Autentificarea pe înțelesul tuturor

SYS Admin TIPS

Top sfaturi pentru securizarea accesului

Work from home

De ce autentificarea multi-factor este esențială pentru accesul de la distanță?

Soluțiile de autentificare multi-factor (MFA) necesită două sau mai multe informații independente pentru verificarea identității unui utilizator. Opțiunea MFA este mult mai puternică decât parolele tradiționale, statice sau autentificarea printr-un PIN.

Peste 80% dintre companii dețin informații de identificare personală (IIP) despre clienții lor, precum și despre proprii angajați.

Sursa: Date colectate de la peste 27.000 de participanți - majoritatea din Uniunea Europeană (UE) prin formularul de verificare a conformității între noiembrie 2017 și mai 2018.

Reducerea riscului aferent forței de muncă de la distanță

Trecerea bruscă la o modalitate de lucru de acasă, cauzată de pandemia COVID-19, a evidențiat necesitatea protejării accesului la sistemele business și la cele critice care prelucrează date cu caracter personal. Numărul ridicat de autentificări necesită măsuri adecvate care să diminueze riscurile la care sunt supuși angajații de la distanță. Prin adăugarea unui nivel suplimentar de securitate la nivelul autentificării, pe lângă un nume de utilizator și o parolă care pot fi ușor compromise, **ESET Secure Authentication îmbunătățește semnificativ securitatea rețelei companiei și a datelor care provin din exterior.**

Eliminați practicile slabe de setare a unei parole

Practicile slabe de setare a unei parole reprezintă un risc semnificativ de securitate cibernetică. Nu doar că unii angajații utilizează parole identice pe mai multe site-uri web și aplicații, ci le comunică uneori prietenilor, familiei și colegilor. Chiar și în cazul în care companiile aplică reguli stricte de configurare a parolelor, acest lucru îi poate determina pe angajați să folosească variante ale parolelor vechi sau să își scrie parolele pe bucăți de hârtie.

Breșe de date

Unul dintre cele mai frecvente moduri în care hackerii pot avea acces la datele dvs. este prin subtilizarea parolelor sau printr-un atac targetat. Prin adăugarea unei soluții MFA, companiile adaugă un strat suplimentar de securitate, îngreunând accesul infractorilor cibernetici la sistemele lor. În mod tradițional, **principalele ținte** pentru breșele de date sunt **organizațiile din domeniile financiar, retail, asistență medicală și cele din sectorul public**, dar hackerii nu se opresc doar aici.

Conformitate

O parte dintre reglementările de conformitate impun MFA, iar majoritatea subliniază necesitatea unor practici de autentificare mai puternice, inclusiv regulamentul GDPR. **Autentificarea multi-factor nu mai este o soluție opțională.** Agențiile de reglementare, cum ar fi ENISA, recomandă constant această metodă companiilor care gestionează cărți de credit sau tranzacții financiare. Toate organizațiile ar trebui să își evalueze conformitatea.

Implementarea autentificării multi-factor

ESET Secure Authentication oferă o modalitate ușoară de implementare a MFA pe sistemele cel mai comun utilizate precum comexiuni VPN, Remote Desktop, Office 365, Outlook Web Access, autentificarea în sistemele de operare și altele.

80% din brețele de hacking implică credențiale compromise sau care nu aveau parole suficient de puternice.

Source: Verizon 2017 Data Breach Investigations Report, 10th Edition

CÂT DE UȘOR ESTE PENTRU UN ADMINISTRATOR SĂ IMPLEMENTEZE MFA?

- Configurare ușoară în câteva minute
- Nu este necesară instruirea angajaților
- Administrare intuitivă de la distanță
- Fără costuri suplimentare de infrastructură
- Suporta numeroase VPN-uri și servicii cloud

CÂT DE UȘOR ESTE PENTRU UTILIZATORII DVS. SĂ UTILIZEZE ACEASTĂ METODĂ?

- Nu este nevoie de parole din ce în ce mai complexe
- Funcționează cu orice smartphone
- Soluție single-tap, nu este nevoie să reintroduceți parolele
- Nu sunt necesare token-uri hardware suplimentare
- Extrem de ușor de utilizat

Utilizarea ESET Secure Authentication este posibilă pe un număr nelimitat de dispozitive business

UTILIZATOR

1
Protejați accesul la **sistemul de operare** de pe stațiile de lucru

2
Securizați datele stocate ale companiei în **aplicații sau servicii cloud**

APLICAȚII GOOGLE
OFFICE 365
DROPBOX
CONFLUENCE
ȘI MULTE ALTELE

3
Asigurați-vă că **VPN-ul** companiei permite accesul doar utilizatorilor autentificați

BARRACUDA
CISCO ASA
CITRIX ACCESS GATEWAY
CHECK POINT SOFTWARE
CYBEROAM
F5 FIREPASS
FORTINET FORTIGATE
JUNIPER
PALO ALTO
ȘI MULTE ALTELE

ADMINISTRATOR

4
Îmbunătățiți controlul accesului pentru **Remote Desktop Protocol (RDP)**

5
Implementați MFA pentru aplicațiile **Microsoft Web**

OUTLOOK WEB APP (OWA)
EXCHANGE CONTROL PANEL
SHAREPOINT
REMOTE DESKTOP WEB ACCESS
TERMINAL SERVICES WEB ACCESS

6
Integrați MFA cu orice **furnizor de identitate** care suportă SAML 2.0

OKTA
OPENAM
AZURE AD
AD FS
SHIBBOLETH

Protejați-vă datele acum, achiziționați soluția târziu. Descărcați un trial full gratuit, fără obligații.