Die wachsende Verwundbarkeit der Netze

Angriffe auf die IT Systeme nehmen zu, werden komplexer und für die Opfer immer kostspieliger. Der Verlust von Unternehmensdaten hat oft unmittelbare finanzielle Folgen, beschädigt das Image und macht so hart erarbeitete Wettbewerbsvorteile zunichte.
IT-Sicherheitsverantwortliche versuchen durch Firewalls und ähnliche Schutzvorkehrungen, unerlaubten Zugriff auf unternehmenseigene Netzstrukturen zu verhindern. Trotzdem gelang und gelingt es Angreifern in vielen bekannten und unbekannten Fällen, diesen Schutz zu überwinden.

Die Mechanismen der Netzwerkforensik kommen in diesem Umfeld ins Spiel. Im Zusammenspiel mit anderen Sicherheitstechnologien kann man durch lückenlose Aufzeichnung und umfassende Analyse von Netzwerkverkehr den Beweis für einen Angriff und Rückschlüsse auf seine Art und Weise führen. Leistungsstarke Such- und Analyse-Funktionen ermöglichen IT-Security Spezialisten das „Finden der Nadel im Heuhaufen", sprich, die Identifizierung und Bestimmung von Angriffsmustern. Auf Basis dieser Erkenntnisse können dann Gegenmaßnahmen eingeleitet und Sicherheitsstrategien umgehend angepasst werden können.

Zeitgemäße Angriffsanalyse

Vor dem Hintergrund verteilter Anwendungen und zunehmender Vernetzung sind Unternehmen mehr denn je von der Verfügbarkeit und Sicherheit ihrer Netzstrukturen abhängig – die Netzwerksicherheit wird zur geschäftskritischen Aufgabenstellung.

Das Umfeld für die Analyse und Absicherung der Netzwerke gestaltet sich jedoch zunehmend anspruchsvoller.

Attacken werden komplexer, subtiler und bösartiger

Vor rund einem Jahrzehnt bestanden die häufigsten Sicherheitsbedrohungen für Netzwerke in Massen von Spam-Mails sowie Würmern oder anderen Viren, die zu einer Überlastung der Netzwerke führten und dadurch – im schlimmsten Fall – den laufenden Betrieb zum Erliegen brachten. Heute sind die Bedrohungen deutlich subtiler, weiter entwickelt und vor allem schädlicher. Anstatt nur Dienste zu unterbrechen oder gefälschte Produkte anzupreisen, ist das Ziel der Angriffe zunehmend die Suche nach Informationen, wie zum Beispiel Produktpläne oder Kundendaten, die gestohlen werden und nicht selten in Systeme internationaler Cyber-Krimineller wandern. Cyber-Vandalismus reicht nicht mehr aus – der Hacker von heute ist auf der Jagd nach geistigem Eigentum sowie vertraulichen Daten, die sich für Identitätsdiebstahl und Finanzbetrug verwenden lassen.

Verizon stellte in seinem „Data Breach Investigation Report 2013" fest, dass 75 Prozent aller erkannten Eindringversuche finanziell motiviert waren. Gleichermaßen beunruhigend: In 66 Protzent aller Fälle dauerte es mehrere Monate, bis die Eindringversuche entdeckt wurden. IT-Organisationen fehlen die notwendigen Tools, um Angriffe und Bedrohungen dieser Art in angemessener Weise zu erkennen, zu untersuchen und zu unterbinden.

Netzwerke werden schneller und Datenvolumen größer

Gigabit-Netzwerke, vor kurzem noch hochmodern, sind inzwischen technologische Normalität. Die Einführung der nächsten Generation schnellerer Netzwerke, basierend auf 10-Gigabit und 40-Gigabit-Leitungen, nahm im Jahre 2012 um 62 Prozent zu. Mittlerweile werden drei Viertel aller Investitionen in Hochgeschwindigkeitsumgebungen in 10G-Leitungen getätigt.

Geeignete Werkzeuge müssen in der Lage sein, mit den exponentiell wachsenden Datenraten umzugehen. Traditionelle Monitoring-Tools stoßen hierbei an Grenzen, den Highspeed-Traffic zuverlässig zu erfassen und zu analysieren. In einer Studie von TraCS Research verliehen kürzlich 59 Prozent aller befragten IT Verantwortlichen ihrer Sorge Ausdruck, dass ihre Monitoring-Tools aufgrund Überlastung eher Netzwerkverkehr übersehen, anstatt den Highspeed-Traffic verlässlich für eine Analyse aufzuzeichnen. 51 Prozent aller Befragten bezweifelten zudem die Genauigkeit der Daten, die ihr Netzwerk-Monitoring-Tool anzeigt.

Die Kosten von Ausfällen

Netzwerkprobleme und -ausfälle verursachen den Unternehmen hohe finanzielle Kosten und können die Reputation beschädigen. Höhere Netzwerkgeschwindigkeiten im Zusammenspiel mit neuen Technologien (SDN, NFV) und neuen Medien (BYOD, IoT) machen es zunehmend schwerer, den Traffic präzise zu überwachen, um so Ausfälle zu minimieren. Zudem erhöht sich die Menge an Daten, der bei einem Netzwerkausfall betroffen ist, was die durchschnittliche Troubleshooting- und Analysezeit enorm erhöht.

Betrachte man die MTTR („Mean Time to Resolution" – Mittlere Zeitspanne zur Lösung von Problemen), die von deutschen Unternehmen in der Umfrage von HP angegeben wird:

- Die Wiederherstellzeit nach einem Ausfall beträgt bei mittelständischen Unternehmen durchschnittlich 3,8 Stunden.
- Ein Netzwerkausfall verursacht Unternehmen Kosten in Höhe von durchschnittlich 25.000 Euro pro Stunde.

Bei einem Netzwerkproblem, das einen Ausfall der Infrastruktur verursacht und dessen Lösung etwa eine Stunde in Anspruch nimmt, verliert das betroffene Unternehmen im Durchschnitt 380.000 Euro pro Jahr. Selbst wenn trotz Berücksichtigung von Produktivitätseinbußen und anderen Effekten nur die Hälfte dieser Kosten entsteht, dann ist dies immer noch für viele IT-Organisationen ein guter Grund, um nach besseren Möglichkeiten zur Lösung

von Netzwerkproblemen zu suchen. Während der Netzwerk-Traffic an Volumen und Komplexität zunahm, haben sich viele Netzwerkanalyse-Lösungen zur Überwachung häufig in Richtung Vereinfachung und Verallgemeinerung entwickelt.

Datenstichproben sind zu ungenau

Anstatt den gesamten Datenverkehr zu betrachten, gibt sich eine Reihe von Lösungen damit zufrieden, lediglich Stichproben zu nehmen, um Übersichtsstatistiken auszugeben. Die Funktionalität reicht aus, wenn es um eine reine Darstellung der Auslastung und anderer zusammenfassender Messgrößen zur Netzwerkaktivität geht. Den Ansprüchen der Netzwerkforensik wird dies nicht gerecht! Mit der Zielstellung, einen Angriff zu untersuchen und beispielsweise festzustellen, ob Nachrichten Malware enthalten sind tiefergehende Detailinformationen notwendig. Security-Analysten müssen die Inhalte von verdächtigem Netzwerkverkehr genau kennen; reine Aussagen zum Umfang in einem Zeitintervall reichen nicht aus. Im Kern geht es also darum, mit den Instrumenten der Netzwerkforensik, im Zusammenspiel mit bereits etablierten Technologien, weiterführende Fragen zu beantworten:

- Wie kann ich einen Alarm untersuchen, der vom IDS (Intrusion-Detection-System) durch Traffic in einem Netzwerksegment in Gebäude 3 ausgelöst wurde?
- Wie kann ich feststellen, ob andere Systeme durch einen kompromittierten Server beeinträchtigt wurden?
- Wie breitet sich der Angriff über unser Netzwerk aus?
- Haben wir Beweise dafür, das ein bestimmter Mitarbeiter vertrauliche Daten an einen Mitbewerber weitergibt?
- Wie kann ich bestätigen, ob eine E-Commerce-Transaktion korrekt verarbeitet wurde und fehlerfrei ist?

Um Antworten dafür zu finden, benötigen Security-Analysten auch retrospektiv den vollständigen Zugriff auf die sich immer schneller rollierenden Datenvolumina.

Verkehr, der bereits die Leitung durchquert hat, steht nicht länger für Analysen zur Verfügung – es sei denn, die Daten wurden vollständig aufgezeichnet.

Packet-Capture ist eine Terminologie für das lückenlose Aufzeichnen aller Datenpakete, die ein Netzwerk durchqueren. Diese Technologie gestattet es Security-Analysten, die wirklich spannenden Fragen zu beantworten, insbesondere dann, wenn dies in Verbindung mit leistungsstarken Such- und Analysefunktionen innerhalb der Netzwerkforensik-Lösung geschieht.

Eine optimale Implementierung ermöglicht Security-Analysten das Auffinden der sprichwörtlichen Nadel im Heuhaufen, unabhängig davon, ob sie nach Beweisen für einen Angriff forschen oder im Detail zu verstehen versuchen, wie einzelne Netzwerkressourcen beeinträchtigt sein könnten.

Anwendungsfälle der Netzwerkforensik

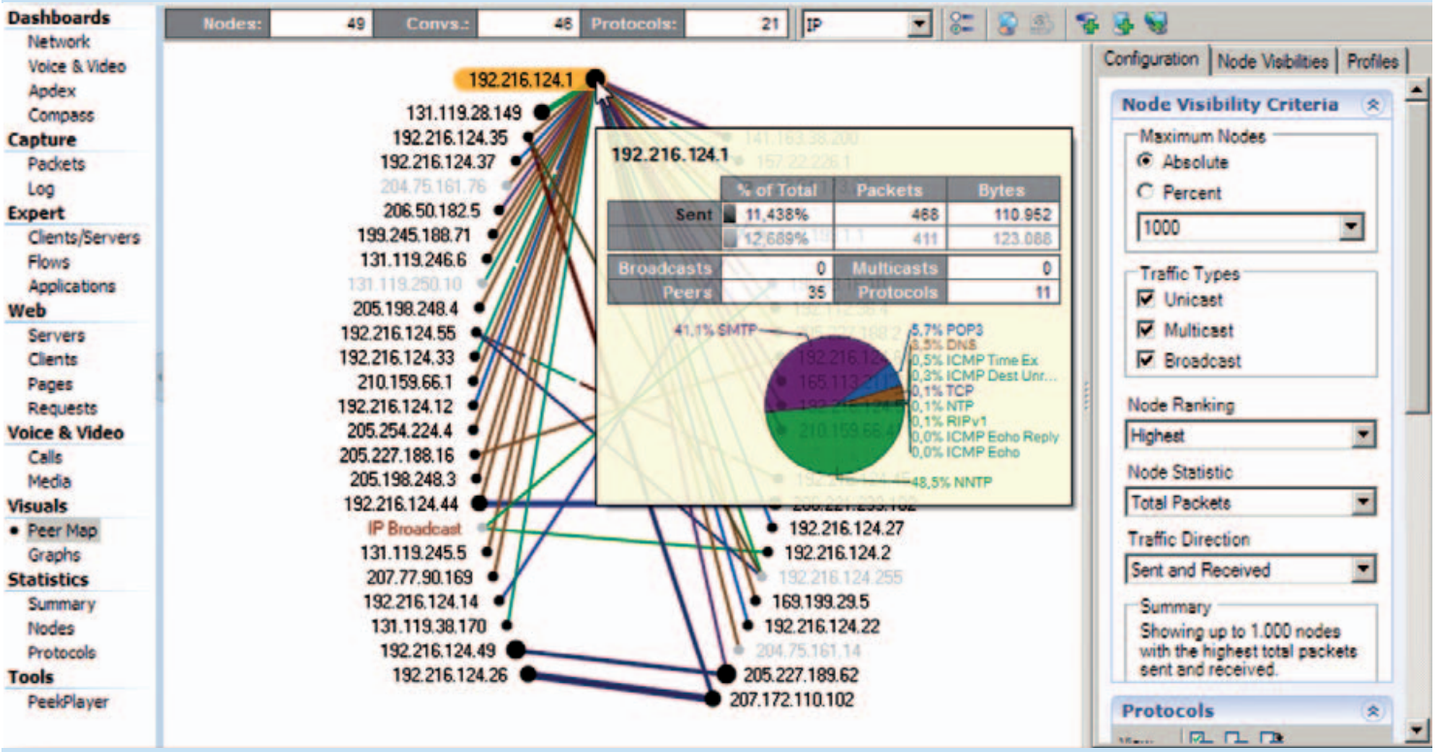
Beweise für einen Angriff sichern

In vielen IT-Organisationen verschafft sich die Netzwerkforensik einen guten Ruf bei der Untersuchung von Sicherheitsvorfällen, wie zum Beispiel Datenmissbrauch. Zumeist löst eine vorgeschaltete Sicherheitslösung wie ein IDS (Intrusion-Detection-System) aufgrund einer verdächtigen

Definition Netzwerkforensik

Netzwerkforensik ist das Mitschneiden, Speichern und Analysieren von Ereignissen in einem Netzwerk. Sie wird manchmal auch als Packet-Mining, Packet-Forensik oder Digitale Forensik bezeichnet. Ungeachtet der Begrifflichkeit ist die Grundidee immer die gleiche: Jedes einzelne Datenpaket des Netzwerk-Verkehrs wird in einem durchsuchbaren Repository aufgezeichnet, damit im Nachgang bei Bedarf eine detaillierte Analyse stattfinden kann.

Das Sammeln eines vollständigen und lückenlosen Mitschnitts von Kommunikationsflüssen erweist sich als besonders nützlich, wenn technische, betriebliche oder organisatorische Probleme zu lösen sind. Es kann Adressen in den unteren Schichten miteinander kommunizierender Systeme aufdecken. Ferner können Analysten Aktivitäten und kritische Transaktionen zu einer physischen Applikation zurückverfolgen. Darüber hinaus unterstützt die Netzwerkforensik die Beantwortung der klassischen W-Fragen: Wer, wann, mit wem, wie, wie oft, wie schnell und wenn nicht schnell genug, warum nicht?



Nexx Networks

Mittels der Omnipeek Peer-Map können Kommunikationsbeziehungen visuell dargestellt werden.

Netzwerkaktivität einen Alarm aus, jedoch ohne den Security-Analysten ausreichende Detailinformationen über den Angriff zu liefern. Eine Untersuchung des Netzwerk-Verkehrs zum Zeitpunkt des Alarms erlaubt den Analysten, vorhandene Beweise zu sichern und weitere Angriffe abzuwehren.

Identifizierung „undichter Stellen"

Ein Spezialfall von IT- und HR-Verstößen ist Industrie-Spionage. Es gibt verschiedenste Möglichkeiten, wie interne Nutzer vertrauliche Informationen per E-Mail, Blog-Posts, sozialen Medien u.a. verbreiten können. E-Mail- und Web-Gateways können unter Umständen einige dieser Kommunikationen auffangen. Die Netzwerkforensik ermöglicht das Aufspüren undichter Stellen, die traditionelle Mechanismen unterlaufen.

Verifikation von Geschäftstransaktionen

Sowohl bei verschlüsselt (HTTPS, SSL, IPSec) als auch unverschlüsselt (SQL, HTTP, FTP) ablaufenden Transaktionen, stellen Netzwerkforensik-Lösungen den idealen Audit-Trail für Geschäftstransaktionen zur Verfügung. Sie tragen dazu bei, Probleme zu lösen oder Betrugsversuche aufzudecken, für die Server-Logs nicht ausreichen. Online-Händler können zum Beispiel mit Netzwerkforensik Diskrepanzen zwischen Angaben von Kunden- und Serverseite beseitigen oder überprüfen, ob Transaktionen manipuliert wurden. Nicht zuletzt liefert die lückenlos aufgezeichnete Übertragung einen umfassend dokumentierten Beweis dafür, dass eine bestimmte Transaktion tatsächlich stattgefunden hat.

Anforderungen an eine Netzwerkforensik-Lösung

Zur Erleichterung digitaler Untersuchungen müssen entsprechende Lösungen folgende grundlegende Anforderungen abdecken:

Datenaufzeichnung

Dies bezeichnet die Fähigkeit, mehrere Terabyte an Daten in Netzwerken mit hohem Durchsatz (inklusive 10G- und 40G-Verbindung) zu erfassen und zu speichern, ohne dabei einzelne Datenpakete zum Beispiel wegen Überlastung, auszulassen. Etwaige Einschränken können und sollten mit Hilfe von Laborversuchen ermittelt und die nachstellbaren Ergebnisse dokumentiert werden.

Datenaufbereitung

Sobald Daten auf dem Speichermedium aufgezeichnet wurden, sollten umfassende Möglichkeiten zum Filtern der relevanten Elemente über Kriterien, wie IP-Adresse, Anwendung, Kontext, Datum, Zeit usw. bereit stehen. Security-Analysten müssen sich beim Durchforsten von Terabytes an Daten verlässlicher Werkzeuge

bedienen, um die kritischen Datenpakete innerhalb eines angemessenen Zeitraums zu finden.

Datenanalyse

Um die Analyse schneller voranzutreiben, profitieren Security-Analysten während des forensischen Analyseprozesses von definierten Mustern zum Erkennen von Anomalien. Automatische Expertenanalyse, die den Kontext von Netzwerkereignissen über die kompletten OSI-Layer darstellt, unterstützen Analysten bei der schnellen Erkennung von anormalen oder sonstigen signifikanten Ereignissen.

Neben diesen grundsätzlichen funktionalen Anforderungen sollte eine umfassende Netzwerkforensik-Lösung weiteren Kriterien genügen:

Vollständigkeit

Highspeed-Traffic muss komplett und ohne Verlust einzelner Datenpakete erfasst werden können. Falls dies im Einzelfall nicht möglich ist, muss das System anzeigen, wann und wieviel Pakete fehlen. Zumindest diese Information muss exakt und hieb- und stichfest sein.

Skalierbarkeit

Für das Mitschneiden von Highspeed-Traffic – zum Beispiel in Netzwerken mit mehreren 10- bzw. 40-Gigabit-Links - müssen entsprechende Datenvolumina, oft mehrere Hundert Terabyte, im Rahmen einer erschwinglichen und einfach zu verwaltenden Konfiguration analysiert werden können.

Flexibilität

Es ist nichts Ungewöhnliches, das Analyse Spezialisten Verkehr in Netzwerk-Segmenten mit unterschiedlichen Geschwindigkeiten mitschneiden müssen, zum Beispiel auf einem 1G, 10G und einem 40G-Link. Eine Forensik-Anwendung sollte in der Lage sein, Schnittstellen für heterogene Netzwerke so zu kombinieren, dass die Sicherheitsteams nicht gezwungen sind, zur Überwachung mehrerer Netzwerke mit unterschiedlichen Geschwindigkeiten separate Komponenten anzuschaffen.

Verfügbarkeit

Um einen umfassenden Zugriff auf relevante Daten zu erhalten, ist eine dauerhafte und lückenlose Aufzeichnung des Netzwerkverkehrs erforderlich. Nur so ist sichergestellt, dass die Daten beim Auftreten entsprechender Ereignisse für die im Vorfeld nicht bekannten Zeiträume verfügbar sind. Neben der permanenten Aufzeichnung des Netzwerkverkehrs sollte auch die Möglichkeit von Echtzeitaufbereitung vorhanden sein, damit Security-Analysten einfach die Vergangenheit mit der Gegenwart vergleichen können und nicht auf unterschiedliche Analyse-Tools (eins für Forensik- und eins für Echtzeitanalysen) zurückgreifen müssen. Durch die Bereitstellung einer Lösungsumgebung, die alle Anforderungen erfüllt, lassen sich auch Implementierungs-, Schulungs- und Wartungsaufwände minimieren.

Die Netzwerke leisten zwar mehr, aber die IT sieht weniger

Die eingeschränkte Sicht kann für das Geschäft kostspielige Folgen haben. Einschränkungen in der Netzwerk-Performance verursachen eine sinkende Mitarbeiterproduktivität. Ohne ausreichende Transparenz der Netzwerkereignisse kann es für die IT schwierig werden, wenn diese Anwendungsdienste optimieren soll.

Unternehmensführungen müssen erkennen, dass die Netzwerkforensik zu einer unverzichtbaren IT-Fähigkeit geworden ist, die für jedes Netzwerk zur Verfügung stehen muss, damit rund um die Uhr und an jeder Stelle die vollständige Transparenz von Geschäftsbetrieb, Netzwerk-Performance und IT-Risiken gewährleistet ist. *(AP)*

Timur Özcan, Geschäftsführer, Neox Networks