PAESSLER

WHITEPAPER

Netzwerk-Monitoring als unverzichtbarer Baustein im IT-Sicherheitskonzept

Whitepaper

PRTG NETWORK MONITOR

Autor: Daniel Zobel, Head of Software Development, Paessler AG
Erstveröffentlichung:Juli 2013

Inhalt

Einleitung 3

Aktuelle Situation 3

IT-Sicherheit in Deutschland 3

IT-Systeme schützen 3

Frühwarnsystem im Netzwerk 4

Security-Aspekte überwachen 5

Firewall und Virenscanner regelmäßig prüfen 5

Bandbreitenengpässe als Problemindikator 6

Physische Umgebungsparameter überwachen 6

Ergebnisse auswerten 7

Fazit 8

Einleitung

Einer Umfrage der Paessler AG zufolge möchten sich Firmen zukünftig besser gegen Cyber-Bedrohungen und andere Schäden schützen. Rund 1200 Anwender wurden zum Einsatz der Paessler-Software PRTG Network Monitor befragt. Das Resultat der Befragung zeigt, dass ca. 75 % von ihnen das Tool als wichtige Sicherheitskomponente für ihr Netzwerk ansehen. Dieses Whitepaper beleuchtet die Rolle, die Netzwerk-Monitoring als zusätzliche Security-Instanz im Unternehmensnetzwerk spielt, wo die Herausforderungen diesbezüglich liegen und wie diese gelöst werden können.

Aktuelle Situation

IT-SICHERHEIT IN DEUTSCHLAND

Studien zur IT-Sicherheit in Deutschland zeigen, dass Unternehmen im Hinblick auf ihre Schutzmaßnahmen Nachholbedarf haben. Hinzu kommt, dass Cyberkriminelle immer intelligentere digitale Schädlinge entwickeln, die sie auf verschiedenen Wegen freisetzen. Eine aktuelle Studie der IT-Sicherheitsinitiative „Deutschland sicher im Netz“ (DsiN) zeigt, dass mehr als die Hälfte von 1400 befragten mittelständischen Unternehmen in Deutschland keine Schutzmechanismen für ihre E-Mail-Systeme einsetzen. Das bietet Hackern & Co. eine breite Angriffsfläche. Außerdem sind 17 % der im Unternehmen genutzten Notebooks sowie 16 % der eingesetzten Smartphones nicht ausreichend abgesichert, wodurch die Erfolgschancen der Cyberkriminellen bei einem Angriff auf Unternehmenssysteme zusätzlich erhöht werden.

Im Hinblick auf das im September 2012 vom Bundeskriminalamt vorgestellte „Lagebild 2011“ im Bereich Internetkriminalität verwundern diese nur oberflächlichen Sicherheitsvorkehrungen. Denn demnach haben bereits 52 % der Online-Nutzer Erfahrungen mit „Cybercrime“ gemacht – so auch viele deutsche Unternehmen. Die durch Viren, Spionage, Phishing etc. entstandenen Schäden belaufen sich dem Bericht zufolge auf mindestens 71,2 Millionen Euro. Daher müssen Unternehmen dem Sicherheitsaspekt ihrer IT-Infrastruktur heute eine deutlich höhere Bedeutung beimessen.

IT-SYSTEME SCHÜTZEN

Viele Firmen gehen davon aus, dass ihre IT-Infrastruktur mit einer zuverlässig arbeitenden Firewall und einem aktuellen Virenscanner ausreichend geschützt ist. Cyberkriminelle entwickeln jedoch immer professionellere Methoden, um sich Zugriff auf Firmenrechner oder -server zu verschaffen. Freigesetzte Trojaner, Würmer etc. werden von Sicherheitsprogrammen manchmal erst dann erkannt, wenn es bereits zu spät ist. Denn sobald Schädlinge Zugang zu einem Rechner des Firmennetzwerks erlangen, ist es meist nur noch eine Frage der Zeit, bis sie das komplette System kompromittiert haben. Die Folge sind unter anderem Datenmanipulationen, -verluste oder die Übernahme von Rechenkapazität für kriminelle Zwecke. Sollten die firmeninternen Systeme durch den Malware-Befall gestört werden, kann weder die geschäftskritische Kommunikation zwischen verschiedenen Unternehmensstandorten noch die Auftragsabwicklung und Kundenkommunikation stattfinden. Der Administrator sieht sich mit einer zeitaufwendigen Suche nach den genauen Ursachen für die Störung des Unternehmenssystems konfrontiert. Welche Teile des Sicherheitssystems sind ausgefallen? Welche Bereiche oder Komponenten wurden mittels Malware angegriffen? Gibt es vielleicht auch andere Gründe für einen Ausfall einzelner Systeme?

Um solche Vorfälle zu vermeiden oder so unwahrscheinlich wie möglich zu machen, sollte die komplette IT-Infrastruktur geschützt sein. Dazu benötigen Unternehmen ein umfassendes IT-Sicherheitskonzept. Zu diesem Konzept zählen oftmals neben dem Virenscanner und der Firewall auch Verschlüsselungssoftware, Datensicherheitssoftware, Contentfilter, Portscanner und andere Tools. Doch um kompletten Netzwerkschutz zu gewährleisten, sollte bei der Planung und Umsetzung des Sicherheitskonzepts das Netzwerk-Monitoring als ergänzende Security-Instanz nicht fehlen. Der zielgerichtete Einsatz einer solchen Lösung kann den Sicherheitsgrad der IT-Umgebung wesentlich erhöhen.

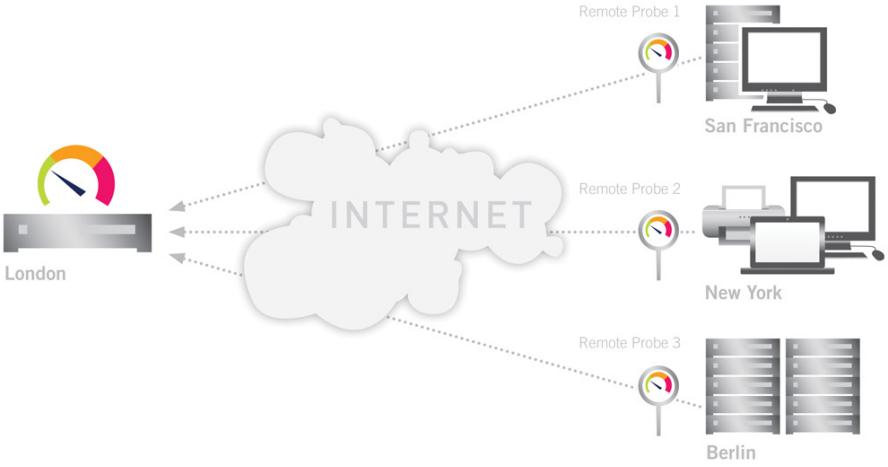
Frühwarnsystem im Netzwerk

Eine Netzwerk-Monitoring-Lösung dient grundsätzlich dazu, die gesamte IT-Infrastruktur mit allen Geräten und Systemen im Auge zu behalten. Prinzipiell können Administratoren alles überwachen, was über eine definierte Schnittstelle verfügt und via Standardprotokoll Informationen über den eigenen Zustand liefert. Die Monitoring-Software muss dazu lediglich über eine IP-Adresse mit dem Gerät oder Dienst Kontakt aufnehmen und kann dann den aktuellen Gerätezustand abfragen. So ist der IT-Verantwortliche in der Lage, den Status nahezu jedes beliebigen Bereiches seiner IT-Infrastruktur rund um die Uhr im Blick zu behalten. Das Ziel ist es, die maximale Verfügbarkeit und die optimale Performance im Netzwerk zu erreichen. Dafür muss das Netzwerk-Monitoring-System drei verschiedene sicherheitsrelevante Aspekte abdecken:

- die Überwachung der eigentlichen Sicherheitssysteme,
- die Identifizierung von ungewöhnlichen Vorkommnissen
- und das Überprüfen der Umgebungsparameter.

Unternehmen mit verschiedenen Standorten können ihr verteiltes Netzwerk durch den Einsatz von „Remote Probes“ effektiv in allen drei Kategorien an einer zentralen Stelle im Auge behalten. Eine „Probe“ ist ein kleines Softwareprogramm, welches ein entferntes Netzwerk von innen heraus überwacht und Monitoring-Daten zum zentralen Datenserver schickt. Eine geeignete Netzwerküberwachungs-Software monitort auf diese Weise beliebige Netzwerkkomponenten sowohl in der Zentrale als auch in den einzelnen Zweigstellen eines Unternehmens. Dazu werden sogenannte „Sensoren“ für die Überwachung der unterschiedlichen Parameter aller Netzwerkgeräte und -verbindungen konfiguriert. Von zentraler Stelle hat der Administrator so das gesamte Netzwerk im Blick.

ABBILDUNG:
Monitoring verschiedener Standorte mit Remote Probes



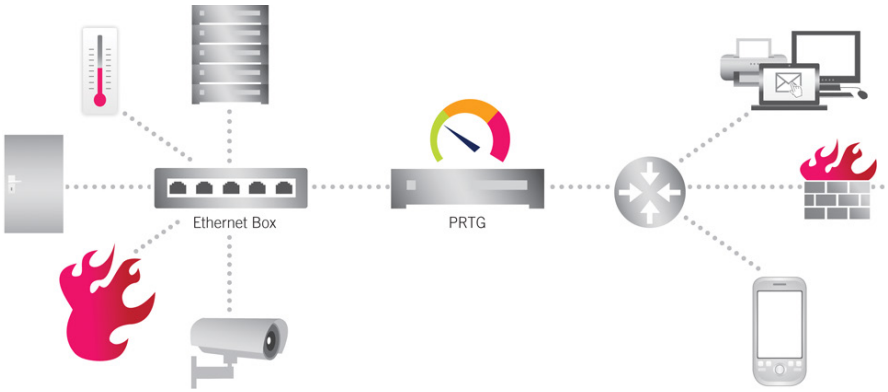
Stellt die Überwachungssoftware einen Ausfall oder ungewöhnliche Vorgänge fest, sendet sie umgehend per SMS oder E-Mail einen Alarm an den zuständigen Systemadministrator. So sind IT-Verantwortliche ortsunabhängig und aktuell immer über sämtliche Vorfälle informiert und können schnell reagieren.

Das Frühwarnsystem der Monitoring-Lösung basiert auf entsprechend definierten Schwellenwerten. Werden diese überschritten, schlägt die Software Alarm. Über das Web-Interface oder per Smartphone App hat der Administrator die Möglichkeit, permanent mit der Monitoring-Installation in Verbindung zu bleiben und Alarme sofort zu überprüfen. Er kann anhand der Live-Daten aus dem Monitoring direkt das Ausmaß der Störung abschätzen und geeignete Maßnahmen einleiten.

Security-Aspekte überwachen

So eine schnelle Reaktionsmöglichkeit wünschen sich IT-Verantwortliche auch bei potenziellen Malware-Angriffen. Entdecken installierte Antivirus-Lösungen und Firewalls Attacken zu spät, können die von den Schädlingen verursachten Auswirkungen den Betrieb bereits komplett lahmgelegt haben. Administratoren ist es dann nur noch möglich, auf das Problem zu reagieren anstatt vorbeugend tätig zu werden und es rechtzeitig zu beheben oder zu verhindern. Dies verdeutlicht, dass Firewall und Virenscanner allein nicht immer ausreichen, um eine „Rundum-Sicherheit“ des Netzwerks zu gewährleisten. Integrieren Unternehmen eine Network Monitoring-Lösung in ihr Sicherheitskonzept, können potenzielle Gefahren für das Firmennetz frühzeitig aufgedeckt werden.

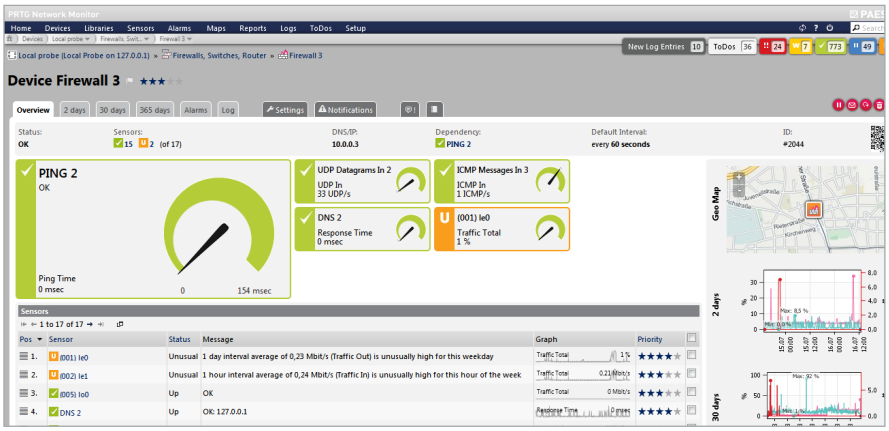
ABBILDUNG:
Die Rundum-Sicherheit des Netzwerks gewähren



FIREWALL UND VIRENSCANNER REGELMÄSSIG PRÜFEN

Eine wichtige Aufgabe der Netzwerk-Monitoring-Lösung ist es, bestehende Sicherheitssysteme wie z.B. Firewalls und Virenscanner auf ihre Funktionstüchtigkeit zu überprüfen. Dazu erfasst die Überwachungslösung z.B. rund um die Uhr detaillierte Daten zu Leistung und Zustand der Firewall. Funktioniert sie nicht ordnungsgemäß, erhöht sich das Risiko eines Malware-Befalls im Netzwerk. Diese „bösartigen“ Angriffe könnten zur Folge haben, dass die CPU auf einmal unkoordiniert Programme ausführt oder dass Ports offen sind, die nicht offen sein sollten. Damit es nicht dazu kommt, werden Administratoren frühzeitig über Auffälligkeiten bei der Firewall informiert.

ABBILDUNG:
Die Software überwacht den Zustand der Firewall



Neben der Firewall kann die Monitoring-Software beispielsweise auch den Virenscanner prüfen, der auf dem zentralen Mailserver läuft. Damit stellen Firmen sicher, dass dieser wirklich kontinuierlich aktiv ist. Mittels spezieller Sensoren prüft die Überwachungslösung auch das Windows Security Center und stellt dabei fest, ob z.B. die Virenscanner und Anti-Malware-Programme auf jedem Rechner innerhalb der Firma aktuell sind und einwandfrei laufen. Somit ist sichergestellt, dass auch die Client-Rechner der Unternehmens-IT jederzeit vor Malware geschützt sind.

BANDBREITENENGPÄSSE ALS PROBLEMINDIKATOR

Eine Netzwerk-Monitoring-Lösung hilft dem Administrator auch, Bandbreiten von Standleitungen, Netzwerkverbindungen oder -geräten (Routern, Switchen) etc. zu messen. Mit detaillierter Überwachung der Bandbreitennutzung können indirekt auch Malware-Attacken entdeckt werden. Anzeichen dafür sind beispielsweise langsame Antwortzeiten von Applikationen und Webseiten. Eine Ursache könnte ein Malware-Programm sein, das einen großen Anteil der Bandbreite für sich beansprucht. Um diese Unregelmäßigkeiten festzustellen, überwacht die Monitoring-Software verschiedene IP-Adressen, Port-Nummern, Protokolle etc. mittels Packet Sniffing oder via Flow-Sensoren. Diese xFlow-Sensoren sammeln die gesendeten Daten und schicken sie zur Auswertung an die Monitoring-Software. Der Administrator kann die Daten somit zeitnah analysieren, Probleme frühzeitig erkennen und weitere Schritte zur Behebung des Problems einleiten. Diese Art der Bandbreitenüberwachung eignet sich besonders für Netzwerke mit einem sehr hohen Datenverkehr. Überschreitet die Bandbreitennutzung festgelegte Schwellwerte oder weicht sie stark vom Durchschnitt und den üblichen Schwankungen ab, deutet das auf ungewöhnliche Einflüsse oder Aktivitäten hin – beispielsweise auf Malware-Angriffe. Der Administrator kann in diesem Fall mit seiner Monitoring-Software überprüfen, welche IP-Adresse, Verbindung oder welches Protokoll die meiste Bandbreite beansprucht, und entsprechend reagieren.

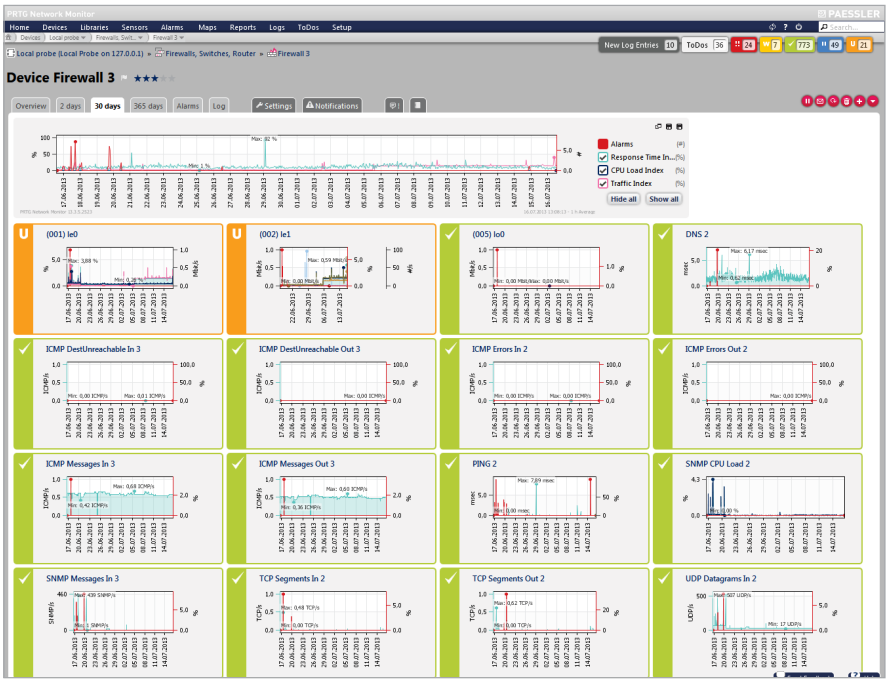
PHYSISCHE UMGEBUNGS-PARAMETER ÜBERWACHEN

Nicht zuletzt liefert das Monitoring einen Beitrag zur Gebäudesicherheit, da es auch die Überwachung von Umgebungs- und Umwelteinflüssen ermöglicht. Spezielle Geräte mit Sensoren für Rauch- und Gasentwicklung melden z.B. Brände oder ähnliche Vorfälle frühzeitig. Zudem können im Gebäude befindliche Schließsensoren so konfiguriert werden, dass sie einen Alarm senden, sobald Türen, Fenster oder Serverschränke unverschlossen sind. Darüber hinaus können IT-Verantwortliche mit entsprechender Hardware die Stromspannung messen und diese Werte an die Network Monitoring-Software übermitteln, die dann Schwankungen in der Stromversorgung identifiziert und den Administrator informiert. Aufgrund der vielen Überwachungsmöglichkeiten weiß das IT-Team jederzeit, ob sein Netzwerk in einer sicheren Umgebung läuft oder ob etwas kurz-, mittel- oder langfristig verändert werden muss.

Ergebnisse auswerten

Hochwertige Network Monitoring-Lösungen werten die gesamten Überwachungsdaten in Berichten aus und bereiten sie zusätzlich übersichtlich in Grafiken oder Dashboards auf. Die von der Software erstellten Reporte fassen die identifizierten Werte einzelner Komponenten und Systeme in einfach zu lesenden Berichten zusammen. Nicht nur Tätigkeiten von Firewall und Virenscanner werden dem Administrator als Report zugeschickt, er erhält auch Leistungsparameter wie die aktuelle CPU- und RAM-Auslastung aller Server und Computer. Zudem wird die Verfügbarkeit aller Netzwerkgeräte für den IT-Verantwortlichen ersichtlich. Darüber hinaus enthält der Report aussagekräftige Trends zur Netzwerk- und Bandbreitenauslastung. Falls nötig, kann der Administrator in verschiedenen Situationen Vergleiche von aktuellen und historischen Daten anstellen. Wenn aktuelle Werte schlechter als die historischen sind, zeigt dies einen eindeutigen Optimierungsbedarf an. Zusätzlich kann der Administrator mittels einer automatischen Analyse von Monitoring-Daten ähnliches Verhalten verschiedener Sensoren aufdecken und so bisher unbekannte Beziehungen zwischen einzelnen Netzwerkkomponenten identifizieren. Die Analyse der historischen Daten, genauso wie die Identifizierung von Sensoren mit ähnlichen Verhaltensmustern, sind besonders für Vergleichsstudien in komplexen Netzwerken hilfreich, um die genaue Auslastung und Art der Nutzung des Netzwerks zu erforschen und potenzielle Sicherheitslücken zu schließen.

ABBILDUNG:
Graphen helfen Monitoring-Ergebnisse auszuwerten



Fazit

Nur ein alle Bereiche umfassendes Security-Konzept bietet Unternehmen im Rahmen des Risiko-Managements eine entsprechende Sicherheit. Netzwerk-Monitoring fungiert hier als ein zusätzlicher, strategisch wichtiger Baustein im IT-Sicherheitskonzept. Dieses Konzept sollte über die Nutzung von Firewalls und Virenscannern hinausgehen. Denn um so sicher wie möglich zu sein, dass das gesamte Unternehmensnetzwerk effizient vor Malware-Attacken oder Ausfällen geschützt ist, müssen sämtliche IT-Bereiche überwacht werden. Dabei ist gerade auch das Erkennen von Trends und Entwicklungen ein wesentlicher Faktor, um sich anbahnende Bedrohungen aufzudecken. Eine Network Monitoring-Software übernimmt dabei die Aufgabe des Frühwarnsystems. Damit ist sie eine sinnvolle Erweiterung des Sicherheitskonzepts und hilft, die vom Unternehmen gewünschte Sicherheit und Kontrolle zu schaffen.

ÜBER DIE PAESSLER AG

Die Paessler AG ist seit Jahren führend in der Entwicklung von leistungsfähiger, bezahlbarer und benutzerfreundlicher Netzwerk-Monitoring-Software. Paessler Produkte sorgen für Ruhe und Sicherheit in IT-Abteilungen von Unternehmen aller Größen - von SOHOs über KMUs bis hin zu global tätigen Konzernen – umfassend, unkompliziert und zuverlässig. Vom Firmensitz in Nürnberg aus betreut Paessler über 150.000 Installationen seiner Produkte, die weltweit im Einsatz sind. Das 1997 gegründete Unternehmen ist bis heute privat geführt und sowohl Mitglied des Cisco Developer Networks als auch ein VMware Technology Alliance Partner.

Freeware und Testversionen aller Produkte können unter
www.de.paessler.com/prtg/download heruntergeladen werden.

Paessler AG
Bucher Straße 79a, 90419 Nürnberg, Deutschland
www.paessler.de, info@paessler.com

UST#: DE 217564187
Steuer#: FA Nürnberg 241/120/60894
Eintragung: Amtsgericht Nürnberg HRB 23757

Vorstand: Dirk Paessler, Christian Twardawa
Vors. d. Aufsichtsrats: Dr. Marc Rössel