Kurzvorstellung

Datenexfiltration einen Riegel vorschieben

Schützen Sie Ihre wertvollsten Unternehmensdaten.

Im **McAfee® Labs Threat-Report vom August 2015** werfen wir einen genauen Blick auf einen der wichtigsten Schritte beim Datendiebstahl: die Datenexfiltration. Hierbei kopiert oder verschiebt der Dieb oder Akteur Daten vom Netzwerk des Dateneigentümers auf ein vom Angreifer kontrolliertes Netzwerk.

In den letzten 10 Jahren nahm die Anzahl der Datenkompromittierungen und der davon betroffenen Personen sowie Unternehmen in noch nie dagewesenen Maße zu. Während es Datendiebe in der Vergangenheit nur auf Kredit- und Geldkartennummern abgesehen hatten, werden nun nahezu alle Informationen gestohlen, die wir im Internet angeben: Es fängt bei Namen, Geburtsdaten, Adressen sowie Telefonnummern an und reicht bis hin zu Gesundheitsdaten, Anmeldedaten für Konten und vielen weiteren Informationen.

Nicht nur Einzelpersonen sind Opfer dieser Angriffe. Vielmehr bedroht Internetspionage durch staatliche Stellen, organisierte Verbrecher und Hacktivisten die sensiblen Daten von Einzelpersonen und Unternehmen auf der ganzen Welt.

Bedrohungsakteure und deren Motive

Ein Bedrohungsakteur ist eine Person oder Gruppe, die nicht autorisierten Zugriff auf Computernetzwerke und Systeme erlangen möchte. Die Sicherheits-Community spricht bei ihrem Versuch einer Bedrohungsklassifizierung von drei Hauptakteuren: staatliche Stellen, organisierte Verbrecher und Hacktivisten. In der folgenden Tabelle werden die Motive sowie die potenziellen Datenarten aufgeführt, die für die jeweiligen Akteure interessant sind.

	Staatliche Stellen	Organisierte Verbrecher	Hacktivisten
Allgemeine Motive	Spionage Einflussnahme	Finanzieller Art	Rufschädigung Sozialer Art
Beispiele für Datenarten	Quell-Code E-Mails Interne Dokumente Militärische Aktivitäten Personenbezogene Informationen von Behördenmitarbeitern	Bankkontodaten Kreditkartendaten Personenbezogene Informationen (u. a. Steuernummer, Gesundheitsdaten usw.)	E-Mails Mitarbeiterdaten Alle sensiblen internen Daten
Volumen der verfolgten Daten	Klein – Groß	Groß	Klein – Groß
Qualität der Exfiltrationstechniken	Hoch	Mittel – Niedrig	Mittel – Niedrig
Speicherort im Netzwerk	Unbekannt / oft verstreut	Bekannt	Sowohl bekannt als auch unbekannt / oft verstreut

intel Security

Datenziele

Sobald ein Angreifer ein System auf dem Netzwerk kompromittiert hat, beginnt er damit, andere Systeme zu untersuchen und nach für ihn attraktiven Daten zu suchen. Da in einem komplexen Netzwerk viele Arten von Daten gespeichert sind, ist dieser Prozess für jeden Akteur ohne Insider-Wissen eine langwierige Aufgabe, die die Wahrscheinlich erhöht, erkannt zu werden. Aus diesem Grund versuchen Angreifer, so heimlich und dauerhaft wie möglich vorzugehen.

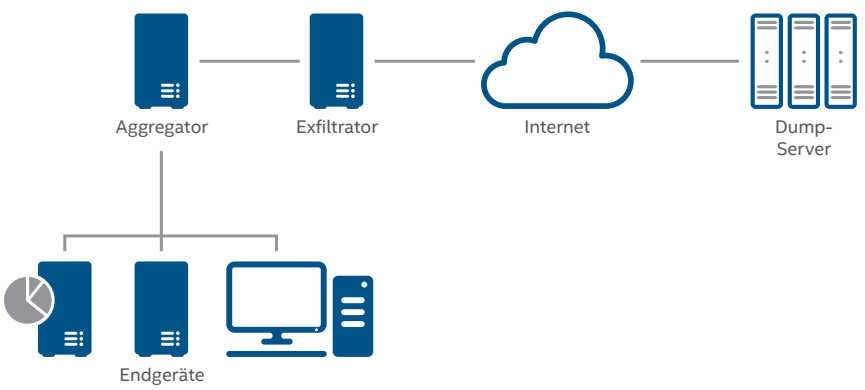
Zu den wichtigsten Datenzielen gehören:

Datenziel	Datenarten	Akteure, die sich dafür interessieren
Datenbanksysteme	Geschützte Gesundheitsinformationen, personenbezogene Informationen, Kreditkarten- und Bankdaten sowie Benutzerkonten	Organisierte Verbrecher, Hacktivisten
Quell-Code-Repositorys	Quell-Code, Anmeldedaten, Schlüssel	Staatliche Akteure, Hacktivisten
Spezialisierte Systeme	Verschieden	Alle, je nach Endgerätetyp
Dateifreigaben und ähnliche Systeme	Quell-Code, Entwürfe, Kommunikation usw.	Staatliche Akteure, Hacktivisten
E-Mail und Kommunikation	Entwürfe, Kommunikation	Staatliche Akteure, Hacktivisten

Datenexfiltration

Sobald die Bedrohungsakteure den Speicherort der gewünschten Daten gefunden haben, beginnt der schwerste Teil ihrer Arbeit: die Exfiltration des Schatzes. Dafür nutzen die Angreifer die Umgebung des Hosts als Mittler zwischen den Netzwerken des Opfers und des Angreifers. Diese Staging-Infrastruktur kann je nach Anzahl der Ebenen und Segmente des Ziels auf dem Netzwerk entweder komplex oder ganz einfach sein. Unter anderem können die Systeme folgende Rollen in einer Staging-Infrastruktur annehmen:

- **Endgeräte:** Einzelne oder mehrere Datenziele auf dem gleichen oder einem Routing-fähigen Segment zum Sammelgerät (Aggregator).
- **Aggregator:** Dient als Sammelstelle für Daten von den Zielendgeräten und lädt die Daten auf den Ausschleuser (Exfiltrator) herunter. Der Aggregator kann Zugang zum Internet haben. In raffinierten Kampagnen übertragen möglicherweise mehrere Aggregatoren Daten an verschiedene Exfiltratoren, um den Pfad der ausgehenden Daten zu verschleiern.
- **Exfiltrator:** Diese Komponente übernimmt Daten von einem Aggregator und ermöglicht deren Transport zum Dump-Server des Angreifers. Das kann über einen einfachen Transfer erfolgen. Es kann aber auch vorkommen, dass der Exfiltrator die Daten für den Angreifer aufbewahrt, bis dieser sie abruft.



Typische Architektur zur Datenexfiltration

Sowohl bei einem einfachen als auch bei einem komplexen Angriffsversuch möchte der Angreifer die kompromittierten Daten auf einen Server transportieren, der sich außerhalb des Netzwerks seines Opfers befindet. Dump-Server sind die ersten Systeme, bei denen sich gestohlene Daten außerhalb der Kontrolle des Unternehmens befinden, wodurch die Angreifer problemlos Zugriff darauf erlangen können. Als Dump-Server können folgende Komponenten fungieren:

- **Kompromittierte Systeme:** Systeme, die im Zuge einer separaten Kampagne vom Angreifer kompromittiert wurden. Beispiele für solche Systeme reichen von privaten WordPress-Blogs bis hin zu Servern von Unternehmen mit schwachen Sicherheitskontrollen.
- **Gehostete Systeme in bestimmten Ländern:** Länder mit strengen Datenschutzgesetzen sind für Angreifer attraktiv, weil sie innerhalb dieser Ländergrenzen ungestört Systeme hosten können, während sie gleichzeitig ein bestimmtes Maß an Schutz genießen.
- **Vorübergehend gehostete Systeme:** Kurzzeitige Systeme, die über Anbieter wie Amazon Web Services, Digital Ocean oder Microsoft Azure in der Cloud gehostet werden.
- **Dateifreigabe-Services in der Cloud:** Allgemein zugängliche Dateifreigabe-Seiten im Internet wie DropBox, Box.com oder Pastebin.
- **Cloud-basierte Services:** Andere Internet-basierte Services wie Twitter und Facebook, über die Benutzer Daten veröffentlichen können.

Datentransporte

Als Datentransporte werden die Protokolle und Verfahren bezeichnet, mit denen Diebe Daten von einem Speicherort oder System zu einem anderen kopieren. Dabei spielt es keine Rolle, ob der Kopiervorgang zwischen zwei internen Systemen (vom Endgerät zum Aggregator) oder von einem internen zu einem externen System (vom Exfiltrator zum Dump-Server) erfolgt. In der folgenden Tabelle sind einige der heute üblicherweise genutzten Transportmöglichkeiten zusammengefasst:

Transport	Beschreibung	Intern	Extern
HTTP / HTTPS	Durch die Dominanz von HTTP bei der Netzwerkkommunikation können über das HTTP-Protokoll exfiltrierte Daten hervorragend in anderem Datenverkehr versteckt werden. Es wird als allgemeines Transportmittel bei Exfiltrationen genutzt, indem Befehle in HTTP-Header und GET / POST / PUT-Methoden eingebettet werden.		■
FTP	Das FTP-Protokoll ist gemeinhin auf Unternehmens-Servern verfügbar. Die Interaktion über systemeigene Befehle ist einfach, wodurch dieses Protokoll eine unkomplizierte Transportmöglichkeit ist.	■	■
USB-Geräte	USB-Speichergeräte werden häufig für Exfiltrationen von Daten aus isolierten Netzwerken eingesetzt. Es gibt zum Beispiel Malware, die nach einem USB-Speichergerät mit einem bestimmten Marker sucht und dann die zu exfiltrierenden Daten in einen verborgenen Sektor des Speichergeräts kopiert. Die Exfiltration beginnt, wenn das Speichergerät an ein anderes infiziertes System mit Zugang zum Netzwerk angeschlossen wird. Darüber hinaus können Insider mithilfe von USB-Speichergeräten leicht große Mengen an Daten kopieren und aus dem Unternehmen tragen.	■	■
DNS	Spezifische DNS-Einträge wie TXT- oder sogar A- und CNAME-Einträge können bis zu einem gewissen Grad Daten speichern. Durch die Kontrolle einer Domäne und eines Name-Servers kann ein Angreifer kleine Datenmengen übertragen, indem er spezifische Suchen auf dem Exfiltrationssystem durchführt.		■
Tor	Das Tor-Netzwerk wird immer beliebter, gibt es doch Angreifern die Möglichkeit, exfiltrierte Daten auf schwer nachzuverfolgenden Servern zu posten. Tor-Datenverkehr auf Unternehmensnetzwerken ist jedoch selten legitim und kann daher leicht entdeckt und gestoppt werden.		■
SMTP / E-Mail	Sowohl über unternehmenseigene als auch über unternehmensfremde SMTP-Server können Daten in Form von Anhängen oder im Textteil von E-Mail-Nachrichten aus dem Unternehmen gelangen.		■
SMB	SMB ist ein äußerst weit verbreitetes Protokoll in Microsoft Windows-Umgebungen, das u. U. bereits auf Systemen aktiviert ist.	■	

Transport	Beschreibung	Intern	Extern
RDP	Das RDP-Protokoll unterstützt verschiedene Aktivitäten wie das Kopieren und Einfügen sowie Dateifreigaben. In manchen Fällen sind Systeme, die RDP zulassen, vom Internet aus zugänglich.	■	■
Benutzerdefinierte Transportprotokolle	Benutzerdefinierte Transportprotokolle werden teilweise bei der Kommunikation des Kontroll-Servers und bei ausgeklügelter Malware eingesetzt. Zuverlässige Datentransportprotokolle sind sehr aufwändig. Zudem können solche Protokolle aufgrund ihrer Einzigartigkeit problemlos auf dem Netzwerk identifiziert werden, was eine der etablierten Transportmöglichkeiten wieder attraktiver macht.	■	■

Datenmanipulation

Angreifer unternehmen alle notwendigen Schritte, um bei der Verarbeitung und Exfiltration sensibler Daten keine Spuren zu hinterlassen. Durch die Manipulation der Daten vor der Übertragung können die Erkennung erschwert, die Übertragungszeit reduziert und sogar die Zeit bis zur Entdeckung der Exfiltration erhöht werden. Zu den in dieser Phase häufigsten Manipulationstechniken gehören:

Technik	Beschreibung
Komprimierung	Das ZIP-Standardformat gewährt nicht nur ein gewisses Maß an Verschleierung, sondern beschleunigt auch die Dateiübertragung.
Chunking	Wenn Daten vor dem Versand in kleine Pakete aufgeteilt werden, kann die Übertragung besser in den regulären Netzwerkaktivitäten versteckt werden.
Verschlüsselung bzw. Verschleierung	Daten werden am häufigsten mittels einfacher Verschlüsselungs- und Verschleierungs-algorithmen manipuliert. Dank einfacher Techniken wie einer XOR-Operation mit einem statischen Schlüssel, der Base64-Verschlüsselung oder der einfachen Umwandlung aller Zeichen in das Hex-Format können die Daten ausreichend manipuliert werden, um eine Entdeckung zu vermeiden.
Verschlüsselung	Es ist verwunderlich, dass nicht alle Exfiltrationen verschlüsselt werden. Vielleicht liegt es an den Leistungseinbußen oder einfach nur daran, dass die Verschlüsselung nicht unbedingt erforderlich ist. Wenn die Daten dennoch verschlüsselt werden, geschieht dies in der Regel mittels RC4- oder AES-Verschlüsselung.

So kann Intel Security vor Datenexfiltration schützen

McAfee DLP Discover

Um Daten richtig schützen zu können, müssen Sie zuerst den Speicherort und das Wesen dieser Daten kennen. **McAfee DLP Discover** vereinfacht diesen ersten Schritt durch folgende Funktionen und schützt so vor Datenexfiltration:

- **Erkennung und Kontrolle vertraulicher Daten:** McAfee DLP Discover scannt automatisch alle verfügbaren Ressourcen und erstellt anschließend eine Inventarliste sowie einen Index, damit Sie Ihre sensiblen Daten unabhängig von deren Speicherort besser kennen. Mithilfe von McAfee DLP Discover können Sie Daten abfragen und auswerten. Darüber hinaus können Sie mit dieser Lösung feststellen, wie diese Daten verwendet werden, wem sie gehören, wo sie gespeichert werden und wohin sie ggf. übertragen wurden.
- **Überprüfung und Beseitigung von Verstößen:** Zum effektiven Schutz sensibler Daten werden Richtlinienverletzungen erkannt, Signaturen registriert sowie generiert und Warnmeldungen versandt. Dank Integration in Vorfall-Workflows und Fall-Verwaltung wird die Verbreitung sensibler Materialien zusätzlich eingeschränkt.
- **Unkomplizierte Festlegung von Schutzrichtlinien:** Die Lösung beinhaltet intuitive und einheitliche Funktionen zur Richtlinienerstellung sowie -verwaltung und zur Berichterstattung, damit Sie Ihre Informationsschutzstrategie besser kontrollieren können.

McAfee DLP Monitor

McAfee DLP Monitor sammelt, verfolgt und meldet Informationen zum Datenverkehr im gesamten Netzwerk. So können Sie unbekannte Gefahren für Daten erkennen, Maßnahmen zu ihrem Schutz einleiten und Ihr Unternehmen damit vor Dateneinbrüchen bewahren.

- **Überprüfung des Netzwerkverkehrs:** Die branchenweit führende McAfee DLP Monitor-Funktion zum Scannen und Analysieren von Daten unterzieht den Netzwerkverkehr einer Tiefenprüfung.
- **Schnelle Erkennung von Daten:** Mit der Echtzeiterkennung können Sie schnell erfassen, wie Daten verwendet werden, wer sie verwendet und wohin sie übertragen werden. Dadurch verfügen Sie über praktisch verwertbare Informationen. McAfee DLP Monitor kann mehr als 300 über beliebige Ports oder Protokolle übertragene Inhaltstypen erkennen, sodass Ihr Unternehmen jederzeit den vollen Überblick behält.
- **Durchführung detaillierter forensischer Analyse:** Forensische Analysen ermöglichen die Korrelation aktueller und vergangener Risikoereignisse sowie die Erkennung von Risikotrends und Bedrohungen, sodass Sie mit McAfee DLP Monitor Situationen schnell erfassen sowie adäquate Richtlinien und Verhaltensweisen entwickeln können.

McAfee DLP Prevent

McAfee DLP Prevent stellt sicher, dass Daten nur dann das Netzwerk verlassen, wenn es situationsgerecht ist – unabhängig davon, ob per E-Mail, Internet-E-Mail, Instant Messenger, über Wikis, Blogs, Portale, HTTP/HTTPS- oder FTP-Übertragungen. Die Lösung bietet damit Schutz vor Datenverlusten. Die schnelle Erkennung und Reaktion bei Exfiltrationsversuchen bewahrt Sie nicht nur vor dem Verlust wichtiger Daten, sondern auch vor negativen Schlagzeilen in den Medien.

- **Übersicht bei Sicherheitsvorfällen:** Dank angepasster Ansichten und Vorfallsberichte erhalten Sie eine Zusammenfassung sowie detaillierte Darstellungen von Sicherheitsvorfällen und den ergriffenen Behebungs-Maßnahmen.
- **Präventive Richtliniendurchsetzung bei allen Datentypen:** Die Lösung gewährleistet die Richtliniendurchsetzung bei offensichtlich sowie weniger offensichtlich vertraulichen Daten. Dank zahlreicher integrierter Richtlinien (z. B. für Compliance, zulässige Nutzung und geistiges Eigentum) können Sie ganze Dokumente oder Teile davon mit einem umfassenden Satz von Regeln abgleichen, sodass alle sensiblen Informationen geschützt werden.

McAfee DLP Endpoint

Mit **McAfee DLP Endpoint** können Sie Datenexfiltrationen innerhalb und außerhalb des Unternehmens sowie in der Cloud überwachen und verhindern. Sie können Vorgänge schnell und einfach in Echtzeit überwachen, zentral verwaltete Sicherheitsstrategien anwenden sowie detaillierte forensische und Datenverbreitungsberichte erstellen, ohne den laufenden Geschäftsbetrieb zu beeinträchtigen.

- **Erweiterte Unterstützung von Virtualisierung:** Benutzerspezifische Richtlinien können für mehrere Sitzungen und VDIs durchgesetzt werden, wodurch Sie mehr Flexibilität und eine bessere Kontrolle des Datenflusses zu gemeinsam genutzten Terminals erhalten.
- **Umfassende Ereignisberichte und Überwachung:** Die Lösung sammelt alle für exakte Analysen, Untersuchungen und Audits sowie zur Risikobewertung und Problembehebung erforderlichen Daten wie Absender, Empfänger, Zeitstempel und Datenspuren.
- **Zentrale Verwaltungskonsole:** Die Verwaltungskonsole McAfee® ePolicy Orchestrator® (McAfee ePO™) wird für die Definition von Richtlinien, die Ausbringung und Aktualisierung von Agenten, die Überwachung von Echtzeitereignissen sowie die Generierung von Berichten zur Einhaltung von Compliance-Anforderungen genutzt.

- **Umfassendes Content-Management:** Sie erhalten die Möglichkeit zur Kontrolle und Blockierung von Kopien vertraulicher Daten auf USB-Geräten, Flash-Laufwerken, Smartphones und anderen externen Speichermedien, einschließlich optischer Medien und Papierausdrucken. Durch die Integration von DLP- und DRM-Lösungen (Digital Rights Management) erhalten Sie zudem Schutz, der über Ihr Netzwerk hinausgeht.

McAfee Device Control

McAfee Device Control schützt Ihre Daten davor, durch Wechselspeichermedien und -datenträger wie USB-Laufwerke, Smartphones, CDs oder DVDs exfiltriert zu werden. Ihr Unternehmen kann Datenübertragungen von allen Desktops und Laptops überwachen sowie kontrollieren – egal, ob die Daten innerhalb oder außerhalb des Unternehmens gespeichert sind. McAfee Device Control bietet Funktionen zur inhaltlichen oder situationsabhängigen Sperrung von Geräten, darunter:

- **Umfassende Geräte- und Datenverwaltung:** Sie können kontrollieren, wie Mitarbeiter Ihres Unternehmens Daten auf USB-Laufwerke, Smartphones, beschreibbare CDs und DVDs sowie viele andere für Datenexfiltrationen geeignete Geräte kopieren.
- **Fein abgestufte Kontrollfunktionen:** Sie können nicht nur festlegen, welche Geräte genutzt und welche Daten auf zugelassene Geräte kopiert werden dürfen, sondern auch das Kopieren von Daten von bestimmten Orten und Anwendungen durch die Benutzer einschränken.
- **Fortschrittliche Reporting- und Audit-Funktionen:** Detaillierte Protokolle auf Anwender- und Geräteebene vereinfachen die Einhaltung von Compliance-Vorschriften. Details wie Gerät, Zeitstempel und Datenspuren werden problemlos protokolliert und weitergemeldet, um Audit- und Compliance-Anfragen zu unterstützen.
- **Zentrale Verwaltung:** Die Integration in die Software McAfee ePO ermöglicht die Echtzeitüberwachung von Ereignissen sowie die zentrale Verwaltung von Richtlinien und Zwischenfällen.

McAfee Next Generation Firewall

Schützen Sie sich mit **McAfee Next Generation Firewall** vor Angriffen, die hochentwickelte Verschleierungstechniken einsetzen. McAfee Next Generation Firewall führt eine spezielle Pakettiefenprüfung, vollständige Stack-Normalisierung und horizontale Datenstrom-basierte Überprüfungen durch, um Datenverkehranomalien wie Malware-Kommunikation mit dem Kontroll-Server oder Datenexfiltrationen aus Ihrem Netzwerk aufzudecken.

- **Abwehr hochentwickelter Verschleierungstechniken:** Die Lösung umfasst Funktionen wie mehrstufige Datenverkehrnormalisierung, Schwachstellen-basierte Fingerabdrücke und Protokoll-unabhängigen Abgleich von Fingerabdrücken.
- **Erkennung von Kontroll-Server-Aktivitäten:** Zur Erkennung von Botnet- und Kontroll-Server-Aktivitäten kommen Entschlüsselung sowie Sequenzanalysen der Nachrichtenlänge zum Einsatz.
- **Blockierung anhand des geografischen Standorts:** Ein- und ausgehende Verbindungen mit Ländern, in denen Ihr Unternehmen nicht aktiv ist, können blockiert werden. Dadurch verringert sich die Wahrscheinlichkeit dafür, dass die Befehle von Kontroll-Servern von IP-Adressen eingehen, die nicht mit Ihrer Umgebung kommunizieren sollten.

62071brf_stop-data-exfiltration_0815

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com