Materiál Ministerstva vnitra

Export z Národní architektury eGovernmentu ČR

Obsah

Bezpečnost elektronické identity

Jak zabezpečit svou e-identitu

e-identita je druh uživatelského účtu, který je svázaný s jednoznačně identifikovanou osobou, která prostřednictvím tohoto účtu – e-identity může dále komunikovat zejména se státní správou.

Prostřednictvím e-identity je možné mít dálkový přístup k údajům konkrétního uživatele/občana, takže pokud útočník získá přístup k Vaší e-identitě, může získat informace o Vás (výpis z rejstříku trestů, z katastru nemovitostí, ze zdravotní dokumentace a dalších připojených služeb). Tedy co můžete získat za informace od státní správy Vy, bude moci i úspěšný útočník.

Útočník bude moci mít přístup do Vaší datové schránky a jejím prostřednictvím podávat žádosti na úřady, komunikovat Vaším jménem, číst doručené datové zprávy.

S ukradenou e-identitou může útočník přenastavit různá upozornění, která můžete mít nastavena (vypršení platnosti občanského průkazu, ohlášení změn v katastru nemovitostí apod.).

Pro ověření identity je využíváno celé řady prostředků, je tedy třeba zajišťovat bezpečnost všech prostředků, které s e-identitou souvisí. Běžně používanými prostředky jsou např. chytrý mobilní telefon, počítač, notebook, mobilní klíč (aplikace), USB klíč (token) nebo čipová karta. Zabezpečení e-identity je tedy přímo úměrné bezpečnosti používaných prostředků.

Zneužití e-identity je však mnohem složitější a vyžaduje značnou míru znalostí a technických prostředků, lze tedy obecně konstatovat, že je mnohem bezpečnější používat e-identitu než běžné užívání fyzických dokladů jako občanský průkaz nebo přihlašovací údaje k běžnému uživatelskému účtu.

Rizika z pohledu bezpečnosti prostředků

Různé prostředky elektronické identifikace jsou spojeny s různou úrovní zabezpečení proti potenciálnímu útočníkovi. Jisté vodítko dává samotná úroveň záruky daného prostředku, která v hrubém měřítku popisuje, co může uživatel od úrovně zabezpečení prostředku očekávat. Požadavky na bezpečnost jsou v tomto případě ukotveny v prováděcím nařízení Komise (EU) 2015/1502, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci.

Ministerstvo vnitra tyto požadavky ještě více rozpracovalo do dokumentu konkretizujícího požadavky na poskytovatele identitních služeb (DKP-IDP) - s dokumentem je možné se seznámit zde:

https:%%//%%www.mvcr.cz/clanek/ministerstvo-vnitra-zverejnuje-dokument-konkretizujici-minimalnipozadavky-na-kvalifikovane-eid-systemy-a-eid-prostredky.aspx).

Pro posouzení bezpečnosti prostředků se primárně pracuje s termínem faktor autentizace, což je termín odkazující na to, jakým způsobem uživatel prokazuje, že je oprávněným vlastníkem prostředku. Obvykle se používají tři kategorie těchto faktorů, je to faktor na základě vlastnictví, faktor na základě znalosti a inherentní faktor. Faktor na základě vlastnictví spočívá v ověření faktu, že něco uživatel vlastní (čipová karta, telefon, bezpečnostní klíč). Faktor na základě znalostí ověřuje, že

uživatel něco ví (Heslo, PIN). Inherentní faktor ověřuje nějakou fyzickou vlastnost osoby (typicky jde o biometrické údaje – nejčastěji otisk prstu, obraz obličeje, méně často pak oční duhovka nebo sítnice či infračervený obraz krevního řečiště lidské dlaně).

Pro nízkou úroveň záruky platí, že autentizační prostředek používá jen jeden faktor autentizace. Typicky se bude jednat o heslo. Pro značnou úroveň záruky je nutné, aby prostředek kombinoval minimálně dva faktory ze dvou různých kategorií. Zde můžeme mezi prostředky najít celou řadu variant využívajících všechny kategorie. Pro nejvyšší úroveň záruky je nutné, aby prostředek efektivně zabraňoval možnosti vytvořit duplikát, a zde se již objevují pouze HW prostředky se silnou ochranou uloženého kryptografického materiálu.

Bezpečnost hesel

Heslo je nejběžnějším znalostním faktorem autentizace. Používá se buď samostatně anebo se kombinuje s jinými faktory. Nejběžnějšími způsoby útoku na hesla jsou buď hádání, snaha o jejich odchycení za pomocí útoku typu „*MITM*“ (Man-In-The-Middle), případně off-line útoky.

Útočník využívající hádání předpokládá, že uživatel používá slabé heslo. Jako ochrana se doporučuje použít silné dlouhé heslo v kombinaci s tím, že služba by měla být schopná detekovat opakované pokusy o zadání hesla a nějakým způsobem útočníkovi takové hádání zamezit (lze rozpoznat například tak: pokud služba umožnuje více jak 3x zadat heslo, aniž by třeba dočasně znemožnila přístup nebo nevyžadovala další reakci uživatele). Existují také různé metody uchovávání hesel na straně služeb, přičemž bohužel některé nejsou dostatečně bezpečné. Existuje služba, která se snaží tyto přístupy kategorizovat a uživatele o nebezpečných metodách informovat. Příkladem může být služba na této adrese: https:%%//%%pulse.michalspacek.cz/passwords/storages. V případě útoku typu MITM může sofistikovaný útočník uživatele přesvědčit, že se přihlašuje ke správné službě, přestože komunikuje s falešnou stránkou. K tomu se používají různě techniky sociálního inženýrství například známý phishing. Uživatel v takovém případě heslo předá útočníkovi nevědomky. Je třeba být maximálně obezřetný, kam se uživatel přihlašuje a pečlivě kontrolovat URL adresu v záhlaví internetového prohlížeče, zejména doménovou část (např. „*mojebezpecnasluzba.cz*“). Off-line útok bývá často prováděn v případě, kdy unikne databáze uživatelských jmen (emailových adres) a hesel (obvykle jejich hashů nebo jiného typu zašifrování) a útočník tak má možnost pokoušet se uhádnout heslo masivní výpočetní silou (brute force). Určitou ochranou je nezadávat stejná hesla u více služeb, čímž se zamezí útočníkovi, který např. tímto způsobem získal heslo od nějaké konkrétní služby, aby toto heslo úspěšně použil jinde.

Bezpečnost SMS autentizace

Pro dosažení vícefaktorové autentizace se často používá ověření faktoru vlastnictví telefonního čísla na základě SMS zaslané na toto číslo. I pro takto koncipovanou autentizaci platí, že v případě MITM útoku má útočník možnost kromě hesla odchytit i kód zaslaný SMS a platí stejná opatření zmiňovaná výše. V případě SMS autentizace hraje velkou roli také zabezpečení telefonu, na který SMS přichází. Bohužel oprávnění přístupu ke čtení SMS zpráv je často uděleváno velkému množství aplikací na chytrých telefonech. Je nutné, aby tyto aplikace byly důvěryhodné. V poslední době se objevují útoky typu SIM swap, který obchází zabezpečení telefonního operátora, určené pro případ, kdy zákazník SIM kartu ztratí. Útočník, který přesvědčí operátora, že SIM kartu ztratil a získá novou s číslem oběti, tak může bez problémů odchytit autentizační SMS. Útočníci mohou také využít k přímému odposlechnutí komunikace zranitelnosti signalizačního protokolu SS7, používaném telefonními operátory.

Bezpečnost mobilních potvrzovacích aplikací

Mobilní aplikace pro potvrzení autentizací vynechávají z komunikace telefonního operátora a tím eliminují některá rizika popsaná výše. Navíc typicky umožňují zapouzdření dvou různých faktorů autentizace. Faktor vlastnictví je zde řešen tak, že v mobilním zařízení je uložen kryptografický klíč, použitý pro podepisování zpráv. Druhý faktor je buď znalostní (typicky PIN) nebo inherentní (otisk prstu nebo obraz obličeje). Aplikace tak nevyžadují zadávání hesla. Ani v tomto případě nicméně není uživatel plně chráněn proti MITM útoku a musí být opatrný při hlídání, kam se přihlašuje. Pro vybuzení autentizace stačí často zadat informaci, která z principu není tajná (číslo smlouvy, email, datum narození atd.). To dává útočníkovi prostor pokusit se v době, kdy se uživatel přihlašuje, zaslat paralelně jiný autentizační požadavek a zmást uživatele tak, aby autorizoval takovýto požadavek místo oprávněného. Toto je možné eliminovat kontrolou ověřovacího kódu, který by měl být pro uživatele stejný jak na webu, tak v mobilní aplikaci. Klíčovou vlastností bezpečnosti je také uložení kryptografického klíče. Moderní verze chytrých telefonů již obsahují tzv. Secure Element, který znesnadňuje zneužití uloženého klíče. Některé starší verze Android telefonů nicméně tento systém nepodporují a bezpečnost je zde tak snížena.

Bezpečnost FIDO tokenu

Technologie FIDO je, podobně jako u mobilních potvrzovacích aplikací, postavena na kryptografii. Navíc v sobě ale nese prvek, který tuto technologii dělá odolnou vůči phishingu. FIDO bezpečnostní klíče jsou k dispozici v mnoha variantách od softwarového řešení po vysoce zabezpečená hardwarová úložiště. Uživatelům k rozlišení slouží FIDO certifikace, která ukazuje, jak důsledně je chráněn kryptografický klíč zabezpečující vlastní přihlášení. V každém případě je rizikem používat necertifikované klíče. Na trhu jsou naopak k dispozici i FIDO bezpečnostní klíče integrující čtečku otisku prstů, jejímž použitím dojde ještě ke zvýšení bezpečnosti.

Bezpečnost čipových karet

Čipové karty umožňují nejvyšší míru zabezpečení. Kryptografické klíče zabezpečující komunikaci jsou i zde uloženy v certifikovaném hardwarovém úložišti bez možnosti jednoduše vytvořit kopii takového klíče. Ve většině případů vyžaduje čipová karta navíc doprovodný software, který je nutné nainstalovat na klientské zařízení a který zajišťuje bezpečnou komunikaci mezi klientem a ověřovacím serverem. Obvykle se nicméně nejedná o otevřené technologie, takže míra důvěry je závislá na důvěře v technologického dodavatele. I zde jsou známé případy selhání, jako např. chyba v systému firmy Infineon, dodavatele pro technologie čipových karet Estonských a Slovenských občanek, která způsobila vysoké riziko zneužití těchto dokladů a vedla k hromadné výměně kryptografických klíčů uložených na těchto kartách.

Jednotlivé faktory autentizace mohou být implementovány různými technologiemi. V následující tabulce je vyznačeno, jaké technologie jsou použité v existujících bezpečnostních prostředcích.

	Heslo	SMS	Mobilní aplikace	FIDO klíč	Čipová karta
eOP					**X**
NIA-ID	**X**	**X**			
MEG			**X**		
I.CA					**X**

	Heslo	SMS	Mobilní aplikace	FIDO klíč	Čipová karta
mojeID	X		X	X	
Bankovní identita	X	X	X		

Obecná doporučení (pro širokou veřejnost)

V oblasti on-line transakcí s využitím elektronické identifikace a autentizace mějte na paměti, že výběr způsobu a prostředku elektronické identifikace by měl odpovídat hodnotě transakce, kterou hodláte provést přes Internet. V reálném „digitálním světě“ využíváme pro různé typy online transakcí mnoho virtuálních identit a zdaleka ne všechny nám technicky umožňují využít státem garantovanou e-identitu. Kromě toho zdaleka ne všechny transakce si zasluhují (z hlediska možných rizik), abychom tu nejvíce zabezpečenou e-identitu využívali všude ve spotřebitelských službách – i proto, že využití více faktorové nebo vícestupňové autentizace bývá o něco pracnější, a přece jen trochu „zdržuje“.

Vaše elektronická identita bude v bezpečí v případě, že budete mít dostatečně zabezpečená zařízení, která budete pro používání elektronické identity používat stejně tak, jako tato zařízení chráníte při přístupu např. do Vašeho internetového bankovnictví.

- Používejte zdravý selský rozum a pečlivě rozmýšlejte, kam zadáváte své údaje (nejen přihlašovací)
- Nikdy nesdělujte přihlašovací údaje a nepůjčujte autentizační prostředky (eOP, tokeny) jiným osobám.
- Nenechávejte druhý autentizační nástroj bez dozoru (USB token, eOP, mobil). Pokud používáte mobil jako autentizační prostředek, mějte vždy nastaveno zamykání obrazovky. Mějte na paměti, že používání speciálních aplikací pro generování a případně i předávání jedinečných přihlašovacích kódů je bezpečnější než zasílání přihlašovacích kódů prostřednictvím SMS. Příjem SMS není chráněn dalších heslem (PINem), a navíc je možné jej u pokročilých útoků „odposlechnout“. Pokud můžete, převeďte dodatečnou autentizaci s využitím mobilu na mobilní aplikaci a zabezpečte její spuštění biometrickým faktorem nebo dodatečným heslem.
- Nainstalujte si antivirový program a pravidelně jej aktualizujte. I ty, které jsou zdarma, nabízí kvalitní ochranu počítače. V poslední době se objevují již i antivirové programy pro ochranu chytrých telefonů – některé z nich jsou i ve „free“ verzi. Používejte ale jen takové, které byly schváleny výrobcem Vašeho mobilního telefonu, resp. jeho operačního systému.
- Zabezpečte přístup na domácí síť Wi-Fi silným heslem (použijte kombinaci velkých a malých písmen, číslic a dalších zvláštních znaků, a celkem doporučujeme délku alespoň 12 znaků) a přesvědčte se, že používáte nyní nejsilnější běžně používanou metodu šifrování přenosu WPA3 (pokud není podporován, tak WPA2; nepoužívat WEP a WPA).
- Nepoužívejte veřejné sítě Wi-Fi, pokud hodláte provést jakoukoli transakci se svojí elektronickou identitou; pokud můžete, použijte připojení přes mobilní data.
- Přesvědčte se, že webová stránka poskytovatele zobrazuje obvyklou URL adresu (že se nejedná o napodobeninu Vaší známé stránky, kterou ale vlastní někdo jiný). Pokud se URL neshoduje s oficiální internetovou adresou služby, kterou hodláte využít, okamžitě stránky opusťte.
- Zkontrolujte, že jste připojeni přes zabezpečené připojení TLS/SSL. Váš prohlížeč to obvykle potvrzuje symbolem visacího zámku vlevo od URL adresy, která musí začínat „https://….“ a nikoli jen „http://….“. Moderní prohlížeče již kliknutím na zámek zobrazí výsledek sady kontrol spojení a dají vodítko typu “spojení je zabezpečené”, nebo Vás naopak varují o opaku.
- Ověřte, že certifikát šifrovaného spojení TLS/SSL byl vydán pro subjekt (organizaci), který má poskytnout zamýšlenou službu. To ověříte (podle typu prohlížeče) rozkliknutím symbolu zámečku, následně “více informací” (nebo podobné) - prohlédnout certifikát. V informačních

polích certifikátu pak uvidíte v poli “Subject name” nebo “Common name” jméno subjektu, komu byl certifikát vydán. Toto jméno se musí shodovat s poskytovatelem služby (nebo jeho mateřskou firmou).

- Pokud můžete, aktivujte přes veřejné sítě zabezpečené tunelování VPN (Virtual Private Network). VPN dávají obvykle k dispozici firmy svým zaměstnancům pro jejich práci odkudkoli a pro běžné spotřebitele to může být obtížně splnitelné doporučení.
- Na stránkách s problematickým obsahem vždy pečlivě zvažte, na jaký odkaz kliknete. Obecně platí, že čím „zajímavější“ je obsah poskytnutý zdarma na dané webové stránce (a není to renomovaný poskytovatel), tím vyšší pravděpodobnost je, že na takové stránce je skrytý škodlivý kód nebo Vám nabízí stažení softwaru, který je pozměněn a obsahuje škodlivý kód.
- Jestliže využíváte svůj emailový účet pro příjem výzvy k resetování hesla, aktivujte si vícefaktorovou nebo alespoň vícestupňovou autentizaci pro přístup do Vašeho emailu, čímž výrazně znesnadníte zneužití Vašeho emailu útočníkům. Kvalitní poskytovatelé elektronické pošty využívají inteligentní „podmíněný přístup“ s průběžným vyhodnocováním rizika každého přihlášení, který si vyžádá druhý faktor např. jen v případě, kdy se jedná o pokus o přístup z neznámého zařízení, prvně použitého prohlížeče nebo z neznámé lokality (IP adresy). Používejte u svého poštovního klienta spamový filtr a antivirovou ochranu. U zavedených poskytovatelů emailu jsou tyto filtry již součástí standardních nabídek.
- Chraňte mobilní telefon či tablet heslem, PINem a lépe otiskem prstu před "volným přístupem".
- Pro přístup na internetové bankovnictví nebo přihlašování k elektronické identitě zadávejte internetovou adresu dané instituce ručně, neklikejte na zaslané nebo zobrazené odkazy.
- V podezřelých e-mailech neklikejte na žádné odkazy. Pamatujte, že banky a platební systémy **NIKDY** nevyžadují osobní údaje ani důvěrná uživatelská data e-mailem.
- Nevyužívejte sdílené počítače/případně využívejte alespoň anonymní režim.
- Využívejte silná a neopakující se hesla.
- Instalujte aplikace pouze z ověřených zdrojů (aplikace odjinud mohou být závadné).
- Pokud si nejste schopni zapamatovat hesla, využívejte správce hesel.
- Nezadávejte hesla na cizích zařízeních.
- Při ztrátě jakéhokoliv prostředku si okamžitě změňte heslo, případně aktualizujte své telefonní číslo. Je tedy nutné vždy zabezpečit všechny prostředky, které se podílí na autentizaci.
- Šifrujte obsah vašich zařízení (full disk encryption jak u mobilního zařízení, tak počítače) za využití silného hesla. Šifrováním prostoru/harddisku/úložného prostoru zařízení zajišťujeme ochranu dat (hesel, klíčů, veškerých dat/informací) proto, aby je případný útočník nebo osoba, která dané zařízení (NB, PC, telefon) získá, nemohla jednoduše přečíst/získat data na něm uložená. Data jsou šifrována obvykle pouze při vypnutém zařízení. Šifrováním zajišťujeme, že informace nebudou jednoduše a ihned dostupné případnému útočníkovi a bude muset použít nějakou technicky nebo časově náročnou metodu k prolomení zvoleného šifrování. Tuto dobu je pak nezbytné využít ke změně hesel, zablokování přístupů.
- Aktualizujte nejen operační systém (mobilu, počítače), ale i všechny aplikace na těchto zařízeních instalované.
- U souborů, které to umožňují, nepovolujte makra, pokud si nejste jisti, že jsou od důvěryhodného odesílatele a neobsahují škodlivý kód.
- Heslo použité pro e-identitu nepoužívejte u jiné služby. Jedním z nejjednodušších způsobu útoků je „hádání hesel“, zejména s dnešním světem digitálních technologii není složité zjistit Vaše zájmy, jména rodinných příslušníků, data narození, domácí mazlíčky a podobně. Zejména pokud se podíváte na zprávy, velmi často se objevují informace o zcizených databázích od různých poskytovatelů služeb. Pokud tedy budete mít stejné heslo na více účtech, útočník, má pak jednoduchou cestu k vašemu účtu, neboť první, co vyzkouší, je již jemu známé heslo.
- Vždy požívejte bezpečná dlouhá hesla. Dlouhá hesla se sice špatně pamatují, ale ztěžují případný útok typu brute force (útok hrubou silou). Jde většinou o automatizovaný typ útoku, kde útočník zkouší veškeré kombinace písmen, číslic a znaků, nebo se používají takzvané

slovníkové útoky, kdy jsou používány slova nebo jejich kombinace. Běžný počítač je teoreticky schopen otestovat 3.000.000.000 kombinací za sekundu. Pokud vezmeme heslo tvořené 6 znaky (abeceda s možností velkých a malých písmen, jde tedy o 52 znaků). Jde tedy o 19.770.609.664 možných kombinací. Takové heslo jde zjistit za 7sekund. U 8 znakového hesla s možností použití číslic a speciálních znaků (98 znaků), pak bude teoretický čas 32 dnů 19 hodin 44 minut 37 sekund (jde samozřejmě o modelový příklad). Proto je třeba používat na hesla velká a malá písmena, číslice, speciální znaky (*-?@÷, atd…)

- Silné přihlašovací heslo do zařízení. Zde jde o stejnou analogii jako u obecného konstatování dlouhých a bezpečných hesel, kterou je třeba doplnit o vazbu na počítač/ zařízení. Ten, pokud by Vám byl odcizen, nebo jste náhodou nechali někde bez dozoru nějaký prostředek (počítač, telefon, tablet), ztížíte případnému útočníkovi možnost buď získat vaše data, nebo jej minimálně zpomalíte.
- Oddělené účty od účtů dětí. Významným rizikem jsou děti a další členové domácnosti. Ne každý musí být vždy obeznámen s bezpečným nakládáním a chováním v elektronickém světě anebo nemusí dodržovat všechna pravidla. Koneckonců i únava a stres mohou vést k nedostatečné pozornosti. A právě proto, aby se snížila pravděpodobnost chyby způsobené jinou osobou, která má přístup na váš počítač, je vhodné alespoň používat oddělené účty, čímž se sníží pravděpodobnost ztráty nebo poškození dat na vašem účtu na počítači.
- Nepoužívejte administrátorská oprávnění (privilegované účty) na svém běžném účtu do počítače. Oprávnění správce/administrátora vám umožňují, v případě potřeby, provádět změny důležitých částí vašeho systému, instalovat programy a nastavovat zařízení. Pokud tedy nebudete používat účet s administrátorským oprávněním, zásadním způsobem tím snížíte možnosti případného útočníka provést nežádoucí aktivitu na vašem zařízení.
- Pro zabezpečení nepoužívejte gesta, ale buď PIN s minimální délkou 6 číslic nebo biometriku. U této problematiky jde zejména o jednoduchost získání přístupu. Nejjednodušeji lze odpozorovat gesto, následuje PIN, přičemž jeho délkou se bráníte zejména proti útokům hrubou silou. Biometrické údaje se však velmi složitě získávají nebo obchází.
- Vypněte automatické přihlašování k uloženým Wi-Fi sítím

Doporučení podle úrovně dopadu zneužití eID

Obecně lze z hlediska rizik a možných dopadů naše identity fyzické osoby rozdělit asi do 3 úrovní:

Nejnižší dopady

Identity ve formě uživatelských účtů ve spotřebitelských službách, při kterých nedochází k platbám přes internet, ve kterých nejsou uloženy údaje o kreditních kartách a se kterými nejsou spojeny žádné citlivé osobní údaje. Toto jsou např. přihlašovací účty do cenových srovnávačů, nákupních portálů, které nás svým obsahem nijak nekompromitují a kde případná platba probíhá přes platební bránu třetí strany. Ve všech těchto případech bývají osobní údaje pouze základní identifikační údaje fyzické osoby – typicky jméno, příjmení, adresa bydliště, emailová adresa a telefon. Zneužitím těchto uživatelských účtů tedy může dojít maximálně k prozrazení těchto údajů, spolu s historií transakcí, provedených s tímto uživatelským účtem – tedy historie nákupů, historie hodnocení produktů, historie příspěvků na sociálních sítích. Ve většině případů lze považovat tyto účty za „anonymní“, kdy se neprovádí kontrola, zda Vámi používané identifikační údaje (jméno, adresa) jsou pravé. Systémy často kontrolují jen Váš přístup k zadané emailové adrese, a někdy i přístup ke sdělenému číslu mobilního telefonu.

Doporučení: u těchto uživatelských účtů je možné využívat mnemotechnická, avšak delší textová hesla (min. 12 znaků) nebo schopnosti prohlížečů zapamatovat si Vaše přihlašovací údaje (jméno, heslo), které souvisí s danou Internetovou stránkou. U těchto použití lze při ztrátě hesla z paměti počítače nebo při jeho zapomenutí provést jednoduchý reset hesla obvykle zasláním výzvy k nastavení nového hesla na Vaši emailovou adresu.

- V případě nejnižších úrovní dopadů lze s výhodou využít i moderní vestavěné funkce typu **“správce hesel” dnešních webových prohlížečů,** které si nejen dokážou zapamatovat uživatelské jméno a heslo, dokážou i vygenerovat “silné” heslo, odlišné pro každý přihlašovací účet. Tato funkce může být třeba aktivována v “Nastavení”, a podle typu prohlížeče je obvykle dále v uživatelském profilu, volba např. “hesla”. Zde je typicky možné spravovat všechny “zapamatované” kombinace jména/hesla pro jednotlivé webové stránky – je možné je smazat, a po znovu potvrzení hesla k účtu prohlížeče je někdy možné i hesla zobrazit v otevřeném textu. Kromě zjevných výhod má využití vestavěného správce hesel i svoje nevýhody: (i) paměť hesel je vázána na konkrétní typ prohlížeče – pokud chcete nebo potřebujete pro jiné webservery použít jiný prohlížeč, hesla nebudou automaticky k dispozici; (ii) hesla se obvykle replikují do cloudu k danému poskytovateli (typicky Google Account, Microsoft Account, Apple ID). To má výhodu v tom, že při použití stejného typu prohlížeče máte “svoje hesla” k dispozici na všech zařízeních (notebooky, tablety, chytré telefony) i po jejich výměně, avšak s tímto musíte mít důvěru k danému poskytovateli, že celý obsah správce hesel bude trvale uložen (samozřejmě v zašifrované formě) u daného poskytovatele.
- **Vazba na evropské nařízení eIDAS:** zde používané prostředky elektronické identifikace (obvykle jen „anonymní“ jméno a heslo) nelze přiřadit ani k nejnižší úrovni „nízká“ dle eIDAS, protože s nimi obvykle není spojeno předání údajů a čísla občanského průkazu nebo jiného průkazu vydávaného státem. Běžně tyto identity považují za identity bez fyzické kontroly skutečné identity uživatele.

Střední dopady

Identity spojené se službami, které ukládají údaje o Vašich platebních kartách a případně i bankovních účtech, avšak ne s takovou transakční hodnotou, která by Vám mohla způsobit existenční potíže – a to jak finančně, tak z hlediska osobní reputace, nebo z hlediska právní odpovědnosti za provedené úkony (tedy nikoli transakce typu převod vozidla, podpis obchodní smlouvy, nebo výpisy z Vaší zdravotnické dokumentace). Omezení zneužití Vaší identity v oblasti elektronického bankovnictví nebo platebních karet je zde obvykle limitováno maximální hodnotou jednotlivých transakcí, nebo sumy denních / týdenních finančních transakcí. Do této úrovně patří oblíbené identity se schopností federace typu Microsoft account, Google account či Apple ID, pokud je skutečně využíváme pro přihlašování do různých dalších Internetových služeb, a pokud se rozhodneme přímo v této službě uložit údaje o platební kartě (pro jednoduchost nákupu přes napojené tržiště aplikací). Obdobně sem lze zařadit uživatelské účty ve službách typu PayPal, Uber, Booking.com a podobným, pokud sem ukládáme i údaje o platebních kartách. Do této úrovně lze zařadit také mnoho podání vůči státní správě, část komunikace přes systém datových schránek a transakce provedené přes Portál občana, které nevyžadují správcem systému elektronickou identifikaci dle úrovně záruk (eIDAS) „vysoká“.

Doporučení: využití těchto elektronických identit by mělo být vždy podmíněno vícefaktorovou nebo alespoň vícestupňovou autentizací (tedy dodatečným ověřením přihlašující se osoby). V současné době již téměř všichni poskytovatelé služeb s takovou transakční hodnotou umožňují vícefaktorovou autentizaci prostřednictvím chytrého telefonu. Služby elektronického bankovnictví jsou dobrým příkladem poskytovatele vlastní služby (správy bankovního účtu) a kromě toho i poskytovatelem ověřené identity. Použití kreditních karet v EU je dnes na tlak vydavatelů (bank) převáděno na metodu

platby „SecureCode“ (VISA/MasterCard) nebo podobnou, tedy kdy uživatelské nastavení využití kreditní karty vyžaduje v průběhu transakce ověření pomocí dodatečné autentizace zadavatele (obvykle mobilní aplikace nebo jedinečný SMS kód). O něco nižší míru zabezpečení než „dvoufaktorová“ vykazuje „dvoustupňová“ autentizace, která nemusí být vázána na jiný prostředek, ale využívá se typicky zasláním dalšího transakčního kódu na Vaši emailovou adresu. Přístup k takovému emailu ale není vázán na daný prostředek, a proto může být pro útočníka snadnější si takový přístup předem zajistit.

- U služeb veřejné správy se naopak očekává, že orgány veřejné moci budou akceptovat a vyžadovat elektronickou identifikaci jednotně prostřednictvím systému e-identita, a to v úrovni záruk nejméně „značná“ (dle eIDAS), kde je uplatnění příslušné úrovně ověření fyzické identity i mechanismu autentizace dáno prováděcími předpisy.
- Jako typické příklady práce s elektronickou identitou pro tuto úroveň záruk je Mobilní klíč eGovernmentu ČR, nebo různé tokeny pro generování jedinečných hesel nebo mobilní aplikace pro bezpečnější přihlašování do elektronického bankovnictví.
- Využití chytrých telefonů a jejich mobilních aplikací je dnes mnoha uživateli využíváno s přihlašováním pomocí biometriky (otisk prstu nebo scan obličeje / oční duhovky). V nejslabším případě tak je možné prolomit celý systém např. krádeží takového chytrého telefonu a schopností napodobit Vaše biometrické údaje útočníkem, který odemkne biometrikou samotný telefon, pak ještě bankovní aplikaci, a potom ještě funkci pro druhý faktor (např. onu speciální autentizační aplikaci). Obecně se v úrovni záruk „značná“ považuje dodatečná autentizace biometrikou za dostatečnou a je spíše na výrobci toho kterého chytrého telefonu, jak obtížné je příslušný biometrický senzor přelstít.
- Jak zde naložit (kromě prostředku druhého faktoru autentizace) s přihlašovacími hesly nebo PINy? Jistěže nejlepší je nikam si je nezapisovat, používat „neslovníková“ hesla, k jejich zapamatování používat mnemotechnické pomůcky a ke každé takové identitě použít jiné uživatelské heslo, To však pro mnoho z nás může být problém si tato hesla zapamatovat, a to tím více, kdy některé identitní systémy vyžadují pravidelnou obměnu hesla. Možná řešení:
  - **použít speciální program typu „password manager“** pro správu a zabezpečené ukládání hesel. Takový program přímo vygeneruje silné heslo pro každou novou identitu (uživatelský účet) a uloží si je do zašifrovaného úložiště. Uživatel si pak pamatuje jen jedno heslo do této zvláštní aplikace, pravděpodobně opět s využitím dvoufaktorového přihlašování. Ověřené speciální programy typu “password manager” mají obvykle vyšší úroveň zabezpečení uložených hesel než pouhý prohlížeč, ale mohou mít další požadavky na zálohování a přenos funkce na jiná zařízení. Doporučujeme zvážit výhody a nevýhody konkrétních řešení, zejména proto, že jde většinou o placenou službu. Přehled těchto programů a jejich porovnání lze nalézt např. zde: Přehled těch nejlepších správců hesel - PCWorld.cz; 5 nejlepších správců hesel pro Windows v roce 2021 [s kupony] (safetydetectives.com); Best password manager in 2021 for business & personal use | ZDNet; □ Nejlepší; Správce Hesel AKTUALIZOVÁNO2021
  - Běžné **automatické ukládání hesla do paměti Vašeho internetového prohlížeče lze doporučit jen v případě**, že využíváte vestavěnou funkci prohlížeče, díky které máte hesla zabezpečena hlavním heslem a máte celý disk počítače nebo mobilu kvalitně zašifrovaný (např. nástrojem BitLocker který je součástí Windows apod.), a kdy máte nastaveno automatické zamykání obrazovky (lock screen) a silnější přihlašování do počítače nebo mobilu rovněž s využitím dvoufaktorové nebo jinak inteligentně řízené autentizace.
  - Kdo nechce jít bezpečnější cestou kvalitního správce “password manager”, může si hesla alespoň zapisovat do šifrovaného souboru s uživatelským heslem (např. u MS Word s využitím funkce „Soubor“, dále „Info“, dále „zabezpečit dokument“, volba „šifrování heslem“). Předpokladem je dodatečná ochrana šifrováním celého disku a zajištění záložní

kopie tohoto zašifrovaného souboru na externí médium a jeho uložení na fyzicky bezpečném místě. Přitom je třeba mít na paměti, že vlastní heslo není vhodné přenášet z jiného zobrazení (např. z onoho dokumentu) pomocí copy&paste, protože obsah clipboardu může být lehce cílem útoku skrytého malwaru. Tento zašifrovaný soubor je také třeba pravidelně zálohovat – nejlépe mimo primární zařízení.

- **Vazba na evropské nařízení eIDAS:** tyto transakce odpovídají využití prostředků elektronické identifikace v úrovni „**značná**“, neboť použití identity zde předpokládá ověřenou fyzickou identifikaci osoby (v bance nebo u orgánu veřejné moci, např. CzechPoint).

Vysoké dopady

Identity spojené nebo využívané s elektronickými službami, které mohou mít na uživatele nejvyšší až existenční dopady. Zde se obecně předpokládá, že tyto kategorie služeb eGovernmentu budou do těchto dopadů zařazeny již správci takových služeb veřejné správy, a budou v souladu s nařízením eIDAS vyžadovat použití prostředku elektronické identifikace s úrovní záruk „vysoká“. Sem budou pravděpodobně patřit služby typu elektronický výpis ze zdravotnické dokumentace a služby veřejné správy s vysokou transakční hodnotou (např. převod vlastnictví automobilu, převod nemovitosti). Dále sem patří scénáře vyžadování kvalifikovaného elektronického podpisu, a případně další scénáře, kdy takové elektronické služby se sami rozhodneme využívat pouze s prostředkem elektronické identifikace v úrovni záruk „vysoká“, tedy zejména eOP. Jak je již uvedeno výše – některé služby budou vyžadovat úroveň „vysoká“ rozhodnutím správce. U jiných služeb, zejména u soukromoprávních poskytovatelů, by mělo být možné si ve svém uživatelském profilu nastavit, jaký způsob a prostředek elektronické identifikace budu sám pro danou službu vyžadovat, tak aby k této službě nemohl získat přístup útočník, který by alternativně využil přihlašování jiného prostředku pro elektronickou identifikaci s nižší úrovní záruk.

Doporučení: pro úroveň záruk „vysoká“ bude ve většině případů třeba použít interní nebo externí čtečku eOP (přes USB port) nebo USB token jako kvalifikovaný prostředek pro elektronický podpis s kvalifikovaným elektronickým certifikátem. Použití externího a jednoúčelového zařízení má velký vliv pro odizolování útočníka, který by mezitím mohl ovládnout Váš osobní počítač, tablet nebo chytrý telefon. Zjednodušeně řečeno se má za to, že vygenerování jedinečného kvalifikovaného el. podpisu nebo autentizačního hashe pomocí externího prostředku v úrovni záruk „vysoká“ představuje značnou ochranu, kterou dnes můžeme systémově zavést proti nejvíce sofistikovaným kybernetickým útokům na elektronickou identitu.

- Jediné, co je třeba k provedení elektronické identifikace v této nejvyšší bezpečnostní úrovni, je mít u sebe příslušný externí token nebo čtečku smart karty, a PIN pro odemknutí podpisového nebo autentizačního certifikátu. Tento PIN je již třeba si zapamatovat a rozhodně nedoporučujeme si jej kamkoli zapisovat (maximálně si zapsat do šifrovaného souboru jen jako mnemotechnický opis, kterému neporozumí jiné osoby).
- **Vazba na evropské nařízení eIDAS: Vazba na evropské nařízení eIDAS:** tyto transakce odpovídají využití prostředků elektronické identifikace v úrovni „**vysoká**“.

Známé typy útoků

Pro stanovení známých typů útoků v kyberprostoru, které mohou vyústit v ohrožení elektronické identity, lze využít popis nejčastějších vektorů útoku, které kybernetičtí útočníci nejčastěji užívají k dosažení svých cílů:

- **backdoor** lze definovat jako zneužití přístupu do zařízení instalací škodlivého kódu umožňujícímu vytvoření zadních vrátek pro následné neoprávněné aktivity ze strany útočníka, ochranou proti tomuto typu útoku je zejména komplexní antivirové řešení;
- **cross-site scripting** nastává za předpokladu zneužití webové aplikace ze strany útočníka ke spuštění nežádoucího kódu v zařízení, ochrana je obdobná jako v případě backdooru, kdy ji lze doplnit bezpečnými webovými prohlížeči;
- **man-in-the-middle** je typ útoku, při kterém je útočníkem zachycena komunikace mezi dvěma zařízeními a neoprávněně nahrazena zcela nebo zčásti daty útočníka, čímž dojde k narušení důvěrnosti a integrity přenášených dat, ochranou je využívání důvěryhodného (vyhnutí se veřejným Wi-Fi sítím) a bezpečného internetového připojení (s dostatečnou úrovní šifrování – na u př. Wi-Fi sítí přinejmenším WPA2), kdy jej lze doplnit VPN službami od důvěryhodných poskytovatelů;
- **sociální inženýrství** je v současnosti jedna z nejčastějších technik využívajících sociální zranitelnosti oběti pro získání informací využitelných pro široké spektrum následných neoprávněných aktivit v kyberprostoru, ochranou proti tomuto typu útoku je zejména obezřetnost uživatele a dodržování zásad kybernetické bezpečnosti (nesdělování údajů, které by mohly být zneužity při následném kybernetickém útoku);
- **phishing** je útok za využití e-mailových zpráv, ve kterých je obvykle zastřen skutečný odesílatel pro získání informací od oběti, kdy je obvykle doplněn technikami sociálního inženýrství, obranou proti tomuto typu útoků je užívání bezpečné e-mailové služby (s kontrolou přijímaných e-mailů v aspektech odesílatele, šifrování, manipulací se záhlavím e-mailu, bezpečnosti obsažených odkazů, příloh a dalších prvků e-mailové zprávy), vlastní kontrola záhlaví e-mailu (IP adresa odesílatele, servery přes který byl e-mail zaslán), kontrola obsažených odkazů (skutečná adresa uvedeného odkazu), případně i zpětné ověřování validity zaslaného e-mailu (kontaktování subjektu odesílající e-mail jinou formou);
- **spear phishing** označení pro cílený phishing na konkrétní jednotlivce, případně organizace pro následné neoprávněné aktivity, ochrana proti tomuto typu útoku je obdobná jako u phishingu;
- **útoky na hesla** je využíván útočníky pro neoprávněné získání přístupu do koncového zařízení, případně uživatelského účtu, přičemž jsou útočníkem užívány různé kombinace hesel (získaných např. v rámci slovníků nejčastěji používaných hesel, ale i informací získaných o oběti jinými způsoby) pro jeho odhalení, ochranou může být užívání silného hesla, které bude zároveň odlišné pro každou službu (včetně jeho pravidelné změny, s možností nastavení kontroly úniku přístupových údajů vázaných na konkrétní uživatelský účet na službách monitorujících úniky uživatelských účtů na internetu) a rovněž doplněného o vícefaktorovou autentizaci pokud je provozovatelem služby k dispozici;
- **zranitelnost nultého dne** je vektor útoku, u kterého útočník neoprávněně zneužívá zranitelnosti hardwaru zařízení nebo softwaru, o kterých obvykle v době útoku nemá povědomí jejich výrobce, je tudíž proti němu velmi obtížná obrana, obecně však lze doporučit využívání nejaktuálnějších produktů jak z hlediska hardwaru, tak softwaru a preference bezpečných výrobců z pohledu historického výskytu známých zranitelností a dalších aspektů.
- **vishing** – vzniklo slovním spojením z anglického "voice" a "phishing". Jedná se o telefonickou obdobu phishingu, kdy útočník obvolává své oběti, vydává se za zástupce určité instituce a následně se z nich snaží vylákat citlivé údaje. Útočník často zneužívá služeb Voice-over-IP pro podvržení telefonního čísla. Obdržený hovor tak vypadá, jako by byl realizován z legitimní klientské linky dané instituce.
- **útoky typu MITM na zařízení** – Útočník se snaží získat přístup k zařízení své oběti. Pokud se mu to podaří může nainstalovat nějaký software na dané zařízení, ať už je to počítač, tablet nebo telefon a toto zařízení může odchytávat komunikaci, kterou generují aplikace na počítači nebo sám uživatel. Útočník tak může např. odchytit heslo nebo PIN zadávané přes klávesnici nebo může nainstalováním nějaké závislé knihovny získat citlivé údaje přenášené mezi aplikacemi. Tento přístup může útočník získat využitím zranitelnosti v neaktuálním software na

počítači, přesvědčením uživatele, že má otevřít nějaký email nebo stáhnout nějaký software z webu (phishing). Jediná možnost, jak se tomuto bránit, je kontrolovat přístup k zařízení, mít vždy aktuální verzi operačního systému a antivirus a neotevírat neznámé přílohy mailů.

- **útoky typu MITM mimo zařízení** – Útočník se může pokusit odchytit komunikaci mezi zařízením oběti a serverem poskytujícím služby. Nejčastější postup je, že útočník vytvoří webovou stránku, která se velmi podobá cílové službě a oběť si tak myslí, že komunikuje s touto službou, zatímco komunikuje s útočníkem. Následně např. phishingem útočník přesvědčí oběť, že je nutné se ke svému účtu přihlásit. Útočník pak sám napřímo komunikuje se službou a předstírá, že je oběť. V průběhu komunikace může útočník vylákat nejen heslo, ale i jednorázové kódy zaslané na telefon nebo souhlas vydaný autentizační aplikací. Uživatel by měl znát a důsledně hlídat doménové jméno v adresním řádku prohlížeče na webové stránce, kde provádí autentizaci. Útočník se může snažit maskovat název domény za podobně vypadající např. (flo.cz místo fio.cz).
- **útoky typu sim swap** – Jelikož je SIM karta pouhý identifikátor, kterým se zákazník prokazuje svému telefonnímu operátorovi, existuje možnost převést telefonní číslo na jinou SIM kartu. Telefonní operátoři mají mechanismy, jak umožnit zákazníkům získat zpět číslo, pokud například ztratili telefon. Tyto mechanismy mohou být různou měrou odolné proti tomu, aby útočník získal telefonní číslo oběti na svojí SIM kartu. Útočník obvykle opět technikou sociálního inženýrství vyláká na oběti některé soukromé informace, které následně využije při komunikaci s telefonním operátorem. Přestože není jednoduché se takovémuto typu útoku bránit, je možné to útočníkovi ztížit např. tím, že operátor umožní nastavit požadavek, že jakékoliv změně SIM musí předcházet fyzická kontrola.

bezpecnost, eid, utok, kyber, kyberbezpecnost, identita