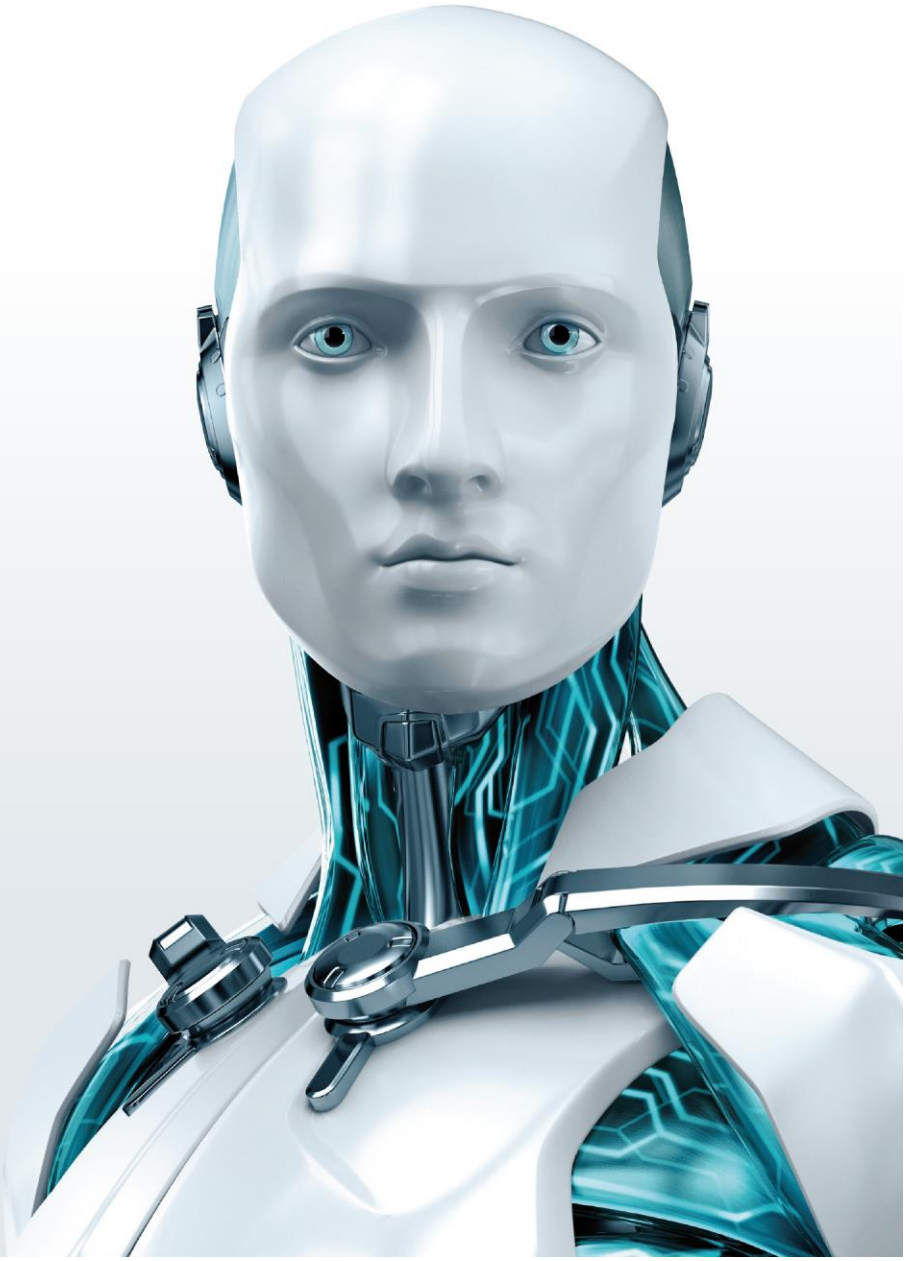
ESET Secure Authentication

Autentifikácia druhým faktorom a súlad s normami



www.eset.sk

UŽÍVAJTE SI
BEZPEČNEJŠIE
TECHNOLÓGIE

Súhrn – autentifikácia druhým faktorom a súlad s normami

Región/krajina	Legislatíva/smernica	ESET Secure Authentication spĺňa explicitnú požiadavku dvojfaktorovej autentifikácie	ESET Secure Authentication vyhovuje požiadavkám na účinnejšiu autentifikáciu
Medzinárodné	Norma ISO27001		✓
Medzinárodné	PCI/DSS – norma odvetvia platobných kariet pre zabezpečenie údajov	✓	
Medzinárodné	ISAE 3402 – International Standards for Assurance Engagements č. 3402		✓
USA	HIPAA – zákon Health Insurance Portability and Accountability Act		✓
USA	FFIEC – smernice Federal Financial Institutions Examination Council	✓	
USA	Federálna vláda USA	✓	
USA	Sarbanes Oxley		✓
Spojené kráľovstvo	„Code of Connection“		✓
Južná Afrika	PPI – Zákon o ochrane osobných údajov		✓

1. Úvod

Pre väčšinu spoločností obchodujúcich v dnešnom dynamickom korporátnom svete sa nutnosť dosiahnutia súladu s rôznymi regulačnými nariadeniami, vládnymi smernicami, normami a audítorskými štandardmi stala prirodzenou súčasťou ich podnikania. Na trhu pôsobí stále viac a viac firiem, ktoré musia povinne zaistiť súlad so špecifickými regulačnými normami vzťahujúcimi sa na ich podnikanie.

Cieľom tohto dokumentu je pomôcť týmto spoločnostiam pri dosahovaní potrebného súladu poskytnutím odpovedí na nasledujúce otázky:

- Aké požiadavky na zaistenie súladu s normami sa vzťahujú na vašu spoločnosť?
- Je v týchto požiadavkách zahrnutá nutnosť používať autentifikáciu druhým faktorom?

Zámerom je zostaviť postup, ktorý vám umožní jednoducho využiť ESET Secure Authentication na dosiahnutie lepšieho celkového súladu s najrôznejšími platnými normami.

2. Požiadavky na zaistenie súladu s platnými normami

Norma ISO27001 (medzinárodná)

Časť o riadení prístupu v kódexe postupov normy ISO 27002 o správe zabezpečenia informácií popisuje požiadavky na riadenie prístupu pre externé sieťové pripojenia. Je evidentné, že sa v tejto norme považujú externé pripojenia za významné riziko, ktoré si vyžaduje nasadenie účinných kontrolných mechanizmov pri ochrane vzdialeného prístupu. S produktom ESET Secure Authentication dosiahnu zákazníci výrazne lepší súlad s touto požiadavkou.

11 Riadenie prístupu
11.4 Riadenie sieťového prístupu
b) pre používateľov aj zariadenia sa používajú príslušné autentifikačné mechanizmy;
11.4.2 Autentifikácia používateľov pri externých pripojeniach
Riadenie: Na riadenie prístupu vzdialených používateľov by sa mali používať príslušné metódy autentifikácie. Pokyny k implementácii: Autentifikáciu vzdialených používateľov je možné vykonávať napríklad použitím šifrovacej techniky, hardvérových tokenov alebo protokolu výzva-odpoveď. Použiteľné implementácie takýchto techník sú súčasťou rôznych riešení virtuálnych privátnych sietí VPN.

Táto časť o riadení prístupu pri povoľovaní fyzického vstupu je explicitnejšia:

11.1.2 Kontrolné mechanizmy na povoľovanie fyzického vstupu
…prístup do priestorov, v ktorých sa spracovávajú alebo ukladajú dôverné informácie, by mal byť obmedzený iba na autorizovaných jednotlivcov implementáciou príslušných nástrojov na riadenie prístupu, napr. implementáciou mechanizmu dvojfaktorovej autentifikácie…

PCI/DSS – norma odvetvia platobných kariet pre zabezpečenie údajov (medzinárodná)

Norma vzťahujúca sa na zabezpečenie údajov platobných kariet je najkonkrétnejšia, pokiaľ ide o dvojfaktorovú autentifikáciu:

Požiadavka 8: Priradenie jedinečného ID každej osobe s počítačovým prístupom

8.3 Začleniť dvojfaktorovú autentifikáciu vzdialeného prístupu (prístup na úrovni siete prichádzajúci z prostredia mimo siete) do siete pre zamestnancov, správcov a tretie strany. (Napríklad vzdialenú autentifikáciu a službu vytáčania RADIUS (Remote Authentication and Dial- In Service) s tokenmi; systém riadenia prístupu k radiču terminálového prístupu TACACS (Terminal Access Controller Access Control System) s tokenmi alebo iné technológie, ktoré využívajú dvojfaktorovú autentifikáciu).

Poznámka: Pri dvojfaktorovej autentifikácii sa vyžaduje použitie dvoch z troch metód autentifikácie. Dve použitia jedného faktora (napríklad použitie dvoch rôznych hesiel) sa nepovažuje za dvojfaktorovú autentifikáciu.

Kedy sa vyžaduje dvojfaktorová autentifikácia?

Dvojfaktorová autentifikácia sa musí používať pri každom vzdialenom prístupe do PCI siete. Inak povedané, vzdialený prístup je možné interpretovať ako ľubovoľné pripojenie alebo ľubovoľný prístup prechádzajúci cez verejné siete. Ak sa ľubovoľná sieť medzi zdrojom prístupu a prostredím Cardholder Data Environment (CDE) považuje za verejnú alebo vlastnenú alebo prevádzkovanú iným subjektom, v takom prípade sa tento prístup považuje za vzdialený. Technológie virtuálnych privátnych sietí (VPN) predstavujú niektoré zaujímavé výnimky, pretože efektívne menia vzdialené siete tak, aby sa správali ako lokálne siete.

V kontexte požiadavky 8.3 je možné koncové technológie VPN považovať za lokálny prístup do siete a technológie Remote Access (RA) alebo klientske technológie VPN by sa mali považovať za vzdialené. V oboch prípadoch môže byť vhodné vykonať ďalšiu revíziu kontrolných mechanizmov, aby sa potvrdilo, že dostatočne spĺňajú požiadavku na používanie dvojfaktorovej autentifikácie pri vzdialenom prístupe do prostredia CDE.

Bežné mylné predstavy

Jeden z nesprávnych výkladov Požiadavky 8.3 sa používa pri interpretácii definície výrazu dvojfaktorová autentifikácia. Niektoré organizácie interpretujú dvojfaktorovú autentifikáciu ako samostatné použitie dvoch autentifikačných identifikátorov pri dvoch rôznych požiadavkách na vykonanie autentifikácie. V týchto prípadoch sa pri každej požiadavke na vykonanie autentifikácie používa jeden autentifikačný identifikátor. Dva kroky pri autentifikácii s použitím jedného faktora nie sú to isté ako dvojfaktorová autentifikácia.

Ďalším nedorozumením býva, že Požiadavka 8.3 sa vzťahuje na všetok prístup do prostredia CDE, nie iba na vzdialený prístup. V týchto prípadoch môžu organizácie nasadiť mechanizmy dvojfaktorovej autentifikácie za účelom autentifikácie prístupov zo všetkých pripojených sietí vrátane tých, ktoré sú pripojené lokálne. Takéto riešenie síce z Požiadavky 8.3 nevyplýva, pomáha ale ešte viac zvyšovať úroveň zabezpečenia a ochrany prístupu do prostredia CDE.

Pridaním ďalších autentifikačných krokov sa môže zvýšiť úroveň celkového zabezpečenia mechanizmu vzdialeného prístupu, toto vylepšenie ale neprináša takú vysokú úroveň zabezpečenia ako mechanizmus skutočnej dvojfaktorovej autentifikácie. Cieľom Požiadavky 8.3 je zaistiť, aby sa v rámci jednej požiadavky na vykonanie autentifikácie používali dva autentifikačné identifikátory.

ISAE 3402 – International Standards for Assurance Engagements č. 3402 (medzinárodné)

Norma ISAE (medzinárodné normy pre poistné zmluvy) č. 3402, Assurance Reports on Controls at a Service Organisation, bola vyvinutá ako medzinárodná bezpečnostné norma, ktorá má umožňovať audítorom vytvárať správy určené pre organizácie používateľov a príslušných audítorov na strane organizácií. Tieto správy sa zaoberajú kontrolnými mechanizmami používanými v servisnej organizácii, ktoré môžu mať vplyv alebo ktoré môžu byť súčasťou systému interného riadenia finančného výkazníctva v organizáciách používateľov.

Od servisných organizácií, v ktorých sa používa ESET Secure Authentication a ktoré svojim zákazníkom poskytujú služby súvisiace s IT, sa môže vyžadovať implementácia kontrolných mechanizmov za účelom splnenia požiadaviek auditu normy ISAE 3402. Riadenie prístupu je pri takomto audite zvyčajne kľúčovým faktorom. Dvojfaktorová autentifikácia externého prístupu umožní servisným organizáciám takýmto auditom bezpečne prejsť.

HIPAA – zákon Health Insurance Portability and Accountability Act (USA)

Americká federálna poradná skupina odporučila v niektorých prípadoch vyžadovanie viacfaktorovej autentifikácie pre Etapu 3 motivačného programu elektronických zdravotných záznamov podľa zákona HITECH Act. Týmto programom sa riadi aj poskytovanie IT služieb podľa zákona HIPAA.

Etapa 3 má byť spustená v roku 2015 a na americkom ministerstve zdravotníctva sa začína diskutovať o príslušných pravidlách.

FFIEC – smernice Federal Financial Institutions Examination Council (USA)

Rada U.S. Federal Financial Institutions Examination Council je oficiálna inštitúcia s dosahom na viaceré agentúry, ktorá môže určovať jednotné zásady, normy a formuláre výkazov na účely skúmania finančných inštitúcií na federálnej úrovni Radou guvernérov federálneho rezervného systému a agentúrami a inštitúciami, ako sú Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency a Consumer Financial Protection Bureau, a ktorá môže presadzovať svoje odporúčania v oblasti jednotného dozoru nad finančnými inštitúciami.

Po publikovaní smerníc FFIEC, ktoré odporúčajú používanie viacfaktorovej autentifikácie, začali viacerí dodávatelia ponúkať riešenia autentifikácie, ktoré nie sú v súlade s definíciou skutočnej viacfaktorovej autentifikácie uvedenou v smerniciach FFIEC. Najviac z rôznych praktických prístupov prevláda používanie výzvy

a odpovede, ku ktorým sa často pridáva zdieľaný tajný obrázok. Pri využívaní osobných informácií v odpovedi na otázku vo výzve sa pracuje s niečím, čo používateľ pozná, čo je podobné ako používanie prihlasovacieho mena, hesla alebo PIN kódu. Toto všetko sú riešenia autentifikácie z rovnakej kategórie. Pokiaľ sa nepoužívajú v kombinácii s niektorým z ďalších dvoch faktorov, napr. s niečím, čo používateľ má, tak ich nie je možné považovať za riešenie viacfaktorovej autentifikácie.

Regulačné úrady opakovane varovali pred uplatňovaním takých metód, pri ktorých sa pracuje s osobnými údajmi. 17. júna 2005 vydal americký úrad FDIC (Federal Deposit Insurance Corporation) dodatočnú smernicu, v ktorej sa finančným inštitúciám dôrazne neodporúča nasadzovať také metódy autentifikácie, pri ktorých sa na účely autentifikácie používajú osobné informácie:

„Zákazníci sa prirodzene obávajú phishingu a zaujíma ich dôveryhodnosť e-mailov, ktoré im posielajú banky, všeobecnejšie je ale rozšírená obava o bezpečnosť ich osobných údajov... Keď sa banky rozhodujú pre niektoré metódy autentifikácie pre svojich retailových zákazníkov, mali by zohľadniť skutočnosť, že títo zákazníci si cenia svoje dôverné informácie a dokážu ich dostatočné zabezpečenie a ochranu oceniť... Zákazníci budú požadovať jasné vysvetlenie akéhokoľvek bezpečnostného mechanizmu a spôsob používania osobných údajov, ktorý sa pri implementácii daného bezpečnostného mechanizmu požaduje... striktné obmedzenia vzťahujúce sa na používanie osobných údajov a existencia ochranných prvkov, ktoré chránia bezpečnosť dôverných údajov, to všetko sú dôležité aspekty, ktoré určujú mieru akceptácie riešenia zákazníkmi... Zákazníkov tiež zaujímajú riziká súvisiace s veľkými databázami s množstvom osobných údajov a zaujímajú sa o to, do akej miery môže byť bezpečnosť týchto údajov používaných pri autentifikácii ohrozená, resp. či ich je možné skopírovať alebo napodobniť. – FDIC“

Rada FFIEC ozrejmila svoje stanovisko 15. augusta 2006 v dodatku s najčastejšími otázkami, v ktorom takéto prístupy vyložene zamietla:

„Skutočná viacfaktorová autentifikácia podľa definície vyžaduje použitie riešení z dvoch alebo troch kategórií faktorov. Použitie viacerých riešení z rovnakej kategórie nepredstavuje viacfaktorovú autentifikáciu. – FFIEC“

Federálna vláda USA (USA)

Regulačné normy vzťahujúce sa na IT, ktoré riadia prístup do systémov federálnej vlády, vyžadujú používanie dvojfaktorovej autentifikácie pri prístupe k citlivým IT prostriedkom (napríklad pri prihlasovaní na sieťovom zariadení za účelom vykonania administratívnych úkonov) a pri získavaní prístupu do ľubovoľného počítača pomocou privilegovaného prihlásenia.

Sarbanes Oxley (USA)

Zákon Sarbanes-Oxley Act (SOX) prikazuje organizáciám používať účinnejšie formy autentifikácie, aby sa úspešnejšie predchádzalo krádežiam údajov, podvodom a aby sa zaistila čo najlepšia ochrana údajov zákazníkov a pacientov.

Code of Connection (Spojené kráľovstvo)

Autentifikácia s využitím druhého faktora pomáha organizáciám pôsobiacim v Spojenom kráľovstve dosiahnuť súlad s požiadavkami, ktoré vyplývajú zo zákona „Code of Connection“ uvedeného do praxe vládnymi online službami, akou je napríklad UK Government Secure Extranet.

PPI – Zákon o ochrane osobných údajov (Juhoafrická republika)

V juhoafrickom zákone o ochrane osobných údajov sa uvádza, že:

Pravidlo 7 Bezpečnostné mechanizmy na ochranu údajov
Bezpečnostné opatrenia vzťahujúce sa na integritu osobných údajov
18. (1) Zodpovedná strana musí chrániť integritu osobných údajov, ktorými disponuje a s ktorými pracuje, vykonaním príslušných primeraných technických a organizačných opatrení, ktoré budú znemožňovať
(b) nezákonný prístup k osobným údajom a ich nezákonné spracovanie.

(2) S dôrazom na pododsek (1) je zodpovedná strana ďalej povinná vykonať primerané opatrenia na
(b) zavedenie a udržiavanie vhodných kontrolných mechanizmov, ktoré zaistia dostatočnú ochranu pred uvedenými rizikami;

Niet pochýb, že pri nedostatočnej ochrane systémami, ktoré v súčasnom IT svete využívajú iba heslo (a umožňujú ho opakovane používať), by každá zodpovedná organizácia mala implementovať dvojfaktorovú autentifikáciu (a ďalšie mechanizmy), ak nechce vystavovať zverené osobné údaje zbytočným rizikám.