



SECURE AUTHENTICATION

Multi-Faktor-Authentifizierung von einem
der führenden IT-Security Anbieter für noch
besseren Schutz Ihrer Integrität

CYBERSECURITY
EXPERTS ON YOUR SIDE

ESET.DE | ESET.AT | ESET.CH



Was ist eigentlich eine **Multi-Faktor- Authentifizierung?**

Bei der Multi-Faktor-Authentifizierung (MFA), oft auch als Zwei-Faktor-Authentifizierung (2FA) bekannt, handelt es sich um eine Authentifizierungsmethode, bei der sich Nutzer mit mehr als einem Element ausweisen müssen. 2FA ist so wesentlich sicherer als althergebrachte, statische Passwortabfragen. Durch Kombination eines statischen Passworts mit einem zweiten, dynamischen Faktor wird die Gefahr von Datenverlusten bedeutend verringert.

Mit ESET Secure Authentication implementieren Unternehmen jeder Größe simpel eine MFA für gemeinsam verwendete Systeme (Windows- & Server-Logins, Microsoft Cloud-Dienste wie Microsoft 365 oder OWA, VPNs und RADIUS-basierte Dienste).

Drei gute Gründe

Oft wird dasselbe Passwort für mehrere Anwendungen und Webseiten verwendet, notiert oder an Dritte weitergegeben.

UNZUREICHENDE PASSWORTPFLEGE

Häufig gelten Mitarbeiter als „größte Schwachstelle“ der IT-Sicherheit eines Unternehmens. Vor allem schlecht gepflegte Passwörter stellen eine große Gefahr für das Business dar. Oft wird dasselbe Passwort für mehrere Anwendungen und Webseiten verwendet, notiert oder an Dritte weitergegeben. Klassische Gegenmaßnahmen wie die Pflicht, Passwörter regelmäßig zu ändern, bringen dabei oft wenig und führen noch mehr in Versuchung, ähnliche Passwörter zu verwenden oder Post-its mit den wichtigsten Kennwörtern an den Rechner zu heften.

Eine Multi-Faktor-Authentifizierung schützt Unternehmen vor diesen Risiken, indem die reguläre Anmeldung um einen zusätzlichen Faktor erweitert wird – z.B. durch die Bestätigung einer Push-Authentifizierung auf das eigene Mobilgerät oder die Nutzung eines Hardware-Tokens in Verbindung mit Ihrem Fingerabdruck. Damit schützen Sie sich vor Angreifern, die versuchen, durch einfaches Erraten schwacher Passwörter Zugang zu Ihren Systemen und Cloud-Anwendungen zu erlangen.

DATENSCHUTZ-VERLETZUNGEN

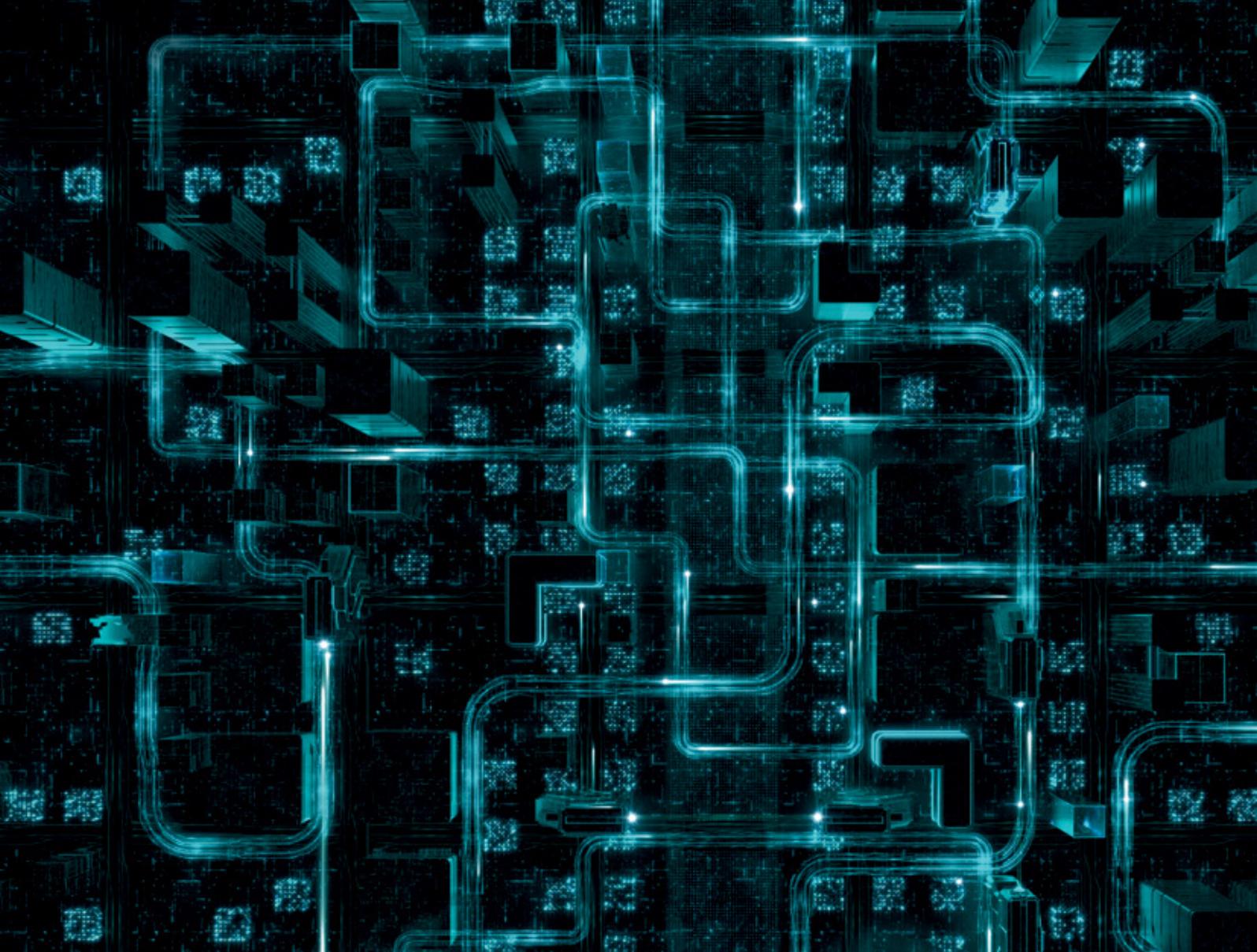
Beinahe täglich wird von Datenschutzverstößen in Unternehmen berichtet. Oft gelangen Angreifer über schwache oder gestohlene Zugangsdaten in das Unternehmensnetzwerk, die sie durch automatisierte Bots, Phishing oder zielgerichtete Angriffe ergattern. Über die Absicherung von Logins hinaus kann die MFA auch privilegierte Zugänge vor unautorisierten Zugriffen schützen.

Mit einer Multi-Faktor-Authentifizierung ist es für Angreifer wesentlich schwerer, Zugriff auf Ihre Systeme und Daten zu erlangen. In der Regel sind Unternehmen von Datenschutzvorfällen betroffen, die mit sensiblen Informationen arbeiten. Dazu gehören insbesondere die Finanzbranche, der Einzelhandel, das Gesundheitswesen und der öffentliche Sektor. Das heißt jedoch keineswegs, dass andere Branchen sicher sind. Wie jeder andere „Unternehmer“ wägen professionelle Hacker Kosten und Nutzen eines Angriffs sorgfältig ab. Entsprechend sollte man es Ihnen so schwer wie möglich machen.

COMPLIANCE

Unternehmen müssen zunächst prüfen, ob sie Datenschutzvorgaben unterliegen oder nicht. Anschließend sollten sie ermitteln, welche Maßnahmen die Vorgaben empfehlen bzw. vorschreiben. Eine starke Authentifizierung ist mittlerweile integraler Bestandteil gesetzlicher und anderer Vorgaben, darunter der EU-DSGVO.

Vor allem Unternehmen, die mit Kreditkarteninformationen oder Gesundheitsdaten arbeiten, sind verpflichtet, den Schutz dieser Daten zu gewährleisten und entsprechende Maßnahmen vorzunehmen. Aber auch alle anderen Firmen sollten sorgfältig prüfen, ob bzw. an welche Datenschutzvorgaben sie gebunden sind.



Bei Nutzung einer Zwei-Faktor-Authentifizierung können Hacker Zugangsdaten nicht einfach erraten und entweder selbst verwenden oder zum Verkauf anbieten.

Nicht umsonst enthalten viele gesetzliche Vorgaben die Pflicht zu Multi-Faktor-Authentifizierung. Die meisten Datenlecks werden durch gestohlene oder schwache Passwörter verursacht.

Authentifizierung via Push-Benachrichtigung



ESET bietet einfach mehr

WÄHLEN SIE IHRE INTEGRATIONS-METHODE

ESET Secure Authentication bietet zwei verschiedene Integrationsmöglichkeiten. Innerhalb eines Windows-Netzwerks lässt sich die Sicherheitslösung ins Active Directory integrieren, für Unternehmen ohne Windows-Domain steht der Stand-Alone-Modus bereit.

KEINE ZUSÄTZLICHE HARDWARE NÖTIG

ESET Secure Authentication erfordert keine zusätzliche Hardware. Nach der Installation der Anwendung auf Ihrem Server können Sie umgehend mit der Bereitstellung starten.

UNTERSTÜTZUNG ALLER GÄNGIGEN MOBILGERÄTE

Ihre Mitarbeiter können bereits eingesetzte Mobilgeräte weiter nutzen. ESET Secure Authentication ist für die Verwendung auf allen iOS- und Android-Mobilgeräten geeignet. Für noch mehr Schutz und Bedienkomfort kann die App mit den Geräte-eigenen biometrischen Verfahren (Touch ID, Face ID, Android Fingerprint) genutzt werden.

IN 10 MINUTEN EINSATZBEREIT

Bei der Entwicklung von ESET Secure Authentication haben wir darauf geachtet, die Installation so einfach wie möglich zu gestalten. Unabhängig von Ihrer Firmengröße beansprucht die Installation von ESET Secure Authentication dank der Möglichkeit, mehrere Nutzer gleichzeitig einzurichten, nur wenig Zeit.

EINSCHLIESSLICH SDK UND API

Zur individuellen Anpassung der Funktionalitäten stellen wir sowohl ein SDK als auch eine API bereit. So können Unternehmen ESET Secure Authentication nach ihrem Bedarf erweitern und die Nutzung auf eigene Anwendungen oder Webservices ausweiten.

VON PUSH-AUTHENTIFIZIERUNG BIS ZUR PASSWORTLOSEN UMGEBUNG

Bequeme Authentifizierung ohne Eingabe eines Einmal-Passworts über die Bestätigung einer Push-Benachrichtigung. Die Nutzung vorhandener Hardware-Tokens oder sogar beinahe passwortlose Umgebungen per Fingerabdruck und FIDO2-Sticks in Verbindung mit dem SAML Standard funktioniert auf iOS- und Android-Mobilgeräten.

„Einfachste Installation, Setup und Integration ins Active Directory. Einer der größten Vorteile war für uns, dass unsere Mitarbeiter sich per App authentifizieren können und nicht andauernd SMS bekommen. Außerdem ließ es sich völlig unkompliziert in unser bestehendes VPN-Setup integrieren.“

— Tom Wright, IT Service Officer, Gardners Books

So funktioniert's

Datenlecks vermeiden

Immer wieder wird von Datenschutz-Vorfällen berichtet, bei denen Unternehmen ihre Kunden nicht über Datenlecks informiert haben.

LÖSUNG

- ✓ Schützen Sie sensible Kommunikation wie z.B. das Remote Desktop Protokoll mithilfe der Multi-Faktor-Authentifizierung.

- ✓ Richten Sie für alle im Unternehmen verwendeten VPNs eine 2FA ein.

- ✓ Verwenden Sie MFA, um den Zugriff auf Geräte mit Cloud-Diensten oder internen Ressourcen abzusichern.

- ✓ Schützen Sie sensible Unternehmensdaten mit ESET Endpoint Encryption.

ESET SICHERHEITSLÖSUNG

- ✓ ESET Secure Authentication

- ✓ ESET Endpoint Encryption

Sichere Logins

Oftmals werden in Unternehmen Rechner und Arbeitsplätze genutzt, an denen sich täglich viele unterschiedliche Nutzer anmelden.

LÖSUNG

- ✓ Mit einer Zwei-Faktor-Authentifizierung sind geteilte Rechner umfassend geschützt.

ESET SICHERHEITSLÖSUNG

- ✓ ESET Secure Authentication

Verstärkung für Passwörter

Nicht selten verwenden Mitarbeiter dieselben Passwörter für verschiedene Anwendungen und Webseiten. Für Unternehmen ein hohes Sicherheitsrisiko.

LÖSUNG

- ✓ Schützen Sie Unternehmensressourcen durch Multi-Faktor-Authentifizierung.

- ✓ Durch die Verwendung einer Multi-Faktor-Authentifizierung stellen selbst unsichere oder gar gestohlene Passwörter kaum noch eine Bedrohung dar.

ESET SICHERHEITSLÖSUNG

- ✓ ESET Secure Authentication



Technische Features und unterstützte Plattformen

PUSH-AUTHENTIFIZIERUNG

Authentifizierung über die Bestätigung einer Push-Benachrichtigung. Funktioniert mit iOS- und Android-Mobilgeräten.

WEITERE AUTHENTIFIZIERUNGSMÖGLICHKEITEN

ESET Secure Authentication unterstützt Push-Benachrichtigungen, die Bereitstellung von Einmal-Passwörtern über die mobile Client-App, SMS oder bestehende Hardware-Token sowie FIDO-basierte Sticks in Verbindung mit Biometrie oder Windows Hello.

REMOTE MANAGEMENT

Zentrale Verwaltung über die ESET Secure Authentication Web-Konsole. Die Lösung lässt sich einfach in Ihr bestehendes Active Directory integrieren und funktioniert zudem auch in kleinen Unternehmen ohne Windows-Domain.

ABGESICHERTE ZUGÄNGE

ESET Secure Authentication unterstützt VPNs, RDP und Outlook Web Access (OWA) ebenso wie VMWare Horizon View und RADIUS-basierte Dienste.

ZUSÄTZLICHER LOGIN-SCHUTZ

Desktop-Logins und privilegierte Zugänge können ebenfalls durch die MFA Sicherheitslösung geschützt werden. Unterstützt sowohl Windows als auch macOS und Linux.

CLOUD-SUPPORT

Nutzen Sie die MFA zur Absicherung Ihrer Zugänge zu Diensten wie Google-Dienste, Microsoft 365 und Dropbox. ESET unterstützt die Integration über das SAML-2 Protokoll, das viele Identity Provider einsetzen.

UNTERSTÜTZUNG VON TOKEN

Während die Nutzung von Hardware-Token nicht erforderlich ist, unterstützt die Sicherheitslösung alle ereignisbasierten OATH-konformen HOTP/TOTP-Token sowie FIDO2 und FIDO U2F Hardware-Schlüssel.



Über ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie, unterstützen Ihren Datenschutz mit Hilfe von 2FA und zertifizierten Verschlüsselungsprodukten oder halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen.

Unsere Endpoint Detection and Response Lösungen und Frühwarnsysteme wie Threat Intelligence Services ergänzen das Angebot im Hinblick auf gezielte Cyberkriminalität, APTs und Forensik. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien wie KI oder Machine Learning, sondern kombiniert Erkenntnisse aus dem eigenen LiveGrid (Reputationssystem) mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN



Seit 2017 durch ESET geschützt
Mehr als 9.000 Endgeräte



Seit 2016 durch ESET geschützt
Mehr als 14.000 Endgeräte



ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT



ESET wurde das Vertrauensiegel „IT Security made in EU“ verliehen



Cloud-Lösungen und Dashboards sind nach Qualitätsstandards entwickelt

ESET IN ZAHLEN

110+ Mio.

Nutzer weltweit

400k+

Business-Kunden

200+

Länder & Regionen

13

Forschungs- und Entwicklungszentren weltweit



welive
security™
ESET