 von Georg Magg

Cash Cow 2005: Content Security
Unter schwerem Boom-Verdacht: Identity und Access Management
Gefährlich vernachlässigtes Stiefkind: eBusiness Security
Vom Aussterben bedroht: Intrusion Detection Systeme

Der führende europäische IT Security-Dienstleister Integralis (www.integralis.de) hat auf die Frage, wohin sich die IT Security im nächsten Jahr entwickeln wird, eine ganze Reihe von Prognosen im Gepäck. Während einige Themen wie Intrusion Detection oder Trusted Operating Systems in ihren gängigen Einsatzbereichen vom Aussterben bedroht sind, scheinen manche Technologien, die bislang als zu kompliziert oder zu teuer galten, ihre Kinderkrankheiten auskuriert zu haben. Dazu gehört beispielsweise das Identity und Access Management, aber auch die vieldiskutierten Managed Security Services. Die folgenden Prognosen stammen von erfahrenen Integralis-Spezialisten, welche den IT Security-Markt, seine Klientel sowie die Schwankungen und Nöte der Branche aus jahrzehntelanger Erfahrung kennen.

1. Wie beurteilen Sie die Entwicklung der folgenden IT Security-Themen in 2005?

Content Security
(E-Mail-/Web-Filtering, Risiko durch eigene Mitarbeiter etc.)
Die Cash Cow 2005 wird Content Security sein. Die Bekämpfung von Adware könnte ein Renner werden, E-Mail- und Web-Filter boomen weiterhin auf hohem Niveau und die reglementierte Nutzung des Internets wird sich weiter verbreiten. Aktuelle Studien bestätigen, dass die meisten Schäden nach wie vor durch die eigenen Mitarbeiter erfolgen. Allerdings handelt es sich hier in der Regel um unabsichtliche Schädigungen, d.h. durch versehentliches Einschleusen von Malware in Firmennetzwerke und ähnliche Versehen. Auch

PrintausgabeIn der Printausgabe der NEWSolutions Februar 2005 ist ein Anriss des Artikels erschienen, lesen Sie hier den vollständigen Artikel.

hier ist Content Security in Kombination mit einer entsprechenden Firmen-Policy die sinnvollste Gefahrenabwehr.

Mobile Security

(WLAN Security, Bluetooth Security, Handy Security)
Mobile Security ist auf dem Vormarsch, allerdings findet der große Boom noch nicht in 2005 statt. Für manche Branchen wie dem Transportwesen, Universitäten oder Anbietern von WLAN Hotspots gewinnt das Thema aber schon in 2005 an Bedeutung. Generell wird der Trend in Richtung Client Security-Lösungen gehen, um Notebooks und PDAs der mobilen Mitarbeiter zu schützen. Solange Handys noch keine PDA-Funktionalitäten haben, werden sie von Firmen als Datenträger auch noch nicht ernst genommen. Bislang werden Mobile Security-Lösungen von kleineren Anbietern angeboten, aber die Branchenriesen rüsten auf.

Identity und Access Management / Biometrie

Identity und Access Management ist der heißeste Wachstumskandidat für 2005: Technologien wie SmartCards sind reif für den breiten Einsatz und der steigende Bedarf in der Wirtschaft ist deutlich spürbar. Zukünftig wollen die meisten Firmen für ihre Mitarbeiter eine Single Sign-on-Lösung, welche den Zugang zu Eingängen, Diensten, PCs, Daten etc. kontrolliert und regelt. Das Einsparpotenzial ist hierbei so überragend, dass die Investitionsbereitschaft in 2005 deutlich ansteigen wird. Im Gegensatz dazu werden sich biometrische Anwendungen vermutlich auf spezielle Teilbereiche wie die grenzüberschreitende Personenkontrolle beschränken.

Managed Security Services

Dieses Thema wird zunehmend wichtiger, vor allem auch für den Mittelstand, der aus Kosten- und Personalgründen zunehmend nach Komplettlösungen und -Services sucht. Da die Betriebskosten für IT-Aufwendungen verstärkt vom Top-Management kontrolliert werden, kommen auch Managed Services zunehmend als kostengünstigere Alternative in Frage. Neben den klassischen Managed Services wie Firewall- oder E-Mail-Management werden neue Dienste wie Managed SSL-VPN oder Managed Authentication gefordert werden. Derzeit besteht noch eine Anbieterschwemme am Markt, die sich aber mittelfristig konsolidieren wird.

eBusiness Security

Im Prinzip ist mittlerweile fast jeder zweite Webauftritt bzw. Webshop hochgradig angreifbar, aber die meisten Firmen wollen das nicht wahrhaben und erfolgreiche Angriffe werden aus Imagegründen sorgsam verschwiegen. Hier wird von Firmenseite aus gefährlich gespart, voraussichtlich auch in 2005. Erst dann, wenn das schwindende Vertrauen der Verbraucher durch die Summe der veröffentlichten Skandale zu einem signifikanten Kundenschwund führt, wird hier ein Umdenken stattfinden.

Intrusion Prevention/Vulnerability Management

Das schnelle Erkennen von Schwachstellen und das sofortige Abwehren von Angriffen in Netzwerken wird in 2005 und den folgenden Jahren ein Wettlauf mit der Zeit und professionellen Hackern werden. Die immer häufiger und schneller lancierten Angriffe gegen Schwachstellen in Betriebssystemen und Programmen sowie der Wettlauf mit dem Einspielen von Patches erfordert komplexe Lösungsansätze, die stark im Kommen sind. Dazu zählen Intrusion Prevention Systeme (IPS), Vulnerability und Patchmanagement sowie die Segmentierung von Netzwerken. Hersteller,

die beispielsweise IPS und Vulnerability Management im Angebot haben, verschmelzen bereits ihre entsprechenden Produkte hierzu.

2. Welche IT Security-Themen werden in 2005 vom Aussterben bedroht sein?

Intrusion Detection Systeme (IDS): ID-Systeme haben sich in der Vergangenheit als zu kompliziert, zu aufwändig und letztlich auch zu kostspielig erwiesen. Die Hersteller selbst unterstützen das Ableben dieser Technologie, um möglichst bald die Nachfolge mit Intrusion Prevention Systemen antreten zu können. Trusted Operating Systems: Die gehärteten Betriebssysteme erfordern einen enormen Konfigurationsaufwand, sehr viel spezialisierte Expertise, sind mit vielen Produkten nicht kompatibel und können durch klassische IT Security-Tools wie Firewalls etc. problemlos ersetzt werden.

3. Wie werden sich die Änderungen von rechtlichen Vorschriften (Sarbanes Oxley, Basel II, neue Zertifizierungen etc.) in 2005 auf die IT Security- Strategien in den Unternehmen auswirken?

Gesetzliche Regelungen und Anforderungen durch Sarbanes Oxley oder Basel II werden in 2005 zwar verstärkt greifen, der subjektive Druck der Firmen, hierauf mit geeigneten IT- Maßnahmen zu reagieren, ist aber noch nicht groß genug. Branchen wie Banken, Versicherungen, Pharmahersteller oder Lotteriegesellschaften sind bereits gewappnet, aber das Gros der Firmen hat noch gar keinen Überblick, was von ihnen zukünftig an Security-Auflagen und -Standards gefordert wird. Sicherheitsstandards wie beispielsweise BS7799 werden mittelfristig zu einem neuen Qualitätsstandard für IT-Dienstleister werden – vergleichbar mit ISO 9000. Insgesamt wird die neue Rechtslage einen entscheidenden Richtungswechsel mit sich bringen: IT Security wird aus Haftungsgründen zunehmend zur Chefsache.

4. Was sind die größten IT Security-Stolpersteine?

A. Management-Fehler

Viele Firmen haben noch nie definiert, was sie warum schützen wollen. Hieraus resultieren oftmals Ad-hoc-Entscheidungen oder Investitionen „aus dem Bauch heraus“. Meist wird dann erst Geld in die Hand genommen, wenn ein gravierender Verlust entstanden ist. Problematisch ist auch, dass das Management häufig nicht das langfristige Firmenwohl, sondern persönliche „Quartalsziele“ anvisiert.