

SICHERHEIT & DATENSCHUTZ

Industrial Security, Blockchains und DSGVO

Industrieller Mittelstand:

Wo KMU großen Nachholbedarf haben

Prozess-IT:

**Warum klassische IT-Security
nicht ausreicht**

Schutz von IC-Systemen:

**Wie Defense in
Depth funktioniert**

Blockchains:

**Wo auch starke Ketten
reißen können**

DSGVO:

**Was Data Discovery und
Data Leakage Prevention leisten**

Security by Design:

Welche Sicherheitskonzepte zukunftsfähig sind



Ihr virtueller Datenraum

Sicherer Austausch vertraulicher Daten



Sicherer Datenaustausch

Mit netfiles können Daten einfach und sicher standort- und unternehmensübergreifend mit Kunden, Lieferanten und Geschäftspartnern ausgetauscht werden. 256-Bit Verschlüsselung bei der Übertragung und Speicherung, individuelle Zugriffsrechte für Lese-, Download- und Schreibrechte und ein detailliertes Aktivitätsprotokoll gewährleisten höchsten Schutz und Kontrolle bei der Bereitstellung und Verteilung von Dokumenten und eine effektive Zusammenarbeit.

Made in Germany

Höchste Sicherheit für Ihre Daten – Die netfiles GmbH ist ein deutsches Unternehmen mit Sitz, Entwicklung und Hosting in Deutschland.

 **Kostenlos testen**
www.netfiles.de

netfiles GmbH
+49 8677 915 96-10 · vertrieb@netfiles.de

IT-Sicherheit ist Zukunftsfähigkeit



Liebe Leserinnen und Leser,

das Jahr 2018 neigt sich dem Ende entgegen. Vor allem die Datenschutz-Grundverordnung (DSGVO) hat in diesem Jahr für viel Bewegung gesorgt und die Gemüter erhitzt. Aber auch die Bedrohungen durch Hackerangriffe, Verschlüsselungstrojaner, Datenlecks, Cyberkriminelle und Hacker im Staatsauftrag sind unverändert hoch. Was werden die Themen 2019 sein? Werden neue Impulse aus der Politik kommen, um die (sichere) Digitalisierung voranzubringen?

So viel ist sicher: Mit Computern, diversen mobilen Endgeräten, Smart-TVs oder auch Staubsaugrobotern sind viele Gegenstände des Alltags heute bereits vernetzt. „Industrie 4.0“, Automatisierung, Digitalisierung und Vernetzung von Produktionsanlagen nehmen immer weitreichendere Ausmaße an. Roboter ersetzen Mitarbeiter, Fahrzeuge fahren autonom. Der Mensch wird zunehmend von smarten Maschinen abgelöst. Dies hat neben einer Veränderung unserer Arbeits(markt)strukturen, der Umgestaltung von Produktionsstätten und neuen Anforderungen im Job auch wachsende Herausforderungen im Bereich der Sicher-

heitsmechanismen zur Folge. Den Fortschritt kann man nicht aufhalten, aber gestalten. „Security by Design“ und „Security by default“ sollten daher schon bei der Planung als Leitkonzepte in die Produkte mit einfließen.

Als TeleTrusT – Bundesverband IT-Sicherheit e.V. möchten wir die Industrie bestmöglich unterstützen. Um ein hohes IT-Sicherheitsniveau zu gewährleisten, hat die TeleTrusT-Arbeitsgruppe „Smart Grids/Industrial Security“ ein Prüfschema nach IEC 62443-4-2 „Industrielle Kommunikationsnetze – IT-Sicherheit für industrielle Automatisierungssysteme“ veröffentlicht. Im Bereich Automatisierungstechnik sollen damit Produkte, die von unterschiedlichen Prüfstellen zertifiziert wurden, in Bezug auf IT-Sicherheit vergleichbar werden. Aber auch die beste Produktionsanlage kommt nicht ohne gut geschultes Fachpersonal aus. So bleibt das Thema Awareness als weiteres Standbein der IT-Sicherheit eine Kernaufgabe.

Die IT-Sicherheitsbranche in Deutschland stellt sich mit ihren Experten den gegenwärtigen und kommenden Herausforderungen. „IT Security made in Germany“ ist und bleibt ein herausragendes Qualitätsmerkmal. Vor allem sind hier kleine und mittelständisch geprägte Unternehmen die innovativen Vorreiter.

Die vorliegende Sonderpublikation informiert Sie über Lösungen und Konzepte, die deutsche Unternehmen im Bereich IT-Sicherheit entwickelt haben. Die Beiträge weisen einen starken Bezug zu Fragen der industriellen Sicherheit und zur DSGVO auf. Gemeinsam mit den TeleTrusT-Mitgliedern wünsche ich Ihnen eine informative Lektüre und hoffe, dass Sie zahlreiche Anregungen erhalten, um die IT-Sicherheit in Ihrem Unternehmen, in Ihrer Behörde und auch in Ihrem privaten Umfeld weiter zu stärken.

*Dr. Holger Mühlbauer
Geschäftsführer TeleTrusT –
Bundesverband IT-Sicherheit e.V.*

Inhalt

Industrieller Mittelstand

Lohnende Investitionen 4

Prozess-IT

Keine Chance für
klassische IT-Security 6

Schutz von ICS

Abwehr mit Tiefenschärfe 8

Security by Design

Stets einen Schritt voraus 13

Data Discovery und Data Leakage Prevention

Technische Hilfe zur DSGVO 15

Blockchains

Nicht so sicher wie gedacht 17

Impressum und Inserentenverzeichnis

18

Lohnende Investitionen

IT-Security verlangt mehr als die Installation neuer Sicherheitssoftware

In mittelständischen Unternehmen lässt sich durchgängig ein signifikanter Nachholbedarf in Sachen Cybersecurity nachweisen. Um industrielle Anlagen und Produktionsketten auf das aktuelle Sicherheitsniveau zu bringen, gilt nach wie vor die alte Weisheit: Zuerst, erkenne dich selbst!

Mit der Vernetzung von Produktionsanlagen zu cyber-physischen Systemen, in der Regel als „Industrie 4.0“ bezeichnet, setzen sich mittlerweile auch viele mittelständische Unternehmen auseinander. Neben Effizienzgewinnen und einer besseren Reaktionsfähigkeit auf Marktveränderungen ist die flexible Anpassung von Produktionsprozessen an Marktgegebenheiten der Haupttreiber für diese Entwicklung hin zu komplex vernetzten Prozessen. Die dazu notwendige Digitalisierung vieler Geschäftsprozesse bringt jedoch neben den oft zitierten Vorteilen auch neue Risiken mit sich. Denn unsicher konfigurierte oder falsch eingesetzte IT-Technologie kann zum Abfluss von Betriebs- und Geschäftsgeheimnissen führen, vergrößert die Angriffsfläche für Sabotage und bietet neue Angriffspunkte für die Kompromittierung von Systemen und Daten.

Die im Vergleich zu Großunternehmen deutlich geringeren Budgets für die IT-Sicherheit führen in vielen Fällen dazu, dass beispielsweise die eingesetzte IT-Security-Technologie unter schwacher Installation, mangelnder Wartung und nachlässiger Anwendung, z. B. der fehlenden Sichtung und Auswertung von Logs und Reports, leidet. Darüber hinaus führt der sich insbesondere im Mittelstand verschärfende Mangel an Fachkräften im Bereich IT-Sicherheit zu Mängeln in den Security-Standardprozeduren, beispielsweise im Patchmanagement, in den Passwort-Policies oder dem Berechtigungsmanagement.

Akute Bedrohungen

Beispiele für teils spektakuläre Sicherheitsprobleme gab es in den vergangenen Jahren genug. So wurden etwa IT-Systeme von Wasserwerken, Energieanlagenbetreibern und Krankenhäusern – nebenbei: allesamt kritische Infrastrukturen – erfolgreich angegriffen. In einigen Fällen wäre wahrscheinlich auch eine Fernsteuerung möglich gewesen, wenn die oftmals ahnungslosen Betreiber vorab informiert worden wären. In anderen Fällen kam die Hilfe zu spät und der Betrieb der zum Teil lebenswichtigen Institutionen wurde empfindlich gestört.

Die IT-Sicherheit in mittelständischen Unternehmen zu verbessern ist daher ein eminent wichtiger Prozess. Dazu sind Aufmerksamkeit und Investitionen in ganz verschiedenen Bereichen notwendig. Die öffentliche Diskussion um spektakuläre Hacks und Zero-Day-Sicherheitslücken versperrt dabei häufig den Blick auf alltägliche Bedrohungen: Ransomware, Innentäter oder der sogenannte CEO-Fraud mit trickreich fingierten Rechnungen bedrohen Unternehmen deutlich häufiger als hochkomplexe Angriffe von dubiosen Geheimdiensten. Doch eine reine Installation von Sicherheitslösungen wie Endpoint-Protection oder Firewalls ist aufgrund der komplexen Bedrohungslage und gesetzlicher Regulierungen nicht ausreichend. Und so steht vor der Beschaffung neuer Hard- oder Software zunächst einmal eine ge-

naue Auseinandersetzung mit den Bereichen Organisation, Compliance und Personal.

Richtlinien aufstellen

Zunächst einmal gilt es, gesetzliche Vorgaben sowie von Kunden erwartete oder branchenübliche Standards zu kennen und in entsprechende Policies umzusetzen. Die Erstellung und konsequente Anwendung dieser IT-Sicherheitsrichtlinien für alle vernetzten Geräte im Unternehmen erfordert ein hohes Maß an Bereitschaft und Durchsetzungswillen. Eine interne Schutzbedarfsanalyse als Teil eines übergeordneten Risikomanagements ermöglicht die effiziente Nutzung der verfügbaren Ressourcen. Unter dem Stress eines akuten IT-Sicherheitsvorfalls kann ein präventiv erstelltes und laufend aktualisiertes Notfallhandbuch entscheidende Hilfe leisten.

Risikoabschätzung bzw. -minimierung beginnt oft bereits beim Einkauf der Technik, speziell bei automatisierten und vernetzten Produktionsanlagen. Fragen nach Zugangs- und Zugriffsschutz, kryptografischer Tauglichkeit, sicherem Auslieferungszustand, integrierten Fernwartungsschnittstellen oder dem Nachweis sicherer Softwareentwicklung sollten zentraler Bestandteil der Einkaufspolicy sein.

Letztlich werden sich jedoch ohne ein für die Notwendigkeit von Sicherheitseinrichtungen und -prozessen sensibilisiertes, zur Beachtung motiviertes und in der Anwendung geschultes Personal signifikante Verbesserungen des Sicherheitsniveaus nicht erzielen lassen. Neben Richtlinien für die Installation von Software auf Arbeitsplatzrechnern und einem Mobile-Device-Management sind auch klare Leitlinien für den Gebrauch privater Geräte notwendig. So sollte der vor wenigen Jahren noch beliebte BYOD-Ansatz als organisatorische Fehlentwicklung abgelehnt werden.

IT-Infrastruktur analysieren

Ein zweites Handlungsfeld erstreckt sich auf die IT-Infrastruktur selbst. Gerade im Mittelstand wachsen die IT-Systeme über die Zeit zu immer komplexeren Konstrukten. Die realisierten Anforderungen orientieren sich dann meist an einem spontanen Bedarf – und nicht an den Erfordernissen der IT-Sicherheit. Daher ist dieses Wachstum oftmals wenig koordiniert. Immer wieder tauchen bei der Analyse von Unternehmensnetzwerken zahlreiche Systeme und Geräte auf, über deren Verwendung die IT-Abteilung zuvor nicht Bescheid wusste (Stichwort: Schatten-IT). Bevor also eine neue Sicherheitsarchitektur entworfen werden kann, ist auch hier eine detaillierte Analyse notwendig.

Denn die Architektur des Unternehmensnetzwerkes ist immer auch ein wichtiger Faktor in Sachen IT-Sicherheit. Die konsequente Segmentierung des Netzwerkes sowie die Trennung von Verwaltungs-,

Produktions-, Mitarbeiter- und Besuchernetz sollte als Grundpfeiler einer IT-Sicherheitsarchitektur eingehalten werden. Der Aufbau einer eigenen Public-Key-Infrastruktur (PKI), ein flächendeckendes Monitoring des Netzwerkverkehrs und der konsequente Einsatz kryptografischer Verfahren heben das Sicherheitsniveau weiter an und sorgen für ein effizientes Identitätsmanagement. Und auf alle Fälle sollte gerade in vernetzten Produktionsumgebungen die Kommunikation zwischen Maschinen durch interne Zertifikate gesichert sein.

Der Einsatz von Benutzerkonten in Betriebssystemen und Anwendungen bildet die Basis für die Auditierbarkeit von Netzwerkzugriffen und ein sinnvolles Berechtigungsmanagement. Die Verwaltung der in aller Regel sehr schnell wachsenden Anzahl künstlicher Identitäten in einem Industrie-4.0-Netzwerk kann schließlich durch entsprechende Verzeichnisdienste unterstützt und vereinfacht werden. In sicherheitskritischen Bereichen bietet sich zudem die Verwendung von Zwei-Faktor-Authentifizierung mittels Hardwaretokens an.

Software absichern

Drittes wesentliches Handlungsfeld ist die im Unternehmen eingesetzte Software. Die Nutzung einer Endpoint-Protection-Lösung sollte unbedingt auch im Mittelstand ein zentraler Baustein für die Sicherheitsstrategie sein – ergänzt um einen dedizierten Perimeter-Schutz. In vielen Fällen sind aber zusätzliche Maßnahmen im Bereich Software sinnvoll. So können Whitelisting-Ansätze genutzt werden um sicherzustellen, dass ausschließlich die Ausführung notwendiger Software genehmigt wird. Damit kann die Installation und Nutzung unerwünschter Anwendungen effektiv verhindert werden. Im Zuge einer Systemhärtung können aus komplexen Softwarelösungen ungenutzte Funktionen und Dienste entfernt werden, um letztlich weniger Angriffsfläche für Hackerattacken und Schadsoftware zu bieten.

Genauso wichtig ist ein konsequentes Patchmanagement. Jede im Unternehmen eingesetzte Software muss durch eine entsprechende Lösung auf dem neuesten Stand gehalten werden. Insbesondere im Bereich vernetzter Fertigungsanlagen mit zum Teil komplexen und individuellen Maschinen sollte bereits im Vorfeld der Anschaffung

geprüft werden, ob und wie oft der Hersteller seine Software patcht und ob dort die notwendigen Ressourcen für eine langfristige Pflege des Codes vorhanden sind. Fragen nach Security Code Audits, Software Escrow oder Open-Source-Entwicklung sollten Bestandteil des oben bereits erwähnten Einkaufsprozesses sein.

Mitarbeiter schulen

Mittelständische Unternehmen sind derzeit häufig noch damit überfordert, das richtige Maß an benötigter IT-Sicherheit zu finden (Stichwort: Schutzbedarfsanalyse). Einerseits hat die Mehrzahl nur wenige konkrete gesetzliche Vorgaben, gleichzeitig steigt der Druck durch Regelungen wie die EU-Datenschutz-Grundverordnung (DSGVO) oder geforderte Branchenstandards. Investitionen in Sicherheitslösungen werden in vielen Fällen durch Mängel in deren Anwendung konterkariert. Denn eine SIEM-Lösung (Security Information and Event Management) beispielsweise liefert zwar viele Informationen, stellt aber selbst noch keine Sicherheit her. Dazu bedarf es gut ausgebildeter Mitarbeiter, die diese Daten auch regelmäßig auswerten. Logfiles zu speichern hilft im Zweifel wenig, wenn diese nicht analysiert werden können.

Fazit

Vor dem Hintergrund der hier nur kurz umrissenen Anforderungen zur Gewährleistung der Sicherheit von IT-Infrastrukturen vertrauen zahlreiche mittelständische Unternehmen auf externe Dienstleister. Aus heutiger Sicht muss sich dieser Trend unter den benannten Rahmenbedingungen eher noch verstärken. Die Auslagerung sicherheitsrelevanter IT-Dienstleistungen mag auf den ersten Blick befremdlich erscheinen, ist aber in anderen Bereichen (Werksschutz, Organisationsberatung, Hosting) längst alltäglich.

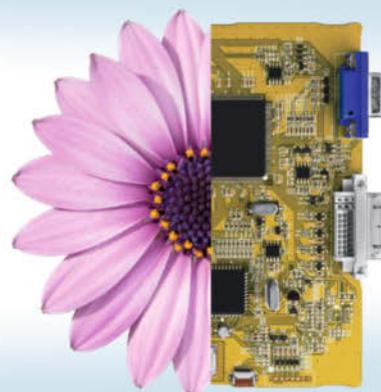
*Hauke Gierow
G DATA Software AG
Michael Zimmer*

G DATA Advanced Analytics GmbH



Was wir wollen:
Deine digitale Seite

www.bsi.bund.de/karriere



Keine Chance für klassische IT-Security

Bei der Absicherung von Prozess-IT sind besondere Schutzmechanismen gefragt

Wenn es um Eingriffe in industrielle Produktionsanlagen geht, lautet die gängige Devise oftmals: Never touch a running system. Dennoch werden die Systeme zunehmend digitalisiert und vernetzt – die IT-Sicherheit bleibt dabei allerdings häufig genug auf der Strecke.

Der Reifegrad der Prozess-IT (PIT) und mithin auch deren Sicherheit liegt weit hinter dem aktueller Enterprise-IT. Der Grund hierfür liegt in den zeitlich versetzten Entwicklungszyklen der Geräte und Technologien, die sich aus den längeren Lebenszyklen der PIT ergeben. Wo in der klassischen IT alle drei bis fünf Jahre neue Komponenten eingesetzt werden, sind in der PIT Lebenszyklen von 10 bis 15 Jahren oder mehr typisch. Betriebszulassungen, Gewährleistungs- und Haftungsfragen sowie spezielle Anforderungen, z. B. die sehr hohe Verfügbarkeit und latenzfreie Datenübertragung, führen dazu, dass nur selten Anpassungen an der PIT vorgenommen werden (dürfen).

Historisch gewachsene Netze

Dass dies keine untypische Entwicklung ist, zeigt die Geschichte des Automobils als nur eines von vielen Beispielen. Im 19. Jahrhundert dachte niemand an Sicherheitsmaßnahmen wie Gurte, Airbags oder Abstandhaltesysteme. Was zählte, war die Funktionalität und Zuverlässigkeit des Automobils. Nach und nach wurde das Auto dann massentauglich, das Verkehrsaufkommen stieg stark an, und die technologische Weiterentwicklung führte zu höheren Geschwindigkeiten. Das Risiko von Unfällen und deren Folgen stieg. Schließlich wurde der Sicherheitsgurt erfunden und durch die Regulierungsmaßnahme der Gurtpflicht flächendeckend verbreitet.

Vergleicht man dies mit der Entwicklung der Prozess-IT, zeichnen sich klar Parallelen ab. In den 1990er-Jahren begann der Umstieg von elektronischen zu digitalen Technologien in der Anlagensteuerung. Es schloss sich die Vernetzung der Systeme an: Über gängige Kommunikationsmedien (LAN, MAN, WAN) etablierte man Automatismen sowie eine zentrale Steuerung und Überwachung.

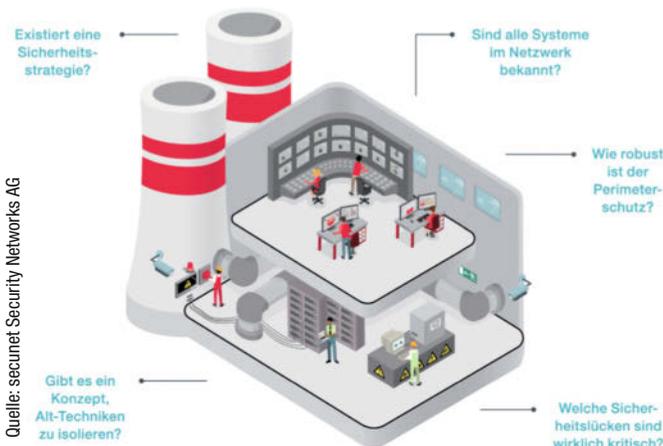
Doch die Vernetzung ungeschützter veralteter Technologien bedeutet ein hohes Sicherheitsrisiko. Das Nachrüsten von Sicherheitssoftware oder das Aufspielen von Software-Patches ist keine Lösung. Denn weder existieren Testumgebungen, noch sind Änderungen an produktiven Systemen gestattet. Nicht nur die Systeme in der PIT selbst sind anfällig, es werden auch Kommunikationsprotokolle eingesetzt, die nicht über die in der modernen Informations- und Kommunikationstechnologie (IKT) üblichen Sicherheitsfunktionen verfügen. Zudem sind klassische Sicherheitsansätze aus der IKT nicht einfach auf die PIT übertragbar. Die Installation von Firewalls etwa birgt die Problematik, die besonders hohen Anforderungen einer latenzfreien Datenübertragung in der Prozessdatenkommunikation nicht zu gefährden.

Sicherheit im Nachhinein

Das ideale Szenario „Sicherheit out of the Box“, bei dem komplett neue Systeme implementiert werden können, in deren Design starke Sicherheitsmaßnahmen enthalten sind, ist in der Anlagensteuerung aufgrund der beschriebenen Besonderheiten der PIT meist weit von der Realität entfernt. Stattdessen stehen die Anlagenbetreiber vor der Herausforderung, ein Geflecht aus Altsystemen, die ursprünglich gar nicht für eine Vernetzung über das Internet konzipiert waren, gegen moderne Cybergefahren zu schützen. Was also ist zu tun?

Wird ein ganzheitlicher Ansatz verfolgt, lässt sich auch in bestehenden Industriernetzwerken ein hohes Sicherheitsniveau erreichen. Zunächst ist Transparenz im PIT-Netz herzustellen, indem einige grundsätzliche Fragen geklärt werden: Welche Kommunikation und welche Systeme existieren überhaupt im Netzwerk? Mag diese Frage auch trivial wirken, in der Praxis kommt es selten vor, dass sie vollständig und nach aktuellem Stand beantwortet werden kann. Wie ist der Sicherheitszustand der einzelnen Systeme? Die gesammelten Informationen und das Lagebild helfen eine ausgewogene und gesamtheitliche IT-Sicherheitsstrategie aufzustellen.

In diesem Rahmen gilt es, einige weitere Fragen zu beantworten: Wo sind präventive Maßnahmen angebracht, weil moderne Techniken, Anlagen und Systeme vorhanden sind, die dies unterstützen? Und an



Bei der Absicherung ihrer Prozess-IT sollten sich Anlagenbetreiber eine Reihe von Fragen stellen.

welchen Stellen müssen Netzbereiche strikt abgeschottet und Maßnahmen zur Erkennung von Anomalien implementiert werden? Manche Maßnahmen lassen sich auch bei alten Technologien leicht nachrüsten – wie der Sicherheitsgurt in einem Automobil. Dazu zählen die Absicherung der Fernwartungszugänge, der Perimeterschutz zum Leitnetz und die Abschottung von Altsystemen. Der Einsatz von passiver Scantechnik zur Erkennung von untypischem und unzulässigem Kommunikationsverhalten oder gar Angriffen unterstützt die nach wie vor wichtigen Barrieren zum PIT-Netz.

Automatisierte IT-Sicherheitsanalyse

Ohnehin wird der gezielte Einsatz von Sicherheitslösungen, die der automatisierten Erhebung und Analyse von Sicherheitszuständen in der PIT dienen, in seiner Bedeutung stark steigen. In Anbetracht der knappen Ressourcen der Betreiber und der starken Heterogenität der Techniken ist hier kaum eine Alternative denkbar. Ein permanentes Sicherheitslagebild und eine damit verbundene kontinuierliche Risikobewertung werden die Auswahl und Priorisierung der geeigneten Sicherheitsmaßnahmen und die Kontrolle der Sicherheitsstrategien erst ermöglichen.

Wie schnell die IT-Sicherheitsstrategie wackelt, wenn die Transparenz im Netzwerk nicht gegeben ist, zeigt das folgende Beispiel eines Betreibers einer kritischen Infrastruktur. Auf der Grundlage einer zehn Jahre alten Netzwerkdokumentation entwickelte dieser eine IT-Sicherheitsstrategie für das Leitnetz, die auf eine starke Perimetersicherheit setzte. Im Rahmen der neuen Strategie wurden eine Infrastruktur zur Absicherung von Fernwartungszugängen sowie zum sicheren Datenaustausch mit der Enterprise-IT etabliert und alle bekannten IT-Systeme daran angeschlossen. Nur einen Monat nach Umsetzung der Sicherheitsmaßnahmen gelang es einem Angreifer, über das Netz der Enterprise-IT die Automatisierungstechnik zu kompromittieren. Der Angreifer konnte eine Engineering-Workstation, die zahlreiche Schwachstellen aufwies, übernehmen und sich im Leitnetz festsetzen. Diese Workstation und ihre Schnittstelle zur Enterprise-IT war einige Jahre zuvor zu Testzwecken eingerichtet und nie zurückgebaut worden. Sie

tauchte in keiner Dokumentation auf und wurde somit nicht an die neue Infrastruktur zum sicheren Datenaustausch angeschlossen. Dies zeigt, wie wichtig es ist, Daten über sämtliche IT-Assets und ihre Schwachstellen zu erheben und aktuell zu halten.

Security Awareness

Ein Thema, das in der klassischen IT schon seit Langem behandelt wird, in der PIT aber gerade erst in den Fokus gerät, ist Security Awareness, die Sensibilisierung der Mitarbeiter für die IT-Sicherheit. Die Digitalisierung mit weitgehender Vernetzung bringt Risiken mit sich, die den handelnden Mitarbeitergruppen bislang oftmals unbekannt waren. Hier gilt es Aufklärung zu betreiben und Verständnis zu schaffen.

Zudem zeigen Vorfälle in jüngster Vergangenheit, dass neben Cyberangriffen auch Herausforderungen wie IT-Komplexität, fehlendes IT-Personal, die Nutzung von externen Diensten oder die Steuerung externer Dienstleister die Betriebssicherheit ins Wanken bringen können. Mittels geeigneter Maßnahmen, Kampagnen, Alltagsroutinen und Trainings sollten Betreiber für die nötige Security Awareness sorgen. Ein Ansatzpunkt kann sein, Security mit Safety – also der physischen Betriebssicherheit – zu kombinieren. Denn mit diesem Themenfeld setzt man sich traditionell schon Jahrzehnte auseinander und hat zahlreiche Prozesse und Trainings etabliert.

Fazit

In den letzten Jahren ist das Bewusstsein dafür angewachsen, dass digital vernetzte Steuerungssysteme für Industrieanlagen ebenso geschützt werden müssen wie das in der Enterprise-IT meist schon der Fall ist. Dabei kommen viele klassische IT-Sicherheitsmaßnahmen nicht in Betracht oder müssen modifiziert werden. Doch mittlerweile liegen spezialisierte Ansätze für den Schutz der PIT vor, die bei der Etablierung einer passenden Sicherheitsstrategie helfen und auch die Themen IT-Sicherheitsanalyse und Security Awareness berücksichtigen.

*Torsten Redlich
secunet Security Networks AG*

Wir bilden aus und zertifizieren Sie als

IT-Sicherheitsbeauftragter (ITSiBe) / Chief Information Security Officer (CISO)
gemäß ISO 27001 und BSI IT-Grundschutz
14. - 17. Januar 2019 | 18. - 21. Februar 2019

BSI IT-Grundschutz-Experte
gemäß BSI IT-Grundschutz-Kompendium und BSI-Grundschutz-Standards
28. - 31. Januar 2019 | 04. - 07. März 2019

Qualifizierter IT Risk Manager
gemäß ISO 31000 und ONR 49003
04. - 06. Februar 2019 | 15. - 17. April 2019

Business Continuity Manager
gemäß ISO 22301 und BSI IT-Grundschutz
11. - 13. März 2019 | 27. - 29. Mai 2019

Datenschutz-Auditor
11. - 13. Februar 2019 | 20. - 22. Mai 2019

Datenschutzbeauftragter
gemäß DSGVO und BDSG
21. - 23. Januar 2019 | 25. - 27. Februar 2019

Datenschutzbeauftragter im Gesundheitswesen
10. - 11. Dezember 2018 | 18. - 19. März 2019

Seminare | Ausbildungen mit Personenzertifikat
Inhouse | Workshops | Sensibilisierung / Awareness

AKADEMIE der
DGI® Deutsche Gesellschaft für
Informationssicherheit AG

- ★ Hohe Anerkennung des Zertifikats
- ★ Über 2.500 Zertifikate seit 2010
- ★ Re-Zertifizierung
- ★ Personalisiertes Siegel
- ★ Aufnahme in unser Zertifikatsregister

Sie wünschen sich Unterstützung bei der Umsetzung Ihres Datenschutzmanagementsystems?

Erwerben Sie unsere DSGVO-konformen Muster für Ihre Organisation

Weitere Informationen finden Sie unter www.dgi-ag.de/datenschutz-muster



Abwehr mit Tiefenschärfe

Industrielle Cybersecurity basiert auf einem mehrschichtigen Sicherheitsansatz

Die zunehmende Vernetzung von ICS (Industrial Control Systems) sowie deren Anbindung an das Internet schaffen neue Sicherheitsprobleme. Das Risiko für Störungen, Schäden und Cyberangriffe steigt erheblich. Erfolgversprechende Abwehrstrategien sollten deshalb auf mehreren Ebenen ansetzen.

Elektrizität, Öl und Gas, Wasser, Transport, industrielle und chemische Produktion sind Schlüsselindustrien. Erstere zählen sogar zu den kritischen Infrastrukturen, deren Ausfall dramatische Folgen für das Gemeinwesen nach sich ziehen kann. Zu den größten Herausforderungen im Bereich der IT-Sicherheit zählen dabei die Systeme selbst: Oft sind individuelle bzw. nichtstandardisierte Anlagen im Einsatz, hochkomplex und auf einen langen Lebenszyklus ausgerichtet. Viele dieser Systeme laufen aufgrund ihres langen Lebenszyklus heute auf veralteten Betriebssystemen für die keine Sicherheitsupdates mehr zur Verfügung stehen. Dies erschwert die Ausweitung klassischer IT-Sicherheitsmaßnahmen aus dem Office-Umfeld auf ICS.

Nachhaltige Sicherheitsmaßnahmen erfordern außerdem, dass Lösungen ständig aktualisiert werden. Doch insbesondere in den oben genannten Schlüsselindustrien kann der Betrieb von Maschinen oder Systemen nicht ohne Weiteres für Wartungsarbeiten angehalten werden, da dies Versorgungsengpässe oder Produktionsstopps verursachen kann. Eine weitere Herausforderung ist der Engpass an IT-Security-Fachkräften. Dieser wird vor allem im Kontext herkömmlicher Sicherheitslösungen spürbar, da diese Lösungen meist personalintensiv sind und viel administrativen Aufwand benötigen, z. B. für das kontinuierliche Pflegen von Black- und Whitelists.

Mehrschichtiges Sicherheitskonzept

Um ICS und ihre physischen und digitalen Assets vor den Gefahren der vernetzten Welt effektiv zu schützen, sind ein mehrschichtiger Sicherheitsansatz und eine Strategie der „Defense in Depth“ unabdingbar.

Zentrale Aspekte sind das Identifizieren, Minimieren und Sichern aller Netzwerkverbindungen zum ICS sowie die kontinuierliche Überwachung und Bewertung der Sicherheit von ICS, Netzwerken und Verbindungen. Indem unnötige Dienste, Ports, Geräte, Anwendungen und Protokolle deaktiviert werden, wird die Anfälligkeit des ICS und der unterstützenden Systeme verringert. Zudem sind klare Richtlinien und Sicherheitsschulungen für alle Bediener und Administratoren erforderlich, denn ein mehrschichtiges Sicherheitskonzept berücksichtigt auch den menschlichen Risikofaktor (Abbildung 1).

Cyberattacken auf ICS

Risiken für ICS können sowohl vorsätzliche als auch zufällige Handlungen umfassen, ausgeführt durch externe Angreifer, Insider, Mitarbeiter oder Auftragnehmer. Letztere zählen zu den internen Bedrohungen, ganz gleich ob hier vorsätzliche Aktionen oder unbeabsichtigte Fehler zu veranschlagen sind. Eine der häufigsten Ursachen für infizierte Systeme in industriellen Umgebungen ist denn auch die unwissentliche oder fahrlässige Nutzung von unautorisierten USB-Geräten.

Für einen effektiven Schutz ist es zunächst wichtig, die Methoden von böswilligen Akteuren zu verstehen, mit denen sie ein ICS angreifen. Bei Cyberangriffen gegen Industrieunternehmen dominieren laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) folgende Methoden: Lösegeldangriffe, infizierte Wechselmedien (z. B. Bad USB), Phishing, Social Engineering und Sabotage.

Cyberattacken bestehen in der Regel aus drei Phasen: ausspähen, angreifen und eindringen (Intrusion). Während der ersten Phase unter-

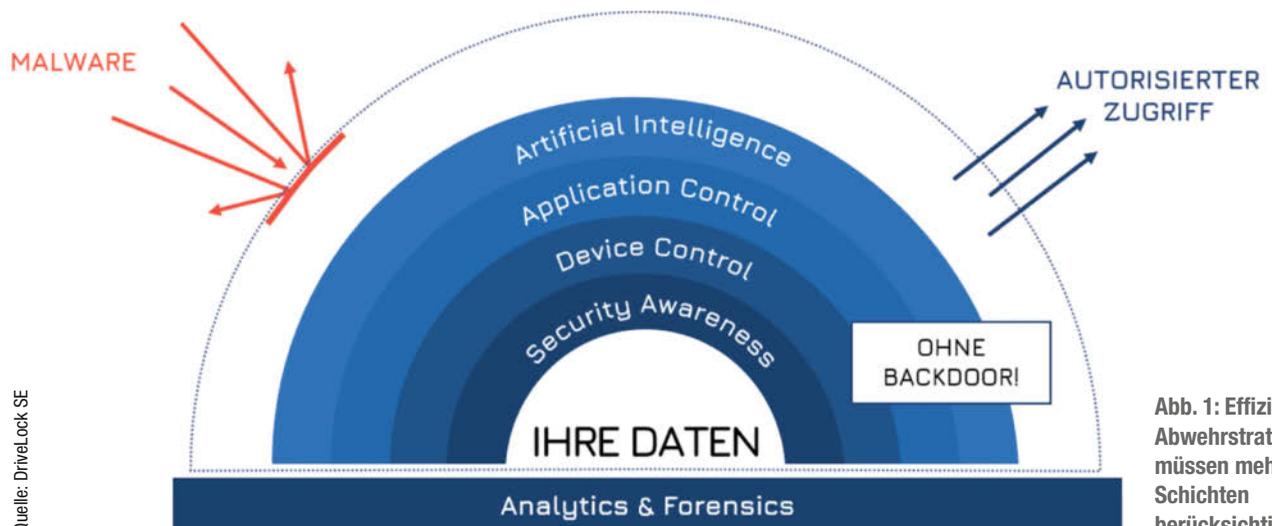


Abb. 1: Effiziente Abwehrstrategien müssen mehrere Schichten berücksichtigen.

Quelle: DriveLock SE

suchen Cyberkriminelle potenzielle Schwachstellen in Hard- und Software. Sie nutzen für ihren Angriff so viele gefährdete Komponenten, Prozesse und Personen wie möglich aus, um auf die Systeme zugreifen zu können. Der eigentliche Angriff kann sich dann auf ein bestimmtes Ziel richten, oder aber der Schadcode wird auf jedem erreichten Gerät abgespeichert, um den unerlaubten Zugriff beizubehalten. Hacker verwenden bestimmte Werkzeuge, um die untersuchten Schwachstellen auszunutzen. Die gängigsten Angriffsmethoden laufen über mit dem Internet verbundene ICS-Geräte, Bad USB, Anmeldungen mit gestohlenen Identitäten u. Ä. m. In der Intrusionsphase hat der Angreifer dann bereits Kontrolle über Geräte und kann auch das System regelmäßig Malware-Updates anfordern lassen. An diesem Punkt sind die Angreifer noch unentdeckt mit weitreichendem Zugriff auf das industrielle Netzwerk sowie dessen Endpunkte und Kontrollsysteme.

Defense in Depth

Nur wer sein System gut kennt, kann es auch entsprechend schützen. Aus diesem Grund sollte ein Cybersecurity-Assessment am Anfang jeder Sicherheitsstrategie stehen. Damit werden Schwachstellen, Risiken und die Wahrscheinlichkeit für Exploits bewertet. Hierfür können Unternehmen zum Beispiel Self-Assessment-Tools wie das „Open Vulnerability Assessment System (OpenVAS)“ des BSI oder das „Cyber Security Evaluation Tool (CSET)“ des US-amerikanischen Departments of Homeland Security verwenden. Auf diese Weise wissen sie genau,

welche Assets geschäftskritisch sind und können diese anhand ihrer Bedeutung und Funktion für den Betrieb bewerten. Systeme, die physische Systeme kontrollieren und verwalten (z. B. Supervisory Control and Data Acquisition/SCADA) zählen zu diesen sensiblen Assets.

Für den Schutz dieser Schwachstellen ist ein mehrschichtiges Sicherheitskonzept notwendig, das auch als Defense in Depth (DiD) bezeichnet wird. Bei diesem Ansatz werden Angreifern möglichst viele Steine in den Weg gelegt, während sich gleichzeitig der Angriff überwachen und entsprechende Gegenmaßnahmen ergreifen lassen. Die Umsetzung von DiD im industriellen Umfeld ermöglicht es, Attacken frühzeitig zu erkennen und die negativen Folgen zu eliminieren bzw. zu reduzieren.

Ansätze für DiD, die priorisierte Maßnahmen und Best Practices enthalten, gibt es unter anderem vom Department of Homeland Security oder vom Center of Internet Security (CIS). Die Anwendbarkeit dieser Kontrollmechanismen auf industrielle Steuerungsnetze, ICS und Endpunkte muss zuerst geprüft werden. Doch bereits der Einsatz von fünf bis sechs Sicherheitsmaßnahmen kann das Sicherheitsrisiko um etwa 85 bis 95 Prozent senken! Dabei spielen die Bestandsaufnahme und Kategorisierung aller ICS-Assets eine wichtige Rolle, denn sie schaffen ein Grundverständnis für die Support-Infrastruktur bei allen Verantwortlichen – sowohl für IT wie auch ICS. Die Inventarisierung von genehmigter Hardware und Software in ICS und im Unternehmensnetzwerk macht es gleichzeitig einfacher, alle nichtautorisierten Assets zu finden und zu blockieren.

Alexander Glatzer,
IT Professional

Valeria Wild,
IT-Kriminalistin

Christian Grafe,
IT-Forensiker

Mein IT-Einsatz bei der Bayerischen Polizei

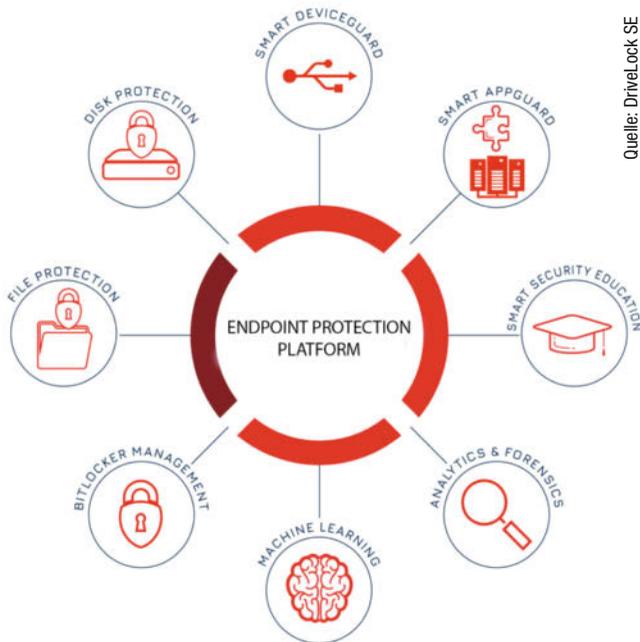
**WELTWEIT ERMITTELN.
IN BAYERN LEBEN.**

IT bei der Bayerischen Polizei ist eine echte Lebensaufgabe. Für alle, die spannende Herausforderungen, vielfältige Karrierechancen und krisenfeste Jobsicherheit suchen.

Jetzt bewerben: www.mit-sicherheit-anders.de/IT



Die Bayerische
POLIZEI



Quelle: DriveLock SE

Abb. 2: Auch bei Endpoint Protection gilt es, verschiedenste Aspekte zu beachten.

Sicherheitskontrollen und Hosts

Kontrollen für die ICS-Sicherheit sind am effektivsten, wenn sie sich nach der Priorisierung richten. Maßnahmen sollten zuallererst an den kritischsten und anfälligsten Systemen vorgenommen werden. Also dort, wo die Folgen von Angriffen am schwersten und ihre Wahrscheinlichkeit am höchsten ist. Dadurch verringert sich das Risiko in ICS erheblich. Sofern der Faktor Mensch eine nicht zu vernachlässigende Rolle spielt, sollten die Maßnahmen auch um das Element Cybersicherheitstraining erweitert werden. Einen hundertprozentigen Schutz gibt es allerdings nicht. Durch den Einsatz der richtigen Sicherheitsvorkehrungen und DiD-Praktiken kann das Risiko jedoch signifikant gesenkt werden.

Damit ein Netzwerk abgesichert ist, müssen auch alle vorhandenen Hosts entsprechend geschützt werden. Das macht die Host- oder Workstation-Ebene zu einer zusätzlichen Sicherheitsebene. Mit Firewalls erhalten die meisten Geräte im Netz Schutz vor Eindringlingen.

Ein wichtiger Bestandteil einer effektiven Sicherheitsstrategie sind Sicherheitsrichtlinien. Organisationen sollten in der Lage sein, jedes Gerät oder jeden ICS-Host im OT-Netzwerk sperren zu können – unabhängig vom Betriebssystem. Entsprechende Maßnahmen sind zum Beispiel strenge Kennwortanforderung, Host-basierte Firewalls, gewissenhaftes Patchen und Aktualisieren von Firmware sowie das Entfernen nicht benötigter Software, beispielsweise vorinstallierter Anwendungen.

Application Control und Whitelisting

Unternehmen müssen alle erdenklichen Infektionswege beachten, um ihre Systeme effektiv vor Schadsoftware schützen zu können. Darunter fallen beispielsweise Wechseldatenträger, Servicestationen, neue Komponenten jeglicher Art (infizierte Speichermedien und Software) sowie Programmiergeräte oder Außenschnittstellen inklusive Verbindungen zum Office-Netz, Internet oder anderen Extranets.

Häufig installieren Angreifer Backdoor-Programme und Bots, wenn sie ein System kompromittieren. So wollen sie sich eine langfristige Kontrolle sichern. Dazu nutzen sie oft Zero-Day-Exploits aus, denn für diese noch nicht gemeldeten Schwachstellen gibt es auch noch keinen Patch vom Softwareanbieter. Eine einzelne kompromittierte Maschine genügt Hackern oft als Staging Point, über den sie kritische Informationen von damit verbundenen Systemen sammeln.

Applikationskontrolle und Whitelisting erlaubt es Organisationen, die Ausführung von Anwendungen zu überwachen und unbekannte Anwendungen zu blockieren. Das Prinzip funktioniert jedoch nicht wie bei Antiviren-Programmen nach dem Prinzip des Blacklistings, bei dem unerwünschte Programme an der Ausführung gehindert werden. Stattdessen wird ausschließlich Software zugelassen, die bekannt und zugelassen ist. Jede Anwendung, die nicht auf der vorher bestimmten Liste ist, wird direkt geblockt und muss explizit freigegeben werden. Mithilfe von Machine Learning kann das Management von Whitelists mit minimalem Personaleinsatz eine Vielzahl an sehr heterogenen ICS sicher verwalten. Intelligente Lösungen sind damit in der Lage, Security-Teams zu entlasten und unternehmensweit zu gewährleisten, dass nur bekannte und sichere Anwendungen ausgeführt werden.

Wechselmedien und mobile Geräte

Mobile Endgeräte wie Service-Laptops oder Wechselmedien wie USB-Sticks bilden aktuell das Haupteinfallstor für Cyberangriffe. Sie können leicht ausgenutzt werden, um Schadsoftware oder Befehle in Sicher-

NACHHALTIGES SCHWACHSTELLEN-MANAGEMENT

Schwachstellen-Management-Systeme dienen dazu, ununterbrochen neue Informationen zu erfassen und zu bewerten sowie passende Maßnahmen zu ergreifen. Dadurch werden Schwachstellen erkannt, behoben und letztendlich wird so das Zeitfenster für Cyberangriffe minimiert. Organisationen müssen proaktiv nach Schwachstellen suchen. Unternehmen, die eine solche Verwundbarkeitsanalyse vernachlässigen, verpassen die Möglichkeit, entdeckte Fehler so schnell wie möglich zu beheben, um die Wahrscheinlichkeit, kompromittiert zu werden, zu reduzieren beziehungsweise zu eliminieren.

Eine gemeldete Schwachstelle bedeutet immer einen Wettlauf gegen die Zeit:

- Angreifer müssen die Attacke durchführen, bevor Sicherheitsteams die Schwachstelle beheben.
- Anbieter müssen schnellstmöglich Patches und Updates entwickeln und bereitstellen, um Angreifern zuvorzukommen.
- Systemverantwortliche müssen Risiken bewerten, Regressions-tests durchführen und Patches installieren, damit sie die Sicherheitslücke schließen, bevor Hacker sie missbrauchen können.

Es ist absolut notwendig, in ICS-Umgebungen automatisierte Softwareupdate-Tools einzusetzen. So ist gewährleistet, dass installierte Software und Betriebssysteme gleichermaßen auf dem neuesten Stand sind. Als Informationsquelle für Schwachstellen-Meldungen dienen in der Regel die Hersteller und CERTs.

heitzonen hinein beziehungsweise sensible Daten hinaus zu befördern. Aus diesem Grund ist umfassende Device Control sehr wichtig. Organisationen sollten es grundsätzlich verbieten oder zumindest sehr stark einschränken, private Geräte für den Datentransport zu verwenden oder an ICS-/OT-Komponenten anzuschließen.

Verwaltungsrechte kontrollieren

Administratorrechte auf Computer, Netzwerke und Anwendungen müssen nachvollziehbar, kontrollierbar, verhinderbar und korrigierbar sein. Dazu sind Prozesse und Werkzeuge für deren Verwendung, Zuweisung und Konfiguration notwendig. Der Missbrauch von Administratorrechten stellt ebenfalls eine Schwachstelle dar, durch die sich Angreifer in den Systemen des Zielunternehmens ausbreiten können. Es genügt, dass ein privilegierter Account auf einer der Workstations eine E-Mail mit böartigem Anhang öffnet oder eine infizierte Datei von einer böartigen Webseite herunterlädt. Angreifer können dank der vorhandenen Administratorrechte den Rechner ihres Opfers komplett übernehmen und mittels Keystroke-Logger, Sniffer und Fernsteuerungssoftware andere Passwörter und sensible Daten herausfinden.

Security Configuration Management

Hersteller richten die Standardkonfigurationen für Betriebssysteme und Anwendungen nicht auf Sicherheit aus, sondern auf leichte Bereit-

stellung und Verwendung. Ob offene Ports und Services, veraltete Protokolle, Standardkennwörter und -konten oder vorinstallierte Anwendungen – im Standardzustand ist alles eine potenzielle Schwachstelle. Mithilfe von Configuration-Management-Lösungen werden die erforderlichen Sicherheitskonfigurationen auf den Endpunkten regelmäßig und automatisch neu zugeteilt und erzwungen. Dafür gibt es auch geprüfte Sicherheits-Benchmarks und Leitfäden, die öffentlich zugänglich sind, damit jede Organisation sie nutzen kann. Dazu gehören zum Beispiel das CIS-Benchmarks™ Program oder das National Checklist Program des US-amerikanischen National Institute of Standards and Technology (NIST).

Datenschutz

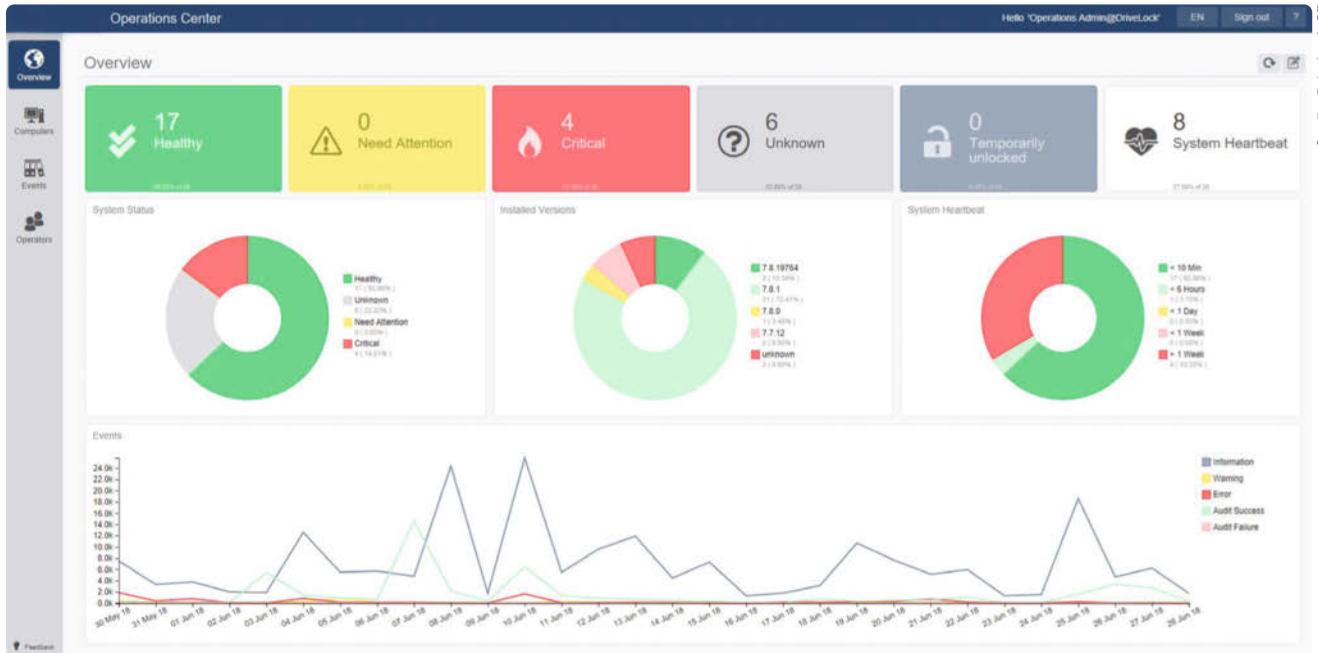
Um Daten an jedem Ort zu schützen, ist eine Kombination aus Data Loss Prevention (DLP), Verschlüsselung und Integritätsschutz erforderlich. Die Vernetzung in ICS/IT, der Einsatz von Cloud-Services sowie der mobile Zugriff haben stark zugenommen. Deswegen ist ein sorgfältiger Umgang mit Daten essenziell. Datenexfiltration muss begrenzt, dokumentiert und deren Folgen abgeschwächt werden. Häufig haben interne Nutzer auf kritische Assets Zugriff – mindestens auf den Großteil, in manchen Fällen sogar auf alle. Wenn ein Angreifer so ein Netzwerk infiltriert hat, kann er mit Leichtigkeit wichtige Informationen extrahieren und Schäden bzw. Betriebsstörungen verursachen.

Es gibt **10** Arten von Menschen.
iX-Leser und die anderen.

3x als Heft

Jetzt Mini-Abo testen:
3 Hefte + iX-Kaffeebecher nur 14,70 €
www.iX.de/test

Magazine titles visible: **Blockchain Hype und ...**, **Chatbot**, **KI schnell und einfach**, **Atom, Sublime Text, Visual Studio Code, Vim**



Quelle: DriveLock SE

Abb. 3: Zweckmäßige Überwachungstools bieten einen schnellen Überblick über potenzielle Bedrohungen.

Um Daten effektiv zu schützen, sollten die Festplatten der mobilen und stationären Endgeräte ausnahmslos verschlüsselt werden. Daneben spielt Device Control auch eine wichtige Rolle. Nur ausgewählte Speichergeräte dürfen erlaubt sein und das Kopieren von Daten auf diese Geräte sollte blockiert werden. Eine zusätzliche Schutzschicht für sensible Informationen bildet eine Multi-Factor-Authentifizierung.

Endpoint Detection und Response

Das BSI erklärt, dass eine frühe Erkennung sicherheitskritischer Ereignisse zusammen mit einer rechtzeitigen Reaktion potenzielle Schäden begrenzen kann. Hier kommt das Thema Endpoint Detection und Response (EDR) ins Spiel (Abbildung 2). Ein Bestandteil von DiD-Strategien ist, Audit-Protokolle von Ereignissen zu sammeln und zu analysieren. Das Ziel ist es, potenzielle Angriffe zu erkennen und entsprechende Schutzmaßnahmen einzuleiten. Auf diese Weise verschaffen sich Organisationen einen wesentlichen Vorteil, weil Cyberkriminelle selten damit rechnen, dass Audit-Protokolle geprüft und ihre Angriffe entdeckt wurden.

Es ist zwar schwierig im ICS-Umfeld, Änderungen, Angriffssignaturen oder anomales Verhalten zu überwachen, umso essenzieller ist dies allerdings für den Schutz von Netzwerken, Systemen und kritischen Assets. Deshalb muss das Sicherheitskonzept frühzeitig Gefahren erkennen und alarmieren, sodass Unternehmen entsprechende Schritte zum Schutz ihrer kritischen Ressourcen tätigen können.

Eine Lösung für das Sammeln, Protokollieren und Korrelieren von Informationen sind Produkte zum „Security Information and Event Management“ (SIEM). Sie können bei spezifizierten Aktivitäten alarmieren und bieten Echtzeitanalysen. Solche Technologien unterstützen auch den Incident-Response-Prozess in ICS-Umgebungen und helfen, die Reaktionszeit auf Vorfälle zu reduzieren (Abbildung 3).

Risikofaktor Mensch

Cyberabwehr nur als technische Herausforderung zu betrachten, ist zu einfach. Die Handlungen der Menschen haben ebenfalls großen Ein-

fluss auf die Sicherheit in Organisationen. Je komplexer ein System ist, umso anfälliger ist es auch für Fehler durch ungeschulte oder unvorsichtige Mitarbeiter oder durch Aktionen von böswilligen Insidern. Deshalb ist es unerlässlich, ein Programm für die Security Awareness einzuführen.

Ein ICS-Sicherheitsverfahren sollte es erlauben, (neue) Mitarbeiter schnell und angemessen zu schulen, sodass sie alle wichtigen Regelungen und Standards einheitlich im kompletten ICS/OT einhalten können. Darüber hinaus muss ein nachhaltiges Security-Awareness-Programm den Mitarbeitern vermitteln, woran sie Versuche von Social Engineering erkennen können und wie sich sensible Daten eindeutig identifizieren und ordnungsgemäß handhaben lassen. Auf diese Weise lässt sich ein versehentliches Veröffentlichendes von kritischen Informationen vermeiden.

Fazit

Effektive IT-Sicherheit für industrielle Anlagen geht stets einher mit einer DiD-Strategie. Es gibt viele öffentlich zugängliche Listen und Anleitungen, die Unternehmen bei diesem Prozess unterstützen. Das BSI zählt beispielsweise Maßnahmen zur Dokumentation der OT-Infrastruktur, sinnvollen Umgang mit Verwaltungsrechten, strenge Authentifizierungsmaßnahmen und Change Management zu den wichtigen Teilaspekten. Organisationen sollten diese Checklisten, Best Practices, Ansätze und Anleitungen auf Anwendbarkeit auf ihre ICS prüfen und auf dieser Basis ein mehrschichtiges Sicherheitskonzept entwickeln und implementieren.

Die Gefahrenquellen steigen mit der Vernetzung und der zunehmenden Komplexität der Systeme. Dabei stellen Insider – ob unbewusst oder beabsichtigt – ein ebenso großes Risiko dar wie externe Angreifer. Deshalb ist es wichtig, den Faktor Mensch in die Cyberabwehr einzubeziehen. Mit den richtigen Trainings werden Mitarbeiter zu einer weiteren Sicherheitsschicht, einer Human Firewall.

Anton Kreuzer
DriveLock SE

Stets einen Schritt voraus

Zukunftsfähige Sicherheitskonzepte folgen dem Security-by-Design-Prinzip

Informationssicherheit wird zukünftig noch wichtiger als bisher für einen anhaltenden Erfolg unserer Unternehmen und unserer gesamten Volkswirtschaft im globalen Wettbewerb. Sie sollte sich deshalb konsequent an einem Security-by-Design-Vorgehen orientieren.

In der industriellen Kommunikation müssen Sicherheits- und Datenschutzarchitekturen als zwingend notwendige Erfolgsfaktoren für global vernetzte Unternehmen und Volkswirtschaften vor allem folgende Eigenschaften aufweisen:

- Security-Management und operativer Betrieb gehen höchst flexibel, adaptiv und weitgehend automatisiert in nahezu Echtzeit (bei Latenzzeiten von ≤ 1 Millisekunde) mit sich ständig verändernden Umgebungsparametern und Bedrohungslagen auf den verschiedenen Technologie- und Business-Ebenen um.
- Der operative Sicherheitsbetrieb erfolgt überwiegend präventiv (statt reaktiv). Er gewährleistet die automatisierte Integration der aktuellsten multidimensionalen Analytikverfahren, Threat-Intelligence- und digitalen Assistenzsysteme in den alltäglichen Expertendialog, was fundiert aufbereitete Soll-Ist-Differenzanalysen und daraus zu treffende Entscheidungen ermöglicht.

Die bisherigen Erkenntnisse aus Standardisierungsprozessen und Forschungsprojekten im Umfeld von 5G und vergleichbaren Zukunftstechnologien sowie den damit verbundenen Möglichkeiten von Industrie 4.0 und IoT machen hingegen deutlich: Gegenwärtig übliche IT-Security-Standardkonzepte in Unternehmen reichen keinesfalls aus, um etwa den in Abbildung 1 beispielhaft aufgeführten 5G-Leistungsmerkmalen als Treiber für eine neue Generation von Anforderungen an Security- und Privacy-Management und Produktivbetrieb im internationalen Wettbewerb gerecht zu werden.

Bewährte Grundlagen

Was heißt das für die Fachverantwortlichen in den Unternehmen? Wissen insbesondere Unternehmer und Entscheider im oft sehr innovativen, leistungsfähigen und vielfach international vernetzten KMU-Segment, was konkret und über den gesamten Lebenszyklus in Entwicklung, Betrieb und Service-Support für Softwareapplikationen sowie in Hardwareprodukten und Dienstleistungsprozessen zu initiieren, zu überwachen und zu verantworten ist? Was sind die Grundlagen und Prinzipien für einen in Iterationsschleifen kontinuierlich sich selbst überprüfenden und sich optimiert an Veränderungen adaptierenden Security-by-Design-Prozess?

Viele geeignete und bewährte Methoden und Vorgehensmodelle im Sinne von Security by Design wurden bei den weltweit erfolgreichsten Unternehmen in der Softwareentwicklungsbranche über mittlerweile mehr als zwei Jahrzehnte zunehmend angewandt, kontinuierlich optimiert und weiterentwickelt. Entsprechend adaptiert sind diese Methodiken auch jenseits des Software Development Lifecycle (SDL) zielführend anwendbar – etwa in den Designphasen für zu entwickelnde Hardwareprodukte und Serviceprozesse. Bewährt haben sich diese Methodiken ebenso bereits in der Entwicklung und Optimierung von Prüf- und Testprozessen im Umfeld von IoT-Geräten und -Systemen.

Threat Modeling

Eine wichtige Kernmaßnahme – und vielleicht der für den gesamten weiteren Prozess grundlegendste Schritt – im Security-by-Design-Lebenszyklus ist nach unseren Erfahrungen (u. a. aus der bisherigen Mitwirkung im BMBF-geförderten Projekt „TACNET 4.0 – Hochzuverlässige und echtzeitfähige 5G-Vernetzung für Industrie 4.0“; Laufzeit: 04.2017 – 03.2020) die sorgfältige Planung und Durchführung eines strukturierten Bedrohungsmodellierungs-Workshops (Threat Modeling). Dies sollte möglichst bald nach der ersten Ideenphase und am Anfang der Funktions- und System-Designphase für das Planobjekt (HW-/SW-Produkt, Serviceprozess, Anwendungsfall ...) geschehen. Hierbei wird in einem moderierten Dialog zwischen allen relevanten Stakeholdern,

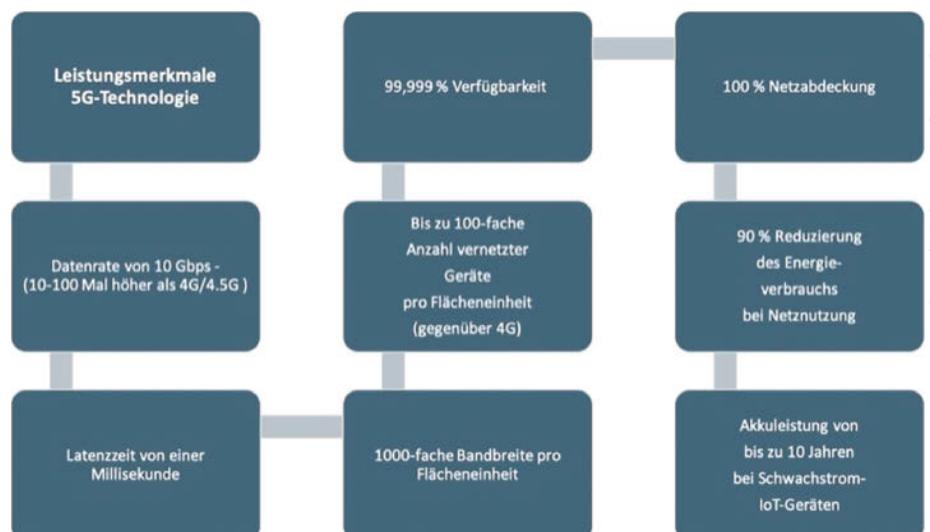


Abb. 1: Übersicht der Leistungsmerkmale der 5G-Technologie

Quelle: OTARIS Interactive Services GmbH

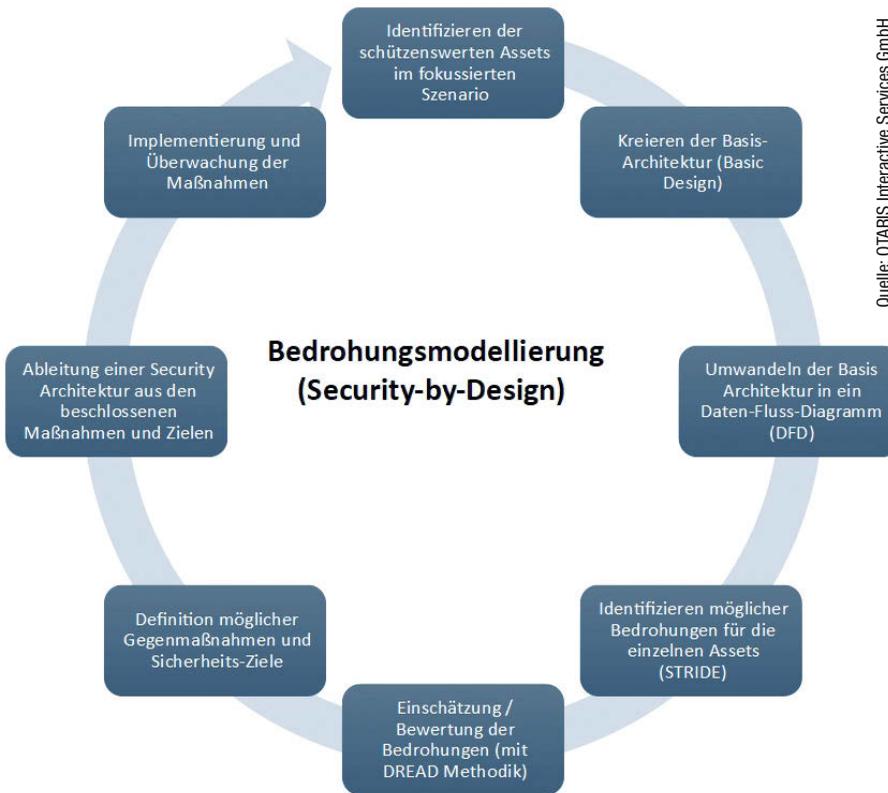


Abb. 2: Schematisch dargestellte Vorgehensweise zur Bedrohungsmodellierung

die in das Planobjekt eingebunden sind und sich hinsichtlich ihrer jeweiligen Verantwortlichkeit, Perspektive und Anforderungen aktiv einbringen, zunächst eine Modellbildung mit der priorisierten Identifizierung der zu schützenden Assets (Prozess-/System- und Datenspeicherelemente sowie Datenflüsse) unter Security- und Privacy-Gesichtspunkten vorgenommen.

In weiteren Schritten werden von allen Stakeholdern die je Element und Datenfluss möglichen Bedrohungen nach den STRIDE-Kriterien (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of Privilege) identifiziert und dokumentiert und nach den vorgegebenen DREAD-Kriterien (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability) bezüglich ihrer relevanten Risikoeinschätzung bewertet (Abbildung 2).

Mit einem so oder qualitativ vergleichbar durchgeführten Bedrohungsmodellierungs-Workshop mit allen betroffenen Stakeholdern und der anschließenden Dokumentationsaufbereitung – vorzugsweise durch kompetente und erfahrene Security-Engineers bzw. -Designer – liegen als Ergebnis spezifisch dokumentierte und von allen Beteiligten mitgetragene Security-Requirements, Schutzziele und geplante Maßnahmen als Grundlage für den weiteren Lebenszyklus des Planobjekts vor. Gemäß dem Regelwerk des im Unternehmen angewandten Information-Security-Management-Systems (ISMS) bzw. des Regelwerks für das Dokumentenmanagement werden diese Ergebnisse wahlweise auch parallel zum Funktions- und Systemdesign als spezifische Sicherheitsarchitektur (Security-Design) separat aufbereitet und im weiteren Prozess optimiert und implementiert. Diese spezifisch beschriebenen Security-Requirements und Schutzziele bzw. das so vorliegende Security-Design bilden damit auch die Soll-Grundlage für die in den einzelnen Phasen im weiteren Lebenszyklus vorgegebenen Überprü-

fungen (Penetrationstests etc.) von möglichen Soll-Ist-Abweichungen.

Abhängig vom im Unternehmen angewandten Lebenszyklusmodell werden in Fällen von relevanten Soll-Ist-Abweichungen Optimierungsschleifen systematisch und dokumentiert bis zur zuverlässigen Erreichung des geforderten Security-Qualitätsniveaus iterativ durchgeführt. Gleichzeitig dienen die beschriebenen Ergebnisse der Security-Requirements und die daraus abgeleitete Sicherheitsarchitektur aus der frühen Designphase sowie die anschließenden Optimierungen auch als Grundlage und Soll-Vorgabe für entsprechende Abnahmekriterien und Tests etwa bei der Übernahme (intern oder extern) durch den Kunden in den Produktiv- bzw. Servicebetrieb.

Quality of Security

Zu den Security-by-Design-Prinzipien gehört in den weiteren Entwicklungsphasen des gesamten Lebenszyklus die Identifizierung und laufende Anpassung von Security-relevanten Kennzeichen (Risiko-Index) und KPI-Konzepten (Key-Performance-Indikatoren). Derartige Quality-of-Security-KPI-Konzepte liefern entscheidende Erfolgskriterien für ein zuverlässiges

und möglichst durchgehend präventives und flexibel adaptiertes Agieren bei unvorhergesehenen und bislang unbekanntem Bedrohungslagen, Anomaliedetektionen und Angriffsvektoren in nahezu Echtzeit. Geeignete Quality-of-Security-Konzepte sind die Grundlage für ein aufzubauendes Frühwarnsystem im zukünftigen Security-Management sowie im Betrieb.

Derzeit am Markt verfügbare Threat-Intelligence-Systeme stellen aktuell quasi per Definition spezifische Informationen und Profile über feindselige Bedrohungen in unterschiedlichen Kontexten bereit. Darüber hinaus unterstützen sie Security-Experten im Rahmen von Analysen darin, zukünftige Situationen vorherzusagen und/oder präventiv Entscheidungen zu treffen. Es bleibt abzuwarten, ob und bis wann diese Systeme auch mit Methoden der künstlichen Intelligenz (Stichwort: Supervised Machine Learning) zumindest einigermaßen zuverlässig generische Angriffsvektorenmuster, etwa für unterschiedliche Branchenkontexte, aufbereiten und die präventive Anomaliedetektion und -analyse im operativen Betrieb unterstützen können.

Fazit

Eine intelligente und umgebungsspezifisch angepasste Nutzung modernster Technologien wie Threat Intelligence sowie die Einbindung von digitalen Assistenzsystemen werden zukünftig wesentlich über unternehmerischen Erfolg im global vernetzten Wettbewerb entscheiden. Ausschlaggebend für die IT-Security-Qualität im Industrie-4.0- bzw. Industrial-IoT-Umfeld wird in den kommenden Jahren der Kompetenzaufbau bei verfügbaren unternehmenseigenen und externen Beratungsressourcen sein – vor dem Hintergrund des Anforderungsniveaus in der Etablierung eines Security-by-Design-Prozesses über den gesamten Lebenszyklus hinweg.

Rolf Blunk
OTARIS Interactive Services GmbH

Technische Hilfe zur DSGVO

Data-Discovery- und DLP-Lösungen erleichtern die Einhaltung der DSGVO-Vorgaben

Seit 25. Mai 2018 gilt die europäische Datenschutz-Grundverordnung (DSGVO). Technische Unterstützung bei der Umsetzung bieten Data-Discovery- und Data-Leakage-Prevention-Produkte, die es zugleich ermöglichen, Kundenanfragen zum Thema schnell und vollständig zu beantworten.

Seit dem Inkrafttreten der DSGVO müssen Unternehmen ihre Kunden darüber informieren können, ob und wie sie personenbezogene Daten von ihnen verarbeiten. Das klingt einfacher als es ist. Das Aufspüren personenbezogener Daten gestaltet sich kompliziert und aufwendig. Denn Namen, Adressen, Kontonummern, IP-Adressen, Kontostände, Rechnungen und Fotos verstecken sich in E-Mails, Datenbanken, Protokolldateien, Programmen, Backups und an vielen anderen Stellen.

Ordnen, finden, kontrollieren

Zunächst müssen die Daten klassifiziert werden. Das hilft auch dabei festzulegen, welche Dokumente und Formulare überhaupt unter die Verordnung fallen. Klassifizierung bedeutet, es wird definiert, wo schützenswerte Daten im Unternehmen liegen und welche Struktur sie haben. Wie sind z. B. Kundennummern aufgebaut? In welcher Tabellenspalte werden Vornamen gespeichert? Und wo sind welche Dateien abgelegt? Mit diesen Informationen lassen sich im nächsten Schritt gezielt relevante Dokumente und Formulare finden. Anschließend gilt es, die Daten sinnvoll zu verwalten. So müssen etwa Adressen gelöscht und Namen geändert werden. Als letzter Schritt folgt die Überwachung der Daten. Wurden alle nötigen Änderungen wie gewünscht umgesetzt? Müssen bei einer Datenwiederherstellung bestimmte Daten erneut geändert werden?

Bei den erwähnten Schritten bieten Data-Discovery- und Data-Leakage-Prevention-Lösungen (auch: Data Loss Prevention/DLP) Unterstützung. DLP-Anbieter sind schon länger auf dem Markt. Sie hatten sich ursprünglich als Ziel gesetzt, den unkontrollierten Abfluss von Daten zu verhindern. Mit Inkrafttreten der DSGVO erleben DLP-Anbieter nun wieder eine Steigerung der Nachfrage, denn sie versprechen, dass ihre Produkte Speicherorte von personenbezogenen Daten finden und Transportpfade aufzeichnen. DLP-Lösungen helfen beim Klassifizieren, Suchen und Überwachen von Daten. Lediglich die Verwaltung lässt sich mit ihnen nicht direkt umsetzen. Da die Überwachung oft durch eine erneute

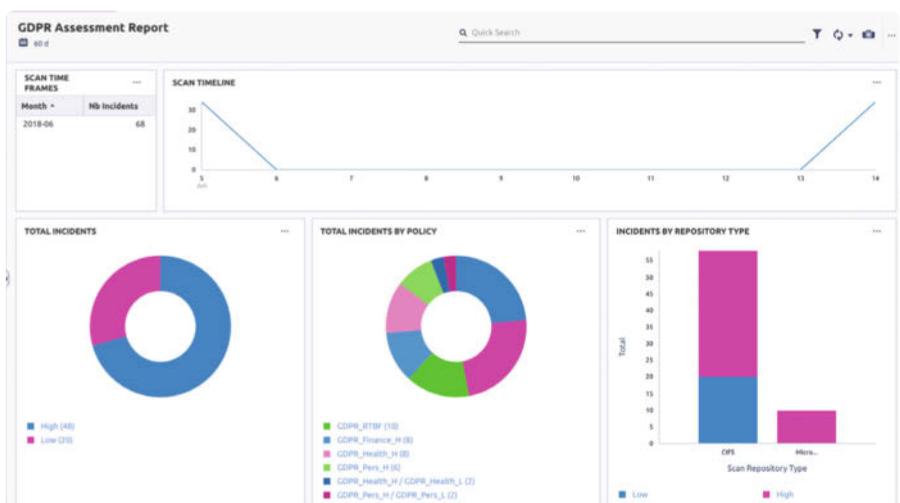
Suche durchgeführt wird, kann man durch einen Vergleich aktueller und alter Suchergebnisse feststellen, ob Daten entfernt wurden.

Auch klassische Data-Discovery-Lösungen gibt es schon lange. Sie stammen aus dem Bereich der Business Intelligence (BI). Ursprünglich wurden diese Lösungen genutzt, um Informationen aus verschiedenen Datenquellen zusammenzubringen und in ein einheitliches Format zu überführen. An einen Einsatz im Security-Umfeld wurde damals noch nicht gedacht. Doch einige, vor allem junge Unternehmen haben angefangen, diese Technik für Security-Lösungen wie das Monitoring von Zugriffsrechten sowie zur Erfüllung der Anforderungen der DSGVO zu nutzen. Die neuen Lösungen klassifizieren Daten und identifizieren deren Speicherorte. Präventive Funktionen stehen bei ihnen nicht im Fokus, sind aber möglich – zum Beispiel in Kombination mit DLP- oder anderen IT-Security-Produkten wie Verschlüsselungslösungen.

Formate und Speicherorte

Die Identifizierung von personenbezogenen Daten in eingescanneten Dokumenten, egal ob hand- oder maschinengeschrieben, ist derzeit noch ein Randthema, wird aber zunehmend wichtiger. Trotzdem beherrschen erstaunlich viele DLP-Lösungen diese Funktion schon heute, wie übrigens auch Funktionen für den Bereich Forensik. Voraussetzung dafür ist eine OCR-Funktionalität. Eine andere Herausforderung stellen Backups dar. Die Suche nach personenbezogenen Daten in Backups insbesondere auf Offline-Datenträgern ist äußerst schwierig. Es ist außerdem wichtig, dass gelöschte oder gesperrte Daten nach

Die Data Protection Suite findet DSGVO-relevante Daten und bereitet sie anschaulich auf.

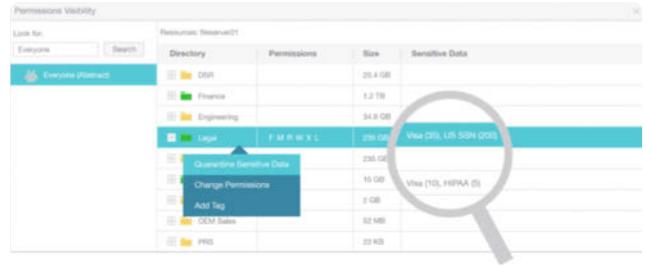


Quelle: Digital Guardian

ERST PRÜFEN, DANN KAUFEN

Welche Software in einem Unternehmen den Ton angeben sollte, hängt stark von der Situation vor Ort ab. Wichtig ist, ob personenbezogene Daten in unstrukturierten Quellen wie E-Mails, SharePoint oder Server-Dateisystemen gespeichert werden oder eher in strukturierten Quellen wie Datenbanken, Verzeichnisdiensten und ERP-Systemen. Vor der Anschaffung einer Lösung sollten sich Verantwortliche deshalb folgende Fragen stellen:

- Kann die Lösung personenbezogene Daten für folgende Anwendungsfälle identifizieren und durchsuchen: Datenbanken, Verzeichnisdienste, ERP-Systeme oder Log-Dateien?
- Ist es möglich, Datenbanken zu durchsuchen, z. B. Oracle, MySQL, MSSQL und PostgreSQL?
- Werden Verzeichnisdienste nicht nur genutzt, um die Authentifizierung der Administratoren durchzuführen, sondern können diese auch als Datenquelle durchsucht werden?
- Ermöglicht die Lösung eine Anbindung von ERP-Systemen, etwa von SAP, Microsoft oder Oracle?
- Kann die Software Log-Dateien nach Informationen wie IP-Adressen, Nutzer-IDs und Positionsdaten durchsuchen?
- Ist die Lösung in der Lage, Daten in Groupware wie z. B. in Microsoft Exchange oder IBM-Notes-Konten zu identifizieren und zu kategorisieren? Hierbei kommt es darauf an, ob lediglich E-Mails durchsucht werden müssen oder auch Kontakte und Kalender. Kommen keine Groupware-Lösungen zum Einsatz, sollten IMAP-Postfächer sowie Kalender und Kontaktendienste mit CalDav und CardDav angebunden werden können.
- Verfügt das Produkt über die Möglichkeit, Inhalte aus Confluence, SharePoint oder anderen Collaboration-Lösungen zu verarbeiten?
- Unterstützt die Lösung alle gängigen Linux- und Windows-Dateisysteme? Werden personenbezogene Daten nicht in Fileshares oder Datenbanken abgelegt, sondern als Datei auf dem nativen Dateisystem des Servers, kann es notwendig sein, diese ebenfalls zu durchsuchen. Beispiele dafür wären der Upload eines PDFs oder eines Bildes in einer Webapplikation.
- Beherrscht das Produkt die Kommunikation mit Cloud-Diensten, die z. B. via Microsoft Azure, Amazon Web Services (AWS) oder Google Cloud angeboten werden?
- Besteht die Möglichkeit, auf verschlüsselte Daten zuzugreifen und/oder verschlüsselten Traffic auszuwerten? Schwierig ist dabei der fehlende Zugriff auf das Schlüsselmaterial. Um diesen Punkt umzusetzen, muss der Anbieter der Lösung eine zentrale Schlüsselverwaltung besitzen, auf die die eingesetzte Data-Discovery- oder DLP-Lösung zugreifen kann. Alternativ muss der Anbieter einen Master- beziehungsweise Recovery-Key bereitstellen.
- Kann mithilfe der Lösung ermittelt werden, ob personenbezogene Daten auf zentralen Fileshares liegen und kann die Lösung diese Dateien darüber hinaus auch auf einzelne Datensätze hin durchsuchen?
- Ist es möglich, personenbezogene Daten während der Übertragung im eigenen Netzwerk und an Netzwerkübergängen zu öffentlichen Netzwerken (Internet) zu identifizieren?



Quelle: Varonis

Mit dem IDU Classification Framework können vor allem kleine Unternehmen ihre Daten im Hinblick auf die DSGVO klassifizieren lassen.

einer Wiederherstellung identifiziert und erneut gelöscht beziehungsweise gesperrt werden können.

In vielen Betrieben dürfen Mitarbeiter Daten nicht auf Client-Systemen speichern. Somit ist eine Analyse, ob und welche personenbezogenen Daten auf Client-Systemen liegen, oft kein Grundkriterium bei der Entscheidung für oder gegen eine Lösung. Kontakte, E-Mails und Dokumente, die auf Endgeräten synchronisiert werden, lassen sich zentral auswerten und bei Bedarf löschen. Wer private Sharing-Dienste unterbinden möchte, kann DLP-Lösungen oder sogenannte Cloud Access Security Broker (CASB) einsetzen. Bei Synchronisierungen ist es wichtig, dass die Lösung der Wahl personenbezogene Daten während der Übertragung identifizieren kann, um zu erkennen, welche externen Partner und Dienstleister die Daten empfangen.

Zugriff und Verwaltung

Die bisher genannten Anforderungen für Data-Discovery-Tools gelten natürlich auch für DLP-Lösungen. Zusätzlich sollte eine DLP-Lösung sicherstellen, dass sich Schnittstellen überwachen und kontrollieren lassen und dass damit festgestellt werden kann, ob Daten, die das Firmennetzwerk verlassen, nur an autorisierte Dritte übermittelt werden. Personenbezogene Daten erfolgreich zu identifizieren, ist der erste Schritt. Der zweite besteht darin, den Zugriff auf die Daten und ihre Verwaltung zu klären. Data-Discovery-Tools müssen auf sämtliche Datenspeicher des Unternehmens zugreifen. Administratoren und Nutzer der Lösung dürfen trotzdem keinen vollständigen Zugriff auf die originären Daten an jeglichen Zugriffsberechtigungen vorbei erhalten. Ein klares Rollen- und Rechtekonzept sowie eine verschlüsselte Ablage der Zugangsdaten für die Datenquellen hilft, die ursprünglichen Zugriffsrechte einzuhalten.

Fazit

Unternehmen, die schnell und vollständig personenbezogene Daten identifizieren müssen, sollten die Anschaffung einer Data-Discovery- und/oder DLP-Lösung ernsthaft in Erwägung ziehen. Die meisten Produkte erleichtern die Suche nach personenbezogenen Daten, auch wenn keines die Anforderungen der DSGVO vollständig abdeckt. Am ehesten in der Lage dazu sind die DLP-Lösungen. Hier merkt man, dass die Anbieter sich schon lange mit dem Thema beschäftigen und entsprechend viel Erfahrung besitzen. Trotzdem kommt es auch hier wie so oft auf den Einzelfall an. Alternativen lohnen sich, wenn DLP-Lösungen spezielle Anforderungen nicht abdecken oder für kleine Firmen zu teuer sind.

*Reimar Karlsburger und Mark Sobol
SVA System Vertrieb Alexander GmbH*

Nicht so sicher wie gedacht

Auch das Blockchain-Konzept ist nicht frei von Sicherheitsproblemen

Während sich der Fokus bei den Implementierungen von Blockchains weg von „Blockchains machen alles besser!“ hin zu „An welcher Stelle liefern Blockchains einen Nutzen bei der Problemlösung?“ verschiebt, muss sich der Blick auch auf die realen Herausforderungen in puncto Sicherheit richten.

Die Frage nach der Sicherheit wird beim Thema Blockchains gern mit dem Argument abgetan, die kryptografischen Verkettungen seien durch ihre verteilte Struktur und die Konsensmechanismen zusammen mit der verwendeten Verschlüsselung per se sicher und vertrauenswürdig. Das stimmt in vielen Fällen – zumindest zum Teil. Nur gibt es eben auch Implementierungsaspekte, die differenzierter betrachtet werden müssen.

Dabei lassen sich mehrere Problemfelder identifizieren: die Art der Blockchain und der eingesetzten Konsensmechanismen; die Metadaten, die bei der Nutzung anfallen; die in der Blockchain selbst vorgehaltenen Daten und deren Verschlüsselung, Pseudonymisierung und Anonymisierung; die nicht in der Blockchain vorgehaltenen Informationen und deren Sicherheit; die Governance der Blockchain und nicht zuletzt der Schutz der Wallets und der darin enthaltenen Informationen wie beispielsweise private Schlüssel.

Wer ist vertrauenswürdig?

Je nach Art der Blockchain oder der alternativen Konzepte, wie etwa dem digitalen Bezahlsystem Iota mit den statt Blöcken eingesetzten Tangles (Knoten), gibt es sehr unterschiedliche Konsensmechanismen. Auch unterscheiden sich die Zugriffskonzepte. Bei sogenannten „permissioned“ Blockchains bedarf es einer Berechtigung, um Pakete hinzuzufügen. Damit lassen sich zwar viel schneller Änderungen durchführen als bei dem anonymen und komplexen Konsensmechanismus „Proof of Work“ (Lösen einer Rechenaufgabe als Arbeitsnachweis), der beispielsweise bei der Bitcoin-Blockchain eingesetzt wird. Dafür müssen die Berechtigungen aber auch überprüft werden.

Bei einigen Ansätzen wie Iota werden Pakete sogar von designierten Stellen hinzugefügt, denen entsprechend vertraut werden muss. Solche Zugriffsberechtigungen stellen ebenso wie privilegierte Nutzer ein potenzielles Sicherheitsrisiko dar. Die adäquate Authentifizierung und Autorisierung solcher Zugriffe ist essenziell für die Vertrauenswürdigkeit dieser Konzepte. Das ist kein grundsätzliches Problem, aber eben ein potenzielles Risiko.

Wer hat alle Daten im Blick?

Das zweite Problemfeld sind Metadaten. Ebenso wie etwa bei der Kommunikation über verschlüsselte E-Mails lassen sich aus Metadaten Rückschlüsse beispielsweise auf finanzielle Transaktionen ziehen, die über die Bitcoin-Blockchain abgewickelt werden. Die Transaktionen werden mit Sender und Empfänger dauerhaft in der Blockchain gespeichert und lassen sich damit potenziell auch rückverfolgen. Sender und Empfänger sind zwar grundsätzlich anonym, aber Muster werden erkannt – und zwar dauerhaft.

Darüber hinaus sind auch die in der Blockchain vorgehaltenen Daten grundsätzlich ein Angriffspunkt, selbst wenn sie mit kryptografischen Verfahren verändert wurden. Letztendlich gilt wie bei allen verschlüsselten oder als Hash gehaltenen Informationen, dass es nur eine Frage des einzusetzenden Aufwands ist, auch die besten Schutzmechanismen zu knacken. Je nach Konzept und Einsatzbereich der Blockchains führt das allein zwar nicht zu aussagekräftigen Informationen. Zusammen mit weiteren Daten wie Metadaten oder Registrierungsinformationen von Bitcoin-Börsen (und warum sollten etwaige Angreifer nicht auch an diese gelangen können?) vielleicht aber dann doch. Man sollte sich jedenfalls nicht blind darauf verlassen, dass alles dauerhaft sicher ist.

Hinzu kommt, dass bei vielen Implementierungen keineswegs alle Daten in der Blockchain selbst gehalten werden. Komplexe Geoinformationen, wie sie für Grundbücher benötigt werden, Patentbeschreibungen und viele andere umfangreiche Informationsquellen lassen sich schon aufgrund ihrer Größe gar nicht sinnvoll in der Blockchain selbst ablegen. Sie liegen also an anderer Stelle. Das schafft einerseits das Problem, diese Daten synchron zu halten. Andererseits stellt dies aber auch eine nicht zu verleugnende Sicherheitsfrage dar. Während sich der Zusammenhang zwischen der Blockchain und den externen Daten verlässlich über Hash-Werte abbilden lässt, sieht es mit der Sicherheit der dezentral gehaltenen Daten anders aus. Die Absicherung muss dann wiederum über separate, ebenfalls dezentrale Mechanismen gewährleistet werden.

Wer ist verantwortlich?

Ein bisher kaum betrachtetes Thema ist die Governance für Blockchains oder die Frage, wem die Blockchain eigentlich gehört. Wer darf über Forks (Abspaltungen) oder gar über Änderungen des Konsensmodells entscheiden? Wer ist letztlich für den Code verantwortlich? Wer stellt den dauerhaften Betrieb auch dann sicher, wenn keine oder nur noch wenige Änderungen erfolgen, aber weiterhin Zugriff auf die Altdaten erforderlich ist. Diese Fragen sind oft entscheidend, weil sie direkte Auswirkungen auf die dauerhafte Verfügbarkeit und Sicherheit der Daten, aber auch auf die Anwendungen, die auf den Blockchains aufsetzen, haben können.

Wer schützt die Endpoints?

Schließlich gibt es noch ein ganz fundamentales Sicherheitsproblem: Wie werden die Wallets geschützt, in denen beispielsweise private Schlüssel, oft aber noch weitere sensitive Daten – so etwa private Daten bei Blockchain-ID-Ansätzen – gehalten werden? Die privaten Schlüssel sind aus Sicht des Benutzers die wirklich heiklen Informa-



Bei Blockchains gibt es eine Reihe von Herausforderungen in puncto Sicherheit.

tionen. Der Standardansatz für den Schutz von Wallets, beispielsweise für den Fall einer Wiederherstellung, ist eine Passphrase. Faktisch ist das allerdings nichts anderes als ein besonders langes Kennwort.

Zwar können komplizierte Kennwörter die Sicherheit etwas verbessern, sie lösen aber die fundamentalen Probleme einer (ausschließlich) kennwortbasierten Sicherheit nicht. Dieses Problem schränkt die Einsetzbarkeit von Blockchains in vielen Szenarien ein – Nutzer, die keine sicheren Endgeräte für Wallets haben, können auch nicht von der sicheren Blockchain-ID, vom sicheren Banking für „unbanked Persons“ oder anderen Anwendungen profitieren, die gerne als Idealbeispiele für das Potenzial von Blockchains genannt werden. Auch hier gilt aber: All das sind keine unlösbaren Herausforderungen, aber solche, auf die

sich das Augenmerk jetzt, in der Phase nach dem ersten großen Hype, richten muss.

Fazit

Das alles spricht natürlich nicht gegen den Einsatz von Blockchains. Und viele der hier genannten Herausforderungen sind für die meisten Anwendungsfälle auch unkritisch. Besonders heikel sind aber der Schutz der Wallets selbst und nicht zuletzt das Thema Blockchain-Governance, das bisher leider viel zu selten in die Betrachtung Einzug erlangt hat.

*Martin Kuppinger
KuppingerCole Analysts AG*

Impressum

Themenbeilage Sicherheit & Datenschutz

Redaktion just 4 business GmbH

Telefon: 08061 34811100, Fax: 08061 34811109,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:

Thomas Jannot (v.i.S.d.P.), Ralph Novak, Martin Fuhrmann (Redaktion),
Rudolph Schuster (Lektorat)

Autoren dieser Ausgabe:

Rolf Blunk, Hauke Gierow, Reimar Karlsburger, Anton Kreuzer,
Martin Kuppinger, Dr. Holger Mühlbauer, Torsten Redlich,
Mark Sobol, Michael Zimmer

DTP-Produktion:

Benjamin Geschwantner, Matthias Timm, Hinstorff Media, Rostock

Korrektur:

Marei Stande, Hinstorff Media, Rostock

Titelbild:

© shutterstock, Sentavio

Verlag

Heise Medien GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 0511 5352-0, Telefax: 0511 5352-129

Geschäftsführer:

Ansgar Heise, Dr. Alfons Schröder

Mitglieder der Geschäftsleitung:

Beate Gerold, Jörg Mühle

Verlagsleiter:

Dr. Alfons Schröder

Anzeigenleitung (verantwortlich für den Anzeigenteil):

Michael Hanke (-167), E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix

Leiter Vertrieb und Marketing:

André Lux

Druck:

Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlages verbreitet werden; das schließt ausdrücklich auch die Veröffentlichung auf Websites ein.

Printed in Germany

© Copyright by Heise Medien GmbH & Co. KG

Die Inserenten

Die hier abgedruckten Seitenzahlen sind nicht verbindlich.
Redaktionelle Gründe können Änderungen erforderlich machen.

BSI	www.bsi.bund.de	5	DGI	www.dgi-ag.de	7
			IT-Bewerberkoordination der Bayerischen Polizei	www.mit-sicherheit-anders.de/IT	9
			Netfiles	www.netfiles.de	2
			Verimi	www.verimi.de	20

Der Treffpunkt für Security-Anwender und -Anbieter!

Seien Sie dabei und profitieren Sie als Besucher von neuesten IT-Security Trends, Produkten oder Software-Lösungen.

16 vertiefende
Workshops
zu aktuellen
IT-Sicherheits-
themen

Bis zu
40
Expert Talks

Wichtige
Unternehmen
aus der
IT-Sicherheits-
branche

Netzwerken
und feiern
auf der
großen
secIT-Party

Mehr als
40 Vorträge
führender
IT-Experten
auf 2 Bühnen

Hochkarätige
Sprecher,
ausgewählt
von unseren
Redaktionen

THEMENSCHWERPUNKTE:

- Cloud Security
- Datensicherheit
- Datenschutz und Privacy (DSGVO)
- Digitalisierung
- Industrie 4.0
- Security as a Service
- Blockchain / IOTA
- IoT

sec-it.heise.de



Die Partner der secIT Hannover

aikux.com

[AirIT](http://AirIT.com)

Bundeskriminalamt

[COMPASS SECURITY](http://COMPASS-SECURITY.com)

[ConSecur](http://ConSecur.com)
[security and consulting]

[DocSetMinder](http://DocSetMinder.com)
Ready for Audit

[PART.LTD](http://PART.LTD.com)

[HORNETSECURITY](http://HORNETSECURITY.com)

[protea networks](http://protea-networks.com)

[TAR-0X](http://TAR-0X.com)
IT-Technologie made im Ruhrgebiet

[tenfold](http://tenfold.com)

[TREND MICRO](http://TREND-MICRO.com)

Veranstalter

[Heise Medien](http://HeiseMedien.com)

Kooperationspartner

[bitm](http://bitm.com)
Bundesverband
IT-Mittelstand e.V.

Organisiert von

[heise Events](http://heise-Events.com)

Jetzt neuen Kunden den Zugang zu meinem Shop erleichtern?

Das macht Verimi

**Verimi
kommt**

JETZT
PARTNER WERDEN

Verimi ist die große europäische Identitätsplattform, die neuen Nutzern die Registrierung für Ihr Online-Angebot vereinfacht.

Lassen Sie Ihr Unternehmen ab sofort von hochwertigen Nutzerdaten und einer besseren Marktpräsenz profitieren.

verimi.com

verimi
Mein digitales Ich