

Hohe Anforderungen an alle

Zuverlässigkeit, Performance und Administrierbarkeit sind heute die Hauptanforderungen an jeden Virenschutz. Dazu kommen geringer Speicherbedarf und proaktive Mal-Code-Erkennung.

WIEN – Viren, Würmer, Trojaner, Rootkits, Ad- bzw. Spyware und Dialer – die Bedrohungen durch Malware sind vielfältig und der Schutz davor ist ein wichtiger Teil der Information Security im Unternehmen. Denn die Werkzeuge der Angreifer sind im Internet leicht für jeden zugreifbar. Zunehmend nutzen auch professionelle Verbrecher und Verbrecherorganisationen das Potenzial von Angriffen, um daraus kommerziell Kapital zu schlagen. Unternehmen schützen sich mit Antivirensoftware, die im professionellen Einsatz hohen Anforderungen gerecht werden muss.

Erwin Klecker ist CISO (Chief Information Security Officer) bei der ÖBB Infrastruktur Bau AG. Er stellt eine wesentliche Veränderung in den Strategien und Zielen der Virusverteiler fest: »Der Hauptunterschied zu früher ist der, dass mittlerweile sehr viel Geld auf Basis von Malware gemacht wird – dazu ist jedoch notwendig, dass Infizierungen möglichst lange unerkannt bleiben!« Vor allem das Ausspionieren von Informationen und der Aufbau von fernsteuerbaren Bot-Netzen sind erklärte Anwendungsgebiete.

»Nicht vertrauenswürdige Webseiten mit Skripten zählen klar zu den Favoriten bei den Angreifern, dicht gefolgt von Dokumentenformaten sowie E-Mails«, skizziert Internet-Security-Experte Rene Pfeiffer die derzeitige Bedrohungslage. Mit der Vielfältigkeit der Bedrohungen steigt auch der Anspruch an die Abwehrmaßnahmen. Ein wichtiger Part kommt dabei dem Virenschutz zu.

HEURISTIK-TECHNOLOGIEN

»Unsere Kunden erwarten sich höchstmögliche Erkennungsrate sowohl über Signaturen als auch über proaktive Virenerkennung«, beschreibt Rainer Witzgall, Executive Vice President des Antivirenherstellers Avira, die Wünsche seiner Anwender. Daher investieren alle Virenhersteller in die Entwicklung so genannter Heuristik-Technologie. Die Avira Technologie hat den Namen AHeAD und soll sicher stellen, dass auch noch unbekannte Bedrohungen gefiltert werden können. Die Heuristik kann anhand der Beschaffenheit einer Datei, der Abfolge signifikanter Code-Sequenzen oder bestimmter Verhaltensmuster mit sehr hoher Wahrscheinlichkeit feststellen, ob es sich um eine schädliche oder virulente Datei handelt. Ist erst einmal Alarm geschlagen, bietet die Virenschutzsoftware die Wahl

die potenziell virenverseuchte Datei in Quarantäne zu nehmen oder vom Rechner zu löschen.

Außerdem sollen auch manipulierte HTML-Dateien proaktiv auf Gateways überprüft werden. Auf diese Weise wird wirksam verhindert, dass Hacker eventuelle Exploits in Browsern ausnutzen können. Die Verteilung von Malware erfolgt außerdem immer mehr über »verseuchte« Web-Server. Einer Untersuchung von Google zu Folge versuchen von 4,5 Millionen URL zirka zehn Malware zu verteilen – das bekannteste diesbezügliche »Produkt« ist *Mpakk* aus Russland. Diese Art der Infizierung wird auch als »drive by infection« bezeichnet.

EINFACHE ADMINISTRIERBARKEIT

»Die einfache Administrierbarkeit ist ebenfalls ein zentraler Punkt«, ergänzt Frank Bieser, CIO von Herold Business Data. Das Einspielen neuer Signaturen in die Virens Scanner muss in höchstem Maße automatisiert und rasch erfolgen können, um etwaigen Angreifern keinen unnötigen Zeitvorteil zu verschaffen. »Wir verlassen uns daher nicht auf ein einzelnes Produkt, sondern arbeiten mit einem mehrstufigen Ansatz.« Denn: »Durch das Einschleusen von Malware können sich bei uns unternehmenskritische Situationen ergeben. Neben klassischen Trojanern, die unsere Systeme mit Breitbandanbindung für Denial-of-Service-Attacken nutzen könnten, gilt es auch Datenverlust bzw. -manipulation zu verhindern. Auch das in letzter Zeit häufiger anzutreffende Data Hijacking stellt eine potenzielle Bedrohung dar.«

Um die Wirtschaftlichkeit der Antivirensoftware sicher zu stellen und dem Benutzer effizientes Arbeiten zu ermöglichen, werden den modernen Tools ein extrem geringer Speicherbedarf und hohe Performance aberlangt. Wenn die Antivirensoftware das Arbeiten für die Mitarbeiter durch lange Wartezeiten und hohen Ressourcenbedarf erschwert, wäre die Sicherheit durch Workarounds und Weigerungsverhalten der Mitarbeiter erst recht gefährdet. Auch im Virenschutz ist trotz aller technischer Möglichkeiten der Faktor Mensch entscheidend.

MITARBEITER SENSIBILISIEREN

Bewusstsein für die Bedrohungen bei den Anwendern ist eben genauso wichtig wie technische Abwehr-

maßnahmen: »Unsere Mitarbeiter sind vom ersten Tag an sensibilisiert. IT-Security und das Phänomen des Social Hacking werden darüber hinaus in der IT-Richtlinie behandelt. Durch diese Maßnahmen schätzen wir unsere Kolleginnen und Kollegen als verantwortungsbewusste Anwender«, beschreibt Frank Bieser die Situation bei Herold.

Doch gerade in letzter Zeit sei durch das Ausbleiben von spektakulären und dementsprechend medienwirksamen Virenoutbreaks das Sicherheitsbewusstsein bei den Anwendern zurückgegangen, klagt CISO Erwin Klecker.

Auch Rainer Witzgall von Avira sieht die Situation gerade in Österreichs Klein- und Mittelbetrieben eher skeptisch: »Leider weiß man in Unternehmen mit zwischen 1 und 100 Mitarbeitern noch sehr wenig über die Verantwortung des Geschäftsführers und Unternehmers, seine Daten und Informationen gegenüber Dritten zu schützen.«

Dabei wird von Gesetz her immer mehr ein sinnvoller Umgang mit Risiken in der IT gefordert. »Sowohl das so genannte Euro-SOX, als auch Basel II und das GmbH-Gesetz sehen einen adäquaten Schutz gegen den Verlust von Informationen vor. Virenschutz ist also ein enorm wichtiger Bestandteil, wenn es um Compliance auch in KMU geht«, beschreibt Compliance-Experte Holger Schellhaas von Evoltas die Dringlichkeit von entsprechenden Maßnahmen.

Rene Pfeiffer weist auf die Veränderung unseres Webverhaltens hin, die das Risikobewusstsein noch mehr geschwächt hat: »Web 2.0 hat die Anwender derart an aktive Inhalte gewöhnt, daß die Gefahr nicht mehr unmittelbar erkennbar ist. Man muss Anwender auf die Benutzung des Webs schulen und sie auf die Gefahren von Webbrowsern aufmerksam machen.«

Laut Pfeiffer werden sich die Bedrohungen weiterentwickeln und sowohl die Benutzer als auch die Antivirenhersteller weiter mit innovativen Attacken auf Trab halten. »Schädlicher Programmcode wird sich auf Webseiten vermehren (Stichwort Syndication und Verknüpfen von Inhalten). Ein ganz großer 'Renner' werden multimediale Inhalte gepaart mit VoIP Technologien – dann werden Bot-Netze durch Anrufe ganze Firmen kompromittieren können«, soweit die Prognose des Experten.

(Michael Gherzolel)