Alles im Fluss, oder wo ist die Nadel im Heuhaufen?

Text: Peter Haag, SWITCH, haag@switch.ch

SWITCH-CERT hat auch im letzten Jahr seine Dienste im Bereich Sicherheit weiter ausgebaut. Dazugekommen ist ein neuer Service, der die Kunden alarmiert, falls Systeme mit Viren und Würmern oder anderer Malware infiziert sind oder ungewöhnliche Aktivitäten zeigen, die auf einen Befall schliessen lassen.

Die Auswirkungen befallener Systeme sind vielfältig und reichen von «kaum erkennbar» bis zur DDoS-Attacke. In jedem Fall hinterlassen sie jedoch Spuren im Netz. Es gilt nun, diese Spuren zuverlässig aufzuspüren und den Kunden zu informieren. Bei der täglichen Datenflut ist das vergleichbar mit der berühmten Suche nach der Nadel im Heuhaufen. Verschiedene Arten von Malware erzeugen verschiedenartige Muster im Netzwerk-Verkehr. Typisch ist zum Beispiel der Zusammenschluss verschiedener gehackter Systeme in Botnets. (Siehe auch der entsprechende Beitrag «Got a Bot?» von Serge Droz). Sie hinterlassen charakteristische Spuren. Für eine zuverlässige Erkennung sind verschiedene Voraussetzungen notwendig. Zum einen braucht es Informationen und Kenntnisse über die zu suchenden Muster. Hier verfügt SWITCH-CERT über ein eigenes Security Lab zur Analyse der Malware. Doch die schnelle Entwicklung von Viren und Botnet Software macht es unabdingbar, die gewonnenen Erkenntnisse in einem weltweiten Netzwerk mit anderen Sicherheitsteams auszutauschen, um so immer auf dem neusten Stand der Technik zu bleiben. Selbstverständlich sind auch Informationen aus unserem Kundenkreis wichtig und tragen dazu bei, das Bild abzurunden. Zum anderen braucht es auch die entsprechenden Werkzeuge zur Suche der entsprechenden Muster und natürlich die Netzwerkdaten. Der eigentliche Wert entsteht nun durch die Korrelation der Informationen und Daten.

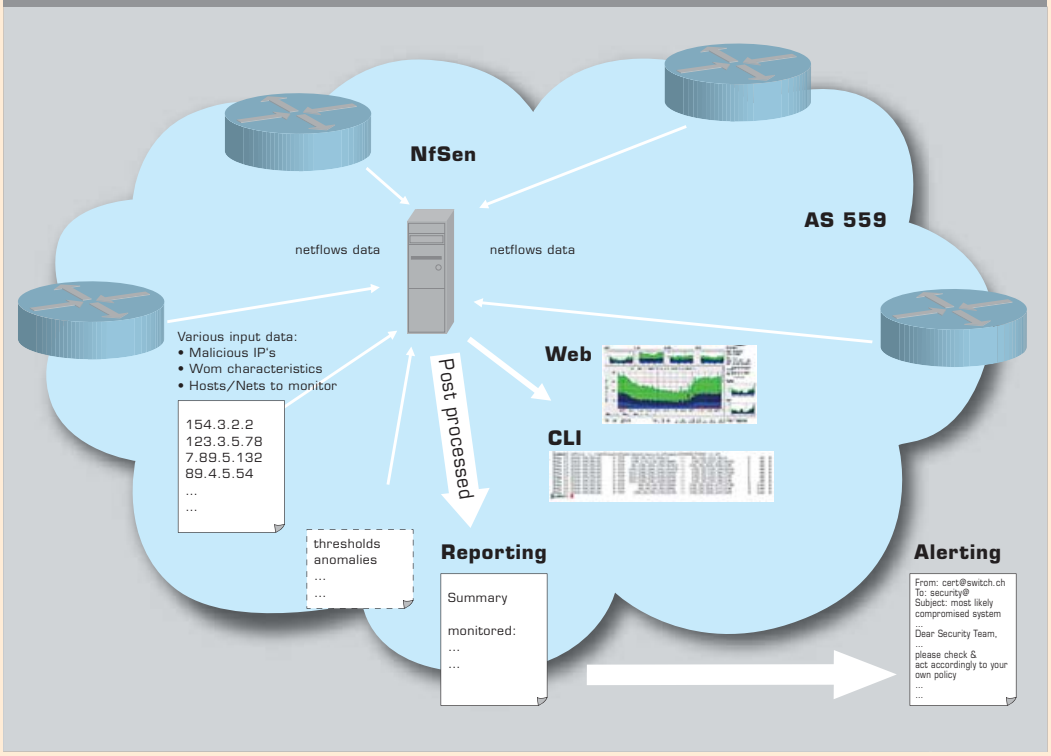
«Der eigentliche Wert entsteht durch die Korrelation der Informationen und Daten.»

Aus den Anforderungen des täglichen operationellen Betriebs hat SWITCH-CERT die Tools NfSen und NFDUMP entwickelt. Sie verarbeiten Netflow-Daten (siehe Textbox), die an den Grenzen des SWITCH Backbones gesammelt werden. Die Netflow-Daten werden nach den entsprechenden Mustern durchsucht. Daraus entstehen Reports, die wiederum als E-Mails aufbereitet und den zuständigen Sicherheitsteams bei den Netzwerkkunden von SWITCH zur weiteren internen Abklärung zugeschickt werden. Alle Reports werden immer noch manuell überprüft, um zu garantieren, dass keine so genannten «False Positives», d.h. nicht betroffene Systeme, gemeldet werden.

Aufbau NfSen Architektur innerhalb des SWITCH Backbones

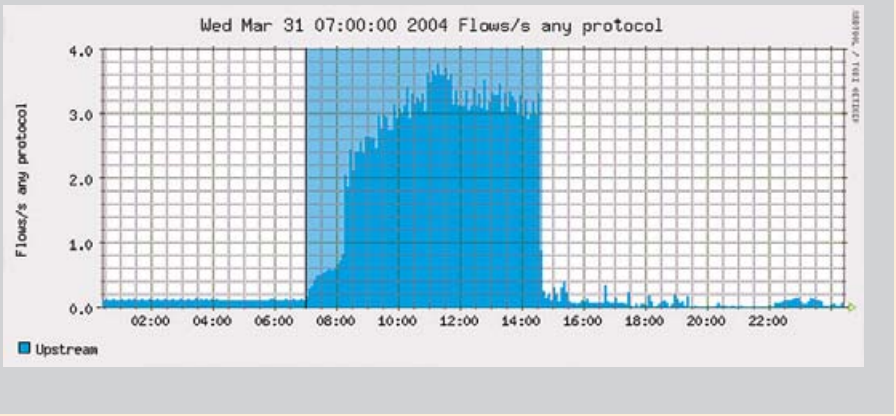
Die Netflow-Daten wichtiger Router im SWITCH-Netzwerk und die relevanten Muster für Würmer und Botnets etc. werden miteinander verarbeitet und generieren schliesslich Alert-E-Mails für den Kunden.
Scanning-Aktivitäten von infizierten Systemen, Verbindungen von Botnets, ein- oder ausgehende DoS-Attacken und vieles mehr werden so sichtbar. Aufgrund der Benachrichtigung hat der Kunde die Möglichkeit, die befallenen Systeme schnell und gezielt wieder von Viren, Würmern oder sonstiger Malware zu be-

Aufbau NfSen Architektur innerhalb des SWITCH Backbones



Die Netflow-Daten wichtiger Router im SWITCH-Netzwerk und die relevanten Muster für Würmer und Botnets usw. werden miteinander verarbeitet und generieren schliesslich Alert-E-Mails für den Kunden.

NfSen für Incident Handling



Profil eines Befalls: Man kann genau erkennen, zu welcher Zeit das System infiziert wurde und unüblicher Verkehr entstand. Die detaillierte Analyse der Netflow-Daten in diesem Zeitabschnitt gibt Auskunft, welche Systeme zusätzlich betroffen waren und von welcher IP-Adresse die Attacke kam.

freien. Dank stetiger Verbesserung der Tools, aber auch aufgrund zunehmender Aktivität im Netz ist die Anzahl verschickter E-Mails im Monat Dezember 2004 auf über 500 Mails angestiegen.

Hat ein Kunde einen grösseren Sicherheitszwischenfall zu verzeichnen, kann SWITCH-CERT auf Wunsch bei den Aufklärungen ebenfalls Support leisten. Mit denselben Netflow Tools kann der Vorfall im Rahmen der Möglichkeiten rekonstruiert werden. Aus dem Profil des gehackten Systems kann die IP-Adresse des Angreifers identifiziert und allenfalls weitere betroffene Systeme eruiert werden. Die Sicherheitsteams der Hochschulen und Fachhochschulen erhalten so zusätzliche Informationen, um den Vorfall zu bewältigen, aber auch, um Systeme ausfindig zu machen, die zwar ebenfalls befallen, aber bis anhin noch nicht negativ aufgefallen sind. Parallel dazu erfolgt die Incident-Koordination oftmals über mehrere Länder hinweg. Dank den guten internationalen Beziehungen zu anderen Incident Response Teams können auch hier in nützlicher Frist positive Resultate erzielt werden.

Natürlich kann dieser Dienst nicht verhindern, dass auch weiterhin Systeme gehackt oder infiziert werden. Aber er kann dazu beitragen, die Zeit vom Befall bis zur Entdeckung zu verkürzen. Damit wird auch das Risiko vermindert, dass infizierte Computer im Netz unbemerkt verweilen und danach als Quelle einer grösseren Attacke oder für Spam E-Mails in Erscheinung treten. Das frühzeitige Entdecken auf der Kundenseite dient somit auch der Schadensbegrenzung.

NfSen und NFDUMP sind von SWITCH geleitete Open-Source-Projekte. Sie sind verfügbar unter http://nfdump.sourceforge.net rsp. http://nfsen.sourceforge.net.

SWITCH-CERT will mit den ständig wechselnden und wachsenden Anforderungen im Internet Schritt halten, die entsprechend notwendigen Tools entwickeln, diese laufend verbessern und anpassen. Das Feedback unserer Netzwerkkunden ist dabei von entscheidender Bedeutung, um immer einen optimalen Service für die Sicherheit im Netz zu bieten.

Was ist Netflow?

Netflow ist eine von Cisco entwickelte Technik, die detaillierte Auskünfte über einzelne Flows ermittelt. Zu einem Flow gehören zum Beispiel die Pakete einer TCP-Verbindung, die in eine gemeinsame Richtung laufen. Ein Router oder ein Switch misst den Datenverkehr der Interfaces und exportiert die gesammelten Flow-Daten zu einem Rechner, der sie für das Netzwerkmonitoring oder Accounting auswertet.

Die Pakete werden zuerst in Flows aufgeteilt. Das geschieht anhand verschiedener Parameter: Source- und Destination-IP-Adresse, IP-Protokoll (TCP, UDP, ICMP, ...), Quell- und Zielports von TCP oder UDP, TOS-Feld (Type of Service). Für jeden Flow gibt es unter anderem einen Paket- und einen Bytezähler.

Netflow-Daten beschreiben immer die Eigenschaften von Verbindungen und haben keinerlei Informationen über den Inhalt der transportierten Daten.

Peter Haag
ist Network Security Engineer bei SWITCH. Er beschäftigt sich neben der Entwicklung der SWITCH Netflow Tools auch mit Computer Incident Handling und Massnahmen zur Erhöhung der Sicherheit. Er ist ebenfalls beteiligt an Foren wie FIRST, TF-CSIRT und SWIRT.