Podiumsgespräch »Datensicherheit in der Wirtschaft«

T · · Systems · HITACHI Inspire the Next Hitachi Data Systems · BUNDESRECHENZENTRUM BRZ · EMC²

Die sichere Speicherung und Lagerung von Daten ist lebenswichtig für Unternehmen. Worauf kommt es beim Schutz vor Datenklau und Ausfällen in der IT an? Wie kompliziert wird es bei dem rasanten Datenwachstum und dem Trend zu mobilen Endgeräten?

Eine hochkarätige Expertenrunde diskutierte am 21. November im Bundesrechenzentrum zu einer Herausforderung in der Wirtschaft, an der Unternehmen trotz technischen Möglichkeiten oftmals aufgrund der Nutzer scheitern: IT-Sicherheit. Mit welchen Ansätzen Unternehmen und Organisationen für mehr Sicherheit sorgen können, was die Wirtschaft bewegt – darüber sprachen Max Schaffer, Geschäftsführer Director Production T-Systems, Johannes Mariel, Chief Security Officer BRZ, Vassil Barsakov, Regional Director EMEA North RSA, Horst Heftberger, Geschäftsführer Hitachi Data Systems, Bernhard Pawlata, Security & Quality Manager Interxion, und Franz Hoheiser-Pförtner, Chief Information Security Officer Wiener Krankenanstaltenverbund, mit Martin Szelgrad, *Telekommunikations & IT Report*. Gastgeber BRZ-Geschäftsführer Roland Jabkowksi begrüßte knapp 80 Gäste aus Wirtschaft und Verwaltung, die gekommen waren. Partner des Podiumsgesprächs waren T-Systems, BRZ, EMC und Hitachi Data Systems.

Report: Herr Schaffer, gerade beim Trend zu Cloud-Services wird derzeit viel über IT-Sicherheit diskutiert. Lohnt sich der Gang in die Wolke für Unternehmen? Überwiegen die Vorteile von Verfügbarkeit und Flexibilität von IT-Services?

Max Schaffer, T-Systems: Die Frage lässt sich mannigfaltig beantworten. Ich bin felsenfest davon überzeugt, dass es sich lohnt. Unternehmen geben bei Cloud Computing ihre Services in professionelle Hände von Dienstleistern, die wissen, was sie tun. Die Branche kennt die Risiken, sie weiß, wie mit Daten umzugehen ist, wie IT produziert wird. Ich sehe dazu eine Analogie zum Automobilsektor. Auch wir IT-Dienstleister haben mittlerweile extrem genaue, sicherheitsgetriebene Prozesse aufgesetzt. Für Unternehmen ist diese Leistung ähnlich wie der Bezug von Strom aus der Steckdose. Was dahinter steckt, diese Sorge, nehmen wir den Unternehmen ab und können natürlich entsprechende Kostenvorteile durch Skalierbarkeit und Flexibilität der Dienste bieten. IT-Dienstleister werden gemäß Vorschreibungen der Wirtschaftsprüfer jährlich auditiert und verfügen über entsprechende Zertifizierungen. Sie können sich sicher vorstellen, wie unsere Reputation am Markt bei einem Security Incident leiden würde. Schon allein aus diesem Grund tun wir sehr, sehr viel für eine sichere Infrastruktur und absolut sichere Services.

Max Schaffer, T-Systems: »Unternehmen geben bei Cloud Computing ihre Services in professionelle Hände von Dienstleistern, die wissen, was sie tun.«

Report: Wie viele Attacken gibt es monatlich auf Ihr Rechenzentrum in Wien? Ist ein Rechenzentrum nicht auch ein Anziehungspunkt für Angriffe?

Schaffer: Die Aktivitäten von Script Kiddies – etwa Port Scans und Denial-of-Service-Attacken – sind eine leicht lösbare Aufgabe für unsere Sicherheitssysteme. So etwas wird im Hintergrund abgearbeitet, unsere Alarmsysteme schlagen da gar nicht mehr groß an. Die Häufigkeit von gezielten Attacken, die auch unseren Chief Security Officer beschäftigen, ist sehr unterschiedlich. Das können in einem Monat zwei, drei Vorfälle sein - dann aber tut sich vielleicht einige Monate gar nichts. Gegenwärtig konzentriert sich das eher auf die südliche Hemisphäre. So ist Afrika beispielsweise ein Brennpunkt für Angriffe hauptsächlich aus dem chinesischen Raum. Meine Kollegen in Südafrika haben hier alle Hände voll zu tun. Sie arbeiten wie alle Standorte von T-Systems aber in einem globalen Sicherheitsnetz. Wir können damit auch in Österreich auf entsprechendes Know-how zugreifen. Alleine die Statistiken des Innenministeriums zeigen, dass wir auch hierzulande nicht von Angriffen verschont bleiben. Dies hat aber auch positive Auswirkungen. Ich darf jährlich einen Gastvortrag in Hagenberg halten und sehe dort die Kompetenz der jungen Menschen hinsichtlich IT-Security. Das zeichnet den Wirtschaftsstandort Österreich aus: die Ausbildung von sehr, sehr guten Securityfachkräften.

Report: Ob Großunternehmen oder die Verwaltung: Machen Unternehmen dieser Größe bereits alles bei Datensicherheit richtig? Was ist Ihre Einschätzung zur Lage am heimischen Markt?

> **Das zeichnet den Wirtschaftsstandort** Österreich aus: die Ausbildung von guten Fachkräften.

Fotos: Milena Krobath

Schaffer: Das Sicherheitsempfinden in den Unternehmen hat sich in den letzten Jahren komplett gewandelt. Stand früher Sicherheit vor allem für Unternehmen, die personenkritische Daten verwalteten, an erster Stelle, so ist dies nun mit Daten- und Systemverfügbarkeit wesentlich breiter besetzt. Kein Unternehmen heute kommt daran vorbei, wenn beispielsweise über Angriffe sogar Hardware manipuliert und ausgeschaltet werden kann. Die Industrie ist auf die IT angewiesen. Wenn früher ein EDI-System ausgefallen war, so konnte beispielsweise ein Billa gewisse Daten eben nicht mit einem Lieferanten austauschen. Das wurde Stunden später nachgeholt. Wenn EDI heute ausfällt, steht spätestens nach zwei Stunden eine Fertigungsstraße in der Automobilindustrie, und das vielleicht sogar an mehreren Standorten. Es wird heute »just in time«, »just in sequence« produziert. Sicherheit müssen wir da wir nicht reaktiv, sondern proaktiv betreiben. Das bedeutet den Einsatz von intelligenten Agents, ständigen Systemanalysen und letztendlich auch in den Budgets, der Security mehr Ressourcen zur Verfügung zu stellen.

Report: Worin bestehen aus Sicht des BRZ die Vorteile, Daten und Applikationen in ein Rechenzentrum auszulagern? Was können Rechenzentrumsanbieter besser als einzelne Ihrer Unternehmenskunden – wenn man etwa die Zertifizierungsthematik betrachtet?

Johannes Mariel, BRZ: Die Kosten für Zertifizierungen beschränken sich im Wesentlichen auf die Aufwände für den Compliance-Nachweis für den ISO 27001-Standard für das Informationssicherheitsmanagement. Diese Kosten sind aber mit knapp unter einer fünfstelligen Aufwandssumme jährlich vergleichsweise gering. Anders sieht es bei den Anforderungen unserer Kunden an das Thema IT-Sicherheit aus. Alles, was wir bei einem unserer Zertifizierungsaudits nachzuweisen haben, erwarten unsere Kunden als Qualitätsmerkmale unserer Dienstleistungen. Am Ende des Tages kommt es aber auf die Unternehmens- und die Sicherheitskultur des Unternehmens an, wie weit man dieses Thema professionalisieren möchte. Mit zunehmender Größe einer Organisation werden diese Kostenstellen entsprechend günstiger. Um dies an einem Beispiel festzumachen: Ein Unternehmen hat bei zehn Windows-Servern den gleichen Aufwand, um die Schwachstellen im Betriebssystem zu identifizieren, wie bei 2.000 Servern. Allerdings ist der Divisor für diesen Aufwand wesentlich verschieden.

Johannes Mariel, BRZ: »Am Ende des Tages kommt es auf die Unternehmens- und die Sicherheitskultur des Unternehmens an, wie weit man dies professionalisieren möchte.«

Vassil Barsakov, RSA: »Es gilt nun für Unternehmen Prozesse aufzusetzen und im Detail zu überlegen, wie man sich vor Angriffen schützen sollte.«

Report: »Bring Your Own Device« ist ein Trend, der heute den CIOs und CSOs den Schweiß auf die Stirne treibt. Wie unsicher wird es dadurch für Unternehmen? Leistet sich das BRZ bereits ein solches Modell?

Mariel: Wir bieten unseren Mitarbeitern und auch Führungskräften Standard-Endgeräte zur mobilen Nutzung. Durch unsere strenge Sicherheitspolitik im Haus sind klar Funktionalitäten und auch Einschränkungen festgelegt. So können wir die IT-Sicherheit auf den jeweiligen Geräteklassen jedenfalls mit gutem Gewissen nachweisen. Den Wünschen über die Zulassung von Bring Your Own Device sind wir in unserem Haus noch nicht nachgekommen – wir arbeiten aber an einer Lösung. Ich denke, dass es in absehbarer Zeit auch für unsere Mitarbeiter möglich sein wird, ihre eigenen Endgeräte an den Arbeitsplatz mitzunehmen. Sicherheit ist immer eine Gratwanderung zwischen Compliance auf der einen Seite und Nutzerakzeptanz auf der anderen. Als Sicherheitsverantwortlicher muss man gemeinsam mit dem technischen Team eine Lösung finden, die beide Aspekte in angemessener Art erfüllt.

> **Einige wesentliche, aber nicht alle** Aspekte bei IT-Security beruhen auf technischen Lösungen.

Report: Sie sagen, jeder Mitarbeiter eines Unternehmens ist auch ein Sicherheitsmitarbeiter. Was meinen Sie damit?

Horst Heftberger, Hitachi Data Systems: »Im Storagebereich herrscht ein großer Kostendruck. Dennoch ist IT-Sicherheit essenziell – ich sehe das als extrem wichtiges Thema.«

Mariel: Ein wesentlicher Teil von IT-Security ist technisch lösbar, doch nicht alle Aspekte beruhen auf technischen Lösungen. Ein großer Teil der Informationen eines Unternehmens verlässt in der Regel zwischen 17 und 18 Uhr unser Haus. Dies passiert in Form von USB-Sticks, mobilen Geräten insbesondere aber in den Köpfen der Mitarbeiter. Technische Geräte kann man bis zu einem gewissen Grad technisch gegen Datenverlust absichern. Bei den Mitarbeitern selbst funktioniert dies nur über Awareness. Sicherheit muss also in Unternehmen Chefsache sein. Den Mitarbeitern müssen Sicherheitsrisiken ständig vor Augen geführt werden, und wie man diesen kompetent entgegen treten kann. Dies passiert im Idealfall nicht nur über regelmäßige Schulungen, sondern im täglichen Betrieb über Risikoanalysen oder auch entsprechenden Audits, um mit den Mitarbeitern gemeinsam technische und organisatorische Schwachstellen aufzuzeigen und zu beheben.

Report: Herr Barsakov, welche Entwicklungen sehen Sie am Cybercrimemarkt? Wogegen – neben der Gefahr, der stets auch von eigenen Mitarbeitern ausgeht – sollten Unternehmen heute gewappnet sein? Wo sehen Sie 2013 die großen Herausforderungen in der Wirtschaft?

> **Man muss sich heute** eingestehen, dass die eigene IT wahrscheinlich bereits kompromittiert ist.

Vassil Barsakov, RSA: Man sieht bereits seit Jahren eine zunehmende Zahl an Bedrohungen und Angriffen, die mittlerweile nicht nur von jungen Menschen, die etwas ausprobieren wollen, sondern von gut organisierten Gruppen ausgehen – sowohl privater, krimineller Natur als auch auf nationaler Ebene mit staatlichen Ressourcen im Hintergrund. Dies bringt Unternehmen in eine neue Situation, wie man etwa bereits bei Stuxnet gesehen hatte. Es eröffnet von Angriffsszenarien und Unternehmensrisiken her neue Gefahren, die man in der Sicherheitspolitik eines Unternehmens definieren und betrachten sollte. Es gilt dazu Prozesse aufzusetzen und im Detail zu überlegen, wie man sich vor Angriffen schützen sollte.

Report: Ist Sicherheit für Unternehmen überhaupt noch leistbar?

Barsakov: Sicherheit muss leistbar sein. Wir können ja auch nicht einfach im öffentlichen Leben die Polizei aus Einsparungsgründen abschaffen. Informationssicherheit ist genauso wichtig. Mit der Verbreitung von EDV-Systemen und der Vernetzung von Daten – ich denke da auch an Smart Grids, die von der EU vorangetrieben werden oder auch an eine zu erwartende Explosion der Gerätezahlen mit dem neuen Internetprotokoll IPv6 – werden mehr und mehr Geräte und Maschinen auch ohne menschliche Hilfe untereinander Informationen austauschen. Wir können uns heute nicht leisten, diese Entwicklungsrichtung aus Kostengründen zu vernachlässigen – schließlich überwiegen die Vorteile dieser Vernetzungen. Freilich haben kein Unternehmen und kein Staat unbegrenzte Ressourcen zur Verfügung. Es gilt also, vernünftige Maßnahmen und Vorgangsweisen zu finden.

Report: RSA ist ja selbst Opfer einer großen Attacke geworden. Welcher Art ist dieser Angriff gewesen, und was hat Ihr Unternehmen daraus gelernt? RSA spricht ja offen über diese Zäsur.

Barsakov: Wir haben einiges daraus gelernt. Ich selbst bin seit drei Jahren für RSA tätig und ich kann Ihnen sagen: Wir sind heute eine andere Firma. Dies betrifft sowohl interne Sicherheitsrichtlinien als auch unsere Kommunikation gegenüber unseren Kunden. Der Angriff erfolgte damals sehr gezielt. Wir gehen von zwei verschiedenen, sehr professionell organisierten und koordiniert arbeitenden Teams aus, die in unsere Netzwerke eingedrungen waren. Zwar konnten wir innerhalb weniger Stunden auf den Einbruch reagieren und konnten erfolgreich die Ausbreitung auf kritische IT Systeme eindämmen, obgleich ein gewisser Schaden nicht mehr zu verhindern war Unsere Erkenntnis daraus: IT-Sicherheit muss mit einem völlig neuen Ansatz betrachtet werden. Man muss sich heute eingestehen, dass die eigene IT wahrscheinlich bereits kompromittiert ist oder noch kompromittiert wird. Allerdings muss bei entsprechenden Maßnahmen das Kompromittieren eines Netzwerkes oder eines bestimmten Systems nicht auch einen Diebstahl von Daten bedeuten. Es wird entscheidend sein, diese Fähigkeit und Strukturen in Unternehmen aufzubauen oder auch über einen externen IT-Dienstleister entsprechende Services zu beziehen. Im Falle des Falles ist dann wenigsten der Schutz besonders sensibler Daten gewährleistet und damit das Risiko minimiert. Heute leben wir dieses Prinzip im gesamten RSA-Konzern. Unsere Prozesse zu Incident Response Management sehen ganz anders als früher aus. Auch wurde unser Critical Incident Response Center personell aufgestockt und überwacht die Systeme zentral. Denn eines ist klar: Die Attacken werden weiter zunehmen. Klassische Produkte wie Firewalls oder Antiviren-Systeme können seit langem keinen angemessenen Schutz der Unternehmens-IT mehr vor gezielten Angriffen gewährleisten.

Report: IT-Security in der Wirtschaft – das heißt, Sicherheit in der Speicherung von Daten zu bieten. Was bedeutet dabei das rasante Datenwachstum in unserer Gesellschaft für die Datensicherheit? Birgt die Verwaltung von immer größeren Datenmengen nicht auch höhere Risiken?

Horst Heftberger, Hitachi: Wir sind in der glücklichen Lage, ein großes Datenwachstum zu haben. Leider geht die Preisentwicklung in die entgegengesetzte Richtung. Bei der Datensicherheit sehen wir einen massiven Bedarf an Konsolidierungen und zentral geführten, skalierbaren Systemen. Zwei- oder Drei-Standort-Konzepte sind in der IT aus Sicherheitsgründen und Gründen der Verfügbarkeit bereits Standard. Ein wesentlicher Trend ist auch das Selbstmanagement der Systeme mit automatischem Lastausgleich und automatischem Tiering. Letztes bedeutet, dass Daten, die hochverfügbar und performant sein müssen, automatisch auf den höchsten Tier-Level gestellt werden. Andere Daten werden wiederum in Speicherbereiche niedrigerer Level verschoben, um Kosten zu sparen. In der Regel herrscht im Storagebereich ein großer Kostendruck. Dennoch ist natürlich IT-Sicherheit auch hier essenziell – ich sehe das als extrem wichtiges Thema. Experten zufolge werden heute gut 50 % der Effizienzsteigerungen in Unternehmen direkt aus der IT generiert. Das heißt: Hier gibt es keine Kompromisse mehr. Abschaffen lässt sich die IT nicht mehr.

Report: Wie ist ein vernünftiges Management von Daten, wie Sie es beschreiben, für kleinere und mittelständische Unternehmen machbar? Werden sich das Unternehmen in Zukunft überhaupt noch leisten können?

Heftberger: Mit den neuesten Entwicklungen am Markt, darunter auch Lösungen von uns, sind solch modulare Systeme mit automatisiertem Tiering und Provisionierung auch für KMU verfügbar. Letztlich dabei wesentlich ist nicht die Art und Weise, wie ein Storagesystem funktioniert, sondern dass die Applikationen rund laufen. Auf welcher Ebene Daten gelagert sind, das interessiert den Anwender nicht. Die IT muss einfach unterbrechungsfrei, 24 Stunden, sieben Tage die Woche verfügbar sein.

Bernhard Pawlata, Interxion: »Unsere Kunden verlangen weniger bestimmte Softwaredienste, sondern einfach eine sichere IT-Umgebung, um ihr Geschäft zu betreiben.«

Franz Hoheiser-Pförtner, KAV: »Veranstaltungen wie diese fördern das Bewusstsein, dass hinter einer E-Mail-Adresse immer noch ein Mensch sitzt.«

Report: Herr Pawlata, wie definieren Sie den Begriff IT-Sicherheit?

Bernhard Pawlata, Interxion: Frei nach ISO 27001 definiere ich es als Konzept, das mir Vertraulichkeit, Verfügbarkeit und Integrität meiner Systeme und Daten garantiert. Als Colocationanbieter haben wir hier einen etwas differenzierten Ansatz. Unsere Kunden verlangen weniger bestimmte System- und Softwaredienste, sondern einfach eine sichere IT-Umgebung, um ihr Geschäft betreiben zu können.

> **Es gibt keine Kompromisse.** Abschaffen lässt sich die Informationstechnologie nicht mehr.

Report: Was spricht aus Ihrer Sicht für die Auslagerung von IT-Infrastruktur an Dritte? Liefern Sie einen besseren Untergrund für den Betrieb eines Servers, als es ein einzelnes Unternehmen selbst vermag?

Pawlata: Wir bieten auf jeden Fall eine leistbarere Infrastruktur: redundante Stromversorgung, Klimatisierung, Branderkennung- und Brandlöschung, Zutrittssicherheit und mehr. Die Kunden kaufen damit Sicherheit und ein über Jahre aufgebautes Know-how bei uns ein. Betreibt ein typisches KMU seine Server im berüchtigten Serverkammerl, wird dies nie jenen Sicherheits- und Verfügbarkeitsstandard erreichen, den ein Rechenzentrumsdienstleister bietet. Darüber hinaus haben auch unsere Kunden die Freiheit zu bestimmen, welchen Mitarbeitern überhaupt Zugang zur IT auch in unterschiedlichen Ausprägungen gewährt wird.

Report: Gibt es aus Ihrer Sicht etwas, was geben die Übergabe von IT-Services an einen Professionisten sprechen würde?

Pawlata: Ich bin der Ansicht: nein. Die Vorteile überwiegen eindeutig.

Report: Die versammelte IT-Branche ist zuversichtlich, die passenden Security-Werkzeuge und Ansätze bieten zu können. Wie dramatisch sieht ein CISO, der gerade mit kritischen Daten wie im Krankenanstaltenverbund zu tun hat, die Entwicklung des IT-Marktes? Welchen Herausforderungen begegnen Sie in der Gesundheitsbranche?

Franz Hoheiser-Pförtner, Wiener Krankenanstaltenverbund: Die Herausforderungen, die uns beschäftigen, kann man einfach mit zwei Worten beschreiben: Safety und Security. Ins Deutsche übersetzt heißt beides Sicherheit – es betrifft aber unterschiedliche, wichtige Aspekte. In Sachen der Einzelbetrachtung von Safety oder Security befinden wir uns im Gesundheitswesen seit vielen Jahren an der Spitze.

Wir erkennen nun aber, dass es in einigen Bereichen Sicherheitsprobleme gibt, die nicht mit den Herausforderungen in der herkömmlichen Büroorganisation vergleichbar sind. Auch sind Sicherheitsmaßnahmen in der IT per se anders konstruiert.

Nehmen Sie das Beispiel Firewall. Ich kenne keine Brandschutzmauer, die nicht lückenlos gemauert ist. Eine Firewall in der IT dagegen muss per Definition Löcher haben, um den Datenverkehr überhaupt zu ermöglichen. Es mutet paradox an, in der eigenen Organisation Sicherheitsmechanismen aufzusetzen, die aber schon aus Prinzip nicht hundertprozentig funktionieren dürfen.

Mir wäre es daher lieber, wenn wir über etwas wie Brandschutzsysteme in der IT sprechen. Die Branche muss hier umlernen. Gerade in der beobachtbar wachsenden Wahrnehmung von Governance-, Risk- und Compliance-Themen sollte nun mehr über die technischen Dinge hinaus in Richtung Organisation und Unternehmensprozesse diskutiert werden. IT-Systeme in der Gesundheitsbranche müssen an unterschiedlichsten Stellen jederzeit über Notein- und -ausgänge verfügen – beispielsweise beim Betrieb von Computertomografen.

Report: Sie sagen, die Awareness für IT-Sicherheit ist gestiegen? Hat da die Branche, haben da die IT-Abteilungen in den letzten Jahren ganze Arbeit geleistet?

Knapp 80 Gäste waren zum Podiumsgespräch des Report gekommen. Li. oben: Margarete Schramböck, NextiraOne. Re. oben: Heinz Janecska, BRZ. Unten: Petra Mossbeck, EMC.

Hoheiser-Pförtner: Dies ist sicherlich der Fall. Ich sehe aber nach wie vor ein großes Problem. Wir haben seit Jahren entsprechende Standardisierungen, Normen und Gesetze, die allesamt aber einzelne Regelwerke für das Querschnittsthema Informationstechnologie darstellen. Im Rechenzentrum und den IT-Services des Krankenanstaltenverbundes gibt es Dutzende Zertifizierungen. Wir unterliegen aber gerade bei der Normungsfrage von Servicequalität einem klassischen Silodenken, das nun aufgebrochen gehört. Sprechen wir von modernen IT-Lösungen, so sollten wir in Ketten und über Organisationsgrenzen hinaus denken. Dazu brauchen wir auch solche Veranstaltungen wie diese hier, um eine gemeinsame Sicht über herkömmliche Grenzen hinweg zu erlangen. Die IT-Anbieter mit ihren unterschiedlichen Lösungen und Systemen bieten gewisse Hilfestellungen für Unternehmen. Letztendlich sind die Aufgaben rund um IT- und Datensicherheit aber nur gesamtheitlich lösbar. Wir Techniker sprechen gerne von Schnittstellen. Im Gesundheitswesen ist dagegen meist von Nahtstellen die Rede. Eine Schnittstelle trennt, aber Nahtstellen verbinden. Vielmehr das sollte gefördert werden und Sicherheit ist immer noch ein Thema, das ich »face to face« leichter lösen kann. Veranstaltungen wie diese fördern das Bewusstsein, dass hinter einer E-Mail-Adresse immer noch ein Mensch sitzt. ❐