



Application Control

Die Kontrolle zurück gewinnen: Sicherheit steigern, Zugang zu Applikationen erlauben und dabei das Unternehmen schützen

White Paper

WatchGuard® Technologies, Inc.

December 2010

Einführung: Produktivität und IT-Security ins Gleichgewicht bringen

Während die Arbeitnehmer mit neuen und kreativen Zugängen das Web nutzen, kämpfen die Unternehmen damit, die Kontrolle über das Unternehmensnetzwerk zu behalten. Gleichzeitig müssen sie sicherstellen, dass Mitarbeiter, Geschäftspartner und andere Akteure auf relevante Funktionalitäten sicher zugreifen können. Applikationen drängen in unüberschaubarer Anzahl ins Netz und täglich kommen weitere dazu. Verkompliziert wird diese Entwicklung durch die Tatsache, dass „gute“ von „bösen“ Applikationen nicht mehr klar unterschieden werden können. Einige der Applikationen wurden für Business-Zwecke konzipiert und sind darauf ausgelegt, Sicherheitsrisiken zu minimieren und die Produktivität zu maximieren. Am anderen Ende der Palette stehen Applikationen, die Daten stehlen, Computer beschädigen und die Netzwerkaktivitäten unterbrechen. Eine Vielzahl an Applikationen fällt in den Graubereich zwischen diesen beiden Extremen.

Applikationsfortschritt verkompliziert Security

Bisher haben IT-Administratoren oft den Zugang zu jenen Applikationen verwehrt, die aus der Consumer-Welt kommen. Dieser Ansatz ist zunehmend problematisch, nicht zuletzt weil sich Anwendungen wie Facebook auch für die Businesswelt als wertvoll erweisen, speziell in den Bereichen Vertrieb und Marketing. Tatsächlich nehmen etwa 1,5 Millionen US-Unternehmen aktiv an Facebook teil (siehe dazu auch <http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/>). Gleichzeitig können Facebook-Spiele Produktivitätsräuber sein. Wenn sie darüber hinaus auch noch Malware beinhalten, stellen sie ein großes Sicherheitsrisiko dar.

Diese Entwicklung fordert auf Administrationsseite ein Umdenken bei der Firewall-Konfiguration, um die Unternehmensumgebung optimal zu schützen. Wenige Jahre zuvor konnte über Firewall-Einstellungen (etwa Blockieren von Ports oder Protokollen) der Zugang zu Applikationen gesperrt werden. Weil aber heute viele Applikationen als Web Traffic über Port 80 oder 443 auftauchen, ist dieser Ansatz nicht mehr ausreichend beziehungsweise effektiv. Als Folge hat das Wartungspersonal ein gewisses Maß an Kontrolle über die im Unternehmen verwendeten Applikationen verloren.

Instant Messaging (IM) und Peer-to-peer (P2P)-Applikationen sind die besten Beispiele dafür, dass neue Security-Standards benötigt werden. Die erste Generation dieser Applikationen konnte durch klassische Zugangskontrolllisten (ACL) reguliert werden, die auf fixen oder beschränkten Ziel-Ports und bereits identifizierten Registration-Servern basieren. Applikationen der zweiten Generation verwendeten dynamische Ports und Registration-Server, welche regelmäßig die Adresse wechselten oder so extensiv gespiegelt wurden, dass ACL zum Blockieren dieser Applikationen weniger effizient wurden. Die aktuelle Generation vom IM und P2P-Applikationen tritt oft als Webverkehr auf. Dabei verzichten diese Applikationen – beispielsweise Ultrasurf, Skype oder Winny – gänzlich auf Registration-Server und sind damit in der Lage, Firewalls zu umgehen. Speziell Unternehmen, die an Branchenbestimmungen gebunden sind, müssen die Zugangskontrolle für diese Applikationen verstärken.

IT-Administratoren müssen die Kontrolle zurück gewinnen



Der unten stehende Zeitplan stellt dar, nach welchen Lösungsmöglichkeiten die Sicherheitsexperten heute suchen.

Um die heutigen Unternehmensumgebungen zu sichern und die Kontrolle zurück zu gewinnen, müssen die Administratoren eruieren und bestimmen, welche der verwendeten Applikationen für das Business zugelassen, welche Malware sind und welche in die Grauzone dazwischen fallen. Bei letzteren müssen die IT-Experten kontrollieren können, wer Zugang zu den Applikationen hat und zu welchem Zweck. Web 2.0-Applikationen wie Audio und Media Streaming können die Breitbandkapazitäten im Unternehmen massiv beanspruchen. Zusätzlich ist es notwendig, dass Unternehmen in regulierten Branchen die Nutzung von Instant Messaging einschränken, weil sie die Aufbewahrungspflicht für elektronische Nachrichten nicht erfüllen können. Um die Sicherheitsanforderungen und gesetzlichen Compliance-Bestimmungen einzuhalten und eine akzeptable Nutzungspolitik zu betreiben, ist die Kontrolle der Nutzung aller Applikationen, die von Mitarbeitern verwendet werden, unabdingbar.

Die Sicherheitsrisiken von Applikationen

Das Internet ist heute die primäre Quelle von Sicherheitsbedrohungen für Unternehmen – Web-Applikationen stehen auch meist im Fokus der Angreifer. Gleichzeitig steigt die Anzahl an sozialen Netzwerken und neuen Web 2.0-Plattformen. Die Anwender sind oft unsicher, welcher Level von Privatsphäre bei diesen Seiten gewählt werden soll. So schaffen die sozialen Netzwerke eine ideale Basis für Hacker, um Social-Web-basierte Angriffe gegen Mitarbeiter im Unternehmen zu starten.

Anwender vertrauen oft dem Link zu einer Website, wenn er im Rahmen eines sozialen Netzwerks bereitgestellt wird. Sie erkennen nicht, dass solche Zusammenhänge leicht vorgetäuscht werden können.

Setzt man voraus, dass Webverkehr und Applikationen die Quelle für viele Sicherheitsrisiken sind, können IT-Administratoren die potenziellen Gefahren dadurch reduzieren, dass sie die Nutzung der Applikationen auf jene beschränken, die für Geschäftszwecke notwendig sind.

WatchGuard Application Control

WatchGuard entwickelt kontinuierlich Lösungen, um mit den neuesten Security-Herausforderungen für Unternehmen aller Größen Schritt halten zu können. So umfasst WatchGuards XTM Appliance (Version 11.4 und höher) auch Application Control. Damit ist es den Administratoren möglich, eine exakt steuerbare Sicherheitskontrolle für hunderte von Applikationen zu schaffen und nachzuvollziehen, welche Applikationen von wem verwendet werden.

WatchGuard Application Control ist ein voll integriertes Security-Lizenzprogramm für alle WatchGuard XTM Appliances. Es bietet eine umfassende Überwachung von über 1.800 Web- und Business-Applikationen mit dem Ziel, die Produktivität und Sicherheit zu erhöhen. Damit können Administratoren akzeptable Nutzungsrichtlinien für Einzelanwender, Gruppen, die Applikation selbst und Sub-Funktionen durchsetzen. Beispielsweise kann die Marketingabteilung Zugang zu Facebook erhalten, nicht aber zu den Spielen auf dieser Plattform.

Mit über 2.500 unterschiedlichen Signaturen und fortschrittlichsten verhaltensorientierten Technologien bietet Application Control von WatchGuard den Administratoren Einblick in die (versuchte) Nutzung von Applikationen, und das in Echtzeit und als Historie. Diese Kontrolle und Übersicht unterstützt die Unternehmen dabei, geeignete Nutzungsrichtlinien umzusetzen, die den Branchenbestimmungen, politischen oder rechtlichen Vorgaben und auch den Unternehmenszielen entsprechen.

Wie WatchGuard Application Control funktioniert

Mit dem WatchGuard XTM Konfigurations-Tool hat der Administrator die Möglichkeit, eine umfassende Strategie oder auch feiner abgestufte Vorgaben umzusetzen, die spezifische Benutzer, Gruppen, Netzwerke oder andere Kriterien betrachten, um die Nutzung von Applikationen zuzulassen oder diese zu blockieren. WatchGuard XTM mit Application Control untersucht in Echtzeit den Datendurchsatz und erkennt, welche Applikationen den Datenverkehr verursachen. Signatur-basierte Technologie kombiniert mit einer Suchmaschine, die das Applikationsverhalten analysiert, ermöglicht es der WatchGuard XTM Appliance, die Applikationen mit hoher Genauigkeit zu bestimmen. So setzt die Appliance die Security-Strategie des Administrators um und zeichnet die Schritte in einem Log auf. Im Report können die Nutzung der Applikationen sowie die jeweiligen Nutzer nachvollzogen werden.

Die Gefahren des World Wide Web

- 40.000 Websites pro Woche sind gefährdet und 0,7 % der Google-Suchergebnisse zeigen Sites an, die mit Malware verseucht sind (Quelle: Google Security Blog, 25. August 2009).
- Angriffe gegen Web-Applikationen stellen dabei mehr als 60 % der gesamten versuchten Attacken im Internet dar (Quelle: SANS Top 10 Security Risks, September 2009).
- 64 % der Personen, die von AVG befragt wurden, klicken auf Links, die von den Mitgliedern sozialer Netzwerke zur Verfügung gestellt werden. Weitere 26 % tauschen Dateien innerhalb sozialer Netzwerke aus (Quelle: AVG, Social Engineering: Hacking people, not machines, 2009).

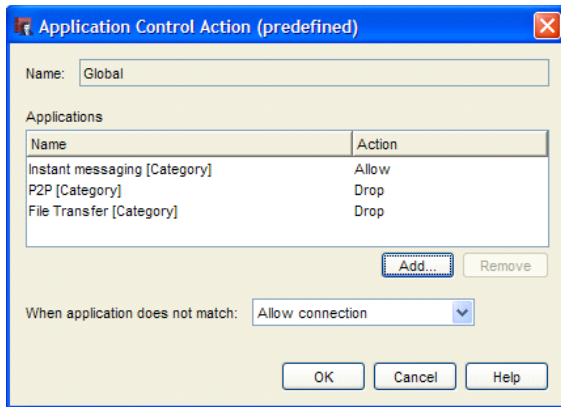


Bild 1: Administratoren können eine umfassende Sicherheitsstrategie im Unternehmensnetzwerk einfach einrichten.

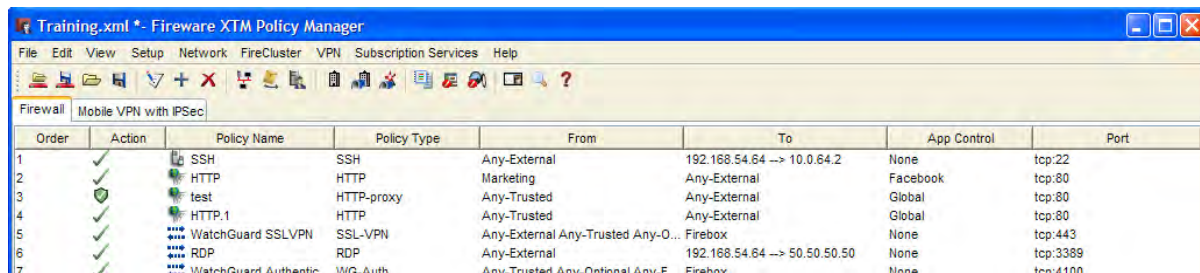


Bild 2: Administratoren können darüber hinaus eine fein abgestufte Kontrolle über hunderte von Applikationen, gereiht nach Kategorie, umsetzen. Dabei ist auch nachvollziehbar, wer welche Applikationen wann verwendet.

WatchGuard Application Control ermöglicht es Unternehmen, eine exakt steuerbare Sicherheitskontrolle für Applikationen, die im Netzwerk verwendet werden, zu realisieren.

Mögliche Szenarien sind:

- Verwendung von YouTube, Skype oder QQ blockieren
- alle P2P-Applikationen für Anwender blockieren, die nicht zum Management zählen
- Zugang zu Social Media Sites wie Facebook und Twitter für die Marketingabteilung erlauben
- Windows Live Messenger für Instant Messaging erlauben, aber Dateitransfer über Windows Live Messenger blockieren
- Media Streaming Applikationen auf bestimmte Zeiten beschränken
- ein Reporting der Top-Ten-Applikationen, die im Unternehmen verwendet werden, erstellen
- ein Reporting der (versuchten) Nutzung von Applikationen durch jeden beliebigen Mitarbeiter im Unternehmen anzeigen

Was bei Application Control zu beachten ist

Bei einer Lösung im Bereich Application Control sind folgende Merkmale wesentlich:

- **Feinstufige Kontrolle:** Um das unterschiedliche Nutzungsverhalten der Benutzer bei Applikationen erfassen zu können, ist es wichtig, einzelne Features zuzulassen, während man andere blockieren kann. Ein Beispiel dafür ist etwa, Windows Live Messenger für Instant Messaging zu erlauben, aber einen Dateitransfer über Windows

Live Messenger zu blockieren, oder den Zutritt zu Facebook zu öffnen, aber Spiele auf Facebook zu sperren.

- **Die Breite von Applikations-Signaturen:** Wichtig ist eine umfassende Auflistung der Signaturen inklusive regelmäßigen Updates und Service durch den Lösungsanbieter. Idealerweise sollten beim Auftreten von neuen Applikationen und Nutzungsverhalten die Signaturen automatisch ein Update erhalten, ohne die gesamte Security-Applikation upgraden zu müssen.
- **Möglichkeit, verschlüsselte Applikationen zu identifizieren:** Die schlauen Programmierer von Applikationen versuchen heute durch Verschlüsseln von Applikationsdaten und -Traffic die Sicherheitsmaßnahmen zu umgehen. Eine hochwertige Lösung verwendet Verhaltensanalysen, um auch gut getarnte Applikationen zu entdecken.
- **Einbindung in die Sicherheitsstrategie:** Es reicht nicht aus, zusätzliche Add-Ons innerhalb eines Intrusion Prevention Service einzusetzen, um ein paar Applikationen anzusprechen. Die Lösung sollte eine Überwachung von Applikationen als Teil der grundlegenden Firewall-Strategie ermöglichen.
- **Gleichgewicht von Performance und Wirksamkeit:** Einige Lösungen, die Kontrolle auf Applikationsebene bieten, setzen teure Hardware voraus, um akzeptable Ergebnisse zu erzielen. Unternehmen sollten sicherstellen, dass die Security-Lösungen hohe Leistung und Wirksamkeit in der Überwachung zu vernünftigen Kosten bieten.

Nutzen für IT-Administratoren und das Unternehmen

Mit Application Control von WatchGuard generieren die Unternehmen vielfältigen Mehrwert. Sie erlangen nicht nur die Kontrolle über die IT-Umgebung im Unternehmen zurück, die Administratoren haben auch mehr Einfluss auf die Applikationen als bisher. Damit können sie mit der laufenden Weiterentwicklung der Applikationen Schritt halten und die Ansprüche des Unternehmens und der Benutzer erfüllen. Mit der Überwachung und Kontrolle der Applikationen stellen die Administratoren sicher, dass die Mitarbeiter zielgerichtet und produktiv ihren Job ausführen und dabei potenzielle rechtliche Schwierigkeiten durch die Nutzung von nicht autorisierten Applikationen vermieden werden können. Die umfassende Application Control ermöglicht den Unternehmen, ihre Sicherheitsrisiken zu beschränken und die Bandbreite an Applikationen zu erhalten, die mit den Unternehmenszielen übereinstimmt.

WatchGuard XTM: Umfassende Firewall für Application Control

Da Mitarbeiter, Partner und weitere Akteure innerhalb der Unternehmensumgebung Zugang zu einer Vielzahl an Applikationen haben, müssen die Unternehmen einen Kompromiss zwischen den Nutzer- und Sicherheitsinteressen finden. Heute lassen sich viele Applikationen nicht in eine klare Organisationsstruktur einreihen, so dass die IT-Administratoren neue Möglichkeiten zur Überwachung benötigen, um feststellen zu

Web-basierte Applikationen sind weit verbreitet

Instant Messaging

QQ, Windows Live Messenger, Yahoo! Messenger, GoogleTalk

Email

Hotmail, Gmail, Yahoo, Microsoft Exchange

Web 2.0

Facebook, LinkedIn, Twitter, Salesforce

Peer to Peer

Gnutella, Foxy, Winny, BitTorrent, eMule

Remote Access Terminals

TeamViewer, GoToMyPC, Webex

Datenbanken

Microsoft SQL, Oracle

Datentransfer

Peercast, Megaupload

Voice over IP

Skype

Streaming Media

QuickTime, YouTube, Hulu

Netzwerk-Management

Microsoft Update, Adobe, Norton, McAfee, Syslog

Tunnel (Web bypass Proxies)

Avoidr, Ultrasurf, Circumventor

können, welche Applikationen von wem zugelassen sind.

Diese Art der Applikationsüberwachung gibt es bereits heute in der WatchGuard XTM Firewall. WatchGuard bietet diese als Teil einer umfassenden Firewall-Lösung, die alle Funktionalitäten für die einfache, komplette und kosteneffiziente Absicherung der Unternehmensumgebung abbildet. Zusätzlich zu der fortschrittlichen, Applikations-basierten Strategie und Umsetzung unterstützt XTM alle traditionellen Port- und Protokoll-basierten Konfigurationen sowie entscheidende Netzwerk-Features wie dynamisches Routing, WAN Failover und Load Balancing. Die VPN-Funktion per drag & drop ermöglicht den einfachen Aufbau von sicheren Site-to-Site Tunnelverbindungen zwischen unterschiedlichen Standorten. Darüber hinaus spart die Palette an interaktiven, Real-Time-Monitoring-Tools Zeit und erleichtert den raschen Überblick über Benutzer, Netzwerk und Security-Aktivitäten.

Neben dem marktführenden Preis-Leistungs-Verhältnis bietet WatchGuard XTM eine Reihe von Security-Lizenzprogrammen, die ein umfassendes Management der Gefahrenabwehr ermöglichen:

- **Reputation Enabled Defense:** Hierbei handelt es sich um eine wirkungsvolle, Cloud-basierte Lösung, die Nutzer vor böswilligen Websites schützt und gleichzeitig den Web-Durchsatz erhöht.
- **spamBlocker:** Blockiert unerwünschte E-Mails mit virenverseuchten Inhalten mit fast hundertprozentiger Sicherheit. spamBlocker erkennt Spam unabhängig von Sprache, Format oder Inhalt der Nachricht und sogar Bild-basierten Spam, der von anderen Lösungen oft nicht identifiziert wird.
- **WebBlocker:** Dieser URL-Filter blockiert den Zugang zu gefährlichen und unzumutbaren Websites am Arbeitsplatz. WebBlocker filtert URLs sowohl mit HTTP- als auch HTTPS-Protokollen, um jene Lücke zu schließen, die andere Filter offen lassen.
- **Gateway AntiVirus:** Ermöglicht einen wirkungsvollen, Signatur-basierten Gateway-Schutz gegen unbekannte Viren, Trojaner, Würmer, Spyware und Malware.
- **Intrusion Prevention:** Überprüft alle Ports und Protokolle, um Angriffe zu blockieren, die mit Standard-Protokollen übereinstimmen, aber böswilligen Inhalt haben – etwa Pufferüberläufe, SQL-Einschleusungen oder Remote File Inclusions.

Weitergehende Informationen zu den WatchGuard Sicherheitslösungen erhalten Sie unter www.watchguard.de oder von Ihrem Händler.

ADDRESS:

Max-Planck-Str. 4
85609 Aschheim-Dornach
Germany

WEB:

www.watchguard.de
germanysales@watchguard.com

Germany Sales:

+49 (700) 92229333

INTERNATIONAL SALES:

+1.206.613.0895

ABOUT WATCHGUARD

WatchGuard, gegründet 1996, entwickelt erschwingliche, ganzheitliche Netzwerk- und Content-Sicherheitslösungen, mit denen Unternehmen ihre Daten, Netzwerke und Geschäfte umfassend schützen können. Die preisgekrönten XTM-Netzwerksicherheitslösungen (Extensible Threat Management) kombinieren Firewall, VPN und Sicherheitsdienste und schützen Netzwerke so vor Spam, Viren, Schadprogrammen und Eindringversuchen. Die neuen XCS-Appliances (Extensible Content Security) schützen darüber hinaus Unternehmensinhalte sowohl in E-Mails als auch im Web und sichern sämtliche wichtigen Inhalte gegen einen Datenverlust ab. Der Hauptsitz von WatchGuard liegt in Seattle im US-Bundesstaat Washington.

©2011 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Firebox und LiveSecurity sind in den USA und/oder anderen Ländern entweder Markenzeichen oder eingetragene Markenzeichen von WatchGuard Technologies, Inc. Alle anderen Markenzeichen oder Markennamen sind Eigentum ihrer jeweiligen Besitzer. Teilnr. CE66721_021511