Berechtigungsmanagement

Innere Sicherheit

Foto: Fotolia / dizain

Mit der Dezentralisierung der Firmen-IT wird das Berechtigungsmanagement zu einer zentralen Herausforderung.

Firmennetzwerke sind in der Regel vor den wichtigsten Gefahren von außen geschützt. Attacken aus dem Internet blockt eine professionelle Firewall und Schutzsoftware hilft, Angriffe durch Malware abzuwehren, die per E-Mail eintrifft. Die Gefahr von innen wird dagegen meistens unterschätzt.

Wie Studien von Marktforschungsunternehmen immer wieder zeigen, geht ein Großteil der Bedrohungen nicht auf das Konto von Kriminellen außerhalb des Unternehmens, sondern wird von Mitarbeitern verursacht – absichtlich oder unabsichtlich.

Laut der aktuellen Corporate-Trust-Studie „Cybergeddon" beläuft sich der Schaden, der durch Industriespionage entsteht, in Deutschland jährlich auf rund 12 Milliarden Euro. Das Sicherheitsunternehmen Protected Networks befragte auf der Messe für IT-Sicherheit it-sa 2014 Fach-und Führungskräfte für Sicherheit und IT nach ihrer Einschätzung, wie viel von den 12 Milliarden Euro auf schlechtes Berechtigungsmanagement zurückzuführen sei. 38 Prozent der Befragten schätzten, dass bis zu 6 Milliarden auf ein schlechtes oder falsches Berechtigungsmanagement zurückgehen könnten.

Azubi-Effekt

In einem Unternehmen sollte jeder Anwender nur auf diejenigen Daten zugreifen dürfen, die er für die tägliche Arbeit benötigt. Dieser Grundsatz nennt sich Need-to-know-Prinzip.

Die Einhaltung dieses Prinzips wird jedoch schwierig, wenn zu den Angestellten, die einer fest umrissenen Tätigkeit nachgehen, Mitarbeiter mit wechselnden Einsatzorten und Tätigkeiten hinzukommen. Zu diesem Personenkreis zählen beispielsweise Praktikanten, Auszubildende, Studenten oder Zeitarbeitskräfte. Solche Mitarbeiter werden vielfach in Zeiten von Produktionsspitzen und flexibel in unterschiedlichen Abteilungen eingesetzt. Ein Abteilungswechsel erfordert aber meist auch neue Zugriffsberechtigungen auf die Firmendaten.

Werden nun die alten Berechtigungen nicht konsequent wieder entzogen, kann sich für einen Benutzer ein stattliches Set an Berechtigungen anhäufen, das sich in vielen Fällen von dem eines Administrators nur noch wenig unterscheidet. Ohne Kontrolle oder die regelmäßige Überprüfung der aktuellen Berechtigungen fällt das mitunter jahrelang nicht auf. Eine solche Anhäufung von Berechtigungen heißt im Fachjargon Azubi-Effekt.

Projekt-Effekt

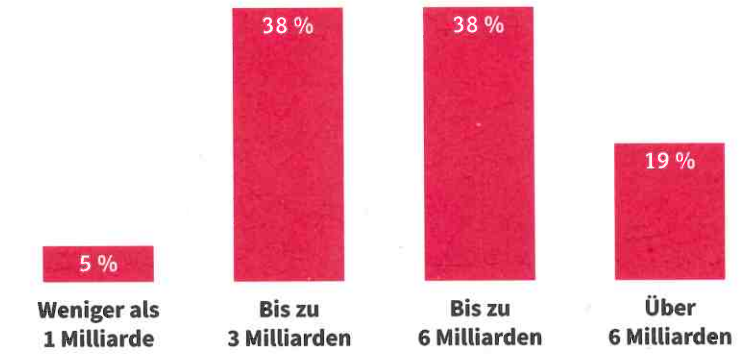
Ähnlich wie beim Azubi-Effekt gestaltet sich die Problematik beim sogenannten Projekt-Effekt.

Hier geht es darum, die Daten eines Projekts richtig zu verwalten. Das bedeutet: Wenn Mitarbeiter von einem Projekt in ein anderes wechseln oder neue Mitarbeiter zu einem bestehenden Projekt hinzustoßen, dann sollte der Administrator darüber informiert werden.

Er muss die Berechtigungen der Benutzer anpassen, bei abgeschlossenen Projekten die Zugriffsrechte wieder entziehen oder bei neuen Projekten die benötigten Verzeichnisse inklusive der Berechtigungen erstellen.

Datensicherheit

38 Prozent der auf der it-sa 2014 befragten IT-Profis schätzten den Schaden durch schlechtes Berechtigungsmanagement auf 3 bis 6 Milliarden Euro.

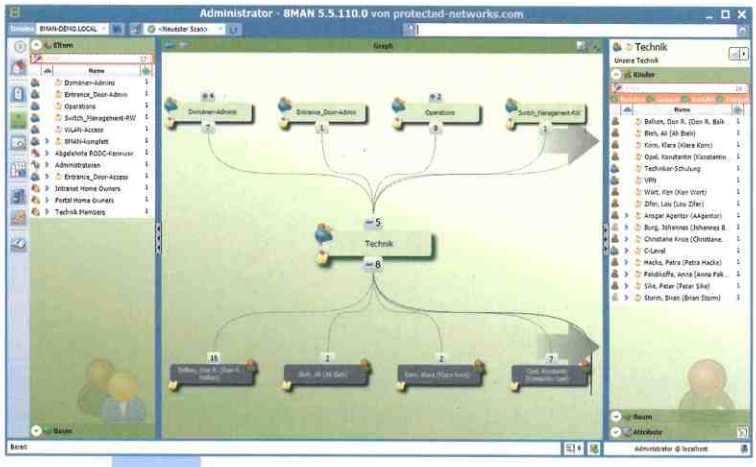


com! professional 3/15
Quelle: Protected Networks

Wenn das nicht rechtzeitig passiert oder die Berechtigungen falsch gesetzt werden, kann sich das negativ auf die Effizienz des Projektteams und den zeitlichen Rahmen des Projekts auswirken. Zu umfangreiche Privilegien führen dazu, dass Mitarbeiter Zugriff auf Daten haben, für die sie eigentlich keine Berechtigungen haben sollten – oder der Projektleiter hat keine ausreichenden Berechtigungen, um seine Arbeit zu erfüllen.

Wenn möglich, sollte hier die Berechtigungsvergabe direkt vom Administrator an den Projektleiter übertragen werden. Der Projektleiter weiß am besten, wer welche Berechtigungen benötigt.

Eine mögliche Lösung ist also die Verlagerung der Berechtigungsvergabe direkt an die Besitzer der Daten wie Projekt- oder Abteilungsleiter.



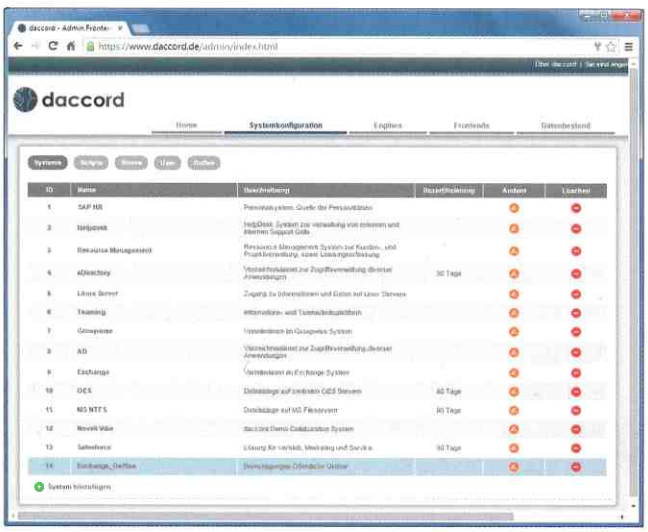
Protected Networks: 8Man ist derzeit vor allem auf Windows-Umgebungen spezialisiert.

Dezentralisierte IT

Die Verwaltung der Berechtigungen wird umso schwieriger, je dezentraler die IT im Unternehmen organisiert ist. Ein Beispiel hierfür ist die Kombination klassischer IT mit Cloud-, Mobile- und M2M-Computing oder ausländischen Beteiligungen und Töchtern.

Dezentralisierung heißt immer auch höhere Komplexität der IT-Strukturen, da viele Berechtigungen von anderen Stellen verwaltet werden und sich so nur schwer kontrollieren lassen. Oft fehlt ein zentrales Identity-Management-Tool mit einem stringenten Rollenkonzept, das die Berechtigungen gebündelt verwaltet. Vielmehr legen verschiedene Administratoren auf Zuruf die Daten direkt in den jeweiligen Systemen an. Die Folge: Im System entstehen viele, unabhängig voneinander betriebene Berechtigungsverwaltungen mit unterschiedlichen Verfahren.

Die Kontrolle darüber, welche internen oder externen Mitarbeiter auf welche Daten und Anwendungen im Unternehmen zugreifen können, ist daher fast unmöglich. So haben externe Mitarbeiter, die schon längst nicht mehr für die Firma tätig sind, oft immer noch Zugriff auf sensible Geschäfts- oder Kundendaten. Solche Altlasten stellen ein hohes Risiko für die Unternehmensdaten dar.



Daccord: Die Access-Governance-Lösung unterstützt neben Windows oder Oracle auch Cloud-Anbieter wie Salesforce.

Lösung: Access Governance

Um die Zugriffsberechtigungen im Griff zu behalten und zu vereinheitlichen, benötigt man eine Plattform, die mit Hilfe sogenannter Connectoren auf die unterschiedlichen Datenquellen zugreifen und diese verwalten kann. Ferner ist es praktisch, wenn sich temporäre Berechtigungen einrichten lassen – das sind Berechtigungen mit Verfallsdatum. Diese Funktion ist zum Beispiel dann von Nutzen, wenn das Ende eines Projekts feststeht oder ein Mitarbeiter in naher Zukunft das Unternehmen verlässt. Ist der definierte Zeitpunkt verstrichen, werden die Berechtigungen ungültig oder vom System aufgehoben.

Hilfreich ist außerdem eine zentralisierte Rechteverwaltung, um den Status quo der aktiven Berechtigungen festzustellen – also aufzuzeigen, welche Nutzer derzeit im System vorhanden und aktiv sind und welche Privilegien ihnen zugeordnet wurden. Auch konkurrierende Berechtigungen sowie Falschzuweisungen lassen sich durch solch ein Audit feststellen und anschließend korrigieren.

Zur Verwaltung der Berechtigungen gibt es verschiedene Access-Governance-Lösungen. Sie unterscheiden sich vor allem hinsichtlich der Schnittstellen zu anderen Teilen der Firmen-IT. So bietet etwa die Software Daccord (www.daccord.de) unter anderem Connectoren für Salesforce, Novell, Oracle oder Windows. 8Man von Protected Networks (www.8man.com) ist aktuell auf Windows-Umgebungen spezialisiert und bietet als Besonderheit die Visualisierung von Berechtigungen an.

Weitere Anbieter von Access-Governance-Lösungen sind beispielsweise NetiQ, Quest, Aveska oder Courion. ■

Oliver Ehm
oe@com-professional.de