Cybersecurity 2016

6. Handelsblatt-Jahrestagung | 21. und 22. November 2016, Berlin

ERGEBNISBERICHT
Die Highlights der Jahrestagung 2016

konferenz.de/cybersecurity

#hbcyber

Konzeption und Organisation:

EUROFORUM
an informa business

Handelsblatt
Substanz entscheidet.

Inhaltsverzeichnis

1. TAG | 21. November 2016

KEYNOTE: Klaus Vitt, Staatssekretär im Bundesministerium des Innern und Beauftragter der Bundesregierung für Informationstechnik 3

KEYNOTE: Herausforderungen der Digitalisierung für Staat, Wirtschaft und Gesellschaft 4

DISKUSSIONSRUNDE: Aktuelle Entwicklungen und Herausforderungen an die nationale und internationale Cyber Sicherheit 6

PRAXISBERICHTE AUS UNTERNEHMEN

Cybersecurity im Zeitalter der Gigabit Gesellschaft 7

Praktischer Ansatz zur Transparenzsteigerung und Risikominimierung als Antwort auf eine zunehmende Cybersecurity Bedrohungslage 8

Die Maschine hält Jahrzehnte – die Bedrohungslage ändert sich jeden Tag 10

Der Weg zu einem ganzheitlichen Cybersecurity Programm 11

Herausforderungen der Digitalisierung an die hardwarebasierte Datensicherheit für unterschiedliche Branchen 12

PERSPEKTIVE VERFASSUNGSSCHUTZ

Keynote: Traum oder Albtraum? – Chancen und Risiken des digitalen Zeitalters 13

Wirtschaftsspionage – Innovation gleich Betroffenheit? 15

PERSPEKTIVE POLIZEI UND MILITÄR

Cybersecurity, Streitkräfte und Innovation 16

EC3's role in tackling the Global Threat 17

Polizei und Privatwirtschaft – Gemeinsame Bekämpfung von Cybercrime 18

Staying one step ahead in cyber security – Current challenges and attacks in cyber space 19

LIVE HACK: Premiere bei der 6. Handelsblatt-Jahrestagung Cybersecurity 2016: „Cherry Picker"-Hack 20

2. TAG | 22. November 2016

DISKUSSION: Die großen Cyber Angriffe aus den Jahren 2015 und 2016 22

Die 10 Gesichter heutiger Schadsoftware 24

RECHTLICHE ENTWICKLUNGEN

Das IT-Sicherheitsgesetz und andere regulatorische Anforderungen an die Cybersicherheit – auf welchem Weg befinden sich Deutschland und Europa? 25

Die richtige Reaktion auf IT-Sicherheitsvorfälle und Datenpannen – die Rolle von interner Rechtsabteilung und externem Rechtsanwalt 26

(Wie) Lässt sich das transatlantische Privacy-Gap überwinden? 27

KRITISCHE INFRASTRUKTUR

IT-Sicherheitskatalog für Strom- und Gasnetzbetreiber nach § 11 Absatz 1a Energiewirtschaftsgesetz 28

Implikationen des IT-Sicherheitsgesetzes für Betreiber Kritischer Infrastrukturen im Energiesektor 29

Flugsicherung und die Frage der Verletzlichkeit – alte und neue Herausforderungen 30

PRAXISBERICHTE AUS UNTERNEHMEN

Sicherheitsvorfallbehandlung in Zeiten von Cybercrime und Advanced Persistent Threats 31

Einführung einer klassifizierungsbasierten E-Mail-Verschlüsselungslösung im Konzern 32

PARALLELE VORTRÄGE

IoT and Industrial Control Systems – Are they a risk to your business? 33

Cyber Defense Strategien im Kampf gegen Cyber Crime – mehr als eine Alibifunktion 34

Supply Chain Security – Es ist Zeit für echten Fortschritt 35

Cyber-Risiken – Versicherung als Teil des Risikomanagements 36

1. TAG

21. November 2016

KEYNOTE Klaus Vitt
Staatssekretär im Bundesministerium des Innern und Beauftragter der Bundesregierung für Informationstechnik

Vitt stellte zu Beginn anhand verschiedener Beispiele von Angriffen auf Geräte des Internet of Things und in den sozialen Medien die Relevanz von Cybersicherheit heraus. Durch den Missbrauch von IoT-Strukturen und Social Bots, die in sozialen Medien Falschmeldungen und Meinungen verbreiteten, würde die organisierte Kriminalität in der digitalen Welt an Einfluss gewinnen. Die Bundesregierung sehe die Digitalisierung als zentrales Zukunftsfeld für die Wirtschaft, die Gesellschaft und den Staat. Cybersicherheit müsse dabei immer mitgedacht werden. Grundaufgabe des Staates sei es, auch die Freiheit der Bürger im Cyberraum zu sichern. Dazu sei unter anderem das IT Sicherheitsgesetz verabschiedet worden. Darin werde ein Mindestrahmen an Cybersicherheit für Betreiber Kritischer Infrastrukturen (KRITIS) festgeschrieben. Zudem helfe die enthaltene Meldepflicht bei Angriffen an das BSI (Bundesamt für Sicherheit in der Informationstechnik) diese optimal analysieren zu können. Am Ende stehe ein Bericht, der den betroffenen Unternehmen und anderen helfen würden, ihre IT Infrastruktur besser zu schützen. Die Meldepflicht solle nach Vitt auf weitere Firmen, die nicht zu KRITIS gehören, ausgeweitet werden.

Im Ausblick verwies Vitt darauf, dass kleine und mittelständische Unternehmen die größten Herausforderungen für die Zukunft der IT-Sicherheit darstellen würden. Hier gäbe es potentiell an vielen Stellen Nachholbedarf. Zudem verband Vitt das Thema Datenschutz mit IT-Sicherheit. Der Austausch von Daten sei die Grundlage aller Entwicklungsprozesse. IT-Sicherheit sei die Grundlage eines effektiven Datenschutzes. Echtzeitdaten wären erforderlich um schnell reagieren zu können. Mögliche Maßnahmen dazu würden oft an die Grenzen des Datenschutzes stoßen. Die Speicherung von Daten durch Telemedienanbieter müsse ausgeweitet werden (Vorratsdatenspeicherung). Auf einen kritischen Einwurf aus dem Auditorium, dass die Speicherung ohne Anlass geschehe, erwiderte Vitt, dass ein solches Verständnis dazu führen würde, dass man erst tätig werden könne, wenn ein Vorfall vorliege. Vorsorge sei besser als Nachsorge.

Auf EU Ebene solle die IT-Sicherheit auch ausgebaut werden. Die NIS Richtlinie sei zentraler Baustein einer einheitlichen Sicherheitsarchitektur und behandle die Themen: EU-weiter Aufbau Nationaler Kapazitäten, bessere Zusammenarbeit und Meldepflichten.

Weiterhin thematisierte Vitt Social Engineering. Im Rahmen der Initiative Wirtschaftsschutz arbeiteten Sicherheitsbehörden auf Bund- und Länderebene zusammen mit dem BSI. Eine gemeinsame Internetplattform biete Informationen zum Einstieg in das Thema.

Bei der Strafverfolgung und Terrorbekämpfung im Cyberraum bestehe zurzeit noch eine Lücke. Die klassische Telefonie werde immer mehr durch IP-Telefonie abgelöst. Die TKÜ (Telekommunikationsüberwachung) müsse sich dieser Situation anpassen. Im Bereich der verschlüsselten Kommunikation müsse ein dualer Ansatz verfolgt werden: Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung. Der Staat solle unter strengen Vorrausetzungen befugt sein über Hintertüren Verschlüsselungen zu umgehen.

Abschließend stellte Vitt fest, dass Cybersicherheit viele Facetten habe. Staat und Gesellschaft seien in der Pflicht sich zu schützen. Diese Pflicht beginne beim Bürger und gehe über zu den Unternehmen. Der Staat müsse Rahmenbedingungen schaffen und dabei das gesamtgesellschaftliche Interesse beachten und Risiken einbeziehen. Konkret plane die Bundesregierung dazu über 30 Maßnahmen. Eine neue Cybersicherheitsarchitektur solle z.B. eine intensivere Zusammenarbeit zwischen Bund und Ländern fördern. Auch eine engere Zusammenarbeit zwischen BSI und Unternehmen, mit kleineren Mittelständlern im Fokus, werde auf den Weg gebracht. Außerdem würden mobile Einsatzteams aufgebaut werden, die im Ernstfall helfen könnten. Dabei sollten Kooperationen mit IT Sicherheitsdienstleitern ins Auge gefasst werden. Der Informationsaustausch über ein Cyberabwehrzentrum werde verbessert. Dabei sei das nächste Ziel, jeden Tag ein aktuelles Bild der Sicherheitslage zu zeichnen. Eine Kennzeichnung der Sicherheit von IT Produkten für Bürger, ähnlich dem Energielabel, werde zudem eingeführt. Die Zertifizierung würde von IT Sicherheitsdienstleistern geleitet. Zusammenfassend stellte Vitt fest, dass in Zukunft dynamisch auf die aktuelle Sicherheitslage reagiert werden müsse. Dies würde über den zentralen Cybersicherheitsrat organisiert. Um diesen zu stärken müsse man weitere Kooperationen aufbauen und IT-Sicherheitsdienstleiter fördern.

Herausforderungen der Digitalisierung für Staat, Wirtschaft und Gesellschaft

KEYNOTE Arne Schönbohm
Präsident, Bundesamt für Sicherheit in der Informationstechnik

Schönbohm forderte zu Beginn dazu auf das Thema IT-Sicherheit in Unternehmen zur Chefsache zu erklären. Bei Themen wie autonomen Fahren, neue Medizintechniken, distributiven Technologien, Industrie 4.0, Smart Factory, Smart Citys, Smart Homes oder Smart Grids seien deutsche Unternehmer „best in class“. Beim Thema IT-Sicherheit würde aber noch zu oft auf den internen IT-Sicherheitsexperten verwiesen. Zentrales Ziel müsse es sein das Thema auf Top Level Ebene zu sensibilisieren.

Weiterhin ordnete Schönbohm die wirtschaftliche Bedeutung der Digitalisierung auch in Bezug auf IT-Sicherheit ein. IT Sicherheit sei in Deutschland ein Standortvorteil. Man hätte eine Vorreiterrolle gegenüber anderen Märkten. Zudem sei IT Sicherheit ein stark wachsender Wirtschaftsfaktor. Nur ein Beispiel sei die IT-SA in Nürnberg als weltweit größte Messe zum Thema. Letztlich sei IT-Sicherheit ein nicht zu unterschätzender Wettbewerbsvorteil.

Schönbohm umriss die aktuelle Gefährdungslage und leitete mit einer Statistik der polizeilichen Kriminalprävention ein. Daraus gehe hervor, dass sich nach Vorfällen mehr als 70% der Betroffenen intensiv mit den Thema IT-Sicherheit auseinandersetzten. Die Statistik der angezeigten Vorfälle zeige zudem nach oben. Allerdings werde häufig erst dann reagiert, wenn ein Schaden vorliege. Auf Grundlage des BSI-Lageberichts vom am 9.11.2016 (www.bsi.bund.de/Lagebericht) kam Schönbohm zum Schluss, dass die Sicherheitslage auf dem IT-Sektor ernst zu nehmen sei. Es finde eine Professionalisierung und Spezialisierung der Hacker statt. Deutschland sei ein bevorzugtes Ziel für Angriffe. Dabei sei kein Industriezweig speziell zu identifizieren. Die Lage sei flächendeckend. Auch deshalb sollten alle Vorfälle immer dem BSI gemeldet werden. Schulungen der Mitarbeiter in Unternehmen sollten zum Standard werden.

Der aktuelle Leitsatz des BSI wurde vorgestellt: „Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft“. Schönbohm betonte dazu die zahlreichen Angebote für die verschiedenen Zielgruppen des BSI. Grundsätzlich müsse mehr darauf geachtet werden „bei jeden anzukommen“, indem z.B. konkrete Bedrohungen deutlicher aufgezeigt werden. Auf wirtschaftlicher Ebene helfen bereits existente bilaterale Kooperationen Gefährdungslagen besser einzuschätzen. In Zukunft solle durch Mobil Incident Response Teams (MIRTs) eine Art „Feuerwehr“ geschaffen werden, die im Notfall sofort ausrücken könne. Allerdings müssten Unternehmen auch über eine „Werksfeuerwehr“ verfügen, also selbst Teams für den Notfall vorhalten.

Im Ausblick sprach Schönbohm verschiedene Digitalisierungsprojekte in naher Zukunft an. Besondern die Energiewende/Smart Metering oder Autonomes fahren/Car-to-X stellten dabei Projekte dar, die sich nicht auf Deutschland beschränkt sehen ließen. Hier brauche es einen Masterplan auf EU-Ebene, bei dem Cybersicherheit von Beginn an mitgedacht werden müsse.

FRAGEN AN SCHÖNBOHM UND VITT

Schönbohm kam zu dem Fazit: Ohne Cybersicherheit könne es keine erfolgreiche Digitalisierung geben. Bei der Entwicklung von neuen Produkten müsse Cybersicherheit immer mitbedacht werden. Zentraler Bestandteile seien Kooperationen aller Beteiligten. Dabei sei eine erfolgreiche Kooperation zwischen dem BSI und der Wirtschaft besonders herauszuheben.

Auf die Frage, woher die Fachkräfte zur Umsetzung verschiedener Pläne kommen sollten antwortete Schönbohm, dass sich das BSI an dieser Stelle vor einer Herausforderung sehe. Würden vorwiegend finanzielle Anreize im Vordergrund stehen, stehe der Bund idR. schlechter da als die Wirtschaft. Würden allerdings Flexibilität und Familie im Vordergrund stehen, dann sei der Öffentliche Dienst attraktiv. Zudem müsse man verstärkt Quereinsteigern Chancen einräumen. Man müsse nicht studiert haben, um Hacker zu sein.

Angesprochen auf Doppelungen und „Ressourcenverschwendung“ in den Strukturen, die durch die föderale Struktur Deutschlands verschuldet würden, erwiderte Schönbohm, dass eine engere Zusammenarbeit die vorhandenen Ressourcen in Zukunft optimaler einsetzen würde. Es gäbe keineswegs zu viele IT-Sicherheitsexperten.

Auf die Frage wie durch das BSI die breite Masse besser im Bereich Cybersecurity geschult werden könne verwies Schönbohm zunächst auf die Unternehmen. Diese müssten ihre Mitarbeiter schulen. Der Staat könne hier nicht alles abdecken. Allerdings unterstütze das BSI gern beim Aufbau von Strukturen. Es gebe Medien zum Thema Sensibilisierung von Mitarbeitern (Videos usw.).

Aktuelle Entwicklungen und Herausforderungen an die nationale und internationale Cyber Sicherheit

DISKUSSIONSRUNDE

Arne Schönbohm
Klaus Vitt
Moderation: Sebastian Schreiber, Geschäftsführer, Syss GmbH
Christof Kerkmann, Redakteur, Handelsblatt

Schreiber leitete die Diskussion mit dem Thema Verschlüsselung ein. Sie würde zu wenig genutzt, besonders in der Emailkommunikation. Daher gebe es enormen Nachholbedarf.

Auf Schreibers Frage, ob es Ansätze gebe die Verschlüsselung zu fördern antwortete Vitt, dass es bereits Angebote für Bürger gebe. Allerdings müsse man nicht alle Mails verschlüsseln. Zudem seien die verfügbaren Verschlüsselungsmethoden umständlich und würden daher nicht genutzt.

Kerkmann sprach das Dilemma von Backdoors in Verschlüsselungen oder Betriebssystemen an. Diese könnten dem Staat dienlich sein, böten jedoch potentielle Angriffsstellen für Hacker.

Vitt sprach in diesem Bezug von einem hochvertraulichen Balanceakt. Durch eine konsequent durchgesetzte Strafverfolgung müsse man zudem abschrecken. Daraufhin merkte Schreiber an, dass eine vertrauliche Behandlung kontraproduktiv zur Schließung von Sicherheitslücken sei. Vitt verwies dazu auf Kooperationen mit Herstellern. Schreiber erwiderte, dass dies schwierig sei, weil Hersteller international ansässig seien und agierten.

Kerkmann fragte, ob es eine Notrufnummer für Cybersicherheitsvorfälle geben würde. Darauf antwortete Schönbohm, dass es zwar bereits ein Einsatzteam gebe, aber eine zentrale Nummer nur schwer umsetzbar wäre. Einsätze würden gefahren, wenn es sich um kritische Infrastrukturen handele.

Schreiber nannte das Thema Crypto-Ransomware. Angriffe diese Art seien technisch relativ einfach und schnell durch das Opfer ausgeführt. Das zu erbeutende Lösegeld werde in Form von Bitcoins eingefordert. Müsste man nicht an dieser Stelle ansetzten? Viele Crypto-Macher seien heute Bitcoin-Millionäre.

Vitt lehnte es ab bei der Onlinewährung anzusetzen. Man müsse sich stets am konkreten Fall orientieren. Sicherheitsmaßnahmen müssten intern implementiert werden. Durch das IT-Sicherheitsgesetz würden Mindeststandards für Sicherheit definiert.

Kerkmann griff erneut das Thema Ransomware auf. Viele Angriffe auf Unternehmen zeigten, dass Mindeststandards nicht umgesetzt werden. Was müsse man besonders den kleinen Unternehmen raten? Schönbohm stellte fest, dass das Erreichen von Mindeststandards wichtig sei. Kontakte zu Geschäftsführungen seien dabei wichtig. Hier müsse Überzeugungsarbeit geleistet werden. Dienstleister sollten zudem Zertifikate haben, damit Qualität gesichert sei. Das BSI stehe für den Grundschutz und für die Sensibilisierung. Darauf stellte Kerkmann fest, dass besonders Vorfälle sensibilisieren. Müsse daher erst etwas

Großes passieren? Darauf erwiderte Schönbohm, dass bereits genug passiere. Es müssten nicht „erst überall das Licht ausgehen“. Man müsse fordern und fördern, sensibilisieren und helfen. „Einer würde sich immer verbrennen“.

Auf die Frage Kerkmanns, ob das IT-Sicherheitsgesetz von den Betreibern kritischer Infrastrukturen auf weitere Bereiche ausgeweitet werden müsse antwortete Schönbohm, dass an dieser Stelle zuerst einmal alle kritischen Infrastrukturen identifiziert und gesichert werden müssten.

Vitt betonte, dass das Gesetz auch eine Meldepflicht beinhalte. Es müsse sich rumsprechen, dass es keine Einbahnstraße sei, sondern dem meldenden Unternehmen der Rücklauf aus dem BSI helfen kann.

Schreiber sprach die Abhängigkeit Deutschlands von anderen Staaten im Bereich Hard- und Software an. Wie könnte die Handlungsfähigkeit Deutschlands gesichert werden, wenn im eigenen Land wenig bis nichts produziert würde?

Vitt bestätigt die hohe Abhängigkeit. Der Versuch in Europa Hardware und Software zu produzieren hielt er für aussichtslos. Andere seien besser. Man müsse daher mit Unternehmen kommunizieren und so auch Verschlüsselungen implementieren.

Zum Schluss der Diskussion stellt Schönbohm fest, dass in Deutschland mit der IT-SA eine der größten IT-Sicherheitsmessen ansässig wäre. Es gäbe eine sehr starke Cybersecurity Industrie in Deutschland.

Cybersecurity im Zeitalter der Gigabit Gesellschaft

PRAXISBERICHT

Abdou Naby Diaw
CSO, Director Corporate Security, Vodafone GmbH

Diaw stellte zu Beginn Technologien und Trends der Gigabit Gesellschaft vor, indem er die Entwicklung des Mobilfunkanbieters Vodafone skizzierte. Der seit mehr als 30 Jahren wirtschaftende Konzern habe heute mehr als 500 Millionen Kunden. Zudem sei Vodafone Marktführer bei der Machine to Machine Kommunikation. Das Mobilfunknetz habe sich vom 2G-Netz der 90er-Jahre über das erstmals 2002 vorgestellte 3G-Netz heute zum 4G-Netz entwickelt. Das 2G-Netz ermöglichte erstmals digitalen Mobilfunk, SMS und eingeschränkte Emailfunktionalität. Das 3G-Netz mit dem UMTS Standard ermöglichte mobiles Internet und Apps wurden populär. Im heute aktuellen 4G-Netz verbessere sich die Sprachqualität deutlich und die flächendeckende Breitbandabdeckung schreite immer weiter voran. Mobiles Videostreaming in hoher Qualität werde möglich. Als nächster großer Schritt stehe das 5G-Netz an, welches ab 2020 zu erwarten sei. Hier läge der Fokus auf vernetzten Maschinen, Gaming und Smart Networks. Aktuell könne die Rede von einem 4,5G-Netz sein, da immer mehr neue digitale Dienste Einzug in den Alltag halten würden und die durchschnittliche Internetgeschwindigkeit im Vodafone-Mobilfunknetz bei 300mbit/Sek. liege. Eine besondere Security Herausforderung für eine sichere Gigabit Welt sei die voranschreitende Vernetzung verschiedener Endgeräte. So würde gleichzeitig die Produktivität, aber auch die Angriffsfläche für Hacker vergrößert. Ein besonderes Problem sei, dass auf PCs viele Nutzer eine Antivirus-Software installiert hätten, auf mobilen Geräten jedoch nur wenige.

Lösungsansätze für mehr Sicherheit im Mobilfunknetz der Zukunft sah Diaw darin Geräte des Internet of Things smarter zu verbinden. Sicherheit sei der Grundstein eines funktionierenden 5G-Netztes. Daran forsche Vodafone an einem eigenen Lernstuhl in Dresden. Eine Echtzeitüberwachung der übermittelten Daten sei nur über ein schnelles Netz möglich. Minimale Latenz (1ms) ermögliche ein taktiles Internet. Auch durch die Reduktion lokaler Datenverarbeitung könne dies erreicht werden. Diaw nannte dieses Vorgehen „Netzbasiertes Schützen". Dieser werde durch weitere Maßnahmen erweitert. Zum Beispiel stelle Vodafone eine Software für mobile Endgeräte bereit, die aktiv würde, wenn dieses sich in ein fremdes Wlan-Netzwerk einwählte. Bei der Machine to Machine Kommunikation müsse man ähnliche Wege gehen.

Zum Abschluss stellte Diaw das Konzpet eines 1 Gbit/s Routers vor. Bei dieser hybriden Technologie werden durch die Bündelung von Fest- und Mobilfunknetz die hohe Geschwindigkeit erreicht.

Praktischer Ansatz zur Transparenzsteigerung und Risikominimierung als Antwort auf eine zunehmende Cybersecurity Bedrohungslage

PRAXISBERICHT

Steffen Hoffmann
CISO, Boehringer Ingelheim Pharma GmbH & Co.

Hoffmann stellte einen praktischen Ansatz zur Risikominimierung aus dem Unternehmen Boehringer Ingelheim Pharma dar. Einleitend stellte er die Entwicklung der Bedrohungslage vor.

Die sei besonders im Bereich Gesundheit besorgniserregend. Patientendaten hätten einen hohen Wert auf dem Schwarzmarkt und auch die Herstellung von Medikamentplagiaten anhand von gestohlener Zusammensetzungsanleitungen sei ein großes Problem. Daher sei Boeringer Ingelheim ein beliebtes Ziel von Angriffen. Dies verdeutlichte Hoffmann anhand einer Email-Statistik aus dem Unternehmen. Daraus ging hervor, dass mehr als 70% aller eingehenden Emails auf Grund von Reputantion Filtering herausgefiltert würden. Anhand einer Statistik zu Phishing Mails stellte er die Breite von Varianten dar, die das Unternehmen erreichen.

Im Folgenden stellte Hoffman vor, wie die Analyse der Ist-Situation und die Feststellung des IT-Security Reifegrades der eigenen Organisation idealtypisch stattfinden müssen. Unter anderen sei der Vergleich mit Firmen in eigenen und fremden Sparten wichtig. Dies müsse über eine gewisse Transparenz im IT-Sicherheitsbereich der Unternehmen erreicht werden. Auch die konkrete Vernetzung mit vielen Wettbewerbern würde gemeinsame Gegner in den Reihen der Hacker identifizierbar machen. Zudem sei eine langfristige Implementierung aller Maßnahmen wichtig.

Als konkrete Maßnahme stellt Hoffmann die, bei Boehringer Ingelheim angewandte, GAP Analysis basierend auf dem CESG Cyber Security Framework (Information Security branch of British Government Communication Headquarter – Intelligence Service) vor. Kern sei das Erkennen und Bewerten von Schwachstellen im System und das Verstehen des eigenen Risikoappetits. Am Beispiel von Nutzerrechten von Mitarbeitern stellte Hoffman dar, welche Risiken im Identitätsmanagement auftreten könnten. Um diesen zu begegnen müsse ein geeigneter und realistischer Maßnahmenkatalog erstellt werden. Darin müsse eine Priorisierung und Festlegung eines Implementierungsfahrplans für die Zukunft enthalten sein.

Zusammenfassend stellte Hoffmann fest, dass ein vollständiges Bild der eigenen IT-Sicherheitslage sehr wichtig sei. Dies müsste kontinuierlich weiter geprüft werden. Zudem müsste der Kontakt zu Wettbewerbern gesucht werden. Eine typische Schwachstelle im Management sei fehlendes Commitment Sicherheitsfragen Konsequenz anzugehen.

FRAGEN AN DIAW UND HOFFMANN

Die Frage, ob Boehringer Ingelheim externe Dienstleister beschäftige um seine IT-Sicherheitsstrategie zu planen verneinte Hoffmann. Allerdings nutze man das vorgestellte externe Netzwerke für Feedback.

Auf die Frage wie man als Provider die Nutzer von veralteten Android Geräten schützen werde antwortete Diaw, dass man dieses Problem im Auge habe. Man verpflichte sich nach Risiken bei den Nutzern zu suchen und die Nutzer zu informieren. Dies gelte auch für Festnetzkunden, die direkte Hilfestellung bekämen. Bei Smartphone-Nutzern sei dies zugegebenermaßen schwieriger. Der netzbasierende Ansatz gebe schon heute Hinweise, wenn eine App veraltet sei.

Auf die Nachfrage, ob dieses Vorgehen in Zukunft ausreichen würde und ob man den Nutzer nicht noch mehr in die Pflicht nehmen müsse sagte Diaw, dass der netzbasierte Schutz additiv sei. Nutzern würde empfohlen clientseitig Software zu installieren.

Auf die Frage wie lange das CESG Cyber Security Framework noch ausreiche, um die IT-Sicherheit zu gewährleisten, antwortete Hoffmann, dass es ein guter Start sei und einen guten Überblick über die eigene Lage gebe. Bei genauerer Betrachtung von speziellen Teilen bräuchte man allerdings externe und andere Frameworks.

Die Maschine hält Jahrzehnte – die Bedrohungslage ändert sich jeden Tag

PRAXISBERICHT

Dr. Thomas Nowey
IM Processes, Governance and Information Security, KRONES AG

Nowey stellte als Vertreter der Firma KRONES AG die zentralen Herausforderungen an ICS Security (Industrial Control System) in den Mittelpunkt seines Vortrags. Als Maschinen- und Anlagebauer sei man im Zugzwang das Thema IT-Sicherheit mitzudenken, da viele verschiedene IT-Systeme in Anlagen verbunden würden. Zudem seien viele Anlagen sehr heterogen strukturiert. Viele Akteure würden die potentielle Angriffsfläche vergrößern. Eine weitere Herausforderung sei, dass Anlagen oft Jahrzehnte funktionieren müssten, sich die aktuelle Bedrohungslage jedoch täglich ändere. Außerdem seien Anlagenbesitzer mehr auf die Produktivität, als auf die IT-Sicherheit fokussiert. Ein großes Problem stelle zudem die Modularität von Anlagen dar. Wenn KRONES nicht die gesamte Anlage mit allen Bestandteilen liefere, müsse anderen Anbietern von Komponenten die Möglichkeit geboten werden für Wartungsarbeiten einen Zugang zum System zu erhalten.

Um diesen Problemen entgegen zu treten sehe man sich in einer Sandwich-Position als Integrator zwischen dem Betreiber einer Anlage und dem Hersteller aller Komponenten. Dazu müsse dem Betreiber IT-Sicherheit als Anforderung für die Anlage vermittelt werden und den Herstellern Dokumentation und Mitwirkungspflicht abverlangt werden. In der Realität liefen diese Kommunikationswege allerdings keineswegs direkt. Die Markmacht verschiedener Hersteller würde es schwer machen Standards festzulegen. Zudem gebe es viele verschiedene Wege eine Anforderung zu erfüllen. Dies verdeutlichte Nowey am Beispiel von Remote Services vom Anbieter zu Kunden für Updates. Es könne eine Remoteserviceplattform vom Anbieter selbst geben, andererseits könne der Kunde einen eigenen Remoteservice zur Kommunikation mit allen Anbietern, mit denen zusammengearbeitet würde, bereitstellen. Als dritte Möglichkeit könne es zudem einen Mediator geben, der vermittelnd auftrete. Aus diesem Beispiel zog Nowey das Fazit, dass es zwar viele Wege aber auch viele bewährte Ansätze gebe um diesem Problem zu begegnen. Ein ISMS nach ISO/IEC 27001 sei auch für ICS Security eine geeignete Basis. Zusätzlich müsse durch Schulungen die Awareness gesteigert werden. Auf organisatorischer Ebene müsse es klare Verantwortlichkeiten geben. Experten müssten die Verantwortung für IT-Sicherheit tragen. Ein angepasstes Sicherheitskonzept erreiche man durch Kapselung in Verbindung mit einer sicheren Gesamtarchitektur.

Dafür müsse beachtet werden, dass die Grundsätze der Sicherheit auch in Zeiten von Industrie 4.0 noch gelten. Die richtigen Maßnahmen hingen vom Angreifer Modell, den Assets und den Schutzzielen ab. Sicherheitszonen und Kapselung für Systeme unterschiedlicher Kritikalität seien unerlässlich. Durch das Minimalprinzip werde die Angriffsfläche reduziert und Verschlüsselung schütze Vertrauliches. Zertifikate stellten sicher, dass es kein Vertrauen ohne Nachweis: geben könne.

Im Ausblick warf Nowey drei Fragen auf. Er sprach das kontroverse Thema Patches an. Wer übernehme die Verantwortung, ob das System nach dem Patch noch korrekt funktioniere? Weiterhin: Wie könne die sichere Authentifizierung bei Machine to Machine Kommunikation sichergestellt werden? Außerdem: Wie rüste man Altanlagen auf?

Der Weg zu einem ganzheitlichen Cybersecurity Programm

PRAXISBERICHT

Matthias Muhlert
Chief Information Security Officer, Hella KGaA Hueck & Co.

Muhlert plädierte zu Beginn seines Vortrags dafür, bei der Implementierung eines ganzheitlichen Cybersecurity Programms mit dem richtigen Mindset zu beginnen. Zudem müsse man zu Beginn das Management von der Dringlichkeit des Themas überzeugen und sich zu jeder Zeit bewusst sein, dass es sehr wahrscheinlich sei, dass es irgendwann einem Hacker gelingen könne alle Sicherheitsmaßnahmen zu umgehen. Daher müsse man Layers erzeugen, die bei einem Angriff behilflich seien einen Angreifer zu lokalisieren und ihn festzuhalten. Andererseits sei redundancy durch Backups zu empfehlen. Ein weiterer Punkt sei, dass man Angriffe verzögere. Durch ein geschicktes designen der Controles könne man Zeit gewinnen oder im Idealfall den Angreifer sogar stellen. Auch von den, in Deutschland eher kritisch betrachteten, aktiven Verteidigungsmechanismen sollte man nicht zurückschrecken. Dies alles müsse man mitbedenken bei der Implementierung eines Cybersecurity Programms.

Anschließend führte Muhlert aus, wie diese Implementierung konkret vonstattengehen müsse. Zuerst müsse das Management zustimmen. Außerdem dürfe es nicht ins Tagesgeschäft integriert werden. Ein eigenes Projekt müsse geschaffen werden. Für den Erfolg sei es kritisch, das ganze Unternehmen mit allen Steakholdern zu beteiligen. Dann verschaffe man sich einen Überblick, welche Cyber Securty Programme es am Markt gebe und suche sich eines, welches möglichst international compliant sei. Mit dem erwähnten Mindset im Hintergrund definiere man 10 bis 15 Themengebiete (Key Arenas). Innerhalb dieser nehme man den Status Quo auf und plane dann neue Maßnahmen. Dabei sei es wichtig an die Capabilities zu denken. Es müsse der Nutzen im Vordergrund stehen. Anwender wollten kein Antivirenprogramm, sondern schlicht keine Viren. Nach der Definition der Keyareas suche man also die Controles heraus (Entweder selbst designt oder später in den verschiedenen Legal Enities implementiert) und achte darauf immer einen Continuous Improvement Process sicherzustellen. Daher müsse der Vorgang am Ende auch immer auditiert werden. Weiterhin sei es wichtig Prozesse zu priorisieren, welche besonders wichtig für das Unternehmen seien. Man solle dabei aber nicht über eine Technologie vorgehen, sondern zuerst ein (potentielles) Problem finden.

Letztendlich sei es zudem wichtig, seine Fortschritte zu dokumentieren und im Auge zu behalten. Dazu biete sich ein System an, in dem bereits erfolgte Schritte für die jeweiligen Legal Entities abgestuft nach Implementierungsgrad festgehalten werden.

Herausforderungen der Digitalisierung an die hardwarebasierte Datensicherheit für unterschiedliche Branchen

PRAXISBERICHT

Dr. Mathias Wagner
Senior Fellow, Chief Security Technologist,
NXP Semiconductors Germany GmbH

Wagner legte den Fokus seines Vortrags auf Endgeräte. Verschlüsselung funktioniere nur, wenn der Empfänger auch wieder entschlüsseln könne. Auf Industriegeräten legen solche Schlüssel lange. Wenn diese Geräte allerdings entsorgt würden, landeten sie oft mit diesen Schlüsseln auf dem Müll. Hier liege ein hohes Sicherheitsrisiko vor. Für das Unternehmen NXP Semiconductors als Marktführer in der Herstellung von Chips auf Karten und Ausweisen, sei dies ein Problem dem man begegnen müsse. In Zukunft würde es immer mehr zu schützende Systeme in diesem Bereich geben.

Grundsätzlich gebe es Angriffe auf funktionale Sicherheitsmechanismen durch Software und Angriffe auf physikalische Sicherheitsmechanismen. Wagner konzentrierte sich auf die hardwarebasierte Datensicherheit und besprach drei physische, gängige Angriffsarten. Information Leakage Attacks nannte er zu Beginn. Dazu gehörten Side-Channel-Attacks oder Seiten Kanal Attacken. Bei diesen würden Wanzen installiert um, mechanischen Geräte abzuhören, wenn zum Beispiel Tagescodes erstellt würden. Dadurch gelange man an geheime Schlüssel. Ein Vorgehen dieser Art sei auch bei Chips möglich. Durch messen von Berechnungszeiten könnten Daten erahnt werden. Auch anhand der Stromkurve könne oft etwas erkannt werden. Man messe hier, was sein Chip abstrahle. Eine weitere Angriffsart seien Fault Attacks. Wagner stellte eine Physical Background to light Attack als Beispiel vor. Mit diesen könne man durch Licht neue Informationen auf einen Chip aufspielen. Dadurch werde ein Fehler auf unterster Ebene (0 und 1) implementiert. Dies könne einen Rechner zum Beispiel bei einer Sicherheitsabfrage zum „wegzuschauen“ bringen, weil randomisiert ein anderer Prozess ausgeführt werde. Eine mögliche Gegenmaßnahme gegen diese Attacke seien mehrere Sicherheitsabfragen hintereinander. Die dritte gängige Art von physikalischen Attacken seien Invasive Attacks. Hier thematisierte Wagner das Reverse Engineering. Es würden zum Beispiel Chips delayert. Man sehe so, wie der Chip arbeite und fände so heraus wo ein Prozess angegriffen werden könne.

Abschließend plädierte Wagner dafür, dass ein Unternehmen, welches Chips herstelle, immer extern geprüft werden müsse. Dadurch werde sichergestellt, dass ein Chip auch sicher sei. Dabei bekannte Systeme seien FIPS 140-2 (vor allem in den USA) und Common Criteria (Europa). In FIPS 140-2 sei oft vorgegeben wie etwas konkret zu tun sei. Dies sei sehr aufwändig in einem sich schnell wandelnden Umfeld. Common Criteria ginge mehr von den Assets aus. Hier würde konkret betrachtet was zu schützen sei. Zwar eigene sich das recht komplexe Common Criteria nicht direkt für die Anwendung in Industrie 4.0, sei aber in einer vereinfachten Version besser für die Zukunft gewappnet als FIPS 140-2.

FRAGEN UND DISKUSSION

Auf die Frage welche Auswirkungen die Übernahme von NXP durch Quadcom haben und ob dadurch das Halbleiter-Knowhow in die US Hand verlagert würde antwortete Wagner, dass bisher keine finale Übernahme stattgefunden hätte. Die Forschung bleibe allerdings in jedem Fall in Deutschland.

Auf die Frage, warum man bei der Auswahl eines Frameworks nicht das BSI-Framework ausgewählt habe antwortete Muhlert, dass für global agierendes Unternehmen der anerkanntere ISO Standard wichtig sei. Das BSI sei ein guter Ideengeber, aber ein internationaler Standard sei oft mehr compliant.

Traum oder Albtraum? Chancen und Risiken des digitalen Zeitalters

PERSPEKTIVE VERFASSUNGSSCHUTZ

Dr. Hans-Georg Maaßen
Präsident, Bundesamt für Verfassungsschutz

Maaßen leitete seinen Vortrag mit einem Überblick über die aktuelle Weltsicherheitslage ein. Die bekannte Weltordnung befinde sich in Teilen in Auflösung. Ehemalige Verbündete fielen weg, die Beziehungen zu Russland seien schwierig und zahlreiche Failed States verstärkten die Unvorhersehbarkeit der Entwicklungen in vielen Teilen der Welt. In diesem Kontext sei das digitale Zeitalter Traum und Albtraum, Chance und Risiko zugleich. Daher sei IT-Sicherheit ein besonders wichtiges Thema. Es gebe immer mehr Angriffe, die heute auch in die Cyber-Spionage und –Sabotage fallen würden. Dies seien Gefahren denen man heute bereits ausgesetzt sei, aber von denen man nicht wüsste was sie in der Zukunft noch bedeuten könnten. Auch das Thema Falschinformationen bzw. Desinformationen im Internet betonte Maaßen als besonders relevant. Der Cyberraum sei ein Gefechtsfeld im militärischen Sinn. Sabotage durch Beeinflussung des politischen Meinungsbildungsprozesses ein großes Problem. Durch die Entwicklung der modernen Informationstechnik sei es Laien möglich zu überschaubaren Preisen einst militärisch genutzte Technik im Internet zu erwerben.

Das Smartphone sei der Schlüssel für die Teilhabe an einer globalen Informationsgesellschaft. Für die Nachrichtendienste sei dies Traum und Albtraum zugleich. In einem Babylonischen Sprachgewirr verschwömmen Banalitäten und hoch brisantes. Daten seien noch nie so leicht abrufbar aber auch verschlüsselbar und anonymisierbar gewesen.

Digitale Kommunikationsmittel seien eine massive Ermächtigung des einzelnen. Dabei gerate die politische Sphäre in den Fokus. Durch Eingriffe in Meinungsbildungsprozesse durch gezielte Beeinflussung eröffne sich eine neue Ebene auf die Propaganda zugreift. Früher sei ein Volk, eine Nation gleich einer Blackbox abgeschottet gewesen. Der Zugriff auf Informationen aus diesem Kreis sei nur Diplomaten oder Kosmopoliten möglich gewesen. Heute habe man ganz selbstverständlich den Zugriff. Zudem gehe die Gatekeeperfunktion der Medien verloren. Traditionelle Bindungen an Interessengruppen, Kirchen, usw. gingen verloren. Zudem sei der soziale Anspruch von Social Media ernst zu nehmen. In

selbstreferentielle Räumen finde viel Beeinflussung statt. Gleiche Meinungen würden über Algorithmen zusammengetragen. Social Media könne daher auch Aufputschmittel zu physischer Gewalt sein. Die Ermächtigung des Einzelnen durch Smartphone und Facebook verstärke den Wandel weg vom Konsumieren vorsortierten Infos der Leitmeiden hin zum „selbst reingestellten“ Inhalten. Trolle verstärkten diesen Effekt. Dies sei besonders bedenklich, da für viele US Amerikaner Facebook das wichtiges Nachrichtenmedium sei. Allerdings finde in diesem keine redaktionelle Bearbeitung statt. Begriffe die wie „Lügenpresse“ sollten alarmieren. Nur kompetent recherchierte Artikel in Qualitätsmedien seien glaubwürdig. Wenn dubiose Internetquellen bevorzugt würden entstünden Verschwörungstheorien. In dieser Gemengelage sei es die Aufgabe der Nachrichtendienste aufzuklären. Allerdings gingen Gegendarstellungen in Social Media in der Regel unter. Dies bebilderte Maaßen anhand verschiedener Beispiele aus der jüngsten Vergangenheit. Dabei legte er besonderen Wert auf politisch motivierte Desinformation.

Abschließend stellte Maaßen fest, dass man täglich neu lernen müsse den Cyberraum nicht nur als Chance, sondern auch als Hochrisikoraum zu betrachten. Dieser befinde sich in einem vorzivilisatorischen Wildwestzustand, in dem das Recht des Stärkeren gelte. Ohne physische Grenzen scheine der Zugang leicht. Sabotage könne Infrastruktur schwächen, Desinformationen treffe direkt auf den Adressaten. Propaganda verschwinde heute hinter digitalen Nebelkerzen. Der moderne Islamismus lebe im Cyberraum, bzw. in einem Cyberkalifat. Propagandavideos seien einfach zu verbreiten. Deutschland könne nicht einfach in den Offlinemodus gebracht werden, aber es brauche ein Mindestmaß an Sicherheit. Dieses dürfe nicht privatisiert werden. Die Masse der Bürger sei auf den Staat angewiesen. Die Dienstleistung des Inlandsnachrichtendienstes sei es sicherzustellen, dass Sicherheit keine knappe Ressource werde.

FRAGEN AN MAAßEN

Auf die Frage, welcher Gefährdungsgrad von Social Bots ausgehe und welche Gegenstrategien man anstrebe antwortete Maaßen, dass Social Bots solange eine Gefahr darstellten, solange man sie nicht als solche ansehen würde. Aufklärung sei der Schlüssel.

Die Frage, welche Rolle die Monopolisierung in den Qualitätsmedien (Springer Verlag usw.) spiele beantwortete Maaßen indem er auf ihre Rolle als Gatekeeper verwies. Zu diesen grundgesetzlichen Aufgaben der Presse hätten sie sich verpflichtet.

Im US Wahlkampf seien Informationen auch über Hacker veröffentlich worden, die den Ausgang beeinflusst haben könnten. Ob es eine solche Gefahr auch in Deutschland gebe und wie so etwas verhindert werden könne antwortete Maaßen, dass es zunächst keine konkreten Hinweise dafür gebe. Die Gefahr sei sehr abstrakt. Allerdings sei man im Gespräch mit den Parteien, um sie zu sensibilisieren. Man mache aufmerksam wie die Gefahr aussehen könne. Politik solle grundsätzlichen transparent sein, aber selbst Kalendereinträge usw. könnten sensibel sein.

Auf die Frage, ob Kräfte zur Verfügung stünden, die staatlich gelenkte Angriffe abwehren könnten, antwortete Maaßen, dass das Verteidigungsministerium bereits aktiv sei. Man brauche aber ein Kompetenzzentrum, auf das Nachrichtendienste zugreifen könnten. Die Bundeswehr sei für den Verteidigungsfall. Im Cyberraum hoffe man keinen Verteidigungsfall zu haben. Daher sei es Aufgabe der zivilen Behörden. Man sei sich aber einig, dass das neue Cyber Command die zivilen Behörden unterstützen müsse.

An Schulen werde zu wenig getan im Bereich Medienerziehung. Auf die Frage, ob es Bestrebungen gebe diesen Missstand zu beheben reagierte Maaßen zunächst mit Zustimmung. Medienpädagogik mit kritischer Betrachtung sei wichtig. Der Verfassungsschutz sei Brandmelder und nicht zuständig für die Pädagogik. Man würde aber die Zuständigen ermutigen.

Auf die Frage wie der Verfassungsschutz auf ausländische Trolle reagiere antwortete Maaßen, dass Aufklärung wichtig sei. Verschiedene russische Desinformationskampagnen seien im vergangenen Jahr aufgeklärt worden. Man versuche zu verstehen, wer hinter etwas stecke. Ausländische Geheimdienste würden mit Hackergruppen zusammenarbeiten und man versuche diese Verbindungen zu enttarnen.

Wirtschaftsspionage – Innovation gleich Betroffenheit?

PERSPEKTIVE VERFASSUNGSSCHUTZ

Jörg Peine-Paulsen
Niedersächsisches Ministerium für Inneres und Sport,
Verfassungsschutzbehörde, Wirtschaftsschutz

Peine-Paulsen warb für eine auszuweitende Cyberawareness, besonders um Wirtschaftsspionage entgegen zu wirken. Aktiver Wirtschaftsschutz sei Spionageabwehr. Dies illustrierte er mit zahlreichen Beispielen. Zu Beginn stellte Peine-Paulsen eine Statistik vor, aus der hervorging, dass der deutschen Wirtschaft jährlich 100 Milliarden Euro Schaden durch Wirtschaftsspionage entstünden. Frage man die betroffenen Unternehmen welche Maßnahmen man zum Schutz gegen weitere Angriffe ergreifen wolle, legten 75 Prozent den Fokus auf bessere Hard- und Softwarelösungen. Nur 56 Prozent der Befragten gaben an für eine bessere Sensibilisierung der Mitarbeiter sorgen zu wollen. Nach Peine-Paulsen sei dieses Ergebnis alarmierend. Es gebe keinen technischen Schutz vor menschlicher Schwäche. Man müsse den Fokus wieder auf den Menschen, vom Social Engineering bis hin zum Innentäter im Unternehmen, lenken.

Im Folgenden besprach Peine-Paulsen aktuelle Fälle aus dem Wirtschaftsschutz. Ein besonders beliebtes Einfallstor seien die Sozialen Medien. Facebook sei eine Self-fulfilling Content Plattform die einen digitalen Zwilling jedes Nutzers abbilden würde. Daher müsse sich jeder Nutzer kontinuierlich fragen, welche Informationen in die sozialen Medien gelangen sollten und wer die Zielgruppe für die Informationen seien könne. Eine strikte Trennung von privatem und dienstlichem sei dabei unerlässlich. Social Engineering Angriffe seien angewandte Sozialwissenschaft und nutzen gezielt menschliche Reaktionen und/oder Schwächen aus. Die Gutgläubigkeit, den Autoritätsgehorsam (z.B. CEO-Fraud) oder auch Gier und Bereicherungsabsichten eines Mitarbeiters in einem Unternehmen böten ein Einfallstor. Daher müssten Szenarien, in denen diese Schwächen ausgenutzt werden könnten, in Schulungen thematisiert werden, um für eine Sensibilisierung zu sorgen. Mitarbeiter müssten Angriffstechniken kennen, um potentielle Angriffe überhaupt erkennen zu können.

Abschließend plädierte Peine-Paulsen dafür IT-Sicherheit zur Chefsache zu erklären. Informationen seien Deutschlands wichtigster Rohstoff. Cyberawareness müsse ein höherer Stellenwert zugesprochen werden.

Cybersecurity, Streitkräfte und Innovation

PERSPEKTIVE POLIZEI UND MILITÄR

Dr. Gundbert Scherf
Beauftragter Strategische Steuerung Rüstung, Leiter Aufbaustab
„Cyber und IT“ der Bundeswehr, Bundesministerium der Verteidigung

Scherf stellte zu Beginn die Aufgabe der Bundeswehr, auch im Bereich Cybersecurity, heraus. In der aktuell sicherheitspolitisch gefährlichsten Lage seit Ende des kalten Kriegs sei es die Aufgabe der Bundeswehr Sicherheit zu gewährleisten. Dafür müsse man agiler, flexibler und anpassungsfähiger werden. Dabei müsse die Digitalisierung als Chance und als Bedrohung zugleich wahrgenommen werden. Als Organisation mit mehr als 42.000 Mitarbeitern befinde man sich in einer schwer überschaubaren Gemengelage. Mitarbeiter kommunizierten zum Beispiel privat über Whatsapp und gäben so potentiell sensible Daten heraus, wenn sie nur Familien kommunizierten, dass sie für einen gewissen Zeitraum nicht erreichbar seien. Daher sei das Schaffen von Awareness und Predictiv Analytics von großen Datenmengen eine wichtige Aufgabe.

Im Rahmen des Konzepts Network-Centric Warfare investiere die Bundeswehr in die digitale Zukunft. Vorhandene Daten müssten besser nutzbar gemacht werden. Daraus ergebe sich eine Bandbreite an neuen Möglichkeiten in der Entscheidungsfindung und ein vorausschauender Instandsetzungs- und Bevorratungsplan. Zudem setzte man auf bessere Vernetzung der Truppe im Einsatz. In Hybriden Einsätzen müssten Informationen mehr geteilt werden. Ein Paradigmenwechsel von „need to know“ zu „need to share“ müsse stattfinden. Dies wolle man durch Programme wie MoTaKo (Mobile Taktische Kommunikation) erreichen. Funkgeräte würden abgelöst durch neue Technik in Zusammenarbeit mit der Industrie. Weiterhin sei kontinuierliche Innovation überlebenswichtig, stellte Scherf fest. Ein Technikzyklus von zwei Jahren sei zu langsam. Daher müsse man durch Kooperationen mit den großen IT-Konzernen Innovationen einkaufen und/oder gemeinsam entwickeln.

Die Deutsche Sicherheit werde auch im Cyberraum verteidigt betonte Scherf. Dabei seien oft einfache Angriffe das Problem, wie der Klick auf einen Link in einer Email. Daher sei ein gesamtstaatlicher Ansatz wichtig. Die Rolle der Bundeswehr in einer allgemeinen Deutschen Cybersicherheitsstrategie sei die der Verteidigung. In Zukunft würden im militärischen Bereich 13.000 Soldaten im Cyberraum tätig. Dabei sollten Deutsche Werte verteidigt werden. Die offene Gesellschaft müsse gerettet werden. Die Verteidigung von Wahrheit und faktischem könne nicht an Algorithmen delegiert werden. Es sei wichtig konkretes zu tun. Die Ministerin habe zu Recht die Digitalisierung zur Hauptbaustelle der Bundeswehr erklärt. Ein gesamtstaatlicher Ansatz könne nicht ohne die Streitkräfte realisiert werden.

EC3's role in tackling the Global Threat

PERSPEKTIVE POLIZEI UND MILITÄR

Steven Wilson
Head of Business European Cybercrime Centre (EC3), Europol

Wilson stellte die Rolle, die Europol im Bereich Cybersecurity einnimmt dar. Europol hätte keine operativen Kapazitäten und würde ausschließlich als Unterstützer nationaler Behörden und Polizei tätig um effektiver gegen internationales Verbrechen vorgehen zu können. Die Behörde setze sich aus vier Operational Units zusammen. Das Information Hub übernehme die Aufgaben eines internationalen Nachrichtendiensts. Hier liefen alle Informationen aus ganz Europa und dem Rest der Welt zusammen. Das EMSC (European Migrant Smuggling Centre) und das EU IRU (European Counter Terrorism Centre) beschäftigten sich mit der Analyse von besonderen Problemfeldern. Letztlich sei der Fokus von Wilsons Vortrag auf dem European Cybercrime Centre (EC3), welches sich mit Themen der IT-Sicherheit auseinandersetze. Das seit 2013 existierende EC3 sei heute mit nahezu allen Bereichen bei Europol verflochten, da viele Verbrechen in der digitalen Welt stattfänden. EC3 bestehe aus drei Abteilungen. Die Abteilung Strategy unterhalte Kontakte zu Unternehmen, um so Profile erstellen zu können woher Angriffe kommen. So würde auch Wissen geteilt, um neue Angriffe im Vorhinein zu vereiteln. Die Forensics Abteilung werde direkt nach einem Angriff tätig. Besonders kleinere Staaten seien auf Grund der Komplexität mancher Angriffe oft auf die Hilfe dieser Abteilung angewiesen. Daher arbeite man auch viel mit Universitäten zusammen. Die Operations Abteilung sei ein internationales Expertenteam, welches sich vorwiegend mit High Level Cybercrime beschäftige. Die Mitglieder kämen aus allen Staaten der Erde und hätten so einen globalen Überblick.

Die 28 Eliten der Cybercrimeeinheiten der Staaten der EU seien in der EUCTF (European Union Cybercrime Taskforce) zusammengefasst. Dieses Team arbeite zusammen an Cybercrimevorfällen in den Mitgliedstaaten. Zweimal jährlich treffe man sich dazu. Am wichtigsten in der EC3 Gruppe seien die Advisory Groups. Universitäten und IT-Sicherheitsfirmen tauschten in diesen, dreimal jährlich, Erfahrungen aus. Unterstützt durch weitere interne Gruppen veröffentliche man jährlich The Internet Organised Crime Threat Assessment (IOCTA). In dieser Bedrohungsanalyse seien alle Trends im Bereich der Cybersecurity angesprochen. Im Bericht aus 2016 sei ein wichtiger Trend der immer einfacher werdende Zugang zu Cybercrime Techniken und Tools. Die bedeutendste Bedrohung gehe allerdings von Ransomware aus. Die Angriffe seien sehr viel gezielter als noch vor ein paar Jahren. Crypto-Currencies seien zudem ein Problem, da viele Erpressungszahlungen und die Bezahlungen von organisierten Verbrechern so nicht rückverfolgt werden könnten.

Bei der Verfolgung von Cybercrime sei Prävention die erste Priorität. Eine effiziente Verfolgung würde zudem abschreckend wirken. Junge Hackingtalente müssten auf „die gute Seite" gezogen werden. Die bereitstehenden Cybercrime Netzwerke müssten zudem aktiv gestört werden. Durch Aufdeckung von Straftaten würden bestimmte Praktiken sukzessive ausgelöscht. Europol habe bereits mit verschiedenen Kampagnen, zum Beispiel gegen Ransomware, auf dieses Problem aufmerksam gemacht. Als praktische Hilfe sei ein Tool, um verschlüsseltes Material wieder entschlüsseln zu können, veröffentlicht worden. Eine wichtige Aufgabe sei es also für mehr Awareness zu sorgen.

Polizei und Privatwirtschaft – Gemeinsame Bekämpfung von Cybercrime

PERSPEKTIVE POLIZEI UND MILITÄR

Heiko Löhr
Leiter, Referat Cybercrime, kommissarischer Leiter,
Gruppe Cybercrime, Bundeskriminalamt

Löhr stellte die Perspektive der Polizei auf den Bereich Cybercrime dar und leitete mit aktuellen Phänomenen, Tätern und Trends ein. Laut einer aktuellen Studie sei das Hellfeld von Cybercrime mit 8,3 Prozent rückläufig. Allerdings sei diese polizeiliche Statistik verfälscht. Andere Schätzungen gingen von weit mehr aus. Daraus sei abzuleiten, dass das Hellfeld nicht realitätsnah erscheine. Phänomenologische Trends seien Identitätsdiebstahl, Ransomware und Phishing, auch im Backend.

Der Umgang mit Verbrechen dieser Art stelle die Polizei vor neue Herausforderungen. Der Zeitpunkt, wann Betroffene zu informieren seien, werde kontrovers diskutiert. Zum einen müsse man verhindern, dass Betroffene möglichst keinen Schaden davontragen. Zum anderen müsse aber auch sichergestellt werden, dass eine Untersuchung der Tat stattfinden könne. Welche Stelle den Accountinhaber final informiere sei zudem problematisch. Die Polizei habe keine Daten, um Betroffene zu benachrichtigen. Telekommunikationsanbieter hätten diese, würden allerdings auf Grund ihres Geschäftsmodells zurückhaltend reagieren. Daher habe das BSI eine Website online gestellt, auf der jeder selbst prüfen könne, ob er betroffen sei. Weitere Probleme bei der Verfolgung von Cybercrime stelle die Zahlung der erpressten Summe bei Ransomware-Angriffen in Bitcoin dar. Die Onlinewährung sei praktisch nicht rückverfolgbar. Auch DDoS-Erpressungen, zum Beispiel auf Onlineshops, würden zunehmen. Da diese das Geschäft gefährdeten, seien Betreiber besonders in der Vorweihnachtszeit bereiter, Lösegeldforderungen umgehend nachzukommen. Zusätzlich beobachte man den „Crime as a Service“-Trend. Allerdings gebe es weniger einen Verdrängungswettbewerb, sondern mehr ein Existieren nebeneinander. Dabei ändere sich die Täterstruktur. Es seien nicht mehr die Nerds, sondern viel mehr als Kundenberater auftretende und hochgradig spezialisierte, organisierte Kriminelle.

Um dieser Entwicklung entgegen zu treten müsse es Kooperationen zwischen Polizei und Wirtschaft geben. Dabei stehe Vertrauen und Vertraulichkeit auf nationaler Ebene im Vordergrund. Man müsse sich vom Mythos verabschieden, dass bei einem Vorfall die Polizei alle Festplatten beschlagnahmen würde und danach kein nennenswerter Fandungerfolg zu erwarten sei. Das German Competence Centre against Cyber Crime eV. sei ein Forum für Unternehmer verschiedener Branchen und dem LKA, um durch Austausch Angriffe vorzubeugen und aus Vorfällen zu lernen. Auf internationaler Ebene können während der Ermittlungen zudem durch Preservations Orders innerhalb von Stunden ausländische Server sichergestellt werden. So wirke man dem Beweismittelverlust entgegen. Im Fazit betonte Löhr nochmals, dass immer wenn ein Angriff stattgefunden habe, es sehr wichtig wäre, den Urheber zu ermitteln. Dies gelinge allerdings nur bei Kooperation mit der Polizei und einem gegenseitigen Vertrauen.

Staying one step ahead in cyber security – Current challenges and attacks in cyber space

PERSPEKTIVE POLIZEI UND MILITÄR

Brigadier General (ret) Rami Ben Efraim
Head of Government, Defense and Critical Infrastructure,
Check Point Software Technologies GmbH

Efraim gab zu Beginn einen kurzen Überblick über die wichtigsten Veränderungen im Cyberbereich in den letzten Jahrzenten. Einst lokale Netzwerke seien heute weltweite Datenclouds. Die Firma Check Point sei durch ihre Präsenz auf dem gesamten Globus international gut aufgestellt, um an jedem Ort auf ein Problem reagieren zu können. Die Bedrohungslage habe sich zudem geändert. Cybersecurity sei längst kein Thema mehr nur für Geeks, sondern ein National Security Issue. Efraim verdeutlichte die Lage an vier Beispielen, die er „Game Changers" nannte. Am Beispiel eines großen Stromausfalls in der Ukraine, bedingt durch einen Angriff, zeigte er, dass kritische Infrastrukturen nicht zwingend an das Internet angeschlossen sein müssten, um ein Ziel zu sein. Angriffe auf Banken zeigten, dass Hacking inzwischen auch eine Dienstleistung sei, die Kriminelle einfach einkaufen könnten. An den Angriffen auf Flughäfen in Vietnam sehe man, dass Terroristen nicht mehr physisch in das Cockpit eines Flugzeugs gelangen müssten. Über einen Hack sei die Fernsteuerung möglich. Ein besonders relevantes System in diesem Zusammenhang sei zudem das international vernetzte Ticketsystem der Airlines. An den aktuellen Angriffen mit Ransomware auf Krankenhäuser sehe man, dass Angegriffene immer häufiger die Bereitschaft zeigen, Lösegeldforderungen nachzukommen.

Um diesen Verbrechen entgegenwirken zu können, müssten Staaten die eigene Cybersecurity-Lage immer im Auge behalten. Dabei sei der Ansatz, dass Vorfälle meldepflichtig seien, grundsätzlich nicht schlecht. Allerdings sei es dann oft bereits zu spät. Das Konzept einer Nationwide Protection von Check Point setzt früher an. Ein zentrales Gateway, durch das alle Daten rein- und rausgingen, müsse vor jedes Unternehmen geschaltet werden. Das Gateway erkenne durch die Vernetzung mit allen anderen Gateways jedes Problem sofort. So könnten Kommunikationsstrukturen erkannt werden. Wenn vor einem Angriff bereits etwas bekannt würde, könnte zudem ein Update alle Gateways sicher machen.

Abschließend plädierte Efraim nochmals dafür, sich nicht nur auf die Erkennung von Angriffen zu verlassen. Vorerkennung sei die Lösung. Diese könne nur über ein System, dass die gesamte Infrastruktur einer Nation umfasse, geleitet werden.

LIVE HACK: Premiere bei der 6. Handelsblatt-Jahrestagung Cybersecurity 2016 „Cherry Picker“-Hack

PERSPEKTIVE POLIZEI UND MILITÄR

Sebastian Schreiber
Geschäftsführer, SySS GmbH

Schreiber stellte zunächst seine Firma, die SySS GmbH vor, die auf Hacking und Penetrationstests spezialisiert ist. Auch Forschung gehöre zum täglichen Geschäft. Diese sei wichtiger denn je, weil heute das Equipment, welches für Hacks benötigt werde, deutlich günstiger erworben werden könne. Daher gebe es eine immer breiter werdende Basis für Hacker.

Aktuell seien Funktastaturen, Funkmäuse und kabellose Präsentationsgeräte wie der Logitech Presenter im Fokus der Arbeit der SySS GmbH. Letzterer verschlüssele nicht. Da sich der Presenter gegenüber dem Laptop als Tastatur und Maus ausgebe, biete er ein großes Einfallstor für Angriffe. Nicht nur eine laufende Präsentation könne gestört werden, auch das Aufspielen von Trojanern über die Eingabe von Befehlen sei möglich. Funkmäuse funken immer unverschlüsselt. Allerdings könne man diese über ein virtuelles Keyboard missbrauchen. Daher seien sie eine besondere Gefahr, weil deren Potential oft unterschätzt werde. Konkret zeigte Schreiber einen Angriff auf eine Tastatur des Deutschen Anbieters Cherry. Die Tastatur wird mit der Zertifizierung nach AES 256 beworben, die auf den ersten Blick Vertrauen in das Produkt schaffen solle. Den Angriff führte Schreiber mit dem von SySS entwickelten Cherrypicker, einem Raspberry Pi-System mit Sende- und Empfangsmodul, durch. Im Szenario meldete sich ein Nutzer bei einem Windowssystem an. Diese Eingabe konnte durch den Cherrypicker aufgezeichnet werden und für eine spätere Anmeldung am System wieder gesendet werden. So erhalte der Angreifer Zugriff auf einen Rechner. Konkret könnte so zum Beispiel morgens in einem Büro aufgezeichnet werden, was Nutzer als erstes über ihre Tastatur eingeben. Dies werde in der Regel das Passwort sein. Das Passwort könne dann zu einem späteren Zeitpunkt erneut an den Rechner gesendet werden. Technisch basiere das Verfahren darauf, dass ein Tastendruck zwei Signale auslöse: Das Drücken und das wieder Loslassen. Daher sei bekannt, dass der letzte Befehl ein Key Release sein müsse.

Die Zwischenfrage, ob das gleiche Verfahren auch bei Autos mit Funkentriegelung funktionieren würde, verneinte Schreiber zunächst. Allerdings könne man Fahrzeuge mit einem Keyless Go-System über eine Funkstreckenverlängerung entriegeln. In einem möglichen Szenario würde der Angreifer, ausgerüstet mit einem Empfänger, neben der Person sitzen, die den Autoschlüssel in der Tasche trage. Ein Komplize neben dem anzugreifenden Auto würde das übertragene Signal empfangen, an den Empfänger des Autos senden und es so öffnen und starten können. Eine Replay-Attacke, wie beim Cherrypicker beschrieben, funktioniere hier nicht.

Weiterhin sprach Schreiber über funkbasierte Heimalarmanlagen. Hier sei das Entschlüsseln noch einfacher als bei der Cherry Tastatur. Einfaches aufzeichnen genüge. In einem Szenario müsse sich der Angreifer nur in der Nähe der Eingangstür befinden. Wenn der Bewohner die Alarmanlage stumm schalte, müsse nur das gesendete Signal aufgezeichnet werden. An einem späteren Zeitpunkt könne es dann über eine Replay-Attacke erneut gesendet werden. Diese Sicher-

heitslücke sei symptomatisch. Elektrotechnikanbieter kümmerten sich nicht um Verschlüsselung. Bei 100 Prozent der getesteten Alarmanlagen funktioniere diese einfache Replay-Attacke. Als Lösung dieses Problems empfahl Schreiber auf Funk zu verzichten. Allerdings wären oft auch zum Beispiel von Mitarbeitern selbst mitgebrachte Funktastaturen ein unerwartetes Einfallstor.

Auf die Zwischenfrage nach der Reichweite antwortete Schreiber, dass Hackingtools Reichweiten von bis zu 1000 Meter erreichen können. Die geringere Reichweite der Tastatur wäre dabei kein Hindernis. Das Signal könne abgeholt werden. Zudem finde man oft Wege, um deutlich näher als 1000 Meter an ein Objekt heran zu kommen. Die Frage ob auch Bluetooth-Verbindungen getestet wurden verneinte Schreiber. Man habe sich auf WLAN fokussiert.

Gefragt, woher das verwendete Toolkit komme, nannte Schreiber verschiedene Open Source Quellen. Dass diese jedem zugänglich seien verstärke das Problem. Auf die Zwischenfrage, wie die Hersteller von Funkprodukten auf solche Angriffe reagieren, beschrieb Schreiber das Vorgehen bei SySS: Man forsche viel im Bereich IT-Sicherheit. Was auch immer in Auftrag gegeben werde, wird getestet. Der Auftraggeber habe natürlich das Recht, dass die Ergebnisse nicht direkt veröffentlicht würden. Responsible Disclosure sei Standard. Wenn eine Schwachstelle gefunden werde und der Kunde auf den Hersteller zugehe, könne dieser es selbst lösen. In der Regel schreibe SySS ein Advisory. Gelegentlich gingen Hersteller juristisch vor. SySS veröffentliche trotzdem. Andere wiederum reagierten gar nicht, andere sind glücklich. Es gebe ein Gap zwischen Anerkennung und Lob und rechtlichen Schritten. Grundsätzlich informiere man den Hersteller und setze eine gewisse Frist, damit Patches ausgerollt werden könnten. Im Jahr 2016 habe man bereits mehr als 120 Advisorys veröffentlicht.

Im Folgenden stellte Schreiber verschiedene, freiverkäufliche Hackingtools vor. Er unterstrich die Verfügbarkeit, indem er verschiedene Onlineshops aufrief, wo die Geräte erworben werden können. Unter anderem präsentierte Schreiber eine USB-Wanze, die alle Daten mitschneiden könne, welche durch den USB-Anschluss laufen. Das Gerät koste 30 Euro und könne die Daten lokal abspeichern oder per Funk weitersenden. Das Hackingtool Rubberducky führte Schreiber live vor. Es glich im Erscheinungsbild einem gewöhnlichen USB-Stick. Dem angeschlossenen Computer gab es sich als Tastatur aus und begann sofort Befehle einzugeben um Schadsoftware auszuführen. Das Tool koste 44 Dollar. Zuletzt zeigte Schreiber einen USB-LAN-Stick mit Linux-System. Am hinteren Ende schließe man ein LAN-Kabel an, per USB werde der Stick mit dem zu infizierenden Computer verbunden. Das Tool gebe sich daraufhin dem PC als Netzwerkkarte aus. Das Linuxsystem eröffne dann einen Tunnel auf ein beliebiges Cloudsystem. So erhalte man eine perfekt getarnte Hintertür.

Zum Abschluss zeigte Schreiber noch einen Angriff auf die App Quizduell, bei der Spieler gegeneinander Quizfragen beantworten. Nachdem ein Freiwilliger aus dem Publikum gefunden war, der Quizduell gegen Schreiber spielen wollte, starteten beide ein Spiel. Der Freiwillige beantwortete drei Fragen zuerst, woraufhin Schreiber an der Reihe war. Dieser nutzte ein Mobiltelefon auf dem eine manipulierte Version der App installiert war. Diese zeige schon vor dem Beantworten der Frage die richtige Lösung, sodass Schreiber nur noch das bereits markierte Feld antippen musste. Schreiber beschrieb im Folgenden wie die App von SySS manipuliert worden war. Es hätte mehrere Sicherheitsverbesserungen durch den Betreiber von Quizduell gegeben. Zuerst habe eine einfach Traffic-Attacke genügt. Seit Einführung von Certificat Pinning hätte man auf die Manipulation der App selbst zurückgreifen müssen. Dieses Beispiel zeige anschaulich, dass eine einfache Reaktion auf ein Sicherheitsproblem oft nicht ausreicht. Kreative Hacker fänden immer wieder neue Wege.

Die großen Cyber Angriffe aus den Jahren 2015 und 2016

DISKUSSION

Christof Kerkmann
Redakteur Unternehmen und Märkte, Schwerpunkt Technologie, Handelsblatt
Wilhelm Dolle
Partner Cybersecurity, KPMG AG Wirtschaftsprüfungsgesellschaft

Handelsblatt Redakteur Christof Kerkmann und der Vorsitzende Wilhelm Dolle diskutierten gemeinsam mit den Teilnehmern aktuelle, kontroverse Themen und die bedeutenden Cyberangriffe aus den Jahren 2015 und 2016. Kerkmann begann mit dem DDoS-Angriffen unter anderem auf den Routing Dienstleister DynDNS. Der Angriff hat viele Webseiten wie zum Beispiel Twitter für längere Zeit unerreichbar gemacht. Wie solle man solchen Angriffen begegnen, die gleich mehrere Websites lahmlegten? Darauf antwortete Dolle, dass man sich zuerst vom naiv, romantischen Bild eines Einzeltäters verabschieden müsse. Es sei eine Industrie, die solche Angriffe durchführe. Verstärkt werde dies dadurch, dass Schadsoftwaretools frei verkäuflich seien. Die DDoS-Angriffe auf konkrete Websites seien dabei besonders interessant. Dolle nannte als Beispiel den Fall Brian Krebs, der in Artikeln beleuchtet, wer die Angreifer hinter Angriffen seien. Die Website von Krebs wurde daraufhin angegriffen, was zu Folge hatte, dass sein Hoster die Website kündigte. Der Traffic sei dauerhaft zu hoch gewesen. Dieses Beispiel zeige, wie konkreten Websites die Grundlage entzogen werden könne. Hoster würden zudem unter Druck gesetzt werden.

Daraufhin fragte Kerkmann, ob zu erwarte wäre, dass 2017 die generellen Höchstgrenzen für Anfragen (Traffic) steigen müssten. Dolle bestätigte dies. Es würden zudem nicht nur Rechner gekapert. Alle IoT-Geräte wie zum Beispiel internetfähige Babyphones, könnten als Teile eines Hackernetzwerks missbraucht werden. Es stelle sich die Frage, wer davon den Schaden trage.

Nutzer von Babyphones, welche Netzwerkpakete rausschickten, seien es oft nicht. Selbst wenn dies entdeckt werde, könne der Nutzer die Geräte oft nicht updaten. Bei Ransomware sei der Nutzer in Gegensatz zum Handeln gezwungen, weil er selbst den Schaden erleide. Daher werde es in Zukunft eher mehr DDoS-Angriffe geben.

Kerkmann fragte darauf, ob man mit mehr Regulierung im Bereich der IT-Sicherheit diesem Trend entgegenwirken könne. Dolle bejahte dies. Die freiwillige Selbstverpflichtung funktioniere nicht. Awareness müsse in die Köpfe der Entscheider. Nicht nachträgliches Sichern sei gefragt, sondern müsse von Anfang an mitgedacht werden. Kerkmann stimmte zu, verwies aber auf Geräte aus China oder aus Kickstarter-Projekten. Diese Hersteller hätten nicht so ausgefeilte Produktionsketten und seien oft schwer adressierbar. Dolle verwies darauf, dass die Käufer durch ihre Kaufentscheidung die Hersteller in die Pflicht nehmen könnten. Ein Gütesiegel würde dabei den normalen Anwendern helfen. Nur wäre zuvor zu klären, wer ein solches Siegel vergeben dürfe. Außerdem brauche man eine einfach erkennbare Maßeinheit.

Kerkmann fragte daraufhin ins Publikum, wer noch eine Yahoo Emailadresse habe. Niemand meldete sich. Kerkmann erklärte daraufhin, dass Yahoo mehr als ein Jahr gebraucht habe, einen Datendiebstahl festzustellen. Die Reaktionszeit sei selbst für einen Internetanbieter viel zu langsam. Dolle bestätigte dies und nannte als Lösung eine eigene Domain zu betreiben. Jedes Mal, wenn man sich bei einem Anbieter neu anmelde, nehme man eine neue Emailadresse. Per Catch-All empfange man alle Mails. So könne man erkennen, wer Daten weitergebe.

Kerkmann bat um ein weiteres Beispiel. Dolle sprach daraufhin die Datenschutzbestimmungen von Websites an. Die Zahl der Websites, die eine Anmeldung erwarteten, steige. Viele Nutzer nutzten die gleichen E-mailadressen- und Passwortkombinationen auf Websites. Wenn also bei einer Website die Daten gestohlen werden, dann haben Hacker potentiell Zugriff auf mehrere Konten. Ein gutes Beispiel sei der Pentagon-Hack. Angegriffen wurde dabei ein privater Server, auf dem sich Mitarbeiter des Pentagon privat verabredeten. Die Passwort-E-Mail-Kombinationen seien dann genutzt worden, um das System des Pentagon zu knacken.

Kerkmann sprach anschließend den Ashely Maddison Hack an. Wie könne es sein, dass derart große Datenmengen unbemerkt kopiert worden waren? Dolle verwies auf die immer weiter steigende, verfügbare Internetgeschwindigkeit. Wenn etwas physisch geklaut werde, würde es oft sofort bemerkt. Datendiebstahl werde oft nicht sofort bemerkt, weil die Daten nur kopiert werden und daher nicht weg wären. Ein Beispiel wären hier die Krankenhaus-Hacks. Diese Systeme seien oft besonders schlecht geschützt.

Kerkmann erinnerte an den Beitrag von Maaßen vom Vortag und sprach politische Angriffe an. Als Beispiel nannte er verschiedene Inhalte, die über Wikileaks veröffentlicht wurden und den Angriff auf den Deutschen Bundestag. Angreifer kämen in vielen Fällen aus Russland. Nun, wo der Wahlkampf zur Bundestagswahl ins Rollen komme, müsse man das Thema wieder auf die Agenda bringen. Dolle stimmte zu und sprach von Verschlüsselung. Man solle bei jeder Gelegenheit Verschlüsselungstechnik nutzen. Wenn nur verschlüsselt werde, wenn es um sensible Daten ginge, wisse der potentielle Angreifer genau bei welchen Daten sich ein Diebstahl lohnen würde. Kerkmann fügte hinzu, dass der Bundestag noch lange mit Windows XP-Systemen gearbeitet habe. Dies sei Dilettantismus. Dolle stimmte zu und bemerkte, dass auch viele Unternehmen bis heute das veraltete Betriebssystem nutzen. Die Awareness müsse steigen, bevor etwas passiere.

Kerkmann sprach daraufhin Sicherheitslücken im mobilen Betriebssystem Android an. Dieses komme in vielen Unternehmen zum Einsatz. Dolle nannte Blackberry als einst beherrschend auf dem Markt der Dienstgeräte. Bis heute seien viele Geräte im Einsatz. Andererseits würden viele zu Apple-Produkten greifen. Aber es gebe eben auch Android-Geräte. Besonders bei einer Bring your own device-Firmenpolitik wären Android-Geräte häufig. Dabei könne eine Schwachstelle bis zu einer Milliarde Geräte betreffen. Bereits aufgedeckte Lücken seine besonders alarmierend. Ohne das aktive tippen des Nutzers sei eine Infizierung des Endgeräts möglich gewesen. Daher müsse festgehalten werden: Wenn eine vertrauliche Besprechung stattfindet und ein Handy dabei im Raum ist, dann sei es keine vertrauliche Besprechung mehr.

Kerkmann warf ein, dass sich Google bemühte, monatliche Updates zu bringen. Samsung als Marktführer bei Android-Geräten habe sich selbstverpflichtet, diesen Zyklus zu fördern. Dolle forderte dazu einen implementierten Automatismus wie bei einem Windowsupdate, damit Nutzer auch tatsächlich updaten. Dem entgegen spreche, dass gelegentlich Apps nach Updates nicht mehr zuverlässig funktionierten.

Abschließend sprach Kerkmann noch an, dass er vom Kauf von günstigen Geräten, wie Mobiltelefonen des Herstellers One+One abrate, weil zu selten Updates veröffentlicht würden. Als Abschlussfrage sprach er die neue Strategie Blackberrys an, die ihr neues Betriebssystem auf Android-Basis aufbauen und eigene Sicherheitsstrategien implementieren würden. Dolle wies darauf hin, dass oft Apps von Drittanbietern das Problem darstellen würden. Wenn der Anwender einer Anwendung weitreichende Rechte einräume, hebele er auch einen sicheren Kern eines Betriebssystems aus. Die Vergabe von Berechtigungen sei nicht so benutzerfreundlich, wie sie sein sollte.

Die 10 Gesichter heutiger Schadsoftware

Marion Marschalek
Principal Malware Researcher, G DATA Advanced Analytics

Marschalek von G DATA Advanced Analytics leitete ein, indem sie ihr Tagesgeschäft beschrieb. Sie beschäftigt sich ausschließlich mit Schadsoftware. Sie erkennt Module, wie Software funktioniere und erforscht, wie sie entfernt werden könne. Im Rahmen ihres Vortrages stellte sie zehn Arten aktueller Schadsoftware vor.

Sophisticated Malware sei sehr aufwändig programmiert, weil damit Geld verdient werden könne. Besonders Ransomware könne direkt monetisiert werden. Bei Scam und Banking Maleware sei daher der Trend rückläufig. Durch Click Fraud, also automatisiertes anklicken von Werbung die per Click bezahlt werde, könne mit Bots Geld verdient werden. Beim Bitcoin Mining, also dem Freigeben von Rechenleistung auf dem eigenen Rechner gegen Bezahlung in Bitcoin, könne legal Geld verdient werden. Hacker würden hier durch Trojaner fremde Rechner fernsteuern und so die Bezahlung einstreichen. Letztlich gehöre noch Adware zum Bereich der Malware. Sie sei grenzwertig legal. Im Unterschied zu Ransomeware sei Adware mit Benutzereinwilligung auf Rechnern installiert.

Schadsoftwareentwickler seien anpassungsfähig, zahlreich und einfallsreich. Seit über 20 Jahren finde ein Wettrüsten zwischen Sicherheitsindustrie und Malwareautoren statt. Packern, Cryptern oder Multi-Komponenten-Malware setze man Firewall, Anitivirus-Software oder Incident Response-Pläne entgegen. Letztere reagiere heute zwei bis vier Stunden nach Erscheinen einer neuen Malware. Noch besser sei Proactive Malware Jagt.

Statistiken zufolge steige die Zahl von Malware immer stärker. Heute zähle man bis zu 140 Millionen Malware Samples. Im Jahr 2006 weniger als 1 Million. Diese Entwicklung sei darauf zurück zu führen, dass es heute viel mehr Varianten einer Schadsoftware gebe.

Häcker fänden immer neue Wege. Das Beispiel Linux veranschauliche dies gut. Erst seit Rechenleistung monetarisierbar sei, sei das Betreibssystem im Fokus der Hacker. Es gebe sogar Tools, die andere Bots entfernten, um die gesamte Rechenleistung des Systems beanspruchen zu können. Bei Windowssystemen fiele die CPU-Belastung hingehen schnell auf.

Schadsoftware sei oft schwer zu fassen und repetitiv. Gegen Fileless Infection seien Virenfilter durch ihre Funktionsweise machtlos, weil kein Zugriff auf das Dateiensystem erfolge. Zudem gebe es Software, die sich gezielt verstecken könne.

Eine große Zahl an Malware funktioniere zudem sehr ähnlich. Viele Ransomware, DDoS-Angriffe, Spionagesoftware oder Download-Bots, die andere Malware herunterladen, würden als Dienstleistung von Hackern angeboten. Dabei sei die Funktionsweise vergleichsweise simpel und linear. Es gebe keine oder wenig klassische Softwareentwicklung im Schadsoftwaredesign. Viele Programme führten wenige Aufgaben aus. Der Code liege oft in einem flachen Softwaredesign, in einem sogenanntem „Spaghetti Code“, vor. Entwickler machten sich nicht viele Gedanken, sondern programmierten einfach runter. Daher sei der Code auch manchmal fehlerhaft. Antivirenanbieter könnten Entschlüsselungen von Ransomware anbieten, weil verschiedene Fehler eingebaut werden. Zudem gebe es viele halb fertige Features. Durch die Verwendung von bereits existierenden Codes würden Kosten auf Seiten der Hacker eingespart, aber auch Fehler weitergetragen.

Im Fazit stellte Marschalek fest, dass Malewareautoren selten wie erfahrene Entwickler agierten. Trotzdem witterten viele das schnelle Geld. Sicherheitsunternehmen müssten die Angriffe so aufwändig und teuer machen, dass es sich für Hacker nicht lohne.

Das IT-Sicherheitsgesetz und andere regulatorische Anforderungen an die Cybersicherheit – auf welchem Weg befinden sich Deutschland und Europa?

RECHTLICHE ENTWICKLUNGEN

Wilhelm Dolle
Partner Cybersecurity, KPMG AG Wirtschaftsprüfungsgesellschaft

Dolle gab in seinem Vortrag einen Überblick über die aktuelle Lage der Cybersecurity-Regulierungen und sprach über das IT-Sicherheitsgesetz. Zunächst schilderte er die bisherigen Auswirkungen der NIS Directive (Directive on security of network and information systems) auf Deutschland und Europa. Diese verlange von allen EU-Mitgliedstaaten die Umsetzung von IT-Sicherheitsgesetzen. Deutschland spiele hier eine Vorreiterrolle. Umgesetzt werden müsste eine nationale KRITIS-Strategie, ein nationaler Krisenkoordinationsplan, eine nationale KRITIS-Behörde, ein nationales CERT sowie Kooperationen zwischen öffentlichen und privatem Sektor.

Die EU-Datenschutzgrundverordnung sei eher auf Datenschutz als auf Cybersecurity ausgerichtet. Allerdings werde die massive Verschärfung des Sanktionsrahmens bei Missachtung auch einen Einfluss auf Cybersicherheitsstrategien haben.

Das deutsche IT-Sicherheitsgesetz betreffe vor allem Betreiber kritischer Infrastrukturen. Da es sich allerdings um ein Artikelgesetz handele, erweitere es andere Gesetze. So könnten zum Beispiel durch die Erweiterung des Telemediengesetzes auch Anbieter von kommerziellen Websites betroffen sein. Der Fokus des Gesetzes liege aber auf den Sektoren Energie, Transport und Verkehr, Informations- und Telekommunikationstechnik, Gesundheit, Finanz- und Versicherungswesen sowie der Wasser- und Ernährungswirtschaft. Die Bestimmungen von KRITIS erfolgten über die Anlagen. Daher könne in einem Betrieb auch nur eine konkrete Anlage betroffen sein.

Die Hauptanforderungen an KRITIS seien die Meldung von Sicherheitsvorfällen, die Etablierung von Sicherheitsstandards und der Nachweis der Umsetzung. Die Fristen zur Umsetzung liefen bereits und seien gestuft bis 2020. Betreiber seien dabei selbst in der Pflicht sich zu melden, wenn sie betroffen seien. Die Umsetzung dieser Forderungen sei besonders schwierig für kleinere Betriebe mit wenigen IT-Mitarbeitern.

Im Ausblick auf die nächsten Jahre fasste Dolle zusammen, dass die aktuellen Entwicklungen durchaus positiv zu betrachten seien. Allerdings sei das IT-Sicherheitsgesetz verbesserungswürdig in Details. Es sei dennoch wichtig, weil es als Gesetz so aufgebaut sei, dass sich nicht nur IT-Mitarbeiter damit beschäftigen müssten. Daher bringe es die Cybersicherheit in die Köpfe von Entscheidern, die sich vorher nicht darum gekümmert hätten.

Die richtige Reaktion auf IT-Sicherheitsvorfälle und Datenpannen – die Rolle von interner Rechtsabteilung und externem Rechtsanwalt

RECHTLICHE ENTWICKLUNGEN

Dr. Martin Braun
Rechtsanwalt, Partner, WilmerHale

Braun sprach aus Sicht des beratenden Rechtsanwalts über Sachverhaltsermittlungen und Reaktionen auf einen IT-Sicherheitsvorfall und die Rolle des Anwaltsgeheimnisses in Deutschland, Europa und den USA. Auch die Benachrichtigungen von Behörden und Betroffenen sowie Haftungsrisiken und Gerichtsverfahren waren Thema seines Vortrags.

Forensik habe aus juristischer Sicht erste Priorität bei einem IT-Sicherheitsvorfall. Auf deutscher Seite gebe es teilweise Vorbehalte, mit amerikanischen Anbietern zusammenzuarbeiten. Diese seien unter Zeitdruck besonders schwierig auszuräumen. Daher sollten Ersthelfer bereits bevor ein Vorfall eintritt hinzugezogen werden. Zudem schütze das US-Anwaltsgeheimnis die Ergebnisse einer forensischen Untersuchung, wenn ein Anwalt diese in Auftrag gebe. In Deutschland sei dies sehr viel beschränkter. Letztendlich müsse man zudem immer abwägen, zwischen einer schnellen Beendigung der Situation und dem Interesse an Beweissicherung. Die Kommunikation mit staatlichen Stellen sei bei einem IT-Sicherheitsvorfall zudem nicht zu unterschätzen. Es bestünden zahlreiche Meldepflichten die sich multiplizieren würden mit der Zahl der Staaten, in denen das Unternehmen tätig sei. Die Gemengelage verschiedener, oft recht kurzfristiger Fristen, dramatisierten die Lage.

Neben behördlicher Kommunikation müsse zudem extern kommuniziert werden. Allgemeine Strategie der Public Relations müsse es sein, Schadensbegrenzung zu betreiben. Verträge mit externen Agenturen könnten hilfreich sein. Dabei müsse immer abgewogen werden, zwischen der Verteidigung der eigenen Reputation und späteren Klagerisiken. Zudem müsse bei den oft komplexen Strukturen moderner Unternehmen bei jedem Vertrag mit dritten geprüft werden, ob der Dienstleiter oder Zulieferer hinreichende IT-Sicherheit betreibe und vor allem in welchen Fällen informiert werden müsse. Man gerate leicht in Konflikt mit gesetzlichen Meldefristen, wenn bei einem IT-Sicherheitsvorfall zuerst interne Aufklärung betrieben werden müsse.

Bei der internen Kommunikation sei es besonders wichtig, dass der Vorstand frühzeitig Risikomanagement betreibe. Arbeitsrechtliche Maßnahmen müssten in Abstimmung mit dem Aufsichtsrat frühzeitig veranlasst werden. Grob fahrlässig handelnde Mitarbeiter müssten zum Beispiel zeitnah angegangen werden. Auch arbeitsrechtliche Maßnahmen gegen Innentäter sollen bei einem Vorfall umgehend ergriffen werden.

Weiterhin müsse der Versicherungsstatus bei IT-Sicherheitsvorfällen geprüft werden. Welche Absicherung gegen Betriebsunterbrechungen oder welche Haftpflicht man abgeschlossen habe, sei oft höchst relevant für betroffene Unternehmen.

Im Fazit kam Braun zu dem Schluss, dass jedes Unternehmen entsprechende Expertise in der internen Rechtsabteilung vorhalten sollte. Externe Rechtsanwälte könnten durch ihre fachliche Expertise und Internationalität oft eine große Hilfe darstellen. Zudem hätten viele Erfahrung im Projektmanagement, welche bei einem IT-Sicherheitsvorfall von großen Vorteil sein könne.

(Wie) Lässt sich das transatlantische Privacy-Gap überwinden?

RECHTLICHE ENTWICKLUNGEN

Peter Schaar
Vorsitzender, Europäische Akademie für Informationsfreiheit und Datenschutz

Schaar zeigte in seinem Vortrag die Anforderungen des neuen EU-Datenschutzrechts an die Übermittlung personenbezogener Daten auf. Zudem sprach er über das Privacy Shield als das EU-US-Rahmenabkommen zum Datenschutz und dem Misstrauen beteiligter Akteure. Zu Beginn zeichnete Schaar die Entwicklung von „Small Data“, also der vorwiegend nationalen Datenverarbeitung und des Filetransfers zum Beispiel durch Datenträger hin zum heute aktuellen „Big Data“. Der Austausch von Daten sei allgegenwertig („Ubiquitous Computing“) und durch die Cloud entörtlicht. Daher funktioniere ein nationaler Schutz heute nicht mehr.

Zudem stehe einem nationalen Schutz die territorial beschränkte Durchsetzbarkeit von Gesetzen sowie die unterschiedlichen nationalen Rechtsrahmen und Datenschutzverständnisse entgegen. In der EU herrsche ein grundrechtbasiertes Verständnis zum Datenschutz vor, in den USA würden daher Daten als Eigentumstitel, die ggf. weitergegeben werden können, eingestuft. Ein Lösungsansatz sei bei der Lokalisierung von Daten anzusetzen. Die USA arbeiteten stark daran, Daten lokal zu verarbeiten. Daran müsse sich die EU ein Beispiel nehmen.

Daraufhin stellte Schaar zehn „Privacy Bridges“ als praktische Lösungsvorschläge vor. Hervorgegangen seien diese aus der 37. International Privacy Conference. Ausgangspunkt sei die Akzeptanz unterschiedlicher Rechtssysteme und Datenschutzkulturen. Sie seien besonders interessant für international arbeitende Unternehmen. Alle „Bridges“ befänden sich in einem online abrufbaren Bericht.

Die EU-Datenschutzrichtlinie RL 95/46/EG unterscheide zwischen der Datenübermittlung innerhalb der Mitgliedstaaten der Europäischen Union und der Übermittlung an Drittstaaten. Daten, die an Drittstaaten übermittelt würden,

seien besonders schutzbedürftig. Daher sei die Übermittlung grundsätzlich nur zulässig bei angemessenem Datenschutzniveau. Um dieses hinreichend zu definierte im Juli 2000 das Safe Harbour-Agreement, welches aus verschiedenen Gründen immer wieder neu diskutiert worden sei. Im Oktober 2015 annullierte der Europäische Gerichtshof dann schließlich Safe Harbour. Als Nachfolgeabkommen sei das EU-US Privacy Shield auf den Weg gebracht worden. Dieses ähnele strukturell zwar Safe Harbour, sei aber verbessert worden. Allerdings sei unklar, ob umgesetzt dieses Abkommen durchgesetzt werden würde, bei einer zu erwartenden „America first"-Politik.

Im Fazit betonte Schaar, dass die rechtlichen Anforderungen wichtig blieben. Allerdings müssten verschiedene Mechanismen durch Praktiken gefüllt werden. International agierende Unternehmen müssten einen Vertrauensrahmen schaffen, der robuster sei als ein Gesetz, welches sich immer wieder ändern könne.

IT-Sicherheitskatalog für Strom- und Gasnetzbetreiber nach § 11 Absatz 1a Energiewirtschaftsgesetz

KRITISCHE INFRASTRUKTUR

Andy Neidert
Referent Energieregulierung, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Neidert ordnete zu Beginn die gesetzliche Lage im Zusammenhang mit der Energiewirtschaft ein. Durch das IT-Sicherheitsgesetz seien KRITIS-Betreiber Mindestanforderungen unterworfen. Zudem bestehe eine Meldepflicht bei IT-Sicherheitsvorfällen. Grundsätzlich zuständig sei das BSI. Zusätzlich gebe es Spezialvorschriften im Energiewirtschaftsgesetz für KRITIS-Betreiber im Energiesektor. Betroffen seien Sonderformen in der Energiewirtschaft und auch im Bereich der Telekommunikation. Zuständig sei hier die Bundesnetzagentur. Ein wichtiger Unterschied sei, dass nach dem Energiewirtschaftsgesetz jeder Betreiber von KRITIS meldepflichtig sei, unabhängig von Grenzwerten.

Hervorgegangen aus § 11 Absatz 1a Energiewirtschaftsgesetz sei der IT-Sicherheitskatalog. Dessen Ziel sei es, die Anforderungen zur Gewährleistung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und EDV-Systeme, die für einen sicheren Netzbetrieb notwendig sind, festzuschreiben. Der IT-Sicherheitskatalog verpflichte die Netzbetreiber zur Gewährleistung eines angemessenen Sicherheitsniveaus für die von ihm identifizierten TK- und EDV-Systeme, die für einen sicheren Netzbetrieb notwendig seien. Es bedürfte eines ganzheitlichen Ansatzes im Sinne eines Informationssicherheits-Managementsystems (ISMS). Dieses lege fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).

Besonders wichtig sei die Festlegung eines Prozesses zur Risikoeinschätzung. Dessen Ziel sei es festzustellen, welches Risiko in Hinblick auf die Schutzziele für die von diesem Katalog erfassten Komponenten, Systeme und Anwendungen besteht. Orientieren solle sich die Einschätzung an den Schadenskategorien mäßig,

hoch und kritisch. Dabei solle „hoch“ Standard sein. Wenn mäßig gemeldet werde, müsse es ausführlich dokumentiert werden. Einen konkreten Schwellwert zur Einordnung in die drei Kategorien gebe es allerdings nicht.

Nach der Risikoeinschätzung müsse eine gut geplante Risikobehandlung folgen. Bei der Angemessenheitsprüfung einer Maßnahme sei insbesondere deren technischer und wirtschaftlicher Aufwand zu berücksichtigen. Dieser solle nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung eines sicheren Netzbetriebs stehen.

Die individuelle Umsetzung des Katalogs sei abhängig vom dem tatsächlichen Risiko. Daher war bereits bis November 2015 jeder Netzbetreiber dazu verpflichtet, einen Ansprechpartner für IT-Sicherheit zu benennen. So solle eine effiziente und schnelle Zusammenarbeit gesichert werden.

Die Umsetzung und Zertifizierung der Anforderungen aus dem IT-Sicherheitskatalog seien bis zum 31. Januar 2018 umzusetzen. Diese Frist sei bewusst kurz gewählt. Fristverlängerungen gegenüber den Netzbetreibern seien denkbar. Eine Native 27001-Zertifizierung reiche dabei nicht aus, da die Anforderungen des IT-Sicherheitskatalogs über die DIN ISO/IEC 27001 hinausgingen. Daher habe man in Zusammenarbeit mit der DAkkS ein eigenes Zertifikat entwickelt. Eine Akkreditierung bei dieser sei daher erforderlich.

Implikationen des IT-Sicherheitsgesetzes für Betreiber Kritischer Infrastrukturen im Energiesektor

KRITISCHE INFRASTRUKTUR

Arslan Brömme
National Information Security Officer Germany, Vattenfall GmbH

Brömme begann seinen Vortrag mit der Frage, was Authentizität sei. In der Praxis erleichtere das Verwenden von fremden Zugangsdaten oft einen Weg zum Ziel, weil keine Freigaben erteilt werden müssten. Jedem müsse klar sein, dass hier ein großes Problem vorliege. Authentizität sei nicht mehr gegeben, wenn Zugangsdaten kurzfristig weitergegeben würden. Daher sollten Unternehmen ein solches Fehlverhalten meldepflichtig machen.

Die aktuell auftretenden Top Level Threats im Bereich Terrorismus (von Individuen, Gruppen oder Staaten) um organisiertem Cybercrime setzten oft auf konstantes Monitoring von User(fehl)verhalten. Die Nutzer seien also kontinuierlich im Fokus der Angreifer. Anhand einer internen Statistik zeigte Brömme die Motivationen der Attacken auf Vattenfall im September 2016. Mehr als 80 Prozent seien dabei Cybercrime zuzuordnen. Staaten reagierten auf solche Zahlen mit der Einführung von nationalen und internationalen Cyber-Abwehrzentren und Programmen. Weiterhin besprach Brömme ausgewählte Vorfälle aus der Vergangenheit und kam zu dem Ergebnis, dass viele Hacks erst Jahre nach dem Hack bekannt würden. Um dem zu begegnen, müsse eine Balance zwischen Usability und Safety, zwischen der Bedrohung und der angemessenen Gegen-

maßnahme gefunden werden. Vattenfall habe dazu ein funktionelles ISMS gefunden, welches auf Grund des IT-Sicherheitsgesetzes auch ISO 27001 zertifizierbar sei. Die Implementierung sei vor allem ein Organisationsprozess in der rechtlichen Welt. Die Einbettung auf funktionaler Ebene verlaufe daraufhin oft nicht ohne Reibereien. Besonders der Bereich 24/7-Security sei hier zu nennen. Die Sicherheitsexperten wären keine Schichtarbeiter. Deren Qualifikation sei zu hoch. Daher müssten Arbeiter vor Ort einen Incident erkennen, um die gesetzliche Meldepflicht zu erfüllen. Klare Abläufe vereinheitlichen diesen Prozess. Bei einem Vorfall erfolge die interne Meldung unverzüglich aus der Schicht. Folgemeldungen könnten folgen. Die externe Abschlussmeldung erfolge allerdings immer über den Fachbereich IT-Sicherheit. Beim Erarbeiten solcher Abläufe müsse man zudem immer die eigenen Sicherheitszonen beachten. Vattenfall nutze ein fünfstufiges, flexibles Modell.

Im Fazit schloss Brömme damit, dass Offline heute keine Alternative sei. Transnationale Informationen seien wichtig für diverse Abläufe. Betreiber von KRITIS aus dem Energiesektor sollten grundsätzlich über eigene IT-Sicherheitszentren nachdenken.

Flugsicherung und die Frage der Verletzlichkeit – alte und neue Herausforderungen

KRITISCHE INFRASTRUKTUR

Osman Saafan
Director Safety & Security Management /CSO and Military Affairs,
DFS Deutsche Flugsicherung GmbH

Saafan stellte gleich zu Beginn seines Vortrags fest, dass die Luftfahrt nicht generell zu den KRITIS gehöre. Man müsse Forderungen im Zweifel eskalieren lassen, wenn man selbst bereits gut aufgestellt sei. Luftfahrt sei sicherer als man denke. Die DFS als privatrechtliches Unternehmen in Form einer GmbH sei bereits historisch gewachsen stark reguliert. Das heute multinational agierende Unternehmen beschäftige sich mit Cyber-Themen seit dem Aufkommen von Radartechnik. Diese sei leicht abzuhören oder zu stören gewesen. Man habe also bereits Dekaden Erfahrungen sammeln können. Heute sei man natürlich voll digital aufgestellt an allen Standorten. In Zukunft plane man einen zentralen Tower in Leipzig, von dem man per Remoteverbindungen viele Standorte fernsteuern könne. Dieser Effizienzgewinn bringe natürlich neue Anforderungen an die IT-Sicherheit mit sich. Man habe sich hier für einen risikobasierten Ansatz entschieden, weil man verstanden habe, dass ein abschließender Schutz nicht möglich sei. Zentrale Punkte seien daher Risiko- und Kritikalitätsbewertungen und eine kontinuierliche Überwachung (z.B. SIEM). Die Etablierung einer Sicherheitskultur im Unternehmen sei zudem unerlässlich. Leadership im Bereich Safety und Security stehe allem voran. Im Training müssten Awareness gesteigert und Innentäter enttarnt werden. Durch eine „Just Culture“ stelle man sicher, dass aus Vorfällen gelernt werden könne.

Organisatorisch nutze die DFS ein Schalenmodell. Bei diesem sei zentral, dass Systeme des inneren Kreises nur miteinander kommunizieren könnten, wenn diese Kommunikation über eine externe Firewall laufe.

Im Fazit stellte Saafan fest, dass an Vernetzung heute kein Weg vorbeiführe. Allerdings müsse man immer zwischen Schutz und Leistung abwägen. Systeme würden unter besonderer Berücksichtigung von Safety- und Security-Aspekten entwickelt: Design to Safety! Desing to Security! Dabei müsste immer das Zusammenspiel zwischen Redundanz und Diversifikation im Auge behalten werden. Die Etablierung einer funktionalen Sicherheitskultur sei eine zentrale Aufgabe.

Sicherheitsvorfallbehandlung in Zeiten von Cybercrime und Advanced Persistent Threats

PRAXISBERICHT

Dr. Tim Sattler
Group Information Security Officer /IT Compliance Manager, Jungheinrich AG

Sattler sprach über aktuelle Entwicklungen in der Bedrohungslandschaft der IT-Sicherheit aus der Perspektive eines Herstellers von Flurförderfahrzeugen. Die Firma Jungheinrich AG, die in Deutschland und China fertigt, stellt alles vom Gabelstapler bis hin zum voll automatisierten Hochregallager her. Daher sei man immer mehr auch ein Softwareunternehmen. Automatisierte Warehousesoftware oder Flottenmanagementlösungen gehören genauso zum Portfolio wie zum Beispiel Smartcard-Lösungen für Gabelstaplerfahrer. Über solche Systeme könne gesteuert werden, wer welchen Stapler fahren dürfte. In Zukunft wären zudem Smart Maintenance-Lösungen denkbar. Gabelstapler wären so zum Beispiel in der Lage selbst anzumelden, welches Ersatzteil bald fällig werden könnte.

Eine kritische Fähigkeit für eine effektive Reaktion auf Cyberangriffe sei kontinuierliche Incident response. Wie im militärischen Bereich habe man keinen ganzheitlichen Überblick, wer die Gegner seien. Daher müsse man sich auch von einem statischen Modell bei der Sicherheitsvorfallbehandlung verabschieden. Vorgehen im Sinne von Vorbereitung, Erkennung, Eindämmung und Nachbereitung seien nicht mehr zeitgemäß. Man sehe sich immer häufiger Advanced Persistent Threats (APT) ausgesetzt. Diese Angriffe richten sich gegen eine bestimmte Organisation und würden, falls erforderlich, auch in mehrere Schritte aufgeteilt. Die Angreifer seien dabei extrem gut vorbereitet, verfügten über ausreichend Zeit, Expertise und Ressourcen und würden ein Entdecken bis zum Erreichen ihrer Ziele oft erfolgreich vermeiden. Daher müsse die Fragestellung bei einem Sicherheitsvorfall sein: Wie entdeckt man Angriffe frühzeitig? Eine Lösung sei die proaktive Suche: Threat Hunting mit Threat intelligence. Motivierte Mitarbeiter müssen aktiv „auf die Jagd gehen“. Dabei sollten öffentliche Quellen wie PasteBin oder Twitter im Auge behalten werden. Mit dem Anlegen von ungenutzten Dummy-Accounts erstelle man sogenannte Honeypots/Honeytokens und könne so beobachten, ob jemand Zugriff auf diese Accounts nehme, indem man überwacht, ob es Aktivitäten gebe. Außerdem müsste sichergestellt werden, dass Beobachtungen Dritter zügig behandelt würden.

Bei der anschließenden Analyse sei Threat Intelligence Forensik gefragt. Verfügbare IT-Daten wie kompromittierte Hosts, Malware-Indikatoren, IP-Reputation, C&C-Infrastruktur, Phishing-Nachrichten, TTPs etc. müssten analysiert werden. Zur schnellen forensischen Analyse könnten Tools wie Endpoint Detection & Response (EDR) verwendet werden. Bei der anschließenden Bereinigung reiche es nicht, das System einfach neu aufzusetzen. Ob eine Bereinigung erfolgreich ist, könne zum Beispiel durch das Anlegen einer Zeitleiste der Ereignisse ermittelt

werden. Nach der Bereinigung müsse trotzdem weiter nach möglichen Rückständen gesucht werden. Nachbereitend sei es sinnvoll, die gewonnen Informationen mit einem vertrauenswürdigen Netzwerk zu teilen.

Zusammenfassend nannte Sattler als Erfolgsfaktor, dass mindestens eine Person für die Sicherheitsvorfallbehandlung in Vollzeit abgestellt werden müsse. Ressourcen müssten dahingehend optimiert werden, dass Prozesse automatisiert würden, wo immer dies sinnvoll möglich sei. Letztlich müsse die Sicherheitsvorfallbehandlung als eine kontinuierliche Aktivität verstanden werden.

Einführung einer klassifizierungsbasierten E-Mail-Verschlüsselungslösung im Konzern

PRAXISBERICHT

Uwe Betz
Director of Information Security (CISO), ROHDE & SCHWARZ GmbH & Co. KG

Betz argumentierte, dass E-mailverschlüsselung ein erstes Vehikel für weitreichendere IT-Sicherheitsmaßnahmen sein könne. Daher sei es sinnvoll, hier anzusetzen. Einleitend thematisierte er, warum E-Mailverschlüsselung in der Praxis bislang scheitere. Komplexität sei der Feind von Sicherheit. Anwender würden sich nicht mit der technischen Seite auseinandersetzen. Zudem gebe es verschiedene Verschlüsselungsmöglichkeiten, bei denen Absender und Empfänger kompatibel sein müssten. Authentizitätsprüfungen seien eine weitere Hürde.

Bei der Wahl der technischen Lösung müsse zwischen Anwenderfreundlichkeit und Sicherheit gewählt werden. Hier sei eine ganzheitliche, schutzbedarfsorientierte Betrachtung wichtig. Bei 95 Prozent der versendeten E-Mails gelte „keep it simple“, bei fünf Prozent „keep it secure“. Zudem müsse das Motto „Stop trying to fix the user“ lauten. Nicht der Nutzer sei das Problem, sondern oft schlechte Usability.

Weiterhin stellte Betz den Phasenplan zur Implementierung von verschlüsselten E-Mails vor. Bereits 2010 haben man begonnen, im Arbeitskreis ein Konzept zu erarbeiten. Über Phasen wie die Rezeption von Fachartikeln und Whitepapers und dem Hinzuziehen von externer Expertise, gelangte man im August 2012 in die Konzeptphase mit der Evaluation der Umsetzbarkeit. Das Executive Concept sei dann vom Top-Management verabschiedet worden. Dies sei ein kritischer Erfolgsfaktor, damit ein solches Projekt erfolgreich ist. Kern des Beschlusses sei eine erzwungene Klassifizierung. Diese werde durchgesetzt durch die Einbettung einer „Klassifizierungsauswahl” im E-Mail-Client auf dem Arbeitsplatzcomputer und das „bouncen” von nach extern verschickten, nicht klassifizierten E-Mails. So sei Verschlüsselung kein Selbstzweck mehr. Die risikobasierte Verschlüsselung basiere auf einer Anwenderklassifizierung. Dabei bestimme der Schutzbedarf das Schutzniveau. Dazu habe man vier Klassifizierungsstufen eingeführt: UNRESTRICTED als zur Veröffentlichung bestimmt und freigegeben und/oder aus öffentlicher Quelle stammend sei die erste Stufe. Darauf folge COMPANY RESTRICTED, welche geschäftliche Kommunikation ohne erhöhten Schutzbedarf (niedriges Schadpotenzial) beinhalte. Diese Stufe sei Standard. Die nächst vertraulichere Stufe, COMPANY CONFIDENTIA (mittleres/hohes Schadpotenzial),

und die vertraulichste Stufe STRICTLY COMPANY CONFIDENTIAL (sehr hohes Schadpotenzial) vervollständigen das Klassifizierungssystem. Die zuletzt genannte Stufe werde allerdings nur äußerst selten angelegt.

Im Fazit legte Betz die Vorteile einer Implementierung von Verschlüsselung auf die dargestellte Weise da. Durch die Implementierung in den E-Mail-Client der Mitarbeiter sei die Nutzung einfach. Durch die erzwungene Klassifizierung müssten sich alle Mitarbeiter täglich mit dem Thema auseinandersetzen. Das schaffe zusätzliche Awareness, auch in anderen Bereichen.

FRAGEN UND DISKUSSION

Die Frage, wie man Anwender in frühen Entwicklungsphasen dazu motivieren könne, die Verschlüsselung zu nutzen, beantwortete Betz damit, dass der Arbeitskreis zunächst geschlossen arbeitete. Die Sichtbarkeit für alle Anwender sei später hergestellt worden. Trotzdem habe man vor dem Launch bereits gemessen, wie und ob verschlüsselt wurde, um eine Quote zu ermitteln. Später habe man alle Anwender per E-Training geschult.

Auf die Frage, welche Tools zur Klassifizierung verwendet wurden antwortete Betz, dass diese in Ermanglung an Tools für Lotus Notes selbst geschrieben worden waren.

Die interne Umsetzung von Verschlüsselung sei die eine Seite. Allerdings müssten E-Mails, die von außen hereinkommen, auch verschlüsselt sein. Auf die Frage, wie man darauf reagiere antwortete Betz, dass dies natürlich nicht direkt gesteuert werden könne. Man würde nach außen kommunizieren, dass intern verschlüsselt würde. Messungen zeigten, dass die Zahl der eingehenden verschlüsselten E-Mails steigen würden.

IoT and Industrial Control Systems - Are they a risk to your business?

PARALLELE VORTRÄGE

Nigel Stanley
MSc (Lond.) CEng MIET MBCS MIEEE, Practice Director – Cyber Security, TÜV Rheinland

Stanley beschrieb zu Beginn die wirtschaftliche Entwicklung, welche heute in Industrie 4.0 ihren Höhepunkt gefunden habe. Der TÜV Rheinland arbeite an Themen der Industrie 4.0 in Deutschland sowie international und spezialisiere sich in Sicherheitsthemen und Cybersecurity sowie der Risikooptimierung.

Den Fokus seines Vortrags legte Stanley auf Geräte des Internet of Things (IoT). Das Vermeiden von Risiken bei der Einführung neuer Technologien habe oberste Priorität. Dies sei nicht immer einfach bei so großen Trends, wie der Maschine to Maschine-Kommunikation. Bereits 2015 hätten über 500 Millionen Geräte untereinander kommuniziert. In den nächsten fünf Jahren steige diese Zahl vermutlich auf über drei Milliarden Geräte an. Hinzu käme die „Bring your own Device“-Politik vieler Unternehmen. Ein diverses Feld an Geräten, die diverse

Zugriffsrechte hätten, sei schwer überschaubar und damit ein weiteres Einfallstor für Hacker.

Auch im medizinischen Bereich hielten IoT-Geräte Einzug. Die Verbindung von persönlichen Daten mit Clouddiensten ziehe Angreifer förmlich an. An einem Beispiel machte Stanley deutlich, welche Angriffsstrategien in diesem Bereich denkbar sein. Ein Krankenhaus habe eine Firma beauftragt, Altgeräte zu entsorgen. Diese verkaufte die Geräte allerdings auf Ebay anstatt sie zu recyceln. Hacker stellten daraufhin Patienten wieder her und boten sie im Internet zum Kauf an. Am Ende stand eine hohe Strafzahlung für das Krankenhaus an, welches in der Sorgfaltspflicht gewesen sei. Das Risiko hätte besser abgewägt werden müssen. Mit diesem Beispiel versuchte Stanley zudem noch zu verdeutlichen, dass Cybersecurity jeden CIO angehe.

Weiterhin verglich Stanley die Sicherheitsanforderungen an Corporate IT und Industrial IT. Die größten Unterschiede liegen in den möglichen Folgen. Diese seien bei der Industrie potentiell weitaus desaströser. Daher müsse für jedes Feld ein eigenständiger Sicherheitsplan entworfen werden. Zudem müsse man zwischen Safety und Cybersecurity unterscheiden. Jedes Feld biete ganz unterschiedliche Möglichkeiten, Risiken abzuschätzen. Der Standard IEC 62443 bringe beides zusammen und werde ständig weiterentwickelt.

Im Fazit kam Stanley zu dem Schluss: „It's all about (business) risk". Trends wie IoT und ICS dürften nicht ignoriert werden. Zur Risikobewertung und Zertifizierung solle man daher am besten auf einen erfahrenen, externen Dienstleiter zurückgreifen.

Cyber Defense Strategien im Kampf gegen Cyber Crime – mehr als eine Alibifunktion

PARALLELE VORTRÄGE

Kai Grunwitz
Senior Vice President Central Europe, NTT Security (Germany) GmbH

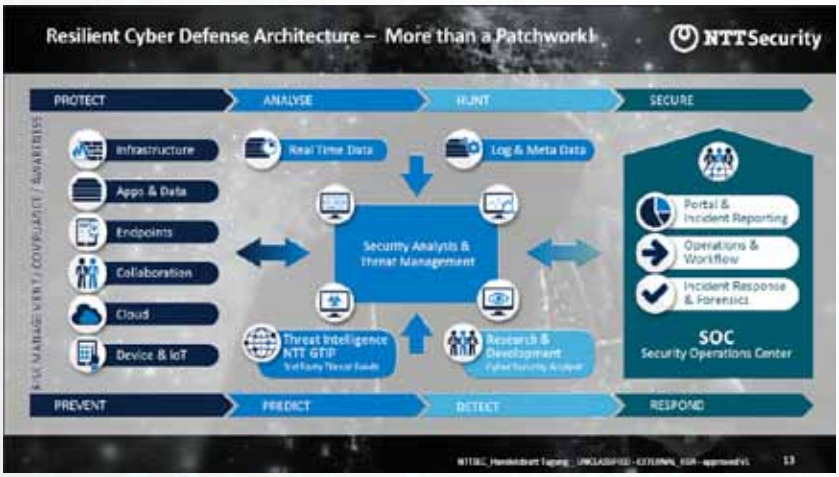
Herr Grunwitz stellt NTT Security als eines der größten globalen Informations- und Technologieunter-nehmen mit einem Gesamtumsatz von 105 Billionen Pfund vor. Das Unternehmen ist in 88 Ländern vertreten und hat 240.000 Mitarbeiter. 3,5 Billionen Pfund investiert NTT jährlich in Research und Entwicklung. Da die Sicherheitsrisiken von überall her kommen, ist es so wichtig, dass NTT auch überall vertreten ist. Um über 10.000 Kunden auf mehr als 6 Kontinenten vertreten zu können, verfügt NTT über mehr als 1.500 IT-Sicherheitsexperten, die weltweit verteilt sind. In mehr als 10 SOCs und 7 Entwicklungszentren werden mehr als 3,5 Trillionen Logs jährlich weltweit analysiert.

Herr Grunwitz macht auf den IT-Sicherheitsreport des World Economic Forums vom Februar 2016 aufmerksam. Dieser Report definiert ein „globales Risiko" als ein unsicheres Ereignis oder einen Zustand, der, wenn dieser eintritt, signifikante negative Auswirkungen auf verschiedene Länder oder Industrien in den nächsten 10 Jahren haben kann. Welche Risiken dies sein können, stellt Herr Grunwitz in seiner nächsten Folie dar: neben wirtschaftlichen, sozialen, umwelt- und geo-politischen Risiken sind es vermehrt technologische Risiken und dabei insbesondere Cyberattacken, die ein globales Risiko mit der höchsten Auswirkung

für Wirtschaftsunternehmen darstellen. Neben Nordamerika ist insbesondere Europa diesem Risiko verstärkt ausgesetzt.

Dabei findet der Cyberkrieg ohne Soldaten, Gewehre, Spione oder Raketen statt. Cyber-Attacken gelten hauptsächlich der Industrie, der Finanzbranche, dem Handel und der Produktion.

Da es zu spät ist, als Unternehmen erst dann zu reagieren, wenn man bereits im Fokus von Cyberattacken steht, muss jetzt gehandelt werden. NTT stellt daher die folgende „unverwüstliche“ Cyberabwehr Architektur vor:



In Ergänzung dazu weist Herr Grunwitz darauf hin, wie wichtig ein Incident Response Plan ist, der regelmäßig in der Praxis getestet und verifiziert werden sollte, um schnell in Notsituationen reagieren zu können. Folgende Punkte sollte ein robuster Incident Response Plan unbedingt enthalten:

- Strukturierte Handlungsanweisungen für den Fall eines Incidents (Vorbereitung, Identifikation, Eindämmung, Abhilfe und Wiederherstellung)
- Verbindung zur Business Continuity Planung (BCM)
- Kommunikationsplan nach außen und nach innen.

Supply Chain Security – Es ist Zeit für echten Fortschritt

PARALLELE VORTRÄGE

Ulf Feger
Chief Security Officer, HUAWEI TECHNOLOGIES Deutschland GmbH

Feger stellte die Herausforderungen an die Sicherheit und den Aufbau einer globalen IT-Infrastruktur im Bezug zu einer sicheren globalen Lieferkette mit entsprechendem Risikomanagement heraus. Diese sei für den wirtschaftlichen Erfolg eines Unternehmens unerlässlich und werde fundamental unterschätzt. Wichtig sei zudem der Kontext, in dem eine weltweite Lieferkette anzusehen sei. In Europa würde zum Beispiel bei einer verspäteten Lieferung der Ausfall eines Standorts primär monetär in Erscheinung treten. In Südamerika könnte beispielweise Diebstahl eine bedeutendere Rolle spielen, im asiatischen Raum die Piraterie. Je nach Lieferort liegen unterschiedliche Risikofaktoren vor. Auch

problematisch können Manipulationen an Produkten auf dem Lieferweg sein. So könnten zum Beispiel Angreifer Wanzen in fabrikneue Anlagenteile schmuggeln. Diese würden dann oft für mehr als zehn Jahre fest erbaut. Im Zweifel kämen auf den Hersteller immense Kosten zu, um einen solchen Fehler zu korrigieren. Ziel müsse der Aufbau eines Lieferkettenmanagements für sichere Produkte und Komponenten sein, um Zwischenfälle dieser Art zu vermeiden.

Weiterhin stellte Feger die Firma Huawei vor. Der international agierende Großkonzern sehe sich ständig mit vielen verschiedenen Kulturen, die teilweise sehr unterschiedliche Vorstellungen von Sicherheit hätten, konfrontiert. Die drei Geschäftszweige EBG (Enterprise), CNBG (Carrier) und CBG (Consumer/Devices) des Unternehmens zeigten zudem die Herausforderungen, vor denen man stehe. Die globalen Lieferketten seien auch divers. Keineswegs würde alles in China hergestellt, obwohl dort natürlich ein großer Schwerpunkt liege. Viele Teile würden durch Huawei in der ganzen Welt eingekauft. Die USA zum Beispiel seien der größte Ressourcenlieferant. Durch die Verkettung all dieser Umstände seien die Anforderungen an eine sicher funktionierende, globale Lieferkette sehr hoch. Auf World-Ebene Huaweis werde die Strategie dazu entwickelt und dann an die nationalen Vertretungen kommuniziert. Ein transparenter, auditierbarer Logistikprozess werde angestrebt. Dabei finde das Monitoring über die KPIs statt. Die Internal Compliance gebe vor, dass alles auditiert werden solle.

Abschließend fasste Feger zusammen, dass es am wichtigsten sei zu erkennen, dass die Lieferkette ein Risikofaktor sei. Die Bedeutung der Cyber-Sicherheit als übergreifendes Thema der Supply Chain Security müsse mitgedacht werden. Risikofaktoren seien nicht nur potentielle Innentäter. Auch Hersteller und Lieferanten müssten kritisch betrachtet werden. Am Ende müsse man sich immer die Frage stellen, wie ein Produkt sicher und vertrauenswürdig hergestellt und geliefert werden könne, wenn Komponenten verschiedenster (globaler) Hersteller verwendet würden.

Cyber-Risiken – Versicherung als Teil des Risikomanagements Typische Cyber Angriffe

PARALLELE VORTRÄGE

ppa. Markus English
Enterprise Risks Underwriting Manager, Tokio Marine Kiln

Herr English stellt zu Beginn seines Vortrages verschiedene Quellen für Cyberattacken und Sicherheitsvorfälle vor: Hacker können dahinter stecken oder auch Staaten oder kriminelle Banden. Manche Sicherheitsvorfälle werden aus Spaß begangen oder durch verbrecherische Angestellte verübt. Ein weiterer Grund kann aber auch menschliches Versagen sein.

Cyberattacken entstehen durch Malware, was sich darin äußert, dass Services verweigert werden, Lösegeld erpresst wird, durch Phishing ein Identitätsdiebstahl verübt wird oder sich durch Social Engineering unerlaubt Zugang zu Firmendaten verschafft wird.

Als bekannter Cybervorfall erinnert Herr English an Ashley Madison. Dieses jüngst von einem Hackerangriff erschütterte Portal wurde nach Aufdecken des Datenlecks von ihren Nutzern verklagt. Die Opfer des Datenlecks verlangen 500 Mio. Dollar Schadenersatz, weil sie zu spät über den Daten-Diebstahl informiert wurden. Die Schadenersatzklagen könnten durch Cyber-Policen von Axis und D&O-Versicherungen von AIG gedeckt sein.

Die IT-Architektur spielt bei der Abwehr von Cyberrisiken eine maßgebliche Rolle. Allerdings ist mit Fortschreiten von Industrie 4.0 Anwendungen die Komplexität dieser Architekturen immer weiter gestiegen. Gerade im Mittelstand kommen Sicherheitsaspekte in der Kommunikation Machine-to-Machine (M2), der industriellen Ausprägung des Internet der Dinge oftmals zu kurz, warnt die nationale Initiative für Informations- und Internet-Sicherheit (NIFIS).

Die gefährdetsten Branchen in Deutschland sind die Automobil-, die Chemie- und Pharmabranche, das Finanz- und Versicherungswesen, die Gesundheitsbranche, der Bereich Medien und Kultur, der Handel sowie die IT- und Telekommunikationsbranche. Dabei ist der Mensch durch Social Engineering eine der größten Schwachstellen.

Herr English stellt heraus, dass Risikomanagement und Cyber Risikomanagement in Deutschland Organaufgabe ist. Nach dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sind Aktiengesellschaften (AGs) in Deutschland gesetzlich zur Risikofrüherkennung, einem Teilbereich des Risikomanagements, verpflichtet, um den Erhalt des eigenen Unternehmens sicherzustellen.

Cyber-Versicherungen, die hauptsächlich aus den USA kommen, können in der Zukunft eine wichtige Rolle dabei spielen. In Deutschland ist dies noch eine junge Sparte, die kein einheitliches Deckungskonzept im Markt hat. Viele Versicherer mit anglo-amerikanischen Wurzeln setzen den Schwerpunkt auf den Haftpflichtteil mit Eigenschaden-Annex. Andere Versicherer haben einen Ansatz aus der Sach- bzw. Technischen Versicherung mit Gefahrendefinition und Kostendeckungen. Bedingungswerke sind nicht oder schwer vergleichbar, aber ein modularer Aufbau der Bedingungswerke scheint sich durchzusetzen.

Die Bewertung des Risikos bleibt weiterhin schwierig. Für den Risikoträger ist dies aber unabdingbar, denn der Betriebsunterbrechungsschaden muss abgeschätzt werden. Dabei müssen IT-Mindeststandards eingehalten werden.

Herr English erklärt den Ansatz von Tokio Marine Kiln. Das Deckungskonzept ist modular aufgebaut mit den Modulen.

EIGENSCHADEN

Betriebsunterbrechung: Einnahmeausfälle und Unterbrechungskosten (Dabei ist der zeitliche Selbstbehalt individuell zu vereinbaren)

Wiederherstellungskosten: Versichert sind alle Kosten und Sonderausgaben welche nötig sind, digitale Daten und Programme der versicherten Unternehmen wiederherzustellen, inklusive forensische Kosten

Cyber-Erpressung: Erpressungsgelder und Erpressungskosten werden von TMK gestellt bzw. übernommen, nach schriftlicher Zustimmung durch TMK

Diebstahl von Betriebsgeheimnissen/Industriespionage: Verlust von „geistigem Eigentum“ durch einen erfolgreichen Cyber-Diebstahl ist versichert.

Cyber-Terrorismus-BU: BU bei zielgerichteten Cyber-Angriffen welche unter einem üblichen Terror-Ausschluss nicht versichert wären

Imageverlust: Markenwertverlust und verminderte Einnahmen der VUs aufgrund eines Imageschadens welcher durch eine Datenpanne bzw. eine Datenrechtsverletzung hervorgerufen worden ist

DECKUNGSKONZEPT

Drittschaden/VH: Multi-Media-Haftung: Versichert sind Ansprüche wegen Rechtsverletzungen durch fehlerhafte Veröffentlichungen auf den Homepages der VUs, durch Mitarbeiter oder Dritte (Hacker)

Datenschutzhaftpflicht und Netzwerksicherheit: Ansprüche aufgrund einer Datenschutzverletzung welche die Versicherten zu vertreten haben

Behördliche Datenschutzverfahren/Verteidigungskosten/Meldekosten

„Breach-Response"- (Reaktion auf Datenverletzung) und Krisenmanagementkosten

PCI -Bußgelder und Strafen (Payment Card Industry): Versichert sind Ansprüche aufgrund Nichteinhaltung von PCI-Datensicherungsstandards im Rahmen der elektronischen Datenverarbeitung durch ein VU

Herr English stellt abschließend heraus, dass die Cyber Versicherung einen großen Mehrwert für ein Unternehmen darstellt. Tokio Marine Kiln ist eine solche weltweit arbeitende Versicherung, die neben vielen anderen Sparten insbesondere auch den Bereich Enterprise Risk abdeckt. Durch operationelle Niederlassungen in Europa haben die Kunden in Europa direkten Zugang zur kompletten Produktpalette von Tokio Marine Kiln.

SIE HABEN EINEN THEMENVORSCHLAG FÜR DIE NÄCHSTE JAHRESTAGUNG CYBERSECURITY?

Dann melden Sie sich gerne bei:

Elke Schneider, Conference Director
+49 (0) 2 11/96 86-35 19
elke.schneider@euroforum.com

konferenz.de/cybersecurity

www.twitter.com/itk_live #hbcyber

www.facebook.com/euroforum.de

www.euroforum.de/news

Wir danken Fabian Wiedenbruch für die Zusammenfassung der Inhalte.