IT Defense 2016: Düstere Aussichten

Nachlässigkeit 4.0

Jörg Riether

Was Experten über den Sicherheitsstatus vernetzter Systeme und vor allem industrieller Steuerungssysteme enthüllen, jagt jedem Sicherheitsbewussten Schauder über den Rücken.

Bei der vom Heilbronner Unternehmen Cirosec ausgerichteten IT-Sicherheits-Fachkonferenz IT-Defense Ende Januar in Mainz malte Kaspesky-Lab-Mitgründer und CEO Eugene Kaspersky in Bezug auf Computerkriminalität heute und in der Zukunft ein dunkles Bild.

Die weltweite Bedrohung durch Verbrechen im digitalen Raum wachse stetig, professionalisiere sich zunehmend und sei heute meist länderübergreifend und straff durchorganisiert. Er sprach in diesem Zusammenhang von CaaS (Crime as a Service). Solche Unternehmungen würden sich in ihrer internen Struktur überhaupt nicht mehr von legalen Großunternehmen unterscheiden. Man habe dort alles – sogar eigene Abteilungen für Benutzer-Support.

Industrie im Fokus

Für die Zukunft würden ihm vor allem weitere Angriffe auf Industriesteuerungen Sorge bereiten. Die Frage sei heute nicht mehr, ob es Angriffe auf kritische Infrastruktur, etwa Kernkraftwerke, geben wird. Die wirklichen drei Fragen, um die es heute gehe, seien vielmehr „Wann?", „Wie schlimm?" und „Wo?".

Kaspersky sieht für derartige Szenarien vier primäre Gruppen von möglichen Angreifern: klassische Kriminelle (etwa um zu erpressen), Terroristen (um Zerstörung und Tod zu verursachen), politische Aktivisten (um politische Ziele zu erreichen) sowie Militär (um Gegner digital anzugreifen).

Sein Fazit fiel düster aus. Was man gegen Bedrohungen dieses Kalibers heute tun könne? Auf die Schnelle – gar nichts. Das Beste wäre vermutlich, zu beten. Unterm Strich gebe es eine ganz nüchterne wie simple Regel, so Kaspersky. Der eigentliche Angriff müsse technisch, logistisch und finanziell teurer werden als die potenziellen Auswirkungen. Davon seien wir aber weit entfernt.

Wenn sich an dieser Situation etwas ändern solle, so Kaspersky, müsse drastisch mehr in Bildung, insbesondere mit Schwerpunkt auf IT-Sicherheit, investiert werden – und zwar weltweit. Gleichzeitig müsste es eine völlig neue Dimension internationaler Zusammenarbeit geben. Parallel solle man endlich aufhören, schon existierende unsichere Industriesteuerungen weiterzuentwickeln. Stattdessen solle man sie von Grund auf neu entwickeln, und zwar von Anfang an mit Fokus auf Sicherheit.

John Matherly, Gründer von Shodan, knüpfte genau dort an. Bei Shodan handelt es sich um eine Internetsuchmaschine, die sich auf das Ausfindigmachen von direkt aus dem Internet erreichbaren Geräten spezialisiert. Das kann im Prinzip alles sein, angefangen bei Webcams über Drucker, Ampeln, Schwimmbad- und Heizungssteuerungen bis hin zu mannigfaltigen Industriesteuerungen, etwa von Kraftwerken.

Das Sicherheitsbewusstsein in Sachen Industriesteuerung ist nach Untersuchungen von John Matherly erschreckend niedrig.

Matherly berichtete in seinem Vortrag von einigen Kuriositäten. So habe er Statistiken erstellen können, die beispielsweise Aufschluss darüber gäben, welche Universitäten in den USA am dringendsten neuen Toner benötigen würden. Mittels 100 offener Verkehrsüberwachungssysteme habe er binnen fünf Tagen 62 857 unterschiedliche Kfz-Kennzeichen einsammeln können und er verfüge über detaillierte Informationen über diverse Windkraftanlagen weltweit. Und all dies ohne jedweden gewaltsamen Einbruchsversuch, sondern einfach nur durch simples Verbinden. Viele direkt im Internet erreichbare Systeme, so Matherly, müsse man einfach nur auf dem richtigen Port besuchen und sie würden einen dankbar und ohne jedwede Authentifizierung förmlich mit Daten bewerfen.

Tausende Systeme via Internet erreichbar

Beim Thema SCADA wurde Matherly dann ernst. Richtig übel sei es um Industriesteuerungen bestellt. In diesem Umfeld, so Matherly, sei die gesamte Idee von IT-Sicherheit auch heute noch allzu selten angekommen. Shodan finde für jedermann einsehbar unzählige Industriesteuerungen, die direkt vom Internet aus erreichbar seien. Als Beispiel sprach er das weitverbreitete Modbus-TCP-Protokoll an, das standardmäßig auf TCP-Port 502 beheimatet ist. Shodan findet Tausende solcher Systeme.

Viele Betreiber oder Hersteller glaubten immer noch daran, dass aufgrund des vermeintlich exotischen Protokolls kaum öffentliches Wissen und ergo kaum Angriffsvektoren vorhanden seien. Diese Annahme sei so falsch wie dumm, so Matherly. Allein auf Stack Overflow, einer bekannten Community für Programmierer, sei das Thema Modbus in den letzten Jahren immer wichtiger geworden, es gebe also sehr wohl zahlreiche Möglichkeiten für jeden, Detailwissen aufzubauen, selbst bei komplexen Fragestellungen.

Einfacher Portwechsel nützt nichts

Dann gebe es noch vermeintlich schlaue Menschen, die durch simples Auswählen eines anderen Ports, etwa 503, dem Irrglauben eines effizienten Schutzes unterlägen. Überhaupt sehe Matherly auch unzählige andere Systeme, etwa SSH- oder VNC-Server, wo man einfach nur den Port geändert habe. Dabei fallen ihm immer wieder die gleichen Muster auf, etwa plus/minus 1, 1000 oder eine schlichte Wiederholung der Zahl. Insofern habe er schon früh seine Infrastruktur dahingehend angepasst, dass für jeden der von Shodan geprüften Ports auch gleich solche und ähnliche Modifikationen erfasst würden.

Wer sich schon immer fragte, wie es sein kann, dass Industriesteuerungen derart oft direkt im Internet erreichbar sind, dem gab Matherly eine verblüffende Antwort – der Hintergedanke sei in vielen Fällen vermutlich vermeintliche Sicherheit gewesen. Viele Planer solcher Strukturen haben sich auf die Fahnen geschrieben, eine Industriesteuerung isoliert vom internen Unternehmensnetzwerk zu etablieren. Erstaunlicherweise werde dies in vielen Fällen schlicht mit Mobilfunk gelöst. Solche Systeme befänden sich dann oft direkt im Internet, ohne Firewall oder NAT, und könnten ergo von jedem Menschen weltweit angesprochen werden.

Und es kommt noch schlimmer. Zum Sicherheitsbewusstsein von Verantwortlichen solcher offener Steuerungen im Internet sagte Matherly, dass ihn unzählige Webmaster ständig anschreiben würden, warum er diesen oder jenen Webserver scannen würde. Genau das, so Matherly, würde er auch erwarten. Demgegenüber aber hätte er in all den Jahren insgesamt weniger als sage und schreibe zehn Anfragen bekommen, warum er diese oder jene Industriesteuerung scannen würde. (ur)