



Haftpflichtpraktiker aus Skandinavien tauschten bei der Swiss Re in München Erfahrungen aus.

Be prepared!

Vom 2. Expertenforum „IT- und Internetrisiken“ bei Swiss Re in München

„Systemausfall bei Lufthansa – nichts ging mehr.“ So oder so ähnlich lauteten die Pressemitteilungen am 24. September 2004. Einen Tag zuvor legte ein Computerfehler weltweit das Check-in-System der Deutschen Lufthansa lahm. Rund 6 000 Fluggäste der Lufthansa sowie insgesamt 46 Fluggesellschaften waren von Stornierungen und Verspätungen betroffen – ein Ausfall mit Folgen. Um das Management solcher und ähnlicher IT-Risiken ging es beim 2. Expertenforum „IT- und Internetrisiken“ der Swiss Re in München mit mehr als 30 Spezialisten aus Forschung, Wissenschaft und Wirtschaft.

Alles schon gehabt?

„Die Diskussion, die wir hier führen, gibt es seit Beginn der Industrialisierung“, so Lothar Schauer von der Fiducia Cash GmbH. „Wir schaffen Systeme, die wir beherrschen wollen.“ Vier Faktoren sind laut Schauer Auslöser für IT-Risiken:

- Arbeitsteilung und die damit verbundene Integration von Systemen und Prozessen
- die durch Kosten- und Zeitdruck entstandene Massenproduktion, die zur Automatisierung von Abläufen führt
- Standardisierung von Produkten, die Systeme angreifbarer machen und eine schnelle Ausbreitung von Viren und Würmern ermöglichen. Und schließlich
- die nicht abgeschlossenen, sich ständig wandelnden und instabilen Systeme, die durch die globale Vernetzung großen Bedrohungen von außen ausgesetzt sind.

Bekannte Risiken bekommen durch Internet- und IT-Technologien eine völlig neue Bedeutung, beispielsweise eine neue Dimension der Urheber-

rechtsverletzungen bei Informationen, Daten und Bildern aus dem Internet. Daneben entstehen laut Constanze Brand von Swiss Re Germany jedoch auch neue Risiken. Das volle Ausmaß beider Risikokategorien sei uns heute noch nicht bekannt. Doch erkennbar sei schon jetzt: Internet- und IT-Risiken können nicht mit traditionellen Versicherungsdeckungen erfasst werden. Dazu wurden zunächst verschiedene Bedrohungsszenarien und -kategorien diskutiert:

Risiko 1: Vernetzung von Systemen:

Durch zunehmende Integration von Prozessen entstehen technisch und wirtschaftlich Abhängigkeiten zwischen verschiedenen Unternehmen. Damit sind nicht nur Sachschäden miteinander verwoben, sondern auch Betriebsunterbrechungen. „Ein Netzausfall hat heute unvorhersehbare Folgen, da verschiedene Systeme miteinander vernetzt werden“, erläuterte Dr. Stephan Lechner von der Siemens AG München. Das Schadensausmaß könne dadurch enorm steigen.

Integration könne auch Kumulrisiken zur Folge haben. Die Auslagerung einzelner Rechenzentren zu einem externen Dienstleister biete durch die hohe Datenkonzentration eine begehrte Angriffsfläche für Kriminelle. Allerdings wurde angemerkt, dass in derartigen Einrichtungen sehr hohe Sicherheitsvorkehrungen getroffen würden und Schäden eher als unwahrscheinlich gelten, obwohl sie freilich nie ganz ausgeschlossen werden könnten.

Risiko 2: Viren, Würmer und andere Attacken: „Operationale Risiken sind das eine, die Bedrohungen das andere“, meint Vera Sönksen von der Deutschen Lufthansa AG. Viren, Würmer, Denial-of-Services Attacken und Hacker-Angriffe seien wohl die bekanntesten Bedrohungen. Dabei werde es nicht bleiben. Die Entwicklung schreitet rasant

voran: Während in den 80er Jahren die Verbreitung eines Virus noch Wochen dauerte, genügten dazu in den 90er Jahren bereits Tage. Heute reichten Minuten aus. Der Sapphire Wurm oder auch „Slammer“ breitete sich innerhalb von 11 Minuten über die ganze Welt aus, berichtete Klaus Lenßen von Cisco Systems GmbH. Zu Spitzenzeiten würden 55 Hosts pro Sekunde gescannt und verursachten Netzwerkausfälle, Flugannullierungen und blockierte Geldautomaten. Mittlerweile komme es täglich zu Hackervorfällen. Risiken, die dadurch entstehen, seien nur schwer zu kalkulieren.

Risiko 3: Der Mensch: Attacken auf IT-Systeme entstehen durch Menschen mit krimineller Energie. „Heute besitzen in Deutschland 3 bis 4 Prozent der Bevölkerung kriminelle Energien“, so Franz-Josef Lang von KoSiB eG. Er rechne damit, dass diese kriminelle Energie in Zukunft noch zunehmen wird. Steigende Unzufriedenheit und Existenzängste sowie abnehmende Loyalität gegenüber Arbeitgebern lasse die Hemmschwelle für kriminelle Handlungen sinken. Die global angelegten Attacken seien dabei eher die Ausnahme. Im Bereich Wirtschaftskriminalität würden 60 Prozent der Schäden von eigenen oder ehemaligen Mitarbeitern verursacht.

Eine andere, nicht kriminelle Bedrohung durch den Menschen stelle das nicht beabsichtigte Fehlverhalten dar. „85 Prozent aller Sicherheitsprobleme in Unternehmen werden von Mitarbeitern verursacht“, erklärte Johann Lehner von Symanec Deutschland GmbH. Die unternehmensinternen Risiken sind laut Thomas Pache von Gerling ähnlich hoch einzuschätzen wie Risiken durch Angriffe von außen. In der öffentlichen Diskussion jedoch würden sie meist vernachlässigt.

Bedrohung 4: Datenmissbrauch: Datenmissbrauch, so meint man, kann durch eigenverantwortlichen Umgang und gute Sicherheitssysteme verhindert werden. Doch ohne unser Wissen gelangen unsere Daten schnell an den falschen

– Anzeige –



English for the Insurance Industry

Die Ergänzung zu Ihren Sprachtrainings: ausgezeichnetes Versicherungsendenglisch



Termine 2005:

- ▶ 14. bis 18. Juni 2005
- ▶ 20. bis 24. September 2005

Auch modular buchbar:
Informationen und Anmeldung:
Studienleiter Keith Purvis:
keith.purvis@versicherungsakademie.de



Nichtstun ist keine Lösung: IT-Experten befassten sich mit den Risiken unserer Cyber-Welt.

Adressaten. Ein Beispiel: Über das Internet werden z.B. täglich verschiedenste gebrauchte Datenträger in Form von PDAs, Festplatten, iPods oder auch Handys verkauft. Nicht immer wurden vor dem Verkauf durch den Vorbesitzer sämtliche Daten gelöscht und gehen in den Besitz des Käufers über. Ein anderes Beispiel ist die so genannte „on-mouse-over-Funktion“: Fährt man bei Websites über einen nicht gekennzeichneten Punkt, so werden automatisch Daten des Website-Besuchers (z.B. E-Mail-Adresse) auf dem Server des Anbieters gespeichert. Auch Suchmaschinen bieten reichlich Möglichkeiten zur Datenbeschaffung: Websites können nach bestimmten Kriterien durchsucht werden und liefern wichtige Informationen, die für kriminelle Handlungen genutzt werden können. Stark zugenommen hat im letzten Jahr der Trend zum „Passwordfishing“. Dabei werden User auf Internetseiten gelockt, die gestaltet sind wie bekannte Websites von Banken. Man wird gebeten, sämtliche Daten inklusive Bankverbindung und Geheimnummer einzugeben. Mit den

Daten lassen sich bequem Abbuchungen vom Konto des Users vornehmen.

Risk Management: Lösungen, die keiner will

„Sicherheit muss als integraler Bestandteil aufgefasst werden“, so Thorsten Gründer von Gründer Consulting GmbH. Doch viele Unternehmen vernachlässigten die IT-Sicherheit und nutzen nicht einmal einfachste Sicherheitssysteme. 17 Prozent aller deutschen Unternehmen haben keine Virensoftware, 26 Prozent keine Firewalls, jedoch 94 Prozent besitzen eine eigene Website und sind per E-Mail erreichbar. Erschreckende Zahlen, meint Dietrich Winter von der Allianz Versicherungs AG. Als Gründe für den nachlässigen Umgang werden Zeitmangel, Kosten und technische Überforderung genannt. Aber auch die Möglichkeit der Versicherung potenzieller Schäden reduziert eigene Risk Management-Maßnahmen. Gesucht werde in den meisten Unternehmen nach der kostengünstigsten Variante. Kommt die Versicherung für den IT-Schaden auf, so bestehe kaum Notwendigkeit, in Sicherheitssysteme zu investieren. „Der Ruf nach Versicherung wird häufig leichtfertig geäußert und unterbindet risikobewusstes, unternehmerisches Handeln“, so Alexander Geschonnek von HiSolutions AG.

Ein Beispiel dafür, dass nicht nur Risikofinanzierung, sondern auch Risikowahrnehmung zum Geschäftsfeld der Versicherungsbranche zählt, war das „Y2K“-Problem. Häufig wurde der Vorwurf laut, die Assekuranz ziehe sich aus der Verantwortung, indem sie Risiken durch Y2K ausschließt, so Matjaz Siencnik von Swiss Re Zürich. Doch dadurch, dass die Versicherungswirtschaft schon lange vor dem Jahr 2000 die Problematik öffentlich diskutierte und mit Ausschlüssen drohte, wenn zu wenige Sicherheitsvorkehrungen getroffen würden, habe sie die Unternehmen zum Handeln gezwungen.

Geeignete Instrumente zur Sicherung von IT-Systemen sind vorhanden. „Dabei ist Qualität nicht immer ein Frage des Preises“, so Prof. Dr. Ruth Breu von der Universität Innsbruck. Tatsache jedoch sei, dass nur die wenigsten Unternehmen gut abgesichert sind. Denn meist würden lediglich Einzelrisiken betrachtet, obwohl der Blick auf das gesamte System unabdingbar sei. Zudem fehlten bis heute internationale rechtliche Rahmenbedingungen für ein annähernd funktionierendes Sicherungssystem.

Und was bringt die Zukunft?

Wie wird die IT-Risikolandschaft mit Jahr 2010 aussehen? Verschiedene Ansätze wurden in Workshops erarbeitet. Ihre Ergebnisse zusammengefasst:

Die Optimisten: Nichtstun ist keine Lösung, wenn man mit IT- und Internetsystemen im Jahr 2010 verantwortungsbewusst umgehen will. In erster Linie ist es wichtig, auf Bedrohungen aufmerksam zu machen und das Risikobewusstsein zu schärfen. Moralpredigten helfen hier selten, vielmehr erwarten die Experten eine Selbstregulierung durch die Wirtschaft. Zertifizierte Sicherungssysteme dienen als Marketinginstrument und gehen in die Bewertung von Unternehmen (Ratings) mit ein. „Im Jahr 2010 ist ein breites Basiswissen Grundlage aller Beteiligten und die meisten Prozesse sind up-to-date“, so das Fazit.

Die Pessimisten: Produktionsabläufe werden zunehmend schneller, die Qualität bleibt dabei auf der Strecke. Durch die voranschreitende Vernetzung wird es weitaus mehr Schäden geben. Hinzu kommt, dass durch steigende Anspruchsmoralität die Klagebereitschaft steigt, globale gesetzliche Regelungen aber noch nicht eingeführt wurden. Die Versicherungswirtschaft ist nicht mehr bereit, IT-Risiken zu decken. Solvency II fordert bei risikanten Deckungen ein höheres hinterlegtes Eigenkapital, um im Schadenfall Solvenz des Versicherungsunternehmens zu garantieren. Da IT- und Internetrisiken 2010 noch schwieriger zu kalkulieren sein werden, da statistische Grundlagen für genaue Tarifierungen fehlen, wird sich die Assekuranz aus diesem Geschäftszweig zurückziehen.

Die Realisten: Meist liegt die Wahrheit zwischen zwei Extremen. So wird sich beim „realistischen“ Szenario bis zum Jahr 2010 im Vergleich zu heute wenig ändern. Zwar kann sich die Risikolage durchaus massiv verschlechtern, jedoch folgen den Risiken in der Regel die Maßnahmen. Das kann verbesserte Sicherheitssysteme zu Folge haben, aber auch bei zu großer Bedrohung eine abnehmende Nutzung des Internets. Klarer als heute wird in der Zukunft zutage treten, dass die Verantwortung für die Sicherheit der IT-Systeme bei jedem einzelnen Unternehmen liegt. Voraussetzungen sind ein verbessertes Risikobewusstsein und eine geschärfte Risikowahrnehmung.

Monika Gruber, Swiss Re, München

Wann kommt die große Flut?

2. Internationale Fachmesse aqua alta mit Kongress für Klimafolgen und Katastrophenschutz

Auf der aqua alta-Messe 2005, die vom 18. bis 20. Januar 2005 in München auf dem Messegelände stattfindet, diskutieren Experten unter anderem über Sturmfluten und Küstenschutz. Die Messe umfasst Bereiche rund um Klimafolgen und Hochwasserschutz. Folgende Themen werden behandelt: Klima, Hochwasserschutz, Katastrophenmanagement, Fluss- und Deichbau, Gebäudetechnik und -materialien, Dienstleistungen, Versicherungen, Lawinen, Muren, Glaziologie, Wassermanagement, Wassermangel, Dürre, Brandbekämpfung, Sturmschäden, Wiederauforstung, Küstenschutz und alpine Naturgefahren. Nähere Angaben zur Messe und zum Kongress (19. bis 20. Januar 2005): www.aqua-alta.de