ABS, ASR, ESP – MERKMALE FÜR AUTOMOBILE SICHERHEIT. ABER GILT DAS AUCH FÜR DIE IT-SICHERHEIT?

In den letzten Jahren hat die wachsende Abhängigkeit von hoch verfügbaren und sicheren IT-Systemen maßgeblichen Einfluss genommen – sowohl auf den täglichen Geschäftsbetrieb als auch den Erfolg (oder Misserfolg) von Forschungs- und Entwicklungsarbeiten.

Viele Unternehmen schenken zuverlässiger Informationstechnik oft zu wenig Aufmerksamkeit. Dabei müssen Unternehmen heute genau wissen, wo Risiken lauern. Das gilt sowohl für große Konzerne oder Banken, aber auch für mittelständische Unternehmen.

„Wie sicher sind Forschungsergebnisse auf IT-Systemen aufgehoben?" Ganzheitliche Sicherheitskonzepte schützen umfassend und helfen bei der Beantwortung dieser Fragen! Aber die Sicherheitsvorgaben gehen noch viel weiter, denn: bei Missachtung von IT-Sicherheitsstandards gehen Geschäftsführer ein hohes Risiko ein – bis hin zu persönlichen Haftung!

Alles nur theoretische Szenarien?

„Da konnte sich die Unternehmensführung nur wundern: Vier Mitarbeiter kündigten, und das binnen weniger Wochen. Alles Leitende. Der Schaden war groß…"

Der Grund: Ein Wettbewerber der geschädigten Firma hatte sich Zugriff auf die Personalakten verschafft und die besten Mitarbeiter abgeworben. Ein gekündigter Mitarbeiter, dessen Passwort nicht sofort zurückgesetzt wurde, behielt Zugriff auf Programme, Prozesse und am Ende auf Daten, von denen der Fortbestand des gesamten Unternehmens abhängen kann.

Tatwerkzeug: USB-Stick

„Einem externen Vertrags-Mitarbeiter gelingt es, geheimes Material aus dem Intranet einer Forschungseinrichtung abzuziehen und auf einem USB-Stick zu speichern."

Der Grund: Bei vielen Unternehmen kommen USB-Sticks in den IT-Sicherheitsrichtlinien gar nicht vor. Dabei bilden unverschlüsselte Firmendaten auf mobilen Speichermedien ein enormes Sicherheitsrisiko. Die Sticks können viele Gigabyte Daten speichern, darunter Verträge, Angebote und andere unternehmenskritische Daten. In vielen Firmen können Angestellte ungehindert Firmendaten auf USB-Sticks speichern.

Weil nur wenige aller beruflich genutzten USB-Sticks mit Passwörtern oder einer Verschlüsselung geschützt sind, stehen die Informationen bei einem Verlust der USB-Sticks jedermann zur Verfügung.

Ähnliches gilt für unverschlüsselte, geheime Forschungsdaten auf Notebooks, wenn Mitarbeiter die Geräte verlieren oder sie entwendet werden und die Daten in „falsche Hände" gelangen.

Grenzen: nicht mehr physisch, sondern virtuell

Im heutigen Internet, oft als „Web 2.0" bezeichnet, verschwimmen die Grenzen des Unternehmens, und dies wirkt sich auch auf die Netzwerksicherheit aus. Anwendungen werden heute über das Internet genutzt und Intranets und Extranets sind wesentliche Teile eines Unternehmens. Einige Unternehmen bauen ihr Geschäft jetzt sogar komplett auf Web-Infrastrukturen auf: der Beweis hierfür sind „virtuelle" Unternehmen, die überhaupt keinen physischen Geschäftssitz mehr haben

Auch interne Mitarbeiter gehen über das interne Netzwerk hinaus, um Informationen aus dem Internet zu erhalten bzw. über das Internet zu vermitteln. Dieser bidirektionale Aspekt des Zugriffs auf Anwendungen über das Internet führt für Unternehmen jedoch zu erheblichen Sicherheitsproblemen. Kommunikationsmethoden sind sowohl nach innen als auch nach außen gerichtet und so gibt es auch Bedrohungen von innen und von außen.

Gefahren durch neuen Technologien: Web 2.0

Unter dem Begriff „Web 2.0" wird die veränderte Nutzung bekannter Technologien zusammengefasst. Anwender können interaktive Funktionen und Elemente auf Webseiten nutzen, die allerdings den Einsatz erweiterter Funktionalitäten (AcitveX, JAVA, …) verlangen. Vorteile liegen auf der Hand: Anwendungen können webbasiert genutzt werden, es bedarf keiner Installation von Software, der Browser zeigt nur die Ergebnisse an. Individualisierung von Webseiten durch den Nutzer, eine effizientere Abwicklung (Beschaffung, Verkauf) sowie Feedbackmöglichkeiten der Anwender unterstützen ein webbasiertes Marketing.

Aber damit verbundenen existieren Risiken durch Viren, Trojaner und Scripting-Attacken. In sogenannten „Social Networks“ gelangen vertrauliche Unternehmensinformationen (beabsichtigt oder unbewusst) in die Öffentlichkeit. Organisatorische und technische Ansätze bieten hier Unterstützung (z.B. durch die Ausprägung des Haftungsbewußtseins der Geschäftsführung, Betriebsvereinbarungen zur privaten Nutzung von eMail und Internetzugang, Proxy-Technologieren, Firewalls).

Sicherheitsbedrohungen: von außen und von innen

Aber nicht nur Dateien, die in Trojanern versteckt in ein Unternehmen eindringen, können Malware installieren. Auch scheinbar harmlose Websites, auf die Mitarbeiter zu legitimen Zwecken zugreifen, können Malware oder Spyware in einem Netzwerk installieren. Dies ist unter Umständen viel gefährlicher. Anwender können darum gebeten werden, nicht auf suspekte E-Mail-Anhänge zu klicken, aber bösartige Websites können aktiven Code enthalten, der automatisch gestartet wird, sobald die Website geöffnet wird. Dies ist ein häufiger Nachteil von Web 2.0-Applikationen wie Blogs, Wikipedia und Networking-Sites wie MySpace, bei denen Anwender auch Code als Teil des erlaubten Inhalts posten dürfen.

Datendiebe, Industriespione und virtuelle Vandalen können innerhalb eines Unternehmens operieren. Aber Bedrohungen von innen sind nicht immer das Ergebnis eines absichtlichen Angriffs durch einen Insider: manchmal entstehen sie, wenn ein Mitarbeiter unbeabsichtigt eine „Hintertür“ öffnet oder sie offen lässt, indem er eine Anwendung herunterlädt, die nicht von der IT-Abteilung genehmigt wurde.

Wenn Daten nach außen gelangen, besteht gleich zweifacher Grund zur Sorge: 1) Es besteht die Gefahr des Verlusts geistigen Eigentums und 2) die Gefahr, gesetzliche Vorschriften zu verletzen. Viele Unternehmen meinen, dass die Filterung von E-Mails ausreichenden Schutz bietet.

Welche Fragen werden an das Unternehmens- und IT-Management gestellt?

Es gibt eine Vielzahl von Fragen, die im Zusammenhang „Sicherheit und IT“ zu beantworten sind:

- „Wie sicher und effizient arbeitet meine IT?“
- „Welche Risiken existieren – und wie können diese mit vertretbarem Aufwand reduziert werden?“
- „Wie hoch sind die IT-Kosten und wie kann ich diese nachhaltig senken?“

Diese und ähnliche Aspekte spiegeln das Umfeld wider, in dem sich das Thema „IT-Sicherheit“ bewegt.

Nur ein Teil aller Unternehmen hat ein Risikomanagement für IT-Sicherheit eingerichtet. Und das, obwohl deutsche Gesetze wie das Bundesdatenschutzgesetz, KonTraG, Aktiengesetz oder HGB die Einführung eines IT-Sicherheitskonzepts vorschreiben. Ab Juli 2008 greifen zudem EU-weit verschärfte Regeln in Bezug auf die Dokumentation der IT- und Telekommunikationsinfrastruktur eines Unternehmens.

Wie sicher sind Ihre IT-Systeme?

Selbst vermeintlich sichere IT-Systeme wie im Bundeskanzleramt konnten Hacker mit vergleichsweise einfachen Mitteln ausspionieren. Der Grund: Effektiver Schutz setzt voraus, dass man sich in die Rolle der Angreifer hineinversetzen kann. Unternehmen und Organisationen beauftragen noch zu selten Spezialisten, um ihre Netze mit Methoden der Angreifer auf Schwachstellen zu prüfen.

Als Faktoren in diesem Spannungsfeld spielen Themen wie **Verfügbarkeit, Integrität** und **Vertraulichkeit der Daten** eine Rolle, um drohenden (Image)-Schaden durch den Verlust von Forschungsergebnissen durch Sicherheitslücken in den IT-Systemen abzuwenden. Die Bedrohung bezieht sich hier auf die Bereiche

- Diebstahl von Zugangsberechtigungen
- Datenveränderung durch Unfälle
- Missbrauch von privilegierten Zugangsberechtigungen
- Datenmanipulation
- Anwendungsmanipulation
- Diebstahl von Hardware (Disks, Server, …)
- Diebstahl von Medien (Tapes)

Die Sicherheit dieser Bereiche ist durch geeignete Maßnahmen unmittelbar zu gewährleisten.

Welche Haftungsrisiken bestehen für die Geschäftsführung?

Neben den vorher genannten Faktoren existieren gestiegene **Haftungsrisiken für Verantwortliche** (die Geschäftsleitung). Bei Verstößen gegen die Einhaltung zahlreicher gesetzlicher Auflagen und Vorschriften für den ordnungsgemäßen Betrieb von IT-Systemen, wurden die Haftungsregelungen erweitert, z.B. um Organisations-, Kontroll-, Auswahl- und Einweisungsverschulden.

Was bedeutet das konkret für die Geschäftsführung?

Die gesetzlichen Regelungen zur IT-Sicherheit umfassen nicht nur das Haftungsrecht, sondern auch Steuer- und sogar Strafrecht. Die Strafen reichen vom Bußgeld bis zur Gefängnisstrafe. Bei der Frage, wer für den jeweiligen Regelungsbedarf verantwortlich ist, taucht überwiegend die Geschäftsführung auf.

- Die Geschäftsführung muss für die Sicherheit sorgen!
- Wer sorglos handelt, haftet! (Quelle: §93 AktG, §43 GmbHG)

Einige Beispiele

- **Szenario 1:** Sie sind Vorstand / Geschäftsführer einer Firma. Ein Hacker dringt in Ihr EDV System ein und entwendet vertrauliche Entwicklungsdaten Ihrer Kunden. Den Kunden entsteht Schaden. Diesen wollen sie von Ihrem Unternehmen ersetzt verlangen. Hilfsweise von Ihnen persönlich. Zu Recht?
    - JA, Manager haften für Datenverlust persönlich
- **Szenario 2:** Sie sind Vorstand / Geschäftsführer einer Firma. Einer Ihrer Mitarbeiter surft in Ihrem Auftrag im Internet und fängt sich einen Virus ein. Das merkt er nicht und er überträgt den Virus an einen Ihrer Kunden. Dem Kunden entsteht ein Schaden. Diesen will er von Ihrem Unternehmen ersetzt verlangen. Zu Recht?
    - JA. Schadensersatz bei Verbreitung eines Computervirus
- **Szenario 3:** Sie sind Vorstand /Geschäftsführer einer Firma. Die Firma betreibt auch einen Internetshop. Für ITSicherheit haben Sie sich nicht interessiert. Der Shop wird Opfer einer Attacke und kann tagelang nicht liefern, weil die Daten verloren gegangen sind. Es kommt zu großen Umsatz-Ausfällen. Ihr Gesellschafter will den Schaden von Ihnen persönlich ersetzt haben? Zu Recht?
    - JA, Schadensersatz bei Serverausfall

Welche Richtlinien spielen eine Rolle?

Der sichere IT-Betrieb bildet als technische Basis eine wichtige Säule für den Erfolg eines Forschungsunternehmens. Eine sichere IT ist notwendig für die Konzentration auf das Kerngeschäft – und sie ist bezahlbar. Dabei geben die gesetzlichen Regelungen den Rahmen vor, der über verschiedene Normen und Standards bis zu einzelnen Richtlinien innerhalb eines Unternehmens umgesetzt wird.

Wo liegen die Herausforderungen?

Die Herausforderungen bestehen unter anderem darin, die zahlreichen Rahmenbedingungen konkret für ein Unternehmen umzusetzen – und zwar unter Einhaltung aller Richtlinien, wobei es sich dabei um Unternehmensrichtlinien oder gesetzliche Richtlinien handeln kann. Man verwendet in diesem Zusammenhang auch den Begriff Compliance. Die sichere Speicherung (Storage und Security) und die Einhaltung gesetzlicher Richtlinien (Compliance) betreffen alle Unternehmen – unabhängig von ihrer Größe. Die Einhaltung gesetzlicher Anforderungen und Richtlinien (Compliance) bietet weitere Vorteile, z.B. bei der Geldbeschaffung am Kapitalmarkt. Durch den Nachweis eines sicheren und geprüften IT-Betriebes erhalten Unternehmen im Rahmen der BASEL II Richtlinien häufig günstigere Konditionen bei Kreditinstituten.

Was bedeutet das für die Praxis?

Beim Thema „IT-Sicherheit eines Unternehmens“ können Untersuchungen durch „Externe“ sinnvoll sein, um die folgenden Bereiche im Rahmen einer Analyse näher zu beleuchten:

- Definition der Sicherheitsanforderungen
- Durchführung von Risikoanalysen
- Revision von IT-Organisation, Technik und Betriebsverfahren
- Entwicklung IT-Security-Policies und sonstigen Betriebsvereinbarungen
- Erarbeitung und Umsetzung von Verbesserungsvorschlägen
- Implementierung von Sicherheits-Managementsystemen

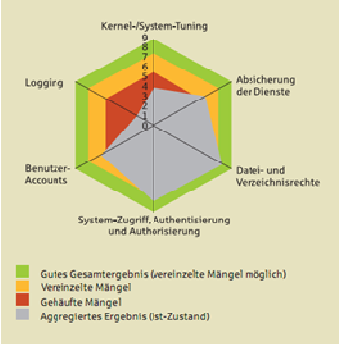
Wie läuft eine IT-Sicherheitsuntersuchung ab?

Bei diesen Untersuchungen (auch Audit genannt) werden sich die IT-Spezialisten zunächst einen **Überblick über das IT-Sicherheitsniveau** im Unternehmen verschaffen und erarbeiten auf Basis der Ergebnisse einen **Maßnahmenplan** zur Optimierung identifizierter **Verbesserungspotenziale**, die sich aus der Sicherheitsuntersuchung ergeben haben.

Dazu sind IT-Experten im Unternehmen **vor Ort** aktiv und befragen Ihre Mitarbeiter. Durch **Interviews** sowie **Einsichtnahme in vorhandene Dokumentationen** und die **Überprüfung von Anwendungs- und Systemkonfigurationen** kann der personelle Aufwand im Unternehmen möglichst gering gehalten werden.

Wie wird das Ergebnis einer Untersuchung präsentiert?

Auf Basis dieser Erhebung erfolgt eine **Ergebnisdokumentation** inklusive Antworten zum Fragenkatalog. Außerdem ist eine Beschreibung der **identifizierten Verbesserungspotenziale**, eine quantifizierte **Bewertung** sowie die managementgerechte **Darstellung der Ergebnisse** Bestandteil der Analyse. Als wichtiges Ergebnis der Analyse wird eine stichpunktartige **Maßnahmenempfehlung** mit einer **Priorisierung** zur Umsetzung abgegeben.



Grafik: Darstellung der Untersuchungsergebnisse

Warum Sicherheits-Audits?

- Proaktives Erkennen von Schwachstellen und Risiken
- Ergreifen von Gegenmaßnahmen, bevor es zu einem Schaden kommt
- Reduzierung der IT-Sicherheitsrisiken auf ein für das Unternehmen akzeptables Maß
- Einhaltung der gesetzlich relevanten Anforderungen
- Berücksichtigung nationaler und internationaler Standards und branchenspezifischer Anforderungen

Welche Bereiche werden untersucht?

- Organisatorische Konzepte
- Logisch/technische Konzepte
- Physische Konzepte
- Notfallkonzepte
- Betriebskonzepte
- Konzepte zu Vertragsbeziehungen
- Konzepte zur Wirtschaftlichkeit

Kontakt:

Markus Dietz
Vertrieb
GRASS-MERKUR AG & Co. KG
Rothwiese 5
30559 Hannover
Telefon: 05 11 47 54 14 – 0
Telefax: 05 11 47 54 14 – 33
Internet: www.grass-merkur.de
eMail: info@grass-merkur.de