MANAGEMENTKOMPASS

02
2015

Digital Security

TREND
Transformationsdruck schafft Fakten

THINK TANK
Den richtigen Schritt voraus

PRAXIS
Cyberangriffe erkennen und angemessen reagieren

FRANKFURT BUSINESS MEDIA
DER F.A.Z.-FACHVERLAG

sopra steria
CONSULTING

Urs M. Krämer
CEO
Sopra Steria Consulting

„Das Thema Cybersicherheit steht spätestens seit Edward Snowden ganz oben auf der Management-agenda. Denn die Schäden durch Sicherheitsdefizite nehmen ein immer größeres Ausmaß an – ob bei Unternehmen oder Behörden. Gleichwohl verdrängen nach wie vor viele Verantwortliche diese Risiken. Umso wichtiger ist es für IT-Entscheider zu wissen, wie sich IT-Sicherheit und Informationsschutz in der eigenen Organisation weiter verbessern lassen."

VORWORT

© Frank Rumpenhorst/Bundesbank

Dr. Andreas Dombret
Mitglied des Vorstands der Deutschen Bundesbank

„Das Bewusstsein für digitale Risiken scheint mir noch nicht in allen Führungsetagen von Banken vorhanden zu sein. Hier gilt es, dringend aufzuholen und den Schutz der IT-Systeme und Kundendaten deutlich zu verbessern."

Dr. Ralf Schneider
CIO der Allianz-Gruppe

„Bei Cyberangriffen geht es heute nicht mehr um partielle Geschäftsverluste, sondern um die Reputation bei einem Datenverlust. Das Vertrauen ist die wichtigste Geschäftsbasis unseres Konzerns. Aber egal welche Größe ein Unternehmen hat, es muss ein funktionierendes Risiko- und Security-Management besitzen."

Derzeit vertieft sich in Industrie, Wirtschaft und Gesellschaft ein Zielkonflikt: Digitale Sicherheit versus Effizienzsteigerung und Funktionalität. Die sich schnell verdichtende Vernetzung in Unternehmen, Behörden, Forschungseinrichtungen und kritischen Infrastrukturen (KRITIS) erhöht die Risiken digitaler Angriffe und Bedrohungen.

Tatsächlich nimmt der Diebstahl von Know-how, Daten und Identitäten ebenso zu wie Spionage, Sabotage und Erpressung. Die Folgen können Ausfälle und Unterbrechungen des geregelten Betriebs, der Verlust erfolgskritischer Informationen an direkte Wettbewerber oder internationale Plagiatoren sowie Beschädigungen der Kundenbeziehungen und der Marktposition sein.

Wirksamem Schutz aber stehen häufig Schwächen der IT-Systeme, der digitalen Geschäftsprozesse und der Kommunikationswege entgegen. Erschwerend kommt die weitverbreitete Sorglosigkeit der Mitarbeiter bei der Nutzung mobiler Endgeräte und sozialer Netzwerke für ihre Arbeit hinzu.

Für Wettbewerbsfähigkeit und künftigen Geschäftserfolg sind die Etablierung und Umsetzung eines umfassenden, unternehmensweiten Sicherheitsmanagements und der zugehörigen Mitarbeitersensibilisierung ganz zentrale Faktoren.

Deshalb zeigt dieser Managementkompass, welche Bereiche derzeit besonderer Aufmerksamkeit der Unternehmensleitung bedürfen und mit welchen Maßnahmen zur intelligenten Prävention und Schadenbegrenzung Entscheider die digitale Sicherheit auf technischer Ebene ebenso erhöhen können wie im operativen Tagesgeschäft.

Sopra Steria Consulting

FRANKFURT BUSINESS MEDIA

SICHERHEIT IST CHEFSACHE

Wo 100-prozentige Sicherheit reines Wunschdenken ist, wird Risikominimierung zum Muss. Klare Richtlinien der Geschäftsleitung aber können nur greifen, wenn in der Umsetzung alle digitalen Einrichtungen, Geräte und Anwendungen auf allen Ebenen berücksichtigt sind. Denn Bedrohungspotenzial verbirgt sich oft auch in Teilprozessen. Wichtigste Grundlage für unternehmerischen Selbstschutz sind daher Transparenz und Achtsamkeit.

1 | » MANAGEMENTEMPFEHLUNG

Digitale Sicherheit ist erfolgskritischer denn je. Entwickeln Sie daher Ihre unternehmensspezifische IT-Sicherheitsstrategie, und verankern Sie das IT-Sicherheitsmanagement als operativen Verantwortungsbereich in der Geschäftsleitung.

Ob Sie aus Ihrem jetzigen CIO einen „Chief Information Security Officer" (CISO) oder CDO (Chief Digital Officer) machen, eine ganz neue Stelle schaffen oder die Position übergangsweise als Vorstand oder Geschäftsführer selbst ausfüllen, ist erst einmal unerheblich. Wesentlich ist, dass Sie eine ganzheitliche Sicherheitsstrategie aufsetzen und die Sicherheitsinitiativen Ihres Unternehmens vorankommen – über alle Geschäftsbereiche hinweg und gut abgestimmt ineinander greifend. Zu den Aufgabenbereichen eines CISO gehören die Erarbeitung und Durchsetzung von Richtlinien ebenso wie die Steuerung und Überwachung aller sicherheitsrelevanter Maßnahmen. Weitere wichtige Aufgabenfelder sind die Verantwortung für das Identitäts- und Zugriffsmanagement, Datenschutz, Datenforensik, das Notfallmanagement und die Sicherstellung der Betriebskontinuität.

2 | » MANAGEMENTEMPFEHLUNG

Ziehen Sie die Etablierung eines wirklich umfassenden Schutzsystems in Betracht. Da die Einhaltung gesetzlicher Regeln (Stichwort: Compliance) in der haftbaren Verantwortung der Geschäftsleitung liegt, bringt Ihnen ein wirksames revisionssicheres Informationssicherheitsmanagementsystem (kurz ISMS) auch ein hohes Maß an Rechtssicherheit.

Ein ISMS, das der Norm ISO/IEC 27001 entspricht, ist ein standardisiertes System zur Definition, Steuerung, Kontrolle und kontinuierlichen Optimierung der Informationssicherheit. In jedem Fall müssen Sie für eine komplette Sicherheitsstrategie von Anlagenschutz bis Zahlungssystem alle technischen Mittel, Geschäftsprozesse, Arbeitsabläufe und Kommunikationsgewohnheiten unter die Lupe nehmen. Jenseits des Risikos digitaler Angriffe gehört auch der physische Schutz Ihrer IT- Infrastruktur dazu, also die Absicherung gegen Feuer, Wasser, Überspannung, Erschütterungen, höhere Gewalt sowie die Zugangskontrolle Ihrer Betriebs- und Serverräume oder der Rechenzentren. Ein weiterer, häufig ignorierter Faktor sind IT-basierte Prozesse und Arbeitsabläufe. Welche Programme/Anwendungen sind im Einsatz? Wer kennt sich damit aus? Kann es passieren, dass wichtige Updates schiefgehen, bestimmte Prozesse lahmliegen und der einzige Kompetenzträger nicht verfügbar ist? Als Führungskraft sollten Sie sich hierüber einen Überblick verschaffen.

3 | » MANAGEMENTEMPFEHLUNG

Sensibilisieren und schulen Sie Ihre Mitarbeiter. Denn mangelndes Sicherheitsverständnis und Sorglosigkeit bei der digitalen Kommunikation sind akute Bedrohungen für Ihr Unternehmen.

Über die Hälfte der 2014 von Wirtschaftsspionage, Sabotage und Datendiebstahl betroffenen deutschen Unternehmen gibt als Täter und/oder Türöffner aktuell oder ehemals Beschäftigte an. Dahinter verbirgt sich jedoch längst nicht immer Böswilligkeit, sondern eher eine zu gering ausgeprägte Sensibilität für Risiken. Davon profitieren unter anderem die Auftraggeber von Social-Engineering-Attacken, die seit etwa zwei Jahren immer häufiger einzelne Mitarbeiter manipulieren, die den Angreifern dann unabsichtlich den Zugang zu unternehmensinternen Systemen ermöglichen. Zur Schaffung einer Sicherheitskultur müssen Mitarbeiter auch zu eigentlich weithin bekannten Risikofaktoren wie etwa WLAN-Nutzung, Passwörtern, externen Datenträgern etc. regelmäßig geschult werden.

4 » MANAGEMENTEMPFEHLUNG

Kümmern Sie sich um das Identitäts- und Rechtemanagement und damit um den Zugangsschutz Ihrer Systeme und Datenbanken. Experten empfehlen eine granulare Zugriffsregelung, die klar definiert und kontrolliert, wer welche Informationen unter welchen Umständen sehen kann und was der einzelne Mitarbeiter damit tun darf und soll.

In größeren Unternehmen und solchen, die viel mit externen IT-Dienstleistern arbeiten, kann der zusätzliche Einsatz einer PAM (Privileged Access/Activity Monitoring)-Lösung zur Überwachung von Anwendern mit besonderen Zugriffsrechten wie Administratoren sinnvoll sein. Anders als Log-Management und SIEM-Lösungen dokumentieren solche Systeme nicht nur das Ergebnis einer Aktion in den Firmensystemen, sondern zeigen auch genau auf, welche Aktionen ein Anwender wie durchgeführt hat. Da sich PAM-Überwachungswerkzeuge die Informationen für ein Audit aus der direkten Kommunikation zwischen Client und Server holen, können die Daten selbst von einem Anwender/Administrator mit umfassenden Rechten nicht im Nachhinein manipuliert werden. Ursache und Wirkung sind also immer transparent, was für datenforensische Ermittlungen (etwa bei rechtlichen Auseinandersetzungen) praktisch ist.

5 » MANAGEMENTEMPFEHLUNG

Entwickeln Sie gemeinsam mit den IT- und Sicherheitsverantwortlichen ein umfassendes Notfallmanagement. Nur so können Sie sicherstellen, dass im Schadenfall alle Systeme und Geschäftsbereiche schnell wieder arbeitsbereit sind.

Wenn Daten abfließen, Systeme und Onlineshops zum Erliegen kommen oder die Produktion unterbrochen wird, weil Angreifer die Sicherheitsabwehr Ihres Unternehmens durchbrochen haben, müssen Sie schnell handeln können, um den Schaden zu begrenzen. Dabei helfen sogenannte Disaster-Recovery- und Business-Continuity-Lösungen, vor allem aber klar geregelte Abläufe. Bisher sind solche Notfallpläne nur bei etwa 49 Prozent der deutschen Unternehmen im Einsatz – und das, obwohl mehr als die Hälfte der befragten Organisationen bereits schmerzliche Erfahrungen mit Sabotageakten und Datendiebstahl gemacht haben. Die Folge sind Know-how-Verlust, Plagiate und Patentverletzungen, Umsatzeinbußen, Versorgungsengpässe und viele andere geschäftsschädigende Vorfälle.

6 » MANAGEMENTEMPFEHLUNG

Schützen Sie die offenen Flanken von Smartphones, Tablets und deren Apps. Viele der App-bezogenen Informationen laden zu Identitätsdiebstahl und Manipulation förmlich ein.

Eine Untersuchung der 10.000 beliebtesten Android-Apps durch die Forscher des Fraunhofer-Instituts AISEC ergab unter anderem, dass zwei Drittel der mobilen Anwendungen Daten unverschlüsselt an Server in aller Welt verschicken. Dazu gehören auch zahlreiche Businessanwendungen. Sie sollten also dringend überprüfen, ob Ihre Mitarbeiter Apps verwenden, die dem Datenmissbrauch und -diebstahl möglicherweise Tür und Tor öffnen. Für Hacker ist es nicht sonderlich schwierig, unsichere WLAN-Netze und Apps für den Direktabgriff von Informationen zu nutzen und später in die Netzwerke von Unternehmen vorzudringen. Führen Sie daher schnellstmöglich klare Richtlinien für das mobile Arbeiten und das Mitarbeiterverhalten unterwegs ein. Mit virtuellen Desktops und Datenspeicherung in der Cloud können Sie die Risiken mobiler Endgeräte übrigens deutlich minimieren, ohne die Flexibilität und den Anwendungskomfort Ihrer Mitarbeiter einzuschränken.

BUCH & WEB

FACHLITERATUR

Sachar Paulus (Hg):
Praxis des Security Managements. Status Quo. Anwendung. Werkzeuge. open source press 2015.

Die Aufsatzsammlung wendet sich an alle, die in der beruflichen Praxis mit Fragen und Aufgaben der Informationssicherheit konfrontiert sind und einen Einstieg in das Thema suchen. Ein wissenschaftlicher Querschnitt aus dem Forschungsbereich „Sicherheitsmanagement" gibt einen guten Überblick, wobei konkrete Szenarien im Vordergrund stehen. Das Themenspektrum reicht von Securitymanagement as a Service über Datenschutzzertifikate , Sicherheitsmechanismen in Datenbanken bis hin zur Messbarkeit von Informationssicherheit.

Gerhard Klett, Heinrich Kersten:
Mobile IT-Infrastrukturen. Management, Sicherheit und Compliance. mitp 2015.

In diesem Buch geht es um die komplexen IT-Prozesse und ihre Anpassungen, wenn mobile IT-Strukturen im Unternehmen geschaffen werden. IT-Sicherheit ist dabei ein wichtiges Thema. Die Autoren erklären unter anderem, wie sich eine Schatten-IT vermeiden lässt und mit welchen Sicherheitsmaßnahmen mobile IT-Infrastrukturen ausgestattet sein müssen, damit keine gravierenden Schwachstellen auftreten. IT-Governance und Datenschutz im Zusammenhang mit der mobilen IT-Infrastruktur sind weitere Themenschwerpunkte.

LINKS

» **www.bsi.de**
Die Internetseite des Bundesamts für Sicherheit in der Informationstechnik bietet vielfältige Informationen auch in Form von Checklisten, die für die Umsetzung einer IT-Sicherheitsstrategie in Unternehmen hilfreich sein können.

» **www.bitkom.org**
Der Digitalverband Deutschland verfügt über eine Themenseite Vertrauen & Sicherheit, die Ihnen einen guten Überblick über die aktuellen Themen und Veranstaltungen liefert.

» **www.it-sicherheit-in-der-wirtschaft.de**
Die Initiative ist im Bundesministerium für Wirtschaft und Energie angesiedelt. Sie gibt aktuelle Tipps zum Thema IT-Sicherheit und verfügt über einen IT-Sicherheitsnavigator, der einen ersten Überblick über herstellerneutrale Initiativen gibt.

» **www.jura.uni-passau.de/sicherheitsrecht-internetrecht/forschung/baywidi/**
Hilfreiche Tipps bietet neuerdings das Bayerische Wissensnetzwerk Digitale Infrastrukturen, IT-Sicherheit und Recht für Unternehmen (BayWiDI).

» **www.dvs-schutzverband.de**
Der Deutsche Versicherungs-Schutzverband e.V. bietet unter anderem Informationen rund um Cyberversicherungen.

Udo Bub, Klaus-Dieter Wolfenstetter Hrsg.:
Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing. Springer Vieweg 2014.

Der Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT-Sicherheit richtet sich unter anderem an Verantwortliche für IT-Managementsysteme und IT-Governance. Namhafte Forscher und Praktiker beschäftigen sich mit Sicherheit im Internet der Dinge und im Cloud Computing, aber auch die Verantwortung zwischen Gesetzgebung und Wirtschaft wird in einem eigenen Beitrag thematisiert.

Joachim Dorschel Hrsg.:
Praxishandbuch Big Data. Wirtschaft- Recht –Technik. Springer Gabler 2015.

Dieses Praxishandbuch bietet einen Überblick der möglichen Anwendungsfelder und der rechtlichen Rahmenbedingungen von Big Data. In einem eigenen Kapitel „Recht" wird ausführlich auf die Bereiche Datenschutz, Leistungsschutz und Integritätsschutz eingegangen. Hier geben die Autoren praktische Hinweise, wie Big-Data-Anwendungen nach geltendem Recht umgesetzt werden können und wie dabei der technische und organisatorische Aufwand minimiert werden kann.

GLOSSAR

Advanced Persistent Threat
Deutsch: fortgeschrittene, andauernde Bedrohung. Bezeichnet einen komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden oder Unternehmen, die aufgrund ihres Technologievorsprungs potenzielle Opfer darstellen oder als Sprungbrett auf dem Weg zu solchen Opfer dienen können.

Compliance
Steht für die Einhaltung von Gesetzen und Richtlinien, aber auch von freiwilligen Kodizes, in Unternehmen.

Cookie
Textinformation, die eine besuchte Website über den Browser im Rechner des Betrachters (Client) platziert. Der Client sendet die Cookie-Information bei späteren, neuen Besuchen dieser Seite mit jeder Anforderung wieder an den Server. So kann bei einer Webanwendung, deren Interaktion mit dem Nutzer über mehrere Seitenaufrufe andauert, eine eindeutige Session-ID gespeichert werden.

Data-Leak/Leakage-Prevention
Schutz gegen ein vermutetes, aber nicht messbares und manchmal auch im Einzelfall gar nicht feststellbares Weitergeben von Informationen an unerwünschte Empfänger.

Data-Loss-Prevention
Schutz gegen den unerwünschten Abfluss von Daten, der Schaden verursacht und auch bemerkt wird.

Denial-of-Service-Attacke (DoS-Attacke)
Belastet den Internetzugang, das Betriebssystem oder die Dienste eines Hosts mit einer größeren Anzahl Anfragen, als diese verarbeiten können. Reguläre Anfragen können dann gar nicht oder nur sehr langsam beantwortet werden. Bei einer DoS-Attacke dringt der Angreifer nicht in den angegriffenen Computer ein.

Distributed-Denial-of-Service-Attacke (DDoS-Attacke)
Eine DDoS-Attacke wird mit Hilfe von Backdoorprogrammen durchgeführt, die mittels Computerwürmern auf nicht ausreichend geschützten Rechnern installiert werden. Sie versuchen selbständig, weitere Rechner im Netzwerk zu infizieren, um so ein Botnetz aufzubauen.

Industrie 4.0
Strategie der Bundesregierung zur Digitalisierung der Industrie. Technische Grundlage sind in Maschinen eingebettete IT-Systeme und deren Vernetzung. Ziel ist die intelligente Fabrik (Smart Factory).

Internet der Dinge
Sensoren, Sicherheitskameras, Fahrzeuge und Produktionsmaschinen kommunizieren miteinander über das Internet, ohne dass Menschen dabei involviert sind.

Intrusion-Detections-System (IDS)
System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken erhöhen.

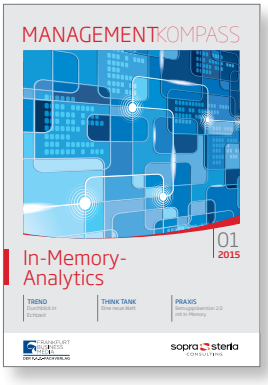
IT-Sicherheitsstrategie
Strategie zur Planung, Gewährleistung und ständigen Aufrechterhaltung der IT-Sicherheit, sollte generell immer mit einer eigenen Jahresplanung mit Budgetierung im Rahmen der unternehmensinternen Planungsprozesse verankert sein.

Log-Management
Das Verwalten von Log-Daten, die Änderungen an Computersystemen protokollieren. Unternehmen sind vielfach verpflichtet, ein Log-Management umzusetzen, um diversen internationalen Standards zu genügen.

Penetrationtest
Umfassender Sicherheitstest von möglichst allen Systembestandteilen und Anwendungen eines Netzwerks- oder Softwaresystems mit Mitteln und Methoden, die ein Angreifer (ugs. „Hacker“) anwenden würde, um unautorisiert in das System einzudringen (Penetration). Der Penetrationtest ermittelt somit die Empfindlichkeit des zu testenden Systems für derartige Angriffe.

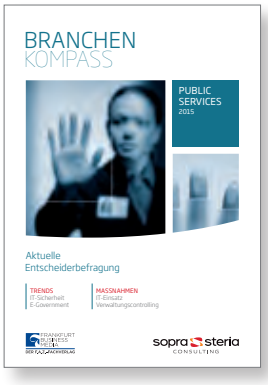
Security Information and Event Management (SIEM)
Umfasst dass Management von Sicherheitsbedrohungen und das Erstellen und Erfassen von Protokolldateien für Audits zur Konformität von internen und/oder externen Vorgaben über Sicherheitslücken.

AKTUELLE STUDIEN



Managementkompass
In-Memory-Analytics

Um die wachsenden Datenströme erfassen und sinnvoll für die eigene Geschäftsentwicklung nutzen zu können, müssen Unternehmen immer mehr unterschiedlich strukturierte Informationen verarbeiten können – und dies möglichst in Echtzeit. Dieser Managementkompass zeigt, welche Möglichkeiten der Wertschöpfung In-Memory-Technik Unternehmen bietet.



Branchenkompass
Public Services

Befragung von 100 Entscheidern aus 100 deutschen Bundes-, Landes- und Kommunalverwaltungen zu den aktuellen Herausforderungen und den bis 2017 geplanten Maßnahmen. Schwerpunkte sind Steigerung der Kosteneffizienz, E-Government mit einem Fokus auf Bürgerkonten, Kooperationen, Bürgerbeteiligung und Business Intelligence.

Studie
Digitale Exzellenz

In einer gemeinsamen Studie haben die Universität Hamburg, HITeC e. V. und Sopra Steria Consulting eine Bestandsaufnahme zur Digitalisierung deutscher Unternehmen und Behörden vorgenommen. Die Untersuchung zeigt, dass die Vorbereitung auf den Transformationsprozess und der Umsetzungsgrad auf dem Weg zur Digitalen Exzellenz erheblich variieren.

IMPRESSUM

Sopra Steria GmbH
Hans-Henny-Jahnn-Weg 29, 22085 Hamburg

FRANKFURT BUSINESS MEDIA GmbH – Der F.A.Z.-Fachverlag
Bismarckstraße 24, 61169 Friedberg
(zugleich auch Verlag;
Geschäftsführung: Torsten Bardohn, Dr. André Hülsbömer
Vorsitzender der Geschäftsleitung: Bastian Frien)

Titelfoto: © Matej Moderc/iStock/Thinkstock/Getty Images

ISBN: 978-3-945999-10-3

Verantwortliche Redakteurin und Autorin
(wenn nicht anders genannt): Jacqueline Preußer
Redaktionelle Mitarbeit: Andrea van Baal
Gestaltung und Satz: Christine Lambert, Jan Hofmann
Lektorat: Vera Pfeiffer

Druck und Verarbeitung: Boschen Offsetdruck GmbH
Alpenroder Straße 14, 65936 Frankfurt am Main
www.boschendruck.de

Mit Ökofarben auf umweltfreundlichem Papier gedruckt.
Diese Studie wurde klimaneutral hergestellt. Der CO_2-Ausstoß wurde durch Klimaschutzprojekte kompensiert.

Wir drucken klimaneutral
mit natureOffice

Ansprechpartner

Sopra Steria GmbH
Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Telefon: (040) 2 27 03-52 19
Telefax: (040) 2 27 03-12 19
E-Mail: birgit.eckmueller@soprasteria.com

FRANKFURT BUSINESS MEDIA GmbH –
Der F.A.Z.-Fachverlag
Jacqueline Preußer
Postfach 20 01 63
60605 Frankfurt am Main
Telefon: (069) 75 91-1961
Telefax: (069) 75 91-19 66
E-Mail: jacqueline.preusser@frankfurt-bm.com

ISBN: 978-3-945999-10-3