GIT CYBER SECURITY

INNENTITEL

HEFT IM HEFT

Mit Innentitel: Tüv Süd
Kernelemente des Datenschutzes

Seite 34

DATENSCHUTZ

Kernelemente des Datenschutzes

Ein Beitrag von Mareike Vogt von der Tüv Süd Sec-IT

Kleinen und mittleren Unternehmen (KMU) fehlt meist das Fachpersonal, um die Anforderungen zum Datenschutz zu identifizieren und umzusetzen. Gleichzeitig steigen technischen Möglichkeiten, gegen die ein Unternehmen seine Daten sichern muss. Wie lässt sich diese Herausforderung meistern? Mareike Vogt, Fachexpertin für Datenschutz bei der Tüv Süd Sec-IT, erklärt, wie Datenschutz rund um die drei Säulen Mensch, Technik und Prozesse auch für KMU funktioniert.

Längst basieren ganze Geschäftsmodelle darauf, Geld mit den Daten anderer Menschen zu machen. Von einem Thema am Rande, über das lediglich Experten diskutierten, avancierte der Datenschutz im letzten Jahrzehnt daher zu einem zentralen Bereich moderner IT-Sicherheit. Im Zuge dieser Aufklärung über die Gefahren unzulänglicher Datenverarbeitung gibt es auf internationaler Ebene unterschiedliche Regulierungen, um die Bürger besser gegen Missbrauch ihrer personenbezogenen Daten zu schützen – in Europa ist es die Europäische Datenschutz-Grundverordnung (EU-DSGVO).

Gleichzeitig stellen die von jedem Nutzer gesammelten Informationen einen wertvollen Rohstoff für Unternehmen aller Art dar, unter anderem in Form von Kundenkontakten oder zur Datenanalyse. Sie sind zu einem wichtigen Aspekt für betriebswirtschaftliche oder strategische Entscheidungen geworden. Wie schaffen aber vor allem kleinere und mittlere Unternehmen (KMU), die besonders unter einem Mangel an Fachkräften leiden, den Spagat zwischen dem Interesse an Daten und Datenschutzkonformität? Eine einfache und effektive Lösung für einen Fachkräftemangel, kann die Unterstützung durch einen unabhängigen externen Berater im Datenschutz darstellen. Gerade bei KMUs bietet es sich sogar an, die Aufgabe des Datenschutzbeauftragen durch externen Fachexperten übernehmen zu lassen. Gemeinsam sollte man sich dann an den drei Säulen des Datenschutzes orientieren.

Faktor Mensch

Die erste Säule, auf die sich EU-DSGVO-konformer Umgang mit personenbezogenen Daten stützt, ist der Mensch. Mitarbeiter, die im Unternehmen mit personenbezogenen Daten zu tun haben, müssen geschult werden. Es muss ein Bewusstsein geschaffen werden, welche Anforderungen zum Datenschutz an die Mitarbeiter und ihre Arbeit bestehen und welche Strafen dem Unternehmen bei Missachtung drohen. Ab einer bestimmten Größe – 20 Mitarbeitende, die regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind – müssen Unternehmen in Deutschland zudem einen Datenschutzbeauftragten benennen. Dieser berät nicht nur zielgerichtet, sondern kontrolliert die Einhaltung der EU-DSGVO im Unternehmen und dient als Ansprechpartner für zuständige Aufsichtsbehörden. Dieser Datenschutzbeauftragte fungiert als erste Anlaufstelle für Datenschutzanliegen, muss aber nicht im Unternehmen selbst beschäftigt sein. Unabhängige Dienstleister wie Tüv Süd bieten deshalb nicht nur Mitarbeiterschulungen zum Datenschutz an, sondern können auch den externen Datenschutzbeauftragten stellen.

> „Wer das Vertrauen der Kunden in sein Unternehmen gewinnen und erhalten möchte, kommt seit einigen Jahren nicht mehr am Datenschutz vorbei.“

Mareike Vogt, Fachexpertin für Datenschutz bei der Tüv Süd Sec-IT

© pickup – Stock Adobe

Faktor Prozesse

Als zweite Säule gilt es, die internen Prozesse zur personenbezogenen Datenverarbeitung an die Anforderungen der EU-DSGVO anzupassen. Das beginnt bei der Sammlung solcher Daten, beispielsweise über die eigene Webseite. Zwar ist es möglich, Nutzerdaten mittels Cookies zu erfassen, allerdings muss der Nutzer vorher oftmals einwilligen. Das passiert über Cookie-Banner, die dem Nutzer beim Besuch der Seite angezeigt werden müssen. Welche Informationen darin enthalten sein müssen und wann eine Einwilligung rechtens ist, regelt die EU-DSGVO. Ergänzend helfen Gerichtsurteile sowie Aufsichtsbehörden bei der Auslegung. Eine unabhängige Beratung kann auch hier helfen, Fallstricke zu erkennen und zu vermeiden.

Faktor Technik

Die dritte Säule des Datenschutzes ist die Technik. Sie beinhaltet die angemessene und sichere Verarbeitung der Daten. Wie stark die durch die EU-DSGVO geforderte Sicherheit der Verarbeitung sein muss, ergibt sich unter anderem anhand einer objektiven Bewertung der Daten und Risiken. Es sollte daher eine Abwägung zwischen dem Schutzbedarf der Daten und den möglichen Sicherungsmaßnahmen getroffen werden. Da sich technische Möglichkeiten stets weiterentwickeln, ist es sehr wichtig, dass diese Abwägungen regelmäßig überprüft und angepasst werden. Nur so wird sichergestellt, dass die Sicherheit der Verarbeitung langfristig angemessen bleibt.

Kein Vertrauen ohne Datenschutz

Wer das Vertrauen der Kunden in sein Unternehmen gewinnen und erhalten möchte, kommt seit einigen Jahren nicht mehr am Datenschutz vorbei. Er gilt heute als Qualitätssiegel. Die drei Säulen des Datenschutzes, Mensch, Prozesse und Technik, bieten eine gute Orientierung, um diese Herausforderung erfolgreich zu meisten. Unternehmen, deren eigene Personalressourcen begrenzt sind, finden die passende Unterstützung bei externen Fachexperten. Denn Strafen sind nicht nur schlecht fürs Image, sondern können auch schnell teuer werden. ■

Kontakt

Tüv Süd AG
München
Te.l: +49 89 5791 0
info@tuev-sued.de
www.tuev-sued.de

CYBER SECURITY

Keine Entspannung

Kriminelle Wertschöpfungsketten: Zum Stand der Cyberbedrohung der deutschen Wirtschaft

© oz - stock.adobe.com

Beim Thema Cybersecurity fangen die deutschen Unternehmen nicht von Null an: Sie haben kräftig investiert in IT-Sicherheit – in Technik, Prozesse und Personal. Das hat den Schutz vor Cyberkriminalität zwar verbessert – andererseits steigt die Zahl der erfolgreichen Hackerangriffe. „Das Bewusstsein ist mittlerweile vorhanden, bei der konsequenten Umsetzung von Abwehrmaßnahmen besteht noch Handlungsbedarf, aber auch der Staat muss nachlegen", sagt ASW-Vorstandsvorsitzender Volker Wagner im Gespräch mit GIT SICHERHEIT.

GIT SICHERHEIT: Herr Wagner, als wir uns vor rund vier Jahren hier in der GIT SICHERHEIT über die aktuelle Gefährdungslage der deutschen Wirtschaft unterhielten, diagnostizierten Sie sehr klar eine Zunahme der Cyber-Bedrohung. Angriff und Abwehr beschrieben jeweils ansteigende Kurven, wobei aber die Angriffskurve steiler sei… Würden Sie das heute wieder so formulieren?

Volker Wagner: Ich würde gerne etwas anderes sagen, aber leider ist die Situation nicht besser geworden. Bei der Cybersicherheit erlebe ich nach wie vor, dass die Schere weiter auseinandergeht. Beispielsweise zeigt eine aktuelle Studie des Bitkom auf, dass 2019 drei von vier deutschen Unternehmen Opfer von Sabotage, Datendiebstahl oder Spionage waren. Ende September hat das BKA das aktuelle Lagebild zum Cybercrime veröffentlicht und die Fakten sprechen auch hier eine eindeutige Sprache. 2019 wurde eine Zunahme von Cybercrime um 15 % auf über hunderttausend Fälle registriert. Zudem gab es im letzten Jahr ca. 114 Mio. neue Malware-Varianten. Das BKA zieht dabei u. a. folgendes Fazit: Die Professionalität von Cyberkriminellen steigt weiter an. Cybercrime erschafft und basiert auf kriminellen Wertschöpfungsketten. Ransomware und DDoS-Angriffe sind die größten Bedrohungen. Von einer Entspannung der Situation können wir daher nicht sprechen.

Ist denn das Bewusstsein für diese Problematik in den Unternehmen aus Ihrer Sicht spürbar stärker ausgeprägt – und zieht man die richtigen Schlüsse daraus?

Volker Wagner: Es ist wahnsinnig viel gemacht worden, darauf kann man auch stolz sein. Die großen Unternehmen haben alle ihre IT-Sicherheitsabteilungen ausgebaut und

sachkundiges Personal eingestellt, Prozesse etabliert und neue Technik eingesetzt. Da ist wirklich viel Geld investiert worden. Und der Schutz ist auch deutlich besser als noch vor fünf oder zehn Jahren. Aber die Bedrohungslage hat sich im gleichen Zeitraum extrem verschärft. Mittlerweile sind fast unglaubliche eine Milliarde Varianten von Schadprogrammen im Umlauf. Gleichzeitig stellen wir im Rahmen der Digitalisierung von Wirtschaft und Gesellschaft immer mehr Geräte ins Internet. Je mehr Systeme miteinander vernetzt und ans Internet angeschlossen werden, desto mehr Angriffsfläche bietet sich. Es ist daher auch logische Konsequenz, dass die Anzahl von erfolgreichen Hackerangriffen steigt. Im gerade veröffentlichten Allianz Risk Barometer ist Cybercrime erstmals das am höchsten bewertete Risiko für die Wirtschaft. Das Bewusstsein ist also mittlerweile vorhanden, bei der konsequenten Umsetzung von Abwehrmaßnahmen besteht noch Handlungsbedarf.

Sie sehen sich beim ASW Bundesverband an der Schnittstelle von Staat und Wirtschaft – und gerade jüngst äußerten Sie sich sowohl lobend als auch kritisch bezüglich des geplanten IT-Sicherheitsgesetzes. Derzeit ist wohl der dritte Entwurf in Arbeit…?

Volker Wagner: Die ersten beiden Entwürfe haben wir von der ASW – wie auch einige andere Verbände – zum Anlass genommen, mit unseren Positionspapieren auf entscheidende Verbesserungspotenziale hinzuweisen. Wir erwarten nun den dritten Entwurf und damit den Start der Novelle des IT-Sicherheitsgesetzes noch in diesem Herbst. Nach meiner Kenntnis ist ein Kabinettsbeschluss noch für dieses Jahr vorgesehen und die Verabschiedung im Bundestag für Anfang nächsten Jahres geplant. Selbstverständlich werden wir uns im politischen Diskurs für die wichtigen Punkte aus Sicht der Wirtschaft einsetzen. Dabei möchte ich unterstreichen, dass wir die Novelle ausdrücklich befürworten. Uns geht es mit unseren Punkten darum, die Qualität und Praktikabilität zu erhöhen.

Sie sehen neben den Unternehmen selbst den Staat in der Pflicht, wenn es um „Cyberresilienz" geht. Überhaupt haben Sie ja zu dem Fragenkomplex der Aufgabenteilung zwischen Staat und Wirtschaft bei der Bekämpfung von Cyberkriminalität vor einiger Zeit sogar ein Positionspapier vorgelegt. Was kann denn, in groben Zügen formuliert, der Staat realistischerweise mehr leisten als bisher?

Volker Wagner: Hier sehen wir schon noch deutliches Verbesserungspotenzial. Beispielsweise bedarf es einer Meldepflicht für kritische Schwachstellen in Software und eine Verpflichtung für Software-Updates sowie Haftung bei Nicht-Behebung. Derzeit gibt es keine Haftung für fehlerhafte Software. Es sollte jedoch ein Haftungsanspruch entstehen, wenn bekannte Schwachstellen und Fehler nicht behoben werden.

Es sollte eine Novelle des Produkthaftungsrechts erfolgen, durch die Soft- und Hardwarehersteller gesetzlich verpflichtet werden, für sicherheitskritische Schwachstellen tatsächlich auch zeitnah Sicherheits-Updates bereitzustellen und bei Unterlassung in Haftung genommen werden können. Ebenso müssen Hersteller verpflichtet werden, Transparenz über den jeweiligen Lebenszyklus von softwarebasierten Produkten zu schaffen. Produkte, deren bekannte Schwachstellen nicht vom Hersteller bereinigt wurden, müssen kenntlich gemacht werden. Ebenso sind Verfahren zu definieren, wie mit Software, die ihren End-of-life-Zeitpunkt erreicht hat, umzugehen ist. Veraltete Software, die nicht mehr unterstützt wird, bietet eine große Angriffsfläche. Die Haftung könnte nach diesem Leitgedanken geregelt werden: Hersteller und Betreiber haften für unterlassene Software-Updates, Verbraucher haften für nicht eingespielte Patches, Restrisiken werden über Risikogemeinschaften in Cyberversicherungen abgedeckt.

Darüber hinaus muss sich die Bundesregierung im Rahmen der Cyberaußenpolitik dafür einsetzen, dass jeder Staat seine Bemühungen zur Erhöhung der Cybersicherheit intensiviert und kritische IT-Infrastrukturen besser gegen Attacken geschützt werden sowie intensiv gegen Cyberkriminalität vorgegangen wird. Mittelfristiges Ziel muss die Verabschiedung eines verbindlichen Abkommens für verantwortliches Handeln im Cyberraum sein.

In der Praxis bleibt für einzelne Unternehmen oft unklar, welche Sicherheitsbehörde mit welchen Kompetenzen ausgestattet ist und wie die Aufgaben zwischen Bundes- und Landesämtern abgegrenzt sind. Im konkreten Angriffsfall wird es gerade für kleine und mittelständische Unternehmen zunehmend von Bedeutung sein, dass auch die örtliche Polizeibehörde im Sinne eines Ersthelfers in die Lage versetzt wird, die richtigen Stellen in eine Strafverfolgung einzubeziehen.

Sie wünschen sich bei staatlichem Handeln im Rahmen des künftigen IT-Sicherheitsgesetzes mehr Transparenz für die jeweils betroffenen Unternehmen. Was genau stellen Sie sich vor?

Volker Wagner: Besorgniserregend ist, dass trotz Einführung des ersten IT-SiGe 2015 die

> **Die Bundesregierung muss sich im Rahmen der Cyberaußenpolitik dafür einsetzen, dass jeder Staat seine Bemühungen zur Erhöhung der Cybersicherheit intensiviert und kritische IT-Infrastrukturen besser gegen Attacken geschützt werden."**

Volker Wagner ist Head of Security bei der BASF Group sowie Vorstandsvorsitzender des ASW Bundesverbands (Allianz für Sicherheit in der Wirtschaft)

Bitte umblättern ▶


© xiaoliangge - stock.adobe.com

Bedrohungslage weiter gestiegen ist. Deswegen ist es umso wichtiger, dass bei der Novellierung auf den Erfahrungen der letzten vier Jahre aufgebaut wird. Wir fordern weiterhin den Austausch über eindeutige quantitative und qualitative Schwellenwerte zu Meldepflichten. Vorteilhaft wäre es hier, nicht nach Trial and Error vorzugehen, sondern dazu aus den bisherigen praktischen Erfahrungen zu den Meldungen aus den aktuellen Kritis-Sektoren zu lernen.

Der in der Novelle des IT-Sicherheitsgesetzes eingeführte Begriff „Unternehmen im besonderen öffentlichen Interesse" führt nicht zu Klarheit, sondern zu Rechtsunsicherheit bei den möglicherweise betroffenen Unternehmen. Die Einführung des Terminus „Unternehmen im besonderen öffentlichen Interesse" ist zu unbestimmt. Insbesondere fehlt eine Benennung konkreter Kriterien, warum eine Infrastruktur und deren Anlagen als „im besonderen öffentlichen Interesse" eingestuft werden.

Behörden sollen, Ihrer Auffassung nach, möglichst privates Know-how und Mitwirken ins Boot holen – zum Beispiel in Form von Public-Private-Partnerships. Haben Sie hier bestimmte Vorbildprojekte im Auge, vielleicht auch aus anderen Ländern?

Volker Wagner: Im Angriffsfall bedarf es einer konkreten Hilfestellung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es sollte daher über ein Rahmenwerk zur Ergänzung bzw. Erweiterung der mobilen Eingreiftruppen durch Public-Private-Partnerships nachgedacht werden. Dazu gehört auch die Einbindung der Wirtschaft in das Nationale Cyber-Abwehrzentrum und ein Konzept zum gemeinsamen Incident Response von Staat und Wirtschaft. Als Beispiel kann die US National Cyber-Forensics & Training Alliance genannt werden, wo staatliche und privatwirtschaftliche Akteure gemeinsam erfolgreich an der Aufklärung von Cyberattacken und an der Analyse von Tatwerkzeugen arbeiten.

Wie genau könnte so eine Public-Private-Partnership aussehen – und wer genau könnten dabei die Protagonisten sein?

Volker Wagner: Unter den vorgenannten Gesichtspunkten ist es erforderlich, dass das Cyber-Threat-Intelligence-System überdacht wird. Aus dem derzeitigen Gesetzestext geht nicht hervor, dass das BSI dazu verpflichtet sein wird, Cyber Threat Intelligence in Echtzeit auszutauschen. Es muss das Ziel sein, diese Informationen möglichst vielen Unternehmen, nicht nur den Kritis-Betreibern oder Betreibern von Infrastruktur im besonderen öffentlichen Interesse, zukommen zu lassen. Aus diesem Grunde fordert die ASW, eine solche Plattform da anzusiedeln, wo die Ressourcen und das Know-how über Einrichtung und Betrieb von Cyber-Threat-Intelligence-Plattformen besteht. Diese Aufgabe können die zahlreich in Deutschland vorhanden und international angesehenen Cybersicherheitsunternehmen übernehmen.

Welche konkreten hoheitlichen Aufgaben könnten aus Ihrer Sicht durch private Stellen – also beliehene Experten – übernommen werden? Es geht ja immerhin um Attacken aus dem Ausland – ist die Lage hier nicht eine andere, als bei Notar, TÜV & Co. oder bei Sicherheitskontrollen am Flughafen, um ein vielleicht passenderes Beispiel zu nennen?

Volker Wagner: Erforderlich hierfür wäre eine klare Regelung, welche Rolle diese Cybersicherheitsunternehmen als Betreiber der Plattformen einnehmen sollen. Ihre Aufgaben und Befugnisse müssen klar festgelegt werden. Insofern ist die Schaffung einer gesetzlichen Regelung erforderlich, die nachfolgende Aspekte zum Gegenstand haben soll: Erstens: Der Rechtscharakter der Einbindung der Cybersicherheitsunternehmen kann als Beliehenenschaft ausgestaltet sein. Zweitens: Erforderlich ist dann eine Registrierung von Unternehmen, die vom Informationsfluss (z. B. Warnung vor Sicherheitslücken) durch die Plattform profitieren wollen. Drittens: Dem BSI kommt die Rolle der Aufsichtsbehörde zu, worüber Kontroll- und Steuerungsrechte des Staates gewahrt werden.

Herr Wagner, lassen Sie uns noch zum derzeit alles beherrschenden Thema kommen – dem Virus und seinen Folgen. Welche Auswirkungen hatte dies auf die Sicherheitsverantwortlichen in der Wirtschaft?

Volker Wagner: Die letzte Zeit war außergewöhnlich. Die globale Pandemie hat unsere komplette Welt auf den Kopf gestellt. In diesen Wochen und Monaten wurde von unseren Sicherheitsverantwortlichen vieles abverlangt. Vor allem mussten die eigenen Mitarbeiter, Kunden und Geschäftspartner geschützt werden. Dabei galt es, wo möglich, die Produktions- und Dienstleistungsprozesse – häufig unter sehr schwierigen Bedingungen – aufrecht zu erhalten. Dies galt insbesondere für die Unternehmen in den sogenannten systemrelevanten Sektoren oder bei den kritischen Infrastrukturen. Dabei waren viele Aspekte zu beachten und die Sicherheitsverantwortlichen unterstützten die Krisenbewältigung – angefangen bei der Einrichtung eines Notfall- und Krisenstabs, über Verhaltensregeln für das Werks- bzw. Firmengelände oder das Büro und Regulierungen von Geschäftsreisen, bis hin zu Vorschriften für die Parteien der Lieferkette.

Welche Folgerungen ziehen Sie verbandsseitig generell aus den Erfahrungen mit dieser Pandemie?

Volker Wagner: Mit den nun seit Mitte Mai geltenden Lockerungen werden wir mit der Idee einer „neuen Normalität" vertraut gemacht. Das Virus ist hier, um zu bleiben, bis wir einen Impfstoff entwickeln. Also müssen wir einen Weg finden, damit zu leben. Wir haben mittlerweile ein viel besseres Verständnis für die konkrete Bedrohung und sind auch besser in der Lage, die damit verbundenen Risiken einzuschätzen. Es ist nicht länger völlig unbekannt, sondern eher unsichtbar. Wir alle müssen lernen, mit diesem neuen Risiko umzugehen, und das wird für jeden von uns unterschiedlich sein. Für mich bedeutet die sogenannte neue Normalität ein Umdenken, was unser gewohntes Handeln betrifft. Dabei geht es um die Abkehr von festen Planungsprämissen – hin zu sich kontinuierlich verändernden Rahmenbedingungen.

Welche Entwicklungen lassen sich erkennen – nach einem Halbjahr des Lebens mit und in der Krise?

Volker Wagner: Für mich lassen sich durchaus einige starke Trends erkennen, die unseren neuen Handlungsrahmen maßgeblich

beeinflussen werden. Erstens: Auch wenn viele durch die wirtschaftlichen Folgen verlieren, gibt es doch auch Gewinner in dieser ungewissen Zeit. Starke Länder und etablierte Unternehmen haben höhere finanzielle Rücklagen und in der Regel auch robustere Notfall- und Krisenprävention. Sie werden zwar auch Einbußen hinnehmen müssen, aber dürften in ihrer Wettbewerbsposition relativ gestärkt aus dieser Krise hervorgehen.

Zweitens: Existierende politische Spannungen werden durch die Corona-Krise verstärkt. Handelskonflikte nehmen an Brisanz zu, beispielsweise der zwischen den USA und China. Aber auch der schwelende Konflikt in Europa zwischen dem reicheren Norden und dem ärmeren Süden erhitzt sich weiter. Dies zeigt sich innerhalb der EU anhand der Diskussionen zur Neuverschuldung für die wirtschaftlichen Hilfen zur Linderung der Corona-Krise. Zudem missbrauchen totalitäre Staaten Corona zur Ausdehnung von Überwachungsmaßnahmen. Drittens: Die zuvor in Teilen von Wirtschaft und Gesellschaft stockende Digitalisierung nahm rasant an Fahrt auf und überwand dank seiner ungeahnten Beschleunigung viele etablierte Hürden. In Zeiten von Social Distancing wurde digitale Kommunikation eine Notwendigkeit. Home-Office oder virtuelle Konferenzräume zogen in unseren Arbeitsalltag ein und sind nun feste Bestandteile, die bleiben werden. Geschäftsreisen und persönliche Kontakte wurden zu Ausnahmen. Diese Entwicklung wird sich nicht mehr komplett zurückdrehen.

Viertens: Die Führungsstärke ist in der Krise essenziell. Eine klare und konsequente Linie, die als Orientierung in ungewissen Zeiten dient, half allen Beteiligten, die Auswirkungen zu bewältigen. Der österreichische Bundeskanzler Kurz ist hierfür ein Paradebeispiel. Er verdeutlichte, wie wichtig es ist, einen klaren Kopf zu behalten und zeigte, dass ein Weitblick im Handeln unablässig ist. In anderen Ländern nahmen die Regierungschefs die Bedrohung zunächst nicht ernst oder veränderten mehrfach den Kurs. Die hohe Zahl von Erkrankten und viele Todesfälle waren dann die bittere Konsequenz.

Sie haben gerade den Finger auf etwas gelegt, was nicht sofort auffällt: Es geht um den Missbrauch des Themas durch totalitäre Staaten – und zwar die missbräuchliche Überwachung unter dem Deckmantel der Corona-Schutzmaßnahmen. Was genau haben Sie hier im Auge – und inwiefern ist unsere Wirtschaft davon bedroht oder betroffen?

Volker Wagner: Präventions- und Kontrollmaßnahmen werden von einzelnen Regierungen für politische Zwecke missbraucht. Kontrollen werden mehr und mehr ausgedehnt, um Oppositionskräfte zu überwachen. Dies zeigt sich in einigen Ländern an der weiteren Ausdehnung von Videoüberwachungssystemen bis hin zu Militäreinsätzen bei Demonstrationen im Inland. Ergänzt wird dies mit Einfuhrbeschränkungen sowie Einreiserestriktionen, womit auch der freie Handel von Gütern und Dienstleistungen betroffen ist. Bei allen Unsicherheiten scheint doch eines gewiss: Wir benötigen aktuell mehr denn je kompetente und leidenschaftliche Security Führungskräfte und Mitarbeiter, um unser aller Schutz zu gewährleisten. ■

Kontakt

ASW Bundesverband
Volker Wagner, Vorstandsvorsitzender
Allianz für Sicherheit in der Wirtschaft e.V.
Berlin
Tel.: 030 200 77 200
wagner@asw-bundesverband.de
www.asw-bundesverband.de

CYBER SECURITY

Noch einiges zu tun

Verband Teletrust: Zur Fortschreibung der „Cyber-Sicherheitsstrategie für Deutschland“

Die „Cyber-Sicherheitsstrategie für Deutschland 2016“ der Bundesregierung wird derzeit fortgeschrieben – bis Mitte 2021 soll die aktualisierte Cyber-Sicherheitsstrategie beschlossen werden. Bis dahin läuft ein Evaluierungsprozess in Form eines Fragebogens. Darin werden Stakeholder aus den Bereichen Wissenschaft, Wirtschaft, Staat und Zivilgesellschaft eingebunden – darunter auch der Bundesverband IT-Sicherheit (Teletrust), dessen Kommentierung wir im Folgenden ausschnittsweise wiedergeben.

Was hat sich bewährt?

Alle vier Handlungsfelder waren in der Vergangenheit und sind in der Zukunft im Prinzip wichtig: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung; Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft; Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur; Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik.

Dennoch müssen wir feststellen, dass der Level an Cyber-Sicherheit und die notwendige Robustheit unserer IT-Infrastrukturen noch nicht hoch genug ist. Die Handlungsfelder und deren Maßnahmen müssen mit deutlich mehr Energie bearbeitet werden. Ein Ziel zu definieren, reicht nicht aus, es muss auch mit konkreten, nachhaltigen Maßnahmen und einer geeigneten Struktur umgesetzt werden.

Aus diesem Grund sollte mit Hilfe einer sehr gut ausgestatteten Task Force eine geeignete Struktur aufgebaut werden, bei der mit allen Stakeholdern gemeinsam die Fortschreibung der Cyber-Sicherheitsstrategie durchgeführt und auch getragen wird. Durch die gemeinsame Verantwortung werden die notwendigen Maßnahmen auch konkreter, wirkungsvoller und nachhaltiger umgesetzt.

Technisch und rechtlich sind wir sehr weit. Es fehlt an der tatsächlichen Umsetzung. Die öffentliche Hand könnte hier viel bewirken, u. a. durch breite Nutzung des digitalen Personalausweises oder Technologien wir die Smartphone Bürger-ID bei behördlichen Angeboten im Netz (Bürgerportale).

Das ITSiG hat vieles bewegt und zum Positivem verbessert. Eine Ausweitung des Geltungsbereichs von ITSiG auf weitere Branchen, weitere Dienste und auch kleinere Betreiber (mehr in die Breite) ist mittelfristig nötig – evtl. unter Senkung der Anforderungen in weniger kritischen Bereichen.

Unternehmen in Deutschland schützen: Der Schutz der Unternehmen durch den Staat bzw. staatliche Organe ist wichtig – besser wäre es aber, die Unternehmen zu befähigen, sich selbst hinreichend zu schützen. Das Augenmerk muss dabei besonders auf KMU liegen, die mit dieser Aufgabe bisher noch meist überfordert sind.

Was hat sich erledigt?

Die Aktivitäten im Umfeld des „Bundestrojaners" durch die ZITiS im Handlungsfeld.

„Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur" sollten umgehend gestoppt werden, weil sie allen anderen Maßnahmen entgegenwirkt und damit die Cyber-Sicherheitsstrategie unglaubwürdig erscheinen lässt.

Was muss dazukommen?

Der Bundesverband IT-Sicherheit würde es begrüßen, wenn mehr Initiativen für die Verschlüsselung werthaltiger Daten von Unternehmen und zum Schutz der Privatsphäre umgesetzt würden, weil es für die fortschreitende Digitalisierung ein wichtiger und mit hohem Schutzpotenzial nutzbarer Sicherheitsmechanismus ist. Außerdem glauben wir, dass es dringend notwendig ist, eine vertrauenswürdige, digitale Cyber- Sicherheitsinfrastruktur aufzubauen, die z. B.: Extended Zertifikates für mehr Vertrauen von Webanwendungen einfach zur Verfügung stellt, eine Alternative zu „Let´s encrypt" (mit einer Identitätsüberprüfung) schafft und für eine einfache Verschlüsselung von E-Mail-Sicherheit, Chats, usw. sorgt. Teletrust würde es begrüßen, wenn die Initiative GAIA-X für die Schaffung von mehr Unabhängigkeit und höhere Cyber-Sicherheit und Datenschutz als gemeinsames Ziel definiert würde.

Weitere Ziele, die in der Cyber-Sicherheitsstrategie eine höhere Bedeutung erlangen sollten, sind die- Wiederansiedlung von IT-Produktion in Deutschland und Europa, um Versorgung zu sichern und Produkte mit hohen und höchsten Sicherheitsanforderungen unter kontrollierten Bedingungen herzustellen (wie GAIA-X).

Wünschenswert ist außerdem ein starkes Bekenntnis zu Open Source durch Einsatz (auch und insbesondere in der öffentlichen Verwaltung) und Unterstützung der Open-Source-Entwicklungsprojekte. Außerdem wichtig ist die Durchsetzung von Komplexitätsreduktion (Komplexität ist der größte Feind der IT-Sicherheit). Ein stärkerer Fokus sollte auf Dezentralisierung von IT-Systemen und Verantwortung gelegt werden. Dies ist insbesondere relevant im Bereich Digitale Identität, Self-Sovereign Identity (SSI), etc.

Ergänzt werden sollte, dass nicht nur mit Providern und (KRITIS)-Anbietern zusammengearbeitet wird, sondern verstärkt mit den Herstellern und Lieferanten – das sowohl auf Hard- und Software-Ebene. Das ITSiG 2.0 schießt inhaltlich insoweit über die aktuelle Strategie hinaus. Die Rolle des BSI sollte überdies stärker als bisher in der neuen Strategie Berücksichtigung finden, da sich das ansonsten mit dem zunehmenden Befugnisausbau nicht rechtfertigen lässt.

Das Identitätsmanagement ist ein Schüsselfaktor in jeder sicheren IT-Infrastruktur. Generell ist eine stärkere Berücksichtigung von eID und den in der eIDAS-Verordnung genannten Vertrauensdiensten in Technologie- oder IT-Sicherheitsrelevanten (Gesetzes) Initiativen wünschenswert.

Beim Thema „Sichere elektronische Identitäten" ist aus unserer Sicht die mobile eID-Funktion zu ergänzen, die eine hochsichere, datensparsame und nutzerfreundliche Ergänzung zur Online-Ausweisfunktion des Personalausweises darstellt und ihn über ein mobiles Endgerät – allen voran dem Smartphone – nutzbar macht. Zur Stärkung der sicherheitstechnischen Souveränität und Schaffung innovativer, nutzerfreundlicher und sicherer digitaler Angebote ist es notwendig, dass Sicherheitsmechanismen wie bspw. das Secure Element im Smartphone für die Wirtschaft zugänglich sind und der Zugriff darauf durch die Smartphone- Anbieter nicht verhindert wird.

Zu ergänzen wäre ein neuer Punkt: „Verstärkung der Kooperation und Vernetzung mit europäischen Einrichtungen, insbesondere der ENISA", um auch das Thema „nationale Alleingänge" stärker zu adressieren. ■

Kontakt

Bundesverband IT Sicherheit e.V. (TeleTrusT)
Berlin
Tel.: +49 30 400 54 310
info@teletrust.de
www.teletrust.de

Mehr zum Thema auf den WIN>DAYS
Talk mit Genetec „Cybersecurity: Gefahrenpotenzial erkennen und Lösungsansätze finden“

CYBER SECURITY

Cyberversichert?

Warum eine Cyber-Haftpflichtversicherung im Ernstfall entscheidend sein kann

Ob System-Hacks, DDoS-Attacken oder die zunehmende Erpressung von Lösegeldern durch gesperrte Daten: Die Liste an Cyberbedrohungen wird von Jahr zu Jahr länger. Im Allianz Risk-Barometer 2020 belegten Cyberangriffe erstmals Platz eins in der Rubrik Geschäftsrisiken – noch vor Betriebsunterbrechungen.

Zwar wurden in den letzten Jahren weniger große Cybervorfälle bekannt, wie z.B. der Fall Yahoo aus 2017, bei dem die persönlichen Daten von rund 3 Milliarden Nutzern veröffentlicht wurden. Dennoch steigt die Zahl von Angriffen auf kleinere Unternehmen und Mittelständler stetig, so dass sich auch Regierungen genötigt sehen, Richtlinien und Standards wie die Datenschutzgrundverordnung (DSGVO) festzulegen und Organisationen zur Verantwortung zu ziehen.

Die meisten Unternehmen arbeiten mit Hochdruck daran, alle Vorgaben und Richtlinien zu verstehen und die internen Prozesse entsprechend anzupassen. Kommt es dann aber doch zu einem Zwischenfall, z.B. durch Cyberangriffe, kommen nicht selten empfindliche Geldstrafen auf sie zu.

Was man über Cyber-Haftpflichtversicherungen wissen sollten

Unternehmen sind heute gegen zahlreiche Arten von Zwischenfällen versichert. Zu den Standards gehören Versicherungen für Rechtsschutz, Gebäude, Transport, Vertrauensschaden oder höhere Gewalt. Da die Risiken durch Cyberangriffe aber immer größer werden, wandeln sich auch die von Versicherungen angebotenen Policen und Produkte. Zahlreiche Versicherungen bieten heute schon Haftpflichtversicherungen gegen Cybervorfälle an, um die durch Attacken teils immensen Kosten abzufangen. Die Allianz rechnet bei Cyberversicherungen bis 2025 mit einem Marktvolumen von rund 20 Milliarden US-Dollar.

Für diese steigende Nachfrage gibt es sehr gute Gründe. Cyber-Haftpflichtversicherungen ermöglichen es Unternehmen, im Ernstfall die finanziellen Mittel zu haben, um alle Prozesse am Laufen zu halten und entsprechend auf Angriffe reagieren zu können.

Systemintegratoren sollten ihren Kunden Cyber-Haftpflichtversicherungen aktiv anbieten. Das bedeutet nicht, dass man der angebotenen Lösung nicht traut und sich daher besser frühzeitig gegen mögliche Schwachstellen versichern sollte. Im Gegenteil: Security-Lösungen, die für eine solche Versicherungspolice in Frage kommen, müssen strenge Sicherheitsprotokolle befolgen und hohe Standards erfüllen. Bevor eine Police nämlich nach einem Zwischenfall ausgezahlt wird, muss der Integrator nachweisen, dass alle gängigen Maßnahmen von Beginn an umgesetzt wurden. Andernfalls könnte die Versicherung eine Auszahlung verweigern.

Übernahme des Risikos über die Versicherung hinaus

Da es sich bei Cyber-Haftpflichtversicherungen um ein noch recht neues Produkt handelt, tun sich viele Versicherer noch schwer, die Risiken richtig einzuschätzen und zu berechnen. In der Regel basiert die Kalkulation der Deckungssumme auf einem standardisierten Fragebogen über gängige IT-Richtlinien, die Organisationhierarchie, die Größe der vorhandenen IT-Infrastruktur und die Unternehmensform. In vielen Fällen neigen Versicherer dazu, die Haftungssumme zu überschätzen, was am Ende zu höheren Prämien führt.

Unternehmen sollten sich aber nicht nur auf eine Cyber-Haftpflichtversicherung verlassen. Denn wenn diese greift, ist es in der Regel schon zu spät. Vielmehr sollten die IT- und Sicherheitssysteme schon im Vorfeld den höchsten Cyber-Sicherheitsstandards entsprechen. Dazu gehören unterschiedliche Sicherheitsebenen wie eine End-to-End Datenverschlüsselung und sichere Authentifizierungs- und Autorisierungsmechanismen, die für einen höheren Datenschutz und eine ordnungsgemäße Installation von Endgeräten mit starken Passwörtern sorgen. Unternehmen sollten sich außerdem ihren Lösungsanbieter und Partner sorgfältig auswählen und

auf Systeme setzen, die effektiv vor Cyberrisiken schützen, schnell über neue Updates und Patches informieren, und somit unnötige Sicherheitslücken vermeiden. Darüber hinaus sollten die eigenen Mitarbeiter durch interne Richtlinien sensibilisiert werden.

Drei Tipps für die richtige Cyber-Haftpflichtversicherung

Wie die individuell zugeschnittene und passgenaue Cyber-Haftpflichtversicherung im stetig wachsenden Angebot der Versicherungen identifiziert werden kann, dabei helfen die nachfolgenden Tipps:

■ Die individuellen Cyberrisken kennen: Cybersicherheit kann viele unterschiedliche Facetten haben. Gleiches gilt auch für passende Haftpflichtversicherungen. Es ist daher besonders wichtig, sich über mögliche Cyberrisiken für das eigene Unternehmen im Klaren zu sein. Das kann eine ganze Reihe virtueller, aber auch realer Risiken beinhalten, wie Datenverlust oder Diebstahl von Unternehmenswerten. Erst wenn das Unternehmen genau weiß, wo die größten Gefahren liegen, kann es sich für eine Versicherung entscheiden, die den individuellen Bedürfnissen entspricht.

■ Wissen, was versichert ist: Eine Cyber-Haftpflichtversicherung kann durch zusätzliche Versicherungspolicen ergänzt werden. Es kann auch sinnvoll sein, unterschiedliche Versicherungen miteinander zu kombinieren, um im Ernstfall die bestmögliche Abdeckungssumme zu erhalten. Deshalb ist es von zentraler Bedeutung, die Bedingungen und Auszahlungsvoraussetzungen der einzelnen Policen genau zu kennen, falls ein Unternehmen für einen etwaigen Datenverstoß haftbar gemacht werden sollte. Darüber hinaus kann es mitunter schwierig sein, den aus Cyberangriffen entstandenen Schaden finanziell zu beziffern. Daher ist es sehr wichtig, mögliche Risiken in ein Finanzmodell umzuwandeln. Auch wenn die Cybersicherheit ein Geschäftsrisiko bleibt, sollten sicherheitsrelevante Aspekte von einem Experten für Cybersicherheit untersucht werden. Optimalerweise kennt sich dieser gleichermaßen im wirtschaftlichen Kontext aus und kennt die Risiken für Cybersicherheit.

■ Was passiert nach dem Ernstfall: Neben der Höhe der Abdeckungssumme sollten Unternehmen auch wissen, wie der Schadensersatzprozess vonstattengeht. Denn jeder Versicherer hat eigene Verfahren, um die Authentizität des Anspruchs zu prüfen, und einen eigenen zeitlichen Rahmen, in dem die Summe ausgezahlt wird. Unternehmen sollten sich daher frühzeitig darüber informieren, wie schnell sie im Schadensfall mit der Versicherungssumme und anderen Hilfsleistungen rechnen können. Einige Versicherungen bieten neben finanzieller Entschädigung nämlich auch die Vermittlung von Cyber-Ermittlern und Kommunikationsagenturen an, die nach einem Cyberangriff unterstützen und in der Krise so eine große Entlastung sein können. ■

Autor
Kay Ohse
Country Manager DACH und ECE bei Genetec

Kontakt

Genetec Deutschland
Frankfurt
Tel.: +49 69 506028 255
www.genetec.com/de

Partner unterstützen digitale Dialogplattform

Ein umfangreiches Anbieter- und Lösungsverzeichnis, interaktive Dialogformate und Neues aus der Welt der Cybersicherheit bietet It-sa 365. Die seit dem 6. Oktober ganzjährig verfügbare IT-Sicherheitsplattform knüpfe ein Band zwischen den Messeterminen, so Frank Venjakob, Executive Director It-sa. Die dann unter itsa365.de erreichbare Plattform ist für registrierte Teilnehmer an 365 Tagen im Jahr frei zugänglich. Anbieter können aus verschiedenen Beteiligungsmöglichkeiten wählen. Wie mit der It-sa Expo & Conference spreche man die richtigen Zielgruppen an und biete Anbietern professioneller IT-Sicherheitslösungen damit ein zusätzliches Instrument für den Marketing-Mix an, so Venjakob. Unterstützt wird das Konzept von Partnern. Allen voran engagieren sich das Bundesamt für Sicherheit in der Informationstechnik und der Digitalverband Bitkom sowie der Bundesverband IT-Sicherheit Teletrust.

www.it-sa.de ■

BSI und EASA vereinbaren strategische Zusammenarbeit

Gemeinsames Ziel des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Agentur der Europäischen Union für Flugsicherheit (EASA, European Union Aviation Safety Agency) ist es, die Cybersicherheit in der internationalen Luftfahrt nachhaltig zu steigern. Dazu haben die beiden Aufsichtsbehörden eine strategische Zusammenarbeit vereinbart. Ein entsprechendes Abkommen (Memorandum of Cooperation, MoC) unterzeichneten BSI-Präsident Arne Schönbohm und EASA-Generaldirektor Patrick Ky. Fliegen werde gemeinhin als sicherste Art der Fortbewegung angesehen. Angesichts der auch in der Luftfahrt zunehmenden Digitalisierung und Vernetzung sei die Cybersicherheit ein wesentlicher Faktor dafür, dass dies weiterhin so bleibt, so BSI-Präsident Arne Schönbohm. In der Luftfahrt könne nur dann erfolgreich digital durchgestartet werden, wenn die Informationssicherheit von Anfang an mitfliegt.

www.bsi.bund.de ■

GESUNDHEITSWESEN

Attacken aufs Gesundheitssystem

Cyber-Angriff auf Uniklinik Düsseldorf zeigt Dringlichkeit des Themas

Der IT-Sicherheitsvorfall im Universitätsklinikum Düsseldorf (UKD) im September beschäftigt Behörden und Öffentlichkeit. Die Täter hatten ein Erpresserschreiben hinterlassen und es wird wegen eines Todesfalls als Folge des Angriffs ermittelt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützte das Klinikum vor Ort mit einem mobilem Einsatzteam. Auch nach Einschätzung des Softwareunternehmens Kaspersky zeigt der Vorfall, wie real die Gefahr für das Gesundheitssystem ist.

Nach dem Ausfall der IT-Systeme am 10. September war die Uniklinik Düsseldorf insgesamt dreizehn Tage von der Versorgung abgemeldet. Am 23.9. hat es sich wieder für die Notfallversorgung im Großraum Düsseldorf angemeldet. Damit konnte der Rettungsdienst die Zentrale Notaufnahme (ZNA) des UKD wieder anfahren.

Bekannte Schwachstelle

Der Cyber-Angriff wurde durch eine Schwachstelle in VPN-Produkten der Firma Citrix ermöglicht: Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) ist sie seit Dezember 2019 bekannt. Dem Amt würden zunehmend Vorfälle bekannt, bei denen Citrix-Systeme bereits vor der Installation der im Januar 2020 bereitgestellten Sicherheitsupdates kompromittiert wurden. Dadurch hätten Angreifer auch nach Schließung

der Sicherheitslücke weiterhin Zugriff auf das System und dahinterliegende Netzwerke. Diese Möglichkeit werde aktuell vermehrt ausgenutzt, um Angriffe auf betroffene Organisationen durchzuführen.

„Angreifer verschaffen sich Zugang zu den internen Netzen

und Systemen und können diese auch Monate später noch lahmlegen", so BSI-Präsident Arne Schönbohm: „Ich kann nur mit Nachdruck appellieren, solche Warnungen nicht zu ignorieren oder aufzuschieben, sondern sofort entsprechende Maßnahmen zu ergreifen. Der Vorfall zeigt zum wiederholten Male, wie ernst man diese Gefahr nehmen muss. Auch deswegen hat die Bundesregierung im Entwurf des Krankenhaus-Zukunftsgesetzes vorgesehen, dass mindestens 15 Prozent der beantragten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit eingesetzt werden müssen".

Einfallstor in interne Netze

Die seit Januar 2020 bekannte Schwachstelle in den VPN-Produkten von Citrix stellt je nach lokaler Netzkonfiguration ein mögliches Einfallstor in interne Netze dar, so das BSI. Entsprechende Sicherheitsupdates stehen bereits seit Januar 2020 zur Verfügung und sollten, falls noch nicht geschehen, dringend eingespielt werden. Von der Ausnutzung betroffen können jedoch auch Systeme sein, die im Januar 2020 gepatcht wurden. Diese wurden unter Umständen bereits vor der Installation der Citrix-Sicherheitsupdates kompromittiert und können somit Angreifern auch jetzt noch den Zugriff auf interne Netze und weitergehende Aktivitäten erlauben, wie etwa die Ausleitung oder Verschlüsselung sensibler Daten oder die Manipulation bzw. Stilllegung von Systemen, Geschäftsprozessen und Betriebsabläufen.

Anwender der Produkte Citrix Gateway (ehemals Netscaler Gateway) und Citrix Application Delivery Controller sollten ihre Netzinfrastruktur und Systeme auf mögliche Anomalien hin überprüfen und ihre Schutzmaßnahmen zwingend anpassen, betont das BSI.

Gefahr für das Gesundheitssystem

Auch nach Einschätzung des Softwareunternehmens Kaspersky zeigt der Vorfall, wie real die Gefahr für das Gesundheitssystem sei. Ransomware, so das Unternehmen, gehörten „in jüngster Zeit zu den häufigsten Angriffsformen auf das Gesundheitswesen". In Krankenhäusern seien kritische Daten gespeichert - somit sei für Hacker die Verschlüsselung dieser Daten mit anschließender Lösegeldforderung erfolgversprechend. Während der Covid-19-Pandemie habe aber auch die Zahl der Phishing-Betrügereien zugenommen, die die gesamte medizinische Lieferkette betrafen. So habe es Fake-Verkäufe von Schutzausrüstung und Angriffe auf Hersteller von Beatmungsgeräten und Prüflabors gegeben.

Die Sicherheitsexperten von Kaspersky verzeichneten in den ersten Wochen der Pandemie einen Anstieg von Phishing, bösartigen Websites und Malware um 30.000 Prozent. Laut Kaspersky-Daten gab es in der ersten Märzwoche dieses Jahres außerdem einen Anstieg auf eine Million Cyberangriffe pro Tag mit Covid-19-Bezug.

Eugene Kaspersky, Gründer und CEO von Kaspersky, bewertet Angriffe auf Gesundheitsorganisationen als terroristischen Akt: „Cyberkriminelle sind es gewohnt, von zu Hause aus zu arbeiten und von dort aus Unternehmen und Einzelpersonen anzugreifen; ihre Umstände haben sich nicht drastisch geändert. Unsere Aufgabe ist es, weiterhin intensiv daran zu arbeiten, unsere Kunden zu schützen. Jeder Angriff auf ein Krankenhaus zu diesem Zeitpunkt kann als gleichbedeutend mit einem Terroranschlag eingestuft werden." ■

CLOUD SECURITY

Deal geplatzt

Cloud-Daten rechtssicher speichern – nach Scheitern des Privacy-Shield-Datenschutzabkommens mit den USA

Rechtssichere Grundlagen für Cloud-Dienste: Unternehmen müssen aktiv werden

Am 16. Juli hat der Europäische Gerichtshof das EU-USA-Datenschutzabkommen „Privacy Shield" als ungültig erklärt. Unternehmen brauchen jetzt dringend eine rechtssichere Grundlage für die Nutzung ihrer Cloud- und Collaboration-Dienste. Das IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity rät dazu, selber aktiv zu werden.

Die EU hatte das Privacy-Shield-Abkommen 2016 mit den USA ausgehandelt, um europäische Daten, die in die USA übertragen werden, vor dem Zugriff Dritter abzusichern. Der Europäische Gerichtshof hat diese Datenschutzvereinbarung am 16. Juli für ungültig erklärt. Als Grund gab der EuGH die zu großen Unterschiede zwischen dem Datenschutzniveau der EU-Mitglieder und dem der USA an. Bei Datentransfers in die USA können europäische Unternehmen sich nun nicht mehr auf die Angemessenheit des Datenschutzniveaus gem. Art. 45 EU-DSGVO berufen. Das Urteil wurde sofort wirksam.

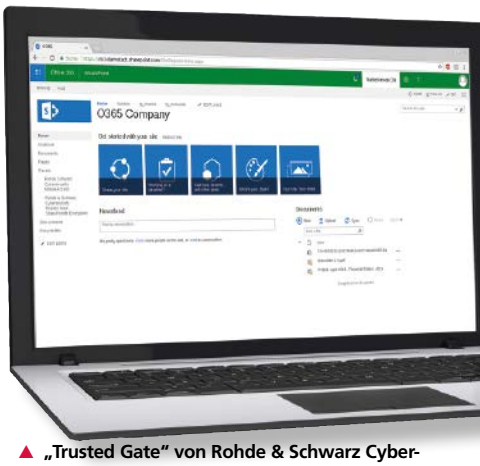
Was der Europäische Gerichtshof jetzt untermauert hat, wurde von Anfang an von Datenschützern kritisiert: Der „Privacy Shield" lässt dem US-Recht Vorrang. Der „Clarifying Lawful Overseas Use of Data Act", besser bekannt als Cloud Act, verpflichtet US-amerikanische Cloud-Provider, den US-Behörden Zugriff auch auf nicht in den USA gespeicherte Daten zu gewähren – und unterläuft damit die EU-DSGVO. Nachdem im Januar 2017 die Behörden in den USA per Dekret aufgefordert wurden, den Datenschutz für Ausländer vollends aufzuheben, war es nur noch eine Frage der Zeit, bis der „Privacy Shield" kippt.

Zukunftsfähige Geschäftsmodelle

Mit dem Ende des „Privacy Shield" geht das Ringen um den Schutz personenbezogener Daten, die aus der EU in die USA übermittelt werden, in eine neue Runde. Leidtragende sind die europäischen Unternehmen. Sie brauchen schnell eine rechtssichere Lösung. Denn für sie werden cloud-basierte Anwendungen immer wichtiger, um zukunftsfähige Geschäftsmodelle umzusetzen. Hinzu kommt: Die marktführenden Cloud-Plattformanbieter sind überwiegend US-amerikanische Unternehmen, und treiben „Cloud-only"-Lösungen mit Nachdruck voran. Immer mehr Daten aus europäischen Unternehmen liegen längst in Rechenzentren amerikanischer Konzerne – und sind dort nicht sicher vor dem Zugriff Dritter.

Auch der Bundesverband der Deutschen Industrie schlägt Alarm. Präsident Dieter Kempf fordert: Europäische Unternehmen brauchen dringend Rechtssicherheit im globalen Daten- und Wirtschaftsverkehr.

Das Problem: Auch die Nutzung der Standardvertragsklauseln, die den



▲ „Trusted Gate" von Rohde & Schwarz Cybersecurity lässt sich in gängige Public Clouds einbinden

Datentransfer in Drittländer regeln, ist durch das Urteil vom 16. Juli ins Wanken gekommen. Zwar hat der EuGH an diesen nichts zu beanstanden. Doch werden die Aufsichtsbehörden dazu verpflichtet, die Übermittlung von Daten auszusetzen oder zu verbieten, sofern die vertraglich festgehaltenen Standards in einem Drittland nicht eingehalten werden oder eingehalten werden können. Für europäische Unternehmen bedeutet dies, dass sie vor einem Datentransfer in jedes Drittland prüfen müssen, ob die Regelungen eingehalten werden. Insbesondere für kleine und mittlere Unternehmen ist der hohe Verwaltungsaufwand nur schwer zu stemmen. Die komplexen Beurteilungen gehen zudem mit einem hohen Risiko einher.

Deutsche Cloud-Standorte keine Lösung

Ausländische Cloud-Provider bieten ihren Kunden nun zunehmend die Möglichkeit, ihre Daten in Deutschland zu speichern. Aber auch solche deutschen und europäischen Cloud-Standorte sind keine Lösung. Denn auch dann können Cloud-Anbieter gezwungen werden, Zugriff auf die bei ihnen gespeicherten Daten zu gewähren.

Aber wie kann eine rechtssichere Lösung aussehen? Der „Privacy Shield" war bereits der zweite Versuch, eine solche zu schaffen. Auch der Vorgänger, die „Safe-Harbour-Entscheidung", war gescheitert. Beiden Vereinbarungen ist es nicht gelungen, amerikanische Unternehmen zu verpflichten, die Daten europäischer Bürger und Unternehmen besser zu schützen.

Die Erfahrung zeigt: US-Gesetze lassen sich nicht zugunsten europäischer Datenschutzvorschriften zähmen. Die Abkommen wurden zudem als machtpolitische Spielbälle missbraucht. Es besteht die Gefahr, dass auch eine neue Regelung Sicherheit vortäuscht, ohne sie garantieren zu können. Eine schnelle Lösung ist zudem aufgrund der Präsidentschaftswahlen in den USA aussichtslos.

Daten entkoppeln

Anstatt auf Vereinbarungen mit den USA zu hoffen, sollten Unternehmen auf innovative technische Lösungen setzen, die ihnen die Kontrolle über ihre Daten zurückgeben. Auf diese Weise legen sie eine nachhaltige Basis für ihre Digitalisierungsstrategie. Dazu müssen sensitive Daten von den Cloud-Diensten entkoppelt werden. Dann lassen sich diese an jedem beliebigen Ort speichern. US-Anbieter Microsoft hat diesen Weg bereits gemeinsam mit dem deutschen IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity eingeschlagen.

Während die Workflows von Microsoft Teams und Microsoft Sharepoint Online weiterhin für die Nutzer aktiv bleiben, werden die Daten mit Hilfe der Datensicherheitslösung für Cloud-Umgebungen aus den Prozessen herausgelöst. Durch die gewonnene Datensouveränität können europäische Unternehmen die EU-DSGVO weltweit ohne Rechtsunsicherheiten erfüllen. „R&S Trusted Gate" lässt sich nahtlos in gängige Public Clouds wie Microsoft Azure, Google, AWS und Collaboration-Tools wie Microsoft Office 365 und Sharepoint einbinden.

Mit Hilfe einer solchen datenzentrischen Lösung gewinnen Unternehmen nicht nur eine rechtssichere Grundlage für die Übertragung ihrer Daten in die USA. Sie machen sich unabhängig von Gesetzen und politischen Entscheidungen in jedem Drittland, in das sie Daten übermitteln. Insbesondere für global agierende Unternehmen spielt dieser Faktor eine große Rolle. Ein weiterer Vorteil einer solchen datenzentrischen Lösung: Die sensiblen Daten, die von den Clouddiensten entkoppelt werden, lassen sich besser vor Hackern schützen. Denn immer wieder kommt es zu schwerwiegenden Angriffen auf öffentliche Clouds. Wenn die Dateien auf dem Server des Unternehmens verbleiben, kann dieses selbstbestimmt für ein hohes Sicherheitsniveau sorgen. ■

Kontakt

Rohde & Schwarz Cybersecurity GmbH
Tel.: +49 30 65 884 222
cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

▲ **Schutz vor Cyberangriffen auf die Cloud**

CYBER SECURITY

Störfeuer auf Produktionsnetzwerke

Studie: „Cybersecurity-Niveau in der Operational Technology“

Eine von Baramundi in Auftrag gegebene Studie untersucht, wie deutsche Industrieunternehmen mit den Gefahren für ihre Produktionsumgebung umgehen

Wo stehen deutsche Industrieunternehmen bei der Absicherung ihrer Produktionsnetzwerke? Dieser Frage widmet sich eine neue Studie, die das Research- und Analystenhaus Techconsult mit Unterstützung des Augsburger Software-Spezialisten Baramundi Software durchgeführt hat. Die Untersuchung trägt den Titel „Cybersecurity-Niveau in der Operational Technology“ – dafür wurden 156 deutsche produzierende Unternehmen befragt.

Vor dem Hintergrund des digitalen Wandels hin zu einer zukunftsweisenden Industrie 4.0 sind Fertigungsunternehmen mit neuen Sicherheitsherausforderungen konfrontiert. Die zunehmende Vernetzung moderner Produktionsanlagen setzt den Schutz des Produktionsnetzwerks nach außen mittels „Air Gap“ außer Kraft: Laut der neuen Techconsult-Studie sind heute bereits in rund 84 Prozent der deutschen Industrieunternehmen sämtliche IT-Geräte im Produktionsumfeld miteinander verbunden. In nahezu all diesen Netzwerken (98 Prozent) besteht eine Verbindung nach außen – und die Quote von direkten Angriffen auf Produktionsinfrastrukturen steigt. Von den in der Studie befragten produzierenden Unternehmen verzeichneten in den letzten 12 Monaten fast 44 Prozent solche Angriffe. Die Dunkelziffer noch unentdeckter Angriffe könnte dabei noch weitaus höher liegen.

Für deutlich mehr als jedes zweite betroffene Unternehmen kam es dabei zu einer Produktionsstörung, und in jedem dritten Unternehmen wurde die Produktivität zumindest beeinträchtigt. Der Anteil der Unternehmen mittlerer Größe liegt in dieser Gruppe sogar bei 58 Prozent. 19 Prozent der attackierten Unternehmen mussten den direkten Ausfall ihrer Produktion infolge von Cyberangriffen in Kauf nehmen. Und bei mehr als jedem vierten betroffenen Unternehmen (26 Prozent) führten Hackerattacken auf ihre Produktionsinfrastruktur sogar zu schweren Reputationsschäden. Die mit solchen Angriffen einhergehenden Produktionsausfälle oder Betriebsunterbrechungen ziehen neben Mehrkosten in der Regel auch Lieferverzüge

und damit einen Vertrauensverlust bei Kunden und Partnern nach sich.

Auch Mittelständler im Fokus

Nach den Zahlen scheinen in der Mehrheit vor allem größere Unternehmen mit 1.000 und mehr Beschäftigten, die über komplexe und gewachsene Produktionsinfrastrukturen verfügen, von Cyberangriffen betroffen zu sein – ihr Anteil liegt hier bei über 65 Prozent. Allerdings ist ihr Risiko durch die höhere Anzahl von Mitarbeitern, die durch unachtsames Verhalten ein potenzielles Risiko für die Netzwerksicherheit darstellen können, auch größer. Vermutlich werden aber auch kleinere Unternehmen deutlich häufiger Opfer von Internetkriminellen, als sie selbst annehmen und angeben. Viele Attacken bleiben evtl. aufgrund unzureichender technischer Sicherheitsausstattung der Produktionsinfrastruktur unbemerkt. Unternehmen unter 1.000 Mitarbeitern erleiden Produktionsstörungen infolge von Cyberattacken deutlich häufiger als größere Unternehmen. Dies weist darauf hin, dass ein umfassendes Security-Konzept mit der dazugehörigen technischen Ausstattung auf hohem Niveau die Auswirkungen von Cyberattacken abschwächen kann.

Wie wird angegriffen?

Neben klassischem Phishing und gezielten Angriffen über ungepatchte Schwachstellen waren vor allem manipulierte Speichermedien die häufigste Waffe der Angreifer. Bei mehr als jedem zweiten erfassten Angriff der letzten zwölf Monate handelte es sich bei den befragten Studienteilnehmern um eine typische Phishing-Attacke. 45 Prozent der im Produktionsumfeld durch Malware ausgelösten Sicherheitsvorfälle zählten zu den sogenannten „Advanced Persistent Threats" (APT)-Angriffen, die mit 58 Prozent vor allem mittelgroße Unternehmen unter 1.000 Mitarbeitern betreffen. Fast jeder dritte Angriff auf Produktionsinfrastrukturen basiert auf manipulierten mobilen Datenspeichern – hier sind mit 33 Prozent vor allem kleinere und mittlere Unternehmen gefährdet. Direkten Hackerangriffen auf ihr Produktionsnetzwerk mit Zugang über Sicherheitslücken im IT- oder Produktionsnetzwerk waren kleinere und größere Unternehmen gleichermaßen ausgesetzt

Mangelnder Schutz der Produktionssysteme

Laut Studie verfügt nur jedes vierte Industrieunternehmen (24 Prozent) über ausreichende Security-Ressourcen, um eine vollständige Sicherheit ihrer Produktionsinfrastruktur zu gewährleisten. Schutzmaßnahmen müssen dabei nicht nur Schwachstellen des Netzwerks ausfindig machen, sondern auch ungewöhnliches Netzwerkverhalten erkennen und Bedrohungen abwenden. In rund einem Drittel der befragten Unternehmen findet eine derartige Netzwerküberwachung statt – allerdings zeigt sich auch hier, dass kleinere Unternehmen im Vergleich zu Großunternehmen technisch schlechter aufgestellt sind. Und lediglich 15 Prozent der Industrieunternehmen verfügen über ausreichendes Personal, um die IT-Security im Produktionsumfeld im vollen Umfang zu gewährleisten.

Sicherheitsstrategie muss zur industriellen Fertigung passen

Schutz vor Angriffen bietet beispielsweise die Segmentierung der Netzwerke und Betriebsfunktionen: Rund ein Viertel der Unternehmen verbesserte dadurch ihre Sicherheit erheblich. Lediglich 18 Prozent der Unternehmen setzen laut Studie produktionsspezifische Management- und Sicherheitstools ein. Eine Mehrheit nutzt dagegen Security-Lösungen der IT – diese IT-Lösungen kommen jedoch an ihre Grenzen, da die verschiedenen Systeme, Geräte und proprietären Netzwerk-Protokolle unterschiedliche Sicherheitsanforderungen stellen. Eine für die Produktionsumgebung zugeschnittene Sicherheitslösung muss vor allem Systeme, Anlagen und Geräte genau erfassen. Mittlerweile gibt es bereits Unified-Endpoint-Management (UEM)-Lösungen, die sich auch auf Operational-Technology-Endgeräte spezialisieren. Bisher nutzt aber laut Studie nur ein gutes Drittel der Unternehmen – und hier vor allem auch größere Unternehmen – technische Lösungen, die sämtliche produktionsnahen Endpunkte automatisiert scannen und erfassen, um mögliche Schwachstellen zu identifizieren, Patches einzuspielen oder Konfigurationsanpassungen vorzunehmen.

Ausblick

Industrieunternehmen müssen damit rechnen, dass ihre Produktionsanlagen jederzeit ins Visier von Hackern gelangen können. Neben geeigneten Maßnahmenplänen für mögliche Angriffe, ausreichenden technischen Ressourcen und qualifiziertem Personal kann auch eine Netzwerksegmentierung sowie der Einsatz von UEM-Lösungen zur automatisierten Erfassung und Inventarisierung aller im Produktionsumfeld eingesetzten Endpoints einen verbesserten Schutz ermöglichen. ■

Kontakt

Baramundi Software AG
Augsburg
Tel.: +49 821 567 08 0
info@baramundi.com
www.baramundi.com

SICHERE AUTOMATISIERUNG

Wenn IT und OT sich treffen

Anforderungen für Betreiber, Integratoren und Gerätehersteller an die OT-Security

Egal ob Hersteller oder Betreiber, Industrie oder kritische Infrastruktur: Das Thema Cyber-Security ist für alle Industriebereiche wichtig, denn die Automatisierungstechnik wächst immer stärker mit der IT-Welt zusammen. Anlagengrenzen lösen sich auf und auch der Austausch von Daten und Informationen erhöht sich kontinuierlich. Aufgrund dieser Vernetzung und Anbindung an das Internet sind die industriellen Automatisierungssysteme zunehmend Cyber-Angriffen ausgesetzt. Doch wie kann man sich davor effektiv schützen?

Mit dem im Juli 2015 verabschiedeten IT-Sicherheitsgesetz werden die Betreiber kritischer Infrastrukturen dazu verpflichtet, die für die Erbringung ihrer wesentlichen Dienste erforderliche IT gemäß dem Stand der Technik abzusichern. Andere industrielle Bereiche handhaben das Thema Security unterschiedlich. Produktionsanlagen und Fernzugriff sind hier oftmals kaum geschützt. Das liegt meist nicht am fehlenden Bewusstsein, dass etwas getan werden sollte, sondern es mangelt am benötigten Wissen sowie einem Leitfaden, wie vorzugehen ist. In diesem Zusammenhang treten folgende Fragen auf:

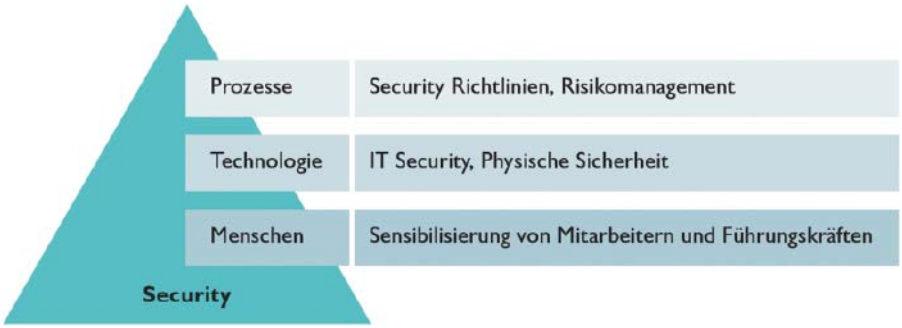
- Was ist notwendig?
- Wie sollte der Sachverhalt angegangen werden?
- Wo lässt sich Unterstützung anfordern?
- Welchen Standards sollte entsprochen werden?

Unterschiedliche Herausforderungen in IT und OT

Industrial Security muss ein ganzheitlicher Ansatz sein, der in den Köpfen des Managements sowie

der Mitarbeiter beginnt. Neben technischen Maßnahmen, wie dem Einsatz von Industrial Security-Produkten (Technologie), dürfen organisatorische Maßnahmen in Form eines Security-Managements (Prozesse) nicht vernachlässigt werden. Eine sichere IT bildet die Grundlage für die Security im Unternehmen, die Kundendaten, Entwicklung und Fertigung, aber reicht das aus?

Im Vergleich zur IT (Information Technology)-Security ist die OT (Operational Technology)-Security, auch Industrial Control Systems (ICS)-Security genannt, bei identischen Themen mit anderen Herausforderungen konfrontiert. Um die Zugriffssicherheit in der OT komplett zu bedienen, sind die von der IT definierten Maßnahmen durch zusätzliche relevante Aktivitäten zu erweitern. Die Norm IEC 62443 beschreibt die Anforderungen für Betreiber, Integratoren und Geräteheresteller zur Umsetzung der Security in der OT. Das Design einer Automatisierungslösung muss daher ergänzend zur eigentlichen Automatisierungsaufgabe auch Security berücksichtigen, wobei die Teile 2-4 und 3-3 der IEC 62443 zu beachten sind.



Security als ganzheitlicher Ansatz

Genaue Erfassung aller Anlageninformationen

Die Konzeption einer Automatisierungslösung unter Security-Aspekten geschieht generell in enger Zusammenarbeit zwischen dem Integrator/Dienstleister und dem Betreiber. Zunächst werden alle Anlageninformationen hinsichtlich der Umgebung (freie Fläche, Gebäude etc.), der Struktur (Netzwerk, Auflistung der Komponenten und deren Installationsort etc.) und des Prozesses (Abläufe, Kommunikationsbeziehungen, schützenswerte Daten etc.) erfasst. Das betrifft sowohl neue ebenso wie bestehende Anlagen. Daran schließen sich folgende Schritte an:

Security-Spezifikation

Auf der Bestandsaufnahme aufbauend erfolgt die Security-Spezifikation für die Anlage. Sie beinhaltet das Netzwerkkonzept sowie eine Asset-Liste sämtlicher vernetzter Geräte und definiert bereits Härtungsmaßnahmen. Für die zukünftige Zugriffssicherheit ist es ein Muss, dass die Realisierung aller bereits zu diesem und zu späteren Zeitpunkten veranschlagten Security-Maßnahmen bei der Übergabe der Anlage verifiziert werden. Deshalb entsteht schon bei der Security-Spezifikation die Testspezifikation, die später die Maßgabe bei der Anlagenabnahme bildet.

Schutzbedarfsanalyse

Im nächsten Schritt erfolgt eine Schutzbedarfsanalyse. Dabei werden die schutzbedürftigen Assets, Daten und Kommunikationswege ermittelt und dokumentiert. Diese Analyse geschieht auf der Grundlage von drei Schutzzielen: Verfügbarkeit, Integrität und Vertraulichkeit. Damit einhergehend findet eine Festlegung der zu schützenden Zonen und Conduits (Verbindungskanäle) in der Anlage statt. Am Ende liegt eine Schutzbedarfsfeststellung für die Automatisierungslösung vor, die für die eingesetzte Informationstechnik ausreichend und angemessen ist.

Bedrohungsanalyse

Hierauf aufbauend erfolgt eine Bedrohungsanalyse. Sie gründet sich beispielsweise auf den Top-10-Bedrohungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und wird gegebenenfalls durch betreiberspezifische Themen erweitert. Gemeinsam mit dem Betreiber werden die Gefährdungen hinsichtlich der Relevanz für die Automatisierungslösung bewertet und schriftlich festgehalten. Der Bedrohungsanalyse liegen ebenfalls die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit zugrunde.

Risikoanalyse

Im Anschluss daran wird auf Basis der festgestellten Bedrohungen eine Risikoanalyse vorgenommen. Das Risiko bemisst sich an den möglichen Schäden und der daran geknüpften Eintrittswahrscheinlichkeit für ein solches Szenario.

- Für Risiken, die für das Unternehmen nicht akzeptabel sind, werden Maßnahmen erarbeitet und die Auswirkung auf die Bewertung geprüft.
- Sofern sich das Risiko auf ein akzeptables Niveau mindern lässt, sollten die Maßnahmen unter Beachtung der Wirtschaftlichkeit realisiert werden.

Im Ergebnis erhält der Betreiber eine Handlungsempfehlung für ein ganzheitliches, individuelles und produktneutrales Sicherheitskonzept, das auf die speziellen Anforderungen seines Unternehmens abgestimmt ist.

Prozess zum Design einer Security-Automatisierungslösung

Risikobehandlung

Im Rahmen der Risikobeurteilung wird entschieden, wie mit den verbleibenden Risiken umzugehen ist. Mögliche Risikobehandlungs-Optionen sind:

- Risiken lassen sich vermeiden, weil beispielsweise die Risikoursache ausgeschlossen wird.
- Eine Reduzierung des Risikos ist möglich, indem eine Modifizierung der Rahmenbedingungen stattfindet, die zur Risikoeinstufung beigetragen haben.
- Risiken werden durch ihre Teilung mit anderen Parteien transferiert.
- Der Betreiber akzeptiert die Risiken.

Durch eine regelmäßige Prüfung der Maßnahmenumsetzung sowie der Bedrohungslage erfolgt ein stetiges Risk Monitoring.

Risk Monitoring

Unternimmt das Unternehmens nichts zur Verminderung eines bestehenden Risikos, so wird dieses akzeptiert. Hier sollte das Management mit dem Ziel einbezogen werden, alle identifizierten, analysierten, bewerteten und priorisierten Risiken angemessen zu behandeln. Sich daraus ergebende zusätzliche Security-Maßnahmen fließen in die Security- und Testspezifikation ein. Generell gilt dabei:

- Sämtliche Prozessschritte müssen nach dem aktuellen Stand der Technik geschehen.
- Die Ergebnisse werden dokumentiert und
- der Betreiber zeichnet die Ergebnisse der Analysen ab.

Implementierung/Verifikation

Der Integrator/Anlagenlieferant führt die festgelegten Maßnahmen der Security-Spezifikation in der Anlage durch. Vor ihrer Übergabe an den Betreiber wird die Realisierung der Security-Maßnahmen anhand der Testspezifikation verifiziert und ist damit Bestandteil der Anlagenabnahme (Site Acceptance Test, SAT). In einem definierten Zeitraum – beispielsweise jährlich – muss überprüft werden, ob neue Bedrohungen oder Risiken vorhanden sind, die eine erneute Bewertung erfordern.

Zertifizierter Dienstleister zur Unterstützung

Zur Bearbeitung der beschriebenen Security-Maßnahmen empfiehlt es sich, dass der Betreiber einen geeigneten Dienstleister auswählt, mit dem er die Themen gemeinsam festlegt. Hierbei sollte es sich um ein Unternehmen handeln, welches gemäß IEC 62443-2-4 als Security-Dienstleister zertifiziert ist. So wird sichergestellt, dass das notwendige Wissen und die Prozesse vorliegen, um eine Automatisierungsanlage nach den Normenanforderungen zu designen.

ICS-Security	IT-Security
Prioritäten	
Verfügbarkeit Integrität Vertraulichkeit	**Vertraulichkeit** Integrität Verfügbarkeit
Eigenschaften	
Verfügbarkeit	
100 %	99 % ausreichend
Neustart	
Schwierig	Möglich
Patch Management	
Große Herausforderung	Automatisiert möglich
Lebenszeit Hardware	
7 - 20 Jahre	3 - 5 Jahre

ICS-Security versus IT-Security

Vielfältiges Leistungsangebot

Phoenix Contact wurde im April 2019 vom Tüv Süd als eines der ersten Unternehmen in Deutschland nach der Normenreihe für OT-Sicherheit IEC 62443-2-4 zertifiziert. Die Zertifizierung bestätigt, dass das Unternehmen gemeinsam mit seinen Kunden sichere Automatisierungslösungen entwickeln und realisieren kann. Folgende Security-Dienstleistungen werden angeboten:

- Erarbeitung von individuellen Lösungen und Konzepten für ausfallsichere Netzwerkstrukturen, zur Absicherung oder Fernwartung von Maschinen sowie für leistungsfähige Funknetzwerke auf der Grundlage der verschiedenen Branchenstandards
- Umsetzung der Security- und Netzwerkanforderungen hinsichtlich Konfiguration und Dokumentation, Einführung von Managementsystemen, Erkennung und Beseitigung von Anomalien, Wartung des Netzwerks sowie Test der in Betrieb genommenen Systeme
- Unterstützung bei der Installation von Sicherheits-Updates sowie der Anpassung der Firewall-Regeln
- Durchführung von Security-Grundlagen- und Expertenschulungen, Security-Awareness-Schulungen, Ethernet-Grundlagenschulungen sowie individuellen Praxistrainings, die speziell auf die jeweiligen Bedürfnisse zugeschnitten sind. ■

Autoren
Werner Neugebauer
Vertical Market Management
Phoenix Contact Electronics GmbH
Bad Pyrmont

Torsten Gast
Leiter Competence Center Services
Phoenix Contact Electronics GmbH
Bad Pyrmont

Kontakt

Phoenix Contact GmbH & Co. KG
Blomberg
services@phoenixcontact.de
www.phoenixcontact.de/security

Funk-Netzwerklösung für digitale Produktion ▲

Die Funk-Netzwerklösung „Nexy" aus dem Geschäftsbereich „Wireless" von Steute ermöglicht die Übertragung von Sensordaten in das Internet der Dinge (IoT) oder andere übergeordnete IT-Systeme. Unterschiedliche Sensoren und elektromechanische Schaltgeräte, aber auch Aktoren und Bediensysteme können in diese kabellose Netzwerklösung einge¬bunden werden. Sie senden und empfangen Daten über den Funkstandard sWave Net, den das Unternehmen für eben diesen Einsatzfall entwickelt hat. Access-Points sammeln die Daten der Funksensorik und -Aktorik und übertragen sie an eine Sensor-Bridge, die als Service-Manager den Datentransfer an übergeordnete IT Systeme des Anwenders übernimmt. So entsteht eine durchgängige Kommunikation von der „Shopfloor"-Ebene bis in die Management-Ebenen der Unternehmens-IT. Ein übersichtlich gestaltetes Dashboard sorgt für die Statusvisualisierung aller in das Netzwerk eingebundenen Endgeräte.

www.steute.com ■

Blitzstrom- und Überspannungsableiter

Die kombinierten Blitzstrom- und Überspannungsableiter der Geräteserie Blitzductorconnect von Dehn schützen Automatisierungs- und MSR-Technik im industriellen Um-

feld wie informationstechnische Schnittstellen. Ein hohes Blitzstrom-Ableitvermögen und ein niedriger Schutzpegel machen sie zu idealen Bausteinen für einen sicheren Endgeräteschutz. Es gibt sie kompakt oder modular aufgebaut mit einer Baubreite von 6 mm. Funktionen wie die Sec-R-Entriegelungstasten und die Push-in-Technik helfen, den Installationsaufwand zu minimieren. Statusanzeige und passende FM-Einheit melden Ausfälle bei Überlast sofort. Für eigensichere Signalkreise stehen Ableiter mit Zulassung für Ex-Anwendungen zur Verfügung. Die Ableiter sind in verschiedenen Varianten verfügbar. Sie schützen zwei Einzeladern mit gemeinsamem Bezugspotenzial (unsymmetrische Schnittstellen) oder eine erdpotenzialfrei betriebene Doppelader (symmetrische Schnittstelle).

www.dehn.de ■

©Kalyakan - stock.adobe.com

GÜTERVERKEHR

Damit die Fracht auch ankommt

Cyberbedrohungen in der Schifffahrt: Güterverkehr als strategisches Angriffsziel

Jährlich werden im weltweiten Handel mehr als zehn Milliarden Tonnen an Gütern auf dem Seeweg verschifft, Tendenz steigend. Die Vernetzung in der Seeverkehrstechnik reicht von den Systemen an Bord wie elektronischen Seekarten und Satelliten-Navigationssystemen bis hin zur Hafenlogistik. So wird ein Cyberangriff auf ein einzelnes Schiff genauso wie auf einen Hafen oder eine Reederei möglich.

Die digitale Piraterie in der Logistik, vor allem in der Hafen-Logistik und Seefahrt ist ein Thema, das bisher selten beleuchtet wurde, und doch wirtschaftliche Schäden in Millionenhöhe anrichten kann. Wolfgang Kiener, Cybersecurity-Experte bei Tüv Rheinland, erklärt: „Containerschiffe bilden den Kern unseres globalen Wirtschaftsverkehrs. Dabei sind sie mittlerweile voll in die digitale Welt integriert. Das sorgt für eine reibungslos funktionierende Lieferkette, macht das System aber auch angreifbar für Cyberkriminelle". Die Vernetzung in der Seeverkehrstechnik reicht von den Systemen an Bord wie elektronischen Seekarten und Satelliten-Navigationssystemen bis hin zur Hafenlogistik. So wird ein Cyberangriff auf ein einzelnes Schiff genauso wie auf einen Hafen oder eine Reederei möglich und wirtschaftliche Schäden sind die Folge.

Cyberangriffe mit wirtschaftlichem und geopolitischem Ziel

Prinzipiell lassen sich drei Arten von Angreifern unterscheiden. Bereits sogenannte Scriptkiddies, die über relativ geringe Kenntnisse verfügen, können mit vorgefertigten Schadprogrammen in die Computersysteme eindringen. Entstehender Schaden ist hier meist singulär und noch recht überschaubar. Zur zweiten Gruppe zählen organisierte Banden, die beispielsweise Erpressersoftware, sogenannte Ransomware, einschleusen und so Containerschiffen den Zugriff auf ihre eigenen digitalen Systeme verwehren – auch um die geordnete Kommunikation im Güterverkehr zu erschweren und um Lösegeld zu erpressen. Der wirtschaftliche Schaden dieser digitalen Piraterie kann schnell hohe Millionenbeträge erreichen.

Ein Beispiel dafür ist der Angriff auf die Reederei Mærsk im Jahr 2017. Cyberkriminelle konnten auf die Logistiksteuerung des Weltkonzerns zugreifen und die Systeme verschlüsseln – mit der Folge, dass per Computer nicht mehr nachvollziehbar war, wo welche Fracht auf den Containerschiffen unterwegs war und wo unterschiedliche Waren lagern. In nur zwei Wochen entstand dem Unternehmen ein Schaden in Höhe von 300 Millionen US-Dollar. „Ein solcher Angriff kann die Existenz eines Global Players bedrohen – und damit erhebliche Auswirkungen für den weltweiten Warenwirtschaftsverkehr verursachen", unterstreicht Kiener.

Schwachstellen im System aktiv aufdecken

„Die Absicherung der Systeme hält mit der zunehmenden digitalen Vernetzung der Seeschifffahrt nicht Schritt. Deshalb ist es umso wichtiger, dass sich die Unternehmen ihrer Schwachstellen bewusst sind und mit einem aktiven Risikomanagement Cyberbedrohungen vorbeugen", rät Kiener. Auf Basis von Risikoanalysen lässt sich feststellen, wo mögliche Einfallstore für Angreifer liegen und wie viel das Unternehmen investieren müsste, um diese zu schließen.

Die zunehmende Bedrohung durch Cyberangriffe in der Schifffahrt ist eines von insgesamt sieben Themen der Cybersecurity Trends 2020 von Tüv Rheinland. Der vollständige Trendreport steht unter www.tuv.com/cybersecurity-trends-2020 zum Download zur Verfügung. ■

Kontakt

Tüv Rheinland Service GmbH
Köln
Tel.: 0221 806 3060
www.tuv.com

Besuchermanagementsystem erweitert

Das Besuchermanagementsystem Visit von Astrum wurde um ein weiteres intelligentes Feature ergänzt. Eine Thermalmessung wurde in den Selbstanmeldeprozess integriert: Präzise Thermalkameras messen aus einer Entfernung von bis zu drei Metern die Temperatur der Besucher. Wird ein Schwellenwert überschritten, können eine vordefinierte Stelle informiert und entsprechende Maßnahmen eingeleitet werden (z. B. Messung über Stirnthermometer o. Ä.). Nach einer Voranmeldung durch einen Mitarbeiter kann sich der Besucher an einem Kiosksystem selbstständig vor Ort anmelden. Der Besucher erhält alle relevanten Informationen und wird um die datenschutzrechtlich notwendige Zustimmung zur Temperaturmessung gebeten. Werden nach seiner Einwilligung keine Unregelmäßigkeiten festgestellt, kann der Anmeldeprozess ohne Verzögerungen in gewohnter Weise fortgesetzt werden.

www.astrum-it.de ■

Switche mit Abwehrmaßnahmen

Die Switche der RY-28-Serie von Barox können so konfiguriert werden, dass sie Sicherheitsnetzwerke und Geräte von Drittanbietern, wie Kameras und Server, vor Ripple20-Cyberangriffen schützen. Ripple20 ist eine Reihe von 19 Schwachstellen in einer Low-Level-TCP/IP-Softwarebibliothek und stellt eine unmittelbare Bedrohung dar.

Wenn es aktiviert wird, könnte es entfernten Angreifern ermöglichen, die vollständige Kontrolle über die Zielgeräte zu erlangen, ohne dass eine Interaktion des Benutzers erforderlich ist. Um Geräte und Netzwerke vor Ripple20-Schwachst ellen zu schützen, müsse ein zweckspezifischer Filter so konfiguriert werden, dass er niemals fragmentierte UDP akzeptiert, so Rudolf Rohr, geschäftsführender Gesellschafter von Barox. Mit den Switchen der RY-28-Serie kann der Deep Cyber Protection so konfiguriert werden, dass fragmentiertes UDP automatisch erkannt und über die integrierten ACL-Switch-Menüoptionen gestoppt wird, dass fragmentiertes UDP blockiert und Netzwerke und ihre Geräte wie IP-Kameras, VMS und Server vor illegalem Zugriff geschützt werden.

www.barox.de ■

Fortschritt für KI-basierte Cybersicherheit

Die „Eberbacher Gespräche" des Fraunhofer SIT bieten ein Forum für einen Dialog, der sich mit KI-basierter Cybersicherheit beschäftigt. Um der Verwendung von KI als Angriffswaffe entgegenzuwirken, empfehlen die Teilnehmer des Eberbacher Gesprächs die Entwicklung eines nachprüfbaren Code of Conduct. KI könne in der Cybersicherheit wesentlich dazu beitragen, auf aktuelle und zukünftige Bedrohungen in Wirtschaft und Gesellschaft geeignet zu reagieren. Eine Voraussetzung dafür sei, dass die Systeme und ihre Leistungen technisch bewertbar bleiben und spezifische Mindestanforderungen für unterschiedliche Branchen und Anwendungsfelder entwickelt werden, so Michael Waidner, Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie und Athene-Direktor.

www.sit.fraunhofer.de ■

Wie sicher sind vernetzte Produktionsumgebungen?

Die von Baramundi in Auftrag gegebene Studie „Cybersecurity-Niveau in der Operational Technology" des Analystenhauses Techconsult untersucht die Gefährdungslage der vernetzten Produktion in deutschen Industrieunternehmen. Sie zeigt, dass die Gefahren für die Produktionsinfrastruktur vielfach noch deutlich unterschätzt werden. Laut der Studie registrierten knapp die Hälfte der befragten Unternehmen im Verlauf der letzten zwölf Monate einen Cyberangriff auf ihre Produktionsinfrastruktur. Neben klassischem Phishing (Abgreifen von (persönlichen) Daten über gefälschte Websites, E-Mails etc.) und gezielten Angriffen über ungepatchte Schwachstellen waren vor allem manipulierte Speichermedien die häufigste Waffe der Angreifer. In jedem dritten Industrieunternehmen kam es aufgrund von Cyberangriffen schon zum Ausfall oder zur Beeinträchtigung der Produktion.

www.baramundi.com ■