Heißes Thema: Sicherheitsrisiko Third-Party-Provider

München, 26. September 2017 - *Verizons diesjähriger Data Breach Investigations Report belegt: Der Missbrauch von Privilegien, über die sogenannte "privilegierte Nutzer" verfügen, ist die dritthäufigste Ursache von Datenschutzverletzungen. Insider Threats entstehen jedoch nicht nur durch Mitarbeiter, die Böses im Schilde führen. Zu "privilegierten Nutzern" gehören auch externe Drittanbieter und diese werden als potenzielle Bedrohung für eine Organisation nicht selten übersehen. Dabei haben auch sie Zugang zu sensiblen Informationen, sei es im Kunden- oder Finanzbereich und entsprechend groß sind die Schäden, die sie anrichten können. Der Sicherheitsspezialist Balabit zeigt Wege auf, wie Unternehmen mit dieser Bedrohung umgehen können.*

Outsourcing der Unternehmens-IT an Dritte - seien es einzelne Dienstleistungen oder gar die gesamte IT-Infrastruktur - sind heute eine beliebte Strategie, Kosten zu senken. Dass diese Kostenreduktion jedoch zu einem Sicherheitsrisiko werden kann, ist weniger geläufig. Denn die Erfahrung zeigt, dass externe Dienstleister schnell zur "Insider-Bedrohung" werden können. Sie sind ein lohnendes Ziel für Cyberkriminelle. In der Tat sind einige der verheerendsten Datenverletzungen in den letzten Jahren über die Accounts von Drittanbietern entstanden wie etwa bei dem Einbruch bei Unicredit, bei dem 400.000 Nutzer-Accounts gestohlen wurden oder dem prekären Sicherheitsvorfall bei einer schwedischen Behörde, bei dem in die Cloud an Dritte ausgelagerte Personendaten, vermutlich tausende persönliche Daten, abgeflossen sind.

Das Sicherheitsrisiko durch Drittanbieter wird durch mehrere Faktoren verursacht.

Problem 1 - Mehr privilegierte Nutzer: Da die externen Dienstleister ähnliche Privilegien und Zugriffsrechte haben wie reguläre Mitarbeiter, steigt die Zahl der "privilegierten Nutzer" und damit das Risiko für das Unternehmen.

Problem 2 - Gemeinsam genutzte Accounts: Gern richten Firmen sogenannte "Shared Accounts" ein, dabei werden administrative Konten und Passwörter gemeinsam genutzt: IT-Mitarbeiter von Drittanbietern loggen sich generell über diesen Account ins System ein. Das ist insofern problematisch, da niemand mehr nachvollziehen kann, wer innerhalb des IT-Systems für welche Aktionen verantwortlich war.

Problem 3 - Passwortsicherheit: Es geht auf das Konto der Passwortsicherheit, wenn sich mehrere Nutzer privilegierte Konten und Passwörter teilen. Erhöht wird das Risiko noch, wenn die gemeinsam genutzten Passwörter nicht regelmäßig geändert werden: Dann könnte im schlimmsten Fall ein (externer) Mitarbeiter noch Zugriff auf das System haben, selbst wenn er gar nicht mehr für das Unternehmen tätig ist.

Wenn IT-Aufgaben outgesourct werden, braucht es daher Maßnahmen, die die Aktivitäten der Drittanbieter kontrollieren und transparent werden lassen. Firewalls und ähnliches nützen wenig, da die Betroffenen bereits "drin" sind. Eine Möglichkeit diese Probleme in den Griff zu bekommen, besteht darin, zuverlässige Daten zu diesen Benutzer-Sessions zu sammeln.

Tools wie die Privileged-Access-Management-Lösung (PAM) von Balabit kontrollieren den Zugriff von privilegierten Accounts und liefern wichtige Informationen darüber. Balabits PAM-Lösung integriert dabei die Analyse des Verhaltensmusters eines Benutzers, um den toten Winkel, in dem sich Drittanbieter möglicherweise bewegen, im Blick zu behalten. Es wird dabei in Echtzeit analysiert, wie Nutzer mit dem IT-System interagieren. Dadurch entsteht ein Profil der einzelnen Nutzer. Registriert das System eine gravierende Abweichung von diesem Profil, erfolgt eine automatische Risikobewertung, das Sicherheitsteam erhält eine Meldung und kann den Fall prüfen und bei Bedarf einschreiten.

Messebesucher, die Lösungen suchen, die Schutz bieten vor dem Verlust vertraulicher Daten, vor internen und externen Bedrohungen durch privilegierte Konten und Unterstützung wünschen, um die

vielfältigen Compliance-Anforderungen wie die neue Europäische Datenschutz-Grundverordnung, PCI-DSS oder ISO 2700x zu erfüllen, sind bei Balabit, dem führenden Anbieter von Privileged-Access-Management (PAM)- und Log-Management-Lösungen an der richtigen Adresse. Auf der it-sa 2017 haben die Besucher die Möglichkeit, sich darüber bei den Experten von Balabit in Halle 10, Stand 401 zu informieren oder sie besuchen einen der Fachvorträge von Balabit im Auditorium.

Mittwoch, 11.10.2016
Forum M10 - Forum Management in Halle 10
11:30 Uhr - 12:00 Uhr
"Catch me if you can: Wie das Tippverhalten Identitäten schützt?"
Referent: Thomas Haak, Sales Director bei Balabit

Nach der it-sa:

https://www.it-sa.de/CDB/download/9efa28c1-c263-4ec9-8730-207ddaaddd9d?Type=FancyBox&Language=de&FairID=itsa#

https://2017.it-sa.tv/8484/balabit-catch-me-if-you-can-wie-kann-ihr-tipp-stil-ihre-identitaet-schuetzen

Donnerstag, 12.10.2016
Forum T10 - Forum Technik in Halle 10
11:30 Uhr - 11:45 Uhr
"Enemy at the gates: Wie geht Privileged Access Management mit raffinierten Cyberkriminellen um?"
Referent: Zoltan Bakos, Senior Pre-Sales Engineer bei Balabit

Nach der it-sa:

https://www.it-sa.de/CDB/download/2ae9d2fe-b4c1-49c0-b51e-7f7e9d59ecef?Type=FancyBox&Language=de&FairID=itsa#

https://2017.it-sa.tv/8485/balabit-enemy-at-the-gates-wie-privileged-access-management-mit-hoch-entwickelten-cyberverbrechern

Über Balabit
Balabit ist ein führender Anbieter von Privileged-Access-Management- (PAM) und Log-Management-Lösungen. Diese unterstützen Unternehmen dabei, die Risiken von Datenverletzungen in Verbindung mit privilegierten Accounts zu minimieren.

Balabits integrierte PAM-Lösung schützt Organisationen in Echtzeit vor Gefahren, die durch den Missbrauch von Accounts mit privilegierten Zugriffsrechten entstehen. Die Lösungsbestandteile Privileged Session Management und Privileged Account Analytics helfen Unternehmen, Cyber-Attacken im Zusammenhang mit privilegierten Accounts zu verhindern sowie diese zu erkennen und entsprechend darauf zu reagieren. Hierzu gehören Bedrohungen durch Insider sowie Angriffe Externer, bei denen gestohlene Accounts zum Einsatz kommen. In Kombination mit bestehenden Sicherheitslösungen stellt Balabits Lösung für das Privileged Access Management einen flexiblen, auf den Nutzer zugeschnittenen Ansatz dar, der ein höheres Maß an Sicherheit bietet, ohne dadurch die Geschäftsabläufe zu beeinträchtigen.

Balabit wurde im Jahr 2000 gegründet. Zu den Kunden zählen 25 der Fortune-100-Unternehmen. Zudem setzen mehr als eine Million Nutzer in Unternehmen die Lösungen ein. Balabit ist weltweit über ein Netz von Niederlassungen in den USA und Europa tätig und arbeitet mit einer großen Zahl von Reseller-Partnern zusammen.

Weitere Informationen: www.balabit.com, im Blog, bei Twitter via @balabit, LinkedIn oder Facebook.