

DAS
SPEZIAL

 SEPPMAIL

Bewusstsein
für Datenschutz stärken
ab Seite 10

RECHENZENTREN UND MANAGED SERVICES

EINE ERFOLGSGESCHICHTE

Ingo Kraupa, noris network AG

SICHERHEITSRISIKEN

Cloud-Native
Architekturen

DATENSCHUTZ

Beziehungsstatus:
kompliziert?

INSELLÖSUNGEN

Security
ganzheitlich denken

SCHWACHSTELLE BENUTZERKONTO

DAS A UND O BEI DER ERMITTLUNG FEHLERHAFTER BERECHTIGUNGEN IN MICROSOFT-UMGEBUNGEN? EINE KONTINUIERLICHE ÜBERPRÜFUNG!

Wie aus dem Studienbericht 2020 zum Thema „Spionage, Sabotage und Datendiebstahl“ der Bitkom hervorgeht, gaben 74 Prozent der befragten Unternehmen an, dass Cyberattacken zugenommen haben. 82 Prozent gehen außerdem davon aus, dass sich die Sicherheitslage künftig noch weiter verschärfen wird. Angesichts dessen ist es wichtig, Sicherheitsmaßnahmen zu ergreifen, um typische Einfallstore zu schließen. Dazu gehören unter anderem veraltete Mitarbeiterkonten, über die sich Kriminelle Zugang zu IT-Systemen verschaffen und sensible Informationen abgreifen können. Mit der in drei Varianten erhältlichen Lösung daccord von G+H Systems lassen sich solche Schwachstellen beheben. Eine von ihnen: die Microsoft Edition zur Analyse und Überwachung der Richtlinien und Benutzerkonstellationen im Active Directory (AD) und im NTFS-Filesystem.

Die manuelle Analyse von AD-Objekten und Fileserverstrukturen ist zeitaufwendig und birgt ein hohes Fehlerpotenzial. So ist es schnell passiert, dass Missstände wie Überberechtigungen oder aktive Benutzerkonten ehemaliger Mitarbeiter unentdeckt bleiben. Damit zu keinem Zeitpunkt der Überblick verloren geht, wer worauf Zugriff hat, ist eine softwarebasierte Auswertung der Berechtigungen nötig. Die daccord Microsoft Edition lässt sich einfach installieren sowie konfigurieren, erfasst die Zugriffsberechtigungen der einzelnen Benutzer und Gruppen innerhalb der firmeninternen Microsoft-Infrastruktur.



Die Top-Features

Verwaiste Konten aufdecken, indem Personendaten integriert werden und ein Bezug zu den natürlichen Personen hergestellt wird.

- Personalstammdaten lassen sich während oder nach der Konfiguration als CSV-Datei hochladen.
- Um die Daten aktuell zu halten, ist es möglich, den Zeitplan des zyklischen Datenimports zu bestimmen, der aus dem Personalsystem bereitgestellt wird.

Jederzeit den Überblick behalten durch eine beständige Überprüfung der Konstellationen.

- Es erfolgt kein einmaliger, sondern ein dauerhafter Check des Datenbestandes. Dies ist essenziell, um Schwachstellen zu vermeiden.

Kontenursprung feststellen und Veränderungen dokumentieren mittels Historienfunktion:

- Anstelle einer Momentaufnahme werden anhand konfigurierter Zeitpläne alle Läufe historisch festgehalten, sodass man jederzeit einen Einblick in die Veränderungen bekommt.

Vollautomatisierte Kontrolle dank vorgefertigter Richtlinienpakete:

- Die mitgelieferten Richtlinien erlauben die Überprüfung der Umgebung auf Konformität zu Microsoft-Empfehlungen oder rechtlichen Anforderungen.
- Jede Richtlinie ist ein- und ausschaltbar und beinhaltet Korrektorempfehlungen.
- Es lassen sich Risikostufen definieren, ab denen ein Wert als kritisch angezeigt wird.

→ Liegen unternehmenseigene Richtlinien vor, kann ein individuelles Richtlinienpaket erstellt werden.

Schnellübersicht durch umfangreiches Dashboard:

- Auf dem integrierten Dashboard erhält man eine anschauliche Übersicht über alle Systeme und Daten.
- Ungereimtheiten im Daten- oder Personenbereich sowie Abweichungen zu den Richtlinien fallen unmittelbar auf.

Sebastian Spethmann
www.daccord.de/microsoft