit seien solche Systeme effizienter als etwa herkömmliche Eindringlingserkennungssysteme.

Auch eine andere klassische Idee und Methode, das bewusste Auslegen von Ködern, sei sehr treffsicher. Man erstelle und platziere einen vermeintlich administrativen und temporären AD-User (Active Directory), dessen Passwort in der AD-Beschreibung steht, an gut auffindbarer Stelle in der AD-Struktur. Anschließend konfiguriere man eine Echtzeitüberwachung auf Anmeldungen genau dieses Kontos.

Strobel hatte noch einen weiteren Vorschlag: Warum eigentlich nicht spezielle Ködereinträge im Zwischenspeicher für Anmeldedaten von Windows platzieren und einen Alarm auf Anmeldungen von exakt diesen Konten setzen? Damit könne man unter Umständen den Einsatz des Hacking-Tools Mimikatz durch einen Angreifer aufspüren. Bei so stark zielgerichteten Ködermethoden dürfte laut Strobel die Falsch-Positiv-Quote nahezu gegen null gehen. (ur@ix.de)