"Die Zeit der getrennten Systeme ist vorüber"

Interview mit Thomas Brandstetter, Program Manager Product CERT, Siemens AG

Computer Emergency Response Teams waren noch vor einigen Jahren der IT-Security vorbehalten. Heute gibt es auch im Bereich Prozesssteuerung und Anlagenbau die ersten CERTS, mit der Aufgabe schnell und koordiniert auf Sicherheitsprobleme zu reagieren. Thomas Brandstetter leitet das Product CERT bei Siemens und erlebt dadurch ungefiltert, wie sich die Bedrohungskulisse für Industrieelektronik verändert.

a+s: *Herr Brandstetter, woran liegt es, dass die SCADA-Branche zurzeit allgemein im Sicherheitsfieber ist? Hat Stuxnet das allein ausgelöst, obwohl der Angriff klar definiert und abgegrenzt war?*

Thomas Brandstetter: Stuxnet war meiner Meinung nach der Tropfen, der das Fass zum Überlaufen gebracht hat. Aber eindeutige technologische Trends waren schon vorher zu erkennen. Klassische IT-Technologien sind immer stärker Bestandteil von Industrieanlagen geworden. Das liegt einfach daran, dass die Interoperabilität zwischen SCADA und IT inzwischen eine klare Marktforderung ist. Man macht es dem Kunden leichter, wenn er standardisierte Umgebungen nutzen kann. Das eröffnet aber natürlich auch die Möglichkeit, bekannte Bedrohungen aus der klassischen IT-Welt in die industrielle Anlagenumgebung zu übertragen. Stuxnet war für viele ein Augenöffner, aber für Insider eigentlich in der logischen Konsequenz keine Überraschung.

a+s: *IT-Systeme, die mit dem Internet verbunden sind, werden heute in der Regel unaufhörlich mit automatisierten Attacken angegriffen. Ist das in der SCADA-Welt auch so?*

Thomas Brandstetter: Im Anlagenbereich und bei der Automatisierung ist so etwas durch die bisher meist ausgeübte Abschottung bei Weitem nicht im gleichen Grad feststellbar. Automatisierungsanlagen sind weitgehend in sich abgeschlossen und nutzen möglichst wenige und sehr kontrollierte Verbindungen nach außen. Früher waren die Technologien noch viel stärker proprietär geprägt als heute, mittlerweile öffnen sich jedoch viele Türen durch Standardtechnologien wie Windows und TCP/IP. Dadurch werden natürlich auch aus der IT bekannte Angriffe möglich. Wenn Sie sich die Veröffentlichungen der letzten Monate ansehen, gibt es einige Beispiele, die zeigen, dass Forscher Automatisierungssysteme unabhängig vom Hersteller im Internet fingerprinten konnten. So etwas rührt von Kunden her, die ihre Systeme direkt mit dem Internet verbinden. Dies entspricht natürlich nicht den bekannten Best-Practice-Vorgaben der Hersteller. Die Entwicklung der letzten Jahre hat aber auch dazu geführt, dass man heute ein System kaum noch komplett von anderen Netzen trennen kann. Diese Zeit neigt sich tatsächlich dem Ende zu. Im Moment muss so etwas je nach Anwendungsfall geklärt werden. Es gibt sicherlich Anlagen, in denen die Steuerungssysteme völlig getrennt vom IT-Netz operieren und wo das auch absolut sinnvoll

ist. Allerdings gibt es auch viele Fälle, bei denen Netzwerke verbunden werden. Hier muss zumindest ein Sicherheitszellenkonzept zum Tragen kommen.

a+s: *Was sind Ihrer Ansicht nach die größten Schwierigkeiten, die SCADA-Systeme bei der Sicherheit haben?*

Thomas Brandstetter: SCADA ist in weiten Teilen in puncto Schutzmöglichkeiten nicht mit Anwendungen im Office-Bereich oder im Rechenzentrum vergleichbar. Steuerungskomponenten sind nun einmal auf sehr spezielle Anwendungsfälle zugeschnitten und verlangen ein völlig anderes Konzept als beim PC, der im Prinzip jede Software für den passenden Prozessor ausführen kann. Bei Automatisierungskomponenten kann es in Anlagen zu Laufzeiten zwischen 10 und 30 Jahren kommen. Deshalb ist konzeptbedingt auch kaum noch etwas nachträglich installierbar, um die Funktion einer bewährt laufenden Anlage nicht zu gefährden. Heute sind überwiegend Systeme im Betrieb, die vor 10 Jahren und oft noch weit früher konzipiert wurden. Mit der aktuell zu erlebenden schnellen Öffnung der Netze und dem Transfer zwischen ihnen kommt es natürlich zu Problemen. Doch die Nachrüstmöglichkeiten sind nicht so gegeben wie unter Windows-PCs.

a+s: *Warum gibt es überhaupt so große Lücken in den Steuerungen? IT-Sicherheit ist seit mehr als 10 Jahren ein etabliertes Thema mit entsprechendem Produkt- und Serviceangebot*

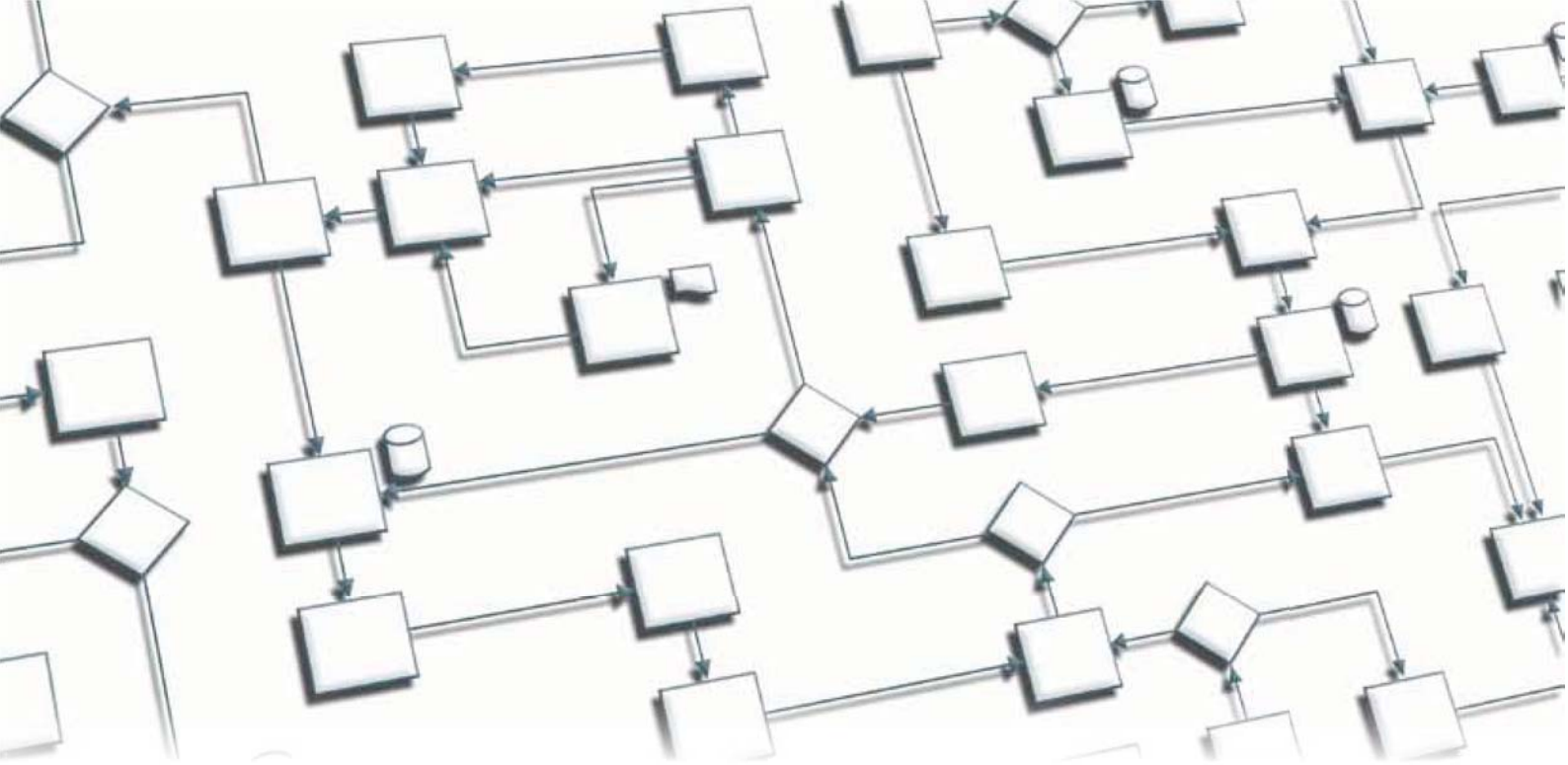
Thomas Brandstetter: Ich würde nicht sagen, dass die Hersteller das Thema Sicherheit verschlafen haben. Als ich vor sieben Jahren zu Siemens kam, wurde dort schon massiv in Anlagensicherheit investiert und geforscht. Jetzt erfährt das Thema noch einmal eine neue Vehemenz, weil die Sensibilisierung steigt. Es gibt mittlerweile Computer Emergency Response Teams (CERT) wie bei Siemens, die zeigen, was an Schwachstellen da ist und worauf sich die Angreifer konzentrieren. Auch im Anlagenbereich werden inzwischen offene Standards und routbare Protokolle eingesetzt, es ist absehbar, dass dadurch auch die Probleme der klassischen IT entstehen werden. Zurzeit bemühen sich die Hersteller um den richtigen Umgang mit solchen Problemen und gehen Fragen nach wie: Wie manifestieren sich Angriffe? Wie geht man mit möglichen Schwachstellen um? Wie bekommt man den erheblich höheren Anteil an OEM-Technologie in den Produkten systematisch in den Griff? Der zweite Punkt sind die recht plakativen Hacking Incidents im Produktumfeld. Es gab bislang sehr wenige Meldungen, doch durch Stuxnet erkannten wir, worauf wir uns vorbereiten müssen. Die Welt ist beim Thema Malware in Industriesystemen langsam aufgewacht. Das hat bestimmt auch etwas mit dem Generationenwechsel zu tun. Wenn ich mir ansehe, mit wem ich im Moment bei den Kunden spreche, dann sind das sehr erfahrene und kompetente Menschen, die über lange Zeit gelernt haben, wie man Prozesse steuert und verwaltet. Das ist klassische Ingenieurskunst einer Altersgruppe tendenziell aus der Vor-IT-Zeit. Diese hat aber den Sicherheitsansatz, der in der IT-Welt in den letzten Jahren doch sehr stark in den Vordergrund drängt, nicht so richtig miterlebt. Die nachrückenden Leute in den Abteilungen sehen mit einem anderen Blickwinkel auf IT- und SCADA-Systeme. Dies ändert natürlich auch die Sichtweise und damit deren Forderungen nach mehr Sicherheit und besserer Reaktion auf mögliche Vorfälle.

a+s: *Inwieweit können klassische IT-Sicherheitskonzepte im Industriebereich angewendet werden? Wo sind die Grenzen?*

Thomas Brandstetter: Die Grenzen liegen dort, wo Prozesse gesteuert werden müssen, die deterministisch sind. Wie kann man das jemals mit Multi-Purpose-Systemen und in Windows-Umgebungen handhaben? Natürlich bringt die Verwendung von standardisierter Hard- insbesondere aber Software auch Vorteile, aber der Betreiber muss genau prüfen, welche Sicherheitsimplikationen dies hat. Wir versuchen passende Empfehlungen gerade zur Absicherung von standardisierter Software zu geben, denn hieraus entstehen derzeit die größten Bedrohungen. Mittlerweile gibt es auch Service-Einheiten, die Kunden unterstützen. Die Grenze liegt aber natürlich auch in der Beschaffenheit und Verteilung eines Produktes beziehungsweise Systems. Wenn wir als Hersteller Komponenten liefern, die beliebig verbaut werden, können wir uns nur auf einen bestimmten Bereich bei der Absicherung konzentrieren. Ein Integrator, der diese Komponenten beim Kunden zu einem Gesamtsystem zusammenfügt, hat hier entsprechend auch die Möglichkeit, für ein System umfassendes Security-Konzept zu sorgen.

a+s: *Sind sich die Hersteller ihrer Verantwortung bewusst? Ist Sicherheit ein inhärenter Bestandteil der Entwicklung?*

Thomas Brandstetter: Mittlerweile kann ich ja sagen, nicht zuletzt auch, weil Sicherheit zunehmend auch von Kundenseite ein Thema ist. Diese fragen gezielt nach Sicherheitsmaßnahmen und möglichen Schwachstellen. Das war viele Jahre lang nicht wirklich im Fokus. Ich denke, auch wenn es ein klassisches Schema der Verantwortungsteilung ist, müssen die Hersteller ihren Teil leisten und Sicherheitselemente in ihre Produkte einbauen. Das haben sie auch gemacht, doch viele der aktuellen Produkte sind schon älter, 10 Jahre und mehr. Der Stand der Technik, auch was die Sicherheit angeht, war damals ein völlig anderer. Nun wird damit begonnen, einen Security-Lifecycle einzuführen. Awareness und Secure Coding



Trainings für die Entwickler – das gehört nun zum festen Repertoire, zumindest bei größeren Herstellern. Ganz große Firmen haben das aufgrund der schieren Menge an Produkten und Entwicklern vielleicht noch nicht durchgehend bis zum letzten Entwickler umgesetzt, aber beispielsweise in unserer Industry Automation-Division läuft ein entsprechendes Projekt.

a+s: *Arbeiten Sie mit Herstellern im Sicherheitsbereich (Anti-Virus, Firewall, IDP/IDS) zusammen?*

Thomas Brandstetter: Ja, das tun wir. Die Industry Automation-Division hat Partnerschaften mit Symantec, Trend Micro und McAfee für Systemlösungen. Wir nutzen neben klassischen Virenscannern, die mittlerweile an ihre Grenzen stoßen, auch andere Konzepte. So sehen wir in Application Whitelisting ein sehr sinnvolles Konzept für die Automatisierungsumgebungen, weil wir es hier mit einer sehr viel statischeren Umgebung im Vergleich zu Office-Anwendungen zu tun haben. Auch das Thema der Integration von SCADA-spezifischen Protokollen in IDP/IDS-Engines ist stärker geworden.

a+s: *Wie sind die aktuell genutzten Protokolle im Industrieautomationsbereich (profinet, etc) für Sicherheit ausgestattet?*

Thomas Brandstetter: Die aktuell genutzten Protokolle sind ein schönes Beispiel für Themen, mit denen die gesamte Industrie kämpft. Die genutzten Protokolle stammen aufgrund der langen Lebensdauer der Anlagen aus einer Zeit, in der Sicherheit ebenso wie Abschottung kein Thema waren. Viele sind Klartext-Protokolle, in den wenigsten Fällen sind echte Krypto-Features enthalten. Damit sind die Protokolle auch vielen Standardprotokollangriffen ausgeliefert. Researcher wie Dillon Beresford, die aus dem reinen IT-Bereich kommen, demonstrieren gerne, dass etwa ein Protokollmitschnitt prima funktioniert. Ich denke, man muss hier eine zweigeteilte Strategie fahren: Es ist unmöglich, diese Technik von heute auf morgen auszutauschen. Während das ein langfristiges Ziel ist, sollte man heute mit zusätzlichen Maßnahmen wie Firewalls, SIEM-Systemen und Whitelisting die bestehenden Anlagen absichern. Was die Entwicklung angeht, sieht man schon deutlich, wohin die Reise geht. So werden in spezifischen Protokollen bereits sehr robuste Sicherheitsfeatures auf Applikationsebene implementiert, auch mit Beteiligung von Siemens. Ein Beispiel ist IEC62351 als Nachfolger von IEC61850 für die Kommunikation im Bereich Substation Energienetze. IEC 62351 definiert eine Reihe von Sicherheitsfunktionen für IEC 61850 und auch für IEC 60870-5 mit dem Fokus auf TCP basierter, serieller und auch (plain) Ethernet basierter Kommunikation auf Applikationsebene.

a+s: *Was ist mit dem Ernstfall? Wie sind die Benachrichtigungsketten? Wer muss benachrichtigt werden? Welche Möglichkeiten gibt es, Angriffe einzudämmen?*

Thomas Brandstetter: Für Siemens kann ich mit gutem Gewissen sagen, dass es einen definierten Incident Response-Prozess für Produkte und Systeme gibt. Dieser wird im Konzern vollständig ausgerollt. Auf Kundenseite sieht die Situation sehr heterogen aus. Es gibt Anlagenbetreiber, die jetzt schon IDS-Systeme haben und die ordentliche Verhaltensbaseline ihrer Systeme sehr gut kennen und damit bei Auffälligkeiten schnell reagieren können. Aber ein durchaus erheblicher Teil hat nach wie vor mit dem Verständnis der Bedrohungen Probleme. Hier werden Standardmittel wie Prüfsummen, Watchdogs, Log-Werte oder Historians genutzt, aber das ist in vielen Fällen eher durch die Anforderung der Dokumentation

des Prozesses getrieben, weniger durch Security-Anforderungen. Demnach gibt es durchaus Nachholbedarf. Zumindest sehen wir, dass es die ersten, speziell auf diesen Bereich zugeschnittenen, Awareness-Schulungen gibt. Auch in unserem eigenen Portfolio sind Security-Beratungen für Anlagen, Risikoanalyse und die Erstellung von Schutzkonzepten zu finden. Solche Angebote werden nachgefragt, wenn auch noch nicht so stark, wie wir uns das wünschen würden.

a+s: *Compliance hat im IT-Security Bereich viel gebracht. Fehlen in der Industrie entsprechende gesetzliche Regelungen?*

Thomas Brandstetter: Wenn ich mir den Stand der Regulierung in Deutschland im internationalen Vergleich ansehe, könnte tatsächlich noch ein bisschen mehr Regulierung auf uns zukommen. In den USA gibt es beispielsweise mit NERC-CIP (Critical Infrastructure Protection) durchaus stringente Sicherheitsvorgaben für Betreiber von Anlagen zur Energiegenerierung, -übertragung und -verteilung. So muss unter anderem einmal jährlich ein Security-Assessment inkl. Schwachstellenprüfung durchgeführt und nachgewiesen werden sowie eine aktuelle Dokumentation über den Cyber-Security Perimeter vorliegen, um zu dokumentieren, was an Sicherheitsmaßnahmen in den Systemen vorhanden ist, und welche Systeme innerhalb des Schutzwalls liegen. Die NERC-Behörde führt Audits durch und verhängt dann pro nicht erfülltem Tag und nicht erfülltem Requirement Strafen – dazu werden Versäumnisse öffentlich gemacht. In gewissem Sinne kann eine auf vernünftigen Anforderungen basierende Regulierung helfen, allerdings muss man auch hier die Grenzen kennen: Compliance-Vorgaben führen nicht in jedem Fall zu einer Verbesserung der Sicherheit, vor allem dann nicht, wenn die Anforderungen des Standards schlecht gewählt sind. Eines wurde mit NERC CIP (Critical Incident Protocol) aber auf jeden Fall erreicht: Die Anwender wurden erstmals dazu verpflichtet, Sicherheitsvorfälle bekannt zu geben. Das zwingt natürlich dazu, sich mit dem Thema auseinander zu setzen und bewirkt damit einerseits eine erhöhte Sensibilität der Betreiber, andererseits erlaubt es erstmals auch die Informationen über geschehene Incidents zusammenzutragen. Dies schafft die Grundlage, sich ein Bild über die Bedrohungslage machen zu können.

a+s: *Sie bauen bei Siemens ein Product CERT auf. Welche Aufgabe soll Ihr CERT haben? Ist das eine Siemens-only Angelegenheit?*

Thomas Brandstetter: Das Siemens Product CERT befasst sich vor allem mit Vulnerabilities in Produkten von Siemens und deren ordentlicher Behandlung sowie mit der Unterstützung bei Hacking Incidents in Kundenanlagen. Wer fürchtet, dass seine Systeme kompromittiert wurden, kann sich an uns wenden. Wir helfen dann mit entsprechenden Methoden wie einer forensischen Analyse sowie dem passenden Produkt-Know-how und untersuchen den Vorfall. Dies kann Bestandteil des Servicevertrags sein oder Individualhilfe. Im Bereich Vulnerability Handling kümmern wir uns darum, dass Schwachstellenmeldungen von externen Stellen wie beispielsweise Security Researchern oder auch Behörden ordentlich angenommen, technisch beurteilt und an den richtigen Produktverantwortlichen gelangen. Daraus entsteht üblicherweise ein Workaround oder Patch sowie ein Security Advisory, das technisch zu einer Schwachstelle Stellung bezieht. Dies ist ein sehr neues und spannendes Feld, da es sowohl technisches Verständnis von Sicherheitsschwachstellen und dem Einsatzgebiet des betroffenen Produktes erfordert als auch diplomatisches Geschick, da wir hier mit sehr vielen Parteien sowohl intern als auch extern zusammenarbeiten müssen, um ein Problem zu bereinigen. Große IT- und Softwarehersteller wie Microsoft und Cisco hatten als erste solche Gruppen eingeführt, typischerweise unter dem Namen PSIRT (=Product Security Incident Response Team). In der Automatisierungswelt ist eine dedizierte, zentrale Abteilung, die sich um Sicherheitsschwachstellen und Incidents bei Produkten kümmert, zum aktuellen Zeitpunk eher noch außergewöhnlich. Gerade in einem Großunternehmen wie Siemens mit tausenden Produkten ist dies aber notwendig geworden, damit sicherheitsrelevante Informationen zeitnah und ordentlich bearbeitet werden können. ■

Über den Autor

Thomas Brandstetter ist seit sieben Jahren bei Siemens im Bereich Produktsicherheit beschäftigt. Er hat lange Zeit präventive Hacking-Tests im Rahmen des Hack-Proof Products Programs durchgeführt und den Bereich Produktsicherheit bei Siemens mitbegründet. Seit dem Stuxnet–Vorfall leitet er das Siemens Product CERT und kümmert sich im Schwerpunkt um das Incident Handling und Schwachstellenmanagement bei Siemens-Produkten