VARONIS + FIREEYE TAP

Unternehmen speichern riesige Mengen unstrukturierter Daten – Dateien und E-Mails – darin enthalten sind zahlreiche der wichtigsten Vermögenswerte eines Unternehmens. Genau diese Vermögenswerte sind es, die häufig bei Sicherheitsverstößen gestohlen werden – entweder von Insidern, die ihre Zugriffsrechte missbrauchen (wie Snowden), oder durch Outsider, die sich Zugangsdaten von Insidern aneignen (wie es bei Sony der Fall war).

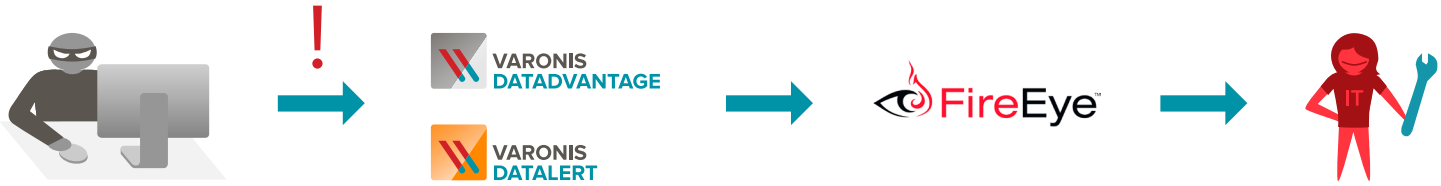
Unternehmen sind mit sich stetig ändernden Technologien und Bedrohungen konfrontiert. Die Netzwerkgrenzen zu sichern ist nicht mehr länger ausreichend, um sich vor Angreifern zu schützen. Dazu kommt, dass Benutzer, die sich bereits im Inneren des Netzwerks befinden deutlich mehr Zugriff auf Daten haben als sie bräuchten. Am schwersten wiegt jedoch die Tatsache, dass Unternehmen oft erst Monate nach einem Angriff – wenn überhaupt – darüber informiert werden. Der Grund: das Benutzerverhalten wird auf vielen internen Systemen nur selten überwacht und im Hinblick auf potenziellen Missbrauch hin analysiert.

Varonis hat bereits tausenden von Kunden geholfen, ihre unstrukturierten Daten durch die Analysen des Benutzerverhaltens bei Dateien und E-Mails, Berechtigungen und Metadaten von Dateisystemen, aber auch durch Analysen des Dateiinhalts zu schützen.

In einer informellen E-Mail-Umfrage haben 31 % der 141 teilnehmenden Varonis-Kunden angegeben, dass sie dank unserer Lösungen bereits verdächtige Insider-Aktivitäten oder Malware erkannt haben.

FireEye-Kunden erhalten gebündelte Informationen zu Bedrohungen aus verschiedensten Quellen, einschließlich IDS/IPS, DLP, Geschäftsanwendungen und Firewall-Logs.

Mit der Integration von Varonis und FireEye TAP erhalten die Kunden von Varonis und FireEye ein **umfängliches Wissen** über ihre unstrukturierte Daten – den Daten, von denen Unternehmen die meisten haben und über die sie gleichzeitig am wenigsten wissen. Von der anfänglichen Sondierung, über das Herausschleusen der Daten und die Verschleierung des Angriffs; Varonis und FireEye TAP helfen Ihnen dabei, die Warnzeichen zur erkennen, bevor Sie sich in den Schlagzeilen der Medien wiederfinden.



BEDROHUNGEN SOFORT ERKENNEN

Sie können Varonis DatAdvantage und DatAlert problemlos mit FireEye TAP integrieren und folgende Ereignisse identifizieren:

- Statistisch ungewöhnliches Benutzerverhalten
- Massenhaft vorgenommene Löschungen und Veränderungen
- Malware– und Ransomware-Infektionen, wie CryptoLocker und Cryptowall
- Rechteausweitungen
- Administrativer Zugriff auf Benutzerdaten
- Ungewöhnlicher oder administrativer Zugriff auf PII
- Hohe Zahlen fehlgeschlagener Login-Versuche
- Änderungen, die außerhalb des dafür bestimmten Fensters gemacht werden
- Weitere mehr

Die Installation von Varonis DatAdvantage und DatAlert kann bereits innerhalb einer Stunde abgeschlossen werden und die Integration mit FireEye TAP ist nicht schwieriger als eine IP-Adresse zu konfigurieren.

ÜBER DATADVANTAGE

Varonis DatAdvantage stellt sicher, dass nur die richtigen Personen jederzeit Zugriff auf die richtigen Daten haben, sowie dass alle Aktivitäten überwacht werden und Missbrauch gemeldet wird.

Varonis sorgt für einen Rundumschutz Ihrer Daten und verwendet maschinelles Lernen, um Muster und ungewöhnliches Verhalten zu erkennen und Verstöße zu stoppen, bevor sie Schaden anrichten.

ÜBER DATALERT

Varonis DatAlert löst Meldungen in Echtzeit über mehrere Plattformen hinweg aus, basierend auf Datei– und E-Mail-Aktivität, Berechtigungsänderungen und anderen kritischen Ereignissen. Damit erkennen Sie potentielle Sicherheitsverstöße, Fehlkonfigurationen und anderen Probleme in Echtzeit.

ÜBER VARONIS

Varonis ist ein führender Anbieter von Software-Lösungen für unstrukturierte, nutzergenerierte Unternehmensdaten.

Varonis bietet eine innovative Software-Plattform, mit der Unternehmen ihre unstrukturierten Daten abbilden, analysieren, verwalten und migrieren können. Erfahren Sie mehr unter www.varonis.com.

Varonis Kostenlos 30 Tage Lang Testen:

INNERHALB WENIGER STUNDEN NACH DER INSTALLATION:

Können Sie sofort eine Berechtigungsüberprüfung durchführen: Kontrolle von Zugriffsberechtigungen auf Dateien und Ordner sowie deren Zuweisung zu bestimmten Benutzern und Gruppen. Sie können sogar Berichte erstellen.

INNERHALB EINES TAGES NACH DER INSTALLATION:

Beginnt Varonis DatAdvantage Ihnen die Arten und Benutzer des Zugriffs aufzuzeigen.

INNERHALB VON 3 WOCHEN NACH DER INSTALLATION:

Erstellt Varonis DatAdvantage zuverlässige Empfehlungen dazu, wie der Zugriff auf Dateien und Ordner beschränkt werden kann, sodass nur die richtigen Personen Zugriff darauf haben.

ÜBER FIREEYE

FireEye ist führend in der Bereitstellung von Cybersicherheitslösungen, um die wertvollsten Vermögenswerte vor Angreifern zu schützen. Durch die Kombination von Technologie, Intelligenz und Fachwissen – zusammen mit dem offensivsten Team um Vorfälle zu beheben – begren-zen wir die Auswirkungen von Sicherheitsverstößen.