Erpressung durch Hacker: Cyberattacke in der Keksfabrik

http://www.spiegel.de/netzwelt/web/erpressung-durch-cyberattacken-angriffsziel-industrieanlage-a-1048034.html

Von Uli Ries

imago

Fabrik (Symbolbild): Die Steuerungsanlagen stehen oft ungeschützt im Netz

Hacker richten mit Cyberangriffen nach Schätzungen von Experten Schäden von Hunderten Millionen Euro an. Sichtbar werden die Attacken auf die Industrie aber selten: Den Tätern geht es um Erpressung.

-
-
-
-

Als die Konstrukteure einer kanadischen Keksfabrik gefragt wurden, welche Folgen sie sich durch Cyberangriffe auf die Anlage vorstellen könnten, antworteten sie: "versalzenen Keksteig". Mehr als der Verlust einer Tagesproduktion sei durch eine bösartige Manipulation nicht zu erwarten, dachten die Ingenieure. Leider falsch.

Tatsächlich stand die Fabrik komplett still, nachdem Unbekannte in deren Netzwerk eingedrungen waren. Die von den Angreifern zur Analyse des Netzes verwendete Software brachte die Steuerungscomputer der Fabrik aus dem Tritt.

Die empfindlichen SPS-Systeme (**S**peicher**p**rogrammierbare**S**teuerung) reagierten mit Chaos: Die Produktion brach zusammen, vorproduzierter Teig trocknete in den Transportrohren ein. Die Verstopfungen waren so hartnäckig, dass die Rohre schließlich herausgeschnitten werden mussten.

Firmenspionage für Spekulanten

Ob der Ausfall ein unglücklicher Nebeneffekt oder gezielte Sabotage war, sei unklar, sagt der auf Industriesteuerungsanlagen spezialisierte IT-Experte Jason Larsen. Das Unglück war wohl kein Einzelfall. Larsen geht davon aus, dass Unternehmen bereits Hunderte Millionen Dollar an Erpresser gezahlt haben, die damit drohen, Produktionsanlagen mit Cyberangriffen zu stoppen.

An die Öffentlichkeit dringen diese Vorfälle in der Regel nicht, wie Larsen erklärt. Nur in kleinen Kreisen würden sie diskutiert - oder ganz unter den Teppich gekehrt. So wie einige Vorfälle, bei denen jüngst die Produktionsnetzwerke von Öl- und Gasunternehmen infiltriert wurden.

Die Eindringlinge sammelten dabei Informationen über den Stand der jeweiligen Vorräte und beobachteten, wie diese sich veränderten. Nutznießer - und eventuell auch Auftraggeber - der Spähaktion, sollen Spekulanten gewesen sein, die durch steigende oder fallende Rohstoffpreise Kasse machten und frühzeitig informiert sein wollten.

Uli Ries

Ergebnis des Angriffs auf eine simulierte Whiskey-Destillerie: Jason Larsen, Experte für Industriesteuerung, ließ während der Hackerkonferenz Def Con ein Fass implodieren, indem er die Druck- und Temperaturkontrolle manipulierte.

Warum davon nichts nach außen dringt? Jeff Moss, Gründer der Hackerkonferenzen Black Hat und Def Con sowie Berater der US-Heimatschutzbehörde, erklärt das unter anderem damit, dass betroffene Unternehmen Imageschäden verhindern wollen.
"Die gehen nur dann an die Öffentlichkeit, wenn sich der Ausfall nicht verbergen lässt

- weil es beispielsweise eine Explosion gab", so Moss. Er fordert eine gesetzliche Pflicht, Cyberattacken zu melden.

Kein Interesse an Verwüstung

Das Beispiel der Keksfabrik zeige laut Jason Larsen, wie unterschiedlich IT-Experten und Produktionsfachleute bei ihren Risikoanalysen vorgehen. Für Produktionstechniker gehörten Fehlfunktionen zum Alltag, bösartige Manipulationen hingegen nicht. Entsprechend löchrig fällt aus IT-Sicht das Schutzkonzept aus.

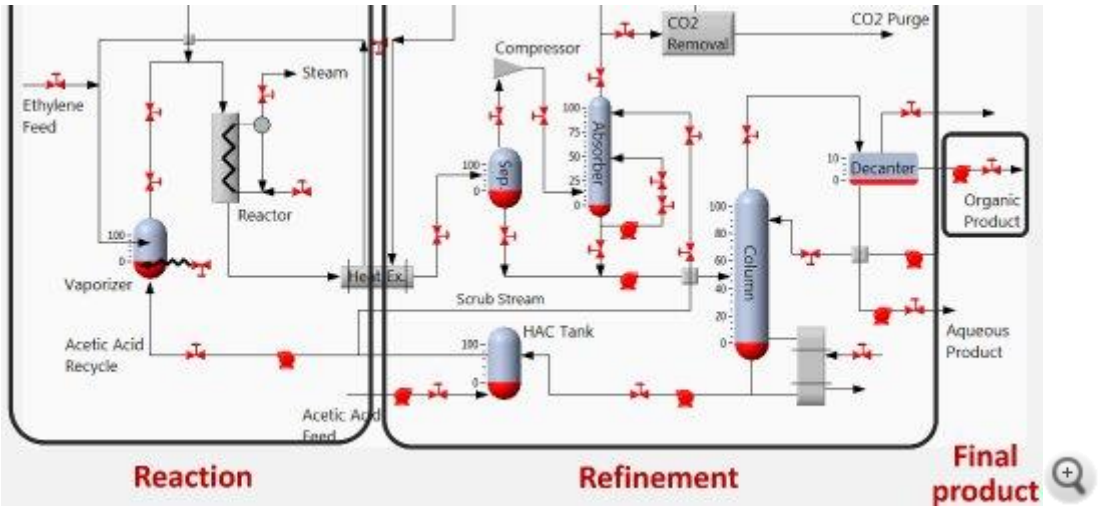
Das führt dann zu Phänomenen wie jenem, das Johannes Klick und Stephan Lau von der Freien Universität Berlin schildern: Anfang August seien rund 28.000 SPS-Systeme für jedermann völlig ungeschützt im Internet erreichbar gewesen, erklären die Experten.

Im Rahmen der Sicherheitskonferenz Black Hat zeigten sie ein Programm, mit dessen Hilfe sie eigene Software auf solche im Netz sichtbaren Geräte einschleusen können. Angreifer mit kriminellem Hintergrund könnten auf diese Weise eigene Kommandos an die Steuergeräte weitergeben und so ganze Fabriken manipulieren. Laut Jason Larsen sind solche sogenannten SPS-Rootkits im digitalen Untergrund seit zehn Jahren bekannt.

Dass über derartige Angriffe nichts nach außen dringt, liege auch daran, dass sie meist keine sichtbaren Schäden hinterlassen. Die Erpresser drohten nur mit dem Stopp der Produktion, hätten aber kein Interesse an Verwüstungen.

Kein Angriffsziel für Amateure

Ein weiterer Grund, weshalb spektakuläre Angriffe auf Industrieanlagen ausbleiben, dürfte laut Marina Krotofil von der Technischen Universität Hamburg die Komplexität solcher Angriffe sein. Sie selbst hat einen Angriff auf eine Fabrik zur Herstellung von Vinylacetat simuliert. Ihre Erkenntnis aus dem Experiment: Eine solche Attacke ist außerordentlich komplex, zumal wenn kein sichtbarer Schaden angerichtet werden soll.



Marina Krotofil

Nichts für Anfänger: Die simulierte Anlage zur Produktion von Vinylacetat muss an der genau passenden Stelle manipuliert werden, um den Ausstoß zu senken, ohne gleichzeitig die Produktion ganz lahmzulegen

In die SPS-Systeme einzudringen, sei dabei der einfache Teil. Für die weiteren Schritte seien tiefe Kenntnisse der jeweiligen Produktions- und Prozesstechnik nötig. Im Fall der simulierten Vinylacetat-Produktion müssten laut Krotofil deshalb auch Chemiker hinzugezogen werden, die den Herstellungsprozess verstehen. Erst mit deren Wissen sei ein erfolgreicher, nicht zerstörerischer Angriff möglich. "Die Kontrolle zu erlangen heißt nicht, auch Kontrolle zu haben", so Krotofil.

Terroristen bräuchten Experten

Selbst wenn eine so via Netz attackierte Produktionsanlage absichtlich oder versehentlich physischen Schaden erleidet - der Ernstfall sähe anders aus: Schlimmer wäre es beispielsweise, wenn unbemerkt die Rezeptur einer Arznei verpfuscht oder die Trinkwasserversorgung einer Stadt manipuliert würde.

Doch dazu könne es derzeit kaum kommen, glaubt Jason Larsen. Für solche Angriffe würde Terroristen wahrscheinlich einfach das Fachwissen fehlen, glaubt der Sicherheitsexperte. Zu hoffen sei deshalb, dass die Absicherung von Industrie-Steuerungsanlagen verbessert werde, bevor sich das ändert. Andernfalls sei mit Schlimmerem zu rechnen als nur mit eingetrocknetem Keksteig.