Risiken aktiv managen, jetzt

Datenschutz Was treibt Unternehmen in punkto Cyber Security derzeit um? Wie weit ist die Umsetzung der europäischen Datenschutzgrundverordnung (EU-DSGVO)? Worum geht es bei der Proaktiven Cyber Security Intelligence und warum ist es so wichtig, die Industrie 4.0 anders als früher abzusichern? Eine Momentaufnahme.

Björn Haan*

Einer der größten Schmerzpunkte ist zurzeit die Umsetzung der europäischen Datenschutzgrundverordnung (EU-DSGVO). Die Anforderungen sind so komplex und hoch wie nie. Nach jüngsten Berechnungen benötigt man für die exakte Umsetzung rund fünf Personenjahre. Das stellt auch veränderte Anforderungen an Berater: Die Auflagen fordern neue Prozesse, Workflows und Kontrollmechanismen, aber auch Antworten auf technische Fragen. Ob es nun um Verschlüsselung, Identity- und Access-Management, Data Leakage Prevention oder Threat Management geht. Wichtig ist es, das gesamte Bild im Blick zu haben. Die EU-DSGVO hat mit Fragen traditioneller Data Privacy-Lösungen nur noch wenig zu tun. Es handelt sich um gewaltige Veränderungen bis hin zur betrieblichen Mitbestimmung und der Beantwortung juristischer Fragen. Ob das Gros der Unternehmen die Deadline wird halten können, ist fraglich. Zu umfänglich sind die notwendigen Anpassungen, die auch ein „neues" bzw. erweitertes Skill Set erfordern.

Angesichts der Dynamik der Bedrohung einerseits und der wachsenden regulatorischen Anforderungen andererseits wird es künftig nicht mehr reichen, die technologische Entwicklung nachzuvollziehen – und damit den Angreifern hinterherzuhinken und sich allein um Abwehr zu bemühen. Zu den spannendsten Themen in der Informationssicherheit zählt aktuell die Proaktive Cyber Security Intelligence. Ziel ist es, Sicherheitsvorfälle nicht mehr nur passiv zu erkennen und „hinzunehmen", sondern über verschiedene Kanäle proaktiv Informationen zu sammeln und so zu verknüpfen, dass Erkenntnisse über mögliche nächste Hacker-Attacken und entsprechende Schutzmaßnahmen möglich werden. Wichtige Stichworte sind hier Darknet und Deepnet Mining, die sich mit Fragen befassen wie: Welche Techniken werden in einschlägigen Hacker-Foren diskutiert? Welche „Tools" und „Services" an Schadsoftware werden auf Marktplätzen gerade angeboten bzw. nachgefragt? Auf Basis maschinellen Lernens und intelligenter Datengewinnung sollen nun bestimmte Lösungen in der Lage sein, mehr als 90 Prozent entsprechender „Produkte" und rund 80 Prozent der Diskussionen, die sich in Foren mit Schadsoftware befassen, präzise identifizieren zu können.

Mit einer solchen kontextbezogenen Advanced Cyber Defense, die Informationen in Echtzeit auswertet, hätten Unternehmen die Chance, ein proaktives Cyber-Security-Management zu betreiben, indem sie Themen identifizieren, bevor sie zu einem echten Risiko werden. Die Daten, von denen hier die Rede ist, nutzten Anbieter von Sicherheitslösungen früher „nur" zur Verbesserung ihrer eigenen Produkte. Heute stellen sie diese gewissermaßen im „Abo" zur Verfügung.

Zudem wächst die Nachfrage nach Penetrationstests exponentiell. Cyber Security war in den Management-Etagen lange nur ein Kostenfaktor. Mit gewachsenem Bewusstsein steigert das jetzt allerdings den Bedarf nach Fachkräften. Obgleich die Automatisierung hier

*Björn Haan, Geschäftsführer im Geschäftsfeld Cyber Security Deutschland, TÜV Rheinland

FUNCTIONAL SAFETY UND CYBER SECURITY

„Die KPI werden sich verändern."

Sie setzen sich dafür ein, dass Cyber Security und funktionale Sicherheit in der Industrie 4.0 integriert betrachtet werden. Warum ist das aus Ihrer Sicht wichtig?
Die Produktionsstraße wird sich immer stärker vernetzen. Alle Player sind miteinander verbunden, vom Hersteller über Zulieferer bis hin zum Maintenance-Dienstleister. Einer der nächsten Level ist die Kommunikation zwischen Werkstoffen, Produkten und den verarbeitenden Maschinen. Das ist ein unglaubliches Potenzial. Es zeigt aber auch, dass es wichtiger denn je ist, die damit verbundenen Risiken aktiv zu managen. Ein erhebliches Risiko ist es, in diesem Zusammenhang Cyber Security zu vernachlässigen. Dies ist für IoT und Industrie 4.0 unerlässlich, zur Absicherung zentraler Versorgungssysteme, als wesentliche Voraussetzung für die funktionale Sicherheit in Fertigungsprozessen, für den sicheren automatisierten Datenaustausch vernetzter Systeme sowie für die Verfügbarkeit der Produktion.

Warum ist dieser Ansatz eine Herausforderung?
Beide Disziplinen – Functional Safety und Cyber Security – haben unterschiedlichste Erfordernisse, die sich diametraler nicht entgegenstehen könnten. Bei ersterer geht es darum, die Menschen vor den Auswirkungen der Technik zu schützen, zum Beispiel durch Fehlfunktionen von Maschinen, hervorgerufen durch ungewollte oder unberechtigte Eingriffe in IT-Komponenten. Functional Safety greift auch, wenn es darum geht, dass Abläufe wie vorgesehen funktionieren und beim Auftreten von Fehlern entsprechende Maßnahmen sichergestellt sind. Cyber Security zielt darauf ab, Fabrikautomation und Prozesssteuerungen abzusichern. Hier geht es um Schutz und Verfügbarkeit von Kontroll- und Steuerungssystemen gegen absichtliche herbeigeführte oder ungewollte Fehler. Ziel muss es sein, eine Störung oder gar einen Ausfall der Produktion zu verhindern.

Wie kann eine verlustfreie Integration von Functional Safety und Cyber Security gelingen?
Aus unserer Sicht ist der „by-design"-Ansatz zentral. Beide Disziplinen werden darin zu Beginn des Lebenszyklus sämtlicher Komponenten integriert berücksichtigt. Die Entwicklung von Anlagen und Komponenten muss so gestaltet sein, dass mögliche Sicherheitslücken schon im kleinsten Bauteil idealerweise vermieden oder bereits so früh wie möglich erkannt und eliminiert werden. Es ist nicht weniger als ein Paradigmenwechsel, der Cyber Security als Teil des Business Case versteht. Dieser muss getrieben werden von Menschen, die beide Seiten begreifen. Etwa der Digitalization Officer, der die Zukunft im Kontext der Digitalisierung auf Basis klassischer IT-Verbindung mit dem Prozess-Know-how versteht. Denn auch die damit verbunden KPI werden sich verändern, die Datenmasse, die entsteht, muss nicht nur erfasst und analysiert werden. Die Verantwortlichen müssen auch die richtigen Empfehlungen daraus ableiten können. Auch hier kommt der proaktiven Cyber Security Intelligence eine enorme Bedeutung zu. Darüber hinaus wird für Hersteller von IoT-Lösungen der Nachweis, Datenschutz und Datensicherheit eine hohe Priorität einzuräumen immer wieder wichtiger, etwa durch Zertifizierungen.


Bild: Lothar Weis

„Die technologische Entwicklung nachzuvollziehen, reicht nicht mehr."

Björn Haan,
Geschäftsführer im Geschäftsfeld Cyber Security Deutschland, TÜV Rheinland

Welche Rolle spielt im Zusammenhang mit der EU-DSGVO das Thema Zertifizierung?
Die EU-DSGVO bietet Verantwortlichen und Auftragsverarbeitern die Möglichkeit, sich einem gesetzlich festgelegten Zertifizierungsverfahren zu unterziehen. Es dient dem Nachweis, dass die Bestimmungen vollumfänglich eingehalten werden. Dies wird zukünftig eine wichtige Rolle spielen, so unter anderem bei der Entscheidung über das Ob und die Höhe von Bußgeldern.

ebenfalls weiter voranschreitet, bedarf es nach wie vor der Menschen, die in der Lage sind, Sicherheit umfassend zu konzipieren, Sicherheitsvorfälle zu monitoren, Ergebnisse auszuwerten und auf dieser Basis die richtigen Entscheidungen zu treffen. Notwendig ist ein völlig neuer, integrierter Ansatz: Schulen und Universitäten müssen den Nachwuchs heranbilden und ganzheitliche Kompetenzen vermitteln, die für eine sichere, vernetzte Zukunft erforderlich sind. Bis dahin werden Unternehmen nicht umhin kommen, mit Managed Services diese Herausforderungen zu bewältigen.

Cyber Security ist nicht alles, aber ohne ist alles nichts. Es ist und bleibt der neuralgische Faktor für eine erfolgreiche digitale Transformation. Das ist der Grund, warum Unternehmen wie TÜV Rheinland selbst viel Zeit und Geld in die Aus- und Fortbildung investiert. Um diese Fachleute zu entwickeln und zu halten, sind wirksame Konzepte rund ums lebenslange Lernen der wichtigste Schlüssel, um am Puls der Zeit zu bleiben und Innovation und Weiterentwicklung von Firmen überhaupt zu ermöglichen. [in]

Ines Stotz,
Chefredakteurin
ines.stotz@vogel.de

Vielen Unternehmen ist es zu raten, die DSGVO über weite Strecken eins zu eins umzusetzen. Warum, zeigt auch dieser Beitrag auf bit.ly/2oSW2MV