Interview mit Herbert Dirnberger, Cyber Security Austria

„Kunden und Hersteller reden aneinander vorbei“

Elmar Török, bits+bites

Herbert Dirnberger ist seit 20 Jahren in einem großen österreichischen Unternehmen beschäftigt. Seit langem beschäftigt er sich mit der IT-Security in der Automatisierungstechnik, zur Zeit als Fachverantwortlicher für technische Informationssysteme. Zudem leitet Herr Dirnberger die Arbeitsgruppe Sicherheit in der industriellen Automation (SCADA) des gemeinnützigen Verbands Cyber Security Austria.

a+s: *Herr Dirnberger, Sie sind in Ihrem Unternehmen auch für die Sicherheit der Produktionsanlagen gegen Cyber-Angriffe verantwortlich. Seit wann schützen Sie sich bewusst gegen diese Angriffe?*

Dirnberger: Angefangen mit Schutzmaßnahmen haben wir etwa im Jahr 2003, aber ich würde Angriffe nicht an erster Stelle als Grund nennen. Viele und weit häufiger auftretende Gefahren sind banaler Natur. Fehlende Backups beispielsweise. Wenn Steuerungsprogramme von Robotern oder Produktionsdaten versehentlich gelöscht werden, sind die Schäden schnell sehr hoch. Schadsoftware kommt auch viel häufiger durch die unkontrollierte Nutzung von USB-Sticks auf Produktionssysteme als durch externe Angreifer.

a+s: *Damals waren Sie vermutlich einer der ersten, der das Thema anging. Wie sah die Situation aus?*

Dirnberger: Wir mussten am Anfang feststellen, dass viele IT-Security-Maßnahmen nicht für den Bereich Automatisierungstechnik geeignet waren, oder zumindest stark angepasst werden mussten. Virenscanner nahmen zu viel Rechenzeit in Anspruch oder belegten zuviel Arbeitsspeicher durch immer größere Signaturdateien. Dazu gab es auch Abstimmungsprobleme mit der IT-Abteilung. So wurde beim Software-RollOut nicht zwischen Office- und Produktions-IT unterschieden und Software auf allen erreichbaren Rechnern installiert. Die frühen Betriebssysteme waren natürlich auch nicht für den Einsatz in Netzwerken geeignet, das haben wir aber durch den Einsatz von Firewalls und Segmentierung in den Griff bekommen.

a+s: *Glauben Sie, dass das Thema IT-Security in der Produktion in den Unternehmen die notwendige Aufmerksamkeit erhält?*

Dirnberger: Nun, hier hat sicherlich der Angriff durch Stuxnet geholfen, die Leute sind wachgerüttelt worden. Ich werde mittlerweile oft angesprochen, was wir in dem Bereich unternehmen. Allerdings glauben die meisten, dass sie einen gezielten Angriff allein durch technische Maßnahmen in den Griff bekommen. Der Prozess und die Struktur, mit der man jede Sicherheitsmaßnahme

umgeben muss, wird gern vergessen. Zum Teil gehen die Leute auch mit der IT-Security so um, wie sie das vom PC zu Hause gewohnt sind und das reicht natürlich in einer Firmenumgebung nicht aus.

a+s: *Dann wird noch zu wenig unternommen?*

Dirnberger: Klar ist, wir werden uns nie hundertprozentig vor Gefahren schützen können. Die so genannten unbekannten „Unbekannten" kann man nicht im Vorfeld abfangen. Aber darum erzähle ich ja auch in der Fachgruppe der Cyber Security Austria, dass es wichtig ist, viele kleine Maßnahmen umzusetzen und dort etwas zu unternehmen, wo man die Mittel und die Möglichkeit hat. Es geht darum, eine Kette aus ineinander verzahnten Maßnahmen aufzubauen, die sich nicht zerstören lässt, nur weil ein Glied durchbrochen wird.

a+s: *Verstehen die Hersteller im Automatisierungsbereich das Problem? Sind die Produkte in punkto Sicherheit gut entwickelt?*

Dirnberger: Das ist recht unterschiedlich. Einige sind sehr aktiv und haben Abteilungen, die explizit an Sicherheitsfeatures für ihre Produkte arbeiten. Viele hingegen tun nichts oder zu wenig. Es ist schon so, dass die Produkte sicherer werden, mit der Zeit. Nur wissen die Maschinen- und Anlagenbauer noch nicht, wie sie die Produkte sicher einsetzen sollen. Die Automatisierungstechnik ist nun einmal sehr heterogen, jeder vertraut seiner Lösung am meisten und weigert sich nach rechts oder links zu blicken. Der Druck durch die Kunden fehlt noch, das ist ein großes Problem. Leider beschäftigen sich auch noch zu wenige IT-Security-Spezialisten mit dem Bereich Automatisierung. Die sehen die Automatisierung oft als separate Nische, aber man kann das heute nicht mehr trennen. Es gibt auch hier ein paar Vorreiter, aber insgesamt ist das zu wenig.

a+s: *Das klingt, als wären gar nicht ausreichend Produkte vorhanden, um die Systeme abzusichern?*

Dirnberger: Das ist alles eine Frage des Standpunkts. Sicherheit hängt ja nicht nur von Produkten ab. Aber man kann schon sagen, dass es sowohl bei den Automatisierungskomponenten als auch bei den Angeboten von IT-Security-Herstellern einigen Nachholbedarf gibt. Es klappt auch nicht, die Systeme für die Office-IT einfach im Automatisierungsumfeld anzubieten, dazu gibt es zu große Unterschiede in den Umgebungen. Zwar stammen beide eigentlich vom gleichen Ursprung ab, doch sie haben sich stark auseinanderentwickelt. Die IT denkt in großen Umgebungen, stark standardisiert und relativ starr. Automatisierung ist projektbezogen, extrem heterogen und sehr flexibel. Dazu kommt eine unterschiedliche Terminologie. Zum Teil reden Kunden, Berater und Hersteller aneinander vorbei.

a+s: *Worin sehen Sie die größte Herausforderung beim Schutz von Industrieanlagen? Gibt es besonders empfindliche Systeme?*

Dirnberger: Als Techniker muss ich eine klare Antwort geben: Es mangelt fast immer an der Integration des Managements. Das Management muss begreifen, dass es seine Aufgabe ist, Sicherheit bereitzustellen und zwar in der IT und in der Automatisierungsabteilung. Das ist nicht einfach, weil die Bereiche traditionell getrennt sind. Es ist aber auch nicht unmöglich. Ich sage immer: „Man muss die Unterschiede suchen, damit man die Gemeinsamkeiten findet."

Wenn ich Ihre Frage auf einen technischen Aspekt reduziere, dann ist die Antwort auch klar. Die größte Herausforderung sind die empfindlichen und komplexen Systeme. Es gibt so viele Altanlagen, CNC-Maschinen, Roboter usw. die seit langem in Betrieb sind und bei denen eigentlich niemand mehr so richtig weiß, wie sie aufgebaut sind. Genauso gefährlich sind alte Programmiersysteme. Das sind richtige Nadelöhre für Sicherheit. Die Software ist umfangreich, läuft mit Adminrechten, weil man das frü-

her eben so gemacht hat, jeder nutzt USB-Sticks, um die Programme zu verteilen – das sind Schwachstellen, die nur darauf warten, ausgenutzt zu werden.

a+s: *Denken Sie, dass man die Situation durch mehr regulatorische Vorgaben verbessern könnte?*

Dirnberger. Ja, das würde helfen. Die aktuell vorhandenen Standards sind nicht praxisgerecht. Ich kenne niemanden, der die VDE/VDI 2182 einsetzt. Das ist erstaunlich, denn im Bereich Safety gibt es alles und das schon seit langem. Da sind solche Vorgaben überhaupt kein Thema, die werden von allen befolgt. Ich gebe Ihnen ein Beispiel eines Kollegen aus der Branche: Dieser erstellt in seiner Firma gerade Richtlinien für die IT-Sicherheit der Programmiersysteme. Die Schulungen dazu sollen dokumentiert werden, um sicherzustellen, dass diese auch absolviert werden. Daraufhin bekam er zu hören: „Wieso das denn, solche Nachweise macht man doch nur bei Safety." Hier sind die beiden Welten Safety und Security noch sehr weit voneinander entfernt. Darum glaube ich, dass mehr Vorgaben helfen würden. Eigentlich wäre schon ein offizielles Gütesiegel eine tolle Sache, dann könnten Firmen wenigstens einen qualifizierten Berater im Branchenbuch finden.

a+s: *Sie sind Vorsitzender der Arbeitsgruppe Sicherheit in der industriellen Automation (SCADA) bei Cyber Security Austria. Was ist Ihr Anliegen in dieser Gruppe?*

Dirnberger: Wir sind niemandem verbunden, gemeinnützig und arbeiten ehrenamtlich. Unser Ziel ist es, das Wissen, das es in dem Bereich gibt, zusammenzubringen und zu teilen. Es gibt einfach noch zu wenig fundiertes Know-how. Wir wollen sensibilisieren, aber nicht abschrecken. Es geht darum neue Technologie einzusetzen, dies aber sicher. Das erreicht man nicht immer mit neuen Schreckensmeldungen. Wichtig ist auch, dass das Wissen wieder in die Branche zurückfließt, entweder über Inhalte für die Ausbildung, durch die Medien oder über direkte Kontakte zu Herstellern, Integratoren und Betreibern. ■