SIMPLYIT
LANWORKS

WIR MACHEN EXPERTENWISSEN WIRKSAM

www.lanworks.de

Digitalisierung beginnt mit sicheren Identitäten – Ist Ihr IAM zukunftsfähig?

Wie gewährleistet die IT einen effizienten, konsistenten und sicheren Zugriff auf Ressourcen innerhalb und außerhalb der eigenen Firewalls? Angesichts steigender Anforderungen an expandierende Arbeitsplätze durch Mobilität und eigene Devices (BYOD), angesichts interner und externer Audits und einer sehr viel intensiveren Nutzung von Cloud Computing bekommt das Management von Identitäten heute eine ganz neue Bedeutung.

Müssen wir im Jahr 2021 wirklich noch über Identity & Access Management reden? Das Thema ist doch eigentlich ein alter Hut, oder? Man sollte meinen, dass sich heute jeder der Wichtigkeit bewusst ist und gute und zufriedenstellende Lösungen in den Unternehmen längst etabliert sind. Schließlich lesen wir doch jeden Tag von Datenklau und gehackten Institutionen in der Zeitung. Doch spätestens seit Beginn der Krise, als sich die Geschäftswelt plötzlich und zum Teil sehr schnell auf mobiles Arbeiten einstellen musste, zeigte sich, dass viele immer noch mit massiven Problemen im Identity Management zu kämpfen haben.

Lanworks AG
IT Engineering • IT Training & Coaching
Fürstenwall 41 • 40219 Düsseldorf
Fon +49 211 95059-69

Ein Ad-hoc Remote-Zugang zu geschäftskritischen Unternehmensressourcen konnte so schnell gar nicht bereitgestellt werden; ein massives Problem für die laufende Produktivität.

Daher ist eine Neubewertung des Identity Management erforderlich - Neue Konzepte für das Identitätsmanagement

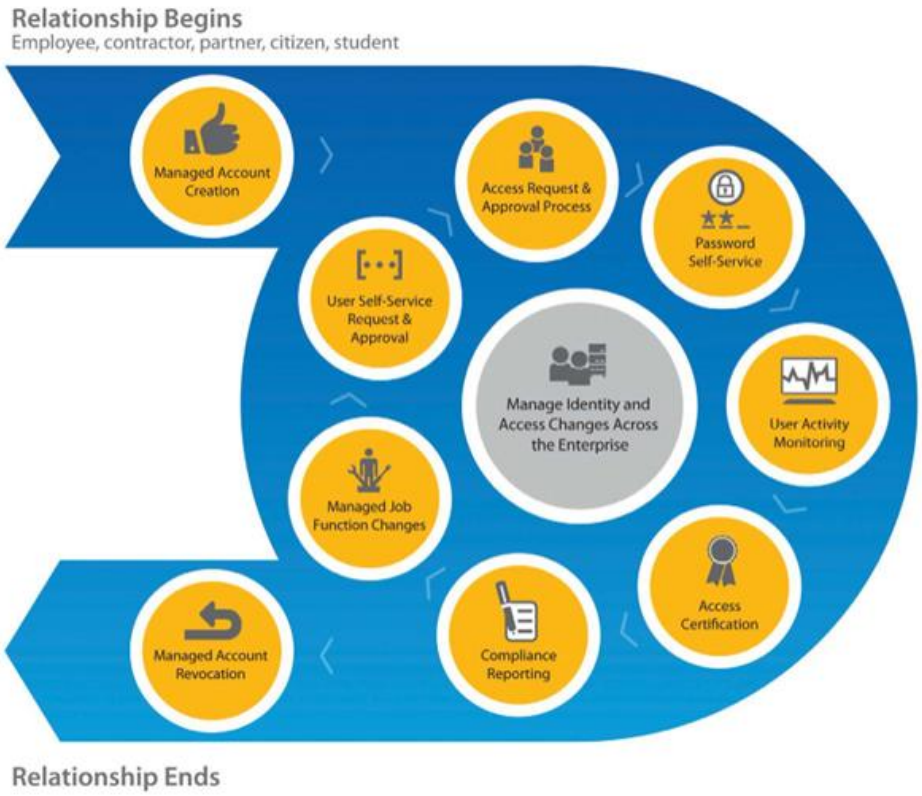
Durch neue Arbeitsweisen und Tools verändert sich das Identitäts- und Berechtigungsmanagement und wird zunehmend komplexer. Dazu kommen neue Compliance-Anforderungen, die mit einem möglichst unkomplizierten und nahtlosen Zugang zu relevanten Infrastrukturen zu vereinen sind. Für die zunehmenden Risiken sind daher anpassungsfähige Werkzeuge und Ansätze gefragt.

Ein durchdachtes Identitätsmanagement ist nicht nur in Zeiten von Home Office gefragt. Wie und wo wir arbeiten, hat sich wahrscheinlich für immer verändert. Das hat nicht nur mit der Pandemie zu tun. Die Anzahl vernetzter Arbeitsgeräte und die Datenmenge steigt ja bereits seit Jahren exponentiell. In Folge der Pandemie erlebt die Arbeitswelt einfach nur einen besonders schnellen Anschub. Manuell ist die Verwaltung der Zugriffsberechtigungen nicht mehr zu schaffen.

Unternehmen jeder Größe haben sich heute mit dem Thema Identity and Access Management (IAM) noch stärker zu beschäftigen. Hier ist auch die Frage, inwiefern die eingesetzten Lösungen die gesetzlichen Compliance Anforderungen erfüllen.

Die Bedrohungslage erfordert ein Umdenken im Identity Management. Eine gestohlene „digitale Identität“ ist heute immer das Einfallstor in ein Zielsystem. Mit der wachsenden Zahl von Benutzern (Mitarbeiter, Partner, Kunden …) erhöht sich auch die Angriffsfläche.

Für die Verwaltung von Benutzeridentitäten und Zugriffsrechten reicht eine IT-zentrierte Form des Identity Management alleine nicht mehr aus. Früher ging es beim Identity Management oft nur um die Automatisierung und Provisionierung der Benutzerverwaltung, um den eigenen Datenschutz- und Compliance-Richtlinien zu entsprechen. Heute geht es darum, in dem hoch dynamischen und kaum noch der eigenen Kontrolle unterliegenden Umfeld den Überblick zu behalten. Die Automatisierung bleibt auch weiterhin ein wichtiger Aspekt, die Frage der Steuerung und damit der Identity Governance rückt aber mehr in den Mittelpunkt.



Wie sieht ein zukunftsfähiges Identity und Access Management (IAM) aus?

Die Aufgabe von IAM bleibt im Kern immer gleich ist einfach zu beschreiben: **Sicherstellen, dass der Berechtigte auf alle benötigten Dienste zugreifen kann - und sonst auf nichts (Least Privilege).** Dazu gehören sowohl die Cloud-Dienste als auch die bestehende Infrastruktur, die vielleicht noch im eigenen Rechenzentrum betrieben wird oder per "lift & shift" in eine private Cloud verschoben wird. Für die meisten Unternehmen wird eine hybride IT auch in den kommenden Jahren der Regelfall bleiben. Das Identity und Access Management bedient dabei die gesamte hybride IT, bis hin zum sicheren und kontrollierten Zugriff auf IaaS-Umgebungen.

Micro Focus bietet mit dem Identity Manager ein ausgereiftes Produkt.

Als Pionier im Bereich Identitätsmanagement bietet Micro Focus mit dem NetIQ Identity Manager heute ein leistungsstarkes Produkt mit integriertem Rollenmanagement und weitegehenden Berichtsfunktionen. Das Produkt hat eine sehr große Verbreitung, ist ausgereift und unterstützt eine breite Palette von Zielsystemen mit individuell anpassbaren Konnektoren. Der auf dem Designer Tool basierende Ansatz ist bisher einmalig.

Wie unterstützt die Lanworks dabei?

Wir helfen dabei, diese neuen und komplexen Anforderungen nach Bedarf umzusetzen. Damit Sie den Betrieb souverän meistern und im Ausnahmefall gelassen reagieren. Wir unterstützen bei der Entwicklung sicherer und innovativer Lösungen für eine moderne IT.

Wir machen Expertenwissen wirksam.

Lanworks AG
IT Engineering • IT Training & Coaching
Fürstenwall 41 • 40219 Düsseldorf
Fon +49 211 95059-69