Bild: iStock

DOSSIER SICHERHEIT
IN KOOPERATION MIT BOLL ENGINEERING

Eine neue Generation

sza. Glaubt man Sicherheitsexperten, dann geht es im Web richtig zur Sache: Angriffe werden professionell und gezielt ausgeführt. Es geht darum, Geld zu stehlen, sich Macht und Einfluss zu sichern oder öffentliche Aufmerksamkeit zu erzeugen. Gut bezahlte Hacker und staatliche Organisationen entwickeln dafür moderne Schadprogramme. Längst geht es nicht mehr um die reine Zerstörungswut von Script-Kiddies und Hobby-Hackern.

Experten raten den Unternehmen deshalb, mehr Geld in ihre Sicherheit zu investieren. Für sie ist klar: Mit alten Abwehrtechniken ist gegen die modernen Angreifer kein Kraut gewachsen. Stefan Thomann vom IT-Sicherheitsunternehmen Infoguard empfiehlt im Interview auf Seite 38, auch beim Risiko «Mitarbeiter» anzusetzen: «Sehr häufig können wir unseren Kunden bei Überprüfungen aufzeigen, wie gut Social-Engineering-Attacken funktionieren.» Doch Geld fliesse dann kaum. Viel eher behelfe man sich mit technischen Werkzeugen, wie zum Beispiel mit sogenannten Next Generation Firewalls.

Ein Unterschied zu konventionellen Firewalls ist, dass bei diesen beispielsweise viel differenziertere Konfigurationen vorgenommen werden können. Unternehmen müssen demnach nicht mehr einfach pauschal eine Domain für alle Angestellten des Unternehmens blockieren – wie zum Beispiel das soziale Netzwerk Facebook. Sondern sie können je nach Nutzer, dem Endgerät oder dem Aufenthaltsort verschiedene Sicherheitslevels einstellen. Zudem kann die «moderne» Firewall auch einzelne Funktionalitäten blockieren, die entweder die Sicherheit im Unternehmen gefährden oder die Produktivität der Mitarbeiter sinken lässt. Der Artikel auf den nachfolgenden zwei Seiten geht auf diese modernen Firewalls ein. <

> **Seite 36**
«Modern Malware» – eine unangenehme Realität

> **Seite 38**
Stefan Thomann, Infoguard: «Insgesamt ist die Erfolgsrate bei Penetration-Tests doch erstaunlich hoch»

«Modern Malware» – eine unangenehme Realität

Viren und Trojaner breit zu streuen oder beliebige Rechner und Datencenter anzugreifern – das war einmal. Moderne Angriffe sind wesentlich gezielter, subtiler und kreativer. Angesichts der sich verändernden Bedrohungslage werden die Einschränkungen konventioneller Firewalls offensichtlich. Walter Benz

Die Liste wird länger und länger – und markiert trotzdem nur die Spitze des Eisbergs. Namhafte Firmen und Organisationen werden durch sogenannte «Modern Malware» gezielt attackiert, müssen Datenverluste eingestehen, werden in ihrer unternehmerischen Tätigkeit behindert oder gehen gar Konkurs.

Zu den namhaften Opfern gezielter Attacken gehörte etwa ein grosser japanischer Konzern, der den Diebstahl von Kreditkartendaten und persönlichen Informationen von über 100 Millionen registrierten Nutzern zu beklagen hatte. Selbst Regierungen sowie Unternehmen, die in den Bereichen Zertifizierung, PKI und Verschlüsselung tätig sind, gehören zum Kreis erfolgreich attackierter Institutionen. Moderne Malware-Angriffe «im grossen Stil» machen auch hierzulande vermehrt von sich reden, was beispielsweise die Melde- und Analysestelle Informationssicherung (Melani) kürzlich dazu bewogen hat, vor raffinierten Attacken auf Zertifizierungsanbieter zu warnen.

Malware-Angriffe «im grossen Stil» hat kürzlich die Melde- und Analysestelle Informationssicherung (Melani) dazu bewogen hat, vor raffinierten Attacken auf Zertifizierungsanbieter zu warnen. Bild: Boll Engineering

Veränderte Bedrohungsformen: gezielter, subtiler, kreativer

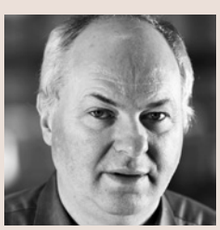
Im Bereich der IT-Security ist ein folgenreicher Paradigmenwechsel festzustellen. Zeichneten sich frühere Angriffe unter anderem durch eine möglichst breite Streuung von Viren und Trojanern oder durch unspezifische zerstörerische Angriffe auf beliebige Rechner und Datencenter aus, sind moderne Angriffe wesentlich gezielter, subtiler, kreativer. Sie sind nicht primär auf die Zerstörung von Daten ausgerichtet und haben nicht «jedermann», sondern klar definierte Individuen oder Personengruppen im Visier.

Die Entwicklung moderner Malware ist das Handwerk ausgesprochen cleverer, gut organisierter, oft bestens bezahlter Hacker oder staatlicher Institutionen. Sie sind nicht aus Spass, zum Zeitvertreib oder aus Mangel an Anerkennung als Hacker tätig. Vielmehr haben sie handfeste finanzielle Gründe, verfolgen wirtschaftliche oder politische Interessen. Zum weiten Repertoire ihres Tuns gehören die gezielte Werkspionage ebenso wie die systematische Aushebelung von Verschlüsselungssystemen und Zertifikaten, Angriffe auf Finanz-Applikationen (z.B. E-Banking), Datenklau im grossen Stil, gezielte Attacken auf staatliche Stellen und wichtige Infrastrukturen oder die Zerstörung von Industrie-Anlageteilen.

Als wesentliche Charakteristika moderner Malware gilt deren «Lebenszyklus». Dieser beginnt mit der Infizierung eines oder mehrerer Rechner beziehungsweise mit dem Einschleusen eines Schädlings. Geeignete Einfalltüren bilden dazu Web-2.0-Anwendungen und «Social Engineering»-Strategien. Sie nutzen Beziehungen, Vertrauen und gefälschte Identitäten aus, um beispielsweise den Empfänger einer E-Mail zu veranlassen, einen mitgelieferten Link anzuklicken und so auf eine infizierte Website zu gelangen. Ist dies der Fall, wird der vorhandene Schadcode unerkannt ins Zielsystem übertragen. Dort nistet er sich ein und macht das System verletzbar (Exploit Vulnerability). Um das kompromittierte System unter Kontrolle des Angreifers zu bringen, veranlasst der Schadcode in der Regel den Download eines Backdoor-Programms, das seinerseits einen unerkannten Kommunikationskanal nach aussen etabliert. Dieser ermöglicht sowohl die Kommunikation mit anderen verseuchten Plattformen als auch die Remote-Steuerung des befallenen Rechners durch den Hacker. So lassen sich spielend DDoS-Attacken reiten, Passwörter abfangen, Daten entwenden, elektronische Systeme wie industrielle Steuerungen (zer-)stören.

Gefahren erkennen, bevor sie wirken

Angesichts der sich verändernden Bedrohungsformen werden die Einschränkungen konventioneller Firewalls offensichtlich. Selbst die Verknüpfung komplementärer



Walter Benz ist Produktmanager bei Boll Engineering.

Technologien wie Paketfilter, VPN-Gateway, Content Filter und IDS/IPS vermag den aktuellen Gefahren nicht mehr ganzheitlich zu begegnen. Denn die vermehrte Nutzung webbasierter Anwendungen wie Facebook, Twitter und Skype, Dropbox und Salesforce, die vermehrte Nutzung von Cloud- und Virtualisierungstechnologien

Moderne Malware zeichnet sich auch dadurch aus, dass der Schadcode nicht zwingend als solcher erkannt wird und folglich auch nicht abgewehrt werden kann. Bild: Boll Engineering

oder die zunehmend mobile Arbeitsweise von Mitarbeitenden führen dazu, dass sich einzelne User nicht mehr klar definierten IP-Adressen zuordnen lassen. Ebenso wenig sind beispielsweise Web-2.0-Applikationen mit fixen TCP-Ports verbunden; sie lassen sich dadurch nur bedingt kontrollieren. Vor diesem Hintergrund wird die Kontrolle von Applikationen über Segment- und Perimetergrenzen hinaus mit konventionellen Mitteln schwierig, wenn nicht gar unmöglich.

Erschwerend kommt hinzu, dass sich moderne Malware auch dadurch auszeichnet, dass der Schadcode nicht zwingend als solcher erkannt wird und folglich auch nicht abgewehrt werden kann. Zu beachten ist ferner die Tatsache, dass die installierte Malware ihr Gesicht im Laufe der Zeit verändern kann und sich allenfalls über lange Zeiten ruhig verhält. Um Herausforderungen dieser Art wirksam zu begegnen, sind zwei primäre Security-Mechanismen notwendig:

- die Einbindung einer Next Generation Firewall
- die Implementierung einer abgeschotteten Testumgebung, um die Wirkungsweise unbekannter Codes in Realität zu testen.

Kontrolle von Anwendungen, Usern und Inhalten

«Next Generation Firewalls» setzen nicht mehr länger auf die alleinige Kontrolle von IP-Adressen und Port-Nummern, sondern auf die Identifikation und Kontrolle von Anwendungen, Benutzern und Inhalten. Dabei werden User unabhängig von IP-Adressen und Applikationen, losgelöst von Port, Protokoll, Verschlüsselung oder Verschleierungsmethoden erkannt. Bekannte Anwendungen und die daraus entstehenden Gefährdungen lassen sich dadurch einfach identifizieren, transparent darstellen und gegebenenfalls blockieren. Auch bei der Umsetzung firmenspezifischer Security-Policies leisten «Next Generation Firewalls» einen wichtigen Beitrag. So lässt sich granular definieren, welche Anwendungen und Zugriffe für welche User und Anwendergruppen freigegeben beziehungsweise gesperrt sind.

Dank der user- und anwendungsbasierten Überwachung schaffen «Next Generation Firewalls» eine maximale Transparenz – selbst bei verschlüsselter Datenübertragung. Sie liefern unter anderem Informationen darüber, was im Netz passiert, welche Anwendungen genutzt werden, welche User mit welchen Programmen beschäftigt sind und wer mit wem kommuniziert. Sie zeigen ferner, zu welchen Ländern und geografischen Regionen Verbindungen bestehen, wer im Unternehmen als kritisch eingestufte Applikationen nutzt, welcher Datenverkehr durch welche Applikationen erzeugt wird oder welche Angriffe am häufigsten vorkommen.

Lösungen mit integriertem Realtime-Monitoring bieten zudem einen stets aktuellen Überblick über das aktuelle Gefährdungspotenzial. Dazu werden mehrere tausend Applikationen erkannt, gefahrenspezifisch eingestuft und – bei deren aktuellen Nutzung – visualisiert.

Analyse unbekannter Dateien: identifizieren, analysieren, unschädlich machen

Laut aktuellen Zahlen handelt es sich bei rund 10 Prozent der weltweit übermittelten Daten um unbekannten Traffic. Zwar sind unbekannte Anwendungen nicht zwingend schädlich – hausinterne Applikationen gehören ja beispielsweise auch in diese Kategorie –, können aber potenziell Schadcode enthalten. Um sicherzugehen, dass nichtbekannte Daten «clean» sind, gilt es diese zu identifizieren, zu analysieren und eventuell unschädlich zu machen. Um diesen Prozess in kürzester Zeit und ohne Gefahren für die User zu bewerkstelligen, bieten erste Unternehmen wie Palo Alto Networks entsprechende Services an.

Identifiziert die Next Generation Firewall eine unbekannte Datei, kann sie automatisch in eine virtuelle, cloudbasierte Umgebung verlagert werden. In dieser wird sie auf Malware-Merkmale und bekannte Signaturen untersucht. Zudem wird der Code in einer «Sandbox» ausgeführt. Diese abgeschottete, als Wildfire bezeichnete Umgebung bildet einen perfekten «Nährboden» für weitreichende Code-Analysen im sicheren Labor, ohne produktive Systeme zu tangieren. Dadurch lassen sich unterschiedlichste Informationen gewinnen. So etwa Erkenntnisse darüber, wie sich die Malware verhält, wie sie sich im Zeitverlauf verändert, welche Angriffsziele sie hat und welche Applikationen betroffen sind.

Auf Basis dieser und weiterer Ergebnisse erstellt Palo Alto Networks automatisch neue Signaturen, die im Rahmen regelmässiger Signatur-Updates an die Next Generation Firewall übermittelt werden. Dadurch verringert sich die «Time to Protection» für alle registrierten Anwenderinnen und Anwender. <

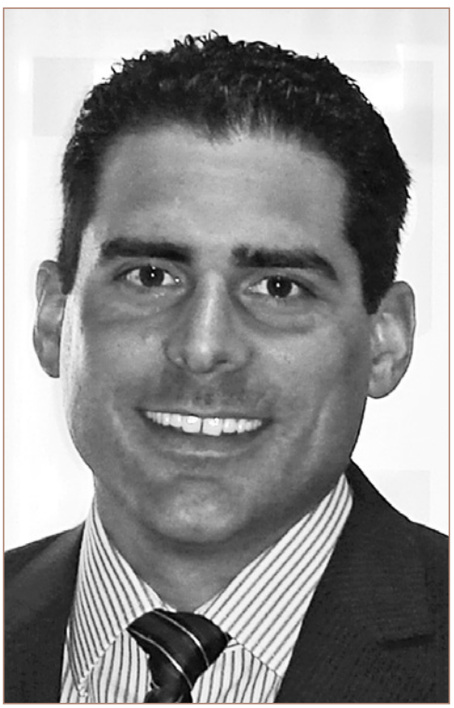
«Insgesamt ist die Erfolgsrate bei Penetration-Tests doch erstaunlich hoch»

Moderne Hackerangriffe haben wenig mit dem herkömmlichen Versenden von Malware zu tun. Unternehmen sind deshalb gefordert, ihren Perimeter-Schutz anzupassen. Was das konkret bedeutet, weiss Stefan Thomann, Verkaufsleiter beim IT-Sicherheitsunternehmen Infoguard. Interview: Simon Zaugg

Herr Thomann, Sicherheitsexperten sprechen von immer professionelleren Angreifern. Viele Attacken blieben unter dem Radar, andere würde man unter den Teppich kehren. Wie nehmen Sie dieses Thema wahr?
Die Professionalisierung der Angreifer ist unbestritten. Ein Problem sehe ich insbesondere darin, dass im Unterschied zu den USA in der Schweiz (noch) keine Meldepflicht besteht, wenn bei Unternehmen Daten abhanden kommen. Würde es diese in den USA auch nicht geben, hätte die Öffentlichkeit möglicherweise gar nie vom grossen Sony-Datenklau im vergangenen Jahr erfahren. Es ist klar, dass Unternehmen versuchen, Vorfälle unter allen Umständen unter Verschluss zu halten. Die Sensibilität für neue Gefahren in den Unternehmen und der Gesellschaft steigt jedoch nur, wenn man von solchen Vorfällen erfährt. Wenn ein Skandal publik wird, dann fragen sich plötzlich alle: Könnte mir das auch passieren?

Welche Gefahr wird denn heute am meisten unterschätzt?
Für Sicherheit wird generell verhältnismässig wenig Geld ausgegeben. So hat Pascal Lamia, der Leiter der Melde- und Analysestelle Informationssicherung Melani, kürzlich an einer Veranstaltung eine eindrückliche Zahl genannt: Demnach gaben Unternehmen 2010 im Schnitt pro Mitarbeiter und Monat mehr Geld für Klopapier als für IT-Sicherheit aus. Meine Beobachtung ist, dass insbesondere beim Risiko Mitarbeiter besonders wenig investiert wird, obwohl man weiss, dass er das grösste Risiko ist. Sehr häufig können wir unseren Kunden bei Überprüfungen aufzeigen, wie gut Social-Engineering-Attacken funktionieren. Die Geschäftsleiter sehen das zwar ein. Doch die Bereitschaft, in Sensibilisierungsmassnahmen zu investieren, bleibt gering. Das Geld fliesst viel eher in technische Tools.

Was sind denn, ausser dem Risiko Mensch, die grössten Herausforderungen für Unternehmen, was die Sicherheit angeht?



Laut Stefan Thomann von Infoguard unterschätzen Unternehmen das Risiko «Mitarbeiter».

Die IT-Infrastruktur ist in den letzten zehn Jahren kontinuierlich gewachsen, wodurch in vielen Bereichen die Übersicht verloren ging. Durch Anpassungen in der Sicherheitsarchitektur und eine geeignete Zonenbildung wird nun diese Komplexität gezielt reduziert. Durch die vermehrte Nutzung von Web 2.0 entstehen für Unternehmen gleichzeitig neue Herausforderungen an die internen Richtlinien und technische Firewall-Lösung. So reicht es heute nicht mehr, nur Port 80, also den HTTP-Traffic zu filtern. Angreifer nutzen mit «Modern Malware» die neuen Möglichkeiten von Applikationen gezielt aus.

Als Lösung gelten sogenannte «Next Generation Firewalls». Was unterscheidet diese denn konkret von «normalen» Firewalls?
Diese Firewalls kontrollieren den Datenverkehr nach Applikationen, Inhalt und dem entsprechenden User und nicht mehr nur den Port. Unternehmen erhalten damit die Möglichkeit, nicht mehr nur eine Domain wie zum Beispiel Facebook für alle pauschal zu blockieren, sondern dies sehr viel differenzierter einzustellen und allenfalls sogar einzelne Services innerhalb der Anwendung zu sperren.

Wie sehr ist Bring your own Device ein Thema? Mobile Geräte sind ja auch deswegen ein beliebtes Angriffsziel, weil sie schlecht geschützt sind.
Bring your own Device ist ja insbesondere auch deshalb ein Thema, weil es stark von den Geschäftsleitungen getrieben wird. Sie selbst wollen ihre privaten Geräte auch im Geschäftsumfeld nutzen. Man muss, egal ob beim Laptop, dem Tablet oder dem Smartphone, davon ausgehen, dass ein vom Mitarbeiter mitgebrachtes Gerät den Sicherheitsanforderungen von Unternehmen nicht genügt. Deshalb muss man sehr vorsichtig sein. Im Grunde geht es darum, die privaten Daten sauber von den geschäftlichen Daten zu trennen und die geschäftlichen Daten jeweils verschlüsselt abzulegen. Gleichzeitig muss aber auch der Zugriff auf das Netzwerk klar geregelt und überwacht werden. Nur so lässt sich eine BYOD-Strategie im Unternehmen sicher einsetzen.

Wie häufig empfehlen Sie Unternehmen, die IT-Infrastruktur zu überprüfen?
Grundsätzlich empfehlen wir, einmal pro Jahr eine Überprüfung mittels gezielten Penetration-Tests zu machen.

Die Empfehlung ist das eine. Wie häufig wird es effektiv auch gemacht?
Das kommt auf das Unternehmen an. Wir finden immer wieder Lücken, bei den Einen mehr, bei den Anderen weniger. Insgesamt ist die Erfolgsrate bei Penetration-Tests aber doch erstaunlich hoch. Zudem empfehlen wir, die technische Infrastruktur zusätzlich zu solchen Tests über automatisierte Schwachstellen-Scans zu überprüfen. <