

SECURITY-KONGRESS 2002

Gefahren von innen und außen

Die Sicherheit in der Informationstechnologie war einer der Schwerpunkte beim Security-Kongress vom 7. bis 10. Oktober 2002 im Rahmen der „Security 2002“ in Essen.

Hundertprozentige Sicherheit gibt es auch im Bereich der Informationstechnologie nicht. Aber man kann etwas für sie tun. Angriffe können durch Intrusion-Detection-Systeme erkannt und unberechtigte Zugriffe durch Firewalls abgewehrt werden. Etwa 80 Prozent der Angriffe erfolgen von innen, also durch Mitarbeiter bewusst oder durch nachlässigen Umgang mit Sicherheitsvorschriften. In der Telekommunikation kommen zu den allgemeinen Gefahren für die Integrität, Vertraulichkeit und Verfügbarkeit von Daten weitere Risiken.

Bei Telebanking, Teleshopping, Tele-Medicine, E- und M-Commerce werden sensible Daten übermittelt. Es muss sichergestellt sein, dass keine Fehlleitung oder Veränderung von Daten, aber auch kein Mithören möglich ist, die Sicherheit der Verbindung muss gegeben sein und es muss auch sichergestellt sein, dass die Gebühren korrekt zugeordnet werden. So genannte „Leistungsmerkmale“ bei Telefonen wie Zeugen- und Konferenzschaltungen bergen die Gefahr, zum Abhören missbraucht zu werden, wenn die automatische Rufannahme freigegeben ist.

Drahtlose Netze (Wireless-LANs) sind immer häufiger anzutreffen, weil man sich Verkabelungsaufwand spart und der Anwender mobil sein kann. Der Nachteil ist, dass sich ein Angreifer nicht einmal mehr in eine Leitung einklinken muss; es genügt, wenn er sich im Empfangsbereich der Funkwellen befindet. Zudem kann er kaum geortet werden.

„War Driving“ oder „Drive-by Hacking“ ist die Bezeichnung der Methode, mobil (vom Auto aus) unbefugt Datenfunk aufzuspüren, ihn mitzuverfolgen (insbesondere Passwörter) und in die Rechner einzudringen. Sicherheitstechnische Schwachstellen bei den Endgeräten werden von den einschlägigen Programmen automatisch abgescannt und angezeigt. Gelingt es einem Eindringling, eine falsche Identität vorzutäuschen, kann er auf Kosten des anderen kommunizieren. Die Herstellung einer Ende-zu-Ende-Sicherheit sowie Datenverschlüsselung und Authentisierung der Teilnehmer sind jedenfalls bei sensiblen Anwendungen zu fordern.

Videoüberwachung

Neue im Netz betriebene Videokameras geben nur dann Alarm, wenn sich wirklich etwas Außergewöhnliches im Überwachungsbereich ereignet. Damit wird auch die Datenfülle bewältigbar, die die menschliche Aufmerksamkeit überfordert. Möglich wird das durch Prozessoren und mathematische Verfahren, die aus einem Videobild Merkmale extrahieren, sodass aus Kontrastübergängen und Bereichen mit gleicher Oberflächenbeschaffenheit (Textur) Objekte erkannt werden und deren Bewegungsrichtung ermittelt werden kann. Derartige Verfahren zur Bildinterpretation lassen sich bis zu Assistenzsystemen im Fahrzeugverkehr ausbauen, etwa zur automatischen Verkehrszeichenerkennung oder zur Spurhaltung auf der Fahrbahn, als Hilfe beim Einparken, zum Erkennen von Geisterfahrern (falsche Bewegungsrichtung) oder zur automatischen Erkennung von Kfz-Kennzeichen.

Gegenstände, etwa „vergessene“ Gepäckstücke, von denen Gefahr ausgehen kann, können ebenso erkannt werden und zur Alarmauslösung bzw. dem Start der Videoaufzeichnung führen wie Objekte, die keine zielgerichtete Bewegung aufweisen: Nur der rechtmäßige Besitzer eines Kraftfahrzeugs bewegt sich direkt auf sein Fahrzeug zu, Diebe bewegen sich einmal zu dem einen, dann wieder zu dem anderen Auto.

Durch solche Verfahren wird die Kamera zu einem Sensor, wie etwa zu einer Einbruch- oder Brandmeldeanlage. Rauchausbreitung wird durch Konturbildung oder Kontrastverringern im Bild erkannt, ebenso offene Flammen. Zutrittskontrollsysteme auf der Basis der Gesichtserkennung beruhen letztlich ebenfalls auf Verfahren der Bildinterpretation.

Kurt Hickisch

BUDAPEST

Security + Safety 2002

Die „Security+Safety“ in Budapest zählt zu den wichtigsten Sicherheitsmessen in Osteuropa. Etwa 150 Aussteller präsentierten auf der „Security+Safety 2002“ vom 6. bis 9. November in der ungarischen Hauptstadt Produkte und Dienstleistungen aus fast allen Bereichen der Sicherheitstechnik.

Vor allem in den Bereichen Videoüberwachung und Brandschutz hätten die Aussteller den aktuellen Stand der Technik präsentiert, betonte Herbert Hübl von Schrack-Seconet, einem der österreichischen Unternehmen, das auf der internationalen Fachausstellung und Konferenz für Sicherheitstechnik und Objektschutz vertreten waren. Die Schrack Seconet Sicherheits- und Kommunikationssysteme AG hat sich spezialisiert auf Brandmeldeanlagen, Kommunikationssysteme für Krankenhäuser, Pflege- und Altenheime, Einbruchmeldetechnik, Videotechnik und Zutrittskontrolle.

Ungarn ist einer der wichtigsten Handelspartner Österreichs. Rund 6.000 österreichische Unternehmen sind in Ungarn vertreten. Zu den größten Investoren zählen die Prinzhorn Gruppe, OMV, Agrana, Voest-Alpine, EVN und die Erste Bank.

SECURITY-KONGRESS

80 Referate

Der traditionelle Kongress im Rahmen der weltgrößten Sicherheitsmesse „Security“ im Congress-Center Süd der Messe Essen wurde von der Simedia GmbH, Bonn organisiert.

Es gab 80 Referate zu Fragen der Sicherheit, mit den Themen-Schwerpunkten Brandschutz und Löschanlagen, Sicherheits- und Krisenmanagement, Unternehmenssicherheit und Werkschutz, Einbruchdiebstahl und Gefahrenmeldetechnik, Zutrittskontrolle, Videoüberwachung, IT- und TK-Sicherheit. Ein Halbtage war dem Thema „Sicherheit und Ästhetik“ in der Architektur gewidmet, wobei Sicherheitslösungen vorgestellt und prämiert wurden, die auch ästhetischen Ansprüchen gerecht werden.

<http://www.simedia.de/>