MEINUNGEN

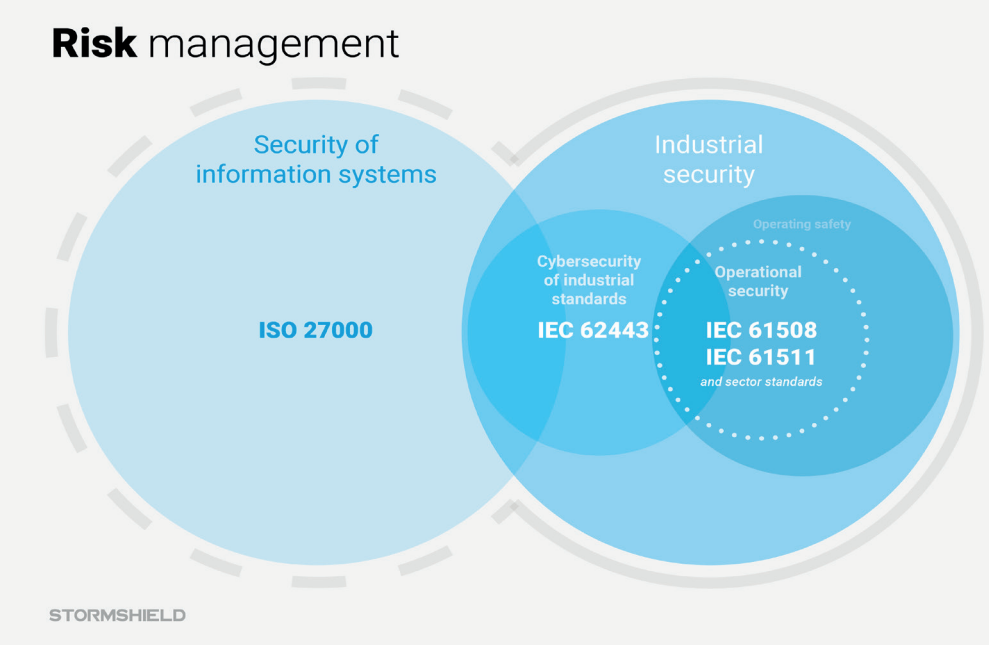
IEC 62443, DIE UNUMGÄNGLICHE NORM IM BEREICH CYBER-SICHERHEIT FÜR DIE INDUSTRIE

Vincent Nicaise
Industrial Partnership and Ecosystem Manager, Stormshield

Lange Zeit schienen die Cyber-Risiken in der Industrie nur empfindliche Branchen wie die Energie- oder die Nuklearbranche zu betreffen Aber die jüngsten Cyberangriffe haben das Gegenteil bewiesen. Egal, um welche operativen Netzwerke und ihre Anwendungsbereiche es sich dreht, sie sind jederzeit böswilligen IT-Angriffen ausgesetzt. Dies ist umso mehr der Fall, da es immer mehr Verknüpfungen mit der IT gibt. Angesichts dieser Herausforderung für die Cyber-Sicherheit für industrielle Anlagen und industrielle IT-Systeme erweist sich die Norm IEC 62443 als unumgänglich. Präsentation.

EINE GEMEINSAME GRUNDLAGE FÜR DIE CYBER-SICHERHEIT FÜR DIE INDUSTRIE

Seit 2007 wurden unter der Führung des Ausschusses 99 der ISA die ersten spezifischen Vorgaben zur Cyber-Sicherheit für die Industrie entwickelt. Einige Jahre später erblickte die internationale Norm IEC 62443 das Licht der Welt. Sie gibt einen Rahmen für die tiefgreifende Cyber-Abwehr für industrielle Systeme vor, egal ob es sich um kleine Schokoladenfabriken an der Straßenecke, um Kläranlagen oder ein Transportnetzwerk handelt. „*Ein Cyberangriff, auch auf ein kleines Unternehmen, das Getränke abfüllt, kann zu einem Stillstand der Produktion und infolgedessen zu finanziellen Einbußen führen, die dem Unternehmen den Todesstoß versetzen können*", erklärt **Khobeib Ben Boubaker,** Leiter des Bereichs Industrial Security Business Line bei Stormshield.



Bis jetzt gab es einerseits die Sicherheit der IT-Systeme (ISO 27000) und andererseits die industrielle Sicherheit (Betriebssicherheit und Funktionssicherheit mit IEC 61508 und den Branchennormen). Die Norm IEC 62443 ist nun eine Verbindung dieser zwei Umgebungen, die immer mehr zusammenlaufen. Sie ist ein **entscheidendes Glied für das allgemeine Risikomanagement der Cyber-Sicherheit für die Industrie.** Aber diese Überschneidung von OT und IT erweist sich noch als komplex. *„Das IT-Universum ist sehr auf Vertraulichkeit und Integrität bedacht. Bei mutmaßlichen Angriffen hat man sofort die Tendenz, das System abzuschalten. Im Gegensatz dazu muss eine Fabrik ohne Unterbrechungen produzieren und mit Risiken für Mensch und Umwelt umgehen können*“, sagt **Fabien Miquet**, Product and Solution Security Officer bei Siemens.

„Das IT-Universum ist sehr auf Vertraulichkeit und Integrität bedacht. Bei mutmaßlichen Angriffen hat man sofort die Tendenz, das System abzuschalten. Im Gegensatz dazu muss eine Fabrik ohne Unterbrechungen produzieren und mit Risiken für Mensch und Umwelt umgehen können."

Fabien Miquet, Product and Solution Security Officer at Siemens

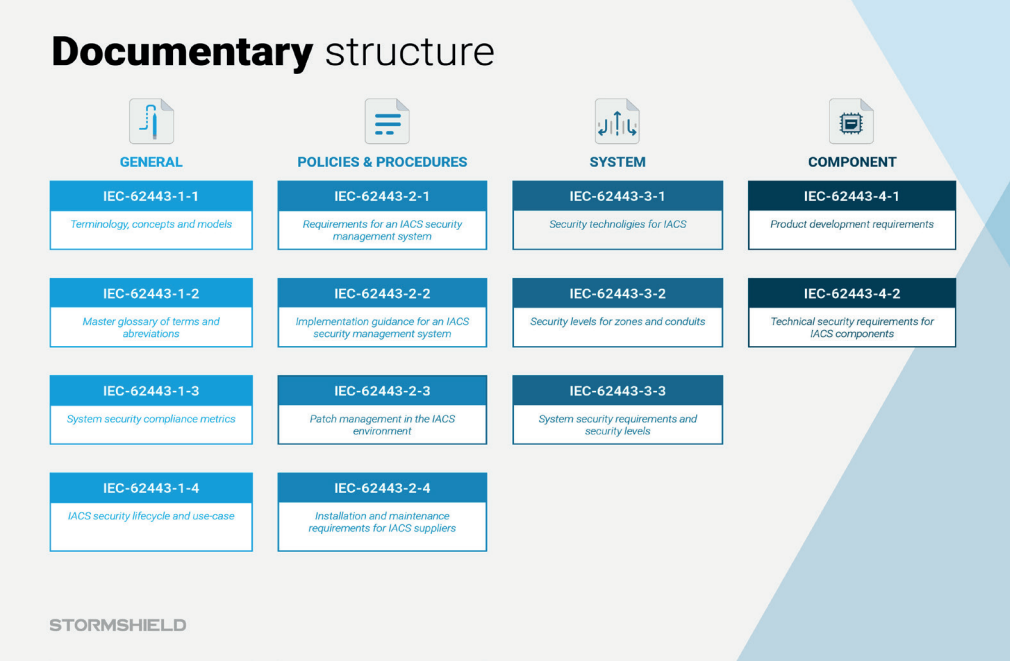
Aber die Norm IEC 62443 besteht aus einer Reihe an Empfehlungen, die der Industrie und ihren kritischen Infrastrukturen nichts aufzwingt. Dank dieser Flexibilität lässt sich die Norm an den jeweiligen Kontext und die Besonderheiten der kritischen Anlagen anpassen. *„**Die Norm IEC 62443 ist eine wahre Referenz für die Cyber-Sicherheit für industrielle Anlagen, da sie eine gemeinsame Grundlage bietet.** Sie kann, je nach Bedarf, teilweise angewandt oder durch eine andere Branchennorm ergänzt werden. So bezieht sich IEC 61850 zum Beispiel auf elektrische Schaltanlagen, deren operative Realität in einem Unterwerk, einem Smart Building oder auch einer Krankenhauseinrichtung*

anders aussehen wird", sagt Khobeib Ben Boubaker. Diese Norm scheint notwendig und strukturierend zu sein, insbesondere, da „*die industrielle Welt heute sehr heterogen ist, wenn man sich die Anzahl der Berufe darin ansieht,* erklärt **Anthony Di Prima**, Senior Manager bei Wavestone. *Abhängig davon, ob man im Gebiet der Chemie oder der Energie arbeitet, unterscheiden sich Komponente und Systeme. Die Norm IEC 62443 ist ein Harmonisierungsprojekt bewährter Cyber-Verfahren in einem fragmentierten Markt und entwickelt sich gewöhnlich in einem geschlossenen System. Diese Norm hat eine internationale Reichweite und ermöglicht die Entwicklung hin zu mehr Interoperabilität.*"

IEC 62443, IM HERZEN DER BESTIE

Die Norm IEC 62443 besteht aus mehreren Dokumenten für Fachleute, die in vier Teilen zusammengefasst sind.

- **„Allgemein 62443-1":** Dieser erste Teil umfasst die Dokumente, die allgemeine Konzepte, die Terminologie und die Methoden beschreiben. Er legt auch ein Glossar fest
- **„Politik & Verfahren 62443-2":** Dieser zweite Teil beinhaltet spezifische Angaben zu organisatorischen Methoden und richtet sich an die Betreiber und Verwalter von Automatisierungslösungen. Er enthält auch Empfehlungen im Bereich Korrekturen und Aktualisierungen der Systemkomponente bei gleichzeitiger Einhaltung der Besonderheiten der kritischen Industrieinfrastrukturen (IEC-62443-2-3);
- **„System 62443-3":** Dieser dritte Teil widmet sich den operativen Sicherheitsmaßnahmen der ICS (Industrial Control Systems) – oder vielmehr der IACS (Industrial Automation and Control Systems, nicht zu verwechseln mit SCADA), da die Norm ihre eigene Definition der Infrastrukturen zur Steuerung und Bedienung hat. Er liefert eine aktuelle Bewertung der Tools für die Cyber-Sicherheit und beschreibt die Methode und die Mittel für die Strukturierung der Architektur in Zonen und Leitungen und die Bestandsaufnahme der Techniken zum Schutz vor Cyberangriffen. Er beschreibt die Segmentierung der IACS in Zonen, abhängig von der Wichtigkeit der Anlagen (62443-3-2), und erinnert daran, dass diese Zonen untereinander kommunizieren können – sei es per USB-Stick, Kabelnetzwerk oder VPN-Verbindung. **Dies ist sicherlich der interessanteste Teil, denn er stellt Elemente einer tiefgreifenden Cyber-Abwehr vor;**
- **„Komponente 62443-4":** Dieser vierte Teil konzentriert sich schlussendlich auf diejenigen, die Lösungen für die Steuerung und Bedienung zur Verfügung stellen: Automaten, Überwachungselemente, Engineering-Systeme und andere Umschaltsysteme. Dieser Teil beschreibt einerseits die Sicherheitsanforderungen für diese Anlagen und stellt die bewährten Verfahren für die Produktentwicklung vor.



„IEC 62443 ist die umfangreichste Norm des Markts. **Sie berücksichtigt die reine IT-Sicherheit und die Betriebssicherheit.** *Sie ist pragmatisch. In industriellen Umgebungen kann im Gegensatz zu Büros die Cyber-Sicherheit nicht umsetzen, wenn man die Betriebssicherheit nicht berücksichtigt. Aus diesem Grund ergibt die Norm IEC 62443 tatsächlich Sinn, wenn man sie bezüglich der Sicherheit der industriellen IT-Systeme betrachtet*", sagt Khobeib Ben Boubaker. Es ist für jede Industrie wichtig, die Zonen und Leitungen ihrer Infrastruktur und das Risikolevel für jede Zone festzulegen und die entsprechenden, in der IEC 62443-3-3 definierten Sicherheitsmaßnahmen anzuwenden.

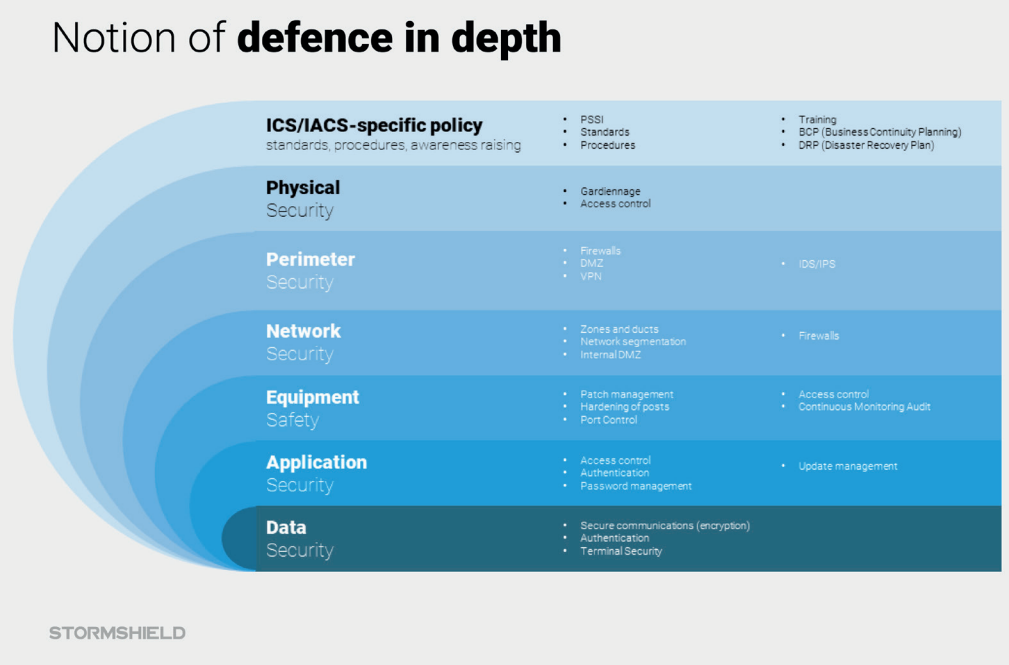
Die sieben Grundanforderungen der Norm IEC 62443 werden auf diese Zonenverteilung angewandt:

- alle Benutzer (Personen, Software-Prozesse und Geräte) vor der Zugangsgenehmigung zu einem System identifizieren und authentifizieren;
- die Nutzung kontrollieren (die Berechtigungen einhalten, die ein authentifizierter Benutzer erhält);
- die Integrität der Daten, Softwares und Ausrüstung sicherstellen;
- die Vertraulichkeit der Informationen in der Kommunikation sowie bei der Datenspeicherung garantieren;
- unnütze Datenströme limitieren;
- auf Angriffe reagieren und die zuständige Behörde fristgerecht informieren;
- und die Widerstandsfähigkeit des Systems im Falle eines DDoS-Angriffs garantieren.

„Die Firewall ist eine der besten Sicherheitsmaßnahmen, mit der man den meisten Sicherheitsanforderungen entspricht. Sie muss jedoch optimiert und physisch gestärkt werden. In einer Raffinerie oder in einem Trinkwassernetz kann man keine traditionelle Firewall nutzen, da die physischen Einschränkungen nicht dieselben sind wie in einem klassischen Computerraum. Sie muss Temperaturschwankungen, Staub und elektromagnetische Wellen aushalten können", erklärt **Simon Dansette**, Product Manager bei Stormshield.

EIN PLÄDOYER FÜR EINE TIEFGREIFENDE CYBER-ABWEHR

Die Norm sendet eine starke und symbolträchtige Botschaft. Das Prinzip der tiefgreifenden Abwehr schützt alle Untereinheiten des Systems und stellt sich einer Vision der Sicherung außerhalb des Systems entgegen. ***„Die Sicherheit eines Systems darf nicht auf einer einzelnen Barriere beruhen“***, sagt Fabien Miquet. *„Aus diesem Grund sieht die Norm IEC 62443 tiefgreifenden Schutz vor. Die Einhaltung dieser Norm ist ein Beweis der Reife im Bereich der Cyber-Sicherheit.“*



Als engagierter Akteur für den Schutz anfälliger Systeme war Siemens einer der ersten großen Konzerne, der auf die Norm IEC 62443 Bezug nahm, um seine Prozesse für die Entwicklung von Automatisierungs- und Schulungsprodukten, einschließlich der industriellen Softwares, zertifizieren zu lassen. *„Die Norm IEC 62443 ist eine der einzigen Normen, mit der man einerseits ein industrielles Produkt schützen und andererseits ein ganzes Produktpaket, ein System, eine Lösung und sogar den Entwicklungsprozess dieses Produkts schützen kann. Außerdem ist sie branchenübergreifend und auf internationaler Ebene in der Industrie bekannt. Das ist ideal für Siemens, denn die Aktivitäten des Konzerns betreffen auch die Energie-, Gesundheits-, Lebensmittel- (Lebensmittel, Getränke usw.) und die Baubranche. Aus diesem Grund hat sie sich auch durchgesetzt,“* sagt Fabien Miquet. *„Ungefähr dreißig Fabriken von Siemens verfügen über ein IEC-62443-Zertifikat. Wir und unsere Kunden glauben an diese Norm: Sie ist ideal, wenn man dieselbe Sprache sprechen will.“*

Man darf allerdings nicht vergessen, **dass die Industriebranche komplex ist**. Der Großteil der Fabriken hat nicht den gewünschten Reifegrad in Sachen Cyber-Sicherheit erzielt. Das liegt vor allem an den Systemen, die über lange Zeit hinweg verwendet werden (20 bis 30 Jahre und sogar noch länger) und die veralten. Die Herausforderung liegt

nicht darin, Systeme für die Cyber-Sicherheit für die Prozesse der Fabriken von morgen bereitzustellen, sondern vielmehr für die Fabriken von heute und von gestern. Maschinen und Automaten auszutauschen würde Millionen von Euro kosten, die die Unternehmen heute nicht unbedingt zur Verfügung haben. Heute ist es wichtig, eine erste Ebene der Cyber-Sicherheit einzurichten, bis diese am Ende in der Entwicklungsstrategie der Fabrik als Notwendigkeit angesehen wird.

IEC 62443, EINE NORM, DIE SICH STÄNDIG WEITERENTWICKELT

Die Erarbeitung der Norm IEC 62443 begann vor einigen Jahren und ist immer noch nicht abgeschlossen. Diese Norm ist das Ergebnis der Arbeitsgruppen der ISA (International Society of Automation), genauer gesagt, der ISA GCA (Global Cybersecurity Alliance) unter der Schirmherrschaft der IEC (International Electrotechnical Commission). „*Wie andere Normen auch, muss die Norm IEC 62443 regelmäßig überarbeitet werden, selbst während des Erstellungsprozesses. Regelmäßige Aktualisierungen sind insbesondere in der Industrie wichtig. Das ist wichtig in einer Umgebung, und allgemein gesehen, einer Industrie 4.0, in der Objekte immer häufiger mit der Außenwelt kommunizieren und in der anfällige Themen wie das industrielle Internet der Dinge, die Cloud oder auch Remote-Möglichkeiten ständig neu bewertet müssen*“, sagt Anthony Di Prima. „*Je mehr neue Funktionen und Funktionsmodi es geben wird, desto mehr wird die Norm weiterentwickelt werden und damit wird ihre Anwendungsrate steigen. Viele nationale und internationale Ausschreibungen beziehen sich bereits auf die Norm IEC 62443. In den letzten fünf Jahren haben wir eine wahre Entwicklung in diese Richtung gesehen*“, sagt Khobeib Ben Boubaker.

Die Produktentwicklung nach dem Prinzip secure-by-design bedeutet, dass die Cyber-Sicherheit von Anfang an ein wichtiges Thema ist. „*Das traditionelle Schema des Produktentwurfs, bevor man sich Gedanken über den Sicherheitsaspekt macht, ist heute nicht mehr aktuell. Die Cyber-Sicherheit ist nicht länger nur eine Option: Sie ist zu einer vollwertigen operativen Leistung geworden*“, sagt Fabien Miquet abschließend.

STORMSHIELD

Weltweit müssen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und erlauben den Schutz der Geschäftstätigkeit. Unsere Mission: Cybersorglosigkeit für unsere Kunden, damit diese sich auf ihre Kerntätigkeiten konzentrieren können, die für das reibungslose Funktionieren von Institutionen, Wirtschaft und Dienstleistungen für die Bevölkerung so wichtig sind. Die Entscheidung für Stormshield ist eine Entscheidung für eine vertrauenswürdige Cybersicherheit in Europa. Weitere Informationen finden Sie unter www.stormshield.com.