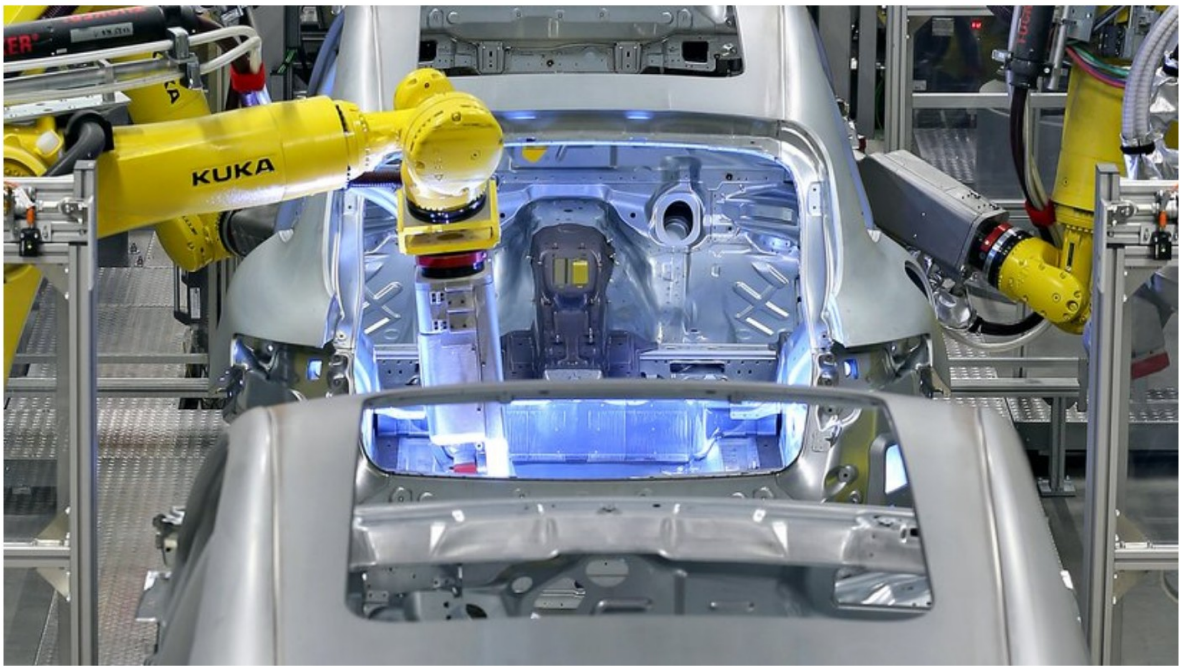
Angriff auf die Infrastruktur

Gefahr für die Weltmarktführer

Die deutsche Industrie digitalisiert ihre Anlagen in Hochgeschwindigkeit. Das verspricht reichlich Profit – für Hacker und Kriminelle.

Von **Karsten Polke-Majewski**

18. September 2015, 9:51 Uhr / 13 Kommentare



Große Teile der Autoproduktion haben längst computergesteuerte Roboter übernommen, so hier im Porsche-Werk in Leipzig. © Jan Woitas/dpa

Das größte Problem der deutschen Industrie steckt in einer Frage. Sie lautet: "Wie lange hält diese Maschine hier?" Der Ingenieur antwortet: "Mindestens zwanzig Jahre, eher länger". Der Programmierer sagt: "Bis zum nächsten Sicherheitsupdate in drei Monaten, vielleicht kürzer."

Deutschlands wirtschaftliche Stärke gründet auf seiner Industrie. Auto- und Maschinenbauer, Chemiker, Elektrotechniker und Metallverarbeiter geben Tausenden von Menschen Arbeit. Ihre Produkte stellen sie in Fabriken her, deren hochkomplexe Anlagen oft über Jahre oder sogar Jahrzehnte ohne Unterlass laufen und gleichbleibende Qualität abliefern. So war es bisher.

Doch damit könnte schnell Schluss sein.

Die Industrie digitalisiert sich in rasender Geschwindigkeit. Maschinen lernen, miteinander zu kommunizieren – nicht nur innerhalb einer Fabrik, sondern über verschiedene Standorte und sogar über Grenzen hinweg. Roboter in der Produktion merken, wenn das Material zur Neige geht und funken eigenständig nach Nachschub. Oft wissen nur noch Computer, wo in den gigantischen Lagern das gesuchte Bauteil liegt. Längst ist von einer Revolution die Rede und von einem Schlagwort: Industrie 4.0. Es verspricht goldene Zeiten für mutige Unternehmer. Und für Kriminelle.

Angriff auf die Infrastruktur

Angriff auf die Infrastruktur

Digitale Netze legen sich über die Welt und werden immer enger. Für Unternehmen, Banken und Behörden ist diese neue Infrastruktur schon genauso wichtig wie ein gutes Straßen- oder Schienennetz. Doch es droht Gefahr. Immer häufiger attackieren Hacker und Kriminelle die neuen Netze. Wie sich Unternehmen und Staat wehren können, beschreibt ZEIT ONLINE in den kommenden Tagen in einem Schwerpunkt.

Internet der Dinge: Ein Ausweis für vernetzte Toaster?

Industrie: Gefahr für die Weltmarktführer

Banken: Der Mann, der unser Geld bewacht

Denn noch nie war es so einfach, mit kriminellen Methoden bei vergleichsweise geringen Kosten und fast ohne Gefahr so viel Profit zu machen. So jedenfalls formuliert es ein Bericht von Intel Security, einem der führenden IT-Sicherheitsdienstleister. In die Systeme von Industrieunternehmen einzubrechen sei oft überraschend simpel, der Gewinn aus Erpressung und Wirtschaftsspionage gewaltig.

Ist das Panikmache einer Firma, die mit ihren Sicherheitsberatungen gutes Geld verdient? Oder doch nicht? Niemand weiß so genau, wie oft Fabriken von Hackern mit bösen Absichten angegriffen werden. Die Unternehmen erzählen es nicht, aus Angst vor dem Imageschaden. Manchmal merken sie es nicht einmal. Das Bundeskriminalamt schätzt, dass nicht einmal zehn Prozent aller Cyberattacken überhaupt bekannt werden. Der Maschinenbauerverband VDMA spricht von 30 Prozent seiner Mitgliedsunternehmen, die schon Vorfälle erlebt hätten. Zwar müssen deutsche Betriebe seit wenigen Wochen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden, wenn sie attackiert wurden. Doch es wird mindestens zwei Jahre dauern, bis aus diesen Meldungen ein halbwegs belastbares Lagebild entsteht.

Karsten Polke-Majewski

Karsten Polke-Majewski ist Leiter Investigativ/Daten von ZEIT ONLINE. Seine Profilseite finden Sie hier.

In der IT-Sicherheitsbranche kursieren mittlerweile unzählige Geschichten über Hackerattacken.

Allein Intel Security behauptet, von Hunderten Sicherheitsvorfällen berichten zu können.

Eine dieser Geschichten handelt von dem Vorstand eines Großkonzerns, der während wichtiger Vertragsverhandlungen von der Gegenseite an die Wand gespielt wurde. Hacker hatten die Kommunikation des Unternehmens ausgespäht und die Gegenseite mit Insider-Informationen ausgestattet. Ein anderer Hackerangriff soll einen weltweit agierenden Ölkonzern getroffen haben. Der Chef der Firma soll hinter vorgehaltener Hand davon erzählt haben, dass das Unternehmen Hunderte von Millionen Dollar verliere, weil wichtige Daten über die Erschließung und Erforschung neuer Ölfelder gestohlen wurden.

Im Jahresbericht des BSI ist die Geschichte von einem deutschen Stahlwerk zu lesen, das einen Hochofen abschalten musste, weil Schadsoftware dessen Steuerungseinheit infiltriert und nachhaltig beschädigt hatte.

Die Hälfte aller Unternehmen wurde schon angegriffen

Und in Großbritannien ging ein Softwarehersteller bankrott, weil Hacker sein Forum kompromittiert hatten, in dem sich Entwickler von Kunden Hilfe holen konnten. Die Hacker hatten wahllos Daten und Maschineneinstellungen gelöscht, nachdem der Softwarehersteller nicht auf ihre Lösegeldforderung eingegangen war.

Sind das nun alles Einzelfälle, oder zeichnet sich eine gefährliche Entwicklung ab? Michael Waidner arbeitet am Fraunhoferinstitut für Sichere Informationstechnologie (SIT) in Darmstadt. Es gilt als eine der führenden Forschungseinrichtungen der Welt, wenn es um IT-Sicherheit geht. Waidner schätzt, dass mindestens die Hälfte aller Industrieunternehmen – vor allem mittelständische Firmen – schon einmal Opfer digitaler Industriespionage wurde. "Große Konzerne haben eine hohe Marktmacht und können ihre Sicherheitsrichtlinien bei ihren Zulieferern durchsetzen", sagt Waidner, "das schützt sie etwas mehr". Mittelständische Betriebe, unter ihnen viele Spezialisten und oft Weltmarktführer ihres Fachs, arbeiteten hingegen oft für viele verschiedene Kunden und müssten häufig sehr unterschiedliche Standards bedienen. Da seien Fehler programmiert.

Erpressung, Spionage, Sabotage

Erpressung, Spionage, Sabotage. Diese drei Tatmotive hat Waidner beobachtet. Die Täter drohen damit, Anlagen zu beschädigen oder Daten zu zerstören und verlangen Lösegeld. Sie brechen in Datenbanken ein und stehlen geheime Verträge, Forschungsergebnisse, Patente oder Designentwürfe, manchmal im Auftrag, manchmal um sie an den Meistbietenden zu verkaufen.

Gerne nehmen sie auch unveröffentlichte Geschäftsberichte, mit denen sich die Finanzmärkte manipulieren lassen. Sie dringen in Anlagen ein und verändern die Konfigurationen von Maschinen oder die Zusammensetzung von Rezepturen, um die Qualität des jeweiligen Produkts herabzusetzen. Sie platzieren Schadsoftware in elektronischen Bauteilen, mit der sie dann wiederum die Kunden ausspähen oder schädigen können, die diese Teile kaufen.

Beliebtestes Ziel solcher Angriffe ist die Fertigungsindustrie, hat der amerikanische Telekommunikationskonzern Verizon ermittelt.

Rund 60 Prozent aller Spionageversuche richten sich gegen Firmen dieser Branche. Und sie nehmen massiv zu. Im vergangenen Jahr hat sich die Zahl der Angriffe auf solche Betriebe im Vergleich zu 2013 verdreifacht.

Deutsche Autos gelten als die sichersten der Welt, deutsche Maschinen als besonders zuverlässig. Wie kann es da sein, dass ausgerechnet die Industrie so anfällig ist für digitale Attacken? Bei Siemens, dem größten deutschen Elektronikkonzern, beschäftigt man sich schon seit zwanzig Jahren mit IT-Sicherheit. Heute leitet Rolf Reinema bei Siemens Corporate Technology das Technologiefeld IT-Security. Also: Herr Reinema, was ist da los?

Uralte Betriebssysteme

"Die zunehmende Digitalisierung führt dazu, dass Systeme, die früher abgekapselt waren, miteinander vernetzt und nach außen geöffnet werden. So werden plötzlich Systeme zugänglich, die die Produktion über Jahre oder sogar Jahrzehnte hin sicher steuern, die aus Sicht der IT-Sicherheit aber manchmal hoffnungslos veraltet sind."

Haben die Unternehmen also die Entwicklung verschlafen? "Überhaupt nicht. Ein Kraftwerk, das konstant Energie produziert, oder eine Anlage, die ein bestimmtes Bauteil, eine Komponente fertigt, läuft oft viele Jahre lang. Die Ingenieure, die sie bauen, haben nur ein Ziel: Die Sache muss funktionieren, ohne Unterbrechung, möglichst fehlerfrei. Wenn dieses Ziel einmal erreicht ist, verändern sie so wenig wie es geht, um keine neuen Fehler zu produzieren."

Aber worin liegt dann das Problem? "In den unterschiedlich schnellen Entwicklungszyklen. Ein Beispiel: Sehr viele große Anlagen laufen immer noch auf dem Betriebssystem Windows XP. Solange die Anlage keine Verbindung nach außen hat, ist das auch kein Problem. Doch Windows XP wird von Microsoft nicht mehr aktualisiert, Sicherheitslücken werden nicht mehr geschlossen. Wenn die Anlage also ans Internet angeschlossen wird, ist sie gegen Angriffe völlig ungeschützt."

Gefährliche Wartungsarbeiten

Die Unternehmen sollten also öfters mal das Betriebssystem wechseln?

"Das ist leichter gesagt als getan. Solche Anlagen bestehen aus vielen verschiedenen Komponenten, die Software und Komponenten unterschiedlicher Hersteller kombinieren. Welches Teil da wie mit wem spricht, ist häufig nicht mehr richtig zu durchschauen oder mangelhaft dokumentiert. Manchmal verbindet eine Komponente sogar zwei Systeme miteinander, die eigentlich getrennt bleiben müssten, und baut dadurch unerwünschten Besuchern eine Brücke. Offenheit und Komplexität – das sind die Widersacher der IT-Sicherheit in der Industrie."

Der dritte Feind ist die Arbeitsteilung. So ist die Verwaltung moderner Unternehmen hoch vernetzt. Auftragsannahmen, Bestellvorgänge, Lagerverwaltung, Auslieferungen – alles ist digital verbunden. Doch die dafür nötigen Office-Programme sind beliebte Eingangstüren für Hacker.

Sind sie irgendwo mit der Produktionssoftware verbunden, vielleicht auch nur, weil ein WLAN-Netz über die ganze Fabrik ausgebreitet wurde und ein Techniker eine Maschine hineingehängt hat, ist die Schutzmauer schon gebrochen.

Vergessene Hintertüren

Oder die Wartung. Fast kein Betrieb kauft mehr alle Maschinen, die er benutzt. Viele werden gemietet oder geleast. Das bedeutet, dass die Verantwortung für diese Maschinen beim Hersteller liegt. Dessen Techniker können nicht überall sein und warten die Maschinen deshalb oft aus der Ferne. Dazu benötigen sie einen Zugang. Der kann geknackt werden. "Das mietende Unternehmen lässt eine Zone im eigenen Haus zu, die es selbst nicht mehr beeinflussen kann", sagt Waidner. "Da stellt sich schnell die Frage: Wie tief kann der externe Techniker eigentlich in das System schauen? Und wie gut ist er selbst abgesichert?"

Schließlich passieren noch viele menschliche Fehler. Da muss es nicht einmal gleich um Social Engineering gehen, also um Kriminelle, die aus einzelnen Mitarbeitern durch geschicktes Charmieren Passwörter oder andere Zugangsdaten herauslocken. Programmierer bauen sich beispielsweise während der Entwicklungsphase oft Hintertüren in Systeme, um leichter zugreifen zu können. Was aber, wenn einer vergisst, diese Tür wieder zu schließen? Kunden wiederum konfigurieren Steuerungssoftware neu, um sie an ihre Systeme anzupassen, und heben dabei Schutzmechanismen auf.

Die Lösung des Dilemmas verbirgt sich in einem vielzitierten Wort: Kulturwandel. Der muss zuerst bei den Erneuerern der industriellen Welt einsetzen, bei Programmierern, Systemadministratoren, IT-Fachleuten. Sie müssen lernen, dass Betriebssicherheit genauso wichtig ist wie Datensicherheit.

Das bedeutet aber auch, dass man ein befallenes System nicht einfach abstellen und den Fehler suchen kann. Vielmehr müssen sie differenzieren: Welches System muss kontinuierlich verbessert werden? Welche Anlage muss abgekapselt werden, weil Sicherheitsupdates die Produktion beeinträchtigen könnten? Welche Abteilungen müssen scharf getrennt werden, Forschung und Produktion beispielsweise oder Fertigung und Verwaltung?

Es bedeutet auch: Selbst in einer 4.0-Industrie muss nicht jeder Sensor mit der ganzen Welt kommunizieren können. Und wer heute einen hypermodernen Verschlüsselungsalgorithmus etabliert, muss ihn so einbauen, dass man ihn auch in zwanzig Jahren noch leicht ersetzen kann.

"Außerdem brauchen Sie digitale Rauchmelder, um Angriffe möglichst frühzeitig erkennen zu können", sagt Reinema. Denn letztlich geht es um Risikomanagement. "Wenn Sie für totale Sicherheit sorgen, kann sich das Unternehmen nicht mehr bewegen. Aber ohne Freiheit ist niemand arbeitsfähig." Besser sei es, die Bedrohungslage zu kennen. Wer Angriffe bis zu einem gewissen Grad zulässt und sie genau beobachtet, der lernt, wie die Angreifer denken und was sie suchen. Dann ist es viel leichter, die wirklich wichtigen Dinge zu schützen.

Die größte Schwachstelle aber bleibt der Mensch – ob nun rachsüchtiger Mitarbeiter oder treuseliger Plauderer. Dagegen hilft nur: Grenzen setzen. Wer lediglich auf den Teil eines Netzwerks zugreifen kann, den er wirklich für seine Arbeit braucht, kann auch weniger Schaden anrichten. Vielen Mitarbeitern ist das vermutlich sogar ganz recht so.

12. Juni 2015:

Bundestag beschließt das IT-Sicherheitsgesetz

- Das Gesetz regelt unter anderem, dass Betreiber sogenannter „kritischer Infrastrukturen“ ein Mindestniveau an IT-Sicherheit

- einhalten und dem Bundesamt für Sicherheit in der

- Informationstechnik (BSI) IT-Sicherheitsvorfälle melden müssen.

- Tun sie dies nicht, droht ihnen entsprechend der beschlossenen Änderung der Regierungsvorlage ein Bußgeld.

- Ebenfalls neu eingefügt wurde in das Gesetz eine Evaluierung

- nach vier Jahren.

- Gleichzeitig werden Hard- und Software-Hersteller zur

- Mitwirkung bei der Beseitigung von Sicherheitslücken verpflichtet.

- Außerdem wird der Aufgabenbereich BSI nochmals erweitert.

Kritische Infrastrukturen

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

In Deutschland werden folgende Sektoren den Kritischen Infrastrukturen zugeordnet:

- Transport und Verkehr (Luftfahrt, Seeschifffahrt, Bahn, Nahverkehr, Binnenschifffahrt, Straße, Postwesen)
- Energie (Elektrizität, Kernkraftwerke, Mineralöl, Gas)

Anhang: 1

- Gefahrstoffe (Chemie- und Biostoffe, Gefahrguttransporte, Rüstungsindustrie)
- Informationstechnik und Telekommunikation (Telekommunikation, Informationstechnologie)
- Finanz-, Geld- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister, Börsen)
- Versorgung (Gesundheits-, Notfall- und Rettungswesen, Katastrophenschutz, Lebensmittel- und Wasserversorgung, Entsorgung)
- Behörden, Verwaltung und Justiz (staatliche Einrichtungen)
- Sonstiges (Medien, Großforschungseinrichtungen sowie herausragende oder symbolträchtige Bauwerke, Kulturgut)[1

.

T-Sicherheitsgesetz

Das **IT-Sicherheitsgesetz** (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist ein am 25.07.2015 in Kraft getretenes Gesetz[1] der deutschen Bundesregierung und resultiert nach Angaben des Bundesinnenministeriums aus der im Februar 2011 beschlossenen Cyber-Sicherheitsstrategie[2]. Zwar gibt es in Deutschland bereits mit der Allianz für Cyber-Sicherheit ein auf Freiwilligkeit beruhendes Verfahren zur Meldung von IT-Sicherheitsvorfällen der Wirtschaft. Dies soll aber nun gesetzlich vorgeschrieben werden. In der Verwaltung selbst werden, entsprechend der IT-Sicherheitsleitlinie des IT-Planungsrates, über den Verwaltungs-CERT-Verbund (VCV) zwischen Bund und den Ländern entsprechende Sicherheitinformationen ausgetauscht. Aber auch hier soll eine Meldepflicht der Länder gegenüber dem BSI auf Ebene des IT-Planungsrates eingeführt werden.

.

Inhalt

Mit dem Gesetz sollen die Betreiber besonders gefährdeter Infrastrukturen (sogenannten Kritischen Infrastrukturen) wie Energie, Wasser, Gesundheit oder Telekommunikation verpflichtet werden, Ihre Netze besser vor Hacker-Angriffen zu schützen. Neben der dann obligatorischen Meldung von IT-Sicherheitsvorfällen werden zudem Mindeststandards für die IT-Sicherheit bei den Betreibern solcher IT-Infrastrukturen branchenweit festgelegt. Dazu sollen die Branchen selbst solche Standards entwickeln, die dann vom BSI genehmigt werden. Danach sollen die Unternehmen alle 2 Jahre nachweisen, dass sie die Anforderungen noch erfüllen.

Das IT-Sicherheitsgesetz beantwortet jedoch noch nicht die Frage, welche Unternehmen konkret als Kritischen Infrastrukturen im Sinne des Gesetzes gelten. Das Gesetz definiert Kritischen Infrastrukturen lediglich abstrakt.

Für jede relevante Branche aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, sollen eigene Rechtsverordnungen zur Klärung dieser Fragestellung erstellt werden. Diese Rechtsverordnung, die alle Sektoren umfasst, liegt mit der BSI-Kritis-Verordnung nun vor.

Allerdings musste das IT-Sicherheitsgesetz auf Grund der zwischenzeitlich Anfang Juli 2016 in Kraft getretenen EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Direktive) wohl nochmals ergänzt werden, da allgemeine größere Online-Plattformen bisher durch das IT-Sicherheitsgesetz nicht erfasst werden. Hierfür hatte Deutschland zwei Jahre Zeit, um die NIS-Direktive vollständig in nationales Recht umzusetzen.

Für diese Überarbeitung hat das BMI einen Referentenentwurf (NIS-RL-Umsetzungsgesetz) im Dezember 2016 vorgelegt. Dabei soll bei diesem Gesetzesvorhaben das im Juli 2015 in Kraft getretenen IT-Sicherheitsgesetz beibehalten und nur durch die NIS-Richtlinie erforderliche Anpassungen vorgenommen werden. Die wesentlichen Änderungen sind im Artikel 1:

- eine Anpassung der Aufsichtsbefugnisse des BSI an die Vorgaben der NIS-Richtlinie
- Regelungen zu MIRTs (Mobile Incident Response Teams) als wirksame Reaktion auf Cyber-Angriffe
- Regelung von Berichtspflichten und Pflichten zur Konsultation anderer Mitgliedstaaten bei grenzüberschreitendem Bezug
- Konkretisierungen der Meldepflichten der Betreiber
- Einführung von Mindestanforderungen und Meldepflichten sowie Aufsichtsbefugnissen und Sanktionen für die in der NIS-RL konkret genannten digitalen (Telemedien)Diensten.

Mit Artikeln 2, 3 und 4 werden aufgrund der NIS-RL notwendige Anpassungen der spezialgesetzlicher Regelungen (AtG, EnWG, SGB V) vorgenommen. Artikel 5 regelt das Inkrafttreten.

Am 25.01.2017 hat nun das Bundeskabinett das NIS-RL-Umsetzungsgesetz beschlossen[3]. Der Bundesrat hat in seinen Beratungen an die Bundesregierung Prüfbitten adressiert, deren Ergebnis jedoch die Bundesregierung nicht zu einer Änderung des Gesetzesentwurfes veranlasste[4]. Am 27. April 2017 hat der Deutsche Bundestag das neue NIS-RL-Umsetzungsgesetz verabschiedet, das dann Mitte 2017 zusammen mit der BSI-Kritis-Verordnung in Kraft trat[5].