Studie

Zero Trust und passwortlose Zugänge

[01.09.2022] Das Access-Management-Unternehmen Okta hat eine globale Studie zu Zero Trust publiziert. Demnach holen Unternehmen in Europa bei der Umsetzung einer Zero-Trust-Strategie auf. Auch Behörden setzen auf Identity als Sicherheitskonzept, haben aber Nachholbedarf.

Dem IT-Sicherheitsmodell Zero Trust liegt zugrunde, dass keinem Akteur, der Zugang zu Diensten oder Ressourcen in einem Netzwerk verlangt, pauschal vertraut wird. Jeder Zugriff muss individuell authentifiziert werden – Benutzeridentitäten stehen im Mittelpunkt des Konzepts. Damit ist Zero Trust ein Gegenentwurf zu dem Konzept eines nach außen geschützten Netzwerks, in dessen Inneren sich User weitgehend ungehindert bewegen können.
Das auf Identitäts- und Zugriffsmanagement spezialisierte Unternehmen Okta hat jetzt zum vierten Mal seinen jährlich erscheinenden, globalen „State of Zero Trust Security Report“ vorgestellt. Demnach habe sich Zero Trust vom Buzzword in kurzer Zeit zu einer geschäftskritischen Notwendigkeit entwickelt. 97 Prozent der befragten Unternehmen gaben an, dass sie bereits eine Zero-Trust-Initiative eingeführt haben oder in den kommenden 12 bis 18 Monaten einführen werden. 2018 habe dieser Wert noch bei 16 Prozent gelegen – dies entspreche einem Anstieg von mehr als 500 Prozent in den vergangenen vier Jahren, so Okta.
Rund 700 Sicherheitsverantwortliche in Unternehmen weltweit und in vielen Branchen seien von Pulse Q&A für den Report befragt worden, gab Okta an.

Behörden im Hintertreffen

Doch nicht in allen Regionen und Branchen wurde die skizzierte Entwicklung vollzogen. So seien Unternehmen im Wirtschaftsraum Europa-Arabien-Afrika bei Zero-Trust-Strategien zögerlicher als in anderen Wirtschaftsräumen. Allerdings stiegen hier auch die Budgets deutlich. Derzeit erhöhten 90 Prozent der Unternehmen im Raum Europa-Arabien-Afrika ihre Investitionen.
Auch über die Branchen hinweg zeigen sich Unterschiede. Eine kennwortlose Authentifizierung ist oft Bestandteil von Zero-Trust-Konzepten, weil sie das Risiko von Kennwortdiebstahl und Phishing senken kann. In Finanzdienstleistungsunternehmen geben gemäß der Untersuchung von Okta knapp 22 Prozent aller Befragten an, in den kommenden 12 bis 18 Monaten die Einführung kennwortloser Zugangsoptionen zu planen. Bei Unternehmen aus dem Gesundheitswesen und der Software-Branche liege der Anteil bei 16 Prozent.
Behörden hinken hier allerdings noch hinterher: Nur sieben Prozent haben entweder bereits einen kennwortlosen Zugang eingerichtet oder planen dessen Implementierung in den kommenden Monaten Allerdings geben fast alle befragten Behörden weltweit an, dass Identity ein wichtiger Bestandteil ihrer allgemeinen Zero-Trust-Strategie sei, so die Studie. 19 Prozent sehen das Konzept gar als geschäftskritisch an.

(sib)

Zur Studie „The State of Zero Trust Security 2022“

Stichwörter: Digitale Identität, eID, Okta, Studie