Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 76 (1998)

Heft: 10

Vorwort: Im Wettlauf zwischen Angriff und Abwehr

Autor: Gysling, Hannes

Im Wettlauf zwischen Angriff und Abwehr

Sicherheitsfragen in der Telekommunikation werden auf absehbare Zeit ein Dauerproblem bleiben. Das ergab sich auf dem Kongress des Münchner Kreises, der am 7. und 8. Juli 1998 im Europäischen Patentamt München stattfand. Ganz bewusst hatten ihn die Veranstalter unter das Generalthema «Vertrauenswürdige Telekommunikation» gestellt, denn angesichts der zunehmenden Abhängigkeit unserer Gesellschaft von den Systemen der Informations- und Telekommunikationstechnik drängt sich die Frage auf, unter welchen Voraussetzungen man sich ihnen und den darauf basierenden Dienstleistungen anvertrauen kann.
Das scheinbar klare Ziel – Schutz der übertragenen Informationen – wird nur unvollständig erreicht. Aber auch das einsetzbare Instrumentarium zur Abwehr von Angriffen auf schutzwürdige Informationen wie technische Massnahmen (Sicherheitsarchitekturen, Verschlüsselungstechniken), organisatorische Massnahmen (Sicherheitsmanagement, Zertifizierungen), gesetzliche Regelungen weist Lücken auf und bedarf ständiger Anpassung.

Angesichts der zunehmenden Expansion des elektronischen Geschäftsverkehrs (Electronic Commerce) wächst die Verwundbarkeit der in diesem neuen Sektor engagierten Unternehmen. Verstärkt wird die Sicherheitsproblematik noch durch die weitgehende Heterogenität der informations- und kommunikationstechnischen Infrastrukturen sowie die wachsende Vermaschung interner und externer Netze (Intranet und Internet). Hier ist wirkungsvolles Sicherheitsmanagement gefragt. Jedoch mangelt es vielerseits noch am Risikobewusstsein. «Die meisten Leute wissen nicht, wie offen ihre Systeme sind», konstatierte US-Referent Dr. Eugene Schultz (SAIC, Menlo Park/Kalifornien). Das US-Verteidigungsministerium veranstaltete 1995 sogenannte «Penetration Tests» in 38 000 Fällen. Davon erwiesen sich 65% als leicht angreifbar, aber nur 3% haben den Angriff bemerkt. Von diesen haben aber bloss 200 von dem Vorfall berichtet, obwohl eigentlich alle dazu verpflichtet gewesen wären.

Über ein wachsendes Bedrohungspotential und ständige Angriffe auf sein System berichtet auch Erich Lambert von der Hypovereinsbank: «Wir werden tagtäglich an unserer Firewall angegriffen.» Nach seinen Beobachtungen wächst die Industriespionage. Penetration Tests gehören deshalb zum täglichen Pensum der Sicherheitsmassnahmen. Zur sicheren Authentisierung werden im Verkehr mit den Kunden Verschlüsselungstechniken (public und private key) eingesetzt. Zum Sicherheitsinstrumentarium gehören raffinierte Verschlüsselungstechniken, ISDN-Sicherheitsmechanismen, Authentisierungsprotokolle und spezifische Zugriffsregelungen.

Sicherheitslücken sind dennoch nicht völlig vermeidbar. Das gilt insbesondere bei der Nutzung des Internets. In den USA begann man vor zehn Jahren mit der Schaffung sogenannter Notfallteams. Das sind Expertengruppen für die pragmatische Hilfe bei konkreten Sicherheitsproblemen. Ziel dieser Computer-Notfallteams ist der richtige Umgang mit Vorfällen und Angriffen. In dem Bewusstsein, dass eine 100-Prozent-Sicherheit nicht erreicht werden kann, geht es dabei vor allem um die Sicherung der Kontinuität, im Extremfall sogar um die Sicherung der Überlebensfähigkeit des Unternehmens. Ein beträchtliches Mass an verbesserter Datensicherheit prophezeit Gerhard Wiehler (Siemens Nixdorf) mit dem Ausbau der Chipkarten-Technologie. Dem Markt für die intelligenten Chipkarten sagt Wiehler ein rasantes Wachstum voraus: Während das weltweite Marktvolumen 1997 noch bei 405 Mio. Dollars lag, werden für 2002 insgesamt mehr als 2,9 Mia. Dollars erwartet. Grösster Markt wird der Zahlungsverkehr (29 %) sein. Die grössten Zuwachsraten wird allerdings mit jährlich 77 % der Sektor «sicherer Zugang» aufweisen.

Hannes Gysling