

Cyber-Ark: MaRisk fordern strikte Regelung der Zugriffsrechte auf IT-Systeme

06.12.2011, 13:41 | IT, New Media & Software

Pressemitteilung von: *Cyber-Ark*

Heilbronn, 6. Dezember 2011 – Über Administratoren-Accounts und -Passwörter ist in der Regel ein problemloser Zugriff auf alle unternehmenskritischen Datenbestände möglich. In zahlreichen Compliance-Richtlinien wird deshalb eine exakte Überwachung solcher Nutzerkennungen gefordert. Regelungen hierzu gibt es laut Sicherheitsexperte Cyber-Ark auch in den MaRisk (Mindestanforderungen an das Risikomanagement) der BaFin, die für Finanzinstitute gültig sind.

User-Accounts von Administratoren und sogenannten Superusern verfügen über weitreichende Rechte. Sie stellen deshalb für jedes Unternehmen ein hohes Sicherheitsrisiko dar. Werden hier keine adäquaten Maßnahmen für ein effizientes Passwortmanagement getroffen, verstößt dies gegen gesetzliche und aufsichtsrechtliche Bestimmungen aus Basel II, ISO 27001, SAS70, PCI-DSS oder dem Sarbanes Oxley Act. In diesen Compliance-Regelungen wird nämlich ein Nachweis gefordert, wer Zugriff auf privilegierte Benutzerkonten hat, welche Veränderungen vorgenommen und ob die Passwörter ordnungsgemäß geschützt und geändert wurden.

Auch in den von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) veröffentlichten Mindestanforderungen an das Risikomanagement (MaRisk), dem zentralen Regelwerk der qualitativen Bankenaufsicht, finden sich entsprechende Regelungen. Deren Einhaltung wird im Rahmen der Jahresabschlussprüfung geprüft und ist gegenwärtig auch häufig Gegenstand von Sonderprüfungen nach § 44 Abs. 1 KWG.

Im Hinblick auf die technisch-organisatorische Ausstattung von Finanzinstituten wird in den MaRisk etwa konstatiert, dass „bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen (ist), insbesondere sind Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt“. Konkret verwiesen wird hier auf die Einhaltung der Standards IT-Grundsatzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und ISO/IEC 2700X.

Die MaRisk wurden zuletzt Ende 2010 überarbeitet. Die Änderungen müssen von den Instituten bis zum Ende dieses Jahres „vollumfänglich“ umgesetzt werden. Eine entscheidende Erweiterung betrifft den Bereich „Zugriffsrechte“. Hierzu heißt es: „Die eingerichteten Berechtigungen dürfen nicht im Widerspruch zur organisatorischen Zuordnung von Mitarbeitern stehen. Insbesondere bei Berechtigungsvergaben im Rahmen von Rollenmodellen ist darauf zu achten, dass Funktionstrennungen beibehalten beziehungsweise Interessenkonflikte vermieden werden.“

Jochen Koehler, Deutschland-Chef von Cyber-Ark in Heilbronn, betont: „Gerade in diesem Bereich sehen wir in der Finanzdienstleistungsbranche noch einen erheblichen Handlungsbedarf. Vielfach gibt es nämlich noch Super-Admins mit uneingeschränkten privilegierten Rechten, das heißt, es erfolgt weder eine strikte 'Separation of Duties' noch eine Implementierung von rollenbasierten Zugriffs- und Kontrollsystemen. Im Hinblick auf die Erfüllung von Compliance-Anforderungen, eine Erhöhung der Sicherheit und auch eine Reduzierung des Administrationsaufwandes sollte aber jedes Finanzinstitut über ein zuverlässiges Privileged Identity Management (PIM) verfügen. Mit einer solchen Lösung können privilegierte Accounts, also Benutzerkonten mit erweiterten Rechten, zuverlässig verwaltet werden.“

Verschiedene PIM-Lösungen sind heute auf dem Markt verfügbar. Dabei gibt es unterschiedliche Lösungsansätze: von der Hardware-Appliance über eine softwarebasierte Virtual Appliance bis hin zu einer reinen Software-Lösung. Gemeinsam ist den Lösungen, dass die Passwörter in einem gesicherten Bereich vor den Zugriffen unberechtigter Personen geschützt werden. Koehler: „Bei der Entscheidung für eine Lösung sollte man darauf achten, dass sie neben einer regelmäßigen Änderung der Netzwerk-, Server- und Datenbank-Passwörter auch Drittanwendungen die

Möglichkeit bietet, die neuen Passwörter automatisch zu beziehen. Zudem sollte eine Zugriffskontrolle und vollständige Überwachung beziehungsweise Protokollierung aller Aktivitäten vorhanden sein.“

Diese Presseinformation kann auch unter www.pr-com.de abgerufen werden.

Portrait

Über Cyber-Ark

Das 1999 gegründete Unternehmen Cyber-Ark ist ein global agierender Anbieter von Informationssicherheits-Software. Das Unternehmen hat sich auf die Verwaltung und den Schutz von privilegierten Nutzerkennungen und sensiblen Daten spezialisiert. Die Lösungen von Cyber-Ark helfen Unternehmen, gesetzliche Richtlinien einzuhalten sowie Insider-Bedrohungen und externen Angriffen vorzubeugen. Der Hauptsitz des Unternehmens befindet sich in Newton (Massachusetts, USA). In Deutschland ist Cyber-Ark seit 2008 mit einer eigenen Niederlassung in Heilbronn vertreten. Cyber-Ark hat weltweit über 900 Kunden aus unterschiedlichsten Branchen.

News-ID: 592356 • Views: 1290 (Stand: 20.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/592356/Cyber-Ark-MaRisk-fordern-strikte-Regelung-der-Zugriffsrechte-auf-IT-Systeme.html>