Gut gewappnet: keine Chance der Cyber-Gefahr

—
Unternehmen fühlen sich mehrheitlich gut vor Cyberangriffen geschützt – obwohl viele schon einmal von solchen betroffen waren. Und nur ein kleiner Anteil schätzt die Bedrohung, die von Cyberattacken ausgeht, als gross ein. Die Infografiken auf dieser und den folgenden Seiten zitieren Befunde aus der Studie «Cyberrisiken in Schweizer KMUs» von ICTswitzerland, im Rahmen derer 300 kleinere und mittlere Unternehmen befragt wurden.

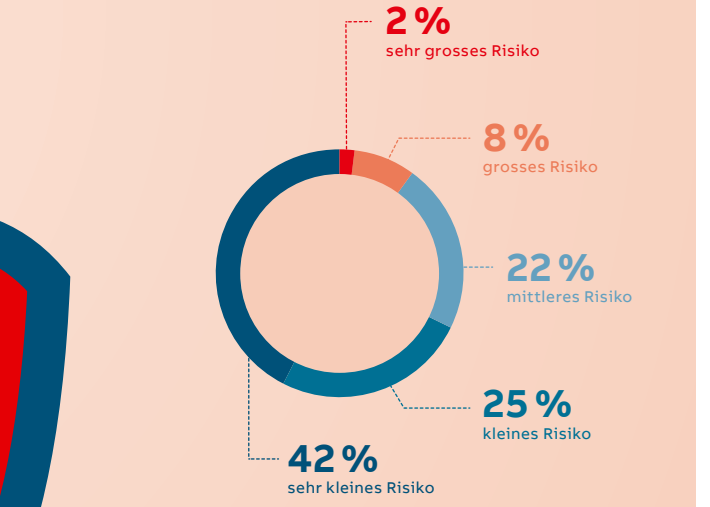
VERMEINTLICHE SICHERHEIT
Mehr als die Hälfte der befragten Schweizer KMUs fühlt sich generell gut oder sehr gut vor Cyberangriffen geschützt.

Die Cyber-Gefahren für industrielle Prozesse sind in den vergangenen Jahren immer mehr in den Fokus geraten. Dennoch unterschätzen viele Verantwortliche das Risiko. Vor diesem Hintergrund ist es wichtig, für geeignete Cyber-Security-Massnahmen zu sensibilisieren und diese auszubauen. ABB hat eine schrittweise Vorgehensweise definiert, durch die die Kunden über mehrere Entwicklungsstufen zu bestmöglicher Sicherheit begleitet werden.

36 %

BEACHTLICHE BEDROHUNG

36 % der befragten KMUs waren schon einmal von Malware wie Viren oder Trojanern betroffen. 6 % waren schon einmal mit einem Datenverlust und 4 % mit einer Erpressung konfrontiert.



GERINGES RISIKOEMPFINDEN

Nur 10 % der befragten KMUs schätzen das Risiko als gross oder sehr gross ein, in den kommenden paar Jahren von einem Cyberangriff betroffen zu sein, der ihren Betrieb mindestens einen Tag lang lahmlegen würde.

Illustration: ©istockphoto.com/akindo

Fragt man in Unternehmen nach Cyber-Kriminalität, gibt es eine bemerkenswerte Diskrepanz zwischen objektiver Gefährdung und deren subjektiver Wahrnehmung. In kleineren und mittleren Unternehmen etwa wird das Risiko von Cyberangriffen unterschätzt: Laut einer Studie im Auftrag des Dachverbands ICTswitzerland und weiterer Partner dürfte mehr als ein Drittel der Schweizer KMUs schon von Cyberattacken betroffen gewesen sein. Eine Mehrheit der Unternehmen fühlt sich aber weiter gut bis sehr gut geschützt. Auch eine Untersuchung des Prüfungs- und Beratungsunternehmens Deloitte zeigt, dass sich insbesondere Firmen, die primär im Schweizer Markt tätig sind, in falscher Sicherheit wiegen. Das liegt auch daran, dass sie sicherheitsrelevante Vorfälle mangels geeigneter Überwachungstools gar nicht entdecken. Die Folgen einer Cyberattacke können allerdings sehr ernst sein: Die potenziellen Schäden reichen von Betriebsausfällen bis zum Diebstahl sensitiver Daten.

Der menschliche Faktor

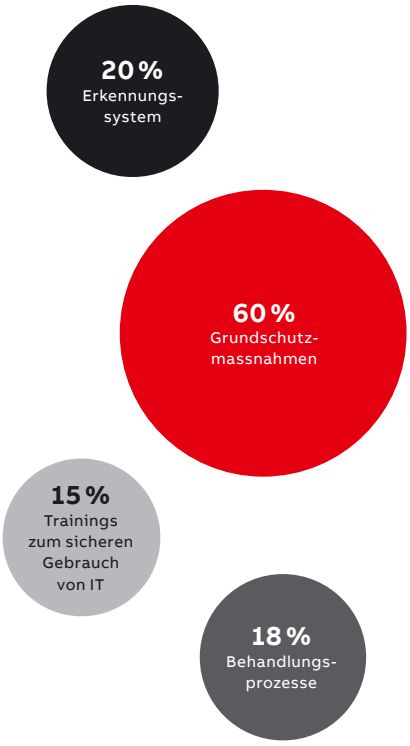
Als wichtiger Aspekt im Zusammenhang mit e-Crime gelten unter anderem auch menschliche Faktoren wie Unachtsamkeit oder ungenügend geschulte Mitarbeitende. Entsprechend sind Wissensvermittlung und Sensibilisierung zent-

rale präventive Massnahmen. Auch lösen Bedrohungen mit grosser Medienaufmerksamkeit – wie WannaCry, das Mirai-Botnetz, Industroyer oder (Not)Petya – in den Organisationen die Reaktion aus, die IT-Sicherheit zu überdenken. Bei der Frage nach den Verantwortlichen für Cyber-Attacken tappen Unternehmen noch vielfach im Dunkeln. Neben einzelnen Hackergruppen stehen häufig organisierte Wirtschaftskriminelle oder staatliche Stellen im Verdacht, sich hinter den Angriffen zu verbergen. Gesicherte Erkenntnisse fehlen aber meist.

Fataler Angriff: ICS Cyber Kill Chain
Häufig folgen externe Angreifer auf industrielle Leitsysteme (Industrial Control System, ICS) dem Handlungsschema der Cyber Kill Chain, das Lockheed Martin entwickelt hat, um Cyber-Angriffe zu beschreiben, und das das SANS Institute für industrielle Leittechnik adaptiert hat. Das Schema besteht zwei grösseren Etappen, die ein immer tieferes Vordringen des Angreifers beschreiben. In Etappe 1 adressiert der Angreifer der Zielorganisation – an sich analog zu «klassischen» Angriffen – auf Unternehmensnetze im Allgemeinen. In Etappe 2 nutzt der Angreifer den Zugang zum Unternehmensnetz, um detaillierte Informationen über die Leittechnik und deren Konfiguration zu sammeln. Auf Basis dieser Informationen entwickelt der Angreifer dann spezifisch auf die Zielorganisation und -anlagen zugeschnittene Angriffspläne, wählt dazu passende Werkzeuge aus oder entwickelt bei Bedarf auch neue Werkzeuge und parametrisiert sie entsprechend der Zielumgebung.

SCION als Internet-Architektur der Zukunft
Eine Arbeitsgruppe an der ETH Zürich ist dabei, mit der neuen Internet-Architektur SCION (Scalability, Control, and Isolation on Next-Generation Networks) viele Sicherheitsmängel des heutigen Internets zu beseitigen. Prof. Dr. David Basin erläutert (siehe auch Kurzinterview auf Seite 14): «Das Internet wurde nicht im Hinblick auf die Sicherheit entwickelt. Bei der Entwicklung der Architektur SCION war Sicherheit von Anfang an ein wichtiges Thema. Die Sender können selbst bestimmen, wie die Daten durch das Netzwerk fliessen. Sobald der Datenverkehr auf einen bestimmten Pfad gelenkt wurde, können Dritte ihn nicht mehr umleiten. Darüber hinaus werden alle netzwerkbezogenen Informationen kryptografisch geschützt.»

Unvollständiger Schutz



Nur 60 % der befragten KMUs geben an, Grundschutzmassnahmen wie Firewall oder Backup voll und ganz umgesetzt zu haben. Systeme zur Erkennung von Cyber-Vorfällen hat nur jedes fünfte Unternehmen vollständig eingeführt. Etwa gleich viele haben definierte Prozesse zur Behandlung solcher Vorfälle vollständig etabliert.

«Das Internet wurde nicht im Hinblick auf die Sicherheit entwickelt.»

Allgemeine Gefahren und spezielle Angriffe
Während der Aufbau von SCION eher noch Zukunftsmusik ist, unterstützt ABB seine Kunden unter den heutigen Gegebenheiten mit einer breiten Auswahl von angepassten Lösungen, um deren Sicherheit effizienter anzugehen. Ragnar Schierholz, Head of Cyber Security bei ABB Industrial Automation, erläutert: «In der IT-Welt sind Verfügbarkeit und Vertraulichkeit von Daten am wichtigsten. In unserer OT-Welt mit hochspezialisierter Leittechnik steht die deterministische Verhaltensweise des Systems im Fokus. Es tut, was es tun soll.» IT und OT überschneiden sich und sind zudem von ähnlichen oder gleichen Gefahren bedroht. «Wir sehen eine Dichotomie, eine Zweiteiligkeit der Gefahren. Einerseits gibt es ein Grundrauschen von Cyber-Gefahren; gegen dieses helfen vergleichsweise einfache Gegenmassnahmen wie regelmässige Patches. Andererseits erleben wir sehr gezielte Angriffe gemäss dem Prinzip der Cyber Kill Chain», sagt Ragnar Schierholz.

—
Einen wesentlichen Anteil an der Verbreitung von Cyber-Gefahren haben Mitarbeitende, die durch Fehler oder Nachlässigkeiten Angriffswege in die Systeme öffnen.

Hier versuchen die Angreifer, sich in mehreren Schritten bis in das Leitsystem vorzuarbeiten. Abhilfe gegen Angriffe auf Unternehmen des Industriesektors und einzelne Anlagen schaffen Gegenmassnahmen, die das Wissen um die Vorgehensweise des Angreifers nutzen und ihn abwehren. «Eine wirksame Abwehrstrategie ist beispielsweise, einen Angreifer in der frühen Phase bereits zu erkennen und zu beobachten, die Sicherheitsmassnahmen auf die spezifischen Charakteristiken des erkannten Angriffs einzustellen und ihn so nichts Wichtiges erreichen zu lassen», erklärt Ragnar Schierholz.

—
«Wir sehen eine Zweiteiligkeit der Gefahren. Einerseits gibt es ein Grundrauschen von Cyber-Gefahren, andererseits erleben wir sehr gezielte Angriffe.»

Mit unterschiedlichen Lebenszyklen umgehen
Erschwerend wirken sich bei der Abwehr von Cyber-Bedrohungen die unterschiedlichen Lebenszyklen von Geräten und Anlagen in den Bereichen OT und IT sowie von (Schad-)Software aus. Während typische Lebenszyklen in der Prozessindustrie bei mindestens zehn bis 20 Jahren liegen, ist die IT-Welt samt Software sehr kurzlebig. «Die Verfügbarkeit und die Prozesskontinuität sind für die Industrie extrem wichtig», sagt Ragnar Schierholz. «Deshalb ist es ratsam, während der Lebensdauer der Anlage jeden Versionensprung über kleinere Updates mitzumachen, um das Risiko für Upgrade-Projekte oder gar Anlagenstopps für grosse IT-Änderungen so gering wie möglich zu halten.»

Vier Mythen zerstören
«Häufig beginnt unsere Beratung bei Industriekunden damit, dass wir die klassischen vier Mythen zur Cyber Security zerstören müssen», sagt Ragnar Schierholz. Der erste Mythos lautet, dass kleine Unternehmen und Branchen ausserhalb der Medienpräsenz kein relevantes Ziel seien. Das ist falsch, weil alles, was es wert ist, besessen zu werden, auch lohnt, gestohlen zu werden. Starke Sicherheit sei Zeit- und Geldverschwendung, lautet der zweite Mythos. Das ist falsch, weil kompromittierte Leittechnik verhindert, Aufträge rechtzeitig oder in erforderlicher Qualität zu erfüllen. Zudem führen nicht adressierte Sicherheitsrisiken zu erhöhten Prämien von Business-Continuity-Versicherungen bis hin zur Ablehnung durch Versicherer. Der dritte Mythos behauptet, unser System sei hermetisch abgeschottet und habe keine Verbindung zur

Aussenwelt. Das ist falsch, weil das Personal Daten in das System ein- und auslagern muss. Wenn keine Kommunikation eingebaut ist, werden praktische und gefährliche Workarounds improvisiert. Das System habe keine direkte Verbindung zum Internet, sodass Angreifer keinen Zugang hätten, lautet der vierte Mythos. Das ist falsch, weil die meisten Vorfälle mehrstufige Angriffe sind und sich die Angreifer im Unternehmensnetzwerk seitlich bewegen, um interessante Ziele zu erreichen.

«Selbst bestimmen, wie Daten fliessen.»

KURZINTERVIEW MIT PROF. DR. DAVID BASIN
ETH ZÜRICH, INSTITUT FÜR INFORMATIONSSICHERHEIT

Welche Sicherheitsrisiken birgt der Datenaustausch über das heutige Internet?
Bedrohungen durch Sicherheitsrisiken sind mittlerweile allgegenwärtig. Unternehmen werden gerne angegriffen, um Informationen zu gewinnen, um sie zu erpressen oder um ihre Systeme und damit ihren Ruf zu schädigen. Extrem problematisch ist die Lage auch bei cyber-physischen Systemen, besonders, wenn ein Zugriff über das Internet möglich ist.

Wie würde die neue Software-Architektur SCION das Internet sicherer machen?
Bei der Entwicklung der Architektur SCION war Sicherheit von Anfang an ein wichtiges Thema. Die Sender können selbst bestimmen, wie die Daten durch das Netzwerk fliessen. Sobald der Datenverkehr auf einen bestimmten Pfad gelenkt wurde, können Dritte ihn nicht mehr umleiten.

Inwieweit hat sich SCION schon in der Praxis bewährt?
Das Team um Professor Adrian Perrig von der ETH hat das Netzwerk SCIONLab gegründet, um SCION in grösseren Umgebungen zu testen. Mit Erfolg: SCIONLab verbindet bereits mehr als 50 autonome Systeme in über 15 Ländern. Darüber hinaus nutzen Internetprovider SCION schon heute, Swisscom beispielsweise seit fast zwei Jahren. Ein Angebot für den industriellen Einsatz wird in den nächsten Monaten bereitstehen.

Das vollständige Interview im Digitalmagazin: http://tiny.cc/davidbasin

In drei Stufen zu mehr Cyber-Sicherheit
Das Ausräumen der Mythen, die Sensibilisierung des Managements und anderer relevanter Ebenen des Unternehmens sowie die Identifikation von Bereichen mit dem grössten Risiko auf der Basis der gemeinsamen Erfahrung zählen zur vorgeschalteten Stufe 0 des dreistufigen Modells von ABB zur Schaffung von mehr Cyber-Sicherheit.

In Stufe 1 führt das Unternehmen den Basisschutz ein und schafft damit die Grundlage für Cybersicherheit im Betrieb. Das mindert die häufigsten Risiken durch Gegenmassnahmen und etabliert ein kontextspezifisches, detailliertes Risikoverständnis.

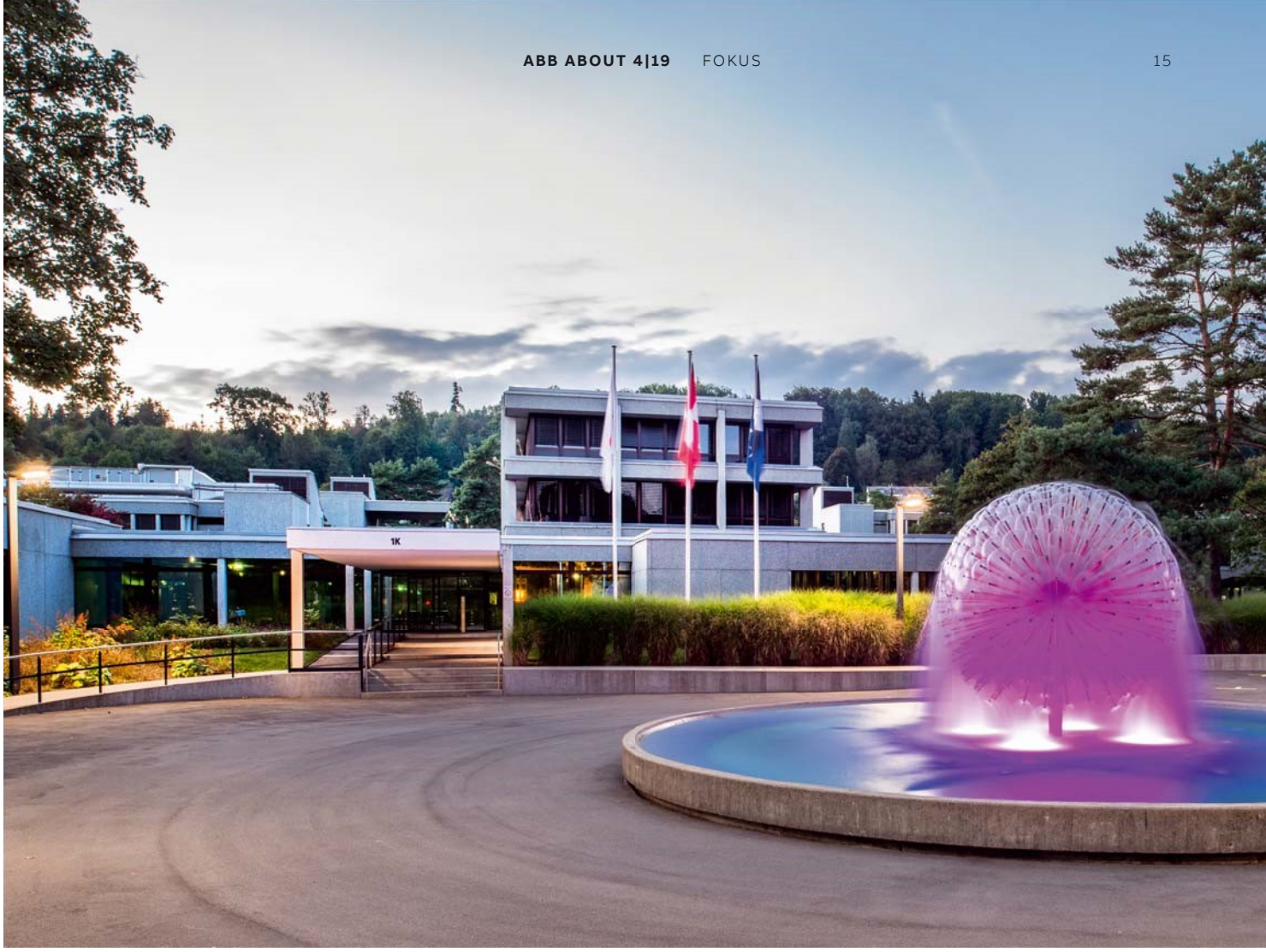
In Stufe 2 baut das Unternehmen unter der Überschrift «Verteidigen Sie Ihr System» ein Sicherheitsmanagementsystem auf der Grundlage der Ergebnisse der Risikobewertung auf, etabliert Sicherheitspraktiken systematisch und hält relevante Normen ein.

«Die Cybersicherheitslösungen von ABB helfen den Kunden, Cyber Security zu einem natürlichen Teil ihrer täglichen Routine zu machen.»

In Stufe 3 beherrscht das Unternehmen seine Risiken. Es verbessert kontinuierlich sein Sicherheitsmanagementsystem entsprechend der Bedrohungslandschaft und dokumentiert die Einhaltung relevanter Normen.

Für die Aufgabenerfüllung in allen Stufen des Modells bietet ABB ineinandergreifende Module aus der ABB Ability Suite an. «Die Cybersicherheitslösungen von ABB helfen den Kunden, bessere Entscheidungen zu treffen, ihre Cyber-Abwehr zu verstärken und Cyber Security zu einem natürlichen Teil ihrer täglichen Routine zu machen», sagt Ragnar Schierholz. Die jeweiligen Servicepakete können selbstständig von Kunden genutzt oder über die ABB-Servicezentren implementiert und verwaltet werden.

Bereit für zukünftige Herausforderungen
An weiteren Lösungen von ABB für Cyber Security in der Zukunft arbeiten die Wissenschaftler im ABB-Konzernforschungszentrum in Baden-Dättwil. Ognjen Vukovic, Head of Cyber



Security Research Team, erläutert: «Im Projekt Service-Ledger untersuchen wir den Einsatz der Blockchain-Technologie in einem Microgrid-Szenario für Smart Contracts und Smart Billing zwischen den Beteiligten des Microgrids.» Als ersten Meilenstein der praktischen Anwendung haben die Forscher blockchainfähige Smart Meter in einer Pilotanlage in der Schweiz eingesetzt. «In einem weiteren Projekt untersuchen wir, welche Gefahren zukünftig beim kriminellen Einsatz von Quantencomputern entstehen könnten, weil diese im Prinzip viele kryptografische Algorithmen knacken, die heute verwendet werden», sagt Ognjen Vukovic. Es ist zwar unwahrscheinlich, dass es in den nächsten zehn bis 20 Jahren praktisch verwendbare Quantencomputer geben wird, aber da ABB digitale Produkte mit einer erwarteten Lebensdauer von über 20 Jahren baut, müssen sie kryptografische Algorithmen verwenden, die von Quantencomputern nicht geknackt werden können. Ein drittes Projekt in Baden-Dättwil hat die Analyse von hochvertraulichen Daten zum Inhalt. «Da viele Kunden sehr sensible Daten wie Betriebsgeheimnisse und Angaben zu Mitarbeitenden nicht in die Cloud senden wollen, untersuchen wir technische Methoden wie die homomorphe Verschlüsselung, die es uns ermöglicht, verschlüsselte Daten zu analysieren, ohne den Schlüssel zu kennen», sagt Ognjen Vukovic. Ein weiteres Thema sind sicherheitskritische Anwendungen, die auf künstlicher Intelligenz basieren: Die ABB-Wissenschaftler forschen daran, wie sich solche Systeme besser gegenüber spezifisch zugeschnittenen Angriffen schützen lassen, die häufig für Menschen nicht erkennbar sind, aber sehr schwerwiegende Folgen haben können.

Weitere Infos:
ragnar.schierholz@de.abb.com
ognjen.vukovic@ch.abb.com

— Sicher in die Zukunft: Im ABB-Konzernforschungszentrum in Dättwil arbeiten Wissenschaftler an der Cyber Security von morgen – mit Technologien wie Blockchain, Quantencomputern und homomorpher Verschlüsselung.