IT-Sicherheitstrends 2011

19.01.2011, 12:08 | IT, New Media & Software

Pressemitteilung von: *Applied Security GmbH*
Presseagentur: *Mainblick - Agentur für Öffentlichkeitsarbeit*

Dr. Volker Scheidemann

Interview mit Dr. Volker Scheidemann, Marketingleiter bei der Applied Security GmbH (apsec), über IT-Sicherheit in Zeiten von Wikileaks

Vollkommene IT-Sicherheit gibt es nicht. Eine vermeintlich ernüchternde Erkenntnis, die wie eine Entschuldigung klingt, um die Händen in den Schoß legen zu dürfen. Doch in Wahrheit ist sie ein mahnender Appell an deutschen Unternehmen, keine sinnvolle Sicherung auszulassen. Denn sonst bleibt dem Datenklau Tür und Tor geöffnet. Dr. Volker Scheidemann, Autor zahlreicher Fachbeiträge und seit mehr als zehn Jahren Referent zu Sicherheitsthemen auf verschiedenen Veranstaltungen, erläutert in einem Interview aktuelle Sicherheitstrends. In diesem Zusammenhang empfiehlt er grundlegende Schritte, damit das Jahr 2011 nicht durch seine Sicherheitslücken in Erinnerung bleibt.

Welche Trends haben im vergangenen Jahr die Entwicklung der IT-Sicherheit geprägt?

Bei vielen Unternehmen haben gestiegene Anforderungen hinsichtlich IT-Compliance und Risikomanagement die Entwicklungen geprägt. Und seit den Wikileaks-Veröffentlichungen Ende letzten Jahres ist natürlich das Thema Datenklau wieder in aller Munde. Dabei werden in der öffentlichen Wahrnehmung hier gerne, wie so häufig, Botschaft und Bote verwechselt. Ich möchte hier noch einmal betonen: Wikileaks hat keine Daten gestohlen, sondern die Allgemeinheit nur darauf hingewiesen, dass sie in unbefugte Hände gelangt sind. Die Diskussion, gerade auch um Julian Assange, der als böser Bube an den Pranger gestellt wird, erinnert mich an die jahrelangen Anfeindungen, die zum Beispiel der CCC (Chaos Computer Club) hinnehmen musste, weil er Sicherheitslücken in Unternehmensnetzen aufdeckte. Auch hier wurde der Bote ungerechtfertigter Weise lange kriminalisiert, um von der Botschaft – mangelnde IT-Sicherheit – abzulenken.

Gibt es aktuell neue Gefährdungen, deren Bedrohungspotenzial von vielen Unternehmen noch nicht ausreichend gewürdigt wird?
Ja und nein. Ja, weil die Angriffe immer ausgefeilter werden, wie uns im letzten Jahr beispielsweise der sehr speziell auf iranische Atomanlagen ausgerichtete Stuxnet-Wurm bewiesen hat. Und nein, weil die Unternehmen bereits die vorhandenen Bedrohungspotenziale nicht hinreichend zur Kenntnis genommen haben. Außerdem beweisen Statistiken wie zum Beispiel die regelmäßigen Umfragen der Zeitschrift , dass die Top-Bedrohung für die Datensicherheit seit Jahrzehnten die gleiche ist: menschliche Fehler.

Welche Sicherungsmaßnahmen sollten deutsche Unternehmen im Jahr 2011 nachrüsten?
Technisch nachrüsten sollte man dort, wo es einerseits bisher wenig Sicherheitsmaßnahmen, andererseits eine große Bedrohung gibt. Dazu gehören meiner Ansicht nach vor allem Systeme zum Identitäts- und Zugriffsmanagement und zur Verschlüsselung sensibler Daten. Auch hier kann ich wieder den Fall Wikileaks anführen. Wie kann es sein, dass auf solch hochbrisante Daten aus dem amerikanischen Ministerium fast eine Million Menschen unkontrolliert Zugriff hatten? Hier gab es offenbar weder eine Zugriffskontrolle, noch waren die Dokumente verschlüsselt. Und daran war definitiv nicht Wikileaks schuld.

In welchem Bereich sehen Sie als Experte den größten Handlungsbedarf?
Bei der Sensibilisierung von Mitarbeitern auf allen Unternehmensebenen – vom Pförtner bis hinauf zum Top-Manager. Von letzterem wünsche ich mir vor allem die Einsicht, dass aus der Wertschätzung der Mitarbeiter unmittelbar eine Wertschöpfung für das Unternehmen resultiert. Ein zufriedener Mitarbeiter ist loyal und lässt nicht mal eben die Kundendatenbank mitgehen. Auch ist er generell achtsamer beim Umgang mit Unternehmensdaten. Das ist eine wirkungsvollere Verteidigung von Unternehmenswerten, als es die stärkste Firewall je sein könnte. Letztlich verbirgt sich hinter den Schlagworten Governance, Risk und Compliance (GRC), die im Zusammenhang mit IT-Sicherheit oft genannt werden, nichts anderes als eine moderne Form des Prinzips vom „ehrbaren Kaufmann“. Ein Prinzip, das viele Unternehmen aber leider vergessen haben. Jetzt versucht man, es unter dem Kürzel GRC den Unternehmen wieder nahezubringen. Ich finde das eine positive Tendenz, die auch wir von apsec in unserem Beratungsangebot unterstützen.

Haben Sie in den letzten Monaten auch erfreuliche Entwicklungen wahrgenommen?
Durchaus. Insbesondere ist die Zahl derer zurückgegangen, die das Bemühen um IT-Sicherheit grundsätzlich negativ bewerten. Lange Zeit musste man sich als Sicherheitsberater wie Kassandra vorkommen, die warnt und auf die niemand hören will. Wir wissen, was mit Troja passiert ist. Heute sind wir zumindest insofern einen Schritt weiter: Man muss mit Unternehmen in der Regel nicht mehr darüber streiten, dass IT-Sicherheit überhaupt notwendig ist, sondern darüber reden, welche Maßnahmen ergriffen werden sollten. Hier können wir von apsec unsere Expertise anbieten. Und wenn es kein Standardprodukt für spezielle Unternehmensanforderungen gibt, schaffen wir eine individuelle Lösung. Das ist unsere Stärke.

Die IT-Sicherheitslage in deutschen Unternehmen verbessert sich 2011, wenn…?
Erstens, wenn sich die Erkenntnis in den Köpfen der Manager weiter manifestiert, dass IT-Sicherheit einen positiven Wert hat, der auch Investitionen rechtfertigt.
Zweitens, wenn ebendiese Manager akzeptieren, dass auch eine 80-Prozent-Lösung gut ist. Viele neigen nämlich zu „digitalen“ Ja-Nein-Entscheidungen: Wenn eine Sicherheitslösung keine 100 Prozent Sicherheit verspricht, verzichten sie gleich ganz. Das Problem ist nur: Hundertprozentige Sicherheit lässt sich nicht ehrlich garantieren.
Drittens, wenn alle einsehen, dass IT-Sicherheit nichts Abstraktes ist, sondern jeden individuell betrifft. Leider habe ich wenig Hoffnung, dass sich diese Einsicht im großen Stil durchsetzt. Denn wir Menschen neigen nun einmal dazu,

Probleme immer zuerst bei „den anderen“ zu sehen. Die Psychologen nennen dies das „It won’t happen to me“-Phänomen.

Welche positive Schlagzeile zum Thema IT-Sicherheit wünschen Sie sich für 2011?
Frei nach Galileo Galilei: „Und sie verschlüsseln doch!“

Weitere Informationen: www.apsec.de.

Portrait

apsec schützt Wissen. Wissen ist der entscheidende Erfolgsfaktor eines Unternehmens. Wir entwickeln für Sie Lösungen, die Ihre IT-Welt sicher machen.
apsec bietet Wissen. Ihre Anforderungen zur Verschlüsselung, zur Data Leakage Prevention oder zur Anwendung digitaler Signaturen sind bei unseren erfahrenen Spezialisten in guten Händen.
apsec arbeitet für Sie. Wir bieten von der Prozessberatung über Softwareentwicklung bis zum Support ein Komplettpaket mit einem einzigen Ziel – Ihre Zufriedenheit.

News-ID: 502384 • Views: 113 (Stand: 02.06.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/502384/IT-Sicherheitstrends-2011.html