Höchste Priorität: **Sicherheit**

von K. Martin

Mit der Öffnung der IT-Netzwerke drohen auch Viren, Würmer und Hacker. Um diese Gefahren abzuwehren, müssen einzelne Lösungen wie Firewalls, Virenschutz oder Intrusion-Detection-Systeme in eine Sicherheitsstrategie eingebunden werden.

Ohne Internet und Intranet, ohne E-Mail und E-Government ist eine moderne Verwaltung heute nicht mehr vorstellbar. Voraussetzung für die Akzeptanz des Online-Behördengangs bei den Bürgern sind allerdings sichere Infrastrukturen – und vor allem in punkto IT-Security sind die Anforderungen an die öffentlichen Verwaltungen sehr hoch. Nicht verwunderlich also, dass nach einer Untersuchung des Marktforschungsunternehmens IDC vom Juni vergangenen Jahres 72 Prozent der europäischen Behörden Sicherheit als das absolute Kernthema ihrer IT betrachten.

Der Grund für diese hohe Priorität: Die zunehmende Vernetzung durch das Internet öffnet die Schwachpunkte jedes einzelnen Systems für alle anderen Netzteilnehmer. Denn sobald zwischen dem lokalen Netz (LAN) und dem Internet eine Verbindung besteht, können Angreifer versuchen, Daten zu stehlen oder Denial-of-Service-Angriffe – Attacken auf die Funktionalität der IT – zu starten. Damit sensible Informationen, beispielsweise Bürgerdaten, nicht in falsche Hände geraten und der Betrieb des eigenen LANs sowie der Server gesichert ist, müssen die Verantwortlichen in den Verwaltungen das lokale Netzwerk vor Angriffen von Außen schützen. Bewährtes Mittel gegen unerwünschte Eindringlinge: Eine Kombination von Firewall- und Intrusion-Detection-Lösungen.

Die Aufgabe einer Firewall ist es, die Kommunikation zwischen zwei Netzen – beispielsweise einem Behördennetz und dem Internet – zu kontrollieren. Dazu überprüfen sie den Datenfluss und vergleichen alle ein- und ausgehenden Datenpakete mit der durch die Konfiguration festgelegten Sicherheitspolitik. Unerwünschte Daten werden dabei herausgefiltert. Ein Intrusion-Detection-System (IDS) setzt bei den möglichen Wirkungen des Datenverkehrs an. Über Sensoren sammelt und analysiert es Daten über den momentanen Zustand von einem oder mehreren Computer-Systemen beziehungsweise Computer-Netzen und gleicht diese mit verschiedenen Mustern ab, die im System hinterlegt sind.

Der wesentliche Vorteil eines IDS: Nicht nur Angriffe von außerhalb des Behördennetzwerkes können dadurch entdeckt werden. Auch Missbrauch durch eigene Mitarbeiter wie Datendiebstahl oder Spionage wird offengelegt. Laut Studien aus den USA kommen rund 60 Prozent aller Angriffe von innen. Ein Intrusion-Detection-System ergänzt somit eine Firewall, welche nicht zwischen Gut und Böse unterscheiden kann, sondern Datenpakete anhand des Zielports und eventuell der Ziel-IP passieren lässt.

IT-Sicherheit: Vorrangiges Thema bei Behörden.

Doch Intrusion-Detection-Systeme sind in der Praxis umstritten. Vor allem eine hohe Anzahl falscher Alarme stellen die IT-Administratoren vor große Herausforderungen. Eine detaillierte

Analyse der Netzwerk-Architektur, des verwendeten Equipments, der Computer-Anwendungen sowie der Betriebsprozesse und Sicherheitsanforderungen ist daher genauso erforderlich wie eine ständige Anpassung des IDS. Und auch Firewall-Systeme sind komplex und bedürfen einer wohlüberlegten Sicherheitsstrategie. Grundlage für den erfolgreichen Einsatz ist ein vorbereitendes Konzept sowie die regelmäßige Wartung, die regelmäßige Analyse der vom Firewall-System erstellten Protokolle und das Anpassen der Policy an veränderte Bedingungen.

Eine weitere Gefahrenquelle für die IT-Systeme der öffentlichen Verwaltung sind Computer-Viren. Nach Angaben unterschiedlicher IT-Sicherheitsdienstleister hatten die Cyber-Bazillen bereits im Jahr 2003 weltweit Schäden in Höhe von bis zu 55 Milliarden Euro verursacht. Und die Prognosen für dieses Jahr sagen noch größere Schäden voraus. In der deutschen Privatwirtschaft werden nach einer Untersuchung der Meta Group Virenbefall und bösartige Codes als eindeutig höchstes Sicherheitsrisiko eingestuft.

Doch die Anwender sind solchen Gefahren nicht schutzlos ausgesetzt. Es existieren zahlreiche wirksame Tools, die derartigen Schädlingen den Garaus machen. Und dennoch: Die Schäden durch Virenattacken nehmen zu, obwohl inzwischen auch Virenschutz-Tools großflächig verwendet werden. Eine Befragung der amerikanischen Sicherheitsexperten von ICSA Labs von 300 IT-Verantwortlichen aus Unternehmen und Behörden ergab, dass mehr als 90 Prozent der Unternehmen über 90 Prozent ihrer PCs mit Virenschutzprogrammen ausstatten. Bei rund 70 Prozent kommen sogar automatisierte Virenschutzprogramme zum Einsatz, welche die Schädlingsbekämpfung ebenso wie notwendige Updates automatisch vornehmen. Permanente Updates müssen aber auch bei Betriebssystemen und der Anwender-Software durchgeführt werden, damit vorhandene Sicherheitslücken geschlossen werden. Ein funktionsfähiges Patch-Management zur Abwehr von Viren ist heute sehr wichtig, wie das jüngste Beispiel „Sasser“ überdeutlich zeigt.

Handlungsbedarf: 55 Milliarden Euro Schäden durch Viren.

Der bloße Einsatz entsprechender Programme und Hardware gegen die einzelnen Bedrohungen ist nicht mehr ausreichend – eine Lösung zu kaufen und einfach zu starten funktioniert nicht. Denn das Thema Security gewinnt zunehmend an Komplexität – so kam auch das US-Marktforschungsunternehmen Gartner Group bereits im Jahr 2002 zu dem Schluss: „Sicherheit von Informationen ist eine Frage von regelorientiertem Sicherheitsmanagement, keine Frage der Technologie.“ Um den vielfältigen Bedrohungen im IT-Umfeld angemessen zu begegnen, müssen beispielsweise Prozesse und Organisation schnell und qualifiziert reagieren können. Für die Umsetzung von umfassenden Sicherheitsmaßnahmen werden Mitarbeiter benötigt, die das notwendige Security-Know-how über alle Themenfelder hinweg besitzen. Unter Umständen benötigt eine Behörde hierfür auch neues Personal, das rund um die Uhr schnell und qualifiziert reagieren kann. Wegen der wechselnden Anforderungen und der sich dynamisch verändernden Bedrohungspotenziale ist eine kontinuierliche, aktive Weiterbildung für die Verantwortlichen unverzichtbar – weit über das Maß anderer Tätigkeitsfelder hinaus.

Nach einer Studie der Meta Group aus dem Jahr 2002 bringen hier externe „Managed Security Services Provider“ (MSSP) eine Reihe von Vorteilen. Die öffentlichen Verwaltungen können beispielsweise davon profitieren, wenn sie die geeigneten Fachkräfte oder das Know-how im Haus nicht verfügbar haben oder sich nicht mit diesen extrem Know-how-intensiven Aufgaben außerhalb ihrer Kernkompetenz intensiver befassen wollen.

Klaus Martin ist Practice Manager Security bei Siemens Business Services Deutschland.