BalaBit IT Security

GUARDING YOUR BUSINESS

EXECUTIVE SUMMARY

Wenn Systemprotokolle nicht ausreichen

www.balabit.com

Die Vorteile der Aktivitätsüberwachung gegenüber der Systemprotokollierung

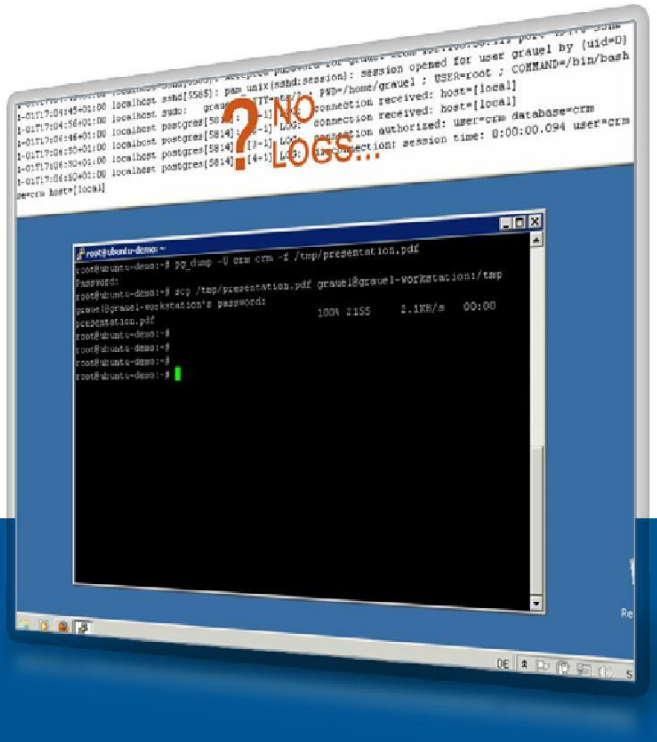
DIE HERAUSFORDERUNG

Die Grenzen von SIEMs

Wenn Sie Tools für die die Verwaltung von Protokollen oder Sicherheitsinformationen und Ereignissen (SIEM) kaufen, lehnen Sie sich wahrscheinlich zurück und gehen davon aus, dass alle Ihre Probleme mit Systemüberprüfungen und Compliance gelöst sind. Leider übersieht dieses rosige Bild die stets vorhandenen blinden Flecke in Prüfberichten: **Wenn Ihre Anwendungen nicht protokollieren, dann ist es in Ihren Prüfberichten nicht sichtbar ...**

Tools für Protokollverwaltung und SIEM leisten gute Arbeit, wenn es darum geht, Ereignisdaten darzustellen. Allerdings gibt es folgende Einschränkungen:

1. Zahlreiche kritische Sicherheitsereignistypen werden überhaupt nicht protokolliert.
2. Die üblicherweise protokollierten Ereignisse zeigen nicht, was wirklich gemacht wurde.
3. Häufig zeigen die Protokolle nur obskure technische Details über Sicherheitsereignisse.



Es gibt eine Reihe von Szenarien, in denen diese blinden Flecke auftreten. Zum Beispiel stellen grundlegende Administratoraktivitäten wie Firewall- oder Webserverkonfiguration ein potenziell hohes Sicherheitsrisiko für Unternehmen dar.

Man sollte meinen, dass diese Aktivitäten hinreichende Protokolleinträge generieren, was aber nicht der Fall ist. Darüber hinaus haben Administratoren als die mächtigsten Benutzer im IT-Umfeld die Möglichkeit, sogar die Spuren ihrer Handlungen aus denProtokollen zu entfernen.

DIE SCHLUSSFOLGERUNG

Privilegierte Benutzer überwachen

Sicherheitsüberprüfungen, die sich allein auf bestehende Systemprotokolle stützen, können löchrig sein. Das liegt daran, dass Systemprotokolle schlichtweg nicht alle nötigen relevanten Daten erfassen. Auch wenn ein Wechsel zu höheren Protokollebenen mehr nützliche Daten produzieren würde, erfordert das Extrahieren relevanter Informationen sehr kompetentes Personal und ist sehr zeitaufwändig. Im Zusammenhang mit IT-Prüfprotokollen lässt sich das Unerwartete vielleicht am besten voraussehen, wenn man keine Aktionen mehr protokolliert, sondern stattdessen einfach alle Benutzeraktionen überwacht. Am einfachsten beseitigt man all diese blinden Flecken mit einer **Überwachung der Aktivitäten privilegierter Benutzer,** wie sie BalaBit Shell Control Box bietet. Dabei werden vorhandene Systemprotokolle so erweitert, dass präzise sichtbar ist, was der Administrator getan hat.

Wir haben zwei Whitepaper und zwei Demonstrationsvideos veröffentlicht, die weitere Informationen zu diesem Thema bieten. Die Dokumente zeigen den Unterschied zwischen Ereignisprotokollierung und Aktivitätsüberwachung in Linux- und Windows-Umgebungen, indem sie die standardmäßige Systemprotokollierung mit der Aufzeichnung kompletter Sitzungen vergleichen. *(Sie können die Dokumente im Abschnitt „Mehr erfahren“ herunterladen.)*

www.balabit.com

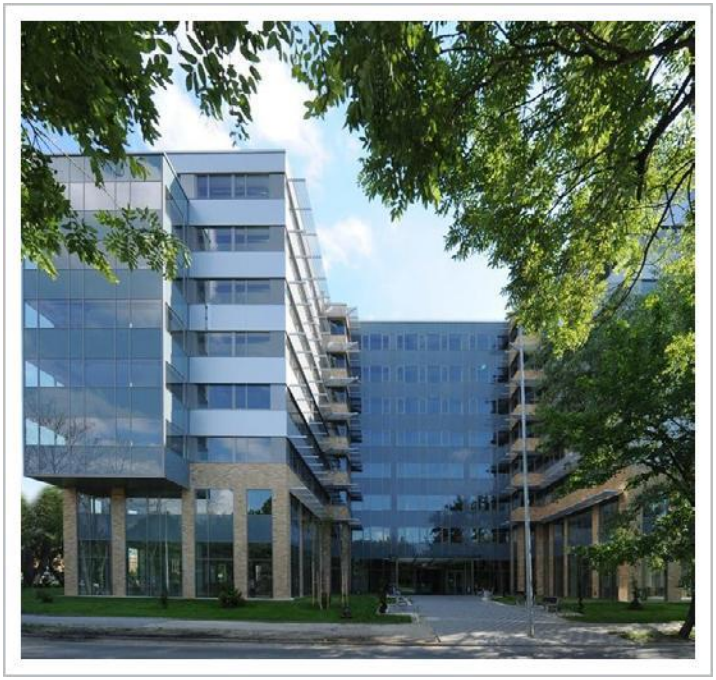
BalaBit IT Security

Über BalaBit

BalaBit IT Security ist ein innovatives Unternehmen für Datensicherheit und weltweit führend bei der Entwicklung privilegierter Aktivitätsüberwachung, vertrauenswürdiger Protokollierung und proxybasierten Gateway-Technologien. Wir schützen Kunden gegen Bedrohungen von innen und außen und helfen ihnen, Sicherheits- und Compliancevorschriften zu erfüllen. BalaBit ist auch als „die syslog-ng-Firma“ bekannt, was sich auf das Flagschiffprodukt des Unternehmens bezieht, eine Open-Source-Lösung für Log Server. Sie kommt in über 650.000 Unternehmen weltweit zum Einsatz und hat sich zum global anerkannten De-facto-Standard der Branche entwickelt.

BalaBit ist laut Deloitte Technology Fast 50 (2010) das am zweitschnellsten wachsende IT-Sicherheitsunternehmen in Mitteleuropa, mit Niederlassungen in Frankreich, Deutschland, England, Russland und den USA sowie Kooperationen mit Partnern auf der ganzen Welt. Sitz unserer F&E- und der globalen Support-Zentren ist Ungarn.

Weitere Informationen: www.balabit.com



Weitere Informationen

Vorteile der Aktivitätsüberwachung im Vergleich zur Systemprotokollierung im Windows-Umfeld

Vorteile der Aktivitätsüberwachung im Vergleich zur Systemprotokollierung im Linux-Umfeld

Shell Control Box Homepage

Rückruf anfragen