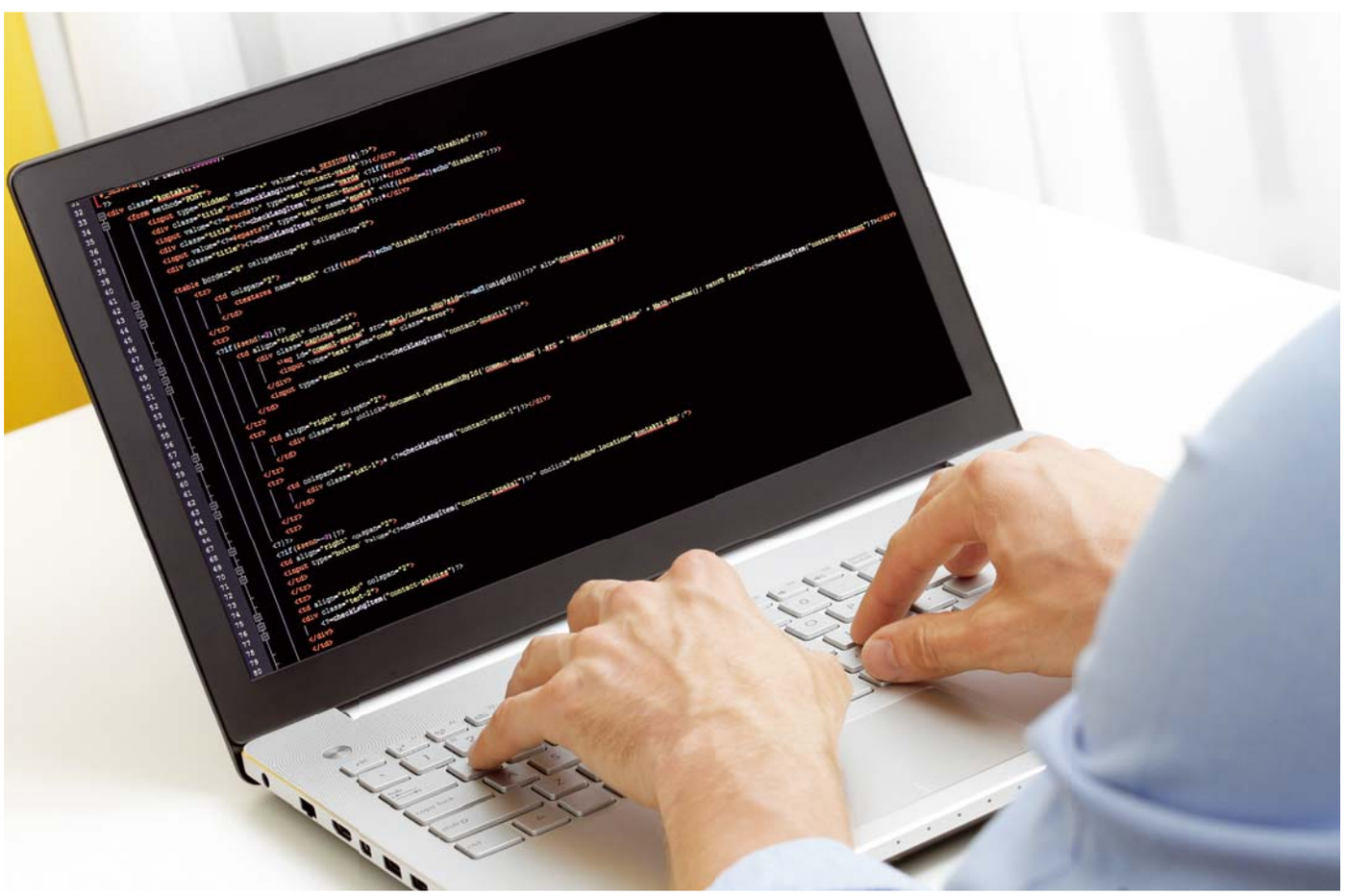
Im Dschungel der Risiken und Regelungen

Sie kommen aus dem Internet, werden über Wechseldatenträger eingeschleust oder verschaffen sich über den Drucker Zugang ins Unternehmensnetzwerk: Die Möglichkeiten potenzieller Bedrohungen aus dem Netz – sogenannter Hacks – werden immer vielfältiger. Gerade in kritischen Infrastrukturen wie der Energieversorgung wird Cyber Security daher immer wichtiger.



Hacker bedrohen immer häufiger Unternehmensnetzwerke. Das neue IT-Sicherheitsgesetz gibt vor, wie den Angriffen vorgebeugt werden soll.

Foto: ronstik/shutterstock.com

Bundesregierung und Bundestag haben im Sommer 2015 Tatsachen geschaffen: Am 25. Juli trat das neue IT-Sicherheitsgesetz in Kraft, das für Betreiber kritischer Infrastrukturen – also Unternehmen, die für ein funktionierendes Gemeinwesen unerlässlich sind – neue Maßstäbe setzt. Krankenhäuser und Labore gehören dazu, Luft- und Schifffahrt ebenso wie Wasserver- und Abwasserentsorgung, Kraftwerke und Energieversorger. Experten und die Bundesregierung gehen derzeit davon aus, dass ungefähr 2.000 Unternehmen aus den Sektoren Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Energie vom IT-Sicherheitsgesetz betroffen sein werden.

Sicherheitskatalog für Netzbetreiber

Das Gesetz schreibt einen Mindeststandard für IT-Sicherheit vor. So müssen beispielsweise „erhebliche“ IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden. Mit Veröffentlichung des IT-Sicherheitskatalogs gelten die neuen Pflichten umgehend für die Betreiber von Strom- und Gasnetzen. Für die anderen kritischen Infrastrukturen – zum Beispiel Kraftwerke – muss den Verpflichtungen erst dann nachgekommen werden, wenn Mitte 2016 die dazugehörige Rechtsverordnung in Kraft tritt. Innerhalb einer Zwei-Jahres-Frist müssen diese Unternehmen dann die gesetzlichen Vorgaben des IT-Sicherheitsgesetzes umsetzen. Andernfalls drohen Bußgelder in Höhe von bis zu 100.000 Euro.

„Die Unternehmen sind jetzt dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zu treffen, um ihren im Gesetz verankerten Verpflichtungen nachzukommen. Wir empfehlen, bald damit zu beginnen, die eigene Situation gegenüber den gesetzlichen Anforderungen zu spiegeln und eventuell vorliegende Defizite aktiv anzugehen“, erklärt Holger Junker, Experte beim BSI. ABB unterstützt Betreiber von Versorgungsnetzen dabei, sich im Dschungel der Risiken und Regelungen zurechtzufinden.

Ein Beispiel: die Stadtwerke Neu-Isenburg GmbH nahe Frankfurt am Main. „Wir wollen uns dem Thema frühzeitig stellen, um mit entsprechendem Vorlauf und strukturiert die Vorbereitungen zu treffen, damit wir unsere Netzleitstelle gesetzeskonform zertifizieren lassen können“, erklärt Uwe Hildebrandt, Technischer Leiter der Stadtwerke Neu-Isenburg. ABB hat den hessischen Energieversorger im September vergangenen Jahres mit einem Cyber Security Assessment (CSA) unterstützt, das neben den technischen Themen wie Netzwerkstruktur, Rechnerkonfigurierung oder Fernwartungszugang auch organisatorische Bereiche, zum Beispiel Notfallpläne, betrachtet. Auch die Prozessdokumentation oder die regelmäßige Schulung der Mitarbeiter gehören dazu. „ABB kann das herstellerunabhängig und technologieneutral durchführen“, so Robert Grey, Vertriebsingenieur bei ABB Power Consulting.

Schwachstellen identifizieren

Am Anfang des CSA steht eine umfangreiche Ist-Aufnahme, die die neuen gesetzlichen Anforderungen berücksichtigt. Dieser Teil wird mithilfe von speziellen Software-Lösungen durchgeführt, die jede einzelne Systemkomponente mit ihren jeweiligen Parametern, zum Beispiel installierte Software und offene Schnittstellen, erfassen. Außerdem werden Aspekte wie die Prozessankopplung und die Zugangskontrolle untersucht.

Die Identifizierung von Schwachstellen auf der Grundlage gesammelter Daten und deren Bewertung anhand von Best Practices und Branchenstandards bilden das Rückgrat der Dienstleistung. Die ABB-Experten werten sämtliche Informationen aus und erstellen einen konkreten Aktionsplan. „Die kontinuierliche Investition in das Thema Sicherheit und die frühe Erkenntnis, dass Cyber Security kein Produkt, sondern ein Prozess ist, hat sich schon für mehrere Unternehmen der Energieversorgung bezahlt gemacht“, sagt Robert Grey. Zwischen dem CSA und dem Abschlussbericht mit den Handlungsempfehlungen liegen nur vier Wochen.

„ABB hat uns im Rahmen des Cyber Security Assessment darauf sensibilisiert, welchen Aufwand es brauchen wird, um die gesetzlichen Anforderungen zu erfüllen und eine spätere Zertifizierung zu erreichen. In einer sehr kompakten Form wurden uns die Untersuchungsergebnisse und aus ihnen resultierende Verbesserungspotenziale aufgezeigt“, erklärt Uwe Hildebrandt von den Stadtwerken Neu-Isenburg.

Weitere Infos: robert.grey@de.abb.com

„Wir wollen uns dem Thema stellen und unsere Netzleitstelle gesetzeskonform zertifizieren lassen.“

Stadtwerke Neu-Isenburg

Gegründet 1898, versorgt die Stadtwerke Neu-Isenburg GmbH heute 37.000 Einwohner der Kommune südlich von Frankfurt am Main. Das Unternehmen hat ungefähr 100 Mitarbeiter. Im Jahr 2014 lieferten die Stadtwerke Neu-Isenburg 163 Mio. kWh Strom, 259 Mio. kWh Gas und 201 Mio. m^3 Trinkwasser an ihre Kunden. Das Stromnetz umfasst 450 km Leitungen; Gas- und Wassernetz sind jeweils circa 100 km lang. Neben den Netzen unterhalten die Stadtwerke Neu-Isenburg zwei Buslinien und sorgen als Betreiber des Waldschwimmbades für Badespaß.

Weitere Infos: www.swni.de