

# Freund oder Feind – nicht immer leicht zu unterscheiden

Joachim Zubke

**Die Gefahren, denen ein Unternehmensnetz ausgesetzt ist, sind heute vielfältiger denn je. Für die Sicherheitssysteme wird es dabei zunehmend schwerer, Angriffe zu erkennen sowie „guten“ und „schlechten“ Datenverkehr voneinander zu unterscheiden. Einen Ausweg bietet die korrelierte Datenanalyse mittels überwachender Netze.**

Online-Systeme wie SenderBase werten täglich gigantische Mengen an Informationen nach unterschiedlichen Parametern aus und stellen die Ergebnisse den Nutzern zur Verfügung. Die mit dem System verbundenen Unternehmen, Hochschulen und sonstige Organisationen speisen die Datenbank im Gegenzug ihrerseits mit eigenen Erkenntnissen über aktuelle Gefahren im Netz. Dieses Prinzip ermöglicht es, potenzielle Gefahren viel schneller zu erkennen und die Datenströme weitaus genauer als bisher in seriös oder unseriös einzuteilen. Diese korrelierte Analyse auf Basis vielfältiger Detailinformationen ist die konsequente Antwort auf die ständig wachsenden Bedrohungen, denen Firmennetze standhalten müssen.

Im Januar 2009 flog ein Online-Betrug auf, der alle bis dahin bekannten Hackerangriffe auf Bankdaten in den Schatten stellte. Internetbetrüger hatten in jahrelanger Arbeit Daten von mehr als 130 Mio. Kreditkarten erbeutet. Ihnen war es gelungen, über Sicherheitslücken eigene Software in die Datenbanken von Finanzunternehmen einzuschleusen. Sie erweiterte die von den Opfern genutzte Datenbanksprache SQL (SQL Injection) um eigene Befehle. Auf diese Weise konnten die Online-Diebe automatisch Kreditkartennummern, Prüfziffern und Kundendaten abfragen und auf ihre eigenen Server überspielen.

Fälle wie dieser sind bei weitem kein Einzelfall, wie beispielsweise eine Studie der Sicherheitsfirma Panda Security belegt. Diese ergab, dass 1,1 % aller untersuchten Rechner mit Malware infiziert waren, mit deren Hilfe persönliche Informationen der Nutzer gestohlen wer-

den sollten. Das Bemerkenswerte daran: Auf mehr als einem Drittel der infizierten Computer war eine aktuelle Virensoftware installiert, die jedoch die Infektion nicht verhindern konnte. Noch bedenklicher waren die Ergebnisse zu Angriffen über Botnetze. Die Untersuchung ergab, dass trotz genutzter Virencanner, Anti-Spyware, Firewalls und Systeme für Intrusion Detection bzw. Intrusion Prevention (IDS/IPS) durchschnittlich 3 % bis 5 % aller IT-Systeme in Unternehmensnetzen durch gezielte Angriffe unterwandert werden.

Ein wesentliches Problem bei der Gefahrenabwehr ist bislang der Variantenreichtum von Malware. Durch das Erscheinen dieser Varianten in immer kürzeren Abständen sind Sicherheitsfirmen gezwungen, mit dem Erstellen von Updates für ihre Produkte Schritt zu halten.

Laut Angaben von Damballa vergehen im Durchschnitt jedoch rund 54 Tage, bis nach dem Auftauchen einer Schadsoftware ein entsprechendes Update für die Antivirensoftware verfügbar ist. So

## Auf einen Blick

**Ein überwachendes Netz sammelt Informationen über den weltweiten Datenverkehr. Damit hilft es Unternehmen, die Qualität von Daten zu bewerten und stellt einen neuen wirksamen Schutz dar. Die relevanten Informationen werden dabei von einer Datenbank geliefert.**

verwundert es kaum, was die Malware-Experten bei einem sechsmonatigen Test herausfanden: Von 200 000 verschickten Malware-Samples blieb die Hälfte in den Unternehmen mind. einen Tag unentdeckt. Rund 15 % der Schadsoftware wurde gar während der gesamten 180-tägigen Untersuchungsdauer nicht identifiziert.

## Breitere Datenbasis erforderlich

Bei der Gefahrenabwehr standen die Verantwortlichen in den Unternehmen bislang außerdem vor einem schier unlösbaren Dilemma. Wenn sie verhindern wollten, dass unerwünschte Daten in das Netz gelangten, konnten sie nicht einfach ihre Kontrollsysteme beliebig verschärfen. Denn das führt beispielsweise bei E-Mails ab einem gewissen Punkt dazu, dass seriöse E-Mails nicht mehr sicher zugestellt werden können. Das Problem: Einzelne Produkte wie Firewalls, SMTP-Gateways (Simple Mail Transfer Protocol) für E-Mails oder IPS-Sensoren können anhand ihrer eigenen Informationen heute oft nicht mehr eindeutig unterscheiden, ob Datenströme gut oder schlecht sind.

Die Lösung für die immer komplexer werdenden Anforderungen liegt in der korrelierten Datenanalyse. Dabei werden die fehlenden Informationen in einem riesigen globalen Netz gepflegt. Dieses steuert eine Vielzahl von ergänzenden Details zu den herkömmlichen Systemen bei und ermöglicht damit eine zuverlässige Gefahrenbewertung auf Basis unterschiedlichster Parameter.

## Ein völlig neuer Ansatz für die Malware-Analyse

Pionier dieses neuen Ansatzes ist das US-Unternehmen IronPort, das 2003 die internetgestützte Reputationsdatenbank SenderBase entwickelte. Ziel war es, die Vertrauenswürdigkeit von E-Mail-Absendern zu analysieren. Als Entscheidungsgrundlage dienen mehr als 110 Parameter, die in Abhängigkeit von statistischen Daten analysiert werden. Diese weltweit erste und größte Datenbank dieser Art legt zehnmal mehr Informa-

tionen zugrunde als konkurrierende Reputationsdienste. Gespeist wird SenderBase aus einem riesigen globalen Netz von mehr als 100 000 teilnehmenden Organisationen. Hierzu zählen z. B. zwölf der fünfzehn weltweit größten Internet-Diensteanbieter, sieben der zehn größten Banken sowie eine Vielzahl global tätiger Unternehmen und Universitäten. Pro Tag werden auf diese Weise Daten von über 5 Mrd. E-Mails ausgewertet und Informationen von mehr als 20 Mio. IP-Adressen gespeichert – das entspricht immerhin rund einem Viertel des weltweiten E-Mail-Verkehrs. Das System registriert beispielsweise die Anzahl der gesendeten Nachrichten, die Akzeptanz von Return-E-Mails, das Herkunftsland, die Beschwerden nach einem Spam-Versand, den physikalischen Ort der Senderorganisation oder die Zeitspanne, seit der eine Organisation bereits E-Mails von diesem Sitz aus versendet.

## **Weltmeister bei Spam-Abwehr**

Mit SenderBase wurde IronPort innerhalb kürzester Zeit zum Weltmeister im Bereich der Spam-Abwehr. 2005 – also zwei Jahre nach Einführung der Datenbank – hatte diese neue Technik bereits mehr als 500 Mrd. Spam-Mails erfolgreich bekämpft. Rund 80 % aller unerwünschten Nachrichten wurden bereits auf Verbindungsebene – also noch vor der Zustellung – abgefangen. Unternehmen, die diese Technik nutzen, benötigen dadurch weniger Bandbreite und Systemressourcen für den E-Mail-Verkehr. Darüber hinaus steigen Sicherheit und Produktivität. Dabei gilt das Prinzip des Gebens und Nehmens: Unternehmen, die SenderBase nutzen, profitieren nicht nur von den topaktuellen Sicherheitsinformationen aus dem Internet, sondern speisen das System auch mit ihren eigenen Erkenntnissen über akute Gefahrenquellen. Auf diese Weise können andere Unternehmen umgehend auf bestehende Risiken reagieren.

## **Entscheidender Informationsvorsprung**

Dass dieses Prinzip der korrelierten Datenanalyse der Schlüssel zum Erfolg ist, hat unlängst auch Cisco erkannt. 2007 übernahm das Unternehmen IronPort und gliederte in der Folgezeit die Idee des SenderBase-Netzes in eigene Produkte ein. Neben der Lösung für Sicherheit im

E-Mail-Datenverkehr hat Cisco das Prinzip auch in Lösungen für Web-Datenverkehr, für IPS-Sensoren und für Firewalls integriert. So verfügen die Firewalls beispielsweise über einen Botnet-Traffic-Filter. Dieser erkennt, wenn Malware versucht, eine Verbindung zu bekannten IP-Adressen von Botnetzen aufzubauen, um private Daten wie Passwörter oder Kreditkartennummern zu versenden. Dabei vergleicht der Botnet-Traffic-Filter ein- und ausgehende Verbindungen mit der dynamischen Datenbank bekannter Domains und IP-Adressen und protokolliert verdächtige Aktivitäten.

Durch die Information von Botnetzen ist eine Firewall in der Lage, Datenverkehr besser zu unterscheiden. So kann beispielsweise ein Verbindungsaufbau über http vom Client im LAN aufgrund des Ziels zu einer Alarmierung führen, wenn es sich um ein Botnetz handelt. Ohne diese Technik würde die Firewall den Zugriff erlauben, weil es sich bei dem Webseitenzugriff um einen scheinbar normalen Vorgang handelt.

Für diese Vorgänge stellt SensorBase nun einen speziellen Filter zur Verfügung. In der Datenbank sind die DNS-Namen (Domain Name System) der weltweit bekannten Botnetze registriert. Sobald zu einer der betreffenden IP-Adressen eine Verbindung aufgebaut wird, erkennt die intelligente Filterung, dass die Zielrechner zu einem Botnetz gehören, und das System schlägt sofort Alarm. Alle notwendigen Informationen über diesen Angriff werden dann wiederum in die zentrale Datenbank eingespeist, sodass sich die angeschlossenen Systeme unmittelbar auf die Gefahrenquelle einstellen können.

## **Geringerer Aufwand – mehr Sicherheit**

Die Tatsache, dass die Datenbank im Internet hinterlegt ist und dynamisch gepflegt wird, bedeutet für den Administrator eine große Entlastung. Er muss die Informationen über neue Gefahren nun nicht mehr einzeln manuell in sein System einpflegen. Über die Datenbank erhält die entsprechende Netzkomponente automatisch und viel schneller die bislang fehlenden Informationen – und zwar in permanent aktualisierter Form. Dadurch lässt sich der Datenstrom wesentlich detaillierter filtern, und neue Gefahren bleiben nicht länger unerkannt.



Joachim Zubke ist Senior Consultant Security bei der avodaq AG in Hamburg.

## **Integration in bestehende Systeme**

Die neue Erkennungstechnik lässt sich auch gut in bestehende Systeme integrieren. Zu den Firmen, die somit sehr effektiv alte und neue Gefahren abwehren, zählt beispielsweise das Chemieunternehmen Lehmann & Voss & Co. Das Hamburger Unternehmen nutzt seit etwa einem Jahr die E-Mail-Sicherheitslösung von IronPort. Das Besondere daran ist die Kombination konventioneller Techniken mit kontextsensitiver Erkennung: Die Anti-Spam-Technik von IronPort beruht neben der Abfrage des Reputationswerts von der Datenbank SenderBase in Echtzeit auf der „Context Adaptive Scanning Engine“ (CASE), die den kompletten Kontext einer E-Mail untersucht. Durch die Kombination des CASE-Werts mit dem Reputationswert von SenderBase wird ein deutlich zuverlässigeres Ergebnis erzielt, als es traditionellen Techniken zur Spam-Filterung möglich ist.

Die E-Mails, die nicht eindeutig als Spam eingestuft werden können, gelangen hierbei nicht unmittelbar zum Empfänger, sondern werden in eine zentrale Quarantäne geschoben. Der Mitarbeiter erhält von der IronPort-Lösung nur einmal täglich eine Benachrichtigung mit einer Übersicht der unerwünschten E-Mails. Zudem hat er Zugriff auf den Spam-Quarantänebereich, um die Nachrichten zu überprüfen und zu verwalten. Darüber hinaus können Nutzer nicht erkannten Spam zur weiteren Überprüfung an das Threat Operation Center von IronPort senden. Dort sorgen Analysten für die Aktualisierung von Regeln in Echtzeit, um neue Spam-Angriffe sofort nach einem Ausbruch zu blockieren. Damit seriöse E-Mails bei Lehmann & Voss nicht fälschlicherweise als Spams eingestuft werden, können die Administratoren beispielsweise spezifische Regeln für den E-Mail-Verkehr festlegen, die gewährleisten, dass alle erwünschten E-Mails auch tatsächlich den Empfänger erreichen. ■