RENDERE SICURO IL LAVORO IN REMOTO PER LE PMI

Elementi essenziali di protezione dei dati: l'autenticazione resa semplice

Perché l'autenticazione a più fattori è essenziale per l'accesso remoto

Le soluzioni di autenticazione a più fattori (MFA, multi-factor authentication) richiedono due o più informazioni indipendenti per verificare l'identità di un utente. La MFA è molto più efficace delle password statiche tradizionali o dell'autenticazione tramite PIN.

Oltre l'80% delle aziende detiene informazioni di identificazione personale (PII) sui propri clienti, come anche sui propri dipendenti.

Fonte: dati raccolti da oltre 27.000 partecipanti, principalmente dall'Unione europea (UE) tramite la verifica di conformità, tra novembre 2017 e maggio 2018

Ridurre il rischio relativo alla forza lavoro in remoto

L'improvviso passaggio al lavoro da casa causato dalla pandemia COVID-19, un evento di una portata senza precedenti, ha messo in evidenza, in maniera chiara, la necessità di proteggere l'accesso ai sistemi aziendali critici e ai sistemi che elaborano i dati personali. Il numero di tentativi di accesso, aumentato a livello esponenziale, richiede misure appropriate per prevenire il rischio legato alla forza lavoro in remoto. Aggiungendo un altro livello di autenticazione oltre al normale nome utente e password, che possono essere facilmente compromessi, **ESET Secure Authentication migliora significativamente la sicurezza della rete aziendale e dei dati immessi provenienti dall'esterno.**

Eliminare la scarsa attenzione alle password

L'utilizzo di password deboli rappresentano un rischio significativo per la sicurezza informatica. Non solo i dipendenti utilizzano password identiche su più siti Web e applicazioni, ma a volte condividono le proprie password con amici, familiari e colleghi. Sebbene le aziende rafforzino le proprie politiche sulle password, i dipendenti continuano ad utilizzare delle varianti della password precedente o a scrivere le proprie password su dei foglietti adesivi.

Violazione dei dati

Una delle modalità più comuni con cui gli hacker riescono ad accedere ai propri dati è attraverso la sottrazione di password o tramite un attacco mirato. Tramite l'aggiunta di una soluzione MFA, le aziende rendono molto più difficile agli hacker l'accesso ai propri sistemi. Solitamente, **gli obiettivi principali delle violazioni di dati sono organizzazioni finanziarie, di vendita al dettaglio, sanitarie e del settore pubblico**. Tuttavia, gli hacker ora stanno prendendo di mira anche altri settori.

Conformità

Diverse normative sulla conformità impongono soluzioni di autenticazione a più fattori (MFA) e la maggior parte sottolinea la necessità di pratiche di autenticazione più rigorose, tra cui il GDPR e HIPAA. **L'autenticazione a più fattori non è più una soluzione facoltativa.** Le agenzie di regolamentazione come l'ENISA la raccomandano vivamente per le aziende che gestiscono carte di credito o transazioni finanziarie. Tutte le organizzazioni dovrebbero valutarne la conformità.

Implementazione dell'autenticazione a più fattori

ESET Secure Authentication fornisce un modo semplice per implementare soluzioni MFA sui sistemi di comune utilizzo, come VPN, Remote Desktop, Office 365, Outlook Web Access, l'accesso al sistema operativo e altri.

L'80% delle violazioni correlate all'hacking riguarda credenziali compromesse e deboli.

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

QUANTO È FACILE PER L'AMMINISTRAZIONE?

- Installazione facile in pochi minuti
- Non è richiesta la formazione dei dipendenti
- Gestione remota completamente intuitiva
- Nessun costo di infrastruttura aggiuntivo
- Supporta numerose VPN e servizi cloud

QUANTO È FACILE PER GLI UTENTI?

- Non sono necessarie password sempre più complesse
- Funziona con qualsiasi smartphone
- Soluzione a singola digitazione, non è necessario digitare nuovamente le password
- Non sono necessari token HW aggiuntivi
- Estremamente facile da usare

Utilizzo di ESET Secure Authentication in un numero sempre crescente di dispositivi e ambienti

PARTE DELL'UTENTE

1

Proteggere l'accesso al **sistema operativo** della postazione di lavoro dei dipendenti

2

Proteggere i dati della propria azienda archiviati con **app e servizi cloud**

APP DI GOOGLE
OFFICE 365
DROPBOX
CONFLUENCE
E MOLTI ALTRI

3

Assicurarsi che la VPN consenta l'accesso solo agli utenti autenticati

BARRACUDA
CISCO ASA
CITRIX ACCESS GATEWAY
CHECK POINT SOFTWARE
CYBEROAM
F5 FIREPASS
FORTINET FORTIGATE
JUNIPER
PALO ALTO
E MOLTI ALTRI

PARTE DELL'AMMINSTRAZIONE

4

Rafforzare il controllo degli accessi per il **Remote Desktop Protocol (RDP)**

5

Utilizzo di MFA con **App Web Microsoft**

OUTLOOK WEB APP (OWA)
PANNELLO DI CONTROLLO DI SCAMBIO SHAREPOINT
ACCESSO WEB DESKTOP REMOTO
ACCESSO WEB AI SERVIZI TERMINAL

6

Integrare le MFA con qualsiasi **provider di identità** che supporti SAML 2.0

OKTA
OPENAM
AZURE AD
AD FS
SHIBBOLETH

Proteggi i tuoi dati ora, acquista in seguito. Ottieni una prova gratuita dalle funzionalità complete.

AUTENTICAZIONE SICURA ESET