**An Rechnernetze in Industriebetrieben werden höhere Security-Anforderungen gestellt als an IT-Verbindungen im Bürobetrieb.**

FOTO: BOGGY/FOTOLIA

# IT-Sicherheit in der Industrie

**Industrie 4.0 – Maschinen kommunizieren untereinander. Bei einer Veranstaltung in Linz wurden Risiken sowie technische und rechtliche Wege zur Erhöhung der IT-Sicherheit in der Industrie aufgezeigt.**

An Rechnernetze in Industriebetrieben werden hinsichtlich der Security andere Anforderungen gestellt als an IT-Verbindungen im Bürobetrieb“, sagte Prof. Dr. Ing. Peter Fröhlich, Dekan der Fakultät Maschinenbau und Mechatronik der Technischen Hochschule Deggendorf bei der Veranstaltung „IT-Sicherheit am Donaustrand“ am 13. September 2016 im *Ars Electronica Center (AEC)* in Linz.

Im Bürobetrieb steht die Vertraulichkeit der Datenübermittlung im Vordergrund. Wird eine Verbindung durch die Firewall abgeblockt oder geht eine Website nicht auf, ist das kein großes Problem. Anders im Industriebereich: Die Produktion kann nicht einfach heruntergefahren werden, wenn ein Verdachtsmoment gemeldet wird. Neben einem Produktionsstillstand hätte es auch schwerwiegende Folgen, wenn durch Manipulation der Steuerungsdaten von Maschinen Qualitätsmängel in der Fertigung auftreten und andere oder fehlerhafte Produkte erzeugt werden. Das kann zu Haftungsfragen bis zu Rückrufaktionen für Produkte führen. Die Integrität der Steuerungsdaten ist für die Industrie von vorrangiger Bedeutung. Angriffsmöglichkeiten auf Daten gibt es viele. Tools, wie sie für Penetrationstests eingesetzt werden, können für kriminelle Zwecke missbraucht werden, um Informationen abzusaugen oder Steuerungsprogramme zu verändern.

Im Internet werden unauffällige Bauteile als USB-Stick angeboten. Werden sie angesteckt, speichern sie alle Tastaturanschläge und somit auch Passwörter. Bei günstiger Gelegenheit werden die Sticks abgezogen und ausgewertet (Key Logger).

Um in ein gesichertes Netz einzudringen, sucht sich der Angreifer wartungsmäßig vernachlässigte Rechner, etwa solche, die mit veralteten und nicht mehr gepatchten Betriebssystemen oder Programmen ausgestattet sind und die nur selten benützt werden.

Auch Fernwartung kann Risiken mit sich bringen, warnte Fröhlich. Wird die Fernwartung über einen verschlüsselten Kanal (Virtual Private Network – VPN) angeboten, werden durch die damit verbundene Verschlüsselung der übermittelten Daten auch die Sicherungssysteme wie Firewalls unterlaufen. Schadsoftware am Wartungsrechner geht ungehindert und direkt auf den zu wartenden Rechner über und kann sich in der Folge auf Nachbarrechner verbreiten.

**Der typische Angriff** erfolgt über Social Engineering. Die Unaufmerksamkeit oder Neugier von Menschen wird ausgenützt, diese zu

verleiten, Anhänge von E-Mails zu öffnen, wodurch Schadsoftware aktiviert wird. Beispielsweise übermittelt ein installierter Trojaner Informationen nach draußen und eröffnet Zugänge in Netze. Mit der für Industriemaschinen ausgelegten Suchmaschine *Shodan* kann weltweit nach Gerätetypen gesucht werden, und man findet immer welche, deren Passwörter nicht ordentlich gemanagt werden und leicht zu knacken sind. Das ist die Einfallspforte, um auf die Steuerungsprogramme der jeweiligen Maschine zuzugreifen und diese zu manipulieren.

Eine Maschine in einem Industriebetrieb kann auch über die steuernden Sensoren manipuliert werden. Wird einer Heizungsanlage ein Temperaturfühler vorgetäuscht, der ständig zu niedrige Werte anzeigt, wird die Anlage weiterheizen. Man wird eine Art digitalen Personalausweis für alle Geräte einführen müssen, die miteinander kommunizieren, damit diese untereinander sicher sein können, mit dem jeweils richtigen Partner verbunden zu sein.

Nicht jeder muss alles wissen und auf alles zugreifen können. Der Hersteller einer Maschine braucht Daten darüber, ob die Maschine richtig läuft, nicht aber, was mit der Maschine hergestellt wird. Der Lieferant von Rohstoffen braucht nicht zu wissen, wie diese Stoffe verarbeitet werden und was daraus hergestellt wird. Der Produzent wiederum braucht keine Daten über die Produktionsmaschinen, sondern nur zu den Produkten.

Laut Fröhlich müsse eine Infrastruktur geschaffen werden, durch die der Zugriff auf Daten administriert und festgelegt wird, wer auf welche Daten Zugriff hat. Verwirklichen ließe sich das durch kryptografische Verschlüsselung der Daten. Die zu vergebenden Schlüssel öffnen jeweils nur bestimmte Bereiche.

**Bei Systemen der kritischen Infrastruktur kann mit wenig Wissen viel Schaden angerichtet werden.**

Die praktische Nutzanwendung von *Shodan* für einen Hacker führte Marco Di Filippo vor, mit Live-Angriffen auf industrielle Steuerungsanlagen *(Industrial Control Systems – ICS)*. „Insbesondere bei Systemen der kritischen Infrastruktur kann mit wenig Wissen viel Schaden angerichtet werden." Mit Kombinationsvermögen und Herumprobieren an Passwörtern öffnen sich Systeme der Haus- und Gebäudeautomation oder die Steuerung von Verkehrsleitsystemen, Windkraftwerken und Solaranlagen. Kann auf die Steuerungsprogramme zugegriffen werden, können die Parameter manipuliert und die Systeme beliebig beeinflusst werden.

**Die Gesetzgebung,** insbesondere auf Ebene des EU-Rechts, setzt Maßnahmen, die diesen Gefahren gegensteuern sollen. Seit 8. August 2016 ist die „Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" („NIS-RL") in Kraft. Die Richtlinie ist von den Mitgliedstaaten bis zum 9. Mai 2018 durch Erlass der erforderlichen Rechts- und Verwaltungsvorschriften umzusetzen.

Während der Datenschutz durch die am 24. Mai 2016 in Kraft getretene und ab 25. Mai 2018 geltende Datenschutz-Grundverordnung (DSGVO) europarechtlich unmittelbar einheitlich geregelt ist, bezieht sich die NIS-RL auf den Informationsschutz, unter den etwa Betriebsgeheimnisse fallen.

Die Richtlinie soll durch die auf ihrer Basis noch zu erlassenden nationalstaatlichen Regelungen die Netz- und Informationssicherheit erhöhen, referierte Mag. Karin Neußl, Lektorin an der FH Hagenberg. Die Mitgliedstaaten werden verpflichtet, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen, eine Kooperationsgruppe und ein Netzwerk von Computer-Notfallteams *(Computer Security Incident Response Teams – CSIRTs)* zu schaffen, Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste festzulegen sowie nationale zuständige Behörden („NIS-Behörden") und Anlaufstellen zu benennen.

Bis zum 9. November 2018 haben die Mitgliedstaaten die Betreiber wesentlicher Dienste in ihrem Hoheitsgebiet zu ermitteln. Es handelt sich um öffentliche oder private Einrichtungen aus den Sektoren Energie, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasserlieferung und -versorgung sowie die digitale Infrastruktur.

Die Dienste sind wesentlich, wenn sie für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich sind, ihre Bereitstellung von Netz- und Informationssystemen abhängig ist und ein Sicherheitsvorfall eine erhebliche Störung der Bereitstellung dieser Dienste bewirken würde. Die Liste der ermittelten Betreiber ist mindestens alle zwei Jahre zu überprüfen und gegebenenfalls zu aktualisieren.

Bei der Festlegung der nationalen NIS-Strategie steht die *ENISA* beratend zur Seite. Ferner sind Überwachungsorgane einzurichten. Den nationalen NIS-Behörden obliegt die Überwachung (Monitoring) der Einhaltung der Richtlinie auf nationaler Ebene. Jeder Mitgliedstaat hat eine zentrale Anlaufstelle zu benennen, die als Verbindungsstelle

FOTO: DIGITALSTOCK/FOTOLIA

**„IT-Sicherheit am Donaustrand“: Vortragende Robert Kolmhofer, Marco Di Filippo, Peter Fröhlich und Karin Neußl.**

zwischen den Mitgliedstaaten und der Kooperationsgruppe fungiert und mit den nationalen Strafverfolgungs- und Datenschutzbehörden zusammenarbeitet. Sie hat jährlich einen Bericht über Meldungen an die Kooperationsgruppe zu erstatten. Die *CSIRTs* haben Sicherheitsvorfälle auf nationaler Ebene zu überwachen, Frühwarnungen und Alarmmeldungen abzusetzen, auf Sicherheitsvorfälle zu reagieren, Risiken und Vorfälle zu analysieren sowie Lagebeurteilungen zu erstellen. Im *CSIRTs*-Netzwerk sind die nationalen Teams vertreten; die EU-Kommission ist Beobachter. Die *ENISA* führt die Sekretariatsgeschäfte und unterstützt die Zusammenarbeit der Teams.

Die Betreiber wesentlicher Dienste sowie die Anbieter digitaler Dienste haben geeignete und verhältnismäßige technische und organisatorische Sicherheitsmaßnahmen zu ergreifen, um die Risiken zu bewältigen. Diese Maßnahmen müssen dem Stand der Technik entsprechen. Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der angebotenen Dienste haben, sind der NIS-Behörde oder dem *CSIRT* zu melden. Die Mitgliedstaaten müssen wirksame, angemessene und abschreckende Sanktionen für Verstöße gegen die nach der Richtlinie erlassenen Bestimmungen festlegen.

**SVG und SVV.** Das Signaturgesetz (SigG) und die Signaturverordnung 2008 (SigV) wurden außer Kraft gesetzt. An ihre Stelle traten das am 1. Juli 2016 in Kraft getretene Signatur- und Vertrauensdienstegesetz (SVG), BGBl. I Nr. 2016/50, und die seit 2. August 2016 geltende Signatur- und Vertrauensdiensteverordnung (SVV), BGBl. II 2016/208.

**Technik/Organisation.** Worin bestehen die „angemessenen Maßnahmen technischer und organisatorischer Natur zum bestmöglichen Schutz der Infrastruktur und zur Informationssicherheit“? Prof. (FH) DI Robert Kolmhofer, Leiter des Departments Sichere Informationssysteme an der FH Hagenberg, verwies auf die zahlreichen Normen, Standards und Empfehlungen.

Die Einhaltung dieser Regelungen liegt im Interesse eines Unternehmens, dienen sie doch dazu, Schaden abzuwenden, nicht nur in finanzieller Hinsicht, sondern auch im Hinblick auf die Reputation eines Unternehmens in der öffentlichen Meinung.

Voraussetzungen sind der physische Schutz der Anlagen im Sinn eines Zwiebelschalenkonzepts und allgemeine Sicherheitsmaßnahmen wie Firewalls, Virenscanner, E-Mail-Signatur und -verschlüsselung, Backups (am besten offline) sowie Notfallpläne.

Beim Informationssicherheitsmanagement kommen hauptsächlich die Standards der Reihe ISO/IEC 270xx in Betracht; im technischen Bereich die Normenreihe IEC 62443 über „Industrielle Kommunikationsnetze – IT Sicherheit für Netze und Systeme“. Darunter fallen die als *ICS (Industrial Control Systems)* oder *SCADA* (Prozess-Steuerung) bezeichneten Systeme.

Von *Tele-Trust* wurde eine im Internet frei verfügbare „Handreichung zum Stand der Technik im Sinne des IT-Sicherheitsgesetzes (IT-SiG)“ herausgegeben. Das Anforderungsniveau des von der NIS-Richtlinie verlangten „Standes der Technik“ liegt zwischen den „allgemein anerkannten Regeln der Technik“ und dem „Stand von Wissenschaft und Forschung“.

*Kurt Hickisch*

## IT-SICHERHEIT

### IT und Recht

Die Veranstaltung „IT-Sicherheit am Donaustrand“ wurde zum 6. Mal vom Bayerischen IT-Sicherheitscluster e.V. in Zusammenarbeit mit der Fachhochschule Hagenberg, Fakultät für Informatik, Kommunikation und Medien, Department Sichere Informationssysteme, organisiert. Das Schwergewicht liegt darin, zwischen Informationstechnologie und Recht eine Brücke zu schlagen. Der IT-Sicherheitscluster ist ein Zusammenschluss von Unternehmen der IT-Wirtschaft; solchen, die IT-Sicherheitstechnologien nutzen sowie Hochschulen, Forschungs- und Weiterbildungseinrichtungen. Der Verein fördert die Erforschung, Entwicklung, Anwendung und Vermarktung von Produkten und Dienstleistungen, die zur Erhöhung der Informationssicherheit sowie der funktionalen oder physischen Sicherheit beitragen. Interessierte werden unter anderem in Veranstaltungen und Workshops über Sicherheitsrisiken sowie technische und organisatorische Lösungen informiert.

*www.it-sicherheit-bayern.de*

FOTOS: KURT HICKISCH