Die erste Cyberwaffe und ihre Folgen

spiegel.de/netzwelt/web/die-erste-cyberwaffe-und-ihre-folgen-a-a0ed08c9-5080-4ac2-8518-ed69347dc147

2008: Der damalige iranische Präsident Mahmoud Ahmadinejad besichtigt die Urananreicherungsanlage Natanz

Foto: HO/ AFP

Am 17. Juni 2010 schrieb Sergey Ulasen in holprigem Englisch ein Stück Computergeschichte. "Current malware should be added to very dangerous category", heißt es in seinem kaum 20 Zeilen langen Eintrag auf der Website von VirusBlokAda , der kleinen weißrussischen Antivirus-Firma, für die er damals arbeitete.

Ulasen beschreibt darin eine bis dahin unbekannte Schadsoftware, die sich über USB-Sticks verbreitet und einen neuartigen Trick beherrscht, um sich unbemerkt auf Windows-Systemen zu installieren. "Es hat ungefähr eine Woche gedauert, bis wir ihn identifiziert hatten", sagt er heute.

Sergey Ulasen

Foto: Kaspersky Lab

Was Ulasen damals nicht wusste: Er hatte gerade die erste echte Cyberwaffe der Geschichte in die Öffentlichkeit gezerrt - ein Meisterwerk, das noch viele weitere Überraschungen in sich trug. Es sollte Monate dauern, bis das wahre Potenzial der Schadsoftware ansatzweise klar wurde. Bekannt wurde sie unter dem Namen Stuxnet.

"Überrascht" sei er damals gewesen, sagt er, und "wahrscheinlich verängstigt". Denn ihm war zumindest eines sehr schnell klar: Dieser Installationstrick, den er durchschaut hatte, würde garantiert auf jedem Windows-PC der Welt funktionieren. Denn Microsoft selbst hatte keine Ahnung von der Schwachstelle in seinem Betriebssystem. Zero-Day-Exploit wird so etwas genannt.Hunderte Millionen Computer wären dagegen machtlos gewesen.

Ein Exploit ist eine Schadsoftware, die eine Sicherheitslücke ausnutzt. Ist diese Sicherheitslücke dem betroffenen Hersteller nicht bekannt, spricht man von einem Zero-Day-Exploit: Der Hersteller hat null Tage Zeit, eine Abwehrmaßnahme zu entwickeln, bevor ein Angriff Erfolg hat.

Die Schwachstelle selbst wird dementsprechend als Zero-Day bezeichnet. Alternative Schreibweise: 0day.

Das Wissen um solche Schwachstellen, insbesondere aber fertige Exploits, wird gehandelt. Hersteller bieten Sicherheitsforschern im Rahmen sogenannter Bug-Bounty-Programme Geld für neu gefundene Lücken an, damit sie ihre Produkte updaten können, bevor es einen

Angriff gibt. Geheimdienste und Strafverfolger kaufen oder entwickeln ebenfalls Exploits, um Verdächtige überwachen zu können. Und auch Kriminelle kaufen und verkaufen Exploits, um mit ihrer Hilfe zum Beispiel Erpressungstrojaner (Ransomware) zu verteilen.

Denn nicht immer ist ein Zero-Day-Exploit gleichbedeutend mit der Fähigkeit, ein Gerät komplett fremdsteuern zu können. Verschiedene Sicherheitsmaßnahmen zumeist auf Betriebssystemebene, die wie Trennwände funktionieren, verhindern das. Mitunter sind also ganze Ketten von Exploits nötig, um ein Opfer wirklich zu hacken und etwa ihre Daten abzugreifen oder weitere Schadsoftware nachladen und installieren zu können. Die berühmte Malware Stuxnet zum Beispiel beinhaltete gleich vier Zero-Day-Exploits.

Die Preise variieren je nach Aufwand, Ziel (Browser, Betriebssysteme, Schnittstellen, Anwendungen etc.) und Wirkung stark. Manche werden für einige Hundert oder Tausend Dollar gehandelt, andere sind Händlern wie Zerodium zufolge bis zu 2,5 Millionen Dollar wert.

Stuxnet, stellte sich später heraus, beinhaltete gleich vier Zero-Day-Exploits. Aber die Schadsoftware sollte nicht möglichst viele Rechner befallen, sondern ganz bestimmte: die in der iranischen Urananreicherungsanlage bei Natanz. Dort sollte sie still und heimlich die Zentrifugen sabotieren und so das iranische Atomprogramm behindern.

"Operation Olympic Games" war der Codename für das gemeinsame Unterfangen der USA und Israels, das nie offiziell bestätigt wurde. Doch die Enttarnung des Sabotage-Programms beendete die Operation - und wird gleichzeitig als Beginn der Cyberkrieg-Ära verstanden.

"Das vielleicht wichtigste Ereignis des ganzen Jahrzehnts"

Costin Raiu, Kaspersky

Costin Raiu, Leiter des Bereichs Forschung und Entwicklung bei Kaspersky Lab, wo auch Ulasen heute arbeitet, nennt dessen Fund "das vielleicht wichtigste Ereignis des ganzen Jahrzehnts". Es habe "so ziemlich alles in der IT-Sicherheitsindustrie verändert", sagt er im Gespräch mit dem SPIEGEL: "Die Art, wie wir über Bedrohungen nachdenken, die Art, wie wir gegen Cyberattacken kämpfen, was möglich ist und was in den kommenden Jahren passieren wird."

Auch für Ralph Langer war Stuxnet "der große Knalleffekt", wie er im Gespräch sagt. Der Beweis, dass etwas, wovor Sicherheitsexperten lange gewarnt hatten, "keine Fiktion ist". Langners Firma gehört zu den wenigen, die sich auf die Cybersicherheit von großen Produktionsanlagen und kritischen Infrastrukturen spezialisiert haben.

Zusammen mit zwei Kollegen hatte Langner 2010 die Payload von Stuxnet entschlüsselt, jene Teile des Codes, die jenseits von Windows-PCs wirksam wurden - nämlich in den von Siemens entwickelten Industriesteuerungsanlagen (Industrial Control Systems, kurz ICS) in Natanz.

"Das Geniale an Stuxnet war, dass es sich um eine Cyberwaffe handelte, die völlig autonom arbeitet", sagt Langner. "So etwas hatten wir vorher noch nie gesehen. Insbesondere in der frühen Version gab es keine Möglichkeit, sie fernzusteuern. Und obwohl wir uns schon damals Tag und Nacht mit diesen Dingen beschäftigt und uns mögliche Angriffsszenarien ausgedacht hatten, gegen die wir unsere Kunden beschützen wollten, wären wir nie im Leben auf die abgefahrenen Dinge gekommen, die wir dann im Stuxnet-Code gesehen haben."

"Damals hat man von einem Weckruf gesprochen"

Ralph Langner

Zum Beispiel sei die Software in der Lage gewesen, zunächst normale Sensorwerte in der befallenen Industriesteuerungsanlage aufzuzeichnen und sie anschließend immer wieder abzuspielen. Dadurch sah für die interne Logik der Anlage alles normal aus, und Stuxnet konnte die automatisierten Sicherheitsvorrichtungen – die sogenannten Safety-Steuerungen – umgehen. "Die aber braucht man überall dort, wo einem Dinge richtig um die Ohren fliegen können", sagt Langer, "wo es Explosionen geben oder wo toxische Substanzen freigesetzt werden könnten. Ein menschlicher Bediener wäre nicht in der Lage, schnell genug zu reagieren."

Stuxnet ist ein Computerwurm, der vermutlich 2007 erstmals eingesetzt und 2010 entdeckt wurde. Die sich selbst verbreitende Schadsoftware (Malware) wurde eingesetzt, um unbemerkt das damalige iranische Atomprogramm zu behindern, insbesondere die Urananreicherungsanlage bei Natanz. Dort beschädigte Stuxnet letztlich Zentrifugen. Es gab jedoch mehrere Versionen von Stuxnet, die sich in ihren Eigenschaften und Fähigkeiten unterschieden. Entdeckt wurde zuerst eine neuere, aggressivere Variante, die sich weiter ausgebreitet hatte als beabsichtigt.

Stuxnet gilt als erste bekannt gewordene Malware, die physische Schäden anrichtete. Sie war zudem komplexer als alles, was IT-Sicherheitsforscher bis dahin je gesehen hatten. Nach der Entdeckung dauerte es Monate, bis sie annähernd verstanden hatten, was Stuxnet konnte. Auf welchen Systemen Stuxnet aktiv wurde und auf welchen nicht, wie sie sich die Malware versteckte und selbst löschte, wie sie den Sprung von einem Windows-Computer in eine Steuerungsanlage für Zentrifugen schaffte, mit der sich nur wenige Spezialisten auskennen, und wie sie dort ihre Spuren verschleierte, all das verblüffte die Experten damals zutiefst.

Offiziell bestätigt wurde es nie, aber es gilt als wahrscheinlich, dass die USA und Israel für die Entwicklung von Stuxnet verantwortlich waren. Der US-Journalist David E. Sanger von der "New York Times" schrieb, das Programm sei von US-Präsident George-W. Bush autorisiert und in der Amtszeit seines Nachfolgers Barack Obama weiterentwickelt worden.

Kim Zetter, die Autorin des Standardwerks zu Stuxnet, "Countdown to Zero-Day", hält den Einsatz von Stuxnet für mäßig erfolgreich. Der Fortschritt von Irans Atomprogramm sei damit nur geringfügig verlangsamt worden.

Doch auf den vermeintlichen großen Knall folgte Stille. "Damals hat man von einem Weckruf gesprochen", sagt Langner, "komischerweise ist man aber sehr schnell wieder in den Tiefschlaf übergegangen. Ich kann das eigentlich auch keinem Unternehmen und keinem Politiker verdenken. Denn in den vergangenen zehn Jahren ist in dem Bereich so gut wie nichts passiert." Nachgewiesene Cyberangriffe auf Industrieanlagen habe es nur "ungefähr eine Handvoll" gegeben. "Aber die Risiken sind nicht verschwunden, sondern werden immer größer, weil immer mehr digitalisiert wird."


Ralph Langner

Foto: Christian Science Monitor/ Getty

Industriesteuerungsanlagen seien immer noch so schlecht geschützt wie damals, "das ist Fakt". Langner weiß, wie es in dieser Hinsicht in entsprechenden Unternehmen aussieht und für wie viele Sicherheitslücken sie anfällig wären: "Das sind Zahlen, da schlackern Sie mit den Ohren."

Er will den Herstellern der Steuerungsanlagen aber "keinen Vorwurf machen". Deren Kunden, also die Betreiber von Industrieanlagen, hätten schlicht "keine Bereitschaft gezeigt, für zusätzliche Cybersicherheit tiefer in die Tasche zu greifen". Das liege an der Komplexität und dem Ausmaß des Problems: "Stellen Sie sich einen großen Automobilhersteller vor. Bei dem geht es ja nicht um drei Industriesteuerungen, sondern vielleicht um 30.000. Wenn Sie da zum Beispiel Mehrkosten von 1000 Euro pro Stück ansetzen, kommt einiges zusammen." Außerdem kämen höhere Wartungskosten dazu, und die Netzwerktechnik rund um die Steuerungsanlagen sei ebenfalls inhärent unsicher.

Erschwerend komme hinzu, dass in der Industrie häufig noch PCs mit veralteten Windows-Versionen wie XP oder Windows 7 eingesetzt würden, für die es keine Sicherheitspatches mehr gibt. Und selbst wenn es sie gibt, würden sie manchmal ignoriert, sagt Langner, weil so ein Update mitunter dafür sorge, dass eine Industrieanwendung nicht mehr läuft. Auch könnten die Anlagen nicht mal eben neu gestartet werden wie ein Desktop-PC, denn sie müssten 24 Stunden am Tag laufen.

Aber ausgehend von "einer statistisch orientierten Risikobetrachtung", sagt Langner, sei die Gefahr eben gering, da steckten Unternehmen ihr Geld vielleicht lieber in verbesserten Brandschutz oder in den Umweltschutz. Er wolle auch keine Angst schüren. Wichtig sei, dass Cybersicherheit nicht als Projekt innerhalb einiger Monate erledigt und abgehakt werden könne, sondern langfristig und top-down, ausgehend von der Chefetage, angegangen werden müsse.

"Ich hatte große Angst", sagt ein IT-Experte

Angebote gibt es reichlich, auch wenn die meisten auf die klassische IT von Unternehmen ausgelegt sind, nicht auf die OT, die Operations Technology. Die Branche ist mittlerweile so groß, dass es jährlich aktualisierte Listen der Top-500-Cybersicherheitsfirmen gibt. Große Anbieter wie Kaspersky haben nach Stuxnet spezialisierte Teams aufgebaut, die sich ausschließlich um die Analyse besonders ausgeklügelter Angriffe kümmern. Ihre Gegner sind mitunter Geheimdienste oder andere staatlich unterstützte Organisationen – was zu vormals undenkbaren Kollisionen führt.

Mitte 2012 zum Beispiel entdeckten Costin Raiu und sein Team die Spionagesoftware Flame auf Rechnern von iranischen Kunden – und darin eine Verwandtschaft zu Stuxnet , die auf eine Zusammenarbeit der Entwickler hindeutete. "Wir sahen damals Anzeichen dafür, dass unsere Arbeit bestimmten Leuten nicht gefiel", sagt er. "Während einer Konferenz in München verfolgten uns Menschen von der Hotellobby bis zu unseren Zimmern und taten dabei so, als würden sie telefonieren. Es gab mehrere solche Vorfälle. Vielleicht wollte man uns nur Angst einjagen, aber das hat funktioniert: Ich hatte große Angst."

Für eine Weile habe das Team dann aufgehört, diese Art Forschung zu betreiben und entsprechende Erkenntnisse zu verkünden. "Wir befürchteten physische Vergeltung gegen uns und unsere Familien", sagt der IT-Experte. Solche Ängste gab es in der Branche noch nicht, als Hacker entweder profitgetriebene Kriminelle oder ideologisch motivierte Aktivisten waren.

Bis heute sind nicht alle Rätsel rund um Stuxnet gelöst. Noch immer suchen manche nach Antworten. So hat Kim Zetter, die Autorin des Standardwerks zu Stuxnet, "Countdown to Zero-Day", erst im vergangenen September erfahren, dass es der niederländische Geheimdienst war, der einen Mann in die Urananreicherungsanlage Natanz einschleusen konnte , um die erste Version von Stuxnet auf einem präparierten USB-Stick ins Innere zu

bringen. Was aus ihm wurde, ist öffentlich nicht bekannt. Costin Raiu sagt: "Stuxnet wird sich bald wie Paläontologie anfühlen. Aber so wie manche Menschen gern Dinosaurier erforschen, untersuchen andere eben Cyberdinosaurier."

Früher oder später wird es weitere Stuxnets geben, spätestens im Kriegsfall, da ist sich Ralph Langner sicher. Zu Friedenszeiten könnten es mittlerweile aber auch Kriminelle schaffen, Schadcode für ICS zu entwickeln, glaubt er. Und es gebe dabei einen wichtigen Unterschied zu regierungsgestützten Angriffen, wie es Stuxnet war: "Bei einem politisch oder militärisch motivierten Cyberangriff möchten Sie beim ersten Schuss treffen, sonst verpufft er. Kriminelle hingegen können es sich leisten, zu experimentieren. Es kann ihnen egal sein, ob ihr Schadcode entdeckt und analysiert wird. Die Betreiber von Industrieanlagen können sich nicht von heute auf morgen schützen."