PREHĽAD

SECURE AUTHENTICATION

Efektívna dvojfaktorová autentifikácia
pre bezpečnejší prístup do sietí a k dátam

Progress. Protected.

Čo je **dvojfaktorová autentifikácia**?

Dvojfaktorová autentifikácia na overenie identity používateľa vyžaduje dve nezávislé množiny informácií. Je oveľa účinnejšia než tradičné overenie pomocou statického hesla alebo PIN kódu. Doplnením bežného overovania o dynamický druhý faktor sa účinne znižuje riziko únikov údajov spôsobených slabými alebo prezradenými heslami.

Riešenie ESET Secure Authentication poskytuje firmám všetkých veľkostí ľahký spôsob implementácie dvojfaktorovej autentifikácie naprieč bežne používanými systémami, ako sú siete VPN, služby Remote Desktop Protokol, Outlook Web Access, prihlasovanie do operačného systému a ďalšie.

Predchádzajte únikom údajov a chráňte svoje firemné aktíva

Dvojfaktorová autentifikácia dokáže zmierniť riziká vyplývajúce z útoku nazývaného „credential stuffing“, pri ktorom útočníci zneužívajú kompromitované informácie o zamestnancoch. Toto riziko je spôsobené používateľmi, ktorí:

- Používajú rovnaké heslo vo viacerých aplikáciách a lokalitách
- Zdieľajú svoje heslá s ostatnými
- Pri aktualizácii hesiel menia len drobnosti

SLABÁ KULTÚRA ZAOBCHÁDZANIA S HESLAMI

Dáta patria medzi najdôležitejšie aktíva vašej spoločnosti. Zamestnanci ich však môžu ohroziť mnohými spôsobmi. Jedným z najväčších rizík je slabá kultúra zaobchádzania s heslami. Nielenže zamestnanci používajú rovnaké heslo na viacerých webových stránkach a vo viacerých aplikáciách, ale niekedy aj voľne zdieľajú svoje heslá s priateľmi, rodinou a kolegami. A akoby už toto nebol dosť veľký problém, zavedenie zásad pre heslá firmami má zvyčajne za následok, že zamestnanci používajú variácie svojho predošlého hesla alebo si zapisujú heslá na lepiace papieriky.

Dvojfaktorová autentifikácia chráni firmu pred slabou kultúrou zaobchádzania s heslami tým, že okrem štandardného hesla implementuje aj ďalší krok overenia, napríklad vygenerovaním údaju v telefóne zamestnanca.

Uplatňovanie tohto riešenia zabraňuje útočníkom získať prístup do vašich systémov jednoducho iba uhádnutím slabého hesla alebo zneužitím kompromitovaných prihlasovacích údajov.

ÚNIKY ÚDAJOV

V súčasnom prostredí kybernetickej bezpečnosti každým dňom narastá počet únikov údajov. Jedným z najbežnejších spôsobov, akými hackeri môžu získať prístup k dátam vašej spoločnosti, sú slabé alebo odcudzené heslá zozbierané prostredníctvom automatických botov, phishingu či cielených útokov. Okrem ochrany normálnych prihlásení používateľov do kritických služieb môžu firmy implementovať dvojfaktorovú autentifikáciu pre všetky elevácie oprávnení, aby sa tak zabránilo neoprávnenému správcovskému prístupu.

Pridaním takéhoto riešenia firmy značne sťažia hackerom možnosť získať prístup k systémom a narušiť ich. Hlavnými odvetviami, ktorých sa týkajú úniky dát, sú tradične sféry s cennými údajmi. Príkladmi sú sektor financií, maloobchodu, zdravotnej starostlivosti či verejný sektor. Neznamená to však, že ostatné odvetvia sú v bezpečí. Ide skôr o to, že hakeri zvyčajne chcú, aby sa im vynaložené úsilie vyplatilo.

SÚLAD S NARIADENIAMI

Pokiaľ ide o súlad s pravidlami, väčšina podnikov musí najskôr zistiť, či ho potrebuje zabezpečiť alebo nie. Potom musia skontrolovať požiadavky, ktorých implementáciu pravidlá odporúčajú a vyžadujú. Pokiaľ ide o dvojfaktorovú autentifikáciu, jej implementáciu už vyžadujú mnohé normy, ako sú PCI-DSS a GLBA, a väčšina noriem vrátane GDPR a HIPAA vo všeobecnosti zdôrazňuje potrebu silnejšieho overovania.

Dvojfaktorová autentifikácia už pre väčšinu firiem, ktoré pracujú s kreditnými kartami alebo v oblasti finančných transakcií, nie je iba dobrovoľným riešením, ale skôr povinným. Všetky spoločnosti by mali preskúmať, ktoré zákony a nariadenia sa na ne vzťahujú, a zabezpečiť, aby dodržiavali stanovené požiadavky.

Nechajte sa overiť jedným ťuknutím bez nutnosti zadávať jednorazové heslo.

V čom je ESET iný

OVEROVANIE CEZ PUSH NOTIFIKÁCIE

Umožňuje overenie jediným ťuknutím bez potreby zadávať jednorazové heslo. Funguje na smartfónoch so systémom iOS aj Android.

ZABEZPEČENIE CLOUDOVÝCH APLIKÁCIÍ

Vďaka dvojfaktorovej autentifikácii posilníte prístup k službám, ako sú Google Apps, Dropbox a mnohé ďalšie. ESET podporuje integráciu prostredníctvom overovacieho protokolu SAML-2, ktorý používajú najväčší poskytovatelia identít.

NASTAVENIE DO 10 MINÚT

Tvrdo sme pracovali, aby ste vy nemuseli. Naším zámerom bolo vytvoriť riešenie, ktoré by si mohla nainštalovať a nastaviť malá firma bez pomoci IT personálu. Nezáleží na tom, či má váš podnik len desiatky alebo tisíce používateľov, nastavenie riešenia ESET Secure Authentication zaberie len minimálny čas, keďže je možné zriadiť viacero používateľských prístupov súčasne.

VIACERO SPÔSOBOV OVERENIA

Zamestnancom nie je potrebné poskytnúť žiadne špeciálne tokeny ani zariadenia. ESET Secure Authentication bez problémov funguje na smartfónoch, zaisťuje vyššiu bezpečnosť vďaka vlastnému PIN kódu a je možné ho integrovať s biometrickými údajmi zariadení (Touch ID, Face ID, Android Fingerprint) pre zvýšenú ochranu a lepší používateľský zážitok. Podporuje aj hardvérové tokeny či bezpečnostné kľúče FIDO.

ŽIADNY ŠPECIALIZOVANÝ HARDVÉR

ESET Secure Authentication má minimálne požiadavky na zdroje – pri používaní cloudovej verzie nebudete potrebovať žiadny vyhradený server. Riešenie zároveň ponúka aj alternatívu v podobe lokálneho nasadenia.

BEZPROBLÉMOVÁ INTEGRÁCIA

Riešenie ponúka dva režimy integrácie – integráciu so službou Active Directory pre organizácie používajúce doménu Windows alebo samostatný režim, ktorý je vhodný pre firmy bez nej. Nastavenie a konfigurácia sú v oboch prípadoch rýchle a jednoduché, pričom je možné celé prostredie bezproblémovo spravovať prostredníctvom cloudovej konzoly.

MULTITENANTNOSŤ

Cloudová verzia ESET Secure Authentication bola navrhnutá s možnosťou multitenantnej správy pre poskytovateľov spravovaných služieb (MSP), ktorí tak môžu riadiť viacero spoločností alebo lokalít. Riešenie ponúka flexibilitu v definovaní špecifických nastavení pre jednotlivé skupiny používateľov.

PODPOROVANÉ PROSTREDIA VDI A SLUŽBY VPN

Podporované sú VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet, FortiGate, Juniper, Palo Alto a SonicWall. Možná je aj podpora vlastnej integrácie s ľubovoľnou službou VPN založenou na protokole RADIUS.

SDK A API AKO SÚČASŤ PRODUKTU

Organizácie, ktoré chcú z produktu vyťažiť ešte viac, môžu využiť SDK a rozhranie API. Aj bez pluginu si tak zákazníci môžu rozšíriť dvojfaktorovú autentifikáciu na aplikácie či platformy, ktoré používajú.

Príklady použitia

Ochrana viacerých lokalít

PROBLÉM

MSP organizácia potrebuje spravovať niekoľko pobočiek alebo spoločností s rôznymi bezpečnostnými politikami a nastaveniami.

RIEŠENIE

- ✓ Vytvorte každú spoločnosť ako lokalitu na portáli ESET PROTECT Hub a priraďte jej určitý podiel licencie ESET Secure Authentication. Po opätovnom prihlásení do konzoly sa zobrazí položka menu Spoločnosti.
- ✓ Multitenantnosť v rámci cloudovej verzie, ktorá nevyžaduje žiadny lokálny hardvér, umožňuje využiť dvojfaktorovú autentifikáciu pre rôzne spoločnosti alebo pobočky z jednej inštancie.

Predchádzanie únikom údajov

PROBLÉM

Firmy každý deň informujú v správach svojich zákazníkov, že došlo k narušeniu ochrany údajov.

RIEŠENIE

- ✓ Chráňte citlivé pripojenia, napríklad k vzdialenej pracovnej ploche, pridaním dvojfaktorovej autentifikácie.
- ✓ Pridajte dvojfaktorovú autentifikáciu pre všetky používané siete VPN.
- ✓ Požadujte dvojfaktorovú autentifikáciu pri prihlásení do zariadení s citlivými údajmi.

Posilnenie ochrany hesiel

PROBLÉM

Používatelia majú tendenciu používať rovnaké heslá vo viacerých aplikáciách a webových službách, čím môžu firmu vystaviť bezpečnostným rizikám.

RIEŠENIE

- ✓ Obmedzte prístup k podnikovým prostriedkom pomocou dvojfaktorovej autentifikácie.
- ✓ Obavy a riziká súvisiace so zdieľanými alebo odcudzenými heslami pomôže zmierniť dvojfaktorová autentifikácia, pri ktorej sa okrem bežného prístupového hesla vyžaduje aj ďalší krok overenia, napríklad schválenie push notifikácie.

Proces overenia prihlásenia používateľa

PROBLÉM

Firmy používajú zdieľané počítače v zdieľaných pracovných priestoroch a vyžadujú overenie všetkých používateľov, ktorí sa prihlasujú počas pracovného dňa.

RIEŠENIE

- ✓ Implementujte dvojfaktorovú autentifikáciu pre desktopové prihlásenia na všetkých zariadeniach v zdieľaných pracovných priestoroch.

Technické informácie a chránené platformy

FUNKCIA	PODROBNOSTI	
MULTITENANTNOSŤ Dostupné iba pre MSP v cloudovej verzii.	Viacero lokalít/spoločností	✓
OCHRANA LOKÁLNEHO PRIHLÁSENIA	Prihlásenie do Windows	✓
OCHRANA VZDIALENÉHO PRIHLÁSENIA	Server RADIUS na ochranu VPN	✓
	Remote Desktop	✓
OCHRANA WEBOVÝCH APLIKÁCIÍ	Microsoft Exchange Server	✓
	Microsoft SharePoint Server	✓
	Remote Desktop Web Access	✓
	Microsoft Dynamics CRM	✓
	Remote Web Access	✓
ACTIVE DIRECTORY FEDERATION SERVICES PROTECTION (AD FS)		✓
KONEKTOR POSKYTOVATEĽA IDENTITY (SAML)		✓
PROXY		✓
API		✓
WHITELISTING IP ADRIES	Globálny whitelisting IP adries	✓
	Whitelisting IP adries podľa služieb	✓
ZRIADENIE	OTP zaslané cez SMS	✓
	OTP vygenerované mobilnou aplikáciou	✓
	Push autentifikácia	✓
	Hardvérový token	✓
	FIDO	✓
UPOZORNENIA	Problém	✓
	Prihlásenie do Web Console	✓
	Používateľ uzamknutý	✓
	Používateľ odomknutý	✓
	Licencie	✓
OBMEDZOVANIE	Časové obmedzovanie	✓
PROTOKOLY A REPORTY O AUDITOCH	Report	✓
	Filter	✓
	Export	✓

Toto je ESET

Proaktívna ochrana. Minimalizujte riziká vďaka prevencii.

Buďte o krok vpred pred známymi aj novými kybernetickými hrozbami vďaka nášmu prístupu, ktorý je založený na umelej inteligencii a zameraný na prevenciu. Kombinovaním sily umelej inteligencie a odborných znalostí našich pracovníkov dokážeme poskytovať jednoduchú a efektívnu ochranu.

Spoznajte najlepšiu ochranu vo svojej triede vďaka našim interným globálnym informáciám o kybernetických hrozbách, ktoré zbierame a skúmame už viac ako 30 rokov a ktoré sú základom našej rozsiahlej siete výskumu a vývoja pod vedením uznávaných odborníkov.

ESET PROTECT, naša cloudová platforma kybernetickej bezpečnosti s podporou XDR, kombinuje schopnosti prevencie, detekcie a proaktívneho vyhľadávania hrozieb novej generácie so širokou škálou bezpečnostných služieb vrátane riadenej detekcie a reakcie (MDR).

Naše vysoko prispôsobiteľné riešenia zahŕňajú podporu v lokálnom jazyku, majú minimálny vplyv na výkon zariadenia, identifikujú a zneškodnia známe aj nové hrozby ešte v zárodku, podporujú plynulý chod prevádzky a znižujú náklady na implementáciu a správu.

ESET chráni vašu firmu, aby ste mohli naplno využívať potenciál technológií.

ESET V ČÍSLACH

1 mld.+
chránených používateľov internetu

400-tis.+
firemných zákazníkov

200
krajín a teritórií

12
globálnych centier výskumu a vývoja

NIEKTORÍ Z NAŠICH ZÁKAZNÍKOV

MITSUBISHI MOTORS
Drive your Ambition

Viac než 9 000 koncových zariadení chránených spoločnosťou ESET od roku 2017

Allianz Suisse

Viac než 4 000 e-mailových schránok chránených spoločnosťou ESET od roku 2016

Canon
Canon Marketing Japan Group

Viac než 32 000 koncových zariadení chránených spoločnosťou ESET od roku 2016

Bezpečnostný partner v oblasti poskytovania internetových služieb 2 miliónom zákazníkov od roku 2008

UZNANIE

AV comparatives APPROVED Business Security DEC 2023

V nezávislých testoch AV-Comparatives dosahuje ESET stabilne **najlepšie výsledky** a najlepšiu mieru detekcie bez falošných poplachov alebo len s minimálnym počtom nesprávne detegovaných položiek.

G2 Leader SPRING 2024

Spoločnosť ESET neustále dosahuje najvyššie hodnotenia od používateľov na globálnej platforme G2 a jej **riešenia oceňujú zákazníci po celom svete**.

kuppingercole ANALYSTS

ESET je podľa spoločnosti KuppingerCole celkovým a **trhovým lídrom** v hodnotení MDR Leadership Compass 2023.