



VERTRAUENSVOLLE ZUSAMMENARBEIT

von Joachim Gutmann, Glücksburg Consulting AG

Erste IT-Sicherheitsplattform für industrielle KMU

Klein- und Mittelunternehmen (KMU) fehlen zumeist die Ressourcen, um Cyber-Angriffen mit spezialisierten Teams zu begegnen (Computer Emergency Response Teams – CERT). Sie müssen sich verstärkt für betriebsübergreifende Kooperationen öffnen. Da ist Vertrauen unbedingte Voraussetzung. Der Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) hat jetzt eine Lösung gefunden: eine CERT-Plattform.

Die digitale Transformation in Richtung Industrie 4.0 eröffnet große Chancen und Wertschöpfungspotenziale – gerade für den Wachstumsmotor Mittelstand. Zugleich steigt aber mit der fortschreitenden Vernetzung der Produktionsanlagen mit modernen Informations- und

Kommunikationssystemen (IKT) das Risiko von Cyber-Angriffen. Die Bedrohungen reichen von System- und Produktionsausfällen über Fehlfunktionen mit Unfallfolgen bis hin zu Industriespionage und Sabotage. Entsprechend schwerwiegend sind die möglichen Folgen.



Kurzprofil Joachim Gutmann

Joachim Gutmann ist freiberuflicher Journalist und Buchautor. Seine beruflichen Stationen waren Berlin, Bonn, Düsseldorf, Gummersbach und Hamburg. Dort war er in den letzten 17 Jahren für die Glücksburg Consulting AG als Kommunikationsexperte tätig.

Umso wichtiger ist es, IT-Sicherheit als kritischen Erfolgsfaktor für Industrie 4.0 und Digitalisierung zu stärken: erstens durch eine verbesserte Prävention bei der Systementwicklung, zweitens durch eine möglichst schnelle Detektion neuer Sicherheitslücken, drittens durch eine systematische und koordinierte Reaktion auf die Angriffe. Hier setzt CERT@VDE an: die erste Plattform zur Koordination von IT-Security-Problemen speziell für KMU im Bereich Industrieautomation. „Unsere Plattform bietet Herstellern, Integratoren, Anlagenbauern und Betreibern aus dem Bereich Industrieautomation die Möglichkeit, intensiv und vertrauensvoll Informationen auszutauschen“, wirbt Andreas Harner, Leiter des CERT@VDE. Auf der Hannover Messe Industrie wurde die in den VDE-Gremien angeschobene und von Industriemitgliedern des Verbandes entwickelte Plattform erstmals präsentiert.

SENSIBILISIERUNG IST DER ERSTE SCHRITT

Wie wichtig dieses Thema auch für die KMU ist, zeigen die Ergebnisse des VDE Tec Reports 2017, einer Umfrage unter den 1.300 VDE-Mitgliedsunternehmen und Hochschulen. Demnach sind 88 Prozent der Befragten davon überzeugt, dass IT-Sicherheit eine wesentliche Säule der erfolgreichen Digitalisierung darstellt. Und nahezu alle (93 Prozent) vertreten die Ansicht, dass Kritische Infrastrukturen – zum Beispiel im Energiesektor – besonders zu schützen sind. Mehr als die Hälfte der Befragten (53 Prozent) war bereits von Cyber-Attacken betroffen; dabei wurden große Unternehmen (71 Prozent) und bedeutende Hochschulen (68 Prozent) deutlich überdurchschnittlich übers Netz angegriffen. Besonders gefährdet sind dabei die Bereiche Forschung und Entwicklung (78 Prozent), IT/Software (70 Prozent), Produktion (57 Prozent) sowie Planung/Projektierung/Engineering (40 Prozent).

IT-SICHERHEIT AUF DER TECHNOLOGIE-POLITISCHEN AGENDA

Die Sensibilisierung ist also durchaus vorhanden, aber an der Umsetzung der Erkenntnisse hapert es noch bei vielen KMU der Industrieautomation. Während große nationale und internationale Unternehmen und Institutionen meist über ein eigenes CERT verfügen, um den Umgang mit Schwachstellen in den eigenen Systemen zu koordinieren und IT-Sicherheitsinformationen strukturiert bereitzustellen, fehlen KMU dazu in der Regel die Ressourcen. Viele KMU haben noch nicht einmal eine ausgebaute IT-Abtei-

lung, geschweige denn die Kapazität für spezialisierte Notfallteams. Und selbst dort, wo diese bereits eingerichtet wurden, fehlt es noch an Strukturen zur vertrauensvollen Zusammenarbeit mit anderen Herstellern.

„Um dieses notwendige Vertrauen zu fördern“, erläutert VDE-Sicherheitsexperte Harner, „haben wir für die Plattform feste Leitlinien verabredet, die für alle Teilnehmer gelten.“ Basis der Zusammenarbeit auf der IT-Sicherheitsplattform ist eine Vertraulichkeitsvereinbarung. Die Leitlinien konkretisieren diese Vereinbarung und bestimmen die Kooperation mit dem CERT@VDE:

- Die Vertraulichkeit der Kundendaten hat höchste Priorität.
- Die Kooperation ist freiwillig und kann jederzeit beendet werden.
- Businessmodelle Einzelner dürfen unter den Aktivitäten des CERT@VDE nicht leiden.
- Durch wechselseitige Beiträge und Informationen sollen die Arbeitsabläufe aller Mitglieder optimiert werden.
- Informationen und Interessen anderer Mitglieder werden geschützt.

Bei regelmäßigen Arbeitstreffen der Plattformteilnehmer werden diese Leitlinien mit Leben gefüllt und um persönliches Vertrauen bereichert.

AUFBAU EINER WISSENSPLATTFORM

Anders als die bereits bestehenden CERTs in Deutschland (beispielsweise der CERT-Bund des BSI, das als zentrale Anlaufstelle für sämtliche Probleme in Computersystemen fungiert) ist die VDE-Sicherheitsinitiative auf den Bereich der Industrieautomation spezialisiert. „Aber natürlich

DIE SICHERHEITSPLATTFORM ERMÖGLICHT EINEN HERSTELLERÜBERGREIFENDEN AUSTAUSCH AUF EINER NEUTRALEN, VERTRAUENSWÜRDIGEN UND SICHEREN PLATTFORM.

suchen wir die Zusammenarbeit mit anderen CERT und dem CERT-Bund“, sagt Harner. „Voneinander lernen ist nicht nur für die Teilnehmer des CERT@VDE, sondern ganz generell die oberste Maxime.“

Die Sicherheitsplattform ermöglicht einen herstellerübergreifenden Austausch auf einer neutralen, vertrauenswürdigen und sicheren Plattform – natürlich unter Wahrung der Anonymität. Ehemals isolierte Informationen werden im CERT@VDE zentral gebündelt, strukturiert und verteilt, sodass verschiedenste Industrieteilnehmer stets über den gleichen und aktuellen Wissensstand im Hinblick auf Sicherheitsstandards und -gefahren verfügen. Der Zugang zur Plattform, die auch als Wissensdatenbank genutzt werden kann, erfolgt über einen kundenspezifischen Zugang. Eine Cockpit-Benutzeroberfläche erlaubt in Zukunft die Zusammenstellung und Anordnung der für den Benutzer relevanten Sicherheitsthemen. Von einem Angriff betroffene Unternehmen können zudem von IT-Sachverständigen kurzfristig eine Lageeinschätzung einholen und Hilfestellung in Anspruch nehmen.

„Wir schaffen damit effiziente und effektive Kooperationsstrukturen für IT-Sicherheits- und Produktionsverantwortliche und ermöglichen, gemeinsam an der Bewältigung des hohen Sicherheitsrisikos zu arbeiten, welches mit Industrie 4.0 zur zentralen Herausforderung geworden ist“, ist sich Andreas Harner sicher.

CYBER-SECURITY FÜR EINE ERFOLGREICHE DIGITALISIERUNG

Die Plattform ist aber nicht nur die zentrale Know-how-Stelle zum Umgang mit Schwachstellen und ermöglicht deren zeitgerechte Bearbeitung. Für die Teilnehmer werden auch zielgruppenorientierte Schwachstelleninformationen aus diversen Quellen aufbereitet und verfügbar gemacht. Zudem wird über die Plattform die Unterstützung beim Schließen von Sicherheitslücken koordiniert.

Ohnehin sind Koordination und Kommunikation die beiden Leitbegriffe, unter die sich das Selbstverständnis der Plattformbetreiber fassen lässt. So wird über die Plattform

ein firmenübergreifender Austausch zu Sicherheitsproblemen in geschützten Interaktionsräumen organisiert und der Austausch über geeignete Vorgehensweisen angeregt. Für die Teilnehmer aus der Automatisierungsindustrie werden Workshops angeboten und gemeinsam mit Partnern Best Practices erarbeitet.

„Wenn die KMU im Wettbewerb mit den Großen der Branche sicherheitstechnisch mithalten wollen“, weiß Harner, „müssen sie in einer geschützten Atmosphäre die aus Konkurrenzfurcht errichteten Mauern niederreißen und firmenübergreifend voneinander lernen.“ Nur aus dem gemeinsamen Lernen erwachsen schnellere Einschätzungen bei Vorfällen und kann eine effektive Schadensbegrenzung angegangen werden. ■

Der VDE-Verband der Elektrotechnik Elektronik und Informationstechnik ist mit 36.000 Mitgliedern (davon 1.300 Unternehmen) einer der großen technisch-wissenschaftlichen Verbände Europas. Neben der CERT-Plattform betreibt der VDE die VDE/DKE-Kontaktstelle Informationssicherheit (KSI) und führt die Begleitforschung für BMBF-Projekte „Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi)“ sowie „Zuverlässige drahtlose Kommunikation in der Industrie (BZKI)“ durch. Mit der Normenreihe IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ und den Normungs-Roadmaps „IT-Sicherheit“ und „Industrie 4.0“ bringt VDE/DKE, bei dem auch das Standardization Council Industrie 4.0 organisatorisch angesiedelt ist, die Standardisierung der IT-Sicherheit und Industrie 4.0 voran. Im Bereich Prüfung und Zertifizierung bietet das VDE-Prüfinstitut das VDE-Zertifikat „Informationssicherheit geprüft“ an.