SECURE AUTHENTICATION

Dvoufaktorová autentizace přístupu do sítě
a k jejímu obsahu

Progress. Protected.

Co je **vícefaktorová autentizace?**

Vícefaktorové ověřování (MFA), také známé jako dvoufaktorové ověřování (2FA), je metoda autentizace, která k verifikaci identity uživatele vyžaduje dvě nezávislé informace. MFA je mnohem silnější než tradiční zabezpečení pomocí hesla nebo kódu PIN. Doplnění tradičního ověřování o dynamický druhý faktor (aplikace, která generuje jednorázová hesla) účinně snižuje riziko úniku dat způsobeného slabými nebo ukradenými hesly.

ESET Secure Authentication nabízí firmám všech velikostí možnost jednoduše implementovat vícefaktorovou autentizaci do běžně používaných systémů, jako jsou VPN, RDP, Microsoft Office 365, Outlook Web Acces nebo přihlašování do systému.

Digital Security
Progress. Protected.

Proč **dvoufaktorová autentizace?**

Vícefaktorové ověřování může pomoci kompenzovat rizika „credential stuffing“ - útoku, který zneužívá informace o zaměstnancích. K tomuto riziku přispívají ti, kteří:

- používají stejné heslo ve více aplikacích a webech,
- sdílejí hesla s ostatními,
- při aktualizaci hesel provádějí pouze drobné změny.

SLABÁ HESLA

Zaměstnanci jsou při ochraně firemní sítě nejslabším článkem řetězce. Největším neduhem už nejsou jen slabá hesla, ale celkový způsob, jak s nimi uživatelé zacházejí. Není výjimkou, že zaměstnanci používají jedno heslo pro přihlášení k různým účtům a službám. V horším případě je rovnou sdílejí s kolegy nebo rodinou. Slabá hesla se sice dají jednoduše vyřešit bezpečnostní politikou, nicméně u těžko zapamatovatelného hesla hrozí riziko, že si ho uživatelé poznačí na papír, který si vystaví na dobře viditelné místo.

Přidáním druhého faktoru do procesu přihlášení (např. v podobě jednorázového hesla v aplikaci) se riziko neoprávněného přístupu do sítě sníží na minimum.

ÚNIKY DAT

Ztráta a zneužití citlivých dat jsou v současnosti jednou z nejčastějších forem počítačové kriminality. Cesta k zisku cenných dat obvykle vede přes slabá nebo ukradená hesla. Pokud firma používá při přihlašování dvoufaktorovou autentizaci, například s využitím mobilního telefonu, značně se snižuje riziko průniku do sítě a odcizení cenných firemních dat.

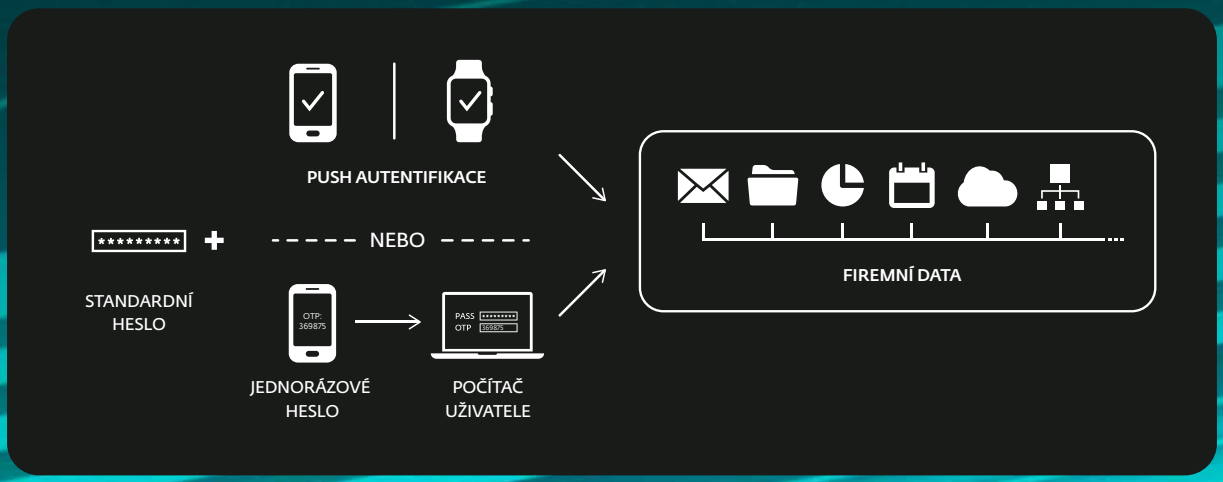
Je logické, že nejohroženějšími firmami jsou tradičně finanční instituce, banky, pojišťovny a veřejný sektor. Ale ani menší společnosti nejsou úplně v bezpečí. Útočníci vždy poměřují riziko útoku s možným výdělkem. Pokud tedy usoudí, že se jim vyplatí zaútočit na malou firmu, pak to udělají.

SOULAD

Firmy by si měly nejprve ověřit, zda musejí vyhovět nějaké zákonné normě, či nikoli. Dalším krokem je zjistit, jaké požadavky daná norma doporučuje a nařizuje zavést. V případě dvoufaktorové autentizace jde o PCI-DSS a GLBA. Nařízení a zákony, jako jsou například GDPR a HIPAA, obecně vyžadují silnou autentizaci přístupu do firemní sítě.

Vícefaktorové ověření proto ve většině případů není jen volitelným způsobem ochrany přístupu, ale vyžadovaným řešením. V dnešním globálním světě se povinnost dodržovat specifické regulační normy, které řídí podnikání, týká stále většího počtu firem a organizací.

Autentizace pomocí jediného kliknutí bez nutnosti přepisovat jednorázové heslo



Technické specifikace

PUSH AUTENTIZACE

Jedním ťuknutím na notifikaci v mobilním telefonu (iOS, Android).

PODPORA CLOUDOVÝCH SLUŽEB

ESET Secure Authentication podporuje webové a cloudové služby typu Google Workspace, Dropbox, Microsoft 365 a mnohé další. Aplikace podporuje integraci přes autentizační protokol SAML-2, který používá většina výrobců.

RYCHLÉ NASTAVENÍ

Vývoj měl za cíl vytvořit produkt, který půjde snadno instalovat a rychle používat. Instalaci ESET Secure Authentication lze dokončit během 10 minut, přičemž nezáleží na počtu uživatelů nebo velikosti firmy.

DALŠÍ ZPŮSOBY AUTENTIZACE

ESET Secure Authentication podporuje doručení jednorázového hesla přes mobilní aplikaci, push notifikaci, lze ji integrovat s biometrickými údaji zařízení (Touch ID, Face ID, otisk prstu v systému Android). V případě potřeby podporuje také hardwarové tokeny nebo bezpečnostní klíče FIDO.

PODPOROVANÉ VPN

VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall a vlastní integraci s libovolnou VPN používající RADIUS.

JEDNODUCHÁ INTEGRACE

Řešení nabízí dva režimy integrace - integraci se službou Active Directory pro organizace používající doménu Windows nebo samostatný režim, který je vhodný pro organizace bez domény. V obou případech je nastavení a konfigurace rychlá a snadná, vše se spravuje bez problémů prostřednictvím cloudové konzole.

NENÍ POTŘEBA ŽÁDNÝ SPECIÁLNÍ HARDWARE

Veškeré náklady na ESET Secure Authentication jsou promítnuty do samotného produktu, takže není potřeba žádný specializovaný hardware. Stačí nainstalovat řešení na libovolný server a můžete začít zřizovat uživatelské přístupy.

MULTITENANTNÍ

Cloudová verze ESET Secure Authentication byla navržena s možností správy více tenantů, aby poskytovatelé řízených služeb (MSP) mohli spravovat více společností nebo lokalit a mohli flexibilně definovat specifická nastavení pro jednotlivé skupiny uživatelů.

SDK A API

S pomocí API lze integrovat řešení do existujícího autentifikačního systému založeného na Active Directory. Aplikace obsahuje nástroje SDK, pomocí kterých můžete řešení implementovat do libovolného vlastního systému – i bez dedikovaného pluginu.

Výhody ESETu

Ověření identity uživatele

Pokud firma umožňuje zaměstnancům sdílet pracovní zařízení, je nutné zajistit jednoznačné ověření identity daného uživatele.

ŘEŠENÍ

- ✓ Implementace vícefaktorového přihlašování na všechna sdílená zařízení

PRODUKTY ESET

- ✓ ESET Secure Authentication

Posílení ochrany hesel

Uživatelé často používají jedno heslo napříč aplikacemi a službami a nechtěně tak vystavují riziku i firemní data.

ŘEŠENÍ

- ✓ Omezení přístupu k citlivým datům zavedením multifaktorové autentizace
- ✓ Zavedení druhého faktoru v podobě jednorázového hesla snižuje riziko zneužití ukradeného hesla na minimum

PRODUKTY ESET

- ✓ ESET Secure Authentication

Prevence průniku do sítě

Průniky do sítě a odcizení citlivých firemních dat jsou v současnosti jednou z nejčastějších podob počítačové kriminality.

ŘEŠENÍ

- ✓ Ochrana zranitelné komunikace, jako je vzdálená plocha, přidáním druhého faktoru do přihlašovacího procesu
- ✓ Přidání multifaktorové autentizace ke všem existujícím VPN
- ✓ Používání multifaktorové autentizace pro přihlášení k zařízením, která obsahují citlivá data
- ✓ Ochrana citlivých dat pomocí ESET Endpoint Encryption

PRODUKTY ESET

- ✓ ESET Secure Authentication
- ✓ ESET Endpoint Encryption

Technické funkce

FUNKCE	POPIS	
MULTITENANTNÍ Dostupné pouze v cloudové verzi	Více lokalit/firem	✓
OCHRANA LOKÁLNÍHO PŘIHLÁŠENÍ	Přihlášení do Windows	✓
OCHRANA VZDÁLENÉHO PŘIHLÁŠENÍ	Radius Server for VPN Protection	✓
	Vzdálená plocha	✓
OCHRANA WEBOVÝCH APLIKACÍ	Microsoft Exchange Server	✓
	Microsoft SharePoint Server	✓
	Remote Desktop Web Access	✓
	Microsoft Dynamics CRM	✓
	Remote Web Access	✓
OCHRANA ACTIVE DIRECTORY FEDERATION SERVICES (AD FS)		✓
IDENTITY PROVIDER CONNECTOR (SAML)		✓
PROXY		✓
API		✓
IP WHITELISTING	Globální IP Whitelisting	✓
	Podle funkce IP Whitelisting	✓
ZPŮSOB AUTENTIZACE	OTP pomocí SMS	✓
	OTP v mobilní aplikaci	✓
	Push notifikace v mobilní aplikaci	✓
	HW tokeny	✓
	FIDO	✓
NOTIFIKACE	Problém	✓
	Přihlášení do webové konzole	✓
	Uzamčený uživatel	✓
	Odemčený uživatel	✓
	Licence	✓
THROTTLING	Throttling v závislosti na čase	✓
PROTOKOLY A ZPRÁVY	Report	✓
	Filtr	✓
	Export	✓

O ESETu

Digitální zabezpečení nové generace

MALWAROVÉ HROZBY UMÍME ZASTAVIT, ALE PŘEDEVŠÍM JIM PŘEDCHÁZÍME.

Na rozdíl od běžných řešení, která se zaměřují na reakci na již aktivní hrozby, nabízí společnost ESET bezkonkurenční preventivní přístup využívající umělou inteligenci, lidské znalosti, renomovanou globální službu Threat Intelligence a rozsáhlou síť výzkumných a vývojových center.

Využijte jedinečnou ochranu proti ransomwaru, phishingu, hrozbám nultého dne a cíleným útokům s oceňovanou cloudovou platformou kybernetické bezpečnosti XDR, která kombinuje prevenci nové generace, detekci a proaktivní vyhledávání hrozeb. Naše bezpečnostní řešení mají minimální dopad na výkon koncových zařízení, identifikují a neutralizují vznikající hrozby dřív, než vás mohou ohrozit, zajišťují kontinuitu provozu a snižují náklady na implementaci a správu. Samozřejmostí je obchodní i technická podpora v českém jazyce.

ESET V ČÍSLECH

1mld+
chráněných uživatelů na internetu

400k+
firemních zákazníků

200
zemí a teritorií

13
vývojových center

NAŠI ZÁKAZNÍCI

MITSUBISHI MOTORS
Drive your Ambition

Zákazníkem od roku 2017, více než 9 000 licencí

Allianz Suisse

Zákazníkem od roku 2016, více než 4 000 mailboxů

Canon
Canon Marketing Japan Group

Zákazníkem od roku 2016, více než 32 000 licencí

T

ISP partnerem od roku 2008, 2 miliony zákazníků

VYBRANÁ OCENĚNÍ

AV comparatives APPROVED Business Security JUL 2023

V červenci 2023 ESET získal ocenění „APPROVED" za ochranu koncových řešení v business security testu společnosti AV-Comparatives.

G2 Leader WINTER 2024

ESET trvale dosahuje špičkových výsledků na celosvětové platformě hodnocení uživatelů G2 a jeho řešení jsou oceňována zákazníky po celém světě.

kuppingercole ANALYSTS

Podle KuppingerCole Leadership Compass 2023 je ESET uznáván jako lídr trhu a celkový lídr v oblasti MDR.

eset® Digital Security
Progress. Protected.