BLINDSPOTTER

ECHTZEIT-ANALYSEN DES BENUTZERVERHALTENS
GEGEN INTERNE UND EXTERNE ANGREIFER

„Das neue Perimeter sind unsere Benutzer“

Der schlimmste Albtraum vieler Unternehmen, ein raffinierter Angriff von außen oder eine böswillige Attacke von innen, könnte bereits Realität sein. Heute sind Angreifer intelligent, gut finanziert und warten mit immer komplexeren und zielgerichteteren Angriffen auf. Eines haben alle spektakulären Delikte, die in letzter Zeit bekannt geworden sind, gemeinsam: Sie wurden sorgfältig geplant und blieben zunächst unentdeckt, sodass sich die Angreifer in der IT-Umgebung des betroffenen Unternehmens frei bewegen konnten. Böswilligen Mitarbeitern oder Auftragnehmern spielt dabei ein Umstand in die Karten: Die Haupt-Sicherheitstools eines Unternehmens richten sich zwar gegen externe Bedrohungen, jedoch nicht gegen Personen, die das Vertrauen ihres Arbeit- oder Auftraggebers genießen. Bei ihren gezielten Attacken verschaffen sich die Angreifer unerlaubten Zugang durch Ausnutzung von IT-Schwachstellen, Methoden der persönlichen Beeinflussung (Social Engineering) sowie gewöhnliches kriminelles Vorgehen. Das heißt, dass das neue Perimeter – und der Bereich, auf den wir unsere Aufmerksamkeit richten müssen – nicht die Infrastruktur ist, sondern der Benutzer. Blindspotter steht für die neue Generation der IT-Sicherheitslösungen, die sich auf privilegiertes Benutzerverhalten konzentrieren.

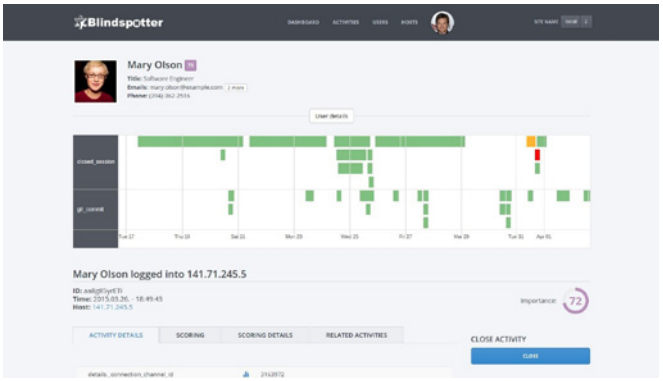
„Mehr Überwachung, weniger Kontrolle“

Blindspotter steht für die neue Generation der IT-Sicherheitslösungen, die sich auf privilegiertes Benutzerverhalten konzentrieren und verdächtige Aktivitäten aufdecken. Entwickelt wurde Blindspotter von Balabit, einem IT-Sicherheitsanbieter, der sich auf Log Management und erweiterte Monitoringtechnologien spezialisiert hat.

Durch die Erkennung von Abweichungen von normalem Verhalten und der Zuweisung eines Risikowerts hilft Blindspotter Unternehmen dabei, ihre Sicherheitsressourcen auf wichtige Ereignisse zu fokussieren. Darüber hinaus können sie bestimmte Kontrollen ersetzen und so ihre Geschäftseffizienz steigern. Wenn Sie mehr Tools einführen, durch die die Benutzer eingeschränkt werden, wird Ihr Unternehmen nicht sicherer – aber Ihre Mitarbeiter arbeiten weniger produktiv.

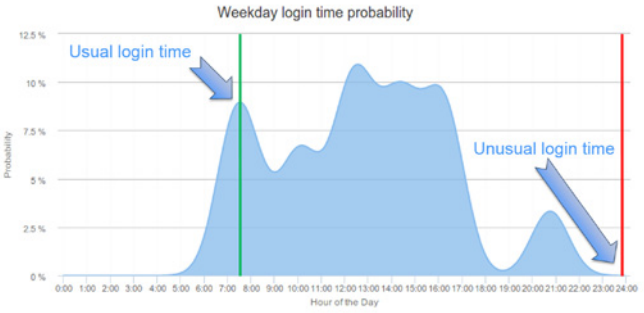
Blindspotter integriert eine breite Palette an Kontextinformationen zusätzlich zu standardmäßigen Logdaten, verarbeitet sie mittels einzigartiger Algorithmen und generiert Benutzerverhaltensprofile, die mithilfe von maschinellem Lernen ständig angepasst werden. Es verfolgt und visualisiert Benutzeraktivitäten in Echtzeit, damit Sie einen besseren Einblick in die Geschehnisse der IT-Systeme erhalten, und bietet eine breite Auswahl an Ausgabemöglichkeiten – von einem Prioritäts-Dashboard bis zur automatischen Intervention. Vordefinierte Korrelationsregeln sind dabei nicht erforderlich. Die Software arbeitet einfach mit Ihren bestehenden Daten. Die integrierten Algorithmen umfassen anpassbare Parameter, mit denen Sie die Ausgabe konfigurieren können, auch wenn Sie kein Datenanalyst sind.

Blindspotter ist die einzige Lösung zur Analyse des Benutzerverhaltens, die nicht nur Metadaten zu Ort und Zeitpunkt des Benutzerzugriffs auf bestimmte Systeme analysiert, sondern auch biometrische Daten wie Eingabemerkmale und Mausbewegungen auswertet. Zu den typischen Aspekten der Tastaturanalyse zählen Tippgeschwindigkeit, zeitlicher Abstand zwischen einzelnen Tastenanschlägen und häufige Tippfehler. Auch wenn mehrere Benutzer für die gleiche Aufgabe zuständig sind, zeigt doch jeder sein ganz eigenes Verhaltensmuster – beispielsweise die Geschwindigkeit, mit der der Mauszeiger bewegt wird, oder einfach die Anzahl einzelner Bewegungen. Die biometrischen Analysefunktionen von Blindspotter erkennen nicht nur einen Identitätenbetrug, sondern dienen zudem als zusätzliche biometrische Authentifizierung. So können Sicherheitsanalysten jederzeit feststellen, ob der Benutzer auch tatsächlich derjenige ist, der er zu sein vorgibt.



Daten werden auf vielfache Art und Weise analysiert, um die Risiko- und Abweichungsstufe jeder Aktivität anzupassen. Blindspotter zeigt alle neuen Abweichungen vom normalen Betrieb in einem nach Priorität geordneten Dashboard auf. Mittels erweitertem Monitoring aller Aspekte eines IT-Systems schützt Blindspotter sensible und kritische Daten vor möglichen Sicherheitsverletzungen, die durch externe oder interne Angreifer verursacht werden.

Blindspotter ist Bestandteil der Contextual Security Intelligence-Plattform von Balabit und daher eng mit dem Log-Management-Tool des Unternehmens, syslog-ng, und dem Privileged-User-Monitoring-Tool Shell Control Box integriert. Blindspotter schöpft mit syslog-ng die Vorteile von Logdaten voll aus und erstellt eindeutige Profile einzelner Benutzer anhand von Daten der Shell Control Box, die die Aktivitätsdetails von Remote-Benutzern wie eine Überwachungskamera aufzeichnet. Mit diesen beiden erstklassigen Monitoringtools ermöglicht Blindspotter tiefer gehende Einblicke in das Benutzerverhalten als jede andere Lösung. Balabit bietet ein umfassendes Portfolio für die Sicherheitsanalyse, damit Ihnen Ihre IT-Umgebung nicht länger Kopfzerbrechen bereiten muss.



DIE VORTEILE

- Verringerung der Wahrscheinlichkeit und Auswirkung von Sicherheitsverstößen: Verdächtige Aktivitäten und unbekannte Bedrohungen von inner- und außerhalb des Unternehmens werden erkannt
- Gesteigerte Effizienz der Sicherheitsteams
- Flexiblerer Geschäftsablauf bei gleichzeitiger Erhöhung der Sicherheit
- Verbesserter Compliance-ROI

FALLSTUDIEN

Gekaperte Konten erkennen

Verringert die Auswirkungen möglicher Sicherheitsverletzungen und bietet eine effektive Verteidigung gegen APTs. Angreifer, die gültige Benutzeranmeldedaten stehlen, verhalten sich anders als echte Benutzer. Blindspotter kann den Grad der Abweichung von normaler Benutzeraktivität erkennen. Ist die Abweichung hoch, wird ein Alarm an das Security Operation Center gesendet, wo der Fall genauer untersucht werden kann.

Missbrauch von Berechtigungen erkennen

Reduziert das Risiko von Berechtigungsmissbrauch maßgeblich. Böswillige Insider verhalten sich anders als reguläre Mitarbeiter. Wenn ein unzufriedener Mitarbeiter Unternehmensdaten stehlen will, kann Blindspotter diese anormalen Aktivitäten erkennen und das Sicherheitsteam benachrichtigen, das dann eine Untersuchung einleiten kann.

Die Effizienz der Untersuchung durch Kontextinformationen über Benutzer steigern

Sicherheitsanalysten müssen schnell handeln. Blindspotter erfasst, sortiert und meldet Daten, die für den privilegierten Benutzerkontext charakteristisch sind. Auf diese Weise können Analysten die ersten Anzeichen für einen Angriff schnell erkennen. Sie benötigen so viele relevante Informationen über die Benutzer wie möglich, um zügig feststellen zu können, ob ein Ereignis das erste Anzeichen eines externen Angriffs oder ein für diesen Benutzer vollkommen normaler Vorgang ist.

Die Nutzung von Systemkonten durch menschliche Benutzer und die Nutzung persönlicher Konten durch Skripte erkennen

Von Personen verwendete Systemkonten, gemeinsam genutzte Konten als auch persönliche Konten, die von Skripten benutzt werden, sind in der Regel Warnsignale, die ein mögliches Sicherheitsrisiko darstellen. Findet ein Angreifer einen Weg, sich Zugriff zu den gespeicherten Anmeldedaten zu verschaffen, die vom Skript genutzt werden, kann er Zugriff auf alle Dienste erlangen, auf die das Skript Zugriff hatte. Sicherheitsanalysten, die eine ungewöhnliche Nutzung von Konten mithilfe von Blindspotter erkennen, können gegensteuern, bevor sich eine Sicherheitslücke zu einer Datenpanne entwickelt.

Diskrepanzen zwischen Richtlinien und der tatsächlichen Nutzung des IT-Systems aufdecken

In großen Unternehmen ist „Berechtigungswuchern" ein großes Problem: Mitarbeiter, insbesondere IT-Mitarbeiter und leitende Angestellte, erhalten mehr und mehr Berechtigungen, um im Laufe der Zeit neue Aufgaben zu bewältigen. Blindspotter gibt einen Überblick darüber, wie die verschiedenen Services im Unternehmen genutzt werden und über welche Berechtigungen einzelne Benutzer verfügen sollten.

Die Contextual Security Intelligence™-Plattform von Balabit schützt Organisationen in Echtzeit vor Bedrohungen durch den Missbrauch von risikoreichen und privilegierten Konten. Zu den Lösungen zählen ein zuverlässiges Log Management für Systeme und Anwendungen, das Aktivitätsmonitoring privilegierter Nutzer und die Analyse des Benutzerverhaltens. Gemeinsam können sie ungewöhnliche Benutzeraktivitäten identifizieren und gewähren tiefe Einblicke in potenzielle Bedrohungen. Zusammen mit den vorhandenen kontrollbasierten IT-Strategien ermöglicht Balabit so einen flexiblen und benutzerorientierten Ansatz – für erhöhte Sicherheit ohne neue Hindernisse für die Geschäftsprozesse.

Besuchen Sie jetzt unsere Website: https://www.balabit.com/blindspotter

Vereinbaren Sie ein Gespräch mit unserem Expertenteam und gewinnen Sie einen ersten Eindruck von der Blindspotter Lösung.