LANline

9,– €

Dezember 2016
21. November

ITP VERLAG

IT ■ Network ■ Datacenter www.lanline.de

Netzwerk-Analyse/Monitoring

Visuelle Übersicht lokal und in der Cloud

SIEM- und Loganalysen

Effektive Bedrohungsbewertung

Mit Marktübersicht Monitoring-Tools/Protokollanalysatoren

Ausfallsicherheit für industrielle Netzwerke
Schutz und Transparenz der Kommunikation

VPT-Technik als VPN-Alternative
Saytrust Access im Praxistest

Das ene… Rech…
Mi…

Testserie Monitoring, Teil 5: Omnipeek

Profischnüffler

Standortübergreifende Datenfluss- und Anwendungskontrolle für das Unternehmensnetzwerk – das klingt nach einer Technik, die nur größeren Firmen vorbehalten ist. Doch das ist nicht der Fall, wie unser Blick auf Savvius Omnipeek 9.2 verriet.

Möglicherweise ist der langgediente Administrator verwundert: eine Paketanalyse-Software in der Version 9.2 von einem Anbieter, dessen Namen man noch nie gehört hat? Doch hinter Savvius steckt die 1990 gegründete Softwareschmiede Wildpackets aus Kalifornien, die sich lediglich 2015 umbenannte. Die Savvius-Software dient dazu, Administratoren den Zustand ihrer Netzwerke besser und vor allem standortübergreifend vor Augen zu führen. Kommunikations- oder Konfigurationsfehler sollen sich damit leichter identifizieren, Netzwerk- und Anwendungsprobleme bereits im Vorfeld erkennen lassen, so der Anbieter. Unsere Erwartung vor dem Test: Mit rund 20 Jahren Erfahrung und Entwicklungszeit müsste der Hersteller der ersten Netzwerkanalyse-Software mit grafischer Auswertung einem Open-Source-Konkurrenten wie Wireshark hoch überlegen sein.

Per Omnipeek-Dashboard haben Administratoren den Überblick über die Netzwerkauslastung.

Omnipeek ist eine reinrassige Windows-Lösung. Die Installation des knapp 750 MByte umfassenden Softwarepakets geht mit wenigen Klicks vonstatten. Bei der Einrichtung legt der Administrator fest, ob die Software in der x86- oder x64-Ausprägung auf das System kommt. Jedes halbwegs aktuelle Windows-System eignet sich für den Einsatz von Omnipeek. Will man es auf Windows 7/2008R2 nutzen, sind verschiedene System-Updates erforderlich, sonst bricht der Einrichtungsvorgang ab. Einen speziellen „Unterbau“ wie Winpcap benötigt die Lösung nicht, bringt sie doch ihre eigene Promiscuous-Mode-Treiber mit. Will der Administrator tiefergehende WLAN-Analysen durchführen, sind nur einige wenige WLAN-Adapter zulässig. Da die Hersteller die Chipsets häufig innerhalb einer Produktlinie ändern, empfiehlt sich die Anschaffung der eigens von Savvius vertriebenen WLAN-Adapter, die jedoch für den regulären Zugriff auf eine WLAN-Umgebung selbst ungeeignet sind.

Bereits beim Download bietet der Hersteller zwei Pakete zur Auswahl an: die reguläre Omnipeek-Software, getestet in Version 9.2, und die „Capture Engine for Savvius Omnipeek 9.2“. Diese Capture Engine ist der entscheidende Unterschied zu vielen anderen Lösungen aus dem Sniffer-Umfeld, da Omnipeek verteilte, standortübergreifende und permanente Netzwerkmitschnitte erlaubt. Der Omnipeek-Familie liegt somit eine klassische Konsolen- und Agentenarchitektur zugrunde.

In der Enterprise-Edition gehört der „Remote Assistant“ zur Lösung. Hier handelt es sich um ein eher kompakt gehaltenes Programm, das auch Personen ohne tiefgehendes IT-Administrationsverständnis bedienen können. Der Anwender muss es lediglich ausführen, ohne es installieren zu müssen, und dann die Aufzeichnung der Störung starten und stoppen. Dann verschickt er die erzeugte Datei zur Analyse an den zuständigen Kollegen. Diese Mitschnitte könnten vertrauliche Daten enthalten, daher sind sie verschlüsselt. Zudem können Administratoren nur Mitschnitte mit den passenden Seriennummern analysieren.

Einfacher Einstieg

Der erste Blick auf die Software offenbart nichts Außergewöhnliches: eine Menüleiste oben, eine Detailauswahl auf der linken Seite und ein Hauptarbeitsfenster, in dem der Benutzer die Informationsbereiche beliebig positionieren kann. Das Eingangsmenü bittet um die Auswahl des nächsten Arbeitsschrittes: Soll das Programm einen neuen Mitschnitt („Capture“) erzeugen oder als Datei öffnen? Möchte der Anwender auf entfernte Capture Engines zugreifen oder ein einfaches Monitoring aktivieren? Sofern der Benutzer sich bereits Templates angelegt hat, kann er sie nun auswählen. Erwartungsgemäß suchen Administratoren selten im kompletten vorbeieilenden Datenstrom – die Datenmenge wäre zu groß. In Templates fasst der IT-Profi deshalb gewünschte Bereiche oder Protokolle zusammen. Dies ist zum Glück sehr einfach und im 644-seitigen, englischsprachigen „User Guide“ detailliert beschrieben.

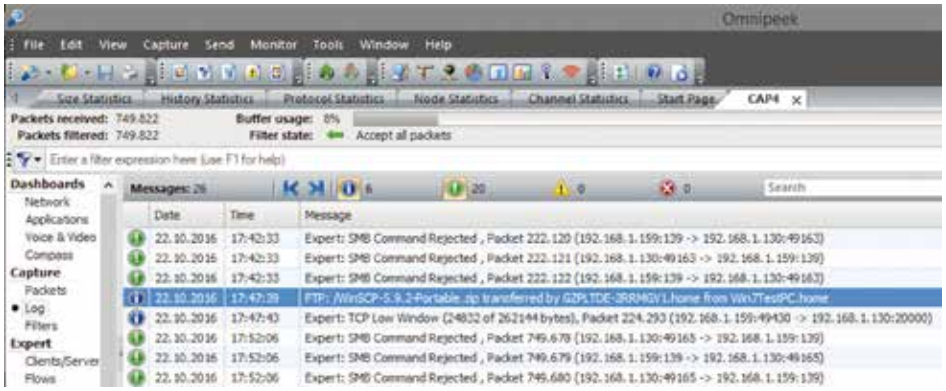
Wie jeder Sniffer erlaubt auch Omnipeek

den Blick bis auf die Datenpaketebene. Mitgeschnittene Sitzungen von FTP- oder HTTP-Sessions zeigen mitunter lesbare Inhalte und die Zusammensetzung der Datenströme. Wem es jedoch nur darum geht, in Datenpakete hineinzuschauen, braucht sich für dieses Ansinnen keine kostspielige Profisoftware zuzulegen. Die Stärken von Omnipeek sind die Analyse von Laufzeiten, Paketverlusten oder Retransmissionen im Netzwerk. Über die Filterfunktion klickt sich der IT-Administrator schnell die gewünschten Daten zusammen. Danach fragt Omnipeek, wie es mit dem Auswahlergebnis verfahren soll: Es kann die selektierten Pakete hervorheben, sie verbergen, die anderen Pakete ausblenden, das Ergebnis in ein neues Fenster kopieren oder einfach nur farblich markieren.

Die Arbeit mit Omnipeek ist recht intuitiv, sofern der Benutzer sich bereits mit Netzwerkanalyse-Programmen auseinandergesetzt hat: Eine gewisse Ähnlichkeit in der Herangehensweise eint die Lösungen. Unterschiede tun sich auf, wenn es um die Analyse von Netzwerk-Flows oder die Visualisierung der Datenverbindungen geht.

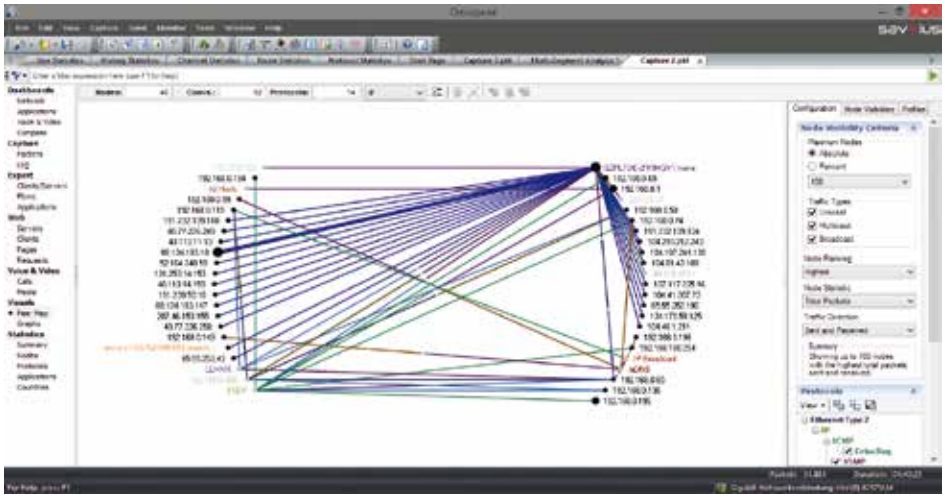
Praktische Flussanalyse

Das Register „Expert“ in der linken Menüleiste enthält einige der wichtigsten Funktionen von Omnipeek: Hier versucht die Software in den Abschnitten „Clients/Servers“, „Flows“ und „Applications“, den Netzwerkverkehr zu interpretieren. Kaum ein IT-Profi möchte sich auf der Ebene von Bits, Bytes und Hexadezimalcodes durch den Datenstrom arbeiten: Entweder fehlt das Know-how, um die Informationen zu interpretieren, oder die Zeit. Die Software von Savvius enthält einige vorgefertigte Helferlein, die die Detailanalyse deutlich vereinfachen und beschleunigen. Insbesondere für den Konversationsfluss bietet



Omnipeek versucht, den mitgeschriebenen Netzwerkverkehr sinnvoll zu interpretieren, im Bild beispielsweise die erfolgreiche Übertragung einer Datei per FTP.

das Programm deutliche Unterstützung, beispielsweise den Packet Visualizer: Er zeigt die interaktiven Anfragen und Antworten zwischen Client und Server an und liefert eine Multisegment-Analyse. Diese stellt die Geschwindigkeit und den Zustand von Flows an vielen Punkten innerhalb des Netzwerks dar. Die „Payload Reconstruction“ baut die Inhalte des Flows nachträglich zusammen. Auch gibt es konversationsorientierte Diagramme, inklusive „tcptrace“. Der Visual Expert enthält außerdem eine „Was wäre, wenn“-Sicht, um die Auswirkungen von Änderungen

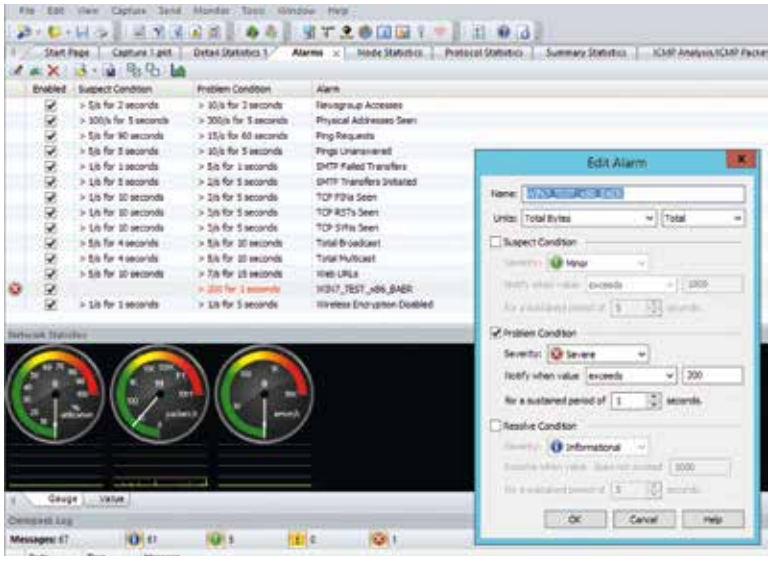


Äußerst spannend ist die Analyse des Netzwerkverkehrs in der „Peer Map“ – je dicker die Linie, desto mehr Traffic.

verschiedener Netzwerk- und Anwendungsparameter auf die Netzwerk-Performance abzuschätzen und darzustellen.

Der „Expert Eventfinder“ liefert Beschreibungen und mögliche Ursachen für jede von Omnipeek erkannte Störung. Bei diesen Ereignissen, die in einer tabellarischen Ansicht („Event Summary“) zusammengefasst sind, kann es sich beispielsweise um eine nur kurze verbleibende Gültigkeit von IP-Paketen handeln („IP Low Time-To-Live“), um gescheiterte TCP-Verbindungen („TCP Connection Refused“) oder zu träge antwortende Server („Slow Server Response Time“). Insbesondere bei langfristigen Messungen im Netzwerk kann der Administrator über die Ereignisse Rückschlüsse über etwaige Fehlkonfigurationen oder Überlastungen ziehen. Kommt es beispielsweise immer in einem bestimmten Zeitfenster zu der Meldung „TCP Stuck Window“, so kann dies daran liegen, dass ein beteiligter Server eine so hohe CPU-Auslastungen hat, dass die Abarbeitung von Netzwerkanfragen darunter leidet. Statt eine Fülle von Logs zu durchforsten, reicht dem Administrator hier der Blick in das Register „Expert“ des Bereichs „Clients/Servers“.

Die „Network Policy Violation Detection“ ermöglicht dem Administrator das Erstellen, Anpassen, Speichern und Laden von Beschreibungen für ein bestimmtes Netzwerk, dessen Teilnehmer und deren erwartetes Verhalten, die der Experte zum Erkennen von Verstößen gegen Netzwerkrichtlinien verwenden kann. Im einfachsten Fall definiert der Administrator Ereignisregeln wie: Wenn das System X



Omnipeek erleichtert die Durchsetzung von Netzwerkrichtlinien, im Bild das Nichtsenden von Paketen von einem spezifischen Rechner, durch eine dauerhafte Überwachung des Netzwerks.

mehr als Y Bytes von sich gibt, soll Omnipeek dies als Hinweis darauf werten, dass eine Sicherheitsregel des Netzwerks nicht eingehalten wurde. Angenehmerweise ist die Definition dieser Einstellungen in der Software denkbar einfach.

In der linken Menüleiste selektierten wir im Test unter „Nodes“ einen unserer Testrechner, der für gewöhnlich nicht in diesem Netzwerksegment aktiv sein soll. Im Kontextmenü wählten wir „Create Alarm“, dann unter Units „Total Bytes“ mit der Einstellung „Total“ und definierten den Störungszustand als ernst („Severe“) mit dem Wert „exceeds 200 for a sustained period of 1 second“ (über 200 für die ununterbrochene Dauer von einer Sekunde). Das Anstecken des betreffenden PCs dokumentierte Omnipeek folgerichtig als Fehler.

Meldungen, Zusammenarbeit und Übersicht

Ab einer gewissen Komplexität und Größe benötigten Adminstratoren ein vernünftiges Zusammenspiel verschiedener Programme, um das Netzwerk sicher zu betreiben. Beim Auftreten vorkonfigurierter oder benutzerdefinierter Ereignisse meldet Omnipeek sich per E-Mail oder SNMP Trap, startet ein Programm oder generiert einen Syslog-Eintrag. Administratoren können in der Software ihre eigenen Schwellenwerte und Abhängigkeiten definieren, um Falschmeldungen zu verhindern. Die Entwickler haben die Benachrichtigungen („Notifications“) gut versteckt in den Optionen untergebracht und verknüpfen letztlich die Benachrichtigungen mit Ereignissen oder Alarmen gemäß den vier Kategorien „Informational“, „Minor“, „Major“ oder „Severe“. Das Zusammenspiel von Alarmen und Benachrichtigungen ist zwar – mit ein paar Einschränkungen – flexibel, erfordert aber einige Zeit zur Konfiguration.

Als äußerst praktisch erwies sich in unserer Teststellung die „Peer Map“, die alle kommunizierenden Knoten innerhalb des Netzwerks anzeigt. Nach einiger Zeit sieht diese Karte auf den ersten Blick etwas undurchsichtig aus, doch erlaubt sie eine freie Skalierung auf eine beliebige Größe. Zudem haben die Entwickler mitgedacht: Je dicker eine Verbindungslinie zwischen zwei Knoten, desto stärker ist der protokollierte Verkehr – einfacher geht es kaum. Wie viele Knoten anzuzeigen sind oder ob dies erst ab einer bestimmten Auslastung erfolgt, bestimmt der Anwender selbst. Dies erleichtert die Überwachung des wirklich wichtigen Datenverkehrs.

Erwartungsgemäß bietet Savvius die Software in mehreren Ausbaustufen an. Die kostenlose 30-Tage-Testversion von Omnipeek, die Grundlage unserer Betrachtung, kommt in der Enterprise Edition mit allen Funktionsbereichen. Dazu zählen die Unterstützung von Gigabit- und 10-Gigabit-Netzwerken, direkte Unterstützung der Access Points von Cisco, Aruba, Xirrus sowie Ruckus, die Verarbeitung von Netflow, Sflow, SNMP und TCP Dump sowie die visuelle Aufbereitung der Verkehrsflüsse auf dem PHY- und IP-Layer. Zudem liefert Omnipeek Enterprise sehr detaillierte Metriken für Sprach- und Videoverkehr inklusive Laufzeitvarianzen (Jitter), Paketverlust, Netzwerkverzögerungen, Signalisierung sowie Sprach- und Bildqualität nach MOS oder R-Faktor. Zusatzfunktionen wie eine Multisegment-Analyse oder die grafische Gegenüberstellung zweier Mitschnitte bietet nur die Enterprise-Version. In der Professional-Variante hat der Administrator den vollen Befehlsumfang, aber keine spezielle Web-, Sprach- und Videoanalyse.

Omnipeek Basic positioniert der Hersteller für den Einstieg in die Protokollanalyse. Die Version bietet Log-Auswertung, Statistiken und grafische Aufbereitungsmöglichkeiten für den Einsatz in Entwicklungsabteilungen, Forschung, Industrial Ethernet und vor allem in kleineren Netzwerken. Im Kleingedruckten der Lizenz schließt der Anbieter jedoch den Full-Duplex-Gigabit- und den WAN-Support der Lösung aus, zudem gibt es keine Peer Map.

Fazit

Omnipeek 9.2 hinterließ im Test einen sehr guten Gesamteindruck. Die Menüführung ist logisch und einfach, die grafische Ausgestaltung der Informationen und die Drill-down-Fähigkeit überzeugten. Praktisch jegliche Aufgabenstellung dürfte der Administrator mit dieser Lösung realisieren können. Bei einem Preis von mehr als 2.000 Euro kann man dies auch erwarten. Im Vergleich zum kostenfreien Wireshark trumpft Omnipeek mit den Möglichkeiten der dauerhaften und verteilten Protokollierung, tiefgreifenden Auswertungen sowie seinen Fähigkeiten im Bereich der 10/40-Gigabit-Netzwerke auf. Omnipeek sollte mit Erscheinen dieser LANline in Version 10 vorliegen. Thomas Bär, Frank-Michael Schlede/wg

- Info: Savvius
  Tel.: 001/925/9373200
  Web: www.savvius.com
- Info: Neox Networks
  Tel.: 06103/37215910
  Web: www.neox-networks.com