ESET SECURE AUTHENTICATION

VERFÜGBAR ALS MANAGED SERVICE

TEIL DES MULTI-SECURED-ENDPOINT-KONZEPTS

SITUATION

Die Mitarbeiter eines Unternehmens sind unzufrieden mit den strengen Passwortregeln. Sie kritisieren, dass sie sich alle drei Monate ein neues, kompliziertes Kennwort ausdenken und merken müssen. Manche Kollegen kleben die Zugangsdaten daher gleich an ihr Endgerät – für das Unternehmen ein großes Sicherheitsrisiko. Der IT- und Datenschutzverantwortliche empfiehlt, mit einer Multi-Faktor-Authentifizierungslösung unsicheren Passwortmethoden ein Ende zu setzen.

UND JETZT?

Die Multi-Faktor-Authentifizierung sollte für die Mitarbeiter so bedienbequem wie möglich sein und bestehende Prozesse nicht unnötig kompliziert machen. Zudem darf die Lösung das IT-Budget nicht überstrapazieren. Ideal wäre eine Software-Lösung, die sich mit bestehenden Mobilgeräten nutzen lässt. Das hieße nämlich, dass sich ein Mitarbeiter weder auf neue Tools einlassen noch das Unternehmen zusätzliche Hardware anschaffen müsste.

ESET HAT DIE LÖSUNG

3 GRÜNDE FÜR ESET SECURE AUTHENTICATION

SICHERER LOGIN PER KNOPFDRUCK

ESET Secure Authentication sichert Zugänge mit einem zusätzlichen Faktor, ohne Nutzer zu überfordern. Die bequemste Bereitstellungsmöglichkeit funktioniert über eine Push-Nachricht auf ein Mobilgerät des Mitarbeiters, die er einfach per Klick bestätigt.

SAMTWEICHE EINBINDUNG

Die Sicherheitslösung unterstützt alle iOS- und Android-Mobilgeräte und lässt sich mit den geräteeigenen biometrischen Verfahren nutzen. Auch FIDO-basierte Sticks und andere Token werden unterstützt. Zusätzliche Hardware wird dabei nicht benötigt.

PASSWORTLOSE ANMELDUNGEN

Bedienbequem muss es sein: Passwortlose Umgebungen per Single Sign-On lassen sich dank der Unterstützung des SAML-Protokolls in die Praxis umsetzen. Mit der Integration von Windows Hello und FIDO-basierter Hardware sind auch passwortlose Window-Logins möglich.

DIE WICHTIGSTEN EIGENSCHAFTEN IN KÜRZE:

- große Flexibilität in puncto Lizenzform, Authentifizierungmethodik, Hardwareeinsatz und Anforderungen an die Infrastruktur
- vielfältige Authentifizierungsmöglichkeiten: Push-Benachrichtigung, Einmal-Passwort via App, SMS oder Hardware-Token
- unterstützt die biometrischen Authentifizierungsverfahren eingesetzter Mobilgeräte (Android und iOS)
- schützt Windows- und Server-Logins, Cloud- und Webanwendungen wie Google-Dienste, Microsoft 365 oder Dropbox, RDP und VPNs
- Realisierung von passwortlosen Umgebungen via Single Sign-On dank Unterstützung des SAML-Protokolls
- Whitelisting von IP-Bereichen und bestimmten Anwendungen zum Finetuning der Multi-Faktor-Authentifizierung