

Industriesteuerungen im Visier von Hackern

Das Sicherheitsbewusstsein in der technischen Datenverarbeitung ist nach übereinstimmenden Berichten schlechter als in der kommerziellen IT. Nur die Kombination aus technischen und organisatorischen Maßnahmen, vereint mit dem Bewusstsein für die Verwundbarkeit, ergibt einen wirksamen Schutz.

Es gilt das Motto: Nach dem Virus ist vor dem Virus. Die Bundesregierung ist wegen möglicher Kopien des Computerwurms Stuxnet besorgt. „Jeder erfolgreiche kriminelle Angriff ermuntert Nachahmer“, warnte Bundesinnenminister Thomas de Maizière in einer Reportage des Norddeutschen Rundfunks (NDR). „Nun ist das ‚Stuxnet‘-Programm so aufwendig, dass die Nachahmung vielleicht kompliziert sein mag. Aber in bescheidenerem Umfang gibt es das bereits, und deswegen müssen wir uns gegen solche Programme so gut wie nur irgend möglich wappnen“, zitierte der Sender den Minister Ende Januar.

Der Computervirus Stuxnet zieht also weiterhin seine Spur durch die Industrie – auch nach seiner Enttarnung. Zwar wohl nicht mehr real als Schadsoftware, aber als Verunsicherung in den Köpfen der IT-Verantwortlichen. Wenn es möglich war, einen solchen Trojaner in eine sicherlich recht gut gesicherte Atomanlage einzuschleusen, so die häufige Überlegung, dann dürfte es für einen interessierten Hacker womöglich so schwierig nicht sein, in eine ganz gewöhnliche Fertigungsanlage einzudringen und dort Dinge anzustellen, die man sich nicht gerne ausmalen mag. Eine Chemieanlage so zu manipulieren, dass sie statt Kunststoffgranulat giftige Gase ausstößt, zum Beispiel. Oder an einem Schweißroboter in der Autoindustrie einen Parameter unauffällig zu verstellen, so dass die Schweißnähte nicht mehr die nötige Festigkeit aufweisen. Die Anzahl möglicher Horrorszenarios ist proportional zu derjenigen von computergesteuerten Fertigungsanlagen. Und: Attacken auf Industrieanlagen sind fokussiert – zugeschnitten auf einen spezifischen Anwendungsfall. Das macht sie so gefährlich. Aber sind sie realistisch?

Die IT liefert praktisch die Steilvorlage für böse Buben: Neuere IT-Konzepte zielen in der Tat darauf ab, die Factory-Floor-Steuerungssysteme für die betriebswirtschaftlichen ERP-Systeme erreichbar zu machen. Auch für Wartungszwecke sind die Systeme von außen erreichbar – über von Fall zu Fall mehr oder weniger gut abgesicherte Zugänge. Damit, so Fachleute, nimmt insgesamt

das Risiko eines Hackerangriffs auch gegenüber Industriesteuerungen zumindest potentiell zu.

Dass das Aktivitätsniveau der ungebetenen Gäste aus dem Cyberspace über die vergangenen Jahre kontinuierlich angestiegen ist, erschließt sich bereits aus der regelmäßigen Lektüre der Tagespresse, die in immer kürzeren Abständen von derartigen Attacken berichtet. Mittlerweile scheint sogar die Bundesregierung nervös geworden zu sein: Als Reaktion auf die Zunahme von Internet-Attacken will sie ein „Nationales Cyber-Abwehrzentrum“ einrichten.

Für die Betreiber computergesteuerter Fertigungsanlagen markiert das Auftauchen von Stuxnet eine Zäsur, selbst wenn die Steuerungen gar nicht unbedingt direkt in das Internet eingebunden sind. „Die Fertigungsbranche hat sich immer als immun gegenüber den bekannten Bedrohungen betrachtet“, kommentiert Pierfrancesco Manenti, Research Director bei der IT-Beratung IDC Manufacturing Insights. „Jedenfalls solange die Steuerungsapplikationen von der Unternehmens-IT getrennt waren.“ Durch die zunehmende Integration beider Welten ändere sich die Situation für die Factory-Floor-IT „dramatisch“.

„Die Bedrohung nimmt zu“, konstatiert auch Rainer Glatz, Leiter des Fachverbands Industrielle Automation beim Branchenverband VDMA. Die Industriesteuerungen würden immer öfter vernetzt, und immer häufiger würden in den Fabriken statt der früher hier anzutreffenden Spezialrechner mit begrenzten Fähigkeiten und exotischen Echtzeitbetriebssystemen Standard-Systeme eingesetzt, die jedem mittelmäßigen Hacker vertraut seien. Dieser Trend mache es den Cyberkriminellen sogar leichter. „Damit entstehen zwangsläufig Einfallstore“, so Glatz.

Auch die Sicherheitsbranche rechnet mit einer Zunahme der Attacken gegen Industriesteuerungen. „Die Sicherheitslage hat sich geändert“, konstatiert beispielsweise Michael Hoos, Computersicherheitsexperte beim Softwarehersteller Symantec: „Auch die industrielle IT gerät ins Fadenkreuz.“ Mittelfristig sei damit zu rechnen, dass Nachahmungstäter aktiv würden. „Wir erwarten Trittbrettfahrer“, so Hoos.

Allerdings wird wohl nicht jeder Hacker in der Lage sein, eine so komplexe Software wie Stuxnet zu entwickeln – immerhin nutzte der Virus vier verschiedene Lücken des Betriebssystems Windows, analysierte seine Umgebung und wurde nur bei Vorliegen bestimmter Bedingungen aktiv. Fachleute schätzen, dass der Aufwand für die Entwicklung von Stuxnet nur von einer großen, personell wie finanziell gut ausgestatteten Organisation zu stemmen war.

Aber selbst wenn Durchschnitts-Cyberkriminelle kaum in der Lage seien, so komplexe Software wie Stuxnet zu entwickeln, so würden sie doch zunehmend

versuchen, Produktionssysteme anzugreifen, fürchtet der Sicherheitsexperte. „Nicht so sehr um zu zerstören, sondern eher um die Betreiber zu erpressen“, sagt Hoos.

Nicht zerstören, sondern spionieren

Auch im Maschinenbauer-Verband VDMA glaubt man, dass die gegenwärtigen und die künftig wohl zunehmenden Attacken in erster Linie aus einer materiellen Motivation heraus erfolgen werden – allerdings aus einer anderen, als Hoos vermutet: Wirtschaftsspionage und Diebstahl geistigen Eigentums. So könnte ein ungebetener Besucher auf einer CNC-Präzisionsfräsmaschine möglicherweise an die Konstruktionsdaten eines komplexen Maschinenteils herankommen, um das Teil nachzubauen. „Industriespionage und Produktpiraterie sind ein Riesenproblem für die Industrie“, sagt Glatz.

Auf technischer Ebene ist durchaus ein Kraut gegen unerwünschte Besucher gewachsen, da sind sich die Beobachter einig. Authentifizierung und starke Verschlüsselung, Firewalls, eine sinnvolle Segmentierung der Netze sind die am häufigsten genannten Mittel, um die Anlagen abzusichern. Antivirensoftware? Im Prinzip ja – aber sie sollte nur eine von mehreren Maßnahmen in einem tief gestaffelten Konzept darstellen. Im Fall Stuxnet hat keine einzige Antivirensoftware Alarm geschlagen, und das lag nicht etwa an einer allzu nachlässig gehandhabten Aktualisierung. Sondern daran, dass die Stuxnet-Virensignatur sehr lange keinem einzigen Antivirenprogramm bekannt war.

So sollte denn auch bei der Schutzkonzeption einer Industriesteuerung keinesfalls nur auf technische Mittel gebaut werden, raten Experten. Sicherheit müsse in die Köpfe. Und das ist leichter gesagt als getan. „Die üblichen technischen Sicherheitsvorkehrungen werden zwar fast überall eingesetzt“, sagt ein Insider, der nicht genannt werden möchte, „aber die Sicherheitsstrategien werden nicht gelebt.“ Jörg Ziercke, Präsident des Bundeskriminalamts (BKA), antwortete dem NDR auf die Frage, ob Deutschland gegen Cyberangriffe gerüstet sei: „Ich sage ganz offen, bei einem Innentäter bekommen wir Probleme.“ Als Innentäter gelten Saboteure, die weitverzweigte Computer-Netzwerke von Regierungen, Militäreinrichtungen oder Unternehmen durch Einfügen von Viren direkt infizieren.

Das Sicherheitsbewusstsein in der technischen Datenverarbeitung ist nach übereinstimmenden Berichten schlechter als in der kommerziellen IT. Dafür mag es materielle Gründe geben. „Sicherheit kostet immer Geld. Das wird erst bewilligt, wenn das Kind in den Brunnen gefallen ist“, sagt der Experte. Aber es gibt auch Gründe, die in der Einstellung der Beschäftigten liegen. Symantec-Sicherheitsexperte Hoos berichtet von laxen Sicherheitskontrollen gerade im Umfeld von

Produktionssteuerungsanlagen. „Ich habe selber die Erfahrung gemacht, wie leicht man sich mit dem Laptop an so eine Anlage andocken kann“, so Hoos. Servicetechniker und externe Dienstleister müssen oft nur die Seriennummer ihres Laptops in ein Formular eintragen und bei der Frage nach einem Virenschutz „ja“ ankreuzen. Mobile Datenträger wie USB-Sticks werden nur selten überhaupt erfasst und noch viel seltener geprüft. Dabei übersprang gerade Stuxnet die Barriere zwischen Internet und SPS-Programmierlaptops mittels USB-Sticks; die Industriesteuerungen besaßen selbst gar keine Verbindung nach außen. Auf den To-do-Listen der Sicherheitsexperten stehen denn auch organisatorische Maßnahmen ganz oben. Bei der dringend angeratenen Bestandsaufnahme sämtlicher existierender Prozesse soll vor allem erfasst werden, wer Zugriff auf das Factory-Floor-Netzwerk hat – und nach Erfahrung von Fachleuten haben gerade im industriellen Umfeld sehr viele externe Mitarbeiter und Dienstleister einen solchen Zugriff. Nicht wenige Berater empfehlen vor dem Hintergrund der gestiegenen Gefährdungslage, die weitere Integration von Office-IT und Produktionssteuerung erst einmal zu überdenken. „Davon würde ich im Moment vollständig abraten“, sagt etwa Hoos von Symantec. Im Gegenteil, man solle den trennenden Graben beibehalten, vielleicht sogar noch vergrößern. Eine Kombination aus technischen und organisatorischen Maßnahmen, vereint mit dem Bewusstsein für die Verwundbarkeit, ergibt also erst einen wirksamen Schutz. Die Benutzer in der Industrie werden ihn noch brauchen, denn die Bedrohung wächst. Das gilt für destruktive Attacken ebenso wie für den Diebstahl geistigen Eigentums mit den Methoden der Cyberkriminalität.

Siemens nach dem Stuxnet-Sturm

Als im Spätsommer 2010 die Meldungen über die Stuxnet-Attacke durch die Medien gingen, schreckte so mancher Verantwortliche für den technischen IT-Betrieb in Fertigungsanlagen auf. Die Prozesssteuerungs- und -visualisierungssysteme, denen die Attacke galt, sind weltweit in vielen Fertigungsstraßen in Betrieb – unter anderem auch in deutschen Vorzeigebereichen wie dem Maschinenbau, in der weitgehend robotergesteuerten Automobil-Produktion und in der Chemie.

Die Zahlen von Sicherheitstechnik-Anbietern überzeichnen jedoch möglicherweise die Gefahr, die von Stuxnet unmittelbar ausgeht: Der Virus befällt zwar eine hohe Zahl von Rechnern, wird jedoch nur selten wirklich aktiv. Einer Siemens-Analyse zufolge richtet sich der Virus nicht gegen bestimmte Prozesstechnologien in ihrer

Gesamtheit, sondern gegen genau definierte Prozesse mit spezifischen Hardwarekonfigurationen. Das Unternehmen schloss umgehend die von Stuxnet genutzten Sicherheitslücken und stellte auf seiner Website eine Software zum Aufspüren und Entfernen der Malware zur Verfügung. „Bisher wurde diese Software mehr als 20.000-mal heruntergeladen“, erklärt Tino Hildebrand, bei Siemens für die Vermarktung der Simatic-Produkte zuständig. Weit weniger oft wurde die Spürsoftware fündig: „In unserem Kundenkreis haben bisher lediglich 22 Unternehmen eine Stuxnet-Infektion bestätigt“, so Hildebrand. Wie viele Prozessleitsysteme diese Kunden betreiben, sagt Siemens nicht, doch ein gewisses Aufatmen ist nicht zu überhören.

Einfach zur Tagesordnung übergehen sollten die Verantwortlichen aber auch nicht. Für jede Anlage, so der Rat der Siemens-Experten, sollte ein individuelles Sicherheitskonzept festgelegt werden. Dabei seien insbesondere die Zugriffsberechtigungen genau zu definieren und die Zahl der Berechtigten zu limitieren. „Nicht jeder, der zugreifen kann, darf das auch dürfen“, so Hildebrand.