Bild: Fotolia

DOSSIER POWER TO CONTROL
IN KOOPERATION MIT BOLL ENGINEERING

Auf gleicher Augenhöhe

jae. «X-as-a-Service» hat sich in der heutigen IT-Welt etabliert. Von SaaS über PaaS hin zu IaaS kann ein Unternehmen alles bekommen, was das Herz begehrt. Zum Leidwesen vieler wird jedoch seit einiger Zeit von kriminellen Organisationen vermehrt eine neue «Dienstleistung» angeboten: «Crime-as-a-Service», kurz «CaaS». Eine Dienstleistung, die sich anscheinend lohnt und laut Patrick Michel, Head of Sales bei Boll Engineering, höchst lukrativ ist. Die erzielten Gewinnmargen sollen sogar über jenen im Drogenhandel liegen. Zudem wird seit 2011 weltweit eine starke Zunahme intelligent durchgeführter Angriffe auf öffentlich-rechtliche Organisationen sowie auf Infrastrukturen privater Unternehmen festgestellt.

Umfassender Schutz nötig

Unternehmen und Organisationen müssen sich also warm anziehen. Doch wie können sie Sicherheitsrichtlinien intern durchsetzen und so verhindern, dass sie zum Opfer von «CaaS» werden? Michel liefert in seinem Beitrag einige Lösungsansätze, um für etwaige Angriffe gewappnet zu sein.

Er plädiert für einen umfassenden Schutz, der dank des Zusammenspiels diverser Sicherheitsmechanismen erreicht werden kann. Dazu gehören unter anderem Richtlinien auf User-Ebene oder die Definition unterschiedlicher Security-Einstellungen für private und firmeneigene Geräte. Zudem soll eine umfassende Lösung einen Überblick über die aktuelle Gefährdungssituation der gesamten IT-Landschaft liefern, damit in einem Notfall rasch eingegriffen werden kann.

Bleibt aber immer noch das Risiko durch einen Angriff seitens eines Mitarbeiters, der dank seiner Position den Zugriff auf alle möglichen Applikationen auf dem Silbertablett serviert bekommt. Sicherheitsverantwortliche können sich also auch mit dem besten Schutz nicht entspannt im Sessel zurücklehnen. Aber vielleicht können sie sich zumindest etwas sicherer fühlen und dem Gegner bei einem Angriff bestenfalls auf gleicher Augenhöhe begegnen. <

> **Seite 32**
«The Power to Control» – auf dem Weg zur konsolidierten Sicherheit

> **Seite 34**
Drahtlos und trotzdem sicher

«The Power to Control» – auf dem Weg zur konsolidierten Sicherheit

Neue Angriffsformen, mehrstufige Attacken, gut organisierte Hackergruppen, eine Vielzahl verletzlicher Systeme, Komponenten und Applikationen – um eine Rundum-Sicherheit für die IT gewährleisten zu können, wird ein übergreifender Ansatz mit integralen Konfigurations-, Analyse- und Kontrollfunktionen benötigt. Patrick Michel

IT-Security-Verantwortliche sind mit immer komplexeren Rahmenbedingungen konfrontiert, mit einer Vielfalt an Systemen, Technologien und Applikationen, die allesamt gesichert werden müssen. Es reicht nicht aus, einen wirksamen Perimeter-Schutz zu etablieren, wenn gleichzeitig Datenbanken – Dreh- und Angelpunkt sämtlicher Firmen-, Kunden- und Projektinformationen – ungeschützt bleiben. Die daraus entstehenden Gefahren sind enorm – und zum Beispiel für viele Banken bittere Realität. Ein weiterer sicherheitsrelevanter Faktor ist die zunehmende Verletzlichkeit der Firmen beziehungsweise deren Abhängigkeit von funktionierenden, stets verfügbaren Systemen, Daten, Applikationen und Kommunikationsdiensten. Lahmgelegte Webshops oder attackierte Onlineportale können verheerende Folgen haben.

Einen ebenso starken Einfluss auf die IT-Sicherheit hat der Trend zur Einbindung privater mobiler Geräte ins Firmennetz (Bring your own Device). Diese Entwicklung stellt für die IT-Security eine eigentliche Zäsur dar und bringt statische Sicherheitsrichtlinien an ihre Grenzen. Technologien wie Benutzer- und Geräte-Authentifizierung (Identity- und Access-Management), VPN, SSL-VPN, Datenverschlüsselung, Device-Härtung, Verschleierung, Konformitätsüberprüfungen oder Enterprise Wipe sind folglich ein Muss.

Grosse Herausforderungen an die IT-Security stellen auch die vermehrte Nutzung cloudbasierter Dienste sowie die rasante Zunahme von Web-2.0-Anwendungen. Sie sind verbunden mit neuen Schwachstellen, zusätzlichen Angriffszielen sowie mit neuen Formen der Bedrohung. Diese strapazieren nicht nur die IT-Sicherheit selbst, sondern erschweren auch das Erfüllen von Compliance-Anforderungen.

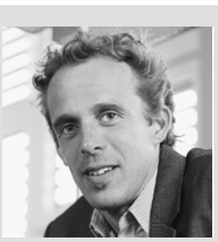
Dank «Application und User Control» erhalten die für die IT-Security zuständigen Personen einen stets aktuellen Überblick über das aktuelle Gefährdungspotenzial sowie eine leistungsfähige Plattform zur Durchsetzung firmenweiter Sicherheitsrichtlinien. Bild: Fortinet

Ob durch die Nutzung von Web-2.0-Anwendungen wie Facebook, Skype, Pinterest, Dropbox und Salesforce, die Verwendung von Cloud- und Virtualisierungstechnologien oder die standortunabhängige Einbindung mobiler Geräte ins Firmennetz: User, Systeme und Programme lassen sich nicht mehr klar definierten IP-Adressen oder TCP-Ports zuordnen. Folglich reichen für deren Kontrolle konventionelle Technologien wie Paketfilter, VPN-Gateway, Content Filter oder IDS/IPS nicht mehr aus.

Intelligent durchgeführte Angriffe

Seit 2011 wird weltweit eine starke Zunahme intelligent durchgeführter Angriffe auf öffentlich-rechtliche Organisationen (Regierungen, Verteidigungsministerien) sowie auf Infrastrukturen privater Unternehmen festgestellt. Eine wichtige Rolle spielen dabei sogenannte «Advanced Persistent Threats» (APT). APTs zeichnen sich unter anderem dadurch aus, dass sie verschiedene bekannte und unbekannte Schwachstellen ausnutzen und unterschiedlichste Angriffsmethoden zu einem gefährlichen «Cocktail» kombinieren. So etwa E-Mail-Phishing, Social Engineering, DDoS- und App-DDoS-Attacken, SQL-Injection und Identitätsdiebstahl. Oft lassen sich die Angreifer mit ihren Aktivitäten viel Zeit, um unentdeckt zu bleiben.

Neben ATPs bilden auch sogenannte «Insider Threats» (also Bedrohungen, die von innen kommen) ein zunehmendes Sicherheitsrisiko. Deutlich wurde dies in der Causa Hildebrand, die zum Fall des früheren Nationalbankpräsidenten führte. Eine weitere Entwicklung kann mit «Target Attacks» (TA) bezeichnet werden. Im Gegensatz zu früheren, breit angelegten und unspezifischen Angriffen handelt es sich bei TAs um gezielte Attacken, mittels derer ausgewählte Organisationen «überfallen» und geschädigt werden. Ghostnet, ein in zahlreichen Botschaften verteiltes Botnet, das dem Ausspionieren des Dalai Lama diente, ist ein populäres Beispiel



Patrick Michel ist Head of Sales bei Boll Engineering.

dafür. Ebenso Stuxnet, eine Schadsoftware zur Störung des iranischen Atomprogramms, sowie das Hacken der Sony Playstation, das den Zugriff auf Privatdaten von mehr als 77 Millionen Nutzern ermöglichte.

Crime-as-a-Service

Ein weiterer unübersehbarer Trend ist die vermehrte Nutzung mobiler Geräte zur Verbreitung von Malware und für die Etablierung mobiler Botnetze. Definitiv Realität ist diese neue Bedrohungsform seit der Entdeckung von «Geinimi» im Jahr 2011, dem ersten auf Android basierenden Botnet, anhand dessen sich infizierte Smartphones aus der Ferne steuern lassen.

Ein entscheidender Faktor ist ferner das Wachstum und die zunehmende Professionalisierung der kriminellen Organisationen. Zu dessen Dienstleistungsangebot gehört der Handel mit noch unbekannten Schwachstellen (Vulnerabilities) ebenso wie der Aufbau von Botnetzen oder wirksame Attacken auf ausgewählte Ziele. Selbst Qualitätsgarantien und QA-Support werden von gut organisierten kriminellen Organisationen angeboten. Dienstleistungen dieser Art – sie werden oft als «Crime-as-a-Service» (CaaS) bezeichnet – sind vergleichsweise leicht zugänglich und für die Anbieter höchst lukrativ. Es werden Gewinnmargen realisiert, die über jenen im Drogenhandel liegen.

Umfassende IT-Security dank integralem Ansatz

Diese und weitere Faktoren führen dazu, dass konventionelle Firewalls – mögen sie noch so leistungsstark sein – nicht in der Lage sind, eine umfassende Rundum-Sicherheit zu gewährleisten. Benötigt wird vielmehr ein übergreifender, konsolidierter Ansatz mit integralen Konfigurations-, Analyse- und Kontrollfunktionen. Diese bilden die Voraussetzung dafür, firmenweite Sicherheitsrichtlinien zu etablieren und durchzusetzen. Von Bedeutung sind in diesem Bestreben unter anderem die folgenden Aspekte:

- **Kontrolle auf User- und Applikationsebene**

Die Kontrolle von Usern, Applikationen und Geräten ist ein zwingendes Leistungsmerkmal jeder tauglichen IT-Security-Strategie. Dies vor dem Hintergrund, dass zum Beispiel sämtliche Webapplikationen das HTTP- beziehungsweise HTTPS-Protokoll verwenden und deshalb nicht über IP-Adressen, Port-Nummern und Protokolle identifizierbar sind. Lösungen, die die Umsetzung von Sicherheitsrichtlinien auf User- und Applikationsebene erlauben, ermöglichen in der Regel eine granulare Definition, welche Applikationen (oder Teile davon) wann und für wen zugelassen oder gesperrt sind (User-based Policy Enforcement). Komfortfunktionen wie die Bildung von Klassen erleichtern diesen Prozess. So ist es zum Beispiel möglich, HTTPS firmenweit freizugeben, hingegen alle Skype-relevanten Anwendungen zu blockieren und die Freigabe und Sperrung von Social-Media-Applikationen wie Facebook oder Pinterest zeitabhängig zu steuern.

- **Erkennen und Blockieren von Schadcode und Angriffen**

Unified-Thread-Management-Systeme (UTM) mit integrierter «Application Control» (oft als «Next Generation Firewall» bezeichnet) sind in der Lage, den gesamten Datenverkehr beziehungsweise User, Geräte und Applikationen in Echtzeit zu überwachen, zu visualisieren und – wenn nötig – auf Basis der definierten Sicherheitsrichtlinien und stets aktualisierter Signaturen aktiv ins Geschehen einzugreifen. Wichtig ist dabei, dass auch bis dato unbekannte Verhaltensmuster – selbst bei verschlüsselter Datenübertragung – erkannt und die möglichen, daraus entstehenden Gefahren dediziert abgewehrt werden.

Um einen umfassenden Schutz erreichen zu können, ist das Zusammenspiel diverser Sicherheitsmechanismen notwendig. Dazu gehören unter anderem die Bestimmung von Policys auf User-Ebene oder die Definition unterschiedlicher Security-Einstellungen für private und firmeneigene Geräte. Auch das Verhalten der einzelnen Devices muss erkannt und ausgewertet werden, sodass beispielsweise mobile Geräte mit einer sich verschlechternden Reputation im Zeitverlauf gesperrt werden. Bedeutsam ist ferner das Erkennen, welche Applikationen auf den Endgeräten installiert sind und welche Anwendungen innerhalb von Applikationen laufen. Auch verschlüsselte Daten, die über Protokolle wie HTTPS, POP3S, SMTPS und IMAPS transportiert wird, sollte entschlüsselt und analysiert werden können. Dasselbe gilt für P2P- und IM-Anwendungen, die via Tunnel kommunizieren.

In diesem Kontext ebenfalls erwähnenswert ist die Zuteilung von Bandbreite auf einzelne Applikationen. Dabei können businesskritische Anwendungen und weniger relevante Applikationen unterschiedlich behandelt werden. Bandbreitenbegrenzungen für Videos beispielsweise helfen, dass geschäftsrelevanten Applikationen eine genügend hohe Datenrate zur Verfügung steht und dass der Download von Videos während der Arbeitszeit an Attraktivität verliert.

- **Minimale Latenz, maximale Verfügbarkeit**

Den zahlreichen Sicherheitsmassnahmen gemeinsam ist, dass sie ausgesprochen ressourcenintensiv sind und dass sie in Echtzeit und ohne spürbare Beeinträchtigung der System- und Netzwerkleistung zur Verfügung stehen müssen. Vor diesem Hintergrund wird offensichtlich, weshalb die Verwendung spezialisierter Hardware und Software notwendig ist. Um selbst das Enterprise-Umfeld mit hoch performanten, latenzfreien Systemen zu bedienen, kann auf eine Kombination aus selbst entwickelter Hochleistungshardware, speziellen Prozessoren und Beschleunigungs-Chips gesetzt werden. Dadurch wird es möglich, spezifische Security-Aufgaben wie IPS, AV-Inspection, SSL-Entschlüsselung oder User- und Application-Control in einer dedizierten Umgebung parallel auszuführen und markant zu beschleunigen. Zum Erreichen einer maximalen Verfügbarkeit (High Availability) der Systeme stehen Features wie Cluster-Installationen, geografische Redundanz oder unterbrechungsfreie Upgrades zur Verfügung.

- **Visualisierung und Reporting – firmenweit und themenübergreifend**

Wer hat wann und für wie lange welche Applikationen genutzt? Wer hat versucht, auf spezifische Daten zuzugreifen? Welche Applikationen wurden wie häufig und wie intensiv genutzt? Von wem und über welche Geräte wurden Viren eingeschleust? Über welche Kanäle waren Angriffe zu verzeichnen? Welche Anwendungen beeinträchtigen die Performance der IT, und welches Gefahrenpotenzial geht von einzelnen Applikationen aus? Um diese und die zahlreichen weiteren sicherheitsrelevanten Fragen beantworten zu können, sind einfach verständliche statistische Reports und Log-File-Analysen notwendig. Wichtig ist dabei, dass möglichst alle für die IT-Security eingebundenen Systeme wie UTM-Appliances, Secure-E-Mail-Lösungen, Appliances zur Sicherung der Datenbanken sowie Secure-Web-Lösungen zentral gemanagt werden können. Sie sollten eine ganzheitliche Überwachung erlauben, die Durchsetzung einer firmenweiten IT-Security-Policy unterstützen und das Generieren übergreifender Reports ermöglichen. Eine derart breit aufgestellte integrale End-to-End-Lösung bildet die perfekte Basis für eine ganzheitliche IT-Security-Strategie mit dem Anspruch auf «The Power to Control». <

Drahtlos und trotzdem sicher

WLANs erfreuen sich grosser Beliebtheit. Doch in puncto Sicherheit stellen sie die Betreiber vor grosse Herausforderungen. Neben sicherheitsspezifischen Themen sind auch Aspekte wie Skalierbarkeit, Vielfalt der APs, Performance sowie Unterstützung sämtlicher Standards entscheidende Kriterien. Patrick Michel

Der Betrieb eines WLANs ist kein einfaches Unterfangen. So ist beispielsweise sicherzustellen, dass Gäste trotz Nutzung des Firmenfunknetzes nicht auf unternehmensinterne Daten zugreifen können. Oder es ist dafür zu sorgen, dass kritische Webzugriffe, die beispielsweise Schadcodes ins Firmennetz einschleusen oder zu Reputations- und Folgeschäden führen können, verhindert werden. Um dies gewährleisten zu können, muss der Datenverkehr kontinuierlich überwacht und gefiltert werden, was sich besonders effizient und einfach mittels Application Control und Webfiltering erreichen lässt.

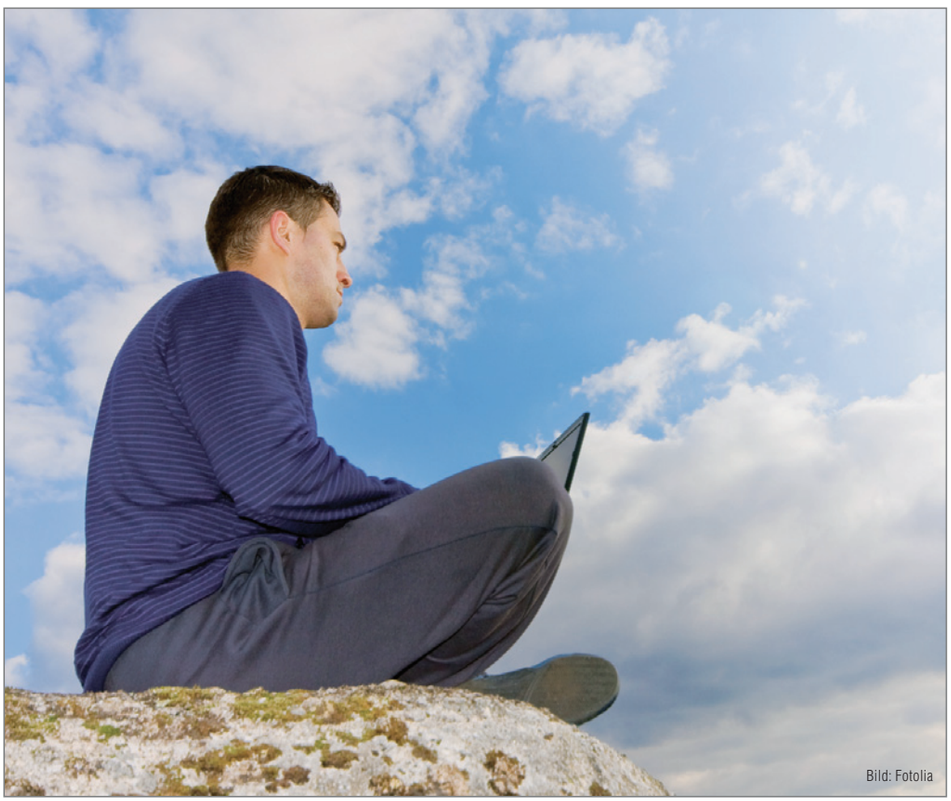


Bild: Fotolia

Für den Aufbau sicherer WLANs stehen seit kurzem Lösungen zur Verfügung, die die einzelnen Access Points (APs) mit einer zentralen Firewall mit integriertem AP-Controller verbinden. Sie leiten den gesamten Datenverkehr des Wireless-LANs über die Multi-Threat Security-Appliances. Diese stellen dem Funknetz sämtliche benötigten Abwehr- und Sicherheitsmechanismen zur Verfügung – so beispielsweise Funktionen wie Stateful Inspection Firewalls, Application Control, Web-Filter, Antivirus, Intrusion Prevention und SSL Traffic Inspection.

Derart integrierte Gesamtlösungen ermöglichen einerseits ein zentrales und umfassendes Sicherheitsmanagement und wissen andererseits hinsichtlich Konfiguration und Skalierbarkeit zu überzeugen. So erfolgt die Einbindung und das Management sämtlicher APs zentral über den in der Security Appliance integrierten AP-Controller. Dieser ermöglicht auch das automatische und umfassende Einspielen der jeweils neuesten Signaturen und der damit verbundenen Sicherheitsfunktionen. Ebenso komfortabel erweist sich die Bildung und Trennung unterschiedlicher virtueller Netze sowie die Bildung netzspezifischer Security-Richtlinien. So ist es problemlos möglich, über die gleichen physischen APs und Controller parallel mehrere unterschiedliche Wireless-Netzwerke zu betreiben.

Notwendige Schutzmechanismen

Bei der Planung und Umsetzung sicherer und skalierbarer Wireless-LANs sind spezifische Leistungsmerkmale zu berücksichtigen. So sollte beispielsweise die Kommunikation zwischen APs und Controller via Tunnel erfolgen. Ein weiteres Kriterium ist das unterbrechungsfreie, AP-übergreifende Mitführen einer Session. Ein nahtloses Roaming unterstützt die Mobilität der User auf dem gesamten Firmenareal.

Von Bedeutung ist ferner das Erkennen sowie das automatische Ausschliessen oder Stören sogenannter «Rogue APs». Dabei handelt es sich um Access Points, die durch Dritte eingeschleust und mit dem internen LAN verbunden werden. Um Rogue APs zu erkennen, überprüfen intelligente WLAN-Lösungen das LAN kontinuierlich nach MAC-Adressen, die nicht erscheinen dürften. Zudem wird ein AP-Frequenzbereich («Radio») dazu verwendet, dauernd nach unerlaubten APs zu scannen. Wird über LAN und Funk ein nicht autorisierter AP erkannt, wird einerseits eine entsprechende Alarmierung ausgelöst und die betreffende AP andererseits via LAN gestört und so ihrer Funktion beraubt.

Neben sicherheitsspezifischen Themen sind auch Aspekte wie Skalierbarkeit, Vielfalt der APs, Performance sowie Unterstützung sämtlicher Standards entscheidende Kriterien. Heute sind Lösungen erhältlich, die bis zu mehrere tausend APs beziehungsweise zehntausende Nutzer gleichzeitig unterstützen. Entsprechende Multi-Threat Security-Appliances mit integriertem AP-Controller weisen WLAN-Kapazitäten von bis zu 49 Gbps auf. Seitens AP sind Lösungen vorhanden, die gleichzeitig zwei Frequenzen (2,4 und 5 GHz) und mehrere «Radios» unterstützen. Diese stellen sicher, dass alle Normen (a/b/g/n) unterstützt sind und folglich sämtliche denkbaren Anwendergeräte eingebunden werden können. Interessant sind ferner Access Points mit PoE-Schnittstelle («Power over Ethernet»), die eine separate Zuführung der Speisespannung überflüssig machen. <