

1. Infotag IT-Sicherheit am 15. September 2011 in München

Security-Herausforderungen meistern

Durch gezielte Spionage und allgemeine Sicherheitslücken entstehen Unternehmen Schäden in Milliardenhöhe. Hinzu kommen hohe Strafzahlungen sowie Image-Schäden. Themen wie Cloud- und Mobil-Computing-Security, Compliance Management, physikalische Zutrittskontrolle, Speichersicherheit und Rund-um-Absicherung der Rechenzentren gewinnen beim Umgang mit sensiblen Daten dramatisch an Bedeutung. Als Plattform zur Diskussion über die neuesten Trends und Schutzstrategien im Zusammenhang mit Know-how und wertvollen Unternehmensdaten hat die Fachzeitschrift IT-SICHERHEIT daher den Infotag IT-Sicherheit geschaffen, der nach der Startveranstaltung am 15. September 2011 in München künftig in unregelmäßigen Abständen mehrmals im Jahr stattfinden wird.

Die Herausforderungen für Unternehmen sowie staatliche und nichtstaatliche Organisationen in Sachen IT-Sicherheit werden täglich komplexer. Hinzu kommt die Umsetzung nationaler, europäischer und internationaler Regelwerke und Gesetzestexte zur Absicherung der Unternehmensdaten und IT-Prozesse. Der neue Infotag IT-Si-

cherheit hat das Ziel, aktuelle Bedrohungstrends aufzudecken und praktische Hilfestellung beim Einrichten geeigneter Schutzmechanismen zu geben.

Nach einer einführenden Status-quo-Analyse der IT-Sicherheit durch Markus Linne- mann von der FH Gelsenkirchen gab Thors-

ten Scharmatinat von itWatch eine Übersicht über die Angriffswege der Industriespione und über die verfügbaren technischen und organisatorischen Mittel, die heute zur Abwehr von Industriespionage zur Verfügung stehen.

Mit der Frage des Vertrauens, das Unternehmen und Privatpersonen in einen Cloud-Anbieter setzen müssen, und andererseits mit der Frage, welche Herausforderungen an den Cloud-Anbieter zu stellen sind, beschäftigte sich Dr. Thomas Loczewski von Ernst & Young. Er gab in seinem Vortrag eine Übersicht darüber, welche Bedenken den Kunden beeinflussen, sowie, anhand von Erfahrungen großer Organisationen, einen Bericht über Fallstricke und Empfehlungen über die Gestaltung der Geschäftsbeziehungen. Dr. Claudia Böttcher von Brainloop übermittelte Empfehlungen, wie mobile Sicherheit von vertraulichen Dokumenten gewährleistet werden kann und wie sich solche Dokumente nach Corporate-Compliance-Regeln über Firmengrenzen hinweg sicher austauschen lassen.

Eine Übersicht über die heutigen Probleme von Unternehmen bei der Definition und Überwachung von Risiken, ihrer Dokumentation sowie beim Reporting von Risiken gab Frank Schlottke von Applied Security. Effektive Sicherheitskontrollen und wirksa-



Der erste Infotag IT-Sicherheit in den Räumen des Süddeutschen Verlags, München, war sehr gut besucht.

Anzeige

50 YEARS
Rittal. Power and Vision!

Rittal – Das System.

Schneller – besser – überall.

**IT-Infrastruktur
von S bis XXL.**



SCHALTSCHRÄNKE

STROMVERTEILUNG

KLIMATISIERUNG

me Mechanismen gegen unberechtigte oder fehlerhafte Datenzugriffe können mit Hilfe eines Werkzeug-gestützten Governance-, Risk- und Compliance-Systems geschaffen werden, in dem auch gewachsene Strukturen und Prozesse des Unternehmens abgebildet werden müssen.

Den gegenwärtig stattfindenden Paradigmenwechsel der Authentifizierung durch biometrische Verfahren übermittelte Silka Müller von Twinsoft biometrics. Nach einer umfassenden Darstellung der Authentifizierung anhand individueller Körpermerkmale verglich Frau Müller verfügbare biometrische Verfahren und behandelte ihre Anwendungsszenarien und Sicherheitsaspekte.

Die Anforderungen an „Data Loss Prevention and Endpoint Security“ des Projekts „Herkules“ – die Modernisierung der nichtmilitärischen ITK der Bundeswehr, die aus 140.000 PCs, etwa 7.000 Servern und 300.000 Festnetztelefonen an mehr als

1.500 Standorten besteht – beschrieb Bernd König, BWI Informationstechnik. Die Zielsetzungen dieses komplexen Systems sind unter anderem die Absicherung der Schnittstellen von dezentralen Arbeitsplätzen, die bedarfsorientierte Nutzung von Geräten, die Kontrolle des Datentransfers, die Überwachung des Im- und Exports von Dateien und die Verhinderung der Nutzung von nicht dienstlichen Geräten. In seinem Vortrag stellte König die Risikoanalyse der technischen Umgebung der Bundeswehr, die potentiellen Angriffswege auf Daten, die technische Begegnung der Risiken, die Schnittstellenkontrolle und die Applikationskontrolle dar. Sehr wichtige Punkte bei der Realisierung von „Herkules“ sind Fragen der Akzeptanz bei Anwendern und die Minimierung des Administrationsaufwands ohne Sicherheitseinbußen.

Die professionelle und nachhaltige Planung und Realisierung von Rechenzentren und Serverräumen, die wirtschaftliche Op-

timierung von IT-Standorten und Energieeffizienz, Lösungen aus der Praxis waren Thema des Schlussreferats von Thomas Sting von proRZ Rechenzentrumsbau.

Roundtable IT-Sicherheit

Bereits am Vorabend der Veranstaltung gab es einen Roundtable, auf dem die Redaktion der IT-SICHERHEIT mit Vertretern einschlägiger Security-Companies über die durch Technologien wie Virtualisierung, Cloud Computing, Web-2.0-Dienste/Social Networking und Mobile Computing veränderte Bedrohungslage diskutierte, um herauszufinden, wie Unternehmen die Oberhand behalten können.

Ein wichtiger Punkt in der Diskussion war die Auslotung der Dinge, die sich für den Sicherheitsverantwortlichen heute gegenüber früher geändert haben, und die Frage, wo aktuell die brisantesten Gefahrenherde liegen. Dabei kamen auch gleich die Tücken der sozialen Netzwerke mit zur Sprache: Dr. Stefan Grotehans: „Die jüngere Generation nutzt heute sehr gerne völlig andere Kommunikationskanäle, als bisher im Business üblich war. Ich denke da an die breite Palette an sozialen Netzwerken. Selbst wenn die Unternehmens-IT versucht, solche Kanäle abzuknippen, finden die jungen Leute immer wieder Wege, sie dennoch einzusetzen.“

Thorsten Scharmatinet sieht zahlreiche Aspekte, die das moderne Bedrohungsszena-

Markus Linnemann von der FH Gelsenkirchen gab eine einführende Status-Quo-Analyse der IT-Sicherheit.



IT-INFRASTRUKTUR

SOFTWARE & SERVICE



www.rittal.de

rio heute „bereichern“: „Das reicht von Stuxnet über Conficker bis hin zu gezielten Attacken, die firmenrelevante, geheime Informationen ausspähen. Einer der auffälligsten Trends dabei ist, dass solche Angriffe auf das geistige Eigentum heute sehr gut getarnt daherkommen – beispielsweise als Anfrage von einem Facebook-Freund –, und von daher gar nicht als Angriff wahrgenommen werden. Bei der Umsetzung von Sicherheitszielen liegt eine der größten Herausforderungen heute sicher darin, den Mitarbeitern dadurch keine Steine in den Weg zu legen. Oft ist es nach wie vor so, dass IT-Sicherheit gerne als „Bremse“ oder „Verhinderer“ wahrgenommen wird. Das sollte nicht sein – die beiden Pole Sicherheit und Effizienz müssen sich nicht widersprechen, sondern können sich sogar positiv ergänzen.“

Eine weitere Herausforderung sieht Scharmatinat im mangelnden Sicherheitsbewusstsein. „Das Problem dabei: Man kann Mitarbeiter nicht auf Vorrat schulen nach dem Motto: Ich stecke euch mal acht Stunden in einen Seminarraum und haue euch das gesammelte Wissen über Sicherheit um die Ohren. So funktioniert das nicht – erstens, weil die Gefahrenherde sich sehr schnell wieder in ganz neue Richtungen entwickeln, und zweitens, weil nach solchen Kompaktkursen sehr wenig für die Praxis Nutzbares hängenbleibt. Man kann beispielsweise lange erklären, dass Dateien eines bestimmten Typs, eines Verzeichnisses oder was auch immer nicht ohne weiteres herausgegeben werden dürfen. Wenn es gerade in den Arbeitsablauf des Mitarbeiters

passt – er damit also effektiv seinen Job erledigen will, wird er sich in einer solchen Situation kaum an das Gefahrenpotenzial erinnern. Es ist also auf jeden Fall nötig, dem Anwender hier mit entsprechenden Hinweisen in Echtzeit mögliche Gefahren vor Augen zu führen und sichere Handlungsweisen entweder schon technisch zu erzwingen oder dem Anwender nahezu legen.“

Jan von Knop machte in diesem Zusammenhang darauf aufmerksam, dass die Definition von Verantwortlichkeiten in puncto IT-Sicherheit noch kaum umgesetzt sei. Das Thema „Accountability“, ohne das eine wirksame Durchsetzung von Sicherheit so gut wie unmöglich ist, gehöre damit ebenso zu den aktuellen Top-Trends.

Ein Thema, das immer offener zur Sprache kommt, ist die geheimdienstliche Spionage – mehr oder weniger offen im Auftrag der jeweiligen Regierung. Wichtige „Partner“ der jeweiligen Geheimdienste sind IT-Firmen des eigenen Landes, die sich im Dienste des Heimatschutzes zur Bereitstellung geeigneter Hintertürchen in ihren Produkten verpflichten lassen. IT-SICHERHEIT wollte von den Teilnehmern wissen, inwieweit dies eine stärker national geprägte IT-Ausrichtung auf den Plan ruft – nicht zuletzt vor dem Hintergrund, dass heute nahezu alle wesentlichen IT-Bestandteile von US-amerikanischen Firmen geliefert werden.

Gereon Tillenburg hält eine solche Strategie nicht für den richtigen Weg. Auch im eigenen Land gäbe es einen Geheimdienst und auch der fordere seine Backdoor. Zudem seien Geheimdienste global sehr eng miteinander vernetzt. „Im Bereich der Telekommunikation

beispielsweise gibt es die „Lawful Interception“ und eine Reihe weiterer internationaler Abkommen, die dafür sorgen, dass Geheimdienste überall auf der Welt auf Daten zugreifen können. Ich denke, eine nationalistische Denkweise bringt uns hier kein Stück weiter.“

Scharmatinat versicherte, dass – zumindest was sein Unternehmen betrifft – noch nie ein Geheimdienst irgendwelche Hintertüren in den Produkten auch nur angefragt habe. Also gäbe es so etwas auch nicht bei itWatch, und das sei durchaus ein wichtiges Verkaufsargument. Gleiches gelte auch für Brainloop: „Die Brainloop AG bietet ihren Service in Deutschland an und befolgt entsprechend die einschlägigen deutschen Gesetze. Diese erlauben die Herausgabe von zum Beispiel personenbezogenen Daten nur mit der vorherigen Zustimmung der betroffenen Person. Daran halten wir uns. Die von uns angebotene Secure Dataroom Solution ist Software-as-a-Service und wird vom jeweiligen Eigentümer selbst verwaltet. Er allein bestimmt, welche Personen Zugriff haben und welche Rechte der einzelne Nutzer bekommt. Systemadministratoren haben ebenfalls keinen Zugriff auf die Dokumente, somit ist ein Operator-beziehungsweise Provider Shielding sichergestellt.“

Und auch Andreas Schuster schlägt in die gleiche Kerbe: „Wir sind ein rein deutsches Unternehmen und haben uns im Rahmen von Initiativen wie ‚IT Security made in Germany‘ verpflichtet, auf Backdoors aller Art zu verzichten. Zugleich unterstützen auch wir alle gängigen Methoden zur sicheren Verschlüsselung, sei es AES, RSA, elliptische Kurven und vieles mehr. Das wird gerade im Hinblick auf Applikationen aus der Cloud und Datenspeicherung in der Cloud immer

Teilnehmer Roundtable IT-Sicherheit

- **Dr. Stefan Grotehans**, Vice President Sales Germany, Brainloop
- **Andreas Schuster**, EMEA Sales Manager, apsec
- **Thorsten Scharmatinat**, Key Account Manager, itWatch
- **Gereon Tillenburg**, Geschäftsführer Twinsoft biometrics

Sowie von Redaktionsseite:

- **Prof. Dr. Jan von Knop**, Chefredakteur IT-SICHERHEIT
- **Stefan Mutschler**, Stellv. Chefredakteur IT-SICHERHEIT (Moderation)



Am Vorabend des Infotags IT-Sicherheit diskutierte die Redaktion der IT-SICHERHEIT unter der Leitung von Stefan Mutschler über aktuelle Trends und neue Security-Ansätze.

„Einer der auffälligsten Trends ist, dass Angriffe auf das geistige Eigentum heute sehr gut getarnt daherkommen – beispielsweise als Anfrage von einem Facebook-Freund – und von daher gar nicht als Angriff wahrgenommen werden“, so **Thorsten Scharmatinat**, itWatch.



Basis vieler Sicherheitsansätze ist eine sichere Authentifizierung. Dabei galt die Biometrie, also die Authentifizierung mittels Körpermerkmalen, einst als Hoffnungsträger – inzwischen überwiegen, zumindest in der öffentlichen Wahrnehmung, eher die Ressentiments, sei es aus technisch-funktionaler oder aus datenschutzrechtlicher Perspektive. Tillenburg als Vertreter eines auf Biometrie fokussierten Unternehmens hat hier natürlich eine völlig andere Meinung: „Zum einen bemerken wir ganz deutlich einen rapiden Schrumpfungsprozess, was die Ressentiments gegenüber Biometrie angeht, zum anderen kristallisiert sich immer mehr heraus, dass Biometrie eine der wenigen, wenn nicht gar die einzige Möglichkeit ist, eine Identität wirklich zu beweisen. Gängige Zwei-Faktor-Authentisierungen beruhen immer auf dem Prinzip, dass ich etwas haben muss – etwa einen Schlüssel oder einen Token – und dass ich etwas weiß – meist ein Passwort. Damit ist aber nur bewiesen, dass jemand etwa hat und etwas weiß, nicht dass dieser Jemand irgendwer Bestimmtes ist. Biometrie ist die Authentifizierung durch das Sein – und dafür gibt es inzwischen für jede Sicherheitsstufe eine technisch und wirtschaftlich angemessene Biometrielösung.“ Auch bei den übrigen Teilnehmern der Runde herrschte weitgehend Konsens darüber, dass der Ruf der Biometrie wahrscheinlich deutlich schlechter ist als ihr tatsächlicher Wert. Immerhin, zur Lösung der Vorbehalte hätte wohl auch der verstärkte Einsatz von Biometrie in Regierungen beigetragen – dem einfachen Bürger würden die Vorteile über seine Ausweisdokumente nähergebracht, die mehr und mehr auch biometrische Merkmale enthalten.



„Die jüngere Generation nutzt heute sehr gerne völlig andere Kommunikationskanäle, als bisher im Business üblich war. Ich denke da an die breite Palette an sozialen Netzwerken. Selbst wenn die Unternehmens-IT versucht, solche Kanäle abzuknippen, finden die jungen Leute immer wieder Wege, sie dennoch einzusetzen“, so **Dr. Stefan Grotehans**, Brainloop.

„Biometrie ist eine der wenigen, wenn nicht gar die einzige Möglichkeit, ist, eine Identität wirklich zu beweisen. ... Biometrie ist die Authentifizierung durch das Sein – und dafür gibt es inzwischen für jede Sicherheitsstufe eine technisch und wirtschaftlich angemessene Biometrielösung“, so **Gereon Tillenburg**, Twinsoft biometrics



„Wir sind ein rein deutsches Unternehmen und haben uns im Rahmen von Initiativen wie ‚IT-Security made in Germany‘ verpflichtet, auf Backdoors aller Art zu verzichten. Auch bei uns hat noch kein Geheimdienst mit einem entsprechenden Wunsch angeklopft. Zugleich unterstützen auch wir alle gängigen Methoden zur sicheren Verschlüsselung, sei es AES, RSA, elliptische Kurven und vieles mehr“ so **Andreas Schuster**, EMEA Sales Manager, apsec.

„Die Definition von Verantwortlichkeiten in puncto IT-Sicherheit ist noch kaum umgesetzt. Das Thema ‚Accountability‘, ohne das eine wirksame Durchsetzung von Sicherheit so gut wie unmöglich ist, gehört damit zu den aktuellen Top-Trends.“, so **Prof. Dr. Jan von Knop**



Weitere Diskussionspunkte waren die Absicherung moderner Rechenzentren, die Nutzung privater Smartphones und Tablets im Unternehmenskontext, die Rolle von Verschlüsselungstechnologien und vieles mehr. Die Erkenntnisse aus der Runde, die bei weitem nicht vollständig in diese Zusammenfassung einfließen konnten, werden sich auch in künftigen Ausgaben der IT-SICHERHEIT widerspiegeln. ■

wichtiger. Unsere Kunden nutzen teilweise auch Cloud-Angebote, die keine Datenhaltung in deutschen Landesgrenzen garantieren. Für sie, aber auch für alle anderen

Cloud-Angebote kommen wir jetzt mit neuen Lösungen, die eine Verschlüsselung direkt in der Cloud und auch für Kollaborationstools wie Microsoft Sharepoint bieten.“

Jan von Knop und Stefan Mutschler