



Security- und Compliance-Guide

Mit Marktübersicht Content-Security-Lösungen

Sonderdruck für Network Instruments

Zero-Day-Attacken erkennen

Forensik und Compliance

„Network Security Forensic“ ermöglicht dem Sicherheitsverantwortlichen eine paketgetreue Erfassung und Speicherung auch hoher Datenmengen mit einer anschließenden eingehenden Sicherheitsanalyse.

Sicherheitssysteme haben die Aufgabe, das Netzwerk sowie sensible Unternehmensdaten vor Angriffen von außen und innen zu schützen. Gegen neuartige Angriffe bedarf es dabei Analyselösungen, die das genaue Maß der Gefahren sowie deren Ursache und unmittelbare Auswirkung zeigen können. Diese Rolle kann „Network Security Forensics“ übernehmen.

Ergänzung für bestehende IDS-/IPS-Systeme

Intrusion-Detection- und -Prevention-Systeme (IDS/IPS) überwachen ein Netzwerk auf bekannte Angriffssignaturen von Hackern, Viren und Trojanern hin und melden diese unverzüglich an die Sicherheitsverantwortlichen. Im Falle eines Intrusion-Prevention-Systems wird auch eine Gegenmaßnahme eingeleitet, wie etwa die Unterbrechung der Verbindung oder das Verwerfen der Datenpakete. Danach muss sich der Anwender allerdings mit einer begrenzten Zahl statistischer Informationen über die Ereignisse begnügen. Genaue Nachforschungen sind so nicht möglich. Diese Informationslücke

kann mit Hilfe von Network-Security-Forensics-Analysatoren gefüllt werden. Diese erfassen alle relevanten Datenströme der jeweils letzten Stunden und Tage und ermöglichen



Bild 1. „Observer“-Benutzeroberfläche zur Langzeitanalyse von Network Instruments
Quelle: Psiber Data

es, jeden Sicherheitsvorfall vor, während und nach dem Angriff zu analysieren. Der Sicherheitsverantwortliche bekommt so einen tieferen Einblick in die Zusammenhänge. Er erfährt zum Beispiel, welche Hardware mit dem gleichen Virus infiziert wurde und welcher Laptop-Nutzer sich unmittelbar vor einem Vorfall ins Netzwerk eingeloggt hat. Da man hierbei auf sämtliche Netzwerkdaten zu-

greifen kann, lassen sich die Ursache und Auswirkung des Vorfalls von verschiedenen Seiten gut durchleuchten.

Alle 15 Minuten neue Angriffssignaturen

Bei der Vielzahl von möglichen Angriffen und angesichts immer neu auftauchender Sicherheitslücken heutiger Netzwerke ist es nicht verwunderlich, dass die Angriffssignaturen, ähnlich wie bei Virencantern, sehr häufig in Abständen bis zu jeder Viertelstunde aktualisiert werden müssen. IDS-/IPS-Anbieter pflegen die Signaturen ständig und entwickeln sie weiter. Zu den verbreiteten Produkten zählt auch die recht häufig verwendete

von Sicherheitsexperten, die ständig neue Snort-Rules bereitstellen. Inzwischen sind über 8000 Signaturen verfügbar, die außer von Snort selbst auch von anderen Anbietern wie Bleeding Edge Threats angeboten werden. Zum Teil können die Signaturen aus dem Internet kostenlos heruntergeladen werden. Um jedoch auf die allerneuesten Signaturen zugreifen zu können, muss man über ein kostenpflichtiges Abonnement verfügen. Diese umfangreiche und ständig aktualisierte Plattform wird unter anderem von Network-Security-Forensics-Analysatoren wie Observer von Network Instruments verwendet, sodass sich dem Analysator ein riesiges Spektrum an Erkennungssignaturen erschließt.

Gedächtnisstütze für IDS/IPS

Mit diesem Arsenal an Erkennungsmustern sowie der Eigenschaft, hohe Datenmengen im TByte-Bereich erfassen und speichern zu können, vermag ein Network Security Forensics Analysator jeden Angriff unter die Lupe zu nehmen. Nachdem das IDS eine Sicherheitsverletzung aufgedeckt und gemeldet hat, kann der Sicherheitsverantwortliche mithilfe des Analysators den Netzwerkverkehr innerhalb einer spezifischen Zeitperiode vor und nach dem Ereignis auswählen und wie mit einer Videokamera abspielen. Dazu bieten die forensischen Analysatoren mithilfe von Expert-Modulen eine genaue Auswertung der relevanten Kommunikationsbeziehungen bis hinunter auf die Paketebene und die Eigenschaft, aus den gesammelten Datenpaketen den ursprünglichen Inhalt einer

Source	Destination	Protocol	Length	Time	Flags	Info
192.168.1.1	192.168.1.2	TCP	60	10:00:00.000000000	0x00000000	64800 → 80 [RST] Seq=1234567890 Win=0 Len=0
192.168.1.2	192.168.1.1	TCP	60	10:00:00.000000000	0x00000000	80 → 64800 [RST] Seq=9876543210 Win=0 Len=0
192.168.1.1	192.168.1.2	TCP	60	10:00:00.000000000	0x00000000	64800 → 80 [RST] Seq=1234567890 Win=0 Len=0

Bild 2. Ergebnis der forensischen Analyse mit Observer von Network Instruments
Quelle: Psiber Data

E-Mail, Instant Message, Webseite, eines VoIP-Gesprächs oder einer anderer Art der Kommunikation zu rekonstruieren.

Zero-Day-Angriffe im Nachhinein identifizieren

Trotz der immer aktualisierten Angriffssignaturen dauert es oft Tage oder sogar Wochen, bis für neuartige Sicherheitsrisiken wie Trojaner oder Internetwürmer entsprechende Gegenmaßnahmen und Erkennungsmuster bekannt sind. Aufgrund der Beschwerden der User, Performance-Einbußen und Ausfälle wird häufig bereits lange vorher Verdacht geschöpft. Man bezeichnet all die Angriffe, die zum ersten Mal aufgetreten beziehungsweise in Umlauf gebracht worden sind und für die es noch keine Signaturen und Abwehrmechanismen gibt, als „Zero-Day“-Angriffe. Da Network-Security-Forensics-Analysatoren die Netzwerkdaten sogar über etliche Tage oder Wochen hinweg erfassen können, ist es möglich, Zero-Day-Angriffe im Nachhinein, nachdem die Signaturen für diese neuen Bedrohungen endlich entwickelt wurden, zu entdecken. Anschließend kann über das Ausmaß des Schadens Auskunft gegeben werden, um ihn schnell und vollständig zu beheben.

Ein Fallbeispiel

An einem Wochenende wurden einige Angriffsversuche innerhalb der DMZ, der Demilitarisierten Zone eines Unternehmens, entdeckt und erfolgreich abgewehrt. Vom IPS jedoch unentdeckt blieb der Versuch des Eindringlings, sich über das Ausprobieren verschiedener Passwörter, also die so genannte Brute-Force-Methode, in das VPN-Gateway einzuloggen und sich einen neuen Admin-Account anzulegen. Da der Angreifer somit in den Sicherheitsbereich vorgedrungen war, konnte er weitere schädliche Trojaner-Software wie Remote-Control-Tools und Keylogger einschleusen. Über letztere hatte er dann die Möglichkeit, Tastatureingaben zu beobachten. Dies gab ihm schließlich die Möglichkeit, weitere Systeme anzugreifen. Diese Vorfälle wurden allerdings mithilfe eines Network-Forensic-Analysators passiv auf Paketebene aufgezeichnet. Der Zeitbereich rund um die bereits erkannten Vorfälle wurde ausgewählt und mit den allerneuesten Signaturen nach möglichen Angriffen, DoS-Angriffen und Login-Vorgängen genau untersucht. Diese Analyse förderte dann den Trojaner zutage, der es dem Hacker ermöglichte, auf die Datei-

server zuzugreifen. Sein Schlupfloch ins Unternehmen ließ sich so beseitigen und der Schaden damit begrenzen. Ein besonderer Fokus richtet sich auf den Schutz sensibler Unternehmensdaten vor unbefugtem Zugriff. Hier gilt die Aufmerksamkeit vor allem dem unberechtigten Zugriff aus den eigenen Reihen sowie der Industriespionage. Neben den eigenen Interessen des jeweiligen Unternehmens, solche Daten zu schützen, um seine Wettbewerbsvorteile zu wahren und finanzielle Schäden durch Insiderinformationen zu vermeiden, wird der Druck durch gesetzliche Regelungen weiter verschärft. Dazu zählen verschiedene gesetzliche und brancheninterne Vorgaben und Regelungen wie der Sarbanes-Oxley Act (SOX), BASEL II, International Accounting Standards (IAS) oder GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen). Konkret ergibt sich daraus, dass alle vertraulichen Informationen wie Finanz- und Kundendaten vor unbefugtem Zugriff geschützt werden müssen. Außerdem sind die Kommunikationsströme zu und von den Systemen zu dokumentieren, wie es zum Beispiel in SOX, Absatz 302 gefordert wird. Des Weiteren müssen solche Daten während der Übertragung gegen Missbrauch geschützt werden, zum Beispiel durch eine angemessene Verschlüsselung. Mithilfe eines Network-Security-Forensics-Analysators lassen sich alle zu und von einem bestimmten Gerät oder Segment gesendeten Daten erfassen. Falls es zu Sicherheitsvorfällen kommt, kann überprüft werden, ob etwa vertrauliche Papiere

per E-Mail, Web-Mail oder FTP das Unternehmen verlassen haben. Für den Nachweis lassen sich diese Informationen rekonstruieren. Außerdem werden Behörden in die Lage versetzt, nachzuprüfen, ob alle vertretbaren Schutzmaßnahmen mit Sorgfalt getroffen wurden. Zudem lässt sich eine eventuelle Sicherheitsverletzung samt anschließenden Gegenmaßnahmen für spätere Audits vorschriftsgemäß dokumentieren.

Fazit

Da es sich bei der Netzwerk- und Datensicherheit um ein zunehmend komplexes Thema mit oft weittragenden, unvorhersehbaren Auswirkungen handelt, muss in schwerwiegenden Fällen die Möglichkeit gegeben sein, über die Bestimmung des Zeitpunkts und der betroffenen Orte hinaus eine detaillierte Analyse eines Vorfalls durchzuführen. Hierzu eignen sich spezielle Analyselösungen mit Network-Security-Forensik-Modulen. Sie können je nach Modell hohe Datenmengen bis zu 48 TByte erfassen und analysieren. Ein optionaler SAN-Anschluss erhöht das Speichervolumen zusätzlich.

Aleš Mahler/wj



Network Instruments
Schubertstr. 29
85653 Großhelfendorf
+49 8095 87 58 58
www.networkinstruments.de

Dipl. Wirtschaftsingenieur Aleš Mahler ist Regional Sales Manager für Zentral- und Osteuropa bei Network Instruments.