Trend Micro Deep Security

Server-Sicherheit

Schutz für dynamische Datenzentren

Ein Trend Micro Whitepaper | August 2009

I. SICHERHEIT IM DYNAMISCHEN DATENZENTRUM

IT-Sicherheit dient dazu, Ihr Unternehmen zu befähigen, und nicht, es zu behindern. Herausforderungen und Komplexität Ihrer IT-Sicherheit nehmen jedoch täglich zu. Anforderungen zur Richtlinieneinhaltung erzwingen Sicherheitsstandards für Daten und Anwendungen auf Servern. Physische Server werden durch virtuelle Maschinen ersetzt, um Kosten einzusparen, umweltfreundlicher zu arbeiten und die Skalierbarkeit zu erhöhen. Cloud-Computing ist eine Weiterentwicklung der herkömmlichen IT-Infrastruktur, um weitere Kostensenkungen zu erzielen und gleichzeitig Flexibilität, Kapazitäten und Wahlmöglichkeiten auszuweiten. Server verbergen sich nicht mehr hinter Abwehrmaßnahmen am Netzwerkrand, sondern verlagern sich – wie zuvor die Laptops – außerhalb von Sicherheitsbereichen und benötigen eine finale Verteidigungslinie. Für Ihre tief greifende Sicherheitsstrategie ist es jetzt unerlässlich, ein System zum Schutz von Servern und Anwendungen zu installieren. Dieses System muss umfassende Sicherheitskontrollen bieten und dabei aktuelle sowie zukünftige IT-Umgebungen unterstützen. Trend Micro bietet Antworten auf diese Herausforderungen, so z. B. die Deep Security Lösung.

SERVER UNTER DRUCK

Laut dem 2008 vom Verizon Business Risk Team erstellten Data Breach Investigation Report sind 59 % der jüngsten Datenverluste das Ergebnis von Hacker-Angriffen und Eindringversuchen. Die Datenverluste bei TJX und Hannaford verdeutlichten das Gefahrenpotenzial von Systemangriffen, die den guten Ruf eines Unternehmens schädigen und die Betriebsabläufe erheblich stören können. Für Unternehmen ist es nach wie vor schwierig, ihre Ressourcen einerseits zu schützen und andererseits immer mehr Unternehmenspartnern und -kunden den Zugriff darauf zu ermöglichen.

Aktuelle Payment Card Industry Data Security Standards (PCI DSS) erkennen, dass herkömmliche Schutzmechanismen nicht mehr ausreichen, um Daten vor den neuesten Bedrohungen zu schützen, und dass heute hinter den anwendungsbasierten Firewall-Systemen und den Systemen zur Erkennung und Abwehr von Eindringlingen (IDS/IPS) weitere Schutzschichten erforderlich sind. Drahtlose Netzwerke, verschlüsselte Angriffe, mobile Ressourcen und unzureichend geschützte Webanwendungen tragen alle zu den Schwachstellen von Unternehmensservern bei und bieten so den Nährboden für Hacker und andere Eindringlinge.

In den letzten fünf Jahren hat sich die Technologie von Plattformen für Datenzentren, die zum Großteil auf physischen Servern basierten, erheblich verändert. Der Ressourcenbedarf herkömmlicher Datenzentren wird kleiner, um mit Hilfe von Serverkonsolidierung Kosteneinsparungen und eine umweltfreundlichere IT zu ermöglichen. Nahezu jedes Unternehmen hat die Aufgaben seines Datenzentrums inzwischen ganz oder teilweise virtualisiert, damit physische Server, die früher nur einem Zweck bzw. einer Aufgabe gedient haben, jetzt mandantenfähig werden. Nach Schätzungen der Gartner Group wird sich bis zum Jahr 2011 die Zahl der virtuellen Maschinen mehr als verzehnfachen. Man rechnet damit, dass bis 2012 die meisten Aufgaben von x86-Servern auf virtuellen Maschinen ausgeführt werden.

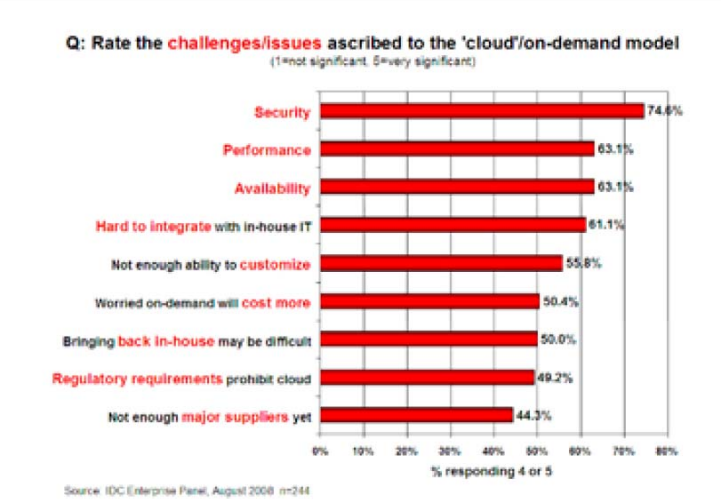
SERVER VERMEHREN SICH SCHNELL UND REGE

Die erheblichen Vorteile der IT-Virtualisierung für Unternehmen haben bereits zu einer weiten Verbreitung beigetragen. Durch Virtualisierung wird die Kapazität erhöht und die Reaktionsfähigkeit auf Nachfragen von Unternehmenskunden verbessert. Außerdem führt die effizientere Nutzung von Hardware- und Software-Lizenzen zu einer weiteren Konsolidierung der Server-Aufgaben. In virtuellen Umgebungen verschwindet die strikte Trennung von Netzwerkgeräten und Servern – beide sind nun auf Virtualisierungsplattformen vereint. Da Sicherheitsanwendungen für Netzwerke jedoch nicht den Verkehr zwischen virtuellen Maschinen überwachen, eröffnet das Hosten von Aufgaben verschiedener Sicherheitsstufen Möglichkeiten für Angriffe. Motion Tools – unerlässlich zur Verwaltung geplanter Ausfallzeiten, der wirksamen Nutzung von Virtualisierungsressourcen und der Anwendungsverfügbarkeit – führen zur weiteren, gemeinsamen Auslastung des Servers und beeinträchtigen die Verwaltung des Regeleinhaltungsverlaufs sowie virtuelle Sicherheitsanwendungen. Außerdem erhöht der sich zwangsläufig ergebende „Wildwuchs“ virtueller Maschinen die Wahrscheinlichkeit, dass unzureichend geschützte Geräte bösartigem Datenverkehr ausgesetzt sind. IT-Mitarbeiter müssen die verwendeten Methoden eingehend prüfen, um virtuelle Instanzen von Unternehmensservern zu schützen.

SERVER UNGESCHÜTZT IM INTERNET

Durch Cloud-Computing kann ein Unternehmen die Anforderungen an den täglichen Betriebsablauf noch besser erfüllen. Je mehr Unternehmen die Vorteile des Cloud-Computings nutzen und je mehr Service-Provider öffentlich zugängliche Cloud-Umgebungen einrichten, desto stärker ist das Sicherheitsmodell gefordert, diese virtualisierten Aufgaben wirksam zu verwalten. Wenn es um die Verlagerung ihrer Geschäftsabläufe in das öffentlich zugängliche Internet geht, lässt die Frage nach der Sicherheit viele Unternehmen zögern. So hat IDC eine Umfrage unter 244 IT-Verantwortlichen/CIOs und ihren Branchenkollegen durchgeführt, um zu erfahren, wie sie zu Cloud-Computing stehen und wie es im Unternehmen genutzt wird. Das Ergebnis: Sicherheit wird als die größte Herausforderung beim Cloud-Computing angesehen.

Wenn ein Server auf eine öffentlich zugängliche Internet-Ressource verlagert wird, bietet das Datenzentrum keinen Schutz, da diese virtualisierten Server jetzt den administrativen Zugriff direkt über das Internet ermöglichen. Probleme, die bereits bei Datenzentren bestanden, wie die Patch-Verwaltung und die Berichterstattung zur Richtlinieneinhaltung, werden demzufolge entsprechend komplexer. Der einzig relevante Schutz im Internet, den der Anbieter in seiner Netzwerkumgebung bieten kann, oder jede andere Art von Schutz, mit der ein Unternehmen seine virtuelle Maschine ausstatten kann, ist der der kleinsten gemeinsam genutzten Ressource, da sie auf Servern zusammen mit den Ressourcen anderer Unternehmen gehostet wird.



„Der mit Abstand wichtigste Aspekt beim Cloud-Computing ist die Sicherheit. Wenn sich ihre Unternehmensdaten und wichtigen IT-Ressourcen außerhalb der Firewall befinden, befürchten Kunden, Angriffen schutzlos ausgeliefert zu sein."

Frank Gens, Senior Vice President and Chief Analyst, IDC

II. ÜBERBLICK: TREND MICRO DEEP SECURITY

Die Lösung Trend Micro Deep Security ist eine Software zum Schutz von Servern und Anwendungen, die Sicherheit für virtuelle, webbasierte und herkömmliche Datenzentren vereint. Mit Deep Security können Unternehmen Datendiebstahl verhindern, Betriebsabläufe stabilisieren, wichtige Richtlinien und Standards, wie PCI, einhalten und Betriebskosten reduzieren, was während der aktuellen Wirtschaftskrise einen entscheidenden Faktor darstellt. Mit der Lösung können sich Systeme selbst verteidigen, ihre vertraulichen Daten werden optimal geschützt, und die Verfügbarkeit von Anwendungen wird sichergestellt. Deep Security bietet umfassenden Schutz mit folgenden Komponenten:

- Deep Packet Inspection wird zur Erkennung und Abwehr von Eindringlingen (IDS/IPS), zum Schutz von Webanwendungen und zur Anwendungssteuerung verwendet.
- Stateful-Firewall
- Integritätsüberwachung für Dateien und System
- Protokollprüfung

III. UMFASSENDE, LEICHT VERWALTBARE SICHERHEIT

Die Deep Security Lösung nutzt Module, um wichtige Sicherheitsanforderungen für Server und Anwendungen zu erfüllen:

	Deep Security Module					
Anforderungen an das Datenzentrum	Deep Packet Inspection			Firewall	Integritäts-über-wachung	Protokoll-prüfung
	IDS/IPS	Schutz von Web anwen-dungen	An-wendungs-steuerung			
Serverschutz – Schutz vor bekannten Bedrohungen und Zero-Day-Angriffen – Schirmt Schwachstellen ab, bis Patches installiert sind	●			●	●	○
Schutz von Webanwendungen – Schützt vor Internet-Bedrohungen wie SQL-Injection, Cross-Site-Scripting und gewaltsamen Eindringversuchen – Erfüllt die Richtlinie PCI DSS 6.5: Firewall für Webanwendungen	●	●			○	●
Virtualisierungssicherheit – Schützt vor bekannten Bedrohungen und Zero-Day-Angriffen – Schirmt Schwachstellen ab, bis Patches installiert sind – VMware vCenter Integration verbessert Transparenz und Verwaltung	●	○		●	●	○
Erkennung verdächtigen Verhaltens – Schützt vor Ausspäh-Angriffen – Erkennt zulässige Protokolle auf ungeeigneten Ports – Warnt bei Betriebssystem- und Anwendungsfehlern, die auf einen Angriff hindeuten können – Warnt bei wichtigen Betriebssystem- und Anwendungsänderungen	○		●	●	●	●
Webbasierte Sicherheit – Verwendet Firewall-Richtlinien, um virtuelle Maschinen zu isolieren – Schützt vor bekannten Bedrohungen und Zero-Day-Angriffen – Schirmt Schwachstellen ab, bis Patches installiert sind	●	○		●	●	●
Berichte zur Einhaltung von Richtlinien – Bietet Transparenz und Prüfkette für alle Änderungen an wichtigen Servern – Prüfung, Abgleich und Weiterleitung wichtiger Sicherheits-ereignisse an Protokollserver zur Bedrohungsbewältigung, Berichterstattung und Archivierung – Erstellt Berichte zu Konfigurationen sowie zu erkannten und verhinderten Aktivitäten	○	●	○	○	●	●

● = unerlässlich ○= von Vorteil

IV. VORTEILE

Server-Sicherheitslösungen in Datenzentren müssen die Voraussetzungen für sich wandelnde IT-Architekturen schaffen, wie z. B. durch Virtualisierung und Konsolidierung, neue Service-Bereitstellungsmodelle und Cloud-Computing. Die Deep Security Lösung bietet für all diese Architekturmodelle folgende Vorteile:

- verhindert Datendiebstahl und Unterbrechungen im Geschäftsablauf
  - errichtet eine Verteidigungslinie direkt am physischen, virtuellen oder webbasierten Server
  - schützt bekannte und unbekannte Schwachstellen in Unternehmens- und Webanwendungen sowie in Betriebssystemen und wehrt Angriffe auf diese Systeme ab
  - ermöglicht Unternehmen, verdächtige Aktivitäten und Verhaltensweisen zu erkennen und vorbeugende Maßnahmen zu ergreifen

- ermöglicht die Einhaltung von Richtlinien
  - erfüllt die sechs wichtigsten Anforderungen für die PCI-Richtlinieneinhaltung, einschließlich Sicherheit auf Webanwendungsebene, Integritätsüberwachung von Dateien und Sammlung von Serverprotokollen, zusammen mit einer Reihe weiterer Anforderungen für die Richtlinieneinhaltung
  - liefert detaillierte, prüffähige Berichte, die verhinderte Angriffe dokumentieren und den Status der Regeleinhaltung anzeigen, um die erforderliche Vorbereitungszeit für die Unterstützung von Audits zu reduzieren
- reduziert Betriebskosten
  - bietet Schutz vor Schwachstellen, so dass Prioritäten bei der Programmierung sicherer Codes gesetzt und ungeplante Patches kosteneffizienter implementiert werden können
  - bietet Unternehmen die erforderliche Sicherheit, um die Kostensenkung durch Virtualisierung oder Cloud-Computing wirksam zu nutzen
  - schützt umfassend durch einen zentral verwalteten Software-Agenten und vermeidet die Notwendigkeit und die Kosten für die Verteilung mehrerer Software-Clients

V. MODULE UND FUNKTIONALITÄT

Die Deep Security Lösung ermöglicht es Ihnen, eines oder mehrere Schutzmodule zu installieren und so genau die richtige Menge an Schutz einzusetzen, um flexibel auf sich verändernde Unternehmensanforderungen zu reagieren. Sie können sich selbst verteidigende Server und virtuelle Maschinen erstellen, indem Sie umfassenden Schutz installieren, oder mit dem Modul zur Integritätsüberwachung beginnen, um verdächtiges Verhalten aufzudecken. Die Installation aller modularen Funktionen auf den Servern oder virtuellen Maschinen erfolgt über einen einzigen Deep Security Agenten, der zentral über die Deep Security Manager Software verwaltet wird und die Sicherheit in physischen, virtuellen und webbasierten Umgebungen vereinheitlicht.

DEEP-PACKET-INSPECTION-ENGINE (DPI)

Ermöglicht Erkennung und Abwehr von Eindringlingen, Schutz von Webanwendungen und Anwendungssteuerung

Die leistungsstarke Deep-Packet-Inspection-Engine untersucht den gesamten ein- und ausgehenden Verkehr, einschließlich SSL-Daten, auf Protokollabweichungen, Richtlinienverletzungen und Inhalte, die auf einen Angriff deuten. Sie kann im Erkennungs- oder im Abwehrmodus betrieben werden, um Betriebssysteme und Schwachstellen in Enterprise-Anwendungen zu schützen. Sie schützt Webanwendungen vor SQL-Injection, Cross-Site-Scripting und anderen Angriffen auf die Anwendungsschicht. Detaillierte Ereignisse geben wertvolle Informationen über Art, Datum/Uhrzeit und Ziel des Angriffs. Administratoren können bei einem Vorfall automatisch durch Warnmeldungen benachrichtigt werden. DPI wird zur Erkennung und Abwehr von Eindringlingen, zum Schutz von Webanwendungen und zur Anwendungssteuerung verwendet.

ERKENNUNG UND ABWEHR VON EINDRINGLINGEN (IDS/IPS)

Schirmt Schwachstellen in Betriebssystemen und Enterprise-Anwendungen ab, bis entsprechende Patches zur Verfügung stehen, und bietet dadurch einen zeitnahen Schutz vor bekannten Bedrohungen und Zero-Day-Angriffen

Regeln für Sicherheitslücken schützen bekannte Schwachstellen, beispielsweise solche, die am Microsoft Patch-Dienstag veröffentlicht werden, vor einer unbegrenzten Anzahl von Angriffen. Die Deep Security Lösung bietet sofortigen Schutz von Sicherheitslücken für über 100 Anwendungen, einschließlich Datenbank-, Web-, E-Mail- und FTP-Server. Regeln, die neu erkannte Sicherheitslücken abschirmen, werden automatisch innerhalb weniger Stunden bereitgestellt und können ohne Neustart in Minuten auf Tausende von Servern verteilt werden.

- Intelligente Regeln entdecken ungewöhnliche Protokolldaten mit bösartigem Code und schützen so vor Zero-Day-Angriffen von unbekannten Exploits, die eine noch nicht veröffentlichte Schwachstelle angreifen.
- Angriffsregeln stoppen bekannte Angriffe und Malware und verwenden ähnlich wie herkömmliche Antiviren-Software Signaturen, um einzelne, bekannte Angriffe zu erkennen und abzuwehren.

Als Gründungsmitglied des Microsoft Active Protections Program (MAPP) empfängt Deep Security Schwachstelleninformationen von Microsoft bereits vor der monatlichen Veröffentlichung der Security Bulletins. Durch diese Vorankündigung können neue Bedrohungen frühzeitig erkannt werden und gemeinsame Kunden mit schnellerem Schutz über Sicherheitspatches wirksam und effizient versorgt werden.

SCHUTZ VON WEBANWENDUNGEN

Die Deep Security Lösung ermöglicht die Einhaltung der Richtlinie PCI 6.6 zum Schutz von Web-anwendungen und der von ihnen verarbeiteten Daten. Regeln zum Schutz von Webanwendungen schützen vor SQL-Injection-Angriffen, Cross-Site-Scripting und anderen Schwachstellen in Web-anwendungen. Sie schirmen diese Schwachstellen ab, bis der Code vollständig repariert ist. Die Lösung verwendet intelligente Regeln, um typische Angriffe auf Webanwendungen zu erkennen und abzuwehren. Ein SaaS-Datenzentrum konnte mit Deep Security 99 % aller schwer wiegenden Schwachstellen abschirmen, die in den Webanwendungen und Servern im Rahmen eines auf Kundenwunsch durchgeführten Penetrationstests entdeckt wurden.

ANWENDUNGSSTEUERUNG

Regeln zur Anwendungssteuerung verbessern den Überblick und die Kontrolle über Anwendungen, die auf das Netzwerk zugreifen. Diese Regeln können auch zur Erkennung bösartiger Software, die auf das Netzwerk zugreift, oder zur Reduzierung von Schwachstellen auf den Servern verwendet werden.

FIREWALL

Verringert die Angriffsfläche Ihrer physischen und virtuellen Server

Das Deep Security Firewall-Software-Modul ist eine bidirektionale Stateful-Firewall auf Enterprise-Ebene. Das Modul ermöglicht die Kommunikation zwischen Ports und Protokollen, die für den ordnungsgemäßen Serverbetrieb erforderlich sind, und sperrt alle anderen Ports und Protokolle, um das Risiko eines unbefugten Zugriffs auf den Server zu senken. Funktionen:

- Isolierung virtueller Maschinen: ermöglicht die Isolierung virtueller Maschinen in webbasierten und mandantenfähigen Umgebungen, bietet dadurch virtuelle Segmentierung, ohne Konfigurationen für virtuelle Switches zu ändern.
- Hochpräzise Filter: Verkehr wird mit Firewall-Regeln zu folgenden Kriterien gefiltert: IP-Adressen, MAC-Adressen, Ports und mehr. Es können unterschiedliche Richtlinien für jede Netzwerkschnittstelle konfiguriert werden.
- Unterstützung aller IP-basierten Protokolle: Die Unterstützung von Full-Packet-Erfassung vereinfacht die Fehlerbehebung und bietet wertvolle Einblicke zum besseren Verständnis ausgelöster Firewall-Ereignisse: TCP, UDP, ICMP und mehr.
- Erkennung von Ausspäh-Angriffen: entdeckt Aktivitäten wie Port-Scans; auch nicht IP-basierter Datenverkehr, wie z. B. ARP-Verkehr, kann eingeschränkt werden.
- Flexible Steuerung: Die Stateful-Firewall ist flexibel und ermöglicht bei Bedarf in kontrollierter Weise eine vollständige Umgehung der Überprüfung. Die Firewall überprüft mehrdeutige Verkehrsmerkmale, die in jedem Netzwerk unter normalen Bedingungen oder als Teil eines Angriffs auftreten können.
- Vordefinierte Firewall-Richtlinien: Gängige Enterprise-Server-Typen, darunter Web, LDAP, DHCP, FTP und Datenbank, werden gruppiert, um auch in großen, komplexen Netzwerken eine schnelle, einfache und einheitliche Installation der Firewall-Richtlinie zu gewährleisten.
- Aktionsberichte: Durch detaillierte Protokolle, Warnungen, Dashboards und flexible Berichterstattung erfasst und verfolgt die Deep Security Firewall Konfigurationsänderungen. Hierzu zählen zum Beispiel Richtlinienänderungen und die Personen, die die Änderungen durchgeführt haben. Die Firewall bietet damit eine ausführliche Prüfkette.

INTEGRITÄTSÜBERWACHUNG

Überwachung unbefugter, unerwarteter oder verdächtiger Änderungen

Das Deep Security Software-Modul zur Integritätsüberwachung beobachtet wichtige Betriebssystem- und Anwendungsdateien, wie Verzeichnisse, Registrierungsschlüssel und -werte, um verdächtiges Verhalten aufzudecken. Funktionen:

- Erkennung nach Bedarf oder Zeitplan: Integritätsprüfungen können nach Bedarf oder Zeitplan ausgeführt werden.
- Umfassende Prüfung der Dateieigenschaften: Dateien und Verzeichnisse können anhand folgender Kriterien auf Änderungen überprüft werden: Inhalte, Attribute, z. B. Eigentümer, Berechtigungen und Größe sowie Zeit- und Datumsstempel unter Verwendung direkt verwendbarer Integritätsregeln. Außerdem kann überwacht werden, ob Windows Registrierungsschlüssel und -werte, Zugriffskontrolllisten und Protokolldateien verändert oder gelöscht werden. Gegebenenfalls wird ein Alarm ausgelöst. Diese Funktion gilt für die Richtlinie PCI DSS 10.5.5.
- Prüffähige Berichte: Das Modul zur Integritätsüberwachung kann Integritätsvorfälle im Deep Security Manager Dashboard anzeigen, Alarme auslösen und prüffähige Berichte bereitstellen. Außerdem können Ereignisse über Syslog an ein System für Sicherheitsinformationen und Ereignisverwaltung (SIEM) weitergeleitet werden.
- Gruppierungen von Sicherheitsprofilen: Regeln zur Integritätsüberwachung können für Gruppen oder einzelne Server konfiguriert werden, um die Installation und Verwaltung von Überwachungsregeln zu vereinfachen.

- Grundlegende Einstellung: Es können grundlegende Sicherheitsprofile eingerichtet und verwendet werden, um Änderungen zu vergleichen, Alarme auszulösen und entsprechende Aktionen zu bestimmen.
- Flexible, praktische Überwachung: Das Modul zur Integritätsüberwachung bietet die notwendige Flexibilität und Kontrolle, um die Überwachungsaktivitäten optimal an Ihre individuelle Umgebung anzupassen. Hierzu zählt die Möglichkeit, Dateien oder Platzhalter und Unterverzeichnisse in Suchparametern ein- bzw. auszuschließen. Außerdem können benutzerdefinierte Regeln für individuelle Anforderungen erstellt werden.

PROTOKOLLPRÜFUNG

Ermöglicht es, in Protokollen nach wichtigen, sicherheitskritischen Ereignissen zu suchen und sich diese zunutze zu machen

Das Deep Security Software-Modul zur Protokollprüfung ermöglicht die Sammlung und Analyse von Sicherheitsereignissen in Betriebssystem- und Anwendungsprotokollen. Regeln zur Protokollprüfung optimieren die Erkennung wichtiger, sicherheitsrelevanter Ereignisse, die sich in mehrfachen Protokolleinträgen verbergen. Diese Ereignisse werden zum Abgleich, zur Berichterstattung und zum Archivieren an ein System für Sicherheitsinformationen und Ereignisverwaltung (SIEM) oder an zentrale Protokollserver weitergeleitet. Außerdem leitet der Deep Security Agent die Ereignisinformationen an den Deep Security Manager weiter. Einige Vorteile des Moduls zur Protokollprüfung:

- Erkennung verdächtigen Verhaltens: Das Modul bietet Einblicke in verdächtiges Verhalten, das möglicherweise auf Ihren Servern auftritt.
- Erfassung von Ereignissen in Ihrer Umgebung: Das Deep Security Modul zur Protokollprüfung kann Ereignisdaten erfassen und miteinander in Beziehung setzen: Ereignisse auf Microsoft Windows, Linux und Solaris Plattformen; Anwendungsereignisse von Webservern, Mail-Servern, SSHD, Samba, Microsoft FTP und mehr; sowie benutzerdefinierte Anwendungsprotokollereignisse.
- Unterschiedliche Ereignisse miteinander in Beziehung setzen: unterschiedliche Warnungen, Fehler und informative Ereignisse erfassen und miteinander in Beziehung setzen. Hierzu zählen Systemmeldungen, beispielsweise bei voller Festplatte, Kommunikationsfehlern, Service-Ereignissen, Herunterfahren und Aktualisieren des Systems (also Anwendungsereignisse), wie z. B. An- oder Abmeldefehler bzw. -sperrungen, Anwendungs- und Kommunikationsfehler, sowie administrative Aktionen, wie z. B. administrative An- und Abmeldefehler bzw. -sperrungen, Richtlinienänderungen und Kontoänderungen.
- Prüffähige Berichte für die Regeleinhaltung: Es kann eine vollständige Prüfkette von Sicherheitsereignissen erstellt werden, um Anforderungen an die Regeleinhaltung, wie PCI 10.6, zu erfüllen.

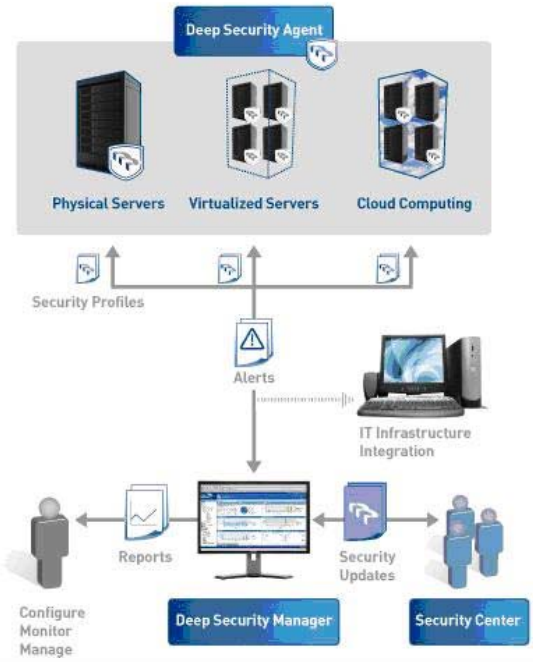
VI. ARCHITEKTUR DER DEEP SECURITY LÖSUNG

Die Architektur der Deep Security Lösung umfasst drei Komponenten:

- Der Deep Security Agent, der auf dem geschützten Server oder der virtuellen Maschine installiert wird.
- Der Deep Security Manager, der zentrale Richtlinienverwaltung, Verteilung von Sicherheitsupdates und die Überwachung durch Warnungen und Berichte bietet.
- Das Security Center: ein gehostetes Portal, auf dem ein dediziertes Team für die Schwachstellenforschung an der Entwicklung von Regel-Updates zum Schutz vor neuen Bedrohungen arbeitet, die regelmäßig vom Deep Security Manager abgerufen werden.

FUNKTIONSWEISE

Der Deep Security Agent empfängt eine Sicherheitskonfiguration – für gewöhnlich ein Sicherheitsprofil – vom Deep Security Manager. Diese Sicherheitskonfiguration umfasst die Regeln von Deep Packet Inspection, Firewall, Integritäts-überwachung und Protokollprüfung, die auf dem Server durchgesetzt werden. Die Regeln, die einem Server zugewiesen werden, können einfach durch Ausführung einer Empfehlungssuche bestimmt werden. Dabei wird die auf dem Server installierte Software ermittelt und empfohlen, welche Regeln zum Schutz des Servers erforderlich sind. Es werden Ereignisse für alle Aktivitäten erstellt, die Regeln überwachen. Diese werden an den Deep Security Manager und optional an ein SIEM-System gesendet. Die gesamte Kommunikation zwischen Deep Security Agents und dem Deep Security Manager wird durch gegenseitig authentifiziertes SSL geschützt.



Der Deep Security Manager initiiert eine Abfrage des Security Centers, um zu bestimmen, ob ein neues Sicherheitsupdate verfügbar ist. Ist dies der Fall, wird das Update vom Deep Security Manager abgerufen und entweder manuell oder automatisch auf den Servern installiert, die den zusätzlichen Schutz des Updates erfordern. Außerdem wird die Kommunikation zwischen dem Deep Security Manager und dem Security Center durch gegenseitig authentifiziertes SSL geschützt. Der Deep Security Manager stellt auch eine Verbindung zu anderen Elementen der IT-Infrastruktur her, um die Verwaltung zu vereinfachen. Der Deep Security Manager kann sich mit dem VMware vCenter sowie mit Verzeichnissen wie Microsoft Active Directory verbinden, um Informationen über Serverkonfiguration und -gruppierung zu erhalten. Außerdem verfügt der Deep Security Manager über eine API für Webservices, um programmgesteuert auf Funktionen zuzugreifen.

Das Security Center überwacht sowohl öffentliche als auch private Quellen mit Schwachstellendaten, um die von Kunden verwendeten Betriebssysteme und Anwendungen zu schützen.

DEEP SECURITY MANAGER

Die Deep Security Lösung bietet praktische, bewährte Steuerelemente, die zur Behebung schwieriger Sicherheitsprobleme beitragen. Operative und verwertbare Sicherheit stellt Ihrem Unternehmen profundes Wissen, nicht nur Informationen, über einen Sicherheitsvorfall zur Verfügung. Häufig geht es hier um Informationen zu „wer“, „was“, „wann“ und „wo“, damit Ereignisse korrekt interpretiert und entsprechende Maßnahmen eingeleitet werden können, die über die vom Sicherheitssteuerelement ausgeführten Aktionen hinausgehen. Die Deep Security Manager Software berücksichtigt über die folgenden Funktionen sowohl Sicherheits- als auch operative Anforderungen:

- Zentrales, webbasiertes Management-System: Über eine vertraute Benutzeroberfläche im Explorer-Stil werden Sicherheitsrichtlinien erstellt und verwaltet sowie vorbeugende Aktionen durchgeführt.
- Ausführliche Berichte: Eine Vielzahl detaillierter Berichte dokumentiert Angriffsversuche und bietet einen prüffähigen Verlauf von Sicherheitskonfigurationen und -änderungen.
- Empfehlungssuche: Die auf Servern und virtuellen Maschinen ausgeführten Anwendungen werden identifiziert und Filter für die entsprechenden Systeme empfohlen, um den geeigneten Schutz bei minimalem Aufwand sicherzustellen.
- Risikoeinstufung: Sicherheitsereignisse können basierend auf Vermögenswert und Schwachstelleninformationen angezeigt werden.
- Rollenbasierter Zugriff: Mehrere Administratoren mit jeweils unterschiedlichen Berechtigungen können unterschiedliche Aspekte des Systems betreiben und entsprechende Informationen erhalten.
- Anpassbares Dashboard: Administratoren können zu bestimmten Informationen navigieren und diese detailliert anzeigen, um Bedrohungen zu überwachen und entsprechende Gegenmaßnahmen einzuleiten. Es können mehrere individuelle Anzeigen erstellt und gespeichert werden.
- Zeitgesteuerte Aufgaben: Für Routine-Aufgaben, wie z. B. Berichte, Updates, Backups und Verzeichnissynchronisierung, können Zeitpläne zur automatischen Ausführung erstellt werden.

DEEP SECURITY AGENT

Der Deep Security Agent ist eine serverbasierte Software-Komponente der Deep Security Lösung, die IDS/IPS, den Schutz von Webanwendungen, Anwendungssteuerung, Firewall, Integritätsüberwachung und Protokollprüfung ermöglicht. Sie verteidigt Server und virtuelle Maschinen, indem sie den gesamten eingehenden und ausgehenden Verkehr auf Protokollabweichungen, Richtlinienverletzungen und Inhalte, die auf einen Angriff hindeuten, überwacht. Bei Bedarf greift der Deep Security Agent ein und schaltet die Bedrohung durch Sperrung des bösartigen Verkehrs aus.

SECURITY CENTER

Das Security Center ist eine zentraler Komponente der Deep Security Lösung. Es besteht aus einem dynamischen Team von Sicherheitsexperten, die Kunden darin unterstützen, den neuesten Bedrohungen immer einen Schritt voraus zu sein. Das Team reagiert schnell auf eine Vielzahl neuer Schwachstellen und Bedrohungen, sobald diese entdeckt werden, und stellt ein Kundenportal für den Zugriff auf Sicherheitsupdates und -daten bereit. Security Center Experten wenden einen strengen, aus sechs Schritten bestehenden Reaktionsablauf an, der durch hoch entwickelte und automatische Tools unterstützt wird:

- Überwachen: Über 100 Quellen öffentlicher, privater und behördlicher Daten werden systematisch und kontinuierlich überwacht, um neue, relevante Bedrohungen und Schwachstellen zu erkennen und miteinander in Beziehung zu setzen. Die Security Center Experten nutzen Beziehungen zu unterschiedlichen Organisationen, um frühzeitige und manchmal noch unveröffentlichte Informationen über Schwachstellen zu erhalten und Kunden dadurch einen zeitnahen und präzisen Schutz zu bieten. Zu diesen Quellen zählen Microsoft, Oracle und andere Händler beratende Stellen, SANS, CERT, Bugtraq, VulnWatch, PacketStorm und Securiteam.
- Prioritäten festlegen: Die Schwachstellen werden dann zur weiteren Analyse nach Priorität geordnet. Hierbei sind die Bewertung des Risikos für den Kunden und SLAs ausschlaggebend.
- Analysieren: Es wird eine tief greifende Analyse der Schwachstellen durchgeführt, um den notwendigen Schutz zu ermitteln.
- Entwickeln und testen: Es werden Software-Filter für die Abschirmung von Schwachstellen und Regeln mit Filterempfehlungen entwickelt und ausführlich getestet, um Fehlalarme zu minimieren und sicherzustellen, dass Kunden die Filter und Regeln schnell und reibungslos installieren können.
- Bereitstellen: Die neuen Filter werden als Sicherheitsupdates für Kunden bereitgestellt. Kunden erhalten bei der Veröffentlichung eines neuen Sicherheitsupdates sofort eine Benachrichtigung über den Deep Security Manager. Diese Filter können dann automatisch oder manuell für die entsprechenden Server übernommen werden.
- Kommunizieren: Die laufende Kommunikation mit Kunden erfolgt über Sicherheitsratschläge, die ausführliche Beschreibungen neu entdeckter Sicherheitsschwachstellen bieten.

PROAKTIVE FORSCHUNG VERSTÄRKT DEN SCHUTZ

Zusätzlich forscht das Security Center Team kontinuierlich weiter, um den gesamten Schutzmechanismus zu verbessern. Diese Arbeit wird durch die Ergebnisse und Entwicklungen stark beeinflusst, die während des Reaktionsprozesses bei der Erkennung neuer Schwachstellen und Bedrohungen erfasst werden. Diese Ergebnisse wirken sich auch auf die Erstellung neuer Filter und Regeln sowie auf die Qualität bestehender Schutzmechanismen aus und verbessern so schließlich die gesamte Sicherheitslösung.

SCHUTZ FÜR EINE VIELZAHL VON SCHWACHSTELLEN

Das Security Center entwickelt und liefert Filter, um kommerzielle Anwendungen „von der Stange“ wie auch benutzerdefinierte Webanwendungen zu schützen. Angriffs- und Schwachstellenfilter sind reaktiv, da sie auf entdeckte Schwachstellen reagieren. Intelligente Filter dagegen bieten proaktiven Schutz. Filter der Integritätsüberwachung überprüfen verschiedene Systemkomponenten sowie ihre Eigenschaften und warnen den Administrator, wenn bestimmte Auslösebedingungen erfüllt sind. Einige der zu überwachenden Komponenten sind Systemverzeichnisse, Dateien, die Windows Registrierung, Benutzerkonten, Ports und Netzwerkfreigaben. Protokollprüfungsfilter analysieren Protokolle von

Betriebssystemen und Drittanbieteranwendungen. Bei Auftreten bestimmter Ereignisse warnen sie den Administrator.

DAS SECURITY CENTER PORTAL

Das Security Center Portal bietet Kunden über einen zentralen, sicheren Zugriffspunkt produktbezogene Informationen und Unterstützung:

- Sicherheitsupdates
- Sicherheitshinweise
- CVSS-Bewertungsinformationen über Schwachstellen
- Alarmzusammenfassungen für den Microsoft Patch-Dienstag
- Erweiterte Schwachstellensuche
- Vollständige Offenlegung von Schwachstellen, einschließlich der, die nicht durch Third Brigade geschützt werden
- Patch-Daten für jede Schwachstelle
- RSS-Feeds
- Problem-Tickets
- Software-Downloads
- Produktdokumentation

VII. INSTALLATION UND INTEGRATION

Die Deep Security Lösung wurde so konzipiert, dass sie sich in großen Unternehmen schnell installieren lässt. Sie ermöglicht die wirksame Nutzung von und Integration in bestehende Infrastrukturen und Investitionen, um die Effizienz der Betriebsabläufe zu steigern und die Betriebskosten zu senken.

- VMware Integration: Durch die enge Integration in VMware vCenter und ESX Server können Unternehmens- und Betriebsdaten von vCenter- und ESX-Knoten in den Deep Security Manager importiert und detaillierte Sicherheit auf die VMware-Infrastruktur eines Unternehmens angewendet werden.
- SIEM-Integration: Detaillierte Sicherheitsereignisse auf Server-Ebene werden über mehrere Integrationsmöglichkeiten in SIEM, einschließlich ArcSight, Intellitactics, NetIQ, RSA Envision, Q1Labs, LogLogic und anderen Systemen, zur Verfügung gestellt.
- Integration von Verzeichnissen: Integration von Verzeichnissen auf Enterprise-Ebene, einschließlich Microsoft Active Directory
- Konfigurierbare Verwaltungskommunikation: Die Kommunikation kann vom Deep Security Manager oder vom Deep Security Agent eingeleitet werden. Hierdurch sind nur wenig oder keine Firewall-Änderungen – die in der Regel in zentral verwalteten Systemen anfallen – erforderlich.
- Verteilung von Software: Die Agenten-Software kann einfach über den Standard-Software-Verteilungsmechanismus wie Microsoft SMS, Novel Zenworks und Altiris verteilt werden.
- Optimierte Filter: Erweiterte Funktionen zur Verarbeitung von Streaming Media, wie z. B. Internet Protocol Television (IPTV), um die Leistung zu maximieren.

VIII. WAS DEEP SECURITY VON ANDEREN LÖSUNGEN UNTERSCHEIDET

Trend Micro Server- und Anwendungsschutz erfüllt die schwierigen Anforderungen, die heute an dynamische Datenzentren in Bezug auf die Stabilisierung von Betriebsabläufen und Richtlinien-einhaltung gestellt werden. Wir bieten umfassenden Schutz, effizientere Betriebsabläufe, hervorragende Plattformunterstützung und engere Integration in bestehende Investitionen. Außerdem reagieren wir schneller auf die sich verändernden Kundenanforderungen. Die Deep Security Lösungen bieten Ihnen folgende Vorteile:

- Gründlicheren Schutz: einschließlich Stateful-Firewall, Erkennung und Abwehr von Eindringlingen, Firewall auf Anwendungsebene, Datei- und Systemintegritätsüberwachung und Protokollprüfung in einer einzigen Lösung.
- Effizientere Betriebsabläufe: Durch die schelle und weit reichende Installation und Automatisierung vieler zentraler Aufgaben, wie der Empfehlung geeigneter Schutzmaßnahmen für jeden Server, kann die Lösung effizienter und mit minimaler Beeinträchtigung vorhandener IT-Ressourcen verwaltet werden.
- Herausragende Plattformunterstützung: liefert volle Funktionalität für mehr Plattformen und unterstützt aktuelle Versionen dieser Plattformen schneller, damit Sie die neuesten Virtualisierungsplattformen und Betriebssystemversionen nutzen können, ohne auf Schutz verzichten zu müssen.
- Engere Integration: Eine engere Integration in IT-Infrastrukturen, einschließlich Verzeichnis- und Virtualisierungsplattformen, und andere branchenführende Sicherheitsinvestitionen wie SIEM, gewährleistet eine wirksame Installation im Unternehmen und kontinuierliche Anbieterflexibilität.

Weitere Informationen erhalten Sie telefonisch oder unter
http://de.trendmicro.com/de/home/enterprise/