< - Zurück zu: it-sicherheit.de

IT-Sicherheit auch 2014 ein Top-Thema für Unternehmen

Sicherheit wird 2014 weiterhin ein Top-Thema in der IT sein, sagt CyberArk. Im Jahr 2013 haben mehrere spektakuläre IT-Attacken gezeigt, welches Gefährdungspotenzial Cyber- und Insider-Kriminalität aufweisen. Unternehmen werden deshalb verstärkt auf zusätzliche Sicherungsmaßnahmen setzen müssen.

Das Jahr 2013 war geprägt von zahlreichen IT-Angriffen: Sie erfolgten sowohl durch Insider als auch Externe. Und gleichgültig, ob sie politisch oder finanziell motiviert waren oder ob der Diebstahl von vertraulichen Informationen oder geistigem Eigentum das Ziel war: Sie haben gezeigt, dass bei der IT-Sicherheit noch vieles im Argen liegt. Folglich wird dieses Thema auch 2014 eine zentrale Bedeutung einnehmen, sagt CyberArk. Dabei werden sich vier Trends herauskristallisieren.

1. Erweiterung des klassischen Perimeter-Schutzes

Bei allen vergangenen zielgerichteten Web-Attacken, den Advanced Persistent Threats (APTs), wurde die Abschottung der eigenen Netze durch Perimeter-Schutz erfolgreich überwunden. Die klassische Perimeter-Sicherheit, die auf dem Einsatz von Firewalls, Anti-Viren-Scannern, Webfilter-Techniken oder VPN-Systemen basiert, hat sich somit als unzureichend erwiesen – auch wenn ein Unternehmen hier auf neue Lösungen wie Next Generation Firewalls oder Sandboxing setzt. Deshalb sind zusätzliche Lösungen und neue Sicherheitskonzepte als Ergänzung dieser Systeme unverzichtbar, und zwar in Bereichen wie Zugriffsschutz und Rechtemanagement.

2. Abwehr von Insider-Bedrohungen

Das vergangene Jahr hat auch gezeigt, dass es beim Thema Sicherheit nicht nur um Cyber-Angriffe geht, sondern auch um Insider-Bedrohungen. Die Snowden-Enthüllungen sind hier ein Beispiel. In vielen Unternehmen ist es üblich, dass Systemadministratoren einen uneingeschränkten Zugriff auf Daten, Applikationen und Server haben, ohne dass es eine Funktionstrennung (Segregation of Duties) gibt. Das war auch der Fall bei Edward Snowden, der als Systemingenieur und -administrator auf hochvertrauliche Informationen zugreifen konnte.

Dabei wurde ein für die Sicherheit wesentlicher Aspekt vernachlässigt: Es ist essenziell, dass Mitarbeiter – und das betrifft natürlich auch Systemadministratoren – nur Zugang zu Daten haben, die sie für ihre tägliche Arbeit benötigen. Zudem muss die Option vorhanden sein, dass auch diese Zugriffsmöglichkeit in Echtzeit entzogen werden kann, falls zum Beispiel verdächtige Aktivitäten bei der Account-Nutzung registriert werden. Auch in diesem Bereich werden Unternehmen künftig verstärkt Lösungen implementieren.

3. Sicherung privilegierter Accounts

Da nahezu bei allen gravierenden externen und internen IT-Attacken der letzten Zeit Passwörter von privilegierten Nutzern als "Einfallstor" verwendet wurden, werden Unternehmen diesen Aspekt in den Fokus ihrer Sicherheitsstrategie rücken. Privilegierte Benutzerkonten mit weitreichenden Rechten stellen für jedes Unternehmen ein hohes Sicherheitsrisiko dar, da sie einen Zugriff auf vertrauliche Informationen, die Installation und Ausführung von Applikationen oder die Veränderung von Konfigurationseinstellungen ermöglichen.

Deshalb ist es für Unternehmen zwingend erforderlich, hier verstärkt präventive Maßnahmen zum Schutz der privilegierten Accounts zu ergreifen. Viele Unternehmen

haben dies bereits erkannt, wie das starke Wachstum des Marktes für Privileged-Account-Security-Lösungen belegt. Mit einer solchen Lösung können privilegierte Zugriffe auf beliebige Zielsysteme zentral berechtigt, jederzeit kontrolliert und revisionssicher auditiert werden.

4. Sicherung von Application Accounts

Eine weitere bekannte, aber oft noch unterschätzte Sicherheitslücke sind die Application Accounts, das heißt die in Anwendungen, Skripten oder Konfigurationsdateien gespeicherten Passwörter. Im Unterschied zu privilegierten administrativen Accounts, die von Personen genutzt werden, greifen Applikationen automatisch auf Backend-Systeme zu, die eine Authentifizierung erfordern. Die Application Accounts werden zum Beispiel für den Datenbank-Zugriff einer Anwendung benötigt. Das Problem dabei ist, dass die Passwörter meistens im Klartext vorliegen und nie geändert werden.

Das heißt auch: Sie sind in der Regel zahlreichen Anwendern wie Systemadministratoren, Applikationsentwicklern oder Testingenieuren zugänglich – und können natürlich auch problemlos von Angreifern genutzt werden, wie dies bereits im letzten Jahr mehrfach geschehen ist. Deshalb werden Unternehmen auch dieses Thema 2014 verstärkt adressieren und Lösungen implementieren, mit denen sie die in Applikationen eingebetteten Klartext-Passwörter gänzlich eliminieren können.

"Marktforscher sehen heute bei Themen wie Big Data, Internet der Dinge, Cloud oder Bring Your Own Device die zentralen IT-Trends des Jahres 2014", sagt Jochen Koehler, Regional Director DACH bei CyberArk in Heilbronn. "Das ist sicher völlig richtig, aber einen Punkt darf man dabei nicht vergessen: Bei allen diesen neuen Lösungen, Services und Technologien wird das Thema Sicherheit von elementarer Bedeutung sein. Und nur wenn dieser Bereich ausreichend berücksichtigt wird oder werden kann, werden sich diese Trends auch reibungslos durchsetzen."

< - Zurück zu: it-sicherheit.de

Datum: 14.01.2014

Kategorie: News