PRODUKTOVÝ LIST

SECURE AUTHENTICATION

Dvoufaktorová autentizace přístupu do sítě a k jejímu obsahu

ENJOY SAFER TECHNOLOGY™

Co je **dvoufaktorová autentizace?**

Jde o autentifikační metodu, která k heslu nebo něčemu, co zná jen uživatel, přidává něco, co uživatel fyzicky vlastní (např. kreditní kartu, USB token nebo klíč), případně něco, čím je charakteristický. Ideální situace nastává v případě, kdy je druhý faktor vyřešený softwarově, takže jako token slouží mobilní zařízení s nainstalovanou aplikací, která generuje jednorázová hesla (OTP).

Jednorázová hesla jsou generována náhodně, takže je nelze předvídat ani znovu použít. Výhody tohoto řešení jsou zřejmé: uživatel se nemusí starat o další zařízení, ale využívá své mobilní zařízení, které má po většinu dne stále v dosahu.

Proč **dvoufaktorová autentizace?**

Zaměstnanci velmi často používají jedno heslo pro přihlášení k různým účtům a službám. V horším případě je sdílejí s kolegy a rodinou.

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 někam 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

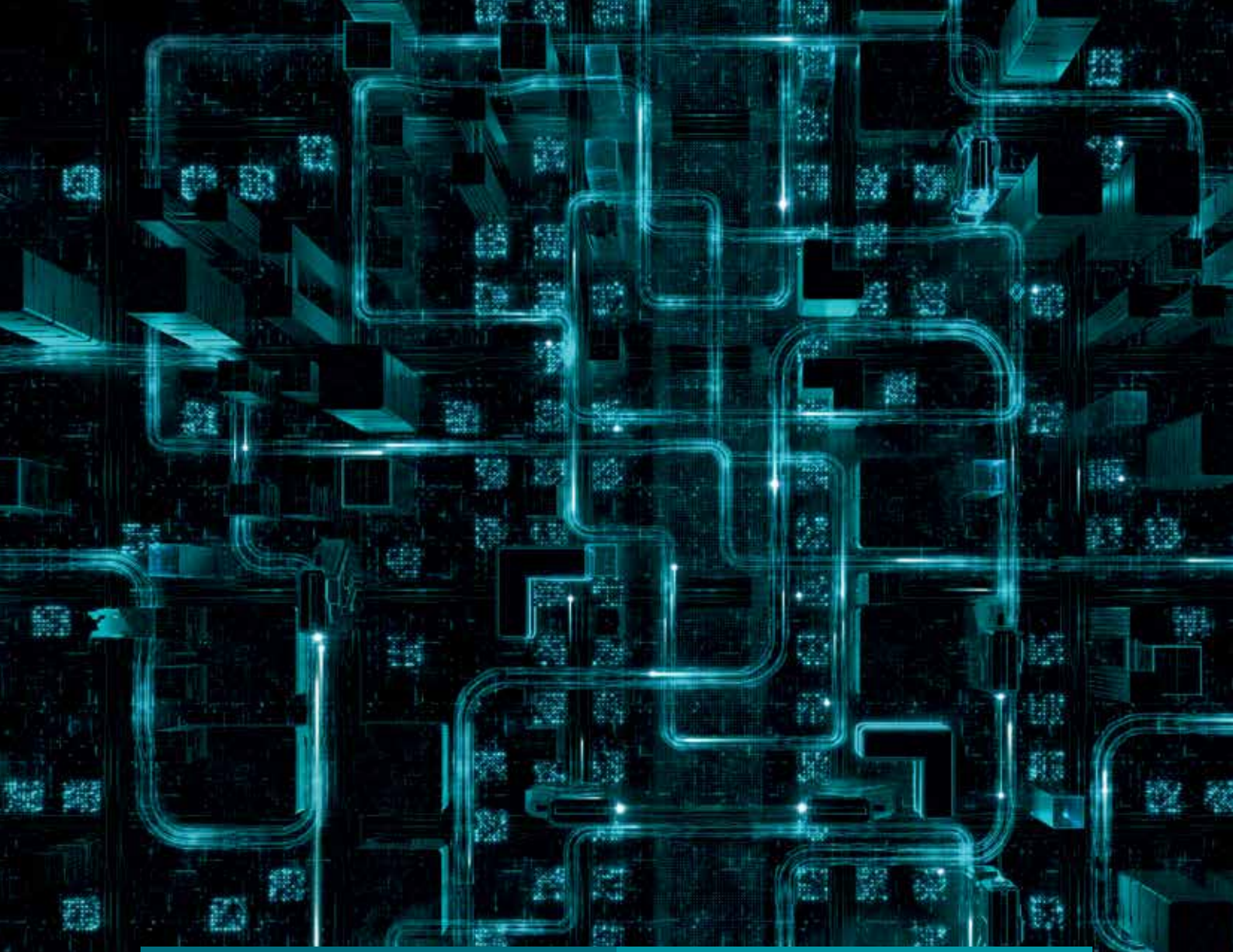
Ztráta a zneužití citlivých dat je v současnosti jednou z nejčastějších forem počítačové kriminality. Cesta k zisku cenných dat vede obvykle přes slabá nebo ukradená hesla. Pokud firma používá při přihlášení dvoufaktorovou autentizaci, například v podobě mobilního telefonu, značně se sníží riziko průniku 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.

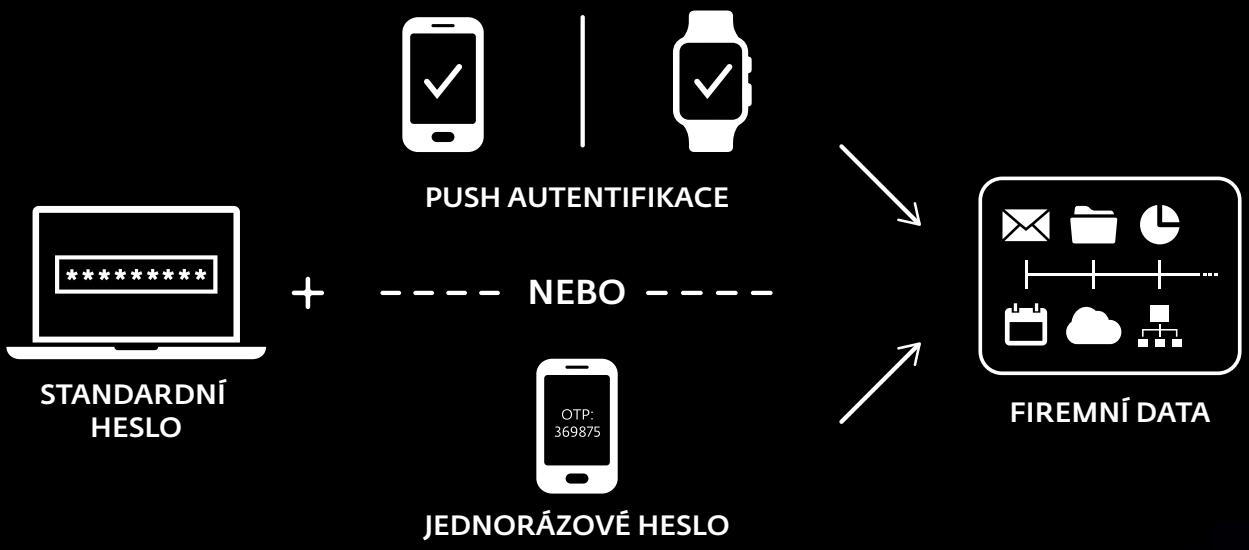
Vícefaktorové ověření proto ve většině případů není jen volitelným způsobem ochrany přístupu, ale vyžadovaným řešením. V dnešním globálním světě se povinnost dodržovat specifické regulační normy, které řídí podnikání, týká stále většího počtu firem a organizací.



Nejčastějším způsobem, jak hackeři pronikají do sítě, je ukradení nebo uhádnutí slabého hesla.

Při implementaci druhého faktoru do procesu přihlášení se riziko neautorizovaného přístupu sníží na minimum.

Autentizace pomocí jediného kliknutí bez nutnosti přepisovat jednorázové heslo.



Výhody ESETu

RŮZNÉ ZPŮSOBY INTEGRACE

Produkt byl navržen, aby fungoval jako samostatné řešení se správou pomocí webové konzole. V prostředí s Active Directory je možné použít ESET Secure Authentication API i User Management API pro jednoduchou integraci do systému.

ŠETŘÍ NÁKLADY

Jde o softwarové řešení, takže není potřeba pořizovat další zařízení nebo token. Jen na jakýkoli server nainstalujete 10MB aplikaci.

PODPORA STÁVAJÍCÍCH TELEFONŮ

Produkt je kompatibilní se všemi telefony, které umožňují přijímat SMS a podporuje široké spektrum mobilních operačních systémů. Přístup do aplikace je chráněn kódem PIN.

RYCHLÉ NASTAVENÍ

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

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.

PUSH AUTENTIFIKACE

Autentifikaci je možné provést s pomocí jednoduchého potvrzení na mobilním telefonu, bez nutnosti přepisovat jednorázové heslo (podporuje iOS, Android i Windows Mobile).

"Jednoduché nastavení, integrace s Active Directory a jedno další hlavní plus – aplikace, kterou jsme mohli uživatelům nainstalovat, takže není nutné neustále používat SMS. Navíc fakt, že ESET Secure Authentication bezproblémově funguje s VPN. Při integraci jsme nastavení VPN vůbec nemuseli měnit."

Tom Wright, IT Service Officer, Gardners Books

Příklady použití

Ověření identity uživatele

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

ŘEŠENÍ

- ✓ Implementace multifaktorového přihlášení 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 sníží 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 zranitelných komunikací, jako je vzdálená plocha, přidáním druhého faktoru do přihlašovacího procesu.
- ✓ Přidání multifaktorové autentizace k 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 specifikace

PUSH AUTENTIZACE

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

DALŠÍ ZPŮSOBY AUTENTIZACE

ESET Secure Authentication podporuje doručení jednorázového hesla nejen přes mobilní aplikaci, push notifikaci, hadrwarové tokeny a SMS, ale i vlastní cestou (např. e-mailem).

VZDÁLENÁ SPRÁVA

Produkt lze spravovat prostřednictvím webové konzole nebo Microsoft Management Console (MMC). Funguje s Active Directory i jako samostatný produkt v prostředí bez domény Windows.

PODPOROVANÉ PLATFORMY

ESET Secure Authentication nativně podporuje služby Virtual Private Networks (VPN), Remote Desktop Protocol (RDP), Outlook Web Access (OWA), VMware Horizon View a RADIUS.

PODPOROVANÉ OPERAČNÍ SYSTÉMY

Windows Server 2003 (32&64bit), 2003 R2 (32&64bit), 2008 (32&64bit), 2008 R2, 2012, 2012 R2, 2016 Windows Small Business Server 2008, 2011 Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials.

PODPORA CLOUDOVÝCH SLUŽEB

ESET Secure Authentication podporuje webové a cloudové služby typu Google Apps a Microsoft ADFS 3.0 (včetně Office 365).

PODPORA HARDWAROVÝCH TOKENŮ

I když hardwarové tokeny nejsou potřeba, produkt podporuje všechny standardní typy (HOTP, OATH).

PODPOROVANÉ VPN

Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.

O ESETu

Společnost ESET byla ve zprávě Magic Quadrant společnosti Gartner* pro rok 2018 jmenována vyzyvatelem v segmentu Endpoint Protection. ESET byl v této zprávě uveden jako jediný vyzyvatel pro danou oblast a oceněn byl zejména za schopnost vytvářet a naplňovat své vize.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. ESET se stal první společností, která díky dlouhodobě vysoké úrovni ochrany získala více než 100 ocenění prestižního magazínu Virus Bulletin VB100. Za těmito úspěchy stojí zejména dlouhodobé investice do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

ESET V ČÍSLECH

110m+
uživatelů po celém světě

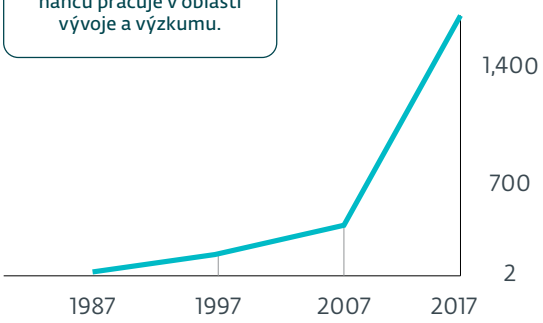
400k+
firemních zákazníků

200+
zemí a teritorií

13
vývojových center

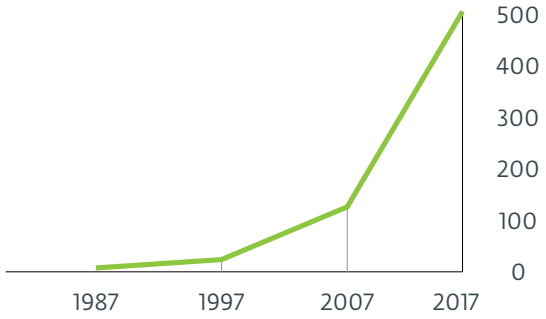
ZAMĚSTNANCI ESETU

Více než třetina zaměstnanců pracuje v oblasti vývoje a výzkumu.



OBRAT ESETU

V milionech eur.



*Společnost Gartner nepodporuje žádného prodejce, produkt ani službu, které uvádí ve svých výzkumných publikacích, a jejím cílem není doporučit uživatelům technologií jen prodejce s nejlepším hodnocením. Výzkumné publikace společnosti Gartner obsahují názory výzkumných organizací Gartner a neměly by vyznít jako tvrzení faktu. Gartner se zříká všech záruk, vyjádřených nebo předpokládaných s ohledem na výzkum, včetně záruky obchodovatelnosti nebo vhodnosti pro konkrétní účel.

NAŠI ZÁKAZNÍCI

HONDA

Zákazníkem od roku 2011

3x prodloužení licence, 2x rozšíření

GREENPEACE

Zákazníkem od roku 2008

10x prodloužení a rozšíření licence

Canon

Zákazníkem od roku 2016

více než 14 000 licencí

T

ISP partnerem od roku 2008

2 miliony zákazníků

NĚKTERÁ OCENĚNÍ

SE Labs AAA ENTERPRISE ENDPOINT OCT-DEC 2016

THE CHANNEL CO. CRN ★★★★★ PARTNER PROGRAM GUIDE WINNER 2017

AV comparatives Approved Business Product 2017

SC MEDIA RECOMMENDED

"Vzhledem ke kvalitě antimalwarové technologie, možnostem správy a globálnímu dosahu by měl být ESET v každém seznamu při výběru nového firemního bezpečnostního řešení."

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018

ENJOY SAFER TECHNOLOGY™