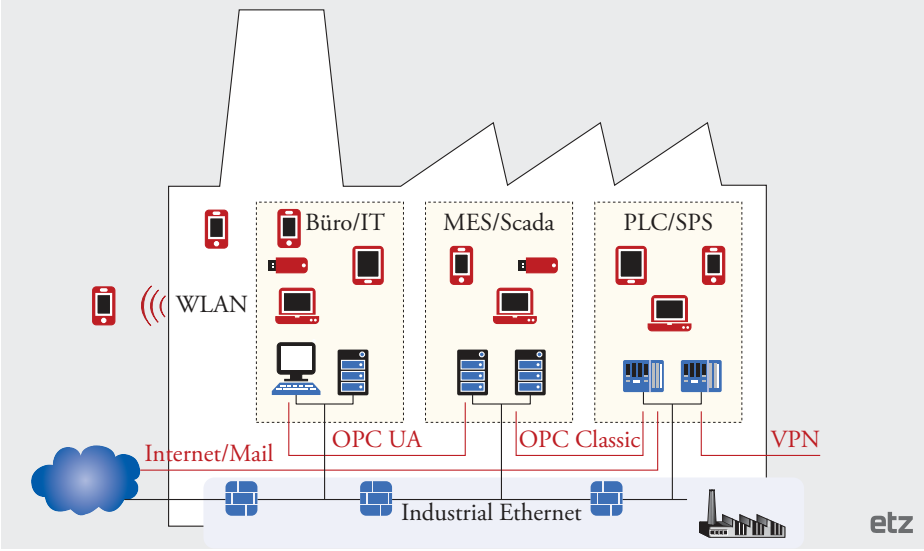


01 Die inzwischen oft durchgängige Vernetzung von der Leit- zur Feldebene sowie die unbeschränkten Zugriffsmöglichkeiten auf die Steuerungen schaffen Möglichkeiten für Cyberangriffe

Effizienter Schutz nach dem IT-Sicherheitsgesetz - Teil 1

Das vom Bundestag mit der Mehrheit der Großen Koalition beschlossene „Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme“ (IT-Sicherheitsgesetz) ist mit Wirkung zum 25. Juli 2015 in Kraft getreten. Es betrifft eine erhebliche Anzahl von Unternehmen – von den großen Betreibern „Kritischer Infrastrukturen“ (Kritis) bis hin zu Betreibern kleiner Webseiten. Was auf die Betreiber von vernetzter Automatisierungs- und Prozessleittechnik im Bereich „Kritis“ und darüber hinaus zukommt und welche Hilfestellung Irma (Industrie Risiko Management für die Automatisierung) von Videc dabei bietet, erläutert der zweiteilige Fachartikel.

Text: Jens Bußjäger, Dieter Barelmann

IT-Angriffe auf Infrastrukturen, die unsere Grundversorgung gewährleisten, stellen eine besondere Bedrohung für unser Gemeinwesen dar. Zu deren Schutz vor Cyberangriffen wurden die gesetzlichen Anforderungen in dem neuen IT-Sicherheitsgesetz festgeschrieben. Demnach müssen die Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen künftig nicht nur einen Mindeststandard an IT-Sicherheit einhalten und nachweisen, sondern auch erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.

Das BSI verantwortet und steuert die Umsetzung des IT-Sicherheitsgesetzes („ITSiG“). Dafür werden nun die Rechtsverordnungen ausgearbeitet sowie mit der Unterstützung der Branchenverbände die Normen, Standards und Sicherheitskataloge erstellt.

Im Rahmen des IT-Sicherheitsgesetz, das als Artikelgesetz verabschiedet wurde, werden eine Reihe an bestehenden Gesetzen ergänzt, verschärft und mit zusätzlichen Sanktionen

belegt. Grundsätzlich ist das alles eigentlich nichts Neues, da bereits in den Vorjahren die rechtliche Verpflichtung für die Einführung eines Risikomanagementsystems in Unternehmen bestand, die sich insbesondere aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich („KonTraG“) ergibt. Jetzt ist ein erster Nachweis zur Umsetzung eines durchgängigen IT-Sicherheitsmanagements nach zwei Jahren zu erbringen.

Natürlich haben auch Unternehmen nicht kritischer Infrastrukturen ihre unternehmerischen Anforderungen und Motivation ihre Produktionsanlagen vor Manipulationen und Schäden zu schützen, denn schließlich haben diese auch einen Werkszaun und weitere Schutzeinrichtungen! Dementsprechend ist eine Ausstrahlungswirkung für Nicht-Kritis-Unternehmen zu erwarten.

Durchgängigkeit birgt Risiken

Der sorglose Einsatz von internetfähigen IT-Systemen wie Smartphones und Tablets fürht zu einem ungeahnten Ausmaß an Sicherheitslücken. Dazu gehören auch alle Komponenten mit USB-Anschluss, da zum Beispiel USB-Speicher-Sticks an internetfähigen PC und später an der PLC stecken können. Zudem reichen Industrial-Ethernet-Verbindungen immer öfter bis in die Feldebene in der Automatisierung hinein.

Viele Produktionssysteme werden seit Jahren Industrial-Ethernet-fähig gemacht. Für die Scada-Infrastrukturen kommen mehr und mehr Standard-IT-Komponenten zum Einsatz. Die Hersteller der Automatisierungen bieten für die Steuerungen webbasierte HMI oder dedizierte Apps für Tablets und Smartphone an. Die Betriebsleitung oder Geschäftsführung kann flexibel von ihrem Arbeitsplatz direkt auf historische Daten zugreifen (**Bild 1**).

Durch diese oft durchgängige Vernetzung und unbeschränkten Zugriffsmöglichkeiten auf die Steuerungen entstehen jedoch Risiken. Unbeschränkt daher, da die aufwendigen Anpassungen in der Netzwerk- und Firewall-Konfiguration sowie die Pflege der Benutzer Accounts unterbleiben. Mit der Vielzahl von Mobilgeräten nehmen die Risiken nochmals zu.

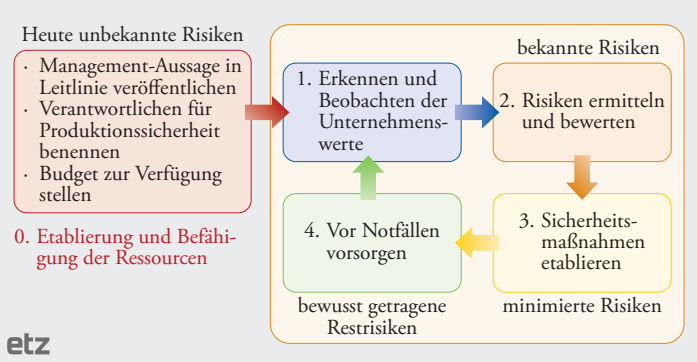
Die Gefahr wächst

Wie groß die Gefahr ist, zeigen exemplarisch zwei Beispiele. Der TÜV Süd setzte bei dem Projekt Honeynet eine realistische Applikation eines Wasserwerks ins Netz. Nach neun Monaten waren 50 000 Angriffe aus 160 Ländern auf das simulierte Wasserwerk zu verzeichnen. Nicht berücksichtigt bei der Analyse wurden alle Scans auf die Anlage. Von den Gesamtangriffen haben sich 130 im Office-Bereich umgeschaut, davon wiederum 17 im industriellen Umfeld. Diese 17 Zugriffe schauten sich vertieft in der Struktur der Anlage um, nahmen sich der Protokolle und Schwachstellen an. Die Angreifer verwendeten dabei zum größten Teil verschleierte IP-Adressen, um eine Rückverfolgbarkeit auszuschließen.

Der Lagebericht 2014 des BSI informiert über die Manipulation und Zerstörung eines Hochofens. Danach erfolgen die Angriffe zunehmend zielgerichteter, technologisch ausgereifter und komplexer. Dabei lässt sich folgender Ablauf erkennen: infizieren, einbrechen, nachladen, sammeln und dann erst schädigen.

Deutschland ist zunehmend Ziel von Cyberangriffen, Cyberspionage und sonstigen Formen der Cyberkriminalität. Hier gilt die Regel des Urwalds: Das schwächste Tier wird gefressen – oder übertragen auf die Industrie: Das Unternehmen mit dem geringsten Schutz wird als erstes angegriffen. Einzelne Sicherheitsbehörden gehen davon aus, dass durchaus in den nächsten zwölf Monaten mit mehreren Angriffen, bzw. mit mehreren Ausfällen bei Unternehmen zu rechnen ist. Die Infektionszeit von sechs bis acht Monaten von dem Eindringen eines Schadcodes bis zum Ausfall/zur Schädigung, in der bereits im Unternehmensnetz vorhandene Schwachstellen gesammelt werden, läuft bereits.

Die Durchgängigkeit der IT-Sicherheit in Technik und Organisation bietet weitere Möglichkeiten. Neue Schwachstellen werden immer schneller ausgenutzt. Es ist eine regelrechte Arbeitsteilung der Hacking-Industrie zu verzeichnen. Man kann heute schon problemlos einen Hackerangriff kaufen. Staaten und Terrororganisationen investieren heutzutage große Summen in Hacker und nicht mehr in Waffen.



02 Betroffene Kritis-Unternehmen müssen einen organisatorischen Regelprozess aufbauen

Die Anforderungen des IT-Sicherheitsgesetzes

Das IT-Sicherheitsgesetz stellt spezifische Anforderungen an die Betreiber kritischer Infrastrukturen. Sie müssen eine ständig erreichbare Kontaktperson für das BSI benennen. Kontaktpersonen können auch mit mehreren Unternehmen gemeinsam eingerichtet werden. Die Unternehmen sind verpflichtet IT-Störungen an das BSI zu melden, damit weitere potenziell Gefährdete gewarnt werden können. Zudem müssen sie die Erstellung eines Lageberichts über die IT-Sicherheit in Deutschland unterstützen. Eine „Anonyme Meldung" ist nur bei Gefährdung von Systemen, nicht bei Eintritt einer Störung, erlaubt. Diese Pflichten bestehen auch dann, wenn Unternehmen ihre IT durch Dienstleister betreiben lassen.

Es sind Maßnahmen zur Erfassung der informationstechnischen Systeme und Komponenten sowie der Vorgänge der Informationsverarbeitung zu treffen. Die Absicherungsmaßnahmen sind an den Stellen einzuhalten, an denen die Informationstechnik Einfluss auf die Erbringung von Dienstleistungen hat. Dabei sind die organisatorischen sowie die technischen Vorkehrungen zur Abschottung besonders kritischer Prozesse, inkl. infrastruktureller und personeller Maßnahmen, zu berücksichtigen.

Dem einzelnen Betreiber steht es frei, auch eigene, dem Stand der Technik entsprechende, Maßnahmen umzusetzen. Diese müssen angemessen sein. Der Stand der Technik ergibt sich aus einschlägigen internationalen, europäischen und nationalen Normen und Standards oder einem vergleichbar effektiven Schutz, den Dokumentationen in entsprechenden Sicherheits- und Notfallkonzepten sowie der Erarbeitung branchenspezifischer Sicherheitsstandards.

Die entsprechenden Maßnahmen sich durch Sicherheitsaudits, Prüfungen oder Zertifizierungen, wie

- Information Security Management (Sicherheitsorganisation, IT-Risikomanagement etc.),
- identifizieren und managen kritischer Cyber-Assets,
- Maßnahmen zur Angriffsprävention und -erkennung,
- Implementierung eines Business Continuity Managements (BCM) sowie
- branchenspezifische Besonderheiten

nachzuweisen. Dies sind zunächst nur die abstrakten Inhalte des IT-Sicherheitsgesetzes. Für einen sicheren Betrieb sollten die betroffenen Kritis-Unternehmen jedoch möglichst umgehend geeignete Ressourcen etablieren und befähigen. Hier muss dann zunächst zwingend ein organisatorischer Regelprozess (**Bild 2**) aufgebaut werden, der

- alle Unternehmenswerte erkennen und beobachten kann,
- Risiken kontinuierlich ermitteln und bewerten kann,
- umgehend geeignete Sicherheitsmaßnahmen ergreifen kann,
- vor Notfällen vorzusorgen weiß.

Ein gutes Gerüst für den Aufbau eines Sicherheitsmanagements bieten insbesondere die Normen der ISO-27000-Reihe. Zur Einführung eines sogenannten Informationssicherheits-Management-Systems („ISMS") positionieren sich bereits diverse Unternehmen im Moment für den Bereich Beratung. Ein Produkt für den Bereich IT-Sicherheit in der Automatisierung ist Irma von Videc [1]. Welche Möglichkeiten dieses Werkzeug bietet, erläutert der zweite Teil dieses Fachartikels, der in der Ausgabe 10 der etz erscheint. (no)

Expertenworkshops Security

Mit Bezug auf das neue IT-Sicherheitsgesetz veranstaltet das Unternehmen Videc eine Reihe von Workshops.

Für die Betreiber der zu den kritischen Infrastrukturen zählenden Branchen kommen kurzfristig gesetzliche Vorgaben, wie das IT-Sicherheitsgesetz, zum Tragen. Zwei Workshops im Oktober richten sich an Betreiber, Planer und Systemintegratoren, die sich mit dem Thema IT-Sicherheit und Automatisierung auseinandersetzen. Die Veranstaltungen am 1. Oktober in Radefeld bei Leipzig und am 15. Oktober in München sind kostenlos. Anmeldung über www.videc.de.
Auch im Rahmen der Veranstaltungsreihe „Sicherheit in der Wasserwirtschaft" nimmt das Thema Security eine Hauptrolle ein. Technologietage zum Thema finden am 17. September in Bayreuth und am 24. September in Ulm statt. Anmeldungen sind über die Website www.aqua-automation.com möglich.

Literatur

[1] Videc Data Engineering GmbH, Bremen: www.videc.info

Autoren

Jens Bußjäger ist Geschäftsführer der Achtwerk GmbH & Co. KG in Bremen.
jens.bussjaeger@acht-werk.de

Dieter Barelmann ist Geschäftsführer der Videc GmbH in Bremen.
DBarelmann@videc.de