«Überstürzen Sie die Wahl einer Softwarelösung nicht»

In Zeiten des Homeoffice sei eine sichere Identitätsverwaltung zwingend, sagt Leo Bolshanin, Head of Cybersecurity Romandie bei AdNovum. Im Interview erklärt er, warum das so ist und worauf ein Unternehmen bei der Einführung einer solchen Lösung achten sollte. Interview: René Jaun

Cyberkriminelle nutzen die technologische Komplexität für Angriffe und binden so die Ressourcen der Security-Teams.

Leo Bolshanin, Head of Cybersecurity Romandie bei AdNovum

Digitale Identitäten sind seit Jahren ein Thema. Welche Herausforderungen bringen Unternehmen dazu, ihm eine höhere Priorität einzuräumen?

Leo Bolshanin: Durch die dezentrale Organisation von Firmen und die verteilte Zusammenarbeit stösst die konventionelle Perimetersicherheit an ihre Grenzen. Die Kommunikation lässt sich nicht mehr vollständig kontrollieren, da sie häufig ausserhalb des Firmennetzwerks erfolgt. Die IT-Infrastruktur ist dabei zunehmend hybrid: Unternehmen betreiben weiterhin lokale Systeme, nutzen aber auch Infrastrukturen, Plattformen und Anwendungen in der Cloud, wie Salesforce oder Office 365 Cloud. Parallel dazu steigt die Zahl der Anwendungen und Geräte unablässig, und die Nutzer sind an einfache digitale Tools gewöhnt und fordern ungehinderten Zugang, z.B. ohne Passwort.

Welchen Nutzen bringt die Einführung digitaler Identitäten einem Unternehmen?

Die identitätsbasierte Perimetersicherheit ergänzt die Systeme, mit denen wir unser Netzwerk bereits schützen. Die Kombination der beiden Instrumente erhöht die Sicherheit und ermöglicht eine feinmaschigere, flexiblere Kontrolle. Die Nutzer profitieren dabei von einfacheren Loginprozessen. Die Unternehmen ihrerseits steigern durch die Nutzung digitaler Identitäten die betriebliche Effizienz und die Resilienz im Fall von Cyberangriffen.

Welche Aspekte und Features sind bei einer Lösung zur Verwaltung digitaler Identitäten am wichtigsten?

Die Identitäts- und Zugriffsverwaltung muss für lokale Systeme und die Cloud vereinheitlicht werden. Die Lösung muss Governance-Tools bereitstellen, um den Lebenszyklus von Identitäten zu verwalten und Rezertifizierungen durchzuführen. Sie sollte ausserdem ein Compliance-Modul bieten und die Verwaltung von Privileged Accounts abdecken. Sowohl für mobile Geräte als auch für Workstations empfiehlt sich zudem die Einführung einer Multi-Faktor-Authentifizierung, die auch passwortfrei funktioniert. Die Stärke der Authentifizierung sollte sich dabei flexibel an den Grad des Risikos anpassen lassen. Die Lösung sollte weiter die Sicherheit der Geräte überprüfen können, welche die Nutzer für den Zugriff auf Anwendungen einsetzen, und sich gut in die digitale Landschaft des Unternehmens integrieren.

Worauf soll ein Unternehmen achten, das digitale Identitäten einführen will?

Überstürzen Sie die Wahl einer Softwarelösung nicht. Beginnen Sie damit, eine möglichst vollständige Liste der aktuellen und erwarteten Geschäftsanforderungen zu erstellen. Führen Sie als Nächstes eine Risikoanalyse durch, indem Sie als Erstes eine Liste der potenziellen Gefahren und der zu schützenden Daten und Infrastrukturen erstellen. Auf dieser Basis erarbeiten Sie eine Strategie für die Verwaltung digitaler Identitäten, die die Geschäftsanforderungen und die Risiken gleichermassen berücksichtigt. Die Strategie sollte langfristig ausgerichtet sein und eine Roadmap beinhalten. Schliesslich empfiehlt es sich, die Strategie agil umzusetzen, weil sie so leichter akzeptiert wird und Produktivitätseinbussen vermieden werden.