Bild: iStock

Dossier IT-Sicherheit

In Kooperation mit **Boll Engineering**

Next Generation Enterprise Security

mur. Wer den neuesten Halbjahresbericht der Melde- und Analysestelle Informationssicherung Melani liest, dem wird schwindlig. Die Bundesstelle braucht geschlagene 58 Seiten, um zumindest einen Teil der Gefahren aufzulisten, die Schweizer Unternehmen und ihren IT-Infrastrukturen auflauern. Die Liste der Bedrohungen scheint endlos: Distributed Denial of Service, Website-Defacements, SQL-Injektionen, Zero-day Exploits, Cross Site Scripting, Spionageangriffe, Cybercrime und so weiter. Viele Unternehmen haben darauf reagiert und unterschiedlichste Systeme installiert, um ihre IT-Sicherheit zu erhöhen. Etwa Firewalls, Intrusion-Detection- und -Prevention-Systeme oder Netzwerkproxies und Endpoint-Security-Suiten. Da die Angriffe immer raffinierter werden, stösst dieser Best-of-Breed-Ansatz heute aber an seine Grenzen. Oft harmonieren die zusammengewürfelten Lösungen nicht richtig, behindern sich gegenseitig oder sind schlicht nicht dafür geeignet, aktuelle Bedrohungen abzuwehren. Die Lösung für das Problem sind integrierte Enterprise-Security-Plattformen. Was diese genau bieten und warum sie für Unternehmen sinnvoll sind, erklärt dieses Dossier. Ein Interview zeigt zudem auf, wie die Next-Generation-Sicherheitsplattformen einem Unternehmen helfen können, seine IT-Infrastruktur effektiv zu schützen – im Beispiel gar weltweit über 20 Standorte hinweg.

Integrale IT-Sicherheit

Die herkömmliche Netzwerk- und Endgerätesicherheit – mit vielen unterschiedlichen Geräten und Softwaretools – versagt angesichts des schieren Volumens und der steigenden Raffinesse der Cyberangriffe. Mit einer integrierten Enterprise-Security-Plattform sind Unternehmen optimal geschützt.

DER AUTOR

Peter Bernold
ist Product Manager für Palo Alto Networks bei Boll Engineering, Wettingen

Es ist kaum mehr vorstellbar, dass ein Unternehmensnetzwerk nicht mit dem Internet verbunden ist. Dies gilt übrigens nicht nur für die klassische IT-Infrastruktur in den Büros, sondern zunehmend auch für industrielle Anlagen und Steuersysteme sowie Point-of-Sale-Netzwerke.

Seit den ersten Stunden des öffentlichen Internets in den 1990er-Jahren drängen auch unwillkommene Kräfte in die Netzwerke. Cyberattacken haben sich in den letzten Jahren explosionsartig vermehrt. Angreifer finden immer raffiniertere Methoden, die Sicherheitsanstrengungen der Unternehmen zu umgehen, und verfolgen damit handfeste kriminelle Ziele: Cybercrime ist heute eine 445-Milliarden-Dollar-Industrie und über 100 Länder befinden sich in einem permanenten Cyberkrieg.

Zu den neuartigen Angriffstypen gehören etwa polymorphe Malware, die immer wieder in anderer Gestalt daherkommt (wobei sich die Signatur ständig ändert), Multi-Stage-Attacken, die in verschiedenen Schritten ablaufen, oder Angriffsmethoden, die explizit auf mobile Anwender zielen. Gleichzeitig nehmen sowohl der Netzwerkverkehr als auch die Anzahl der Nutzer und Geräte im Netzwerk massiv zu. Die zunehmende Nutzung von Public-Cloud-Services – manchmal ohne Absprache mit den IT- und Sicherheitsteams – macht das Unternehmensnetzwerk noch angreifbarer und die Arbeit des Security-Teams nicht einfacher. Eigentlich legitime Anwendungen wie etwa Teamviewer werden genutzt, um Anwender auszuspionieren.

IT-Security kommt nicht nach

Die Sicherheitsarchitektur ist in fast allen Unternehmen organisch gewachsen. Meist hat sich dabei ein Arsenal unterschiedlicher Technologien wie Firewalls, Intrusion-Detection- und -Prevention-Systeme, Netzwerkproxies, Gateways, Sandboxes sowie Endpoint-Security-Suiten angesammelt, die nach dem Best-of-Breed-Ansatz kombiniert wurden. Ein solches Patchwork lässt sich schwierig verwalten, es fehlt an Übersicht und Integration. Die einzelnen Lösungen generieren zwar laufend Warnmeldungen, arbeiten aber nicht wirklich zusammen. Um Malware zu eliminieren, sind oft manuelle Prozesse nötig. Ein derart zusammengewürfeltes Gesamtsystem ist zudem nicht gut gerüstet, um mit unbekannten Bedrohungen fertig zu werden. Und nicht selten konzentriert sich die Abwehr auf den Perimeter und vernachlässigt Angriffe, die durch eingeschleuste Malware oder Social Engineering direkt auf den Nutzer zielen und dann innerhalb des Unternehmensnetzwerks wüten.

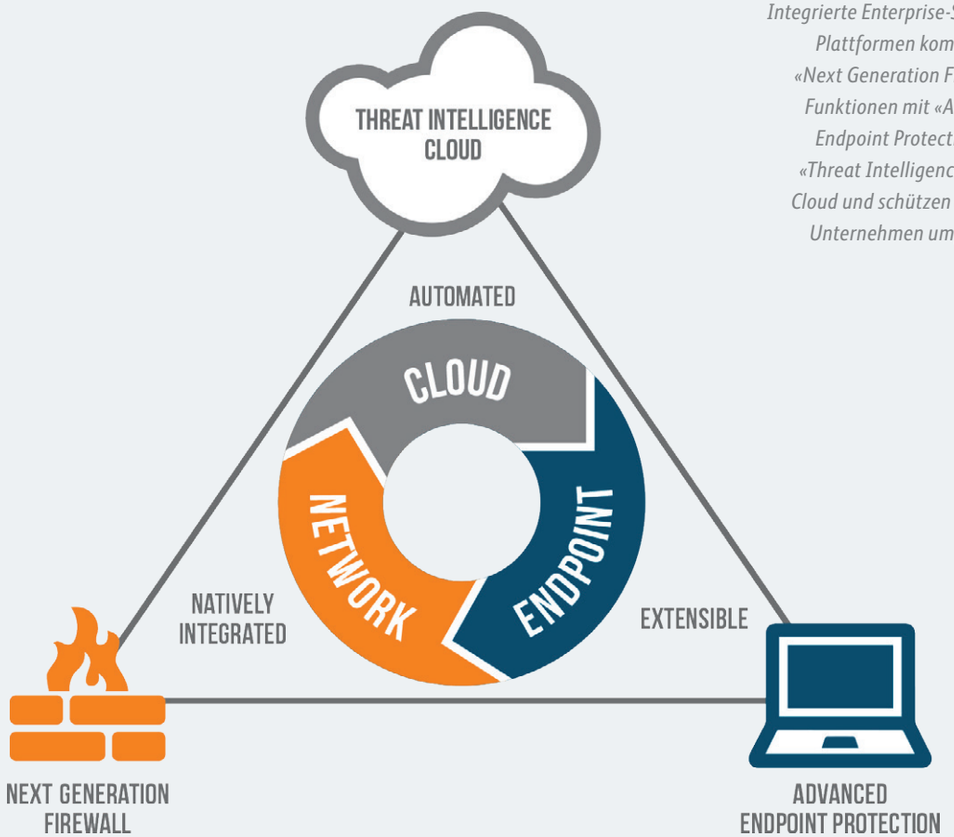
Eine Auswertung von Firewall-Logs durch einen Security-Anbieter zeigt, dass zwar die meiste Malware nach wie vor über die Standard-Ports für Web- und Mailverkehr ins Netz gelangt. Immer mehr kommen aber auch andere, applikationsspezifische Eintrittsstellen zum Zug. Ein Beispiel: Da der Standard-Port für FTP vielerorts gesperrt ist, werden FTP-Zugänge auf anderen Ports eingerichtet. Die übliche Regel für die Ports 20 und 21 deckt solche Fälle nicht ab. Einige weitere Resultate: Ganze 6 Prozent der analysierten Dateien waren Malware, bei den ausführbaren Dateien sogar 50 Prozent. Und 77 Prozent der Files waren den klassischen Virenscannern unbekannt.

Eine Best-of-Breed-Sicherheitsarchitektur ohne echte Integration der Funktionsbereiche und Komponenten kann angesichts der immer raffinierteren Angriffe, des steigenden Malware-Volumens und der zunehmenden Zahl und Diversität der Nutzer eigentlich nur versagen. Was es vielmehr braucht, ist ein neuer Ansatz, der Bedrohungen durch das ganze Unternehmen hindurch erkennt und eliminiert.

Security-Architektur der neuen Generation

Den dringenden Bedarf nach einer neuen Art von IT-Sicherheit stellt auch das Marktforschungsunternehmen Enterprise Strategy Group (ERG) fest. Eine umfassende Sicherheitsarchitektur für grössere Unternehmen sollte demnach unter anderem folgende Ansprüche erfüllen:

- Zentrales Management: Um eine valable Gesamtübersicht zu erreichen, müssen alle Services und Geräte der Security-Infrastruktur von einer zentralen Stelle gesteuert und überwacht werden.
- Unterstützung für verschiedene Formfaktoren und an jedem Ort: Security-Dienste sollten in Form von physischen und virtualisierten Geräten sowie als Cloud-Services zur Verfügung stehen, damit sie an jeder Stelle im Unternehmen passend eingesetzt werden können – vom Hauptsitz über die Filialen bis zum mobilen Anwender.
- Ein Sortiment von Netzwerk-Sicherheits-Diensten, die unabhängig von Ports, Protokollen und Anwendungen zwischen legitimen und bösartigen Datenpaketen unterscheiden können. Sie sind dazu auf den Ebenen 2 bis 7 des OSI-Schichtenmodells aktiv und unterstützen Paketfilterung im gesamten Netz (Ubiquitous Packet Filtering), vom Perimeter bis zum Rechenzentrum. Auch die Endgeräte müssen in die Gesamtarchitektur eingebunden sein, damit die Bedrohungsabwehr im Netzwerk und am Endpunkt koordiniert abläuft.
- Blockieren von bekannten und unbekannten Bedrohungen am Endpunkt: Die Endgeräte müssen vor allen Angriffen geschützt werden, insbesondere auch vor bisher unbekannten Bedrohungen. Dies erfordert neue Technologien, die sich auf generelle Angriffstechniken statt einzelne Bedrohungen konzentrieren.
- Integration mit globalen Bedrohungsanalysen: Die interne Netzwerk- und Endpunktsicherheit sollte durch automatisierten Rückgriff auf cloudbasierte «Threat Intelligence»-Dienste er-



Integrierte Enterprise-Security-Plattformen kombinieren «Next Generation Firewall»-Funktionen mit «Advanced Endpoint Protection» und «Threat Intelligence» in der Cloud und schützen dadurch Unternehmen umfassend.

gänzt werden. So lassen sich Bedrohungen, die anderswo bereits aufgetreten sind, leicht erkennen und abwehren. Idealerweise liefern solche Dienste Erkenntnisse zu unterschiedlichen Aspekten wie neue Software-Sicherheitslücken, bösartige URLs, neu entdeckte Malware und neuartige Malware-Taktiken.

- Umfassende Visibilität: Die Sicherheitsarchitektur sollte die sicherheitsrelevanten Daten in Echtzeit erheben und das Security-Team mit situations- und branchengerechten Analysen versorgen, sodass es rechtzeitig reagieren kann. Dabei muss auch der SSL/TLS-verschlüsselte Verkehr analysiert werden – wichtig angesichts der zunehmenden Nutzung von Mobilgeräten und Cloud-Services.

Einheitliche Enterprise-Security-Plattform

Am besten gelingt die Umsetzung dieser Anforderungen mit einer integrierten Plattform, die von Anfang an auf die nahtlose und automatische Zusammenarbeit aller Funktionsbereiche ausgelegt ist. Eine «Next Generation Enterprise Security Platform» lässt sich zum Beispiel in Form eines geschlossenen Kreislaufs umsetzen:

- Die «Next Generation Firewall» kombiniert die herkömmlichen Firewall-Funktionen wie Paketfilterung, Stateful Inspection, NAT und VPN mit einer tiefergehenden Analyse des Netzwerkverkehrs auf höheren Schichten des OSI-Modells («Application Firewall»), einem Intrusion-Prevention-System und Techniken wie SSL- und SSH-Interception und URL Filtering. Sie wendet bekannte Bedrohungen ab, leitet unbekannte, potenziell bösartige Pakete an die Cloud weiter und unterscheidet etwa zwischen geschäftsrelevanten und unerwünschten Daten, die problemlos blockiert werden können.
- Die «Threat Intelligence Cloud» sammelt die Bedrohungsangaben aus den Netzwerken und Endpunkten der angeschlossenen Unternehmen, analysiert und koordiniert die Erkenntnisse und liefert die Ergebnisse an die Firewalls und die Endpunkte.
- Die «Advanced Endpoint Protection» untersucht alle Prozesse und Dateien, mit denen die Nutzer auf den Endgeräten umgehen. Sie wehrt bekannte und unbekannte Bedrohungen direkt auf dem Endgerät ab und nutzt dazu die Informationen aus der Cloud. Bei der Analyse stellt sie zum Beispiel fest, dass Dateien verschlüsselt werden sollen und blockt den Versuch ab – so kann Ransomware erkannt und abgewehrt werden.

Wenn alle Komponenten reibungslos zusammenarbeiten, wird die sehr aufwendige Analyse- und Filterungsarbeit durch geschickte Techniken wie die parallele Verarbeitung verschiedener Schritte beschleunigt und der Kontext bleibt über den gesamten Kreislauf erhalten. So «weiss» zum Beispiel der URL-Filter, woher die Daten ursprünglich kamen und kann die Bedrohungslage besser beurteilen. Im herkömmlichen Best-of-Breed-Ansatz wäre dies nicht möglich.

«Eine zukunftsorientierte Sicherheitsplattform musste die Firewall ersetzen»

Remo Lüchinger ist Geschäftsführer der Allit GmbH. Der IT-Dienstleister hat bei einem Kunden, der an über 20 Standorten aktiv ist, eine altgediente Firewall-Lösung durch eine Next-Generation-Sicherheitsplattform abgelöst. Im Interview mit der Redaktion erklärt Lüchinger, wie die Herausforderungen in diesem Projekt gemeistert wurden. Interview: George Sarpong

«Die Enterprise-Sicherheitsplattform von Palo Alto verkörpert einen völlig neuen Denkansatz im Bereich IT-Sicherheit.»

Remo Lüchinger, Geschäftsführer von Allit

Herr Lüchinger, wie kam es zu dem Projekt?
Remo Lüchinger: Der Kunde – ein international tätiges Industrieunternehmen aus der Ostschweiz, das aus Sicherheitsgründen nicht genannt werden möchte – hatte seit 15 Jahren eine Firewall-Lösung im Einsatz. Sie hat, was die Firewall-Funktionalität angeht, gut funktioniert, zeigte aber Schwächen bei der Applikationserkennung, beim Management und beim Reporting. Das Unternehmen floriert und expandiert stark, sodass die bestehende Lösung durch eine zukunftsorientierte Sicherheitsplattform ersetzt werden sollte, die nicht nur klassische Firewall-Funktionen bietet.

Wie wurde die neue Lösung evaluiert?
In der engeren Wahl waren die Hersteller Cisco, Check Point und Palo Alto Networks. Nach einer eingehenden Analyse des Produktangebots haben wir die drei Hersteller eingeladen, je ein Proof-of-Concept zu erstellen. Die Lösungen wurden auf Herz und Nieren geprüft, vor allem auch was die Leistungsfähigkeit und Flexibilität betrifft. Die Plattform von Palo Alto hat sich als klarer Testsieger erwiesen.

Was war für den Entscheid massgebend?
Die gewählte Lösung war nicht die preisgünstigste, aber in puncto Performance lag sie deutlich vorne. Zudem hat sie genau die Probleme gelöst, die der Kunde hatte. Ausserdem war die technische Unterstützung durch den Hersteller hervorragend – das war sicher mit ausschlaggebend. Ganz wichtig war auch das zentrale Management und das Reporting. Das funktionierte bei der früheren Lösung nicht zufriedenstellend.

Wie sieht die gewählte Konfiguration aus?
Der Kunde ist weltweit an über 20 Standorten vertreten. Am Hauptsitz sind ein Cluster mit 4-Gbps-Firewalls und das zentrale Managementsystem installiert. Die grösseren Standorte sind mit 2-Gbps-Firewall-Clustern, die kleineren je mit einer 100-Mbps-Einheit ausgestattet. Vernetzt sind die Standorte per Site-to-Site-VPN.

Eine wichtige Komponente ist der cloudbasierte Threat Intelligence Service, der vom Input der Nutzer lebt. Übergibt der offenbar datensensible Kunde seine Angaben über potenzielle Bedrohungen an die Cloud?
Ja, das tut er. Denn diese Informationen sind anonymisiert und können ohne Risiko geteilt werden.

Was waren für Sie die Besonderheiten des Projekts?
Die Produkte waren für uns als Dienstleister neu, unser Know-how noch beschränkt. Wir haben die Lösung gemeinsam mit dem Kunden evaluiert, wobei uns Hersteller und Distributor tatkräftig unterstützt haben. Sonst wäre es wohl nicht möglich gewesen, das Projekt erfolgreich umzusetzen. Für den Betrieb entscheidend ist, dass das zentrale Managementsystem eine einfache Überwachung der gesamten Netzwerksicherheit ermöglicht und viel Automation bietet. Denn der Kunde hat eine relativ schlanke IT-Abteilung, die auf optimale Softwareunterstützung angewiesen ist.

Und was zeichnet das Produkt besonders aus?
Die Enterprise-Sicherheitsplattform von Palo Alto verkörpert einen völlig neuartigen Denkansatz im Bereich IT-Sicherheit mit ganz neuen Möglichkeiten. Man spürt auch, dass es sich um Enterprise-Produkte handelt: Es funktioniert einfach, und zwar so, wie es sollte. Aufgrund unserer Erfahrungen in diesem ersten Projekt werden wir die Lösung in Zukunft sicher auch bei weiteren Kunden einsetzen können.

Remo Lüchinger, Geschäftsführer der Allit GmbH.