MEINUNGEN

STUXNET, WELCHE LEHREN LASSEN SICH ZWÖLF JAHRE SPÄTER ZIEHEN?

Vincent Nicaise
Industrial Partnership and Ecosystem Manager, Stormshield

Im Jahr 2010 entdeckte die Welt Stuxnet. Diese Malware traf damals die Automaten, die für die Zentrifugen eines iranischen Atomkraftwerks zuständig waren, und machte deutlich, wie verwundbar industrielle Umgebungen sind. Seit dieser Episode, die auf einen kleinen infizierten USB-Stick zurückzuführen war, hat sich das Cyberrisiko auf die gesamte Industrie ausgeweitet. Und mehr als zehn Jahre später wurden die Infrastrukturen von JBS Foods (Lebensmittel) und Colonial Pipeline (Energie) Opfer von Cyberangriffen und sollten ihre Produktionslinien wochenlang beeinträchtigt sehen.

Trotz der Jahre haben sich die Vorgehensweisen von Cyberangreifern weiterentwickelt, aber das industrielle Kontrollsystem von Fabriken bleibt ein beliebtes Ziel. In diesem Artikel entschlüsseln wir die Auswirkungen, die Stuxnet im Jahr 2010 hatte. Welches Vermächtnis hat dieser Angriff den Cyberkriminellen des Jahres 2022 hinterlassen? Was haben die Industriellen daraus gelernt? Elemente einer Antwort und Blickwechsel.

STUXNET, DER ALBTRAUM FÜR INDUSTRIELLE UMGEBUNGEN

Aber **was ist denn eigentlich Stuxnet**? Im Juni 2010 wurde der Computerwurm Stuxnet auf einem Rechner eines Mitarbeiters des Atomkraftwerks Buschehr im Iran entdeckt. Ziel des Wurms war es, die Funktionsweise von Industrieautomaten der Marke Siemens umzuprogrammieren, um den ordnungsgemäßen Betrieb der Zentrifugen zu beeinträchtigen und so das in der Entwicklung befindliche iranische Atomanreicherungsprogramm zu stoppen.

Der Wurm infizierte 30.000 Computeranlagen im ganzen Land und wurde später auch in Deutschland, Frankreich, Indien und Indonesien entdeckt, wodurch die Zahl der kompromittierten Anlagen auf 45.000 anstieg. Aufgrund seiner Konzeption hätte Stuxnet jedoch eine unauffindbare Malware sein müssen. Diese konnte die an die Automaten gesendete Kommunikation analysieren und sich durch eine seitliche Verschiebung selbst auf einem Host installieren. Dazu analysierten die Cyberangreifer die Funktionsweise der OT-Kommunikationsprotokolle und entdeckten technische Schwächen im Zusammenhang mit der Authentifizierung. **Marco Genovese**, Pre-Sales Engineer und Industrieexperte bei Stormshield, erklärt: „*Die Schöpfer von Stuxnet haben für ihren Angriff die fehlende Authentifizierung und Verschlüsselung des S7-Protokolls von Siemens sowie das Fehlen einer Anti-Replikationskontrolle ausgenutzt. Diese Schwäche führte zu der Erkenntnis, dass diese OT-Protokolle eine Sicherheitsschicht hätten einbetten müssen. Dieser zusätzliche Sicherheitsbedarf wird später in der zweiten Version des Protokolls namens S7 Plus implementiert. Leider verwenden auch heute noch viele Industrieunternehmen dieses Protokoll in der Version von 2010.*“Dieser Angriff basierte auf einer Reihe von Zero-Day-Schwachstellen im Windows-Betriebssystem und zielte auf das Prozessleitsystem (SCADA) ab. Dieser Cyberangriff war für viele **der erste gezielte Angriff, der es ermöglichte, die Funktion von Industriemaschinen in einer hochsicheren Umgebung zu beeinträchtigen**. Die Kompromittierung eines solchen industriellen Steuerungssystems, das nicht mit dem Internet verbunden ist, schien zu diesem Zeitpunkt eine äußerst komplexe Aufgabe zu sein, da 2010 Cyberangriffe hauptsächlich auf IT-Umgebungen abzielten. Stuxnet war der erste bekannte Angriff auf OT-Umgebungen und führte zu der Erkenntnis , **dass die Industrie nun selbst zum Opfer werden könnte.** Vor dieser Episode hatten die Komplexität des industriellen Umfelds und die Schwierigkeit der Umsetzung darauf hingedeutet, dass ein Angriff auf diese Art von Zielen keine lohnende Investition darstellte.

Und um einer solchen Komplexität gerecht zu werden, erforderte die Entwicklung dieser Malware **erhebliche finanzielle und personelle Mittel**, um die Funktionsweise des iranischen Atomanreicherungsprogramms und der technischen Infrastruktur von Siemens zu verstehen. All diese Arbeit ermöglichte es, Schicht für Schicht Kompromittierungspunkte zu entwickeln, mit dem Ziel, am Ende der Kette die S7-300-Steuerung zu erreichen, die für die Drehzahlregler der Zentrifugen zuständig ist. Für **Ilias Sidqui**, Senior Consultant bei Wavestone, hat die Komplexität des Angriffs schnell dazu geführt, dass er einem staatlichen Akteur zugeschrieben wurde: „*Um diese*

Malware entwickeln zu können, musste ein identisches Modell gebaut werden, indem sehr teure Industriehardware erworben wurde, was Kenntnisse über die Versionen der im Iran verwendeten Maschinen voraussetzte. Die Komplexität all dieser Parameter machte also schnell deutlich, dass nur ein oder mehrere Staaten in der Lage waren, solche Mittel einzusetzen."Eine Kombination von Zero-Day-Angriffen, die Kompromittierung eines Informationssystems mithilfe eines USB-Sticks, seitliche Verschiebung, Diebstahl von Administratorenzugang, die Fähigkeit, die Steuerung umzuprogrammieren... Ohne es zu wissen, legte dieser Wurm die Grundlage für eine neue Komplexität in der Cyberkriminalität.

„Die Komplexität all dieser Parameter machte also schnell deutlich, dass nur ein oder mehrere Staaten in der Lage waren, solche Mittel einzusetzen."

Ilias Sidqui, Senior Consultant Wavestone

Durch die Erfüllung seines Hauptzwecks hat Stuxnet geopolitische Geschichte geschrieben. *„Es gab eindeutig ein Vorher und ein Nachher von Stuxnet, und auch die NATO-Verbündeten haben sich nicht geirrt, als sie im Juli 2016 auf dem Warschauer Gipfel den Cyberspace als vollwertigen Bereich für militärische Operationen anerkannten, genauso wie Land, See und Himmel*", sagt **Fabien Miquet**, Officer of Product Security & Solutions bei Siemens. Der Wurm hat aber auch aufgrund seiner technischen und strategischen Hinterlassenschaften, die später von den wichtigsten Gruppen von Cyberangreifern für die kommenden Jahrzehnte wiederverwendet wurden, Geschichte in der Cybersicherheit geschrieben.

DIE VIELFÄLTIGEN HINTERLASSENSCHAFTEN VON STUXNET

Von der Demonstration der Machbarkeit eines solchen Angriffs bis hin zum innovativen Charakter der Vorgehensweise werden Cyberangreifer nach Stuxnet zwangsläufig von diesem Angriff beeinflusst worden sein. Zwölf Jahre nach seiner Entdeckung ist **er aufgrund seiner technischen und schwierigen Umsetzung bis heute ein Fall für die Schule**. Es ist der erste Wurm einer wachsenden Malware-Familie und wird für immer der erste Wurm bleiben, der sich der Kompromittierung von industriellen Kontrollsystemen widmet.

Und bei dieser Demonstration des Eindringens in und der Kompromittierung einer hochsicheren Umgebung wird Stuxnet Berufungen auslösen und einige Monate später kopiert werden. Auch wenn sich die Angriffstechniken und -vektoren unterscheiden, wird das Ziel bei mehreren Cyberangriffen, die weltweit folgen, dasselbe bleiben: Industrieautomaten ins Visier zu nehmen. Von Russland bis zum Iran wird diese Malware in einer eigenen Familie kategorisiert, die als „*Stuxnet-like*" bezeichnet wird. Bereits im Jahr 2012 wurden die Unternehmen Saudi Aramco und RasGas Opfer

eines Cyberangriffs, der dem iranischen Staat zugeschrieben wurde. Die Neuerung im Vergleich zu Stuxnet wird darin bestehen, dass eine Ransomware, in diesem Fall Shamoon, verwendet wird, um die Aktivitäten dieser Industrieunternehmen lahmzulegen. Im Jahr 2013 ist es das Kontrollsystem der Entlastungsventile des Bowman-Staudamms in den USA, das kompromittiert wird. Laut einer Untersuchung des Wall Street Journal soll dieser Angriff eine Reaktion der iranischen Behörden auf Stuxnet sein. 2015 werden die Öfen eines Stahlwerks in Deutschland wiederum Opfer eines Cyberangriffs. Der deutsche Geheimdienst definiert den Angriff als „*Stuxnet-ähnlichen*" Angriff, Details und Auswirkungen des Angriffs werden jedoch nicht bekannt gegeben. Zur gleichen Zeit wurde auch die Ukraine von Malware heimgesucht, die diesmal auf die elektrischen Anlagen des Landes abzielte, und zwar mit den Malware-Programmen „*Black Energy*" und „*CrashOverride*" im Jahr 2015 und „*Triton*" im Jahr 2017. Angriffe, die den Aktionen russischer Cyberkriminellengruppen zugeschrieben wurden und vor allem die Entwicklung der Bedrohung veranschaulichten: „*Während der Black-Energy-Angriff die Möglichkeit demonstrierte, ein Kraftwerk ohne besondere Kenntnisse über industrielle Nachrichten auszuschalten, zeigte der Triton-Angriff die Verwundbarkeit des Schutzsystems des OT-Netzwerks selbst auf*", erläutert Marco Genovese.

Parallel zu den Cyberangriffen hat auch die Vorgehensweise von Stuxnet die Cybersicherheitsforscher beeinflusst. Im Jahr 2015 schufen deutsche Forscher einen weiteren Computerwurm namens PLC Blaster, der die neueste Generation von Siemens-Steuerungen der S7-Reihe ins Visier nehmen konnte, indem er einen Teil der Vorgehensweise von Stuxnet übernahm. Und wo Stuxnet einen Host-Rechner benötigte, der mit dem Industrienetzwerk verbunden war, kann die Malware PLC Blaster die Steuerungen untereinander direkt über das TCP/IP-Protokoll infizieren. Derwährend der Black Hat USA-Konferenz vorgestellte Konzeptnachweis zeigte, wie anfällig Industrieumgebungen sind und wie leicht sich der Wurm von einem Gerät zum anderen verbreiten kann.

KÖNNTE DER STUXNET-ANGRIFF NOCH OPFER FORDERN?

Ist ein Angriff wie Stuxnet im Jahr 2022 denkbar? Eine relevante Frage und die Antwort ist für Ilias Sidqui eindeutig: „*Ein Stuxnet-ähnliches Szenario ist auch 2022 noch möglich. Denn das Prinzip bleibt das gleiche; es gab, gibt und wird immer Zero-Days-Lücken geben, die Cyberkriminellen einen offensiven Vorteil verschaffen. Ein Angriff ist also immer noch möglich, aber nicht mehr unbedingt gegen die Atomindustrie*", sagt Marco Genovese: „*Es wird heutzutage sicherlich schwieriger sein, einen mit Stuxnet vergleichbaren Angriff auf ein Atomkraftwerk durchzuführen, aber die jüngsten Aktionen in der Ukraine zeigen, dass es nun möglich ist, physische Energienetze (Wasser, Gas, Strom) mit einem Cyberangriff zu beeinträchtigen.*"

Wichtig ist auch, dass bei den letzten bedeutenden Cyberangriffen keine sehr fortschrittlichen Vorgehensweisen verwendet wurden. Die Cyberangriffe auf Colonial Pipeline und JBS Foods ähneln im Übrigen eher opportunistischen Handlungen als geplanten Angriffen wie Stuxnet. Da bei Colonial Pipeline ein im Darkweb geleaktes Passwort und bei JBS Foods eine bekannte Schwachstelle in einem Fernverbindungstool verwendet wurde, war die Schwierigkeit des Eindringens und der Durchführung weit weniger komplex als bei Stuxnet. Denn de facto **wächst die Angriffsfläche für Industrieunternehmen**. Dieser Trend lässt sich seit einigen Jahren durch die Annahme einer IT/OT-Konvergenz in den Informationssystemen erklären. Ein gefundenes Fressen für Cyberkriminelle. Heutzutage *sind IT-Umgebungen, klassische Büroumgebungen und industrielle OT-Umgebungen miteinander vernetzt*", erklärt Ilias Sidqui. *Ein Gateway, das auch von Gruppen von Cyberkriminellen genutzt wird; spezielle Entwicklungen oder die Suche nach Zero-Day-Schwachstellen sind daher nicht mehr nötig. Aus diesem Grund werden immer mehr Ransomware-Angriffe beobachtet, die auf industrielle Umgebungen abzielen. „Die beschleunigte Digitalisierung bringt schließlich Chancen für alle mit sich: Sie, ich, unsere Kunden ... aber auch für Angreifer auf unsere immer stärker vernetzten Systeme*", ergänzt Fabien Miquet. *Das ist alles andere als ein unabwendbares Schicksal, man muss sich dessen nur bewusst sein, und wir haben gewissermaßen eine Warnpflicht: keine Digitalisierung ohne Cybersicherheit!*"

Aber wie **reif ist denn der Industriesektor angesichts dieser Bedrohung?** Eine Zahl von Gartner, die erklärte, dass 60 % der erfolgreichen Angriffe im Jahr 2020 auf der Ausnutzung bekannter, aber nicht behobener Schwachstellen beruhen würden, gibt einen ersten Hinweis auf die Antwort ... In unserem Barometer 2021, das der Cybersicherheit in operativen Netzwerken gewidmet ist, gaben 51 % der Befragten an, mindestens einen Cyberangriff auf ihr operatives Netzwerk erlebt zu haben. Und 27 % hatten bereits einen Produktionsstopp oder eine Produktionsstörung erlebt. Dennoch gibt es viele Ansatzpunkte für Schutzlösungen. Aufspüren von Schwachstellen, Patchmanagement, Netzwerksegmentierung, Schulungen ... Lösungen für die Cybersicherheit scheinen bei der Umsetzung im industriellen Umfeld vor einer Herausforderung zu stehen. Wie Fabien Miquet bestätigt: „*Es ist in der Tat eine echte Herausforderung, eine Fabrik zu sichern, deren oberstes Ziel nicht die Weiterentwicklung ihrer Technologien ist, sondern eine stabile und nachhaltige Produktion. Und es spielt keine Rolle, ob diese Technologien „insecure by design" sind; die Tatsache, dass sie seit dreißig oder vierzig Jahren funktionieren, reicht vielen Industriellen auch heute noch, selbst wenn sie nicht für die Implementierung von Cybersicherheit konzipiert wurden. Die Mentalitäten ändern sich definitiv nicht alle mit der gleichen Geschwindigkeit. Dies hängt in der Regel von der Häufigkeit der Cyberangriffe ab ... Als Reaktion auf diese Ereignisse hat Siemens neue Sicherheitsmechanismen in seine Maschinen implementiert. Dazu haben wir gute Praktiken aus der IT in die OT-Welt importiert, z. B. am Beispiel unserer Automaten, die nun das für seine Robustheit bekannte und anerkannte Verschlüsselungsprotokoll TLS enthalten.*"

So haben die Autoren von Stuxnet, ohne es zu wissen, die Komplexität von Cyberangriffen in OT-Umgebungen weitgehend beeinflusst und weiterentwickelt. Und die Konvergenz der IT/OT-Umgebungen scheint es Angreifern zu erleichtern, sich von einer Umgebung in eine andere zu bewegen. Es wird interessant sein zu beobachten, wie sich OT-Manager in den nächsten Jahren anpassen werden, um technische Schulden, die Koexistenz von OT/IT-Umgebungen, den Einsatz neuer Technologien und Cybersicherheit unter einen Hut zu bringen. Ein umfangreiches Programm.