

Tatort Computer

Cyber-Verbrecher agieren zunehmend professioneller, ihr Motiv ist das schnelle Geld. Die Hersteller von Antiviren-Lösungen befinden sich im Katz- und Maus-Spiel mit den Hackern.



Sicherheitscheck

Hacker haben Windows aufgrund seiner hohen Verbreitung besonders ins Auge gefasst. Microsoft versucht daher mit seiner weltweiten Sicherheitsinitiative das Bewusstsein der Anwender für Computersecurity zu schärfen. Für Unternehmen bietet der Konzern mit dem Microsoft Security Assessment Tool (MSAT) ein kostenloses Programm zur IT-Risiko-Selbsteinschätzung. Dabei erhält man auch Informationen und Empfehlungen zu Industrie-Sicherheitsstandards. Die Anwendung richtet sich gezielt an Unternehmen mit weniger als 1.000 Mitarbeitern und ist auf der Website www.microsoft.com/austria/security unter dem Punkt „Informationen für Geschäftskunden“ zu finden.

Wer die Überprüfung des Sicherheitsstands seines Unternehmens durch einen Profi wünscht, kann den Check auch von einem Partner-Unternehmen des Software-Konzerns durchführen lassen.

Mensch mag es bequem. Wegen einer Überweisung geht man nicht mehr extra zur Bank, man schaltet einfach den Computer ein und erledigt die Transaktion mit wenigen Klicks. Das geht auch ganz flott vom Arbeitsplatz aus. Soweit so gut. Die schlechte Nachricht: Bei über 200 neuen Banking-Trojanern täglich überlegt man es sich zweimal, ob man nicht doch lieber selbst zur nächsten Bank-Filiale geht. Tatsache ist, die Anzahl der Internetschädlinge nimmt zu und die Cyber-Kriminellen werden immer professioneller. Unternehmen, die ihren Virenschutz vernachlässigen, gehen ein hohes Risiko ein.

Virentrend: Trojaner

Trojanische Pferde und gehackte Websites sind derzeit die größten Sicherheitsbedrohungen für Unternehmen, sind sich die Virenexperten einig. „Die aktuellen Gefahren sind vielfältiger und das Risiko eines Angriffs ist größer geworden“, fasst Candid Wüst, Virenexperte von Symantec zusammen. Vor allem kleine und mittlere Unternehmen sind in der Hacker-Gemeinde beliebte Zielscheiben, da hier oft nur geringe Mittel für die Sicherheit der IT-Infrastruktur zur Verfügung stehen.

Über die Motive der Hacker darf man sich keine falschen Vorstellungen

machen. Es geht nicht darum, einfach nur mal zu probieren, in welche Netzwerke man reinkommt. Der finanzielle Gewinn steht im Vordergrund – Informationen werden manipuliert, Finanzergebnisse oder Strategien ausgespielt oder auch Daten – etwa Kinderpornografie – am Server „zwischenlagert“, erläutert Joe Pichlmayr, Geschäftsführer des österreichischen Unternehmens Ikarus Software.

Das Business mit den Viren

Die Cyberkriminellen agieren höchst professionell, sodass sich mittlerweile eine regelrechte Cybercrime-Community gebildet hat. Es werden Infrastrukturen wie Mailserver, Trojaner-Kits oder sogar Services wie Spamversand angeboten. „Firmen – etwa das Russian Business Network – bieten Komplettpakete inklusive Schutz vor anlaufenden Gegenmaßnahmen all-



network

ARNING

erate in this area

in den letzten Monaten jedoch nicht, muss Pichlmayr zugeben und spricht von einem Katz und Maus-Spiel. „Jeder neuen Attacke wird mit neuen Sicherheitsmechanismen begegnet, die wiederum neue Attacken nach sich ziehen.“

Kombi-Lösungen

Für Unternehmensnetze empfiehlt Symantec-Experte Wüst jedenfalls eine Kombination aus einer Software- und einer Hardware-Firewall. Die Gateway Firewall (also die Hardware) sichert dabei den Zugang zum Netzwerk selbst und stellt sicher, dass beispielsweise unbekannte Geräte wie firmenfremde Notebooks nicht angeschlossen werden.

Die Desktop Firewall ist für die Feinarbeit zuständig und kann auf Applikationsebene bestimmen, welche Software auf das Internet zugreifen darf. Auch USB-Sticks, die direkt an den Arbeitsplatzrechner angeschlossen werden, können damit geblockt werden.

Alternative Lösungen

Patentrezepte gibt es gerade für Unternehmenslösungen bekanntlich keine. „Immer wesentlicher werden Verhaltensregeln und Problembewusstsein“, so Pichlmayr. Mitarbeiterschulungen und Lösungen mit „policy enforcement“ können weitere Sicherheit im Unternehmen schaffen. Sich für weniger Viren-anfällige Systeme – also Linux oder Mac – zu entscheiden ist eine Option, bietet aber auch nur für gewisse Zeit Schutz. Denn je mehr Anwender diese Architekturen nutzen, desto mehr werden sie für Hacker interessant. Immerhin ist Mitte Jänner mit Mac Sweeper das erste Betrugsprogramm für Apple aufgetaucht.

Und schließlich treten auch die Managed Security Services immer mehr in den Vordergrund, bei denen Sicherheitskomponenten an einen spezialisierten Dienstleister ausgelagert werden.

Pichlmayer fasst zusammen: „Neben dem Problembewusstsein und entsprechenden Ressourcen für die Umsetzung von Sicherheitskonzepten rückt Sicherheit immer mehr in einen gesamtheitlichen Blickpunkt.“

Birgit Riegler



Unternehmens-Lösungen

Symantec Endpoint Protection 11

Features: Virenschutz, Antispyware, Desktop-Firewall, Intrusion Prevention, Applikations- und Gerätekontrolle; Verwaltung über eine zentrale Konsole

Preis: ab 44 Euro pro Lizenz bei 100 Lizenzen; 31,50 Euro pro Lizenz bei 1000 Lizenzen
Weitere Infos: www.symantecendpoint.com

Ikarus Virus Utilities und Security Manager

Features: Virenschutz und Firewall für Clients mit VU, zentrale Verwaltung mit SM

Preis: VU ab 40,80 Euro pro Lizenz; SM für 5 - 50 User ab 288 Euro für ein Jahr
Weitere Infos: www.ikarus.at

Kaspersky Enterprise Space Security

Features: Virenschutz; Antispyware, Spam- und Phishingschutz, Firewall, Schutz von Mail- und Dateiservern; zentrale Verwaltung

Preis: für 10, 15, 25 oder 50 Workstation ab 548 Euro für ein Jahr
Weitere Infos: www.kaspersky.com

Sophos Enterprise Security and Control 8.0

Features: Virenschutz, Firewall, Antispy- und Adware, Kontrolle von VoIP, Instant Messaging und Spielen, Schutz für Notebook, Handhelds, Desktops und Fileserver, Network Access Control

Noch keine Angaben zum Preis
Weitere Infos: www.sophos.at

McAfee Total Protection for Enterprise

Features: Virenschutz, Antispyware, Firewall, Anti-Rootkit, Spamschutz, zentrale Verwaltung
Preis: 116 Euro pro Lizenz bei 1 - 25 Lizenzen, 101 Euro ab 26 Lizenzen, 90,84 Euro ab 51 Lizenzen usw.

Mehr dazu: www.mcafee.com

fälliger Betroffener an“, so Pichlmayr. Es wird daher immer schwieriger Gefahren aus dem Web abzublocken. Vor allem gezielte Angriffe auf einzelne Unternehmen sind selbst für Experten nicht immer sofort erkennbar. Die Anbieter von Virenschutz-Lösungen empfehlen daher eine Kombination verschiedener Schutzmaßnahmen. Einerseits, weil Kombi-Lösungen bestehend aus Firewall, Virenscanner und Co alle Angriffspunkte abdecken und miteinander interagieren, andererseits aus Kostengründen. All-in-One ist oft günstiger als Single-Lösungen.

Nach wie vor sind dabei Programme zu bevorzugen, die Malware nicht nur basierend auf den Virensignaturen erkennen, sondern auch das Verhalten von Applikationen auswerten. Bei verdächtigen Vorgängen wird die Applikation geblockt oder Alarm gegeben. Viel getan hat sich bei der Technologie