Bild: Fotolia_ bluebay2014

IT-Security – Theorie und Praxis gehen getrennte Wege

In der Theorie ist jedem klar, wie wichtig Netzwerk-Security ist – nicht zuletzt durch Vorfälle, wie Wannacry und Nyetya. Dennoch hapert es in der Praxis oftmals an entsprechenden Sicherheitskonzepten, einem Notfallmanagement oder der Sensibilisierung der Mitarbeiter. Dabei hält der Markt ein breites Angebot an unterschiedlichen Security-Lösungen und -Dienstleistungen bereit, wie die folgenden Beispiele belegen.

Inge Hübner

Mehr als die Hälfte der Unternehmen in Deutschland (53 %) sind in den vergangenen beiden Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Dadurch ist ein Schaden von rund 55 Mrd. € pro Jahr entstanden. Das ist das Ergebnis einer Studie des Digitalverbands Bitkom, für die 1069 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Branchen repräsentativ befragt wurden. Verglichen mit der ersten Studie vor zwei Jahren ist der Anteil der Betroffenen von 51 % auf 53 % gestiegen, der Schaden ist zugleich um rund 8 % von 51 Mrd. € auf 55 Mrd. € gewachsen. „Die Studie unterstreicht, dass wir in Zeiten von Digitalisierung und Industrie 4.0 unser besonderes Augenmerk auf die Abwehr von Spionageangriffen auf die deutsche Wirtschaft richten müssen. Im Sinne eines ganzheitlichen und nachhaltigen Wirtschaftsschutzes gehören dazu nicht allein IT-bezogene Maßnahmen, sondern risikominimierende Pläne in den Bereichen Organisation, Personal und Sensibilisierung“, sagt Bitkom-Präsident Achim Berg. Die Studie führt zudem deutlich vor Augen, wie wenig Unternehmen auf Hacker-Angriffe vorbereitet sind: In lediglich vier von zehn Unternehmen (43 %) existiert ein Notfallmanagement, das festlegt, was zu tun ist. Dabei sind selbst die Betreiber sogenannter kritischer Infrastrukturen (Kritis), wie Energieversorger oder Finanzdienstleister, kaum besser vorbereitet als die übrigen Branchen. So verfügen 53 % der Kritis-Unternehmen über einen Notfallplan, bei den Nicht-Kritis-Unternehmen sind es 41 %. Unter den großen Unternehmen mit

mehr als 500 Mitarbeitern verfügen rund zwei Drittel (68 %) über ein Notfallmanagement, bei Mittelständlern mit 100 bis 499 Mitarbeitern sind es 61 % und bei den kleineren Unternehmen mit 10 bis 99 Mitarbeitern haben sich sogar nur 40 % vorbereitet.

Fragt man andere, stellt sich die Lage nicht besser dar: Im Vorfeld der Fachmesse It-Sa, die vom 10. bis 12. Oktober 2017 in Nürnberg stattfand, wurde eine Umfrage „Trends und Prognosen zur IT-Sicherheit" durchgeführt. Die wichtigsten Erkenntnisse zeichnen ein ähnlich erschreckendes Bild: Obwohl die Budgets wachsen, wappnen sich die Kunden der Aussteller mehrheitlich nicht, bevor ein Angriff erfolgt, sondern investieren erst nach einem IT-Sicherheitsvorfall. Auch hier ist ein deutlicher Unterschied zwischen großen und kleinen Unternehmen bei der Implementierung von IT-Sicherheitsmaßnahmen zu erkennen: Je größer der Betrieb, desto wahrscheinlicher ist es, dass ein systematisches IT-Sicherheitsmanagement verfolgt wird. Konkret verfolgen 70 % der Unternehmen mit mehr als 250 Mitarbeitern nach Einschätzung der It-Sa-Aussteller ein systematisches IT-Sicherheitskonzept. Demgegenüber stehen nur 37 % der Firmen bis 50 Mitarbeitern. Bei Unternehmen zwischen 51 und 250 Mitarbeitern beträgt der Anteil 52 %.

Wer sich schützen will, braucht erst einmal Transparenz

Klaus Mochalski, Experte für Cybersecurity und Monitoring von industriellen Steuernetzen ist Geschäftsführer des Technologieunternehmens Rhebo. Er erklärt: „Gut 10 % der vom Bitkom veröffentlichten Schadenssumme fallen auf Störungen der Fertigung durch Hardwarediebstahl, Sabotage und Manipulation zurück. Die Malwares Wannacry, Industroyer und Notpetya haben dieses Jahr bereits Methoden offenbart, wie Cyberangriffe selbst ganze Produktionen lahmlegen können." Mit der zunehmenden Vernetzung rücke somit auch die Anlagenverfügbarkeit und Produktivität ins Visier der Cyberkriminellen.

Aus Sicht des Experten wird sich dieser Trend sogar verschärfen, wenn die neuen Bedrohungen und die grundlegende Veränderung der IT-Infrastrukturen in automatisierten Unternehmen nicht ernst genommen werden. „Wenn Betreiber von Steuernetzen nicht einmal mit Sicherheit sagen können, wie viel Komponenten in ihrer Fertigung miteinander vernetzt sind – geschweige denn, wie diese miteinander kommunizieren – müssen wir uns über die Schlagkraft von Wannacry und Co. nicht wundern. Transparenz erhält aber nur, wer vollständigen Einblick in alle Aktivitäten seines Steuernetzes hat. Dazu gehört eine detaillierte Analyse jedes

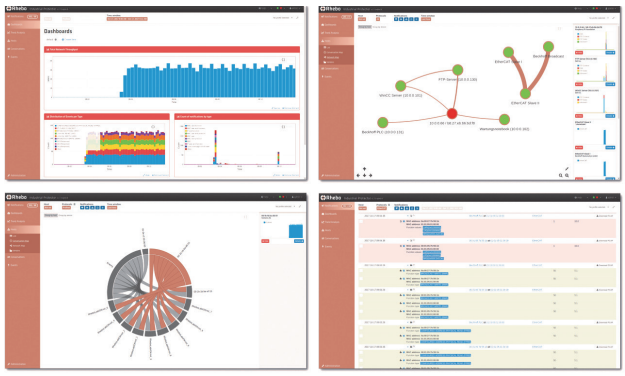


Bild: Rhebo

Rhebo Industrial Protector bietet digitale Transparenz im industriellen Netzwerk in Echtzeit und schützt damit vor Störungen und Cyberangriffen

Datenpakets genauso wie die Meldung jeder verdächtigen Abweichung im Kommunikationsmuster und die Priorisierung der Vorfälle durch ein eindeutiges Risk Scoring. Das Stichwort ist hier Anomalieerkennung." Dabei stärkt diese Form des Network Monitorings aus seiner Sicht Unternehmen nicht nur in Bezug auf Cybersicherheit, sondern optimiere auch die Produktivität und Störungsfreiheit von Fertigungsanlagen und kritischen Infrastrukturen. „Unternehmen müssen endlich beginnen, wieder Herr ihrer Steuernetze zu werden", ruft K. Mochalski zum Handeln auf. Mit seinem Unternehmen Rhebo hat er sich auf die Ausfallsicherheit industrieller Steuersysteme mittels Überwachung der Datenkommunikation spezialisiert. Das Angebotsspektrum umfasst Hardware, Software und Dienstleistungen, um vernetzte industrielle Steuerungssysteme und kritische Infrastrukturen zu schützen und ihre Produktivität zu steigern.

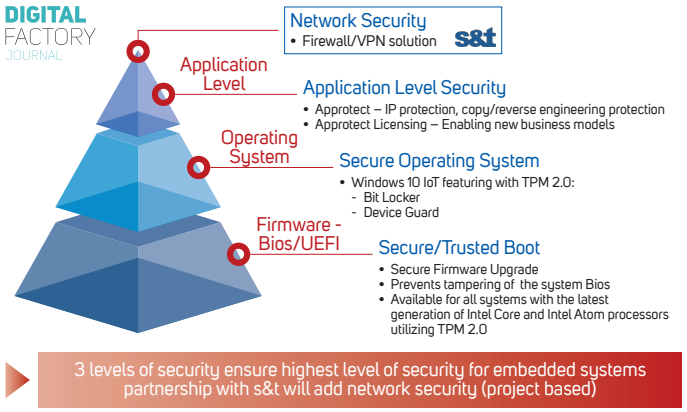
Dreistufiges Secure-System-Konzept

Aus Sicht von Kontron gehört es für Unternehmen, Behörden und Organisationen zur Pflicht nicht nur die Vorteile des Internet der Dinge, von Industrie 4.0, Smart Home und Co. mitzudenken, sondern mindestens gleiches Augenmerk auf die damit verbundenen Risiken zu legen. Aufgabe von Komponentenanbietern sei es, Lösungen und Systeme zur Risikominimierung anzubieten sowie diese einfach und kostengünstig implementierbar zu machen. Dazu bietet Kontron seit Anfang 2017 das Secure-System-Konzept an, das auf drei Stufen beruht: der Absicherung des Bios, des Betriebssystems sowie der Anwendungen und ihrer Daten. Eine Säule bildet dabei die Security Solution Approtect, die in allen neuen Kontron-Produkten standardmäßig enthalten ist und sich teilweise auch bei bereits implementierten Komponenten einfach nachrüsten lässt. Leitgedanke bei der Entwicklung von Approtect war, den komplexen Prozess der effizienten Absicherung von Endgeräten, in günstigere kleine, je nach Bedarf individuell kombinierbare, Teilstücke zu gliedern. „So lassen sich auch spezifische Sicherheitsanforderungen abdecken, ohne zum Ressourcenfresser zu werden. Kunden sind nicht länger gezwungen, sich mit teuren Investitionen vor unendlich vielen, für sie teils hypothetischen Bedrohungsszenarien zu schützen", informiert dazu Norbert Hauser, Vice President Marketing von Kontron.

Der von Kontron in seiner Security Solution zu diesem Zwecke verwendete Sicherheitschip von Wibu-Systems, verfügt über einen Kontrollmechanismus, der die Verschlüsselung der Anwendung überprüft. So wird sichergestellt, dass das Programm auch wirklich nur von den dafür vorgesehenen Geräten ausgeführt werden kann. „Durch einen stetigen Austausch mit dem Chip, der im laufenden Betrieb kontinuierlich Teile der Applikation entschlüsselt, wird zudem dafür gesorgt, dass Anwendungsdaten nicht einfach aus dem Arbeitsspeicher ausgelesen werden können. Kontron schützt damit Anwendungen ohne zusätzlichen Kompilierungsaufwand oder komplizierte Schlüsselverwaltungsprozesse", erklärt N. Hauser weiter.

Darüber hinaus lassen sich mit Approtect Licensing neue Geschäftsmodelle etablieren. So könnten beispielsweise einzelne Anwendungsfunktionen auf einen bestimmten Zeitraum oder eine definierte Ausführungszahl beschränkt werden. Das kann für Testszenarien nützlich sein, aber auch andere innovative Einsatzmöglichkeiten sind denkbar.

„Für Kontron ist die IT-Sicherheit im IoT ein zentrales Element der Digitalisierungsstrategie unserer Kunden und deshalb als Kontron-Standard in allen Produkten serienmäßig enthalten. Eine Hardwarebasis, die Sicherheitsmechanismen schon von Haus aus integriert, vereinfacht den Implementierungsprozess von IoT-Anwendungen enorm, macht die Produktentwicklung effizienter und unsere Kundendesigns zukunftssicher. Bestehende Systeme können per Nachrüstkits auf Basis von ‚mPCIe'-



Kontron-Secure-Systems-Konzept. Kontron bietet damit als einer der ersten Embedded-Computer-Hersteller einen ganzheitlichen Ansatz zur Absicherung von Embedded-Systemen unter Einbeziehung von drei sicherheitsrelevanten Ebenen eines Endgeräts: der Bios- (Secure Bios), der Betriebssystem- (Secure OS) und der Anwendungsebene (Secure Application)

Handlungsempfehlungen von Cisco

Im Rahmen der Veröffentlichung der Ergebnisse seines Cisco Midyear Cybersecurity Report haben die Netzwerkspezialisten auch Handlungsempfehlungen herausgegeben. Um komplexere Angriffe zu bekämpfen, raten sie Unternehmen zu einer proaktiven Haltung und folgender Vorgehensweise:

- Infrastruktur und Anwendungen stets auf dem neuestem Stand halten, damit Angreifer öffentlich bekannte Schwachstellen nicht ausnutzen können.
- Ein integrierter Verteidigungsansatz reduziert die Komplexität; isolierte Investitionen vermeiden.
- Frühzeitig die Führungsebene einbeziehen, um ein umfassendes Verständnis der Risiken, Vorteile und Budgeteinschränkungen zu gewährleisten.
- Eindeutige Kennzahlen definieren, um Sicherheitspraktiken zu validieren und zu verbessern.
- Sicherheitsschulungen im Unternehmen nicht übergreifend durchführen, sondern auf die jeweilige Funktion abgestimmt.
- Verteidigung und aktive Reaktion ausbalancieren; Sicherheitskontrollen oder Prozesse nicht „einmal einrichten und vergessen".

www.cisco.com

Modulen oder USB-Sticks mit der Lösung ausgerüstet werden", erklärt N. Hauser zusammenfassend.

IT-Sicherheitslösungen für digitale Industrieprozesse

Ein ebenfalls mehrstufiges Sicherheitskonzept für den Netzwerkschutz in der Industrie 4.0 bietet Rohde & Schwarz Cybersecurity an. Das Angebot umfasst zum einen die Lösung R&S Industrial Network Analytics, bestehend aus der IP Probe R&S Net Sensor und der Analyseplattform R&S Net Reporter, welche in Echtzeit Informationen über den Zustand eines Netzwerks liefert. Damit werden frühzeitig Probleme erkannt, die aus infizierten Maschinensteuerungen, Fehlkonfigurationen oder potenziellen Cyberangriffen resultieren können. Zum anderen lassen sich auf Basis dieser Analyse mit den Gateprotect-Firewalls der „Specialized Line", die notwendigen Schutzmaßnahmen einrichten und Angreifer schnell und sicher abwehren. Die Firewalls wurden speziell für komplexe industrielle Umgebungen mit hohem Schutzbedarf konzipiert und unterstützen Scada-Protokolle, wie IEC 60870-5-104, Modbus oder DNP 3.

Mit der Lösung R&S Industrial Network Analytics gewinnen Industrieunternehmen den Überblick und die Kontrolle über ihre dynamisch wachsenden Industrienetzwerke. Das Event-Monitoring des R&S Net Reporters weist Administratoren und Betreiber industrieller Netze proaktiv auf mögliche Probleme im Netz hin und ermöglicht ein zeitnahes Troubleshooting, bevor die Produktion davon beeinflusst wird. Dies verschafft den Unternehmen die Grundlage zur Sicherung eines kontinuierlichen Betriebs und ermöglicht darüber hinaus eine genauere Planbarkeit hinsichtlich Netzwerkauslastung und -dimensionierung. Vor allem angesichts einer zunehmenden Vernetzung mit externen Partnern bei der Fernwartung von Anlagen, des Austausches von Produktdaten zwischen Produktionssystemen, der permanenten Zustandsüberwachung

Bild: Rohde & Schwarz Cybersecurity

Mit R&S Industrial Network Analytics erhalten Unternehmen Überblick und Kontrolle über ihre dynamisch wachsenden Industrienetzwerke

von Anlagen (Condition Monitoring) und der engen Synchronisation mit Logistikprozessen, sind solche Analysen aus R&S-Sicht zunehmend erforderlich.

Sowohl die „Specialized Line" als auch der R&S Net Sensor arbeiten mit der „Deep-Packet-Inspection"-Technologie (DPI): Diese versetzt beide Lösungen in die Lage, Datenströme auf Inhaltsebene zu decodieren und zu klassifizieren. Auf Grundlage dessen kann in der Firewall ein feingranulares Regelwerk eingerichtet und dementsprechend nicht erlaubter Datenverkehr vollständig abgeblockt werden. Dieses sogenannte „Whitelisting" stellt sicher, dass Industrienetzwerke nur von autorisierten Personen mit definierten Befehlen angesteuert werden können. Die DPI-Engine R&S Pace 2 kann um Kommunikationsprotokolle erweitert und passgenau in die Prozessnetzwerke integriert werden.

Verteidigung – in der Tiefe gestaffelt

Das Thema Fernwartung bzw. Remote Control ist bereits angeklungen. Es ist davon auszugehen, dass es im Zeitalter von Industrie 4.0 weiter an Bedeutung gewinnen wird. Diesem Thema widmet sich die Zedas GmbH bereits seit Längerem. Aus ihrer Sicht gilt es, den Wildwuchs von Lösungen für den Remote Service zu beseitigen und ihn durch eine zentrale und sichere Lösung zu ersetzen, die der eigenen Verantwortung unterliegt. „Bewährte Sicherheitskonzepte, ergänzt mit einer einfachen Steuerung und Kontrolle durch Mitarbeiter aus den Produktionsbereichen, sind zwingende Grundlagen dafür, die Hoheit über die eigenen Anlagen zu behalten", sagt Ulrich Lieske, Leiter der Business Unit Systemintegration. Aus den jahrelangen Erfahrungen der Integration eigener Softwarelösungen entwickelte die Zedas eine Remote-Service-Lösung, die erprobte Sicherheitsverfahren mit einer speziellen Staffelung in der Tiefe bei einfacher Handhabung kombiniert. „Unsere standardisierte Lösung ‚SecureFactoryRAS by zedas' gewährleistet den Schutz auf mehreren Ebenen. Sie ermöglicht es produzierenden Unternehmen, einfach und schnell eine zentrale Lösung out-of-the-box für alle seine externen Service-Dienstleister zu etablieren", verdeutlicht U. Lieske. Neben den bekannten und üblichen Maßnahmen zur Absicherung der Netzwerkzugänge (Authentifizierung mit PIN und Einmal-Passwort, Network Admission Control) und der Netzwerksicherheit (Zertifikate, Verschlüsselung, Firewall, Sicherheitszonen) erfolgt zusätzlich eine Absicherung auf den Ebenen der zentral bereitgestellten Fernwartungsrechner, der für den Service verwendeten Softwareanwendungen sowie der betrieblichen Organisation der Zugriffssteuerung und -protokollierung. „Mit dem umfassenden Einsatz von Virtualisierungstechnologien ist unsere Lösung sehr gut skalierbar. Sie bietet tief gestaffelte Sicherheitsfunktionen auf Hardware-, Netzwerk-, Software- und Organisationsebene. Im praktischen Einsatz loben Produktionsverantwortliche die schnelle Erfassung von Serviceanforderungen sowie die einfache Handhabung", stellt U. Lieske abschließend heraus.

SecureFactoryRAS by zedas® - Checkliste Sicherheitsfunktionen

- ☑ Zugang über gesichertes Internet-Web-Portal
- ☑ Starke Authentifizierung (Pin und One-Time-Password)
- ☑ (Mehrere) virtuelle Fernwartungsrechner pro externer Servicefirma in DMZ (Demilitarized Zone)
- ☑ Getrennte DMZ pro externer Servicefirma
- ☑ Abgesicherter Desktop und einfaches Freischalten/Sperren einzelner Service-anwendungen
- ☑ …

Die komplette Checkliste finden Sie auf unserer Homepage www.zedas.com

Checkliste der verfügbaren Sicherheitsfunktionen

Cyber Security Rating für Unternehmen

Neben diesen Lösungen, die dem aktiven Schutz vor Hacker-Angriffen dienen, beschäftigt sich der Hamburger IT-Sicherheitsspezialist Secion mit einem ganz anderen Thema: der Klassifizierung der IT-Sicherheit von Unternehmen. Dazu hat er mit der Marke Ratingcy einen neuen Geschäftsbereich eingerichtet. „Vor dem Hintergrund des immensen Schadens, der in Unternehmen jährlich durch Spionage, Sabotage und Datendiebstahl entsteht, bekommt die Evaluierung der IT-Sicherheit von Unternehmen eine ganz neue Bedeutung", erklärt Marcus Henschel, Geschäftsführer bei Secion. „Üblicherweise einbezogene Bewertungskriterien, wie Bonitätsindex und Ausfallrisiko, lassen allein keine valide Klassifizierung von Drittunternehmen zu. Vielmehr muss der Bewertungsfaktor IT-Sicherheit als dritter Indikator anteilsgleich mit in das Ergebnis einfließen, um eine objektive Bewertung des Unternehmensrisikos zu erreichen. Die Lösung ist ein einheitliches Sicherheits-Rating. Wir machen diese Erfahrung auch im Beratungsalltag: Nach Abschluss unserer Security Audits werden wir immer wieder von Kunden gefragt, wie sie im Vergleich zu anderen Kunden aus ihrer Branche abgeschnitten haben. Auf diese Nachfrage reagieren wir als Erste in Europa mit Ratingcy."

Ratingcy setzt auf ein zweistufiges Verfahren, um die Frage nach einem einheitlichen und vergleichbaren Cyber Security Rating zu beantworten. Im ersten Schritt findet eine technische IT-Sicherheitsüberprüfung statt. „Alle vom Internet zugänglichen Dienste des Unternehmens werden vollautomatisch auf vorhandene Sicherheitslücken untersucht. Im Anschluss erstellt Ratingcy

automatisiert ein Risk Score aus allen gefundenen Schwachstellen", sagt M. Henschel.

Der zweite Teil der Sicherheitsbewertung beinhaltet einen organisatorischen Fragebogen, der an die Vorgaben des IT-Grundschutzes sowie an die ISO 27001 und ISO 27002 angelehnt ist. Dabei geht es unter anderem um die organisatorische Bewertung von implementierten Geschäfts- und IT-Sicherheitsprozessen.

„Die beiden Teilergebnisse verrechnen wir nach einem transparenten Verfahren. Als finales Ergebnis erhalten die Kunden unter anderem einen Risk Score sowie ein Ratingcy-Ergebnisdiagramm, aus dem der Wert der IT-Sicherheit des Unternehmens im Vergleich zum Branchendurchschnitt abgelesen werden kann. Auch fachfremde Personen können hieraus konkrete Empfehlungen zur Verbesserung des Ratings ableiten", erklärt M. Henschel.

Fazit

Der Beitrag gibt lediglich einen sehr kleinen Einblick in den Gesamtmarkt an Security-Lösungen und -Möglichkeiten. Abschließend sei noch auf die Normenreihe IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme" hingewiesen. Sie legt den Grundstein für eine ganzheitliche Betrachtung von Industrial Security im gesamten Lebenszyklus von Automatisierungslösungen. In Deutschland wurde 2016 die erste Zertifizierung nach dieser internationalen Norm durch TÜV SÜD vorgenommen. Der ZVEI hat einen kostenlosen „Orientierungsleitfaden für Hersteller zur IEC 62443" herausgebracht. Er bietet eine Übersicht relevanter Anforderungen für Herstellerunternehmen, gibt einen Einstieg in die IEC 62443 und unterstützt bei der Anwendung der Norm bzw. geht auf die Anforderungen für Hersteller ein.

www.bitkom.org
https://cybersecurity.rohde-schwarz.com/de
www.it-sa.de
www.kontron.de
www.ratingcy.com
www.rhebo.com
www.tuev-sued.de
www.wibu.com/de
www.zedas.com
www.zvei.org