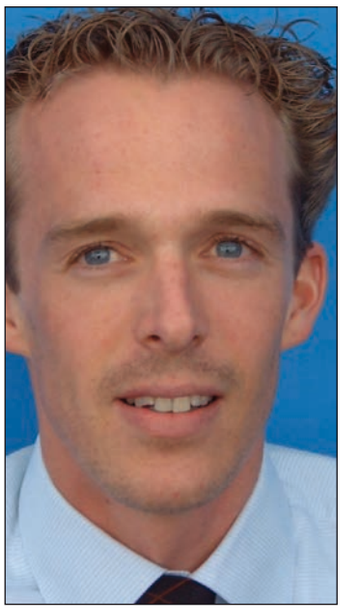
«Der Kauf von Daten ist nur ein Mausklick entfernt»

Sicherheitsexperte Patrick Michel erklärt im Interview die neuesten Trends im Security-Umfeld und zeigt auf, weshalb IT-Security auch 2014 eine riesige Herausforderung ist.

Von Marcel Wüthrich



Patrick Michel arbeitet bei Boll Engineering als Head of Sales und ist als Produkt Manager zuständig für die Security-Produkte des Herstellers Fortinet. Er ist ein profunder Kenner des IT-Security-Markts, in dem er seit über 16 Jahren in verschiedenen technischen (Senior Security Engineer, CTO, COO) sowie Verkaufs-Positionen (Produkt Manager, Head of Sales) aktiv ist, bei Security-Integratoren, Distributoren, Managed-Security-Providern sowie Security-Herstellern. Als Autor hat er dutzende Fachartikel sowie Kolumnen zum Thema IT-Security geschrieben.

Attacken auf IT-Infrastrukturen und Anwendungen nehmen kontinuierlich zu, werden vielschichtiger, komplexer und gezielter. Sie stellen Unternehmen und Institutionen vor enorme Herausforderungen. Patrick Michel, IT-Security-Spezialist seit über 16 Jahren und Head of Sales bei Boll Engineering, äussert sich im Interview zur Herausforderung IT-Security.

Swiss IT Magazine: Patrick Michel, im Bereich der Netzwerk-Security wurde der Begriff Firewall durch Bezeichnungen wie Unified Threat Management (UTM), Application Control, Next Generation Firewall (NGF) und Advanced Persistent Threat (APT) abgelöst. Was hat sich im Laufe der Jahre verändert?

Patrick Michel: Allen Begriffen gemeinsam ist das Bestreben, unterschiedlichste Security-Funktionen – von Layer 3 bis hin zur Applikationsebene – in einer leistungsfähigen Appliance zu integrieren beziehungsweise zu konsolidieren. Dies mit dem Anspruch, die zahlreichen Gefahren bereits am Gateway oder in einem Datacenter zu erkennen und abzuwehren. Viele der heute angebotenen Systeme beinhalten Sicherheits-Module wie Firewall, VPN, Anti-Malware, Antivirus, Webfilter, Intrusion Prevention und Application Control in einer Appliance. Viele leistungshungrige Funktionen, für die in der Vergangenheit dedizierte Systeme benötigt wurden, lassen sich in performante, in der Regel hardwarebeschleunigte Appliances integrieren. Über die Jahre wurden immer mehr Funktionen in Firewalls konsolidiert.

Ist der früher praktizierte Best-of-Breed-Ansatz folglich obsolet?

Der Best-of-Breed-Ansatz wird auch heute noch angewendet. Das kann unter anderem an unterschiedlichen Verantwortlichkeiten für den Betrieb solcher Systeme liegen oder an Security-Konzepten, die seit mehreren Jahren bestehen und nicht hinterfragt werden.

Zu den typischen Funktionen, die sowohl konsolidiert auf einer Firewall als auch in einer dedizierten Best-of-Breed-Lösung eingesetzt werden können, zählen Intrusion Prevention und Intrusion Detection sowie Proxy-Server mit Webfilter und AV-Scanning. Doch die Konsolidierung hat auch ihre Limiten und verlagert sich in andere Bereiche. So zeichnet sich in den Bereichen Load Balancing, Application Delivery Control (ADC) und Web Application Firewalling (WAF) eine ähnliche Entwicklung ab wie bei Firewalls.

Ein eher neuer Themenbereich, in dem sich der Best-of-Breed-Ansatz manifestiert, sind Lösungen zur Abwehr von DDoS-Attacken (Distributed Denial of Service). Zwar beinhalten Firewalls häufig DDoS-Funktionalitäten, diese reichen für einen effektiven Schutz hochsensibler Applikationen in der Regel aber nicht aus. Vor diesem Hintergrund bieten viele Security-Hersteller dedizierte DDoS-Appliances an.

Bleiben wir noch kurz bei der Auslegeordnung von Begriffen und Funktionen. Wie unterscheiden sich die sogenannten Next Generation Firewalls von klassischen Multi-Threat-Sicherheitssystemen?

Next Generation Firewalls haben den Anspruch, entstehende Gefahren auf Applikationsebene zu identifizieren und transparent darzustellen. Dazu setzen sie nicht auf die Kontrolle einzelner Ports, wie dies bei klassischen Firewalls der Fall ist, sondern auf die Identifikation und Kontrolle von Anwendungen, Usern und Inhalten. Obwohl NGFs oft als eigene Kategorie definiert werden, ist Application Control und User Authentication ein Standard-Feature innovativer Network-Security-Plattformen. Wer sich mit dieser Thematik befasst, merkt schnell, dass es sich vor allem um Marketing-Positionierungen handelt, die massgeblich von Gartner, IDC und anderen Analysten-Firmen getrieben werden.

Welche Entwicklungen sind im Firewall-Bereich absehbar?

Zu den aktuell wichtigen Trends gehören Speed und Performance. Getrieben wird diese Entwicklung durch den zunehmenden Bedarf an Bandbreite – ausgelöst beispielsweise durch die vermehrte Nutzung von Multicast und Video-Streaming oder durch Trading-Applikationen. Letztere benötigen – ohne die Si-

cherheit zu beeinträchtigen – tiefste Latenzzeiten. Firewalls müssen heute vermehrt in der Lage sein, 10-Gbps-Netze ohne Leistungseinbussen zu unterstützen. Und vergessen wir nicht: 40 und 100 Gbps schnelle Netzwerke stehen vor der Tür. Angesichts dieser Entwicklung wird es für Firewall-Hersteller noch wichtiger, auf hardwarebeschleunigte Architekturen zu setzen. Ein weiterer Bereich ist das IPv6-Protokoll, mit dem Firewalls klarkommen müssen.

Zudem beobachte ich auch Bewegung bei virtualisierten Software-Appliance-Firewalls, die auf Basis von Vmware, Xen, HyperV und KVM laufen. Diese bringen zwar nicht die Performance von hardwarebeschleunigten Appliances, doch sie haben den Vorteil, in einer bereits bestehenden virtualisierten Infrastruktur betrieben werden zu können. Interessant wird es sein, zu beobachten, ob auch hier Hardwarebeschleunigung für leistungshungrige Umgebungen Einzug halten wird. Im Zuge von Software Defined Networking (SDN) kann ich mir gut vorstellen, dass dies früher oder später passieren wird.

Welche Einflüsse auf die IT-Sicherheit hat die vermehrte Nutzung mobiler Devices?
Da sprechen Sie ein vielschichtiges Thema an. Die Omnipräsenz mobiler Devices führt zu einer starken Zunahme an WLANs, was – bezogen auf die IT-Security – viele neue Probleme schafft. Wie beispielsweise kann verhindert werden, dass nur berechtigte Endgeräte und Personen Zugang ins Netz erhalten? Oder wie wird dafür gesorgt, dass die Kommunikation zwischen Endgeräten, Access Points und LAN denselben Sicherheitsstandards entspricht wie im kabelgebundenen Netz? Diese und weitere sicherheitsrelevante Fragen haben einige Firewall-Hersteller dazu bewogen, Lösungen zu entwickeln, die eine sichere und nahtlose Einbindung von WLANs ins Firmennetzwerk ermöglichen. Entsprechende Secure-WLAN-Lösungen beinhalten in der Regel zentral gemanagte Access Points, unterstützen das stetige Einspielen neuester Signaturen, die verschlüsselte Übertragung der Daten, intelligente Authentifizierungsmechanismen, das Erkennen eingeschleuster Access Points (Rough AP) und vieles mehr.

Inwieweit ist das Zusammenspiel zwischen sogenannten Mobile-Device-Management (MDM)-Lösungen und Firewalls von Bedeutung?
Damit sprechen Sie den Begriff Bring your own Device (BYOD) beziehungsweise die nicht neue Thematik Endpoint Control an. Diese wird in der Praxis entweder gar nicht oder mit dedizierten MDM- beziehungsweise Endpoint-Security-Lösungen adressiert. Entsprechende Lösungen sollten sämtliche Sicherheits-, Management- und Verwaltungs-Funktionen für ein unternehmensweites Smartphone- und Mobilgeräte-Management beinhalten. Dadurch stellen sie sicher, dass nur autorisierte und vorgabenkonforme Geräte Zugriff auf die Unternehmens-Ressourcen erhalten. Und sie sorgen dafür, dass bei Geräteverlust oder beim Firmenaustritt von Mitarbeitenden keine Daten in falsche Hände gelangen. Bedeutsam sind ferner das Monitoring von User-Aktivitäten – zum Beispiel Downloads, SMS oder Telefongespräche – sowie die zentrale Verwaltung neuer Richtlinien, Einstellungen, Zertifikate und Zugriffsmöglichkeiten auf Unternehmenskonten. Soweit die Idealvorstellung. In der Praxis sieht die Situation oft anders aus. Ungeachtet aller technischer Möglichkeiten zur sicheren Nutzung privater mobiler Devices erfolgt die Einbindung ins Firmennetz häufig auf Kosten der Sicherheit, was die Gesamtsicherheit des Unternehmens beeinträchtigen kann.

«Die Omnipräsenz mobiler Devices führt zu einer starken Zunahme an WLANs, was – bezogen auf die IT-Security – viele neue Probleme schafft.»

Patrick Michel, Head of Sales, Boll Engineering

Wir haben vorher über DDoS-Attacken gesprochen. Wie gross ist dieses Problem und wie lassen sich entsprechende Angriffe abwehren?
Diverse Studien machen deutlich, dass DDoS-Attacken zu den aktuell grössten Gefahren für IT-Infrastrukturen und Applikationen gehören. Sie sind in der Lage, Applikationen und Server lahmzulegen und Systeme wie Firewalls, Webserver, Applikationsserver, Datenbanken oder Storage-Lösungen so zu stören, dass sie ihre Aufgaben nicht mehr erfüllen können. Dazu bedienen sich Hacker einerseits breit angelegter Attacken, die nicht nur Firmen mit interessanten Angriffszielen im Fokus haben. Andererseits lancieren sie mehr und mehr gezielte, intelligente Multivektor-Angriffe sowie Attacken auf Anwendungsebene, die schwer zu erkennen sind. Um entsprechende Angriffe auf allen Ebenen wirksam abzuwehren, ist der Einsatz spezialisierter, performanter DDoS-Defense-Systeme (DDS) unabdingbar. Firewalls bieten hierzu einen limitierten Schutz.

Sie haben es erwähnt: Attacken werden zunehmend cleverer. Warum?
Ein wichtiger Grund für diese Entwicklung ist die deutliche Professionalisierung des Verbrechens via Internet. Da wird – vergleichbar mit der realen Welt – reger Handel betrieben. So lassen sich weit verzweigte, hoch effektive Bot-Netze mieten, unbekannte Produkteschwachstellen kaufen und gezielte Attacken als Dienstleistung in Auftrag geben. Auch der Kauf umfangreicher Datensätze – etwa E-Mail-Adressen und Kreditkartendaten – ist nur ein Mausklick respektive Chat entfernt. Und so ist es nicht verwunderlich, dass die Angriffe dreister, die Methoden vielfältiger und professioneller werden. Treibende Kräfte für diese Entwicklung sind unter anderem die zunehmende Bedeutung der Industriespionage sowie das politisch motivierte Aufrüsten der Angreifer.

Wie reagieren denn die Anbieter von Sicherheitslösungen auf diese Situation?
Damit Anbieter von Security-Lösungen mit diesem Tempo Schritt halten können, sind grosse Anstrengungen notwendig. Fortinet beispielsweise betreibt dazu mit Fortiguard ein eigenes Security-Lab. Dieses beschäftigt über 200 Security-Spezialisten. Zu deren Aufgaben gehören die Analyse neuer und unbekannter Gefahren ebenso wie die kontinuierliche Aktualisierung der Signatur- und Reputationsdatenbanken, die aktive Suche nach Schwachstellen sowie die Entwicklung wirksamer Abwehrmechanismen. Die zentrale Bedeutung dieser Investition lässt sich anhand weniger Zahlen verdeutlichen. So entwickelt und implementiert das Fortiguard-Team wöchentlich rund 130'000 Antiviren-Definitionen, 70 IPS-Signaturen, 600'000 URL-Signaturen und 34 Millionen Antispam-Signaturen. ■