PAESSLER
THE NETWORK MONITORING COMPANY

WHITEPAPER

Ist Ihre Sicherheit sicher?

Whitepaper

PRTG NETWORK MONITOR

Autor: Thomas Timmermann, Senior Manager Technical Marketing, Paessler AG

Erstveröffentlichung: Februar 2016

Inhalt

Einleitung

Viele heiße Trends in der IT entpuppen sich schon nach kurzer Zeit als Silvesterkracher: Ein lauter Knall, es leuchtet kurz und schon ist es wieder vorbei. Nicht so Sicherheit oder neudeutsch Security. Seit den Anfängen der Vernetzung ist Security eines der Top-IT-Themen, heute mehr denn je. So gaben 2015 bei einer Umfrage der Paessler AG 58% der befragten Administratoren IT-Sicherheit als eine ihrer zentralen Aufgaben und ständige Herausforderung an. Wo vor Jahren noch eine Firewall und ein Virenscanner ausreichten, um das Netzwerk eines mittelständischen Unternehmens und die darin kursierenden Daten zu schützen, greift heute eine Vielzahl unterschiedlicher Lösungen ineinander, um den ständig neuen Bedrohungen entgegenzuwirken. All diese Security-Tools können aber nur dann umfassende Sicherheit gewährleisten, wenn ihre Funktion sichergestellt ist und wenn der Überblick über alle Maßnahmen gewährleistet ist. Dazu bedarf es einer umfassenden Sicherheitsstrategie, die mögliche Gefahren identifiziert, passende Werkzeuge als vorbeugenden Schutz einrichtet und alles mit einer zentralen Lösung kontrolliert und abbildet.

Die größten Bedrohungen Ihrer IT

Viren und Trojaner sind heute nicht weniger gefährlich, nur weil sie schon seit den Anfängen des Internets existieren. Immer wieder schafft es neue Malware in die Schlagzeilen und durch die immer weiter voranschreitende Vernetzung von allem und jedem öffnen sich ständig neue Türen. Von daher haben Virenscanner, Firewall und Intrusion-Detection-Systeme nach wie vor ihre Berechtigung.

Bring Your Own Device (BYOD) oder Internet of Things (IoT) schaffen neue Einfallsmöglichkeiten für Malware. Wo früher ein einfaches Verbot von privaten Disketten, CDs oder USB-Sticks reichte, verbinden sich heute zahlreiche Geräte mit dem Netzwerk. Ein generelles Verbot ist in vielen Unternehmen weder praktikabel noch sinnvoll: Viele Mitarbeiter nutzen Smartphones, Tablets oder Laptops privat und beruflich und steigern so ihre Effizienz. Auch das IoT schafft neue Einfallstore, indem es zahlreiche Geräte ins Netz einbindet, die nicht zur eigentlichen IT gehören und deren Gefahrenpotenzial oft schwer abzuschätzen ist. Den damit verbundenen Risiken muss die IT schon im Vorfeld begegnen und den richtigen Kompromiss zwischen neuen Möglichkeiten und mehr Flexibilität auf der einen und notwendiger Sicherheit auf der anderen Seite finden.

Aber nicht nur bösartige Angreifer bedrohen Ihre Daten: Ausfälle oder falsch konfigurierte Geräte und Applikationen können ebenso zu Datenverlusten führen. Dabei geht es nicht darum, Schutzwälle zu errichten, sondern vielmehr muss ein Kontroll- und Frühwarnsystem errichtet werden, das ständig alle kritischen Komponenten kontrolliert und bei Fehlern umgehend Maßnahmen ergreift oder im besten Fall schon erste Anzeichen für drohende Probleme erkennt und warnt, bevor die Situation kritisch wird.

Neben systemimmanenten Gefahren bedrohen auch physikalische Katastrophen wie Brände, Überschwemmungen, Hitze oder Diebstahl die IT und dürfen bei einem umfassenden Sicherheitskonzept nicht außer Acht gelassen werden. Was nützt der beste Virenscanner, wenn das Rechenzentrum unter Wasser steht oder die Klimaanlage im Serverraum ausfällt und die Temperatur in kritische Bereiche steigt.

Für so gut wie jede Bedrohung gibt es das passende „Gegenmittel“. Virenscanner und Firewalls schützen vor Malware, Backup-Tools sichern Daten, Umgebungssensoren kontrollieren Luftfeuchtigkeit und Temperatur und Überwachungskameras haben unerwünschte Eindringlinge im Blick. Solange all diese Systeme zuverlässig arbeiten, ist Ihre IT relativ sicher. Wie aber stellen Sie sicher, dass auch alles funktioniert? Und vor allem: Wie behalten Sie den Überblick über die Vielzahl von Systemen, die für die Sicherheit Ihrer IT unentbehrlich sind? Für ein umfassendes Sicherheitskonzept benötigen Sie eine Monitoring-Lösung als eine Art Meta-Security-Tool für die Kontrolle und Steuerung der einzelnen Maßnahmen.

Aufgaben der Monitoring-Lösung

Sind die Virusdefinitionen aktuell? Werden valide Backups erstellt. Ist die Firewall online? Nur wenn Security-Tools zuverlässig arbeiten, ist Sicherheit gewährleistet. Die Meta-Security-Lösung muss in der Lage sein, klassische Security-Tools entsprechend zu überwachen und ihr korrektes Funktionieren sicherzustellen. Aber was passiert, wenn ein Virus nicht erkannt wird oder ein Trojaner die Firewall umgeht? In dem Fall muss die Monitoring-Lösung ungewöhnliches Verhalten wie die starke Zunahme von Traffic, das schnelle Volllaufen von Speicher oder untypischen E-Mail-Verkehr erkennen und Sie entsprechend benachrichtigen.

Geeignete Monitoring-Lösungen überwachen kontinuierlich Funktion und Leistung aller Komponenten Ihrer IT-Infrastruktur, egal, ob es um Hardware, Software oder um Datenströme geht. So beugen Sie Datenverlusten vor und gewährleisten optimale Arbeitsbedingungen für Ihre Kollegen. Darüber hinaus muss die Monitoring-Lösung in der Lage sein, die Funktion von physischen Messfühlern ebenso zu überwachen wie von Videokameras und so sicherzustellen, dass alle Systeme arbeiten, um jenseits der IT-immanenten gefahren auch physikalische Risiken im Blick zu behalten und Sie gegebenenfalls zu benachrichtigen bzw. zu alarmieren.

Einen zentralen Aspekt eines umfassenden Sicherheitskonzepts bildet der Überblick. Nur wenn Sie jederzeit in der Lage sind, schnell und unkompliziert all Ihre Security-Tools einzusehen, ohne dass Sie jede Lösung einzeln aufrufen müssen, haben Sie eine reelle Chance, die gesamte Sicherheitslage ständig im Blick zu haben. Die Monitoring-Lösung muss dazu in der Lage sein, alle eingesetzten Tools einzubinden und ohne großen Aufwand in einer zentralen Übersicht abzubilden.

Nicht jedes Monitoring-Tool ist in der Lage, all diese Aufgaben zu erfüllen. Einige bringen nicht den erforderlichen Funktionsumfang mit, andere sind zu teuer, wieder andere zu komplex und aufwändig. Im Folgenden finden Sie eine Übersicht der Kriterien, die Sie bei der Evaluierung beachten sollten.

Evaluierungs-Checkliste

UMFASSENDE MONITORING-FEATURES PLUS API

Es ist wichtig, dass Ihr Kandidat alle Funktionen zum Monitoring der gesamten IT-Infrastruktur mitbringt und möglichst viele der gängigen Protokolle beherrscht, wie z.B. SNMP, Ping, FTP, http, NetFlow, sFlow, jFlow, WMI oder Packet Sniffing. Aber keine Monitoring-Lösung kann out-of-the-Box Ihre gesamte IT überwachen, dafür sind moderne Infrastrukturen viel zu komplex und heterogen. Mit einer gut dokumentierten API lassen sich fast alle Geräte und Applikationen anbinden – wie auch andere Security-Tools, Messfühler, Überwachungskameras etc. Wenn sich das mit Hilfe von Vorlagen und Beispielen einfach umsetzen lässt, dann haben Sie die geeignete Lösung schon fast gefunden.

„ALL INCLUSIVE“

Viele Monitoring- Systeme werden als Baukasten angeboten und erfordern für fast jede Funktion ein kostenpflichtiges Add-on. Das verursacht oft erhebliche Folgekosten. Achten Sie darauf, dass Ihr Monitoring-Kandidat schon in der Basisversion möglichst viele Optionen bietet und beziehen Sie möglicherweise später benötigte Module in Ihre Anfangskalkulation ein.

„UNUSUAL BEHAVIOR“

Natürlich müssen Sie bei Ihrer Monitoring-Lösung individuelle Grenzwerte für Benachrichtigungen und Alarme definieren können. Darüber hinaus sollte die Software aber auch intelligent genug sein, ungewöhnliches Verhalten auch dann zu erkennen, wenn die definierten Grenzwerte nicht erreicht werden. Fängt beispielsweise ein Virus an, erhöhten Datenverkehr in Ihrem Netzwerk zu produzieren, kann eine intelligente Lösung die untypische Zunahme erkennen und Sie entsprechend informieren, sodass Sie rechtzeitig Maßnahmen ergreifen können.

DATENSPEICHERUNG

Die meisten Monitoring-Lösungen nutzen SQL-Datenbanken für die Ablage der Überwachungsdaten. Nachdem SQL-Datenbanken nicht für das Speichern von Monitoring-Daten (viele kleine Datensätze, die chronologisch in kurzen Intervallen einlaufen, und auf die kein Schreibzugriff mehr erforderlich ist) konzipiert sind, können diese in der Regel die Daten nicht im RAW-Format speichern, sondern legen sie lediglich als komprimierte Durchschnittswerte ab. Das kann vor allem beim Einsatz einer Monitoring-Lösung als Security-Tool problematisch werden, wenn langfristige Recherche zum Identifizieren von Sicherheitslücken erforderlich wird.

PUBLIKATION VON DATEN

Monitoring-Daten werden auf unterschiedliche Weise publiziert:

- Als Live-Anzeige in Form von Dashboards oder Maps über unterschiedliche Oberflächen. Achten Sie darauf, dass die Lösung nicht nur ein Windows-GUI mitbringt, sondern zumindest noch ein Web-Interface und wenn möglich auch Apps für die gängigen Mobilsysteme. Die Dashboards und Maps sollten individuell einstellbar sein und eine Darstellung der Daten in möglichst übersichtlicher und attraktiver Form erlauben: Das Auge isst mit und hübsch aufbereitete Graphen werden mit mehr Genuss und damit Aufmerksamkeit wahrgenommen als altmodische und unansehnliche Tabellen und Listen.

- Als Reports, üblicherweise in HTML- oder PDF-Format. Diese Berichte können mit Bordmitteln oder über Third-Party-Tools realisiert werden, on-the-fly oder regelmäßig zu festgelegten Zeitpunkten. Reports bieten normalerweise die Option, die Daten eines definierten Zeitraums anzuzeigen. So lassen sich auch historische Daten abbilden und auswerten.

Idealerweise bietet die Lösung bordeigenes Reporting ebenso wie Möglichkeiten zum einfachen Erstellen individueller Dashboards und Maps. Sehr interessant ist hier die Option, individuelle HTML-Maps zu generieren, auf denen sämtliche Bausteine des Security-Konzepts übersichtlich dargestellt werden können. Evtl. mit einem Gebäudegrundriss als Hintergrund, auf dem physikalische Sensoren, Überwachungskameras und ähnliches positioniert werden können.

USABILITY

Selbst wenn eine neue Monitoring-Lösung als Meta-Security-Tool im Rahmen eines Projektes eingeführt und installiert wird: Ist die Lösung im täglichen Einsatz zu komplex, wird sie mit großer Wahrscheinlichkeit nicht hinreichend genutzt werden. Eine nicht genutzte Security-Software ist nicht nur eine sinnlose Investition, sie bildet auch ein Sicherheitsrisiko. Das Vorhandensein der Lösung gaukelt Sicherheit vor, die tatsächlich aber nicht gegeben ist. Deshalb sollte die einfache Bedienbarkeit der Software bei der Evaluierung ganz oben auf der Liste stehen. Unter Umständen macht es sogar Sinn, auf das eine oder andere zusätzliche Feature zu verzichten, wenn dafür Akzeptanz und Nutzung der Lösung gewährleistet sind.

PREIS UND LIZENZIERUNG

Natürlich spielen Preis und Lizenzgestaltung eine wesentliche Rolle beim Kauf einer Monitoring-Lösung. Wichtig ist hier vor allem Transparenz. Sind sämtliche Preise verfügbar? Ist die Lizenzierung nachvollziehbar? Falls Module und Add-ons angeboten werden, welche davon benötigen Sie von Beginn an oder in absehbarer Zeit? Oft gibt es versteckte Kostenfallen in Form von Modulen oder Sie müssen aufgrund schwer nachvollziehbarer Lizenzierungsmodelle schon nach kurzer Zeit auf größere Lizenzen upgraden.

TEST

Installieren und testen Sie die Software! Verlassen Sie sich nicht auf Feature-Listen, Consultants oder gar das Marketing des Herstellers. Eine Meta-Security-Lösung ist ein zentraler Baustein in einem umfassenden Sicherheitskonzept. Nur wenn sich die Software „gut anfühlt“ wird sie die nötige Akzeptanz finden, um ihrer Rolle gerecht werden zu können. Und wenn sich schon die Testversion als schwer erhältlich oder umständlich installierbar erweist, dann drohen mit der Vollversion ernste Probleme.

ÜBER PAESSLER AG

PRTG Network Monitor von Paessler ist eine preisgekrönte Lösung für leistungsfähiges, bezahlbares und benutzerfreundliches Unified Monitoring. Die flexible Software eignet sich ideal, um komplette IT-Infrastrukturen im Blick zu behalten. PRTG sorgt in Unternehmen und Organisationen aller Größen und Branchen für Ruhe und Sicherheit. Aktuell vertrauen über 150.000 IT-Administratoren in mehr als 170 Ländern auf die Software der Paessler AG. Das 1997 in Nürnberg gegründete Unternehmen wird bis heute privat geführt und ist sowohl Mitglied des Cisco Solution Partner Program als auch ein VMware Technology Alliance Partner.

Kostenlose Testversionen und weitere Informationen stehen unter www.paessler.de/prtg/download zur Verfügung.

Paessler AG
www.paessler.de, info@paessler.com