Fraunhofer

FORSCHUNG KOMPAKT

Profilbasierte Anomalieerkennung für SIEM-Systeme

Datenklau – schnell entdeckt!

Computerexperten haben bislang kaum eine Chance, Unternehmen oder Behörden dauerhaft vor Netzwerkeinbrüchen zu schützen. Zu zahlreich und wenig aussagekräftig sind die Ereignisse, die auf mögliche Hacker-Angriffe hindeuten. Mit PA-SIEM bekommen IT-Verantwortliche ein effektives Werkzeug an die Hand. So können sie Datenklau und Co. schneller entlarven und Daten besser schützen.

Bundestag gehackt – diese Meldung sorgte im Jahr 2015 für Schlagzeilen. Das Bedenkliche dabei: Der Datenklau blieb geraume Zeit unbemerkt, nur durch Zufall wurde er entdeckt. 16 Gigabyte Daten, vor allem Dokumente, E-Mails und Tastatureingaben, waren zu diesem Zeitpunkt schon in unbefugte Hände gelangt. Gefahr droht neben Behörden auch Unternehmen und anderen Organisationen. Als Einfallstor dienen den Angreifern häufig Phishing-Emails, über die sie Zugriff auf die Computer der Empfänger erhalten, oder aber sie infizieren regelmäßig besuchte Webseiten. IT-Sicherheitsexperten haben dem momentan noch wenig entgegenzusetzen. Zwar laufen in vielen Organisationen Ereignismeldungen in SIEM-Systemen zusammen, kurz für »Security Information and Event Management«. Diese enthalten jedoch riesige Mengen von Meldungen über den täglichen Betrieb – etwa darüber, welche Benutzer sich angemeldet haben oder welche Internetseiten geöffnet wurden. Für die Computerexperten ist es ein Ding der Unmöglichkeit, in der nicht enden wollenden Datenflut die auf einen Einbruch hindeutenden Meldungen zu finden. Ergo: SIEM-Systeme gleichen oft einem Datengrab.

Hinweise in Ereignismeldungen erkennen und korrelieren

Künftig ist es möglich, Netzwerkangriffen schneller auf die Spur zu kommen. Möglich macht es die Software PA-SIEM, kurz für »Profilbasierte Anomalieerkennung für SIEM-Systeme«. Entwickelt wird sie von Forschern am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE in Bonn und ihren Kollegen der Ostbayerischen Technischen Hochschule OTH Regensburg und der NETZWERK GmbH im gleichnamigen Projekt des Bundesministeriums für Bildung und Forschung BMBF. »Statt Angriffe lediglich durch vorher festgelegte Regeln zu erkennen, berechnet PA-SIEM typische Angriffsmuster auch aus unvollständigen oder schwachen Hinweisen«, sagt Rafael Uetz, Wissenschaftler am FKIE. »Auf diese Weise lassen sich Netzwerkeinbrüche deutlich effektiver und schneller erkennen.«

Kontakt
Janis Eitner | Fraunhofer-Gesellschaft, München | Kommunikation | Telefon +49 89 1205-1333 | presse@zv.fraunhofer.de
Silke Wiesemann | Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE | Telefon +49 228 9435-103 | Fraunhoferstraße 20 | 53343 Wachtberg | www.fkie.fraunhofer.de | silke.wiesemann@fkie.fraunhofer.de

Die Forscher setzen dabei auf einen dreistufigen Prozess: Zunächst einmal sammelt die SIEM-Software wie bisher die Ereignismeldungen der einzelnen Arbeitsplatz-PCs und Server. Im zweiten Schritt durchsuchen spezielle Algorithmen diese Ereignismeldungen auf bekannte Hinweise sowie auf Anomalien, also auf Abweichungen vom üblichen Verhalten. Die Suchergebnisse können auf einen Einbruch hinweisen, müssen dies aber nicht zwangsläufig. Sendet ein PC beispielsweise plötzlich auffällig viele Daten ins Internet, so kann es sich dabei um einen Einbruch handeln – oder aber der Mitarbeiter schickt lediglich außergewöhnlich große Dokumente an einen Kunden. Systeme, die solche Anomalien erkennen, gibt es bereits. Allerdings haben sie meist eine hohe Falsch-Positiv-Rate. Selbst wenn diese nur bei einem Promille liegt – also eine von hundert Meldungen fälschlicherweise als Bedrohung gesehen wird – laufen bei den Computerexperten je nach Größe des Unternehmens schnell mehrere Tausend Alarme pro Tag auf.

Ereignisketten sind der Weg zum Ziel

»Der Clou liegt quasi im dritten Schritt: Wir kombinieren die Hinweise und können die Fehlerrate somit stark senken«, erläutert Uetz. Ein vereinfachtes Zahlenbeispiel erläutert das: Bei einem Ereignis, das zu neunzig Prozent durch einen Angriff ausgelöst wurde, läge die Falsch-Positiv-Rate bei zehn Prozent. Reiht man zwei solcher Meldungen hintereinander – kommt also etwa eine E-Mail mit einem PDF-Anhang an und steigt später die ins Internet gesendete Datenmenge – sinkt diese Rate bereits auf ein Prozent – also auf zehn Prozent von zehn Prozent –, bei einer Dreier-Verknüpfung gar auf 0,1 Prozent. Eine solche Ereigniskette, Experten sprechen von der »Intrusion Kill Chain«, gab es auch im Bundestag: Eine Spear-Phishing-E-Mail installierte Schadsoftware, die anschließend Benutzernamen und Passwörter von Administratoren ausspähte und den Angreifern somit den Weg bereitete, um Daten zu klauen, zu löschen oder zu manipulieren. Mit der Software PA-SIEM wäre dies deutlich schneller aufgefallen.

Fraunhofer

Datenklau schneller auf die Spur kommen – dabei hilft die profilbasierte Anomalieerkennung für SIEM-Systeme. © Fraunhofer FKIE | Bild in Farbe und Druckqualität: www.fraunhofer.de/presse.