VIAVI Solutions

Whitepaper

Quelldaten zur Sicherheitsuntersuchung in Netzwerken

So halten Ihre Netzwerkdaten vor Gericht stand!

Immer komplexere Netzwerke sind auf mehr als eine Universallösung angewiesen, um eine angemessene Leistung und die Integrität der Daten zu gewährleisten. Zusätzlich zu den üblichen Leistungsstörungen wie langsamen Anwendungen, höheren Bandbreitenanforderungen und einer mangelnden Transparenz der Cloud-Ressourcen besteht immer die Gefahr eines bösartigen Angriffs.

Während viele Lösungen wie Firewalls und IDS-Systeme zum Erkennen unberechtigter Zugriffe Angriffe verhindern sollen, bietet keine von ihnen eine absolute Sicherheit. Allerdings gibt es heute proaktive Maßnahmen, die ein IT-Team ergreifen kann, um eine Sicherheitsverletzung umgehend zu erkennen, deren Folgen effektiv abzumildern und dafür zu sorgen, dass gerichtsfeste Daten zur Verfügung stehen, falls ein Zivil- oder Strafprozess eingeleitet werden sollte.

3 Möglichkeiten zur Verringerung der Auswirkungen einer Sicherheitsverletzung

Um die Auswirkungen eines erfolgreichen Angriffs gegen das Netzwerk zu erkennen und abzumildern, ist es unverzichtbar:

- die IP-Verbreitung zu kennen.
- eine Baseline für das Netzwerk festzulegen.
- die richtigen Quelldaten zu erfassen.

Die IP-Verbreitung kennen

Der Netzwerk-Experte und zertifizierte E-Commerce-Betrugsermittler Tim O'Neill meint, dass Netzwerktechniker mit der geografischen Verbreitung ihrer IT-Ressourcen und dem Nutzerverhalten vertraut sein sollten. Dazu müssen sie die IP-Adressen der autorisierten Benutzer sowie die üblichen Zieladressen ihres Unternehmensnetzes kennen.

> „Ich sage den Leuten immer wieder, dass sie ihre IP-Verbreitung kennen müssen."
>
> – Tim O'Neill
>
> *Zertifizierter E-Commerce-Betrugsermittler*

„Welche IP-Adressen sind intern in Ihrem Netzwerk vorhanden? Welches sind die üblichen externen Ziele bzw. IP-Adressen, die Ihre Mitarbeiter aufrufen? Sie müssen diese typischen internen und externen Ziele kennen und wissen, zu welchen Tageszeiten sie normalerweise angeklickt werden. Wenn Sie dann merken, dass jemand eine ungewöhnliche IP-Adresse ausgewählt hat, Sie zahlreiche Datenlecks erkennen und das Verkehrsvolumen langsam ansteigt, dann können Sie gezielt nach der Person suchen, die diese Aktion aus Versehen oder mit Vorsatz ausgelöst hat."

Hacker „leihen“ sich selbst $1 Milliarde.

Bösartige Aktivitäten im Netzwerk können verschiedene Formen annehmen, doch letzten Endes geht es fast immer um Geld. Bei Banken und anderen Einrichtungen kann ein umfassender Überblick über das Netzwerk dazu beitragen, dass eine Datenrechtsverletzung umgehend erkannt wird.

„Vor ein paar Jahren hat es weltweit einen massiven Angriff auf Banken gegeben“, sagt O'Neill. „Die Hacker, die als das Carbanak-Team bekannt sind, sollen eine Milliarde Dollar gestohlen haben. Das Kernproblem war, dass damals auffälliger Datenverkehr nicht erkannt wurde. Die Hacker waren in das Netzwerk eingedrungen und hatten eigene Dokumente erstellt. Sie hatten sich Berechtigungen angeeignet. Doch wenn damals jemandem die IP-Adresse aufgefallen wäre, dann wäre klar gewesen, dass dieses Ziel für das Netzwerk nicht normal war.“

Die tatsächliche Höhe des finanziellen Schadens wurde niemals bekanntgegeben. Man kann aber davon ausgehen, dass mehr als 100 Banken in elf Ländern mehrere Tage lang täglich viele Millionen Dollar verloren. Wenn sich die Netzwerk- oder Sicherheitstechniker einige simple Fragen gestellt hätten, hätten sie wichtige Fakten in Zusammenhang mit der ungewöhnlichen IP-Adresse und dem auffälligen Verkehr ermitteln können.

„Das war keine andere Bank“, sagt O'Neill, der betont, wie wichtig es ist, ungewöhnliche IP-Adressen und damit in Zusammenhang stehenden Verkehr zu erkennen. „Das war auch keine andere Filiale oder ein sonstiges Büro. Warum wurden Kredite aufgenommen?

Der Betrüger hat 38 Banken angegriffen. Zumindest haben diese Banken zugegeben, dass sie angegriffen wurden. Die Kostenschätzung der Banken, die bereit waren, reinen Wein einzuschenken, liegt bei gut über 10 Millionen US-Dollar.“

O'Neill empfiehlt eine einfache und effiziente Vorgehensweise, um normale Aktivitäten (Baseline) zu vergleichen und zu prüfen und den üblichen oder durchschnittlichen Verkehr sowie die entsprechenden Benutzer zu protokollieren.

„Man muss nur alle IP-Adressen eine Woche lang in einer Excel-Tabelle zusammenfassen. Dann können Sie alle miteinander vergleichen oder die übliche Reaktionszeit zwischen zwei Büros oder das Verkehrsvolumen ermitteln. Wenn Sie beispielsweise wissen, dass ein Büro in Kalifornien immer zwischen 7:00 und 18:00 Uhr auf einen spezifischen Server zugreift, dürfte abends kein Verkehr verzeichnet werden, wenn die Server nachts abgeschaltet sind. So beginnen Sie, sich einen Überblick zu verschaffen und Referenzwerte als Baseline festzulegen.“

Eine Baseline festlegen

Cisco beschreibt das Baselining als eine „in regelmäßigen Abständen erfolgte Untersuchung des Netzwerks, um sicherzugehen, dass es wie vorgesehen funktioniert."

Diese Vorgehensweise erlaubt:

- wertvolle Einblicke in den Status der Hardware und Software zu gewinnen.
- den aktuellen Auslastungsgrad der Netzwerkressourcen zu ermitteln.
- die Alarmschwellwerte im Netzwerk exakt festzulegen.
- auffälligen Verkehr zu erkennen.
- aktuelle Netzwerkprobleme zu identifizieren.
- zukünftige Probleme vorherzusagen.

Mike Canney, ein 26 Jahre alter Experte für Netzwerk-Performance, hat bereits Tausenden Unternehmen auf der ganzen Welt geholfen. Er empfiehlt jedem Netzwerkadministrator und Netzwerktechniker, sich die Ermittlung von Baselines als grundlegende Qualifikation anzueignen.

> „Ein Administrator muss sein Netzwerk wie seine Westentasche kennen."
>
> – Mike Canney
>
> *Network and Application Performance Analyst*

„Sie müssen ihre gesamte Kompetenz nutzen, um zu wissen, was in ihrem Unternehmensnetzwerk vor sich geht. In den Anfangszeiten der Netzwerke drehte sich alles um die Bandbreite. Damals erreichte die Datenrate in einem Highspeed-WAN nur 56 kBit/s und jeder gute Netzwerktechniker hatte eine Baseline seiner Infrastruktur erstellt. Er wusste immer, was wie genutzt wurde. Jeder hatte einen Überblick über den Verkehr und wusste, was alles über das Netzwerk übertragen wurde. Das alles ist mit der Verbreitung offener Netzwerke weitaus komplizierter geworden. Jedes Mal, wenn ein Gerät mit dem Netzwerk verbunden wird, entsteht ein neuer potentieller Gefahrenpunkt."

Netzwerk-Teams, die Daten erfassen und die Verkehrsmuster verstehen, können Baselines ermitteln und Alarme festlegen, die ausgelöst werden, wenn eine Abweichung von den normalen Parametern festgestellt wird.

Der 300-Dollar-Bandit

Finanzinstitute werden nicht nur durch betrügerische Kreditvergaben geschädigt. So hat O'Neill bereits Sicherheitsangriffe erlebt, bei denen das Geld in bar gestohlen wurde.

„Eine große Bank hatte nicht gemerkt, dass es nach Mitternacht viel ungewöhnlichen Netzwerkverkehr gab, weil sie niemals Baselines erstellt hatte", sagt O'Neill. „Die ganze Nacht über lief der Verkehr weiter und sie wussten es nicht, weil niemand das Netzwerk überwachte. Sie hatten keine Ahnung, was normal war. Also ließen sie es geschehen, obwohl es sich um einen Angriff gehandelt hatte."

O'Neill gelang es, den Verkehr zu identifizieren und was er herausfand, war schockierend.

„Da hat jemand jede Nacht die Geldautomaten an zehn oder zwölf Standorten angewiesen, jeweils 300 US-Dollar auszugeben", sagt er. „Und der Mann fuhr dann einfach die einzelnen Geldautomaten ab. Kaum kam er dort an, spuckte der Automat schon die 300 Dollar aus. Er griff sich die Scheine und verschwand. Das ging mehrere Wochen fast jede Nacht so, bevor jemand merkte, dass Geld abgehoben wurde und niemand wusste, von wem und von welchem Konto es kam. Das ist ein ideales Beispiel für auffälligen Verkehr."

Die richtigen Quelldaten erfassen

IT-Teams, die die IP-Verbreitung ihres Netzwerks verstehen und eine exakte Baseline erstellen möchten, müssen dafür normalerweise Netzwerkdaten erfassen. Doch ist es nicht nur für die oben genannten Ziele wichtig, die richtigen Quelldaten aufzuzeichnen. Diese Informationen sind darüber hinaus für viele Zwecke, angefangen bei einem umfassenden Überblick über die Ereignisse im Netzwerk bis zur Rekonstruktion der tatsächlichen Verkehrsströme, äußerst nützlich. Mit den erfassten Netzwerkdaten ist das Unternehmen zudem in der Lage, das Netzwerk zu überwachen, die aktuelle Situation zu erkennen, auf Zwischenfälle zu reagieren, Sicherheitsalarme festzulegen und andere Routine-Aufgaben zu erledigen.

Getarnter Netzwerkverkehr

Bei einem Unternehmen gelang es aufgrund des Überblicks, den der Netzwerktechniker über das Netzwerk hatte, in Verbindung mit den richtigen Quelldaten, einen verdächtigen Vorgang aufzuklären.

„Einmal fuhr ich zu einem Kunden, um dort eine Baseline zu erstellen, die unser Sicherheitskonzept bestätigen sollte", sagt Canney. „Wir haben uns mit dem Netzwerk verbunden und uns die Metadaten angesehen. Da fiel uns auf, dass in sehr kurzer Zeit Gigabytes von E-Mails übertragen wurden. Es war, als ob dieser Server von Hunderten oder Tausenden von Benutzern verwendet wurde oder riesige Anhänge per E-Mail verschickt wurden. Ich wies den Netzwerktechniker darauf hin und er meinte sofort, dass das kein E-Mail-Server sei.

Bei der Prüfung der Metadaten stellten Canney und der Techniker ein auffälliges Verkehrsmuster fest.

„Die Angreifer haben Verkehr über den offenen E-Mail-Port durch die Firewall getunnelt", sagt er. „Dieser Server war ein Primary Domain Controller (PDC), der Gigabytes übertrug, die wie E-Mails aussahen. Da gingen bei mir die Alarmlichter an. Als externer Berater bin ich mit den Namen der Server nicht vertraut. Der Techniker aber, der das Netzwerk kannte, kannte natürlich auch die Server."

Um die Inhalte der Payload zu identifizieren, begannen die beiden, Pakete aufzuzeichnen. Mithilfe der Trace-Dateien gelang es ihnen, einen laufenden Angriff zu erkennen.

„Wir haben das Netzwerk sofort vom Switch getrennt und es heruntergefahren. Die gute Nachricht war, dass wir den Angriff sofort mit den Trace-Dateien auswerten konnten. Die schlechte Nachricht lautete, dass wir nicht ausreichend Pakete aufgezeichnet hatten, um den Beginn des Angriffs zu erfassen. Wenn das Netzwerk-Team auf der Paketebene eine sorgfältige Überprüfung und Überwachung durchgeführt hätte, wäre bekannt gewesen, auf welche Dateien der Angreifer zugegriffen, in welche Richtung er sich bewegt und welche anderen verkehrsbasierten Systeme er kompromittiert hatte."

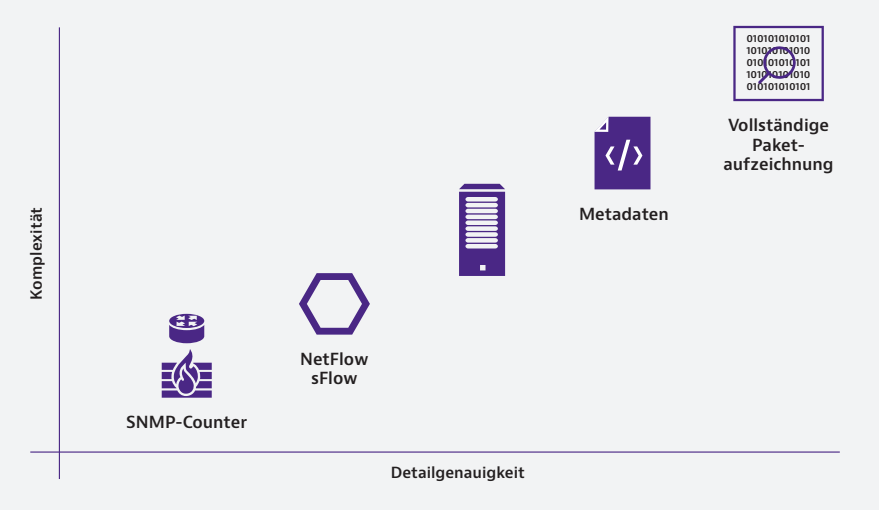
Die verschiedenen Datentypen verstehen

Netzwerktechniker nutzen verschiedene Tools und Datentypen, um die Integrität ihres Netzwerks zu gewährleisten. Dazu zählen SNMP-Counter, NetFlow, Metadaten und die vollständige Paketaufzeichnung (DPI).

Das folgende Diagramm verdeutlicht die Detailgenauigkeit, die diese gängigen Datenquellen im Verhältnis zur Komplexität ihrer Anwendung ermöglichen.

Detailgenauigkeit von Netzwerk-Datenquellen

1. SNMP-Counter
2. Syslogs
3. NetFlow
4. Metadaten
5. Vollständige Paketaufzeichnung



SNMP-Counter

SNMP-Counter zählen die Pakete und Bytes des Netzwerkverkehrs. Sie vermitteln einen guten Überblick über eventuelle Engpässe und andere Probleme. Da sie aber keine detaillierten Einblicke zulassen, sind sie für eine tiefgehende Fehlerdiagnose oder die Sicherheitsforensik wertlos. Allerdings können die Protokolle die Teams auf ungewöhnlichen Verkehr und abweichende Uhrzeiten aufmerksam machen.

Syslogs

Die Syslog-Überwachung ist ein passives Verfahren. Damit unterscheidet es sich von der kontinuierlichen, aktiven SNMP-Überwachung, die das gesamte Netzwerk erfasst. Der Studie 2017 State of the Network zufolge wird diese Form der Überwachung von Netzwerk-Teams am häufigsten genutzt, um Informationen zur Quelle möglicher Angriffe zu erhalten. Die gewonnen Daten sind ausreichend, um zu verstehen, welche Benutzer und Systeme auf spezifische Netzwerk-Ressourcen, wie Server, Dateien und Datenbanken, zugreifen. Aber Syslogs können keine Aussage dazu treffen, ob sich ein Angreifer erfolgreich für einen berechtigten Benutzer ausgibt, und auch keine tiefgehenden forensischen Nachweise liefern, wie es andere Datenquellen ermöglichen. Die Syslog-Daten werden für gewöhnlich zu Beginn einer Untersuchung geprüft.

NetFlow

Die NetFlow-Statistik ist eine gute Hilfe, um Baselines zu ermitteln und ungewöhnliche Verkehrsvolumen und ein auffälliges Verkehrsverhalten zu identifizieren. Wenn eine Überwachungslösung unerwartete Verkehrstypen oder -volumen erkennt, kann NetFlow die Baseline- und Alarme-Systeme informieren. Dieser Datentyp ist gut geeignet, um die Teams auf die Symptome eines Angriffs aufmerksam zu machen. Laut Cisco versetzt NetFlow den Anwender in die Lage, Verkehrsfluss-Statistiken an den Routern zu erfassen. NetFlow basiert auf der Identifikation von Paketströmen eingehender IP-Pakete. Die Software benötigt kein Protokoll zum Verbindungsaufbau, weder zwischen den Routern noch zwischen einem anderen Netzwerk- oder Endgerät. Auch erfordert NetFlow keine externen Änderungen, weder am Verkehr noch an den Paketen selbst oder an anderen Netzelementen.

Metadaten

Die Metadaten eines Netzwerks werden häufig genutzt, um die Lücke zwischen NetFlow und der vollständigen Paketaufzeichnung zu schließen. Der Begriff selbst ist relativ neu und noch nicht eindeutig definiert. Daher kann die Detailgenauigkeit schwanken. Typischerweise umfassen Metadaten bei einer SMB-Anwendung den Dateinamen und bei einer Web-Anwendung die URL. Metadaten werden häufig von Lösungen und Netzwerk-Tools verwendet, um Echtzeitansichten anzuzeigen und Probleme wie einen auffälligen Verkehr und eine zu langsame Übertragung zu untersuchen. Gleichzeitig vermitteln sie erste Einblicke für Sicherheitsuntersuchungen. Die Datenquelle lässt sich einfach zusammenfassen, sodass weniger Verarbeitungs- und Speicherressourcen als bei der vollständigen Paketaufzeichnung benötigt werden. Sie bietet sich für die Analyse von Langzeittrends an, die die Planung erleichtern sollen. Allerdings sind Metadaten und Kennwerte dahingehend beschränkt, dass sie den Teams zwar erlauben, die Symptome von Problemen zu untersuchen, die Granularität aber nicht ausreicht, um die eigentliche Ursache zu ermitteln. Der Wert der Metadaten erhöht sich, wenn zusätzlich eine Komplettaufzeichnung des Netzwerkverkehrs erfolgt. In dieser Kombination steht den Teams ein lückenloser Workflow zur Verfügung, um jede einzelne Sekunde eines Angriffs oder einer Datenrechtsverletzung zu identifizieren, zu untersuchen und vollständig zu rekonstruieren.

Vollständige Paketaufzeichnung

Die vollständige Paketaufzeichnung (DPI) stellt den Teams alle Beweise für Sicherheitsverletzungen und Leistungsstörungen zur Verfügung. So können sie alle Ereignisse im Netzwerk im konkreten Zusammenhang analysieren. Hierbei ist zu beachten, dass die vollständige, unbearbeitete Aufzeichnung und Speicherung der Pakete nicht nur erforderlich ist, um jeden Augenblick eines Angriffs zu rekonstruieren, sondern dass Gerichte dieses Verfahren auch bei Vorlage des Netzwerkverkehrs als Beweismittel verlangen können.

Auch ist es wichtig, mit einer handelsüblichen Lösung zu arbeiten, die den relevanten Verkehr für die Untersuchung schnell logisch zerlegen (parsen), analysieren und darstellen kann. Ohne diese Fähigkeit, kann es schwierig werden, die benötigten Pakete einzugrenzen. Zudem werden unter Umständen Tools zur Leistungsüberwachung benötigt, die den Zeitaufwand für die Untersuchung verringern, indem sie die Visualisierung und Analyse des Verkehrs rationalisieren. Ansonsten ist es möglich, dass das Team die reine Menge des Verkehrs nicht mehr handhaben kann.

Die folgende Tabelle erläutert den Anwendungsbereich der einzelnen Datenquellen bei der Überwachung und Untersuchung von Sicherheitsverletzungen.

Datenquellen

	Über-wachung	Fehler-diagnose	Forensische Untersuchung
SNMP-Counter	◒	○	○
Syslogs	○	●	◒
NetFlow	●	◒	○
Metadaten (Statistik)	●	◒	○
Vollständige Paketaufzeichnung (DPI)	◒	●	●

Wert der Datenquelle bei der jeweiligen Aktivität

○ Gering ◒ Ausreichend ● Hoch

Datenquellen und das Gesetz

Metadaten können vor Gericht als Beweismittel genutzt werden. Der Southern District von New York hat im Fall Aguilar gegen Immigration & Customs Enforcement Division (2008) Metadaten untersucht und nach den drei Typen „substanziell", „systembedingt" und „eingebettet" unterschieden.

- **Substanzielle** Metadaten werden „als Funktion der Anwendungssoftware erstellt, die verwendet wird, um das Dokument oder die Datei zu erstellen". Sie informieren über Änderungen am Dokument, wie frühere Bearbeitungen oder redaktionelle Kommentare.

- **Systembedingte** Metadaten „sind Informationen, die vom Benutzer oder dem Informationsmanagement-System des Unternehmens erstellt wurden" und umfassen Angaben zum Autor, zum Datum und zur Uhrzeit der Erstellung sowie zum Änderungsdatum des Dokuments.

- **Eingebette** Metadaten bestehen aus „Text, Zahlen, Inhalten, Daten oder sonstigen Informationen, die von einem Benutzer direkt oder indirekt in eine native Datei eingegeben wurden und die für den Benutzer, der die Bildschirmausgabe betrachtet, normalerweise nicht sichtbar sind." Beispiele für eingebettete Metadaten sind Formeln von Kalkulationstabellen, Hyperlinks und Datenbankangaben.

Darüber hinaus haben 48 US-Bundesstaaten, der District of Columbia, Guam, Puerto Rico und die Jungferninseln Gesetze erlassen, die Unternehmen und Behörden auffordern, natürliche Personen über Sicherheitsverletzungen bei personenbezogenen Daten zu informieren.

Für gewöhnlich umfassen Gesetze zu Sicherheitsverletzungen Bestimmungen, die festlegen, für wen das Gesetz gilt. Weiterhin enthalten sie eine Begriffsbestimmung der „personenbezogenen Daten", definieren, was eine Verletzung ist, und legen die Mitteilungspflichten, die Mitteilungsempfänger sowie die Ausnahmen fest.

In der Europäischen Union (EU) tritt im Mai 2018 die neue Datenschutz-Grundverordnung (DSGVO) in Kraft. Sie wird Auswirkungen auf alle Unternehmen haben, die Daten zu EU-Bürgern erfassen und kommunizieren.

EU-Arbeitsgruppen, die diese Verordnung ausgearbeitet haben, definieren personenbezogene Daten als Datensätze, die die folgenden Angaben beinhalten:

- Name, Adresse und Telefonnummer des Kunden,
- IP- oder MAC-Adresse eines Smartphones, Tablets oder Laptops,
- Passnummer,
- Daten von Zahlungskarten,
- Fotos, die zur Gesichtserkennung nutzbar sind.

Die wichtigste Bestimmung betrifft die Pflicht zur Benachrichtigung der natürlichen Personen, da diese Information sowohl in der Presse öffentlich gemacht als auch den zuständigen Aufsichtsbehörden mitgeteilt werden muss. Während die Metadaten vor Gericht sicherlich zugelassen werden und den Geschworenen/Schöffen häufig erlauben, einen allgemeinen Eindruck zu gewinnen, enthalten die Pakete die eigentlichen Beweise. Diese Pakete, die im Rahmen der Sicherheitsforensik genutzt werden, um einen Angriff zu rekonstruieren, können auch nachweisen, welche Angaben oder personenbezogenen Daten nicht kompromittiert wurden.

DDoS-Angriffe und viel Lärm um Nichts

„Vor etwa einem Jahr habe ich mit einem Finanzinstitut, das eine Sicherheitsverletzung bemerkt hatte, zusammengearbeitet", sagt Canney. „Es war das Ziel eines DDoS-Angriffs geworden und hat diesen nach 30 bis 60 Minuten erkannt. In diesem Fall handelte es sich um eine TCP-/HTTP-SYN-Flood. Die Netzwerktechniker haben die vollständigen Trace-Dateien der Pakete dieses spezifischen Angriffs untersucht, um herauszufinden, welches Ziel dieser verfolgte. Häufig wird ein DDoS-Angriff gestartet, um Aufmerksamkeit zu erregen. Anschließend dringen die Hacker mit einem anderen Trick durch die Hintertür in das Netzwerk ein. Oder in dem ganzen auffälligen Netzwerkverkehr versteckt sich ein Data-Mining-Angriff."

In diesem konkreten Fall hatte das Finanzinstitut jedoch alle Paketdaten aufgezeichnet und war daher in der Lage, die Trace-Dateien zu prüfen.

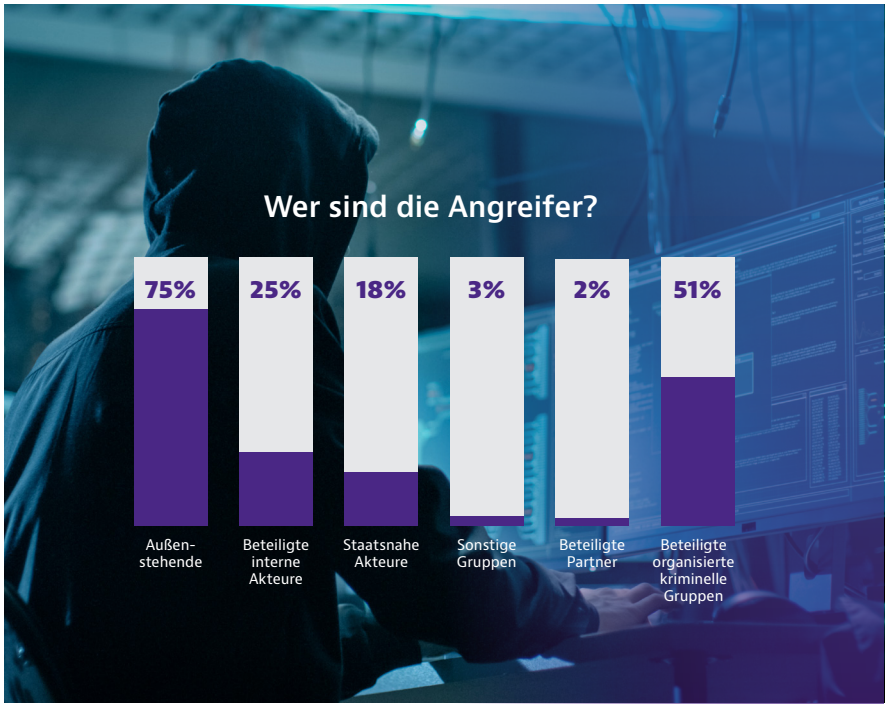
„Das Netzwerk-Team hat die Trace-Dateien untersucht, um zu erkennen, um welche Art von Angriff es sich handelte, worauf er abzielte sowie ob und wie weit er bereits die Firewall überwunden hatte", sagt Canney. „Nach Prüfung der Paketaufzeichnung vor und hinter der Firewall war klar, dass kein Hacker es geschafft hatte, in das Netzwerk einzudringen. Es war eben doch nur ein DDoS-Angriff. Wir haben uns die Trace-Dateien vor und hinter der Firewall angesehen.
Wir wussten genau, wie der Angriff funktionierte. Das Netzwerk-Team konnte die Geschäftsführung überzeugen und nachdem der DDoS-Angriff geklärt war, hatte das Finanzinstitut die beruhigende Gewissheit, dass alles vorbei war."

Da das Finanzinstitut in der Lage war zu bestätigen, dass keine sensiblen Daten betroffen waren, konnte es nachweisen, dass die Daten der Kunden sicher waren.

Ein Mitarbeiter öffnet einem Angreifer die Tür

Sicherheitsrichtlinien sollen ein Unternehmen, einschließlich der Mitarbeiter und deren Daten, schützen. Wenn ein Angestellter diese Richtlinien allerdings nicht einhält und eine Sicherheitsverletzung eintritt, sind alle gefährdet.

Dem FBI zufolge haben Angriffe auf E-Mail-Konten von Unternehmen und anderen Einrichtungen seit 2013 möglicherweise einen finanziellen Schaden in Höhe von 1,6 Milliarden US-Dollar in den USA und von 5,3 Milliarden US-Dollar weltweit verursacht.



Quelle: 2017 Verizon Data Breach Investigations Report - Executive Summary, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

„Daher haben viele Großunternehmen heute ziemlich strenge Zugriffsverfahren eingerichtet", sagt O'Neill. „So darf der Mitarbeiter seinen Computer immer nur für bestimmte Anwendungen nutzen und nur ausgewählte Internet-Seiten aufrufen. Und das sind dann die einzigen Windows-Dienste, die der Computer ausführen kann. Wenn ein Angestellter gegen eine Sicherheitsrichtlinie verstößt und eine Datenrechtsverletzung im Unternehmen verursacht, hat das Unternehmen das Recht, von dem Mitarbeiter Schadensersatz zu fordern sowie eine Anzeige zu erstatten. Wenn der Verstoß vorsätzlich erfolgte, kann ein Strafverfahren die Folge sein."

Ein Unternehmen, das seine normale IP-Verbreitung kennt, Baselines festgelegt hat und die richtigen Daten, also Pakete und Metadaten, aufzeichnet, ist eher in der Lage, die benötigen Beweise vorzulegen.

„In einem Unternehmen hatte ein Mitarbeiter eine Website besucht und einen Download gestartet, der einen Angriff auf das ganze Netzwerk ausgelöst hat", sagt O'Neill. „Vor Gericht konnte ich den Angriff dann in Bits, Bytes, Halbbytes und Oktets, wie sie beispielsweise durch die vollständige Paketaufzeichnung mit Observer GigaStor zur Verfügung stehen, beweisen. Ich konnte ihn mit den Syslogs zeigen. Ich konnte ihn anhand der NetFlow-Daten erläutern."

Um den hochtechnischen Sachverhalt einer typischen Jury aus zwölf Geschworenen verständlich zu machen, begann O'Neill mit den Metadaten und konkretisierte das entstehende Bild anschließend mit den verfügbaren Paketdaten.

„Mit den Metadaten konnte ich zeigen, dass der betreffende Mitarbeiter eine Website aufgesucht und eine Datei heruntergeladen hatte, die dann den Angriff auslöste", sagt er. „Die Metadaten verschaffen einen Gesamtüberblick." Das ist wie ein Video oder ein Foto. Anschließend kann man das Foto anhand der Paketdaten genauer untersuchen und auch jeden einzelnen Schritt während des Zugriffs prüfen. Der Mitarbeiter hatte gegen die Sicherheitsrichtlinien des Unternehmens verstoßen, sodass das Unternehmen weder fahrlässig noch schuldhaft gehandelt hatte.

Wenn die Daten aber zeigen, dass der Mitarbeiter häufig so vorgegangen war oder er der Vize-Präsident oder ein Vorstandsmitglied ist, dann muss er dafür die Verantwortung übernehmen."

> „Wenn Sie mit einem GigaStor mit lückenloser Paketaufzeichnung arbeiten, haben Sie einen unbefangenen Zeugen."
>
> – Tim O'Neill
>
> *Zertifizierter E-Commerce-Betrugsermittler*

Angesichts der immer komplizierteren Angriffe werden die meisten großen Unternehmen mit hoher Wahrscheinlichkeit irgendwann einmal von einer Sicherheitsverletzung betroffen sein. Doch mit den richtigen Daten und dem nötigen Überblick über das Netzwerk kann sich ein Unternehmen besser auf seine Beweisführung vor Gericht vorbereiten.

Quellen

Cisco Baseline Process Best Practices White Paper
https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15112-HAS-baseline.html

Cisco IOS Switching Services Configuration Guide, Release 12.2
https://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfnfc.html

Love My Tool: What is Network Metadata?
http://www.lovemytool.com/blog/2016/07/what-is-network-metadata-network-metadata-is-human-readable-data-that-describes-your-network-traffic-it-is-generated-and-c.html

2017 Verizon Data Breach Investigations Report - Executive Summary
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Security Ledger: Business Email Compromise is a $5 Billion Industry
https://securityledger.com/2017/05/fbi-business-email-compromise-is-a-5-billion-industry/

Carbanak: How would you have stopped a $1 billion APT attack?
https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/

Article 29 Data Protection Working Party Opinion 4/2007 on the concept of Personal Data
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

VIAVI Solutions

Kontakt +49 7121 86 2222

Sie finden das nächstgelegene
VIAVI-Vertriebsbüro auf
viavisolutions.de/kontakt

© 2017 VIAVI Solutions Inc.
Die in diesem Dokument enthaltenen Produktspezifikationen und Produktbeschreibungen können ohne vorherige Ankündigung geändert werden.

datasecurity-wp-ec-de
30186304 900 1017