Kurzvorstellung

Verhinderung von Datenlecks im Unternehmen

Daten fließen bei den meisten Unternehmen ab. Manchmal gelangen sie über Insider nach draußen, doch meist werden sie von externen Akteuren gestohlen. Die Formen und Kanäle zur Exfiltrierung der Daten sind vielfältig. Unternehmen versuchen aus unterschiedlichen Gründen und mit wechselndem Erfolg, diesen Informationsfluss zu unterdrücken. Intel Security gab die *Intel Security 2016 Data Protection Benchmark Study* (Intel Security-Umfrage zu Datenschutz-Benchmarks 2016) in Auftrag, um die Motivationen der Angreifer, die Art der gestohlenen Daten sowie die Exfiltrationswege aus dem Unternehmen besser zu verstehen.

Im *McAfee Labs Threat-Report vom September 2016* haben wir die Umfragedaten analysiert und unsere Erkenntnisse im Detail vorgestellt. Unter anderem fanden wir Folgendes heraus:

- Die Lücke zwischen einer Datenkompromittierung und ihrer Erkennung wird größer.
- Dienstleister und Hersteller im Gesundheitswesen sind nicht auf Gefahren eingestellt.
- Die typischen Schutzmaßnahmen gegen Datenkompromittierung sind bei neuen Diebstahlzielen zunehmend ineffektiv.
- Die meisten Unternehmen kümmern sich nicht um die zweithäufigste Ursache für Datenkompromittierungen.
- Schutz vor Datenkompromittierung wird aus gutem Grund eingesetzt.
- Transparenz ist unverzichtbar.

Empfohlene Richtlinien und Verfahren zum effektiven Schutz vor Datenkompromittierung

Für Unternehmen ist es unverzichtbar, Richtlinien und Verfahren zum Schutz vor Datenkompromittierung zu implementieren, um die ungewollte oder absichtliche Übertragung vertraulicher Daten an nicht autorisierte Dritte zu verhindern. Eine erfolgreiche Initiative zum Schutz vor Datenkompromittierung beginnt schon in der Planungsphase mit der Definition der geschäftlichen Anforderungen. Beispielsweise sollte die Anpassung von Datenklassifizierungs- und Datenkompromittierungsrichtlinien an die Datenschutzrichtlinien und Datenweitergabestandards des Unternehmens bereits in der Planungsphase erfolgen. Mit der Einführung sinnvoller geschäftlicher Anforderungen kann sich die Initiative zum Schutz vor Datenkompromittierung auf die richtigen Stellen konzentrieren – und eine unnötige Ausweitung wird vermieden.

intel Security

Ein weiterer wichtiger Schritt bei einer solchen Initiative ist die Erkennung vertraulicher Daten innerhalb des Unternehmens. Technologien zum Scannen von Servern und Endgeräten ermöglichen die Klassifizierung von Dateien mithilfe regulärer Ausdrücke, Wörterbücher sowie unstrukturierter Datentypen. Produkte zum Schutz vor Datenkompromittierung bieten häufig integrierte Klassifizierungen für typische Kategorien vertraulicher Daten, beispielsweise Zahlungskartendaten oder Gesundheitsdaten, die den Erkennungsprozess beschleunigen können. Es können jedoch auch individuelle Klassifizierungen erstellt werden, um Datentypen zu definieren, die für das jeweilige Unternehmen einmalig sind.

Dieser Schritt wird erschwert durch von der IT-Abteilung zugelassene sowie nicht zugelassene Anwendungen und ihre zugehörigen Daten in der Cloud. Bei von der IT-Abteilung zugelassenen Daten in der Cloud kann und sollte die Erkennung vertraulicher Daten beim Abonnieren des Cloud-Dienstes bereits Teil des Prozesses sein. In diesem Fall lässt sich dieser Datentyp relativ leicht klassifizieren.

Abteilungen innerhalb von Unternehmen umgehen jedoch häufig die IT-Abteilung, um ihre geschäftlichen Ziele zu erreichen, indem sie in Eigeninitiative Cloud-Dienste abonnieren. Wenn die IT-Abteilung nichts von diesen Diensten und ihren Daten weiß, steigt die Wahrscheinlichkeit für eine Datenkompromittierung. Aus diesem Grund sollten die Unternehmensabteilungen in diesem Schritt einbezogen werden, um die Speicherorte von Daten in der Cloud zu identifizieren und diese Daten im zuvor genannten Prozess zu klassifizieren.

Sobald der Erkennungsprozess für vertrauliche Daten abgeschlossen ist, bietet die Implementierung von Produkten zum Schutz vor Datenkompromittierung im vertrauenswürdigen Netzwerk sowie auf allen Endgeräten Übersicht und Kontrolle für wichtige ruhende sowie übertragene Daten. Um den unerwarteten Zugriff auf vertrauliche Daten oder ihre Übertragung zu erkennen, sollten Richtlinien implementiert werden. Ereignisse wie die Übertragung vertraulicher Daten auf USB-Geräte oder über das Netzwerk an einen externen Speicherort können ein ganz normaler Geschäftsprozess sein, aber ebenso gut eine absichtliche bzw. ungewollte Aktion, die zu Datenlecks führt.

Effektive Schulungen zur Verbesserung des Sicherheitsbewusstseins können die Wahrscheinlichkeit von Datenkompromittierungen verringern. Informationsmeldungen können helfen, die Benutzer zu zulässigen Aktionen bei der Übertragung vertraulicher Daten zu schulen und ihnen im Rahmen ihrer täglichen Arbeit die Funktionsweise von Datenschutzrichtlinien nahezubringen. Diese Meldungen können die Benutzer beispielsweise darüber informieren, dass ihre Übertragung vertraulicher Daten gegen eine Richtlinie verstößt, und Alternativen anbieten (z. B. vorschlagen, die vertraulichen Daten vor der erneuten Übertragung bearbeiten).

Die Eigentümer von Daten kennen diese meist besser als andere Unternehmensabteilungen. Dateneigentümer sollten dabei unterstützt werden, die Datenkompromittierungen zu beheben. Wenn die Aufgaben zwischen den Dateneigentümern und dem Sicherheitsteam aufgeteilt werden, verringert das die Wahrscheinlichkeit, dass ein einziges Team gegen die Datenschutzrichtlinien verstößt.

Sobald bestätigte Datenübertragungen definiert und die entsprechenden Richtlinien in Produkten zum Schutz vor Datenkompromittierung implementiert wurden, können die Richtlinien zum Blockieren unzulässiger Übertragungen vertraulicher Daten aktiviert werden. Dadurch werden die Benutzer an Aktionen gehindert, die gegen die Richtlinien verstoßen. Wenn der Geschäftsbetrieb dies erfordert, können die Richtlinien flexibel angepasst werden, sodass die Benutzer ihre Aufgaben erfüllen können und dennoch geschützt sind.

Nach der Einführung der Initiative zum Schutz vor Datenkompromittierung müssen die Richtlinien in festgelegten Abständen überprüft und angepasst werden. Manchmal sind Richtlinien zu restriktiv oder zu lax, sodass die Produktivität beeinträchtigt wird oder Sicherheitsrisiken entstehen.

So kann Intel Security vor Datenlecks 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:

- Legen Sie Klassifizierungen zur Erkennung von Daten in der vertrauenswürdigen Umgebung fest. Verwenden Sie hierfür die integrierten (z. B. HIPAA, PCI, SOX) oder benutzerdefinierte Klassifizierungen.
- Führen Sie einen Inventar-Scan durch, und prüfen Sie die Ergebnisse anhand der Klassifizierungen, um zu verstehen, wo sich welche Datentypen in der vertrauenswürdigen Umgebung befinden. Suchen Sie in der McAfee DLP Discover-Benutzeroberfläche nach Verletzungen der aktuellen Richtlinie.
- Führen Sie einen Behebungs-Scan durch, um Daten zu finden, die an nicht autorisierten Speicherorten abgelegt sind, und verschieben Sie diese Daten an einen autorisierten Speicherort.
- Inventar- und Behebungs-Scans können für lokale Ressourcen wie Netzwerkfreigaben oder Cloud-Ressourcen wie Box durchgeführt werden.
- Erstellen Sie basierend auf den Ergebnissen des McAfee DLP Discover-Scans neue Datenschutzrichtlinien.

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.

- Erstellen Sie nach Abschluss der Erkennungsphase Datenschutzrichtlinien, die Richtlinienverletzungen melden. Dadurch werden die notwendigen Daten bereitgestellt, um die Datenübertragung im Unternehmen besser zu verstehen und die Durchsetzung von Blockierungsregeln zu ermöglichen. McAfee DLP enthält integrierte Klassifizierungen (z. B. für HIPAA, SOX, PCI und ITAR), mit denen Daten innerhalb des Unternehmens identifiziert werden können.
- Erstellen Sie Coaching-Seiten für Benutzer, damit diese bei alltäglichen Datenübertragungen die Datenschutzrichtlinien besser verstehen und einhalten. Diese benutzerdefinierten Informations-Pop-Up-Meldungen sind sehr nützlich und verringern gefährliche Datenübertragungen durch Mitarbeiter.
- Rufen Sie den Vorfall-Manager auf, um die Eigenschaften der an nicht autorisierte Speicherorte übertragenen Daten zu untersuchen. Dazu gehören Informationen dazu, wie die Übertragungen durchgeführt werden und wer dafür verantwortlich ist.
- Aktivieren Sie nach der Erstellung und Optimierung der Datenschutzrichtlinien die Blockierung nicht autorisierter Datenübertragungen.
- Aktivieren Sie manuelle Klassifizierungen, damit die Benutzer selbst erstellte Dokumente klassifizieren können. Wenn das automatisierte Klassifizierungsmodul keine strukturierten Daten erkennen kann, wissen sie als Eigentümer der Daten wahrscheinlich am besten, ob es sich um vertrauliche Dokumente handelt. Diese Funktion ist in McAfee DLP Endpoint integriert und erfordert keine zusätzlichen Tools von Drittanbietern.
- Erstellen und implementieren Sie für zusätzlichen Schutz eine Zugriffsschutzregel für Anwendungen, die mithilfe von McAfee Threat Intelligence Exchange verhindert, dass unbekannte Anwendungen auf vertrauliche Daten zugreifen können. Dadurch können autorisierte Anwendungen vertrauliche Daten übertragen, während der Zugriff nicht verifizierter oder böswilliger Anwendungen darauf blockiert wird.

McAfee DLP Monitor
McAfee DLP Monitor sammelt, verfolgt und meldet Informationen zum Datenverkehr im gesamten Netzwerk. Sie können problemlos Bedrohungen für Daten aufdecken und Maßnahmen zu ihrem Schutz ergreifen.

- Aktivieren Sie relevante integrierte Richtlinien zur Erkennung potenzieller Verletzungen innerhalb des Netzwerks.
- Zusätzlich können Sie benutzerdefinierte Richtlinien und Regeln erstellen, z. B. zur Überwachung der Übertragung vertraulicher Daten in die Cloud.
- Forensische Analysen ermöglichen die Korrelation aktueller und vergangener Risikoereignisse sowie die Erkennung von Risikotrends und Bedrohungen. Mit McAfee DLP Monitor können Sicherheitsexperten Situationen schnell erfassen sowie adäquate Richtlinien und Verhaltensweisen entwickeln.
- Erstellen Sie zusätzliche Capture Filter zum Ausschließen irrelevanter Daten und Optimieren von Regeln zur Minimierung von False-Positives.
- Konfigurieren Sie Warnungen, die beim Verstoß gegen Richtlinien an Absender, Empfänger, Dateneigentümer sowie Systemadministratoren gesendet werden.

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.

- Integrieren Sie McAfee DLP Prevent mithilfe enthaltener Richtlinien in Web-Proxys und Message Transfer Agents, um nicht autorisierte Datenübertragungen über E-Mail-Gateways oder Web-Proxys zu verhindern.
- Erstellen Sie Regeln in McAfee DLP Prevent zum Zulassen oder Blockieren vertraulicher Dokumente anhand des Übereinstimmungswerts.
- Verhindern Sie mithilfe integrierter DLP-Vorlagen, dass vertrauliche Daten in die Cloud übertragen werden.
- Überprüfen Sie Berichte zu Sicherheitsvorfällen, und passen Sie die Richtlinien an, um False-Positives zu minimieren und einen störungsfreien Geschäftsbetrieb zu gewährleisten.
- Konfigurieren Sie Warnungen, die beim Verstoß gegen Richtlinien an Absender, Empfänger, Dateneigentümer sowie Systemadministratoren gesendet werden.

Weitere Informationen
Intel Security Expert Center Center-Community

- McAfee Data Loss Prevention

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