Zákon o kybernetické bezpečnosti – správa, uchování a sdílení hesel

Zákon o kybernetické bezpečnosti (dále jen ZKB) se mimo jiné věnuje bezpečnosti uživatelů systémů, které spravují citlivá data. Pro případného útočníka je totiž mnohem snazší a efektivnější zaměřit se právě na uživatele než na systém, ve kterém pracuje.

Pokud začínáte číst tento článek, jste s největší pravděpodobností uživatelem a s velkou pravděpodobností uživatelem některého informačního systému používaného ve veřejné správě. Je také pravděpodobné, že pro vás platí nějaká směrnice, která předepisuje, jak dlouhé a složité máte mít heslo, jak často ho máte měnit (ZKB nařizuje, že se heslo musí měnit nejpozději po 3 měsících, ale my si v dalším textu ukážeme, že účinnost tohoto opatření je pochybná), zda a kam můžete jít na internet v pracovní době apod. Pokud se v problematice hesel orientujete, nenuďte se a přeskočte na sekci RainMan nebo rovnou na Sdílení…

Kdyby byl autorem tohoto článku právník, vyjmenoval by, co jako uživatel nesmíte, a měl by problém za vyřešený. Ukažme si to na důležitém tématu hesla a jeho bezpečnosti (pro milovníky certifikátů – i karta, na které je uložen certifikát, má heslo – často se mu říká PIN a to pak mívá jen čtyři znaky…). Důležité je, aby heslo bylo **kvalitní**, nedalo se odhadnout podle jmen dětí, partnerů či zvířátek, a bylo použito jen jednou. To se lehce řekne, ale hůře udělá. Obecně platí, že čím kvalitnější heslo je, tím hůře se pamatuje. Lidský mozek si po tisících letech evoluce dokáže pamatovat tisíce příběhů a kdykoliv je zopakovat ne slovo od slova, ale tak, že si posluchači odnesou podstatu. Heslo si ale potrpí na **absolutní přesnost**, se kterou má mozek problém. Proto má tendenci si vypomáhat třeba tím, že jej tvoří například první slabiky křestních jmen dětí v pořadí podle věku. To je jednak významné usnadnění pro útočníka, ale hlavně je to jen **jedno heslo**. Co se týče hesel, nikdo nemá pracovní a soukromou polovinu mozku – kromě pracovních účtů máme ještě soukromý email, facebook, twitter a vůbec vše „sociální“, platební karty, mobilní telefony, alarm, alza, mall, amazon a vůbec všechny e-shopy, věrnostní systémy atd…

Nejsnazší je použít pěkné a zapamatované heslo vícekrát. Tak to mnoho lidí dělá a proto se útočníci namáhají s útoky na jinak bezvýznamné erotické weby, veřejné emailové systémy, online prodejny videoher apod – je jim úplně jedno, zda jste si koupili poslední vydání známé střílečky. Útočník chce zkusit, zda použitá emailová adresa prozradí, kdo jste, kde pracujete a zda použité uživatelské jméno a heslo lze použít pro **přístup k nějakému vašemu pracovnímu systému**. Toto je například podstata úspěšných útoků na banky v poslední době – přihlášení na existující a oprávněný účet bankovního úředníka a následně převod peněz po malých částkách, které ujdou podrobnější kontrole. Samozřejmě, toto se vám nestane, pokud použijete každé heslo skutečně jen jednou a pokud to budou hesla kvalitní.

RainMan?

Protože výše uvedeným požadavkům na práci s hesly dokáže vyhovět jen RainMan a jemu podobní, jsou vytvořeny speciální programy, tzv. **„Správci hesel“** (Password manager). To je obecně řešení, které dokáže uložit neomezený počet různých hesel včetně dalších informací (jméno a k jakému systému tato dvojice patří), certifikáty, dokumenty apod. Vše odemknete jedním heslem, které jediné si musíte pamatovat, a zdá se, že problém je za cenu mírného nepohodlí (přece jen je snazší všude psát „kopretina123“) vyřešen. Samozřejmě, je otázka, zda vám zaměstnavatel dovolí si něco takového nainstalovat na pracovní počítač. Může se například obávat, že prostřednictvím takového programu, nad kterým potažmo nemá kontrolu, může dojít k masiv-

Příběh o zadávání hesla a pití kávy

Jeden uživatel a mimochodem špičkový lékař, razí zásadu, že autentizace na klávesnici musí být možná jednou rukou beze změny její polohy, protože ta druhá je vyhrazena pro transport kávy v hrnku zvíci malé kočky. Takže vždy, když je těmi otravnými hláškami donucen si heslo změnit, dá si tu práci a najde novou kombinaci, kterou zadá na klávesách dosažitelných prsty jedné ruky a která vyhovuje neméně otravné politice. Není to nijak jednoduché a tak vždy, když je hotov, předá toto nové heslo všem svým kolegům, aby si také mohli usnadnit život a nemuseli pokládat kávu na stůl kvůli pouhé autentizaci. Díky němu má přibližně 200 uživatelů nezvěřejněné nemocnice stejné heslo, vědí to o sobě a nástroje IT oddělení s tím nic nezmůžou – nastavené politice odpovídá a porovnávat hesla uživatelů nelze. Generátory hesel mají své nesporné výhody nejen kvůli dosažení požadované kvality…

nímu úniku všeho, co si do něj uložíte, a to včetně přístupových údajů do centrálních systémů. RainMan si vše dokázal zapamatovat a mohl tudíž psát zpaměti kamkoliv. Vy si můžete takový program pořídit pro svůj chytrý mobilní telefon. Můžete si nastavit dostatečně kvalitní heslo, pamatovat si ho a nikomu ho neříci. A opět jsme téměř ve stavu vyřešeno. Jenže v pracovním i soukromém životě potřebujeme minimálně **část těchto informací sdílet**. S kolegy, s rodinou a prakticky i s těmi, kteří vám údaj přidělí – musí vám ho nějakým bezpečným způsobem předat. Odstrašující příklad jsou některé e-shopy, které vám po registraci zašlou uvítací email: „Děkujeme, že jste se stal naším zákazníkem. Zde pro kontrolu zasíláme uživatelské jméno a heslo, které jste si u nás zvolil.“ Pokud v takovém emailu uvidíte jméno a heslo do práce nebo k něčemu důležitému, máte **problém** a je třeba jednat rychle a všechny postižené účty změnit – pokud to tedy jde a nemusíte o změnu žádat správce nebo provozovatele.

Sdílení

V praxi reálně použitelný systém musí umět vybrané informace sdílet. V IT je to například sdílení přístupových údajů k zařízením jako jsou switche, routery, WiFI AP, RAID pole, HW servery atd. Máme-li 3 správce, kteří se mají navzájem zastupovat, a přitom chceme, aby každé zařízení mělo „své“ bezpečné heslo, potřebují **bezpečné úložiště**, kam se všichni dostanou a kde budou mít aktuální nastavení. Nejde ale zdaleka jen o IT. Organizace využívají mnoho systémů, kde je jeden účet pro organizaci a ne pro každého uživatele, který s ním pracuje. Takto se využívají různé portály provozované státem, e-shopy, kde si objednáte kancelářské potřeby apod. Akci v požadovaném terminu pak provede ten pracovník účtárny, který zrovna není nemocen a nemá dovolenou. K tomu potřebuje přístupové údaje.

Bílé obálky v trezoru

Probíráme-li sdílení, nesmíme opominout jeden specifický případ. Některé účty nejsou sdíleny, protože jejich znalost definuje uživatelovu zodpovědnost – jméno a heslo ví jen on, jen on se mohl přihlásit a provést nějakou akci. Pokud ale o uživatele přijdeme, ať už jde o tragickou nehodu nebo situaci, kdy se rozejde s organizací opravdu ve zlém, potřebujeme se k informacím dostat a předat je někomu jinému. Tento problém se velmi často řeší selským rozumem – uživatel napíše ta důležitá jména a hesla na papír (všimněte si, certifikát takto reálně uložit nelze), papír vloží do obálky, obálku zalepí a uloží do trezoru třeba v účtárně nebo v kanceláři ředitele. Pokud dojde na nejhorší, otevřeme trezor, rozlepíme obálku a při troše štěstí máme **správné jméno a heslo**. Pro uživatele totiž není úplně snadné heslo po změně updatovat a tak se může stát, že máme papír s původními hesly a ne s těmi, která platí dnes.

Vynucené změny hesel

Tím se vracíme k otázce, zda je účelné nutit uživatele do změny hesel, zda nám to skutečně přinese vyšší bezpečnost. A odpověď zní **NE**. Pokud uživatel použije totéž heslo někde v internetu, máme problém, který změna hesla za 3 měsíce nevyřeší. Pokud nutíme uživatele vymyslet za sebou 10 různých hesel (obvyklé nastavení), **kvalita těchto hesel klesá** – mozek není na tuto činnost stvořen a snaží se si pomoci něčím jako heslo1, heslo2 nebo brezen2016, cerven2016… a tak podobně. Úplně extrémní případ pak je situace, kdy jeden uživatel pomáhá ostatním tím, že vymyslí heslo na další 3 měsíce a všichni si ho nastaví. Že se to nemůže stát? Vsadíte se? Kvalitní heslo má jednu podstatnou výhodu oproti certifikátu – s počtem použití neklesá jeho bezpečnost. Dobré heslo můžete používat celá léta, pokud ho nikomu neřeknete, nepoužijete nikde jinde a nezadáte na stanici, na které je aktivní tzv. **keylogger**.

Bezpečnost pracovní stanice

Ochrana pracovní stanice je kritickým prvkem bezpečnostního řešení jak pro práci s hesly, tak s certifikáty. Pokud můžete pracovat z počítače, nad kterým organizace nebo provozovatel informačního systému nemá žádnou kontrolu, můžete významně **ohrozit bezpečnost**, i když jinak všechna doporučení z tohoto článku a jiná poctivě dodržujete. A nemusí vždy jít o zákeřný program číhající na chvíli, kdy zadáte své heslo nebo PIN. Pokud si informační systém nemůže ověřit, zda má vaše stanice například aktivní automatické zamykání, nemůže vám ani v nejmenším pomoci v situaci, kdy od přihlášení stanice ve stressu odběhnete a útok provede náhodný kolemjdoucí kolega. Dvě třetiny všech útoků provedou nebo se na nich podílejí kolegové. To je realita. Bezpečnost stanice je téma na samostatný článek, ale nelze ho zde nezmínit.

Závěr

Vyšší bezpečnosti dosáhneme pouze, pokud uživatele poučíme jak se chovat bezpečně a umožníme jim chovat se bezpečně. Nestačí jen říci „nepoužívejte jedno heslo více než jednou“, je nutné mít **nástroje**, které to umožní a bezpečnost ještě nezhorší. Řešení, které použijete, musí také zahrnovat **generátor hesel**, který dokáže vytvořit bezpečná ale přitom použitelná hesla – tedy taková, která si například na chvíli zapamatujete, než je zadáte do systému, do kterého je nemůže přenést přes clipboard nebo která nelze doplnit automaticky.

Ing. Václav Šamša
autor je ředitelem společnosti TDP

Nedovolte, aby vás někdo mohl sledovat webkamerou!

Během nedávné konference ve Středisku pro strategická a mezinárodní studia (CSIS) ředitel FBI James Comey doporučil řadu účelných opatření pro lepší ochranu soukromí. Jednou z jeho rad bylo zakrývat si webkameru u počítače.

Nezalepené webové kamery mohou otevřít cestu hackerům a vytvořit tak ideální podmínky například pro vydírání nebo průmyslovou špionáž. *„Zamykáme naše domy a auta, proč by tedy naše počítače měly být přístupné zločincům?”* ptá se hlava FBI. A mnoho uživatelů počítačů si skutečně uvědomilo, že webkamery mohou narušit jejich soukromí.
Elegantnějších možností zakrytí, než jsou lepicí pásky, je samozřejmě na trhu celá řada. Jedním z nich je například řešení společnosti MMD, které mění webovou kameru notebooku nebo monitoru na manuálně ovládanou hardwarovou funkci, která je prakticky nenapadnutelná.

pk