AUDITOR

časopis Komory auditorů České republiky číslo 3/2021

Téma: Kybernetická bezpečost

aktuality • informace z komory • stanoviska, názory, diskuze • nabídka vzdělávacích akcí • auditorské postupy • vybrané účetní problémy • daňová a právní problematika • informace ze zahraničí

AUDITOR 3/2021

Obsah

Toto číslo vyšlo **29. 3. 2021**

Jak probíhají zkoušky na komoře v době pandemie

Zdeněk Grygar

Situace v České republice v posledním roce velmi ztížila činnost výboru pro auditorské zkoušky. V souladu s bezpečnostními opatřeními vlády ČR byly v loňských jarních a podzimních měsících rušeny plánované termíny dílčích částí auditorské zkoušky. Náhradní termíny těchto zkoušek byly koncentrovány do června a prosince 2020. Tato situace velmi snížila komfort uchazečů při skládání zkoušek. Vedle toho byla zrušena řada přípravných kurzů před zkouškou, které KA ČR nabízí a organizuje. Ve druhém pololetí 2020 jsme některé kurzy začali postupně organizovat online formou, avšak v řadě případů se nesetkaly s kladnou odezvou u účastníků i lektorů. Důvodem byl nezájem uchazečů o tuto formu kurzu, nebo lektor formu nedoporučil vzhledem k tomu, že kurz předpokládá specifickou interakci mezi lektorem a účastníkem. I přes tuto situaci však KA ČR v roce 2020 dostála svým povinnostem, které jí ukládá § 8 odst. 6 zákona o auditorech, a to stanovit v každém kalendářním pololetí nejméně jeden termín pro konání každé dílčí části auditorské zkoušky.

Auditorská zkouška je upravena § 8 zákona o auditorech a Zkušebním řádem KA ČR. Zkouška se skládá z 12 písemných dílčích částí a uchazeč má na jejich složení lhůtu pěti let. V současné době ve svém zkouškovém systému evidujeme celkem 278 uchazečů, přičemž podíl mužů a žen je vzácně vyrovnán. Věkově není uchazeč o auditorskou zkoušku nijak omezen, musí však počítat s tím, že zkoušky prověřují celé spektrum vědomostí, od znalosti práva, zdaňování, finančního účetnictví vč. účetnictví specifických subjektů a procesů, podnikových financí až po specializované zkoušky z auditingu. Obtížnost těchto zkoušek je v zásadě na úrovni studijních programů magisterského studia na vysoké škole. Aktuálně je nejmladšímu uchazeči 24 a nejstaršímu 64 let. Průměrný věk našich uchazečů je 34,5 roku. Z celkového počtu uchazečů zhruba tři čtvrtiny již složily dvě a více zkoušek.

V posledních letech přibývá odvolání uchazečů proti výsledku zkoušky. Zatímco KA ČR např. v roce 2015 řešila tři odvolání, v roce 2019 čtyři a v roce 2020 šest, v letošním roce řešíme šest odvolání za pouhé první dva měsíce. KA ČR v těchto případech ustavuje odvolací zkušební komisi. Úkolem této komise je, aby na základě písemného zkouškového zadání, vzorového řešení, stanoviska autora písemky k námitkám uvedeným v odvolání a vlastního zkoumání rozhodla o oprávněnosti námitek účastníka k bodovému hodnocení. Zkouška je složena úspěšně, pokud účastník dosáhne bodového hodnocení 60 a více bodů ze 100 možných. Zatímco dříve se odvolávali uchazeči, kteří dosáhli bodového hodnocení mezi 50–60 body, v posledních dvou letech je trendem stále nižší hranice bodů pro odvolání. Účelem toho je v odvolacím procesu uspět ve zkoušce cestou „zkusím se odvolat, třeba to vyjde“.

V nejbližším období bude činnost výboru pro auditorské zkoušky zaměřena zejména na problematiku elektronizace zkoušek a realizaci nového systému auditorských zkoušek plánovaného od 1. ledna 2022.

Zdeněk Grygar
předseda výboru
pro auditorské zkoušky

Ze zasedání Výkonného výboru KA ČR

Výkonný výbor se na svém on-line zasedání, které se uskutečnilo 15. února 2021, zabýval jak standardní agendou, tak aktuálními činnostmi jednotlivých odborných výborů KA ČR. Významnou částí jednání byla analýza možností realizace distančního sněmu a potřebných úprav vnitřních předpisů KA ČR.

Výkonný výbor schválil:
- jmenování Jana Molína členem redakční rady časopisu Auditor,
- metodický pokyn pro šifrování souborů dílčích částí auditorských zkoušek,
- pondělí 10. května 2021 jako předběžný termín pro konání sněmu KA ČR,
- aktualizaci směrnice B18 Zásady organizace přípravy a oprav auditorské zkoušky a rozdílové auditorské zkoušky.

Výkonný výbor dále projednal:
- návrh programu sněmu KA ČR,
- a vzal na vědomí novelizaci Kárného řádu, která bude předložena sněmu KA ČR,
- a schválil postup pro úpravu vnitřních předpisů pro možnost pořádání distančního sněmu,
- a schválil možnosti využití platformy pro distanční vzdělávání

a vzal na vědomí:
- informace z výboru pro správu profese o slibu nových auditorů,
- informaci o přípravě vnitřních předpisů předkládaných sněmu,
- plnění rozpočtu komory za období leden–prosinec 2020,
- Zprávu o činnosti kárné komise za II. pol. roku 2020,
- zápisy ze zasedání prezidia, komisí a odborných výborů,
- statistiku uložených kárných opatření,
- informace o podnětech vyřizovaných kárnou komisí v roce 2020 a 2021,
- legislativní monitoring.

Jiří Mikyna
ředitel úřadu Komory auditorů ČR

Proč bude XXVII. sněm KA ČR korespondenční

Výkonný výbor na svém mimořádném zasedání dne 11. března 2021 schválil konání distančního sněmu v korespondenční podobě. Výkonný výbor a zejména prezidium se otázkou konání sněmu intenzivně zabývá v podstatě od září 2020. Poté, co bylo zrušeno konání původně plánovaného prezenčního sněmu na podzim 2020, jsme hledali cestu, jak uspořádat sice opožděný, ale stále prezenční sněm. O podrobných důvodech jsme informovali již v dřívějších číslech časopisu Auditor, ale hlavním důvodem bylo to, že předpisy KA ČR neumožňují konání distančního sněmu a volby do orgánů komory musí být tajné.

Sněm však nelze odkládat neustále. Nejen, že to není dobré pro profesi, ale také se blíží konec lhůty, kterou zákon (lex covid) umožnil prodloužení funkčního období členů orgánů právnických osob. Výkonný výbor se tedy na svém únorovém zasedání usnesl, že sněm se bude konat v květnu. Nejprve to vypadalo na klasický prezenční sněm, ale s ohledem na stále se zhoršující vývoj kolem pandemie covid-19 se jako jediné přijatelné řešení začalo přece jen jevit uspořádání sněmu distanční formou.

KA ČR tedy iniciovalo diskuzi s ministerstvem financí ohledně alespoň dočasné změny zákona o auditorech, která by konání distančního sněmu umožnila. Tomu nakonec MF nebylo nakloněno, na druhou stranu však ve svém přípisu zastalo názor, že lex covid by mohl být využit ke konání distančního sněmu, který by změnil vnitřní předpisy tak, aby distančně bylo možné uspořádat i tajné volby. Distanční volby, pokud je statut a vnitřní směrnice nepřipouští, totiž nelze uspořádat ani za pomoci ustanovení lex covid.

Aby bylo možné distanční sněm uspořádat, i když to neumožňují naše dosavadní předpisy, je nutné pro takový sněm přijmout specifická pravidla. K vydání těchto pravidel zmocňuje zákon (viz ustanovení § 19 odst. 2 lex covid) statutární orgán právnické osoby, kterým je v případě KA ČR dle zákona o auditorech prezident (resp. prezidentka) komory. V této souvislosti tedy prezidentka přijala nezbytná pravidla, která byla zveřejněna na webových stránkách komory. Tato pravidla byla podrobena jak připomínkám výkonného výboru, tak byla po dobu 10 dnů předložena k připomínkování celé auditorské obci, ač zákon žádné takové připomínkování nevyžaduje. Prezidentka všechny obdržené připomínky zvážila a nakonec vydala finální a závazné znění pravidel pro konání distančního sněmu.

Sněm bude rozhodovat v písemné formě, bude se tedy konat korespondenční formou. Všichni auditoři proto předem obdrží hlasovací a volební lístky. Hlasovací lístky budou ke stažení na webu komory (z důvodu jejich přípravy těsně před sněmem v důsledku čekání na připomínky), volební lístky budou rozeslány poštou. **Hlasovací lístky** jsou určeny k hlasování o všech záležitostech, o kterých bude sněm rozhodovat, mimo voleb do orgánů komory. Hlasovací lístek

není anonymní, naopak musí být ztotožněn s hlasujícím auditorem, aby bylo možné ověřit, že hlasy pochází od oprávněné osoby. Na hlasovacím lístku proto bude nezbytné uvést jedinečný kód, který každý auditor obdrží také poštou.

Hlavním důvodem korespondenčního hlasování je tajnost voleb (která také vylučuje využití datových schránek). Tajnost voleb bude zaručena tak, že **volební lístky** (nikoli hlasovací), které jsou anonymní, auditor zalepí do zvláštní neoznačené obálky, kterou přiloží ke svému (neanonymnímu) hlasovacímu lístku. Až společnost CENTIN, a.s., která je dlouholetým partnerem KA ČR pověřeným sčítáním hlasů na sněmech, obdrží hlasovací lístek, zkontroluje, zda pochází od oprávněné osoby, a poté připojenou zalepenou obálku s (anonymním) volebním lístkem vhodí do urny. Teprve poté, až budou do urny vhozeny všechny platně obdržené obálky s volebními lístky, dojde k otevření urny, otevření obálek a spočítání volebních hlasů. Na celý proces bude dohlížet volební komise.

Aby vůbec došlo na proces voleb, je nutné, aby předtím došlo ke změně statutu, jednacího řádu a volebního řádu KA ČR. O těchto změnách se bude hlasovat prostřednictvím již zmíněných neanonymních hlasovacích lístků. Jejich vyhodnocení a zveřejnění výsledku hlasování tedy musí předcházet otevření volební urny. Pouze za předpokladu, že sněm odhlasuje změny v těchto dokumentech, dojde na samotné vyhodnocení voleb. V případě, že sněm změny uvedených interních předpisů neschválí, volby neproběhnou a všechny obdržené obálky s volebními lístky budou skartovány.

Zvláštností hlasování na korespondenčním sněmu bude vypořádání připomínek. V případě běžných sněmů byly všechny připomínky k projednávaným bodům posouzeny výkonným výborem, který k nim vydal své doporučení a poté bylo jak o těchto doporučeních, tak o samotných připomínkách hlasováno na plénu sněmu. Toto hlasování bylo často složité, protože připomínky si mohly navzájem odporovat nebo měnit části předpisů tak, že vznikaly rozpory s jinými částmi týchž předpisů. Protože korespondenční hlasování nedokáže reagovat na vývoj jednání, změní se i přístup k připomínkám: po obdržení připomínek od členské základny k programu sněmu výkonný výbor navrhne usnesení, jak v daném případě postupovat, a toto své rozhodnutí předloží sněmu. Hlasovat se tedy bude pouze o návrzích výkonného výboru, jak danou připomínku vypořádat.

Distanční sněm se nemusí nutně konat korespondenční formou, mohl by se také konat pomocí využití technických prostředků. Komora je na tuto variantu na první pohled připravena: máme k dispozici potřebné licence ke komunikačnímu software Webex (který využíváme na on-line školení) a také již na podzimním sněmu se počítalo s hlasováním pomocí mobilních telefonů (pomocí SMS nebo aplikace). Nicméně tyto systémy neumí zaručit tajnost voleb, maximálně by bylo možné uvažovat o neveřejnosti voleb. Hlasuje-li se pomocí techniky, v systému obvykle zůstává nějaký údaj o tom, kdo hlasoval (jinak totiž není možné ověřit, že daná osoba je oprávněna hlasovat). Sofistikovanější systémy, které by toto umožňovaly, komoře nejsou v současné době dostupné ani známé.

Jakmile se ukázalo, že tajnost voleb dokážeme zaručit pouze korespondenčním hlasováním pomocí vložené neoznačené obálky, bylo nasnadě, že i hlasování o ostatních záležitostech by mělo proběhnout korespondenčně, protože tak bude moci vše proběhnout najednou a poměrně jednoduše. V případě konání sněmu za pomocí technických prostředků jsme se také obávali nepředvídatelných technických obtíží, které by mohly způsobit i neplatnost sněmu a tak zmařit jak hlasování, tak volby. Navíc pravidla prezidentky pro takový sněm by musela být mnohem složitější. Protože zvolení nových členů výkonného výboru je naprosto zásadní pro další fungování komory, rozhodli jsme tato rizika nepodstupovat.

Na druhou stranu ale možnost živé diskuze a prezentace předložených materiálů ke sněmu patří. Z toho důvodu vedení komory **zorganizuje 28. dubna 2021 prostřednictvím systému Webex informační schůzku**, která toto umožní. Samotná informační schůzka nebude oficiální součástí sněmu, a tak pokud se vyskytnou případné technické obtíže, nemůže dojít k ohrožení platnosti hlasování či voleb.

S ohledem na korespondenční hlasování nebude možné hlasovat na základě plných mocí. Auditorské společnosti nicméně mohou zaslat hlasy „svých auditorů“ hromadně, musí však být dodrženo pravidlo, že hlasovací lístek každého auditora bude ve separátní obálce, do které bude vložena další neoznačená obálka s volebním lístkem.

Podrobnější informace včetně pravidel korespondenčního sněmu, harmonogramu a důležitých lhůt jsou uvedené na webových stránkách KA ČR v uzavřené sekci Pro členy. Tyto stránky je potřeba sledovat, pokud chcete být informováni o aktuálním vývoji včetně např. vypořádání připomínek. Každému auditorovi budou také zaslány hlasovací a volební lístky včetně návratových obálek.

Závěrem bych Vám rád všem poděkoval za Vaši účast na letošním sněmu i za Váš čas, který si vyžádá tato nezvyklá forma. I korespondenční sněm bude usnášeníschopný, pouze pokud se ho zúčastné potřebné minimum auditorů. Snad se příště sejdeme za normálnějších podmínek.

Jiří Pelák
první viceprezident KA ČR

Kontrolní činnost Dozorčí komise KA ČR v roce 2020

Kontrolní činnost Dozorčí komise KA ČR (dále „DK“) podléhá plánu kontrolní činnosti schváleného Radou pro veřejný dohled nad auditem (dále „RVDA“). Dozorčí komise v roce 2020 pracovala v plném počtu jedenácti členů. Od 1. ledna 2020 je členem DK Milan Pašek, který ve funkci nahradil Lenku Bízovou, která k 4. prosinci 2019 odstoupila z pracovních důvodů.

Pro plnění svých povinností dle § 35 odst. 1 zákona o auditorech měla DK v roce 2020 k dispozici sedm kontrolorů kvality a jednu asistentku (zaměstnance oddělení kontroly kvality auditorské činnosti – dále „OKK“).

Systém provádění souhrnných kontrol, kontrol dodržování členských povinností a mimořádných kontrol kvality auditorské činnosti je, v souladu s § 24, odst. 4 zákona o auditorech, nastaven tak, aby bylo zajištěno provedení kontroly kvality u auditorů, kteří neprovádí povinný audit ani u jednoho subjektu veřejného zájmu, nejméně jednou za šest let.

Kontroly provádí členové DK spolu s kontrolory kvality (zaměstnanci z OKK). Souhrnné kontroly a mimořádné kontroly kvality jsou vykonávány ve většině případů dvoučlenným týmem, který je zpravidla tvořen jedním zaměstnancem z OKK a jedním členem DK. Kontroly kvality u auditorů OSVČ a auditorských společností, které provádějí auditorskou činnost v menším rozsahu, a kontroly dodržování členských povinností jsou vykonávány pouze kontrolory kvality z OKK. Kontroly prováděné u větších společností jsou časově náročnější a jsou prováděny vícečlennou kontrolní skupinou.

Kontroly provedené v roce 2020

Na rok 2020 bylo naplánováno celkem 238 kontrol (tj. souhrnných kontrol, kontrol dodržování členských povinností dle § 2 b) a c) Dozorčího řádu a mimořádných kontrol kvality), z čehož bylo následně provedeno 192 kontrol a 46 kontrol nebylo realizováno.

Důvodem neprovedených kontrol byly buď vážné zdravotní důvody auditora, či v několika málo případech i žádost o zánik oprávnění auditora před datem zahájení kontroly. Další část kontrol nebyla realizována z důvodu vyhlášení nouzového stavu vládou ČR a zdravotních komplikací auditora souvisejících s infekcí covid-19.

Neprovedené kontroly byly přeřazeny na následující plánované období, tj. na rok 2021.

Počet kontrol provedených v letech 2016–2020

	2016	2017	2018	2019	2020
Naplánováno	250	222	231	266	238
Provedeno	231	201	194	241	192
Neprovedeno	19	21	37	25	46

Z celkového počtu 192 kontrol provedených v roce 2020 bylo uskutečněno 189 souhrnných kontrol a 3 kontroly dodržování členských povinností (91 kontrol bylo realizováno u auditorských společností a 101 kontrol bylo provedeno u auditorů samostatně činných). Nebyla provedena žádná mimořádná kontrola kvality.

V roce 2020 bylo nově, vzhledem k vyhlášení nouzového stavu vládou ČR a z důvodu výskytu epidemie covid-19, auditorům nabízeno provedení kontroly „na dálku“, tedy korespondenčním způsobem. Takto byl postupně zaveden institut distančních kontrol, který byl nejprve realizován zejména u těch auditorů a auditorských společností, kteří vedou své spisy v elektronické formě a mohli kontrolní skupině poskytnout kompletní elektronický spis. Následně byly distanční kontroly rozšířeny i o skupinu auditorů, kteří vedou spis v papírové formě a zajistili jejich doručení do prostor KA ČR.

Distančním způsobem bylo v roce 2020 provedeno celkem 40 kontrol, což je 21 % z celkového počtu realizovaných kontrol.

Hodnocení výsledků provedených kontrol v roce 2020

Výsledky provedených kontrol hodnotí DK v souladu s Dozorčím řádem na svých zasedáních, která jsou zpravidla jednou za měsíc. Výsledné hodnocení každé kontroly u auditora či auditorské společnosti podléhá v DK schvalovacímu procesu, jehož výsledkem je i určení časové periody provedení příští kontroly. Toto hodnocení může v návaznosti na výsledky kontrolní činnosti u auditora vyústit i v návrh DK na zahájení kárného řízení.

Výsledné hodnocení nevylučuje provedení mimořádné kontroly kvality v dřívějším termínu.

Z celkového počtu 200 ukončených kontrol bylo u 28 zkontrolovaných subjektů schváleno provedení příští kontroly v zákonem stanovené šestileté lhůtě. U 72 zkontrolovaných subjektů bylo z důvodu zjištění méně závažných nedostatků schváleno provedení následné kontroly v mírně zkrácené periodě a u 100 zkontrolovaných subjektů bylo vzhledem ke zjištěným nedostatkům opakování kontroly naplánováno ve zkrácené lhůtě 2–3 let. Toto opakování kontroly v krátkém časovém horizontu bylo schváleno u 57 auditorských společností a 43 auditorů OSVČ.

Počet kontrol ukončených v letech 2016–2020 dle hodnocení kontrol

	2016	2017	2018	2019	2020
Opakování kontroly v zákonné lhůtě	34	38	41	33	28
Opakování kontroly po 4 až 5 letech	79	56	58	92	72
Opakování kontroly v kratším čase	133	109	94	96	100
Celkem ukončených kontrol	246	203	193	221	200

K opakovaným kontrolám v kratší časové lhůtě je přistupováno v případech, kdy je shledána nekvalita provedeného auditu či zjištěn nedostatek alespoň v jedné z prověřovaných oblastí (ISA, Etický kodex či ISQC 1). Pokud je zjištěna významná chyba či významná nekvalita provedeného auditu nebo porušení zákona o auditorech, je ze strany DK podán návrh na zahájení kárného řízení.

Častým důvodem pro podání návrhu na zahájení kárného řízení jsou také opakované nedostatky v auditorských spisech, zjišťované při provádění následných kontrol kvality.

Z celkového počtu 200 ukončených kontrol bylo na jednotlivých zasedáních DK v roce 2020 38 kontrol ukončeno podáním návrhu DK na zahájení kárného řízení. V procentním vyjádření se jedná o 19 % kontrol ukončených v tomto období. V porovnání s předchozím obdobím došlo ke snížení počtu podaných návrhů na zahájení kárného řízení, neboť v roce 2019 bylo z celkového počtu 221 uzavřených kontrol 60 kontrol ukončeno podáním návrhu na zahájení kárného řízení (tj. 27,1 % ukončených kontrol).

Návrhy na zahájení kárného řízení v letech 2016–2020:

	2016	2017	2018	2019	2020
Počet návrhů na zahájení kárného řízení	50	28	24	60	38
Počet uzavřených kontrol v jednotlivých letech	246	203	193	221	200
Podíl návrhů na kárné řízení z celkového počtu kontrol	20,3 %	13,8 %	12,4 %	27,1 %	19 %

Nedostatky zjišťované v rámci kontrolní činnosti

V rámci prováděných kontrol je stále větší pozornost věnována prověřování plnění vybraných povinností dle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti.

U souhrnných kontrol je ověřováno:

- plnění povinnosti identifikace osoby, účastníka obchodu v hodnotě převyšující částku 1 000 EUR,
- plnění oznamovací povinnosti povinné osoby dle § 18 zákona č. 253/2008 Sb.,
- zajištění proškolení zaměstnanců dle § 23 zákona č. 253/2008 Sb.

V těchto kontrolovaných oblastech jsou shledávána dílčí pochybení, jako například:

Společnost dle § 23 zákona č. 253/2008 Sb. zajistila proškolení zaměstnanců v této oblasti. Toto školení je v auditorské společnosti realizováno každý rok. Poslední školení proběhlo v září roku 2020, ale společnost nemá dokumentaci o proškolení. Případně ze školení byl pořízen záznam obsahující osnovu školení, ale v obsahové náplni chybí typologie a znaky podezřelých obchodů. Toto je nutné do obsahu proškolení zaměstnanců doplnit.

Auditor provedl identifikaci klienta, ale jeho dokumentace neobsahovala všechny povinné údaje o identifikaci dle § 8, odst. 2 zákona č. 253/2008 Sb., které ověřil z průkazu totožnosti. (Těmito údaji jsou jméno, příjmení, datum narození, bydliště, pohlaví, orgán, který průkaz totožnosti vydal a doba jeho platnosti).

Nedostatky v dodržování ISA

Složení nejčastějších nedostatků v dodržování ISA zjištěných při kontrolách provedených v roce 2020 je téměř shodné se skladbou nejčastějších nedostatků, které byly zjištěny v předchozích letech a byly již opakovaně publikovány. Kromě nich jsme zaznamenali nedostatky nové a četností narůstající, a to v oblastech:

a) Kontrola ÚZ před jejím zveřejněním (ISA 330, ISA 700), relativně častým nedostatkem bývá to, že auditor nezkontroluje konečnou verzi účetní závěrky před jejím zveřejněním, zvláště pak informace uvedené v příloze ÚZ.

b) Přezkoumání hospodaření (AS 52), nejčastějším nedostatkem zjišťovaným při kontrole přezkumných zakázek bývá nedostatečná dokumentace postupů (testů) k jednotlivým dílčím předmětům přezkoumání uvedeným v § 2 zákona č. 420/2004 Sb., o přezkoumávání hospodaření územních samosprávných celků a dobrovolných svazků obcí.

Zprávy auditora o výsledku přezkoumání hospodaření pak auditoři v některých případech nesestavují podle vzoru uvedeného v příloze č. 2 k AS 52 (zvláště do zpráv často uvádějí nadbytečné informace).

Závěrem alespoň tři hojně se opakující nedostatky zjišťované při prováděných kontrolách:

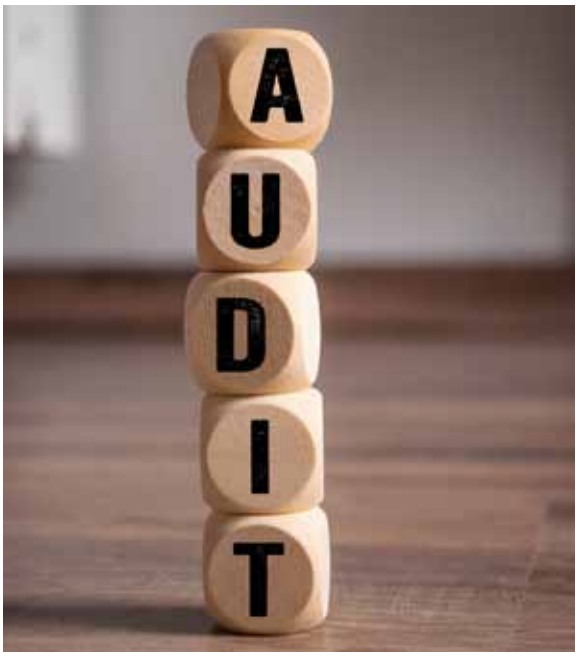
- ISA 330 (reakce na vyhodnocená rizika): V auditní dokumentaci často nebývá uvedeno, jaké auditor navrhl a provedl auditorské postupy v reakci na vyhodnocená rizika. Plánovaná reakce auditora na vyhodnocená rizika včetně dopadu na velikost testovaných vzorků by měla být obsažena již v plánu auditu a ve fázi realizace auditu by měly být navržené testy provedeny, vyhodnoceny a zdokumentovány.
- ISA 501 (důkazní informace): Auditoři také často nedostatečně dokumentují svou účast při fyzické inventuře zásob. Auditor je povinen (pokud jsou zásoby materiálně významné) získat dostatečné a vhodné důkazní informace o existenci a skutečném stavu zásob.

Při kontrolách kvality je častým zjištěním, že auditor deklaruje, že se fyzické inventury zásob zúčastnil, ale do svého spisu nezaznamená, kdy a jak vlastní inventura probíhala, jaké položky k přepočítání fyzického stavu vybral a zda inspekcí zásob byla prokázána nejen jejich existence, ale zhodnocen i jejich stav, a zda byly dodrženy pokyny vedení upravující postupy při fyzických inventurách.

Dále, pokud se datum inventury neshoduje s datem účetní závěrky, auditoři zapomínají, že je nutné otestovat pohyby mezi datem inventury a datem účetní závěrky.

- **ISA 540 (audit účetních odhadů):** Dle ISA 540.15 je auditor povinen u účetních odhadů způsobujících významná rizika, vedle testů věcné správnosti dle ISA 330, také posoudit, jak vedení zvážilo alternativní předpoklady nebo výsledky a proč je odmítlo, nebo jak jinak vedení řešilo nejistotu stanoveného účetního odhadu a zda jsou významné předpoklady použité vedením přiměřené. Dále dle ISA 540.23 je auditor povinen do dokumentace auditu uvést podklady pro závěry auditora o přiměřenosti účetních odhadů a jejich zveřejnění. Dokumentace testů, týkajících se specificky účetních odhadů, je ale ve spisech auditorů poskrovnu.

Petra Fridrichová
vedoucí oddělení kontroly kvality
auditorské činnosti KA ČR



Dozorčí komise upozorňuje na povinnost auditora zjišťovat skutečného majitele

Povinnost auditora zjišťovat skutečného majitele, která platí již nyní dle zákona 253/2008 Sb., bude od 1. června 2021 posílena další právní úpravou (§ 8 a 16 zákona č. 37/2021) a rozšířena o další povinnosti auditora (§ 15a zákona č. 253/2008 Sb.). Pokud auditor při provádění identifikace nebo kontroly klienta bude mít důvodně za to, že zjistil nesrovnalost podle zákona upravujícího evidenci skutečných majitelů (dále jen „nesrovnalost"), je povinen upozornit na to klienta, přičemž uvede, v čem nesrovnalost spatřuje. Pokud klient bez zbytečného odkladu nesrovnalosti neodstraní či nevyvrátí, musí auditor ohlásit nesrovnalost soudu, který je příslušný k řízení o nesrovnalosti podle zákona upravujícího evidenci skutečných majitelů. Obsahem podání musí být oznámení o zjištění nesrovnalosti spolu s doložením skutečnostmi nebo písemnostmi, které nesrovnalost osvědčují, a vyjádření klienta, pokud jej učinil.

Orgánem, který kontroluje dodržování těchto povinností, je dle § 35 odst. 1 zákona o auditorech dozorčí komise. Při zjištění přestupku v oblasti AML bude dozorčí komise postupovat dle zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich tzn. postoupí kárné komisi oznámení o přestupku a s auditorem bude vedeno řízení.

Tomuto tématu bude věnováno šesté číslo časopisu Auditor, které vyjde koncem června.

Petra Fridrichová
vedoucí oddělení kontroly kvality
auditorské činnosti KA ČR

Doporučení KA ČR k ESEF

Výbor pro metodiku auditu KA ČR vydal doporučení pro vyjadřování auditora o souladu s požadavky nařízení o ESEF (jednotný elektronický formát pro podávání zpráv) včetně XBRL značkování.

Doporučení se zaměřuje na umístění vyjádření auditora o souladu s nařízením ESEF ve zprávě auditora, charakter posuzování (typ ověřovací zakázky) souladu s ustanoveními nařízení o ESEF, na postup auditora při vydávání zprávy auditora a na problematiku vydávání dalších verzí výročních zpráv. Dále doporučení obsahuje ilustrativní příklady zpráv auditora ke konsolidované účetní závěrce.

Doporučení naleznete na stránkách komory v sekci metodické pomůcky – audit účetní závěrky.

oddělení metodiky KA ČR

Editorial

Žijeme v době nových možností informačních a komunikačních technologií. A stejně jako u jiných technických vynálezů v minulosti si nejprve užíváme výhod, které nové technologie přinášejí, a teprve se zpožděním si začneme uvědomovat nová rizika, která přinášejí. Teprve když zažijeme negativní důsledky takových rizik, začneme se učit proti nim bojovat. ICT a jejich rozvoj je specifický svou složitostí, rychlostí a rozsahem, s jakým zasahuje prakticky všechny oblasti našeho života. Počítače nemáme jen na pracovním stole nebo v podobě mobilu, ale dnes už také v televizi, ledničce, pračce nebo svém robotickém vysavači či centrální jednotce, která ovládá světla, topení a klimatizaci našeho bytu. Co je však ještě závažnější, počítače řídí telekomunikační zařízení, výrobní procesy, bankovní systémy, dopravu a také zdravotnické přístroje a systémy v nemocnicích. Napadení jakéhokoliv z těchto systémů se může ve svých důsledcích podobat válečnému napadení, a proto je nutno se kybernetickou bezpečností zabývat nejen z hlediska možných ekonomických ztrát jednotlivých firem, ale také uvažovat o rizicích napadení kritických informačních systémů na úrovni celého státu a tím ohrožení jeho národní bezpečnosti. Vše, co jsem výše zmínil, se samozřejmě týká i auditorů, a to jak s ohledem na jejich posuzování vnitřních kontrolních systémů a rizik u jejich klientů, tak i rizik jejich vlastních počítačových systémů v auditorských firmách. Další nový rozměr problematika kybernetické bezpečnosti dostala v souvislosti s omezeními pohybu osob v důsledku boje proti koronaviru, kdy došlo k ještě rychlejšímu rozvoji digitální výměny dokumentů, práce na dálku, online jednání a výuky apod. V řadě ohledů všechny tyto novinky přináší nová rizika, která je nutno řešit. Z uvedených důvodů jsme toto číslo časopisu Auditor věnovali právě kybernetické bezpečnosti.

V prvním článku jsem se pokusil o encyklopedický přehled škodlivého software a jeho forem, který čtenáře provede historií malware od prvních virů až po současné formy vyděračského software. Na úvodní článek navazuje Oto Křivanec a Tomáš Matějíček nejprve příspěvkem o motivaci kybernetické kriminality a základních pravidlech obrany proti ní. Tomáš Matějíček pak pokračuje popisem toho, jak probíhá typický kybernetický útok, a tento úvodní blok uzavírá článek shrnující právní předpisy v oblasti kybernetické bezpečnosti a jmenovitě pak zákon o kybernetické bezpečnosti. V druhém bloku jsme dali prostor dvěma odborníkům, kteří se zabývají kybernetickou bezpečností ve svých funkcích, a to Janu Humlovi a Janu Kloudovi. Položil jsem jim oběma nezávisle deset stejných otázek (témat) z oblasti kybernetické bezpečnosti a věřím, že pro vás bude zajímavé porovnat, v čem se jejich názory shodují či liší. Za třetí ucelenou část tohoto čísla pak považuji článek Michala Wojnara a Petra Šimsy, který je stručným průvodcem tím, jak se zabývat kybernetickou bezpečností z pohledu auditora u jeho klientů. Téma čísla pak uzavírají dva rozhovory – s Monikou Zahálkovou, která je výkonnou ředitelkou České bankovní asociace, a Markem Richterem, který vede oddělení auditu finančních institucí v PwC. Oběma jsem kladl i otázky související s kybernetickou bezpečností.

Uvědomuji si, že by se mohlo někomu zdát, že toto číslo vybočuje poněkud z řady témat zabývající se otázkami z oblasti práva, daní, účetnictví a auditu, ale věřím, že se jedná o námět pro auditory aktuální a důležitý. Vždyt kybernetický útok na benešovskou nemocnici začal tím, že někdo v ní kliknul na fakturu v příloze e-mailu, která byla ve skutečnosti virem, a ten umožnil útočníkům proniknout dovnitř počítačové sítě nemocnice a prolomit administrátorská hesla, což vše skončilo výpadkem provozu nemocnice s odhadovanou škodou 40 mil. korun. Věřím, že vám téma a články tohoto čísla časopisu přinesou dostatek informací o nebezpečnosti kybernetické kriminality a možnostech ochrany proti ní, abyste tato rizika minimalizovali jak ve svých auditorských firmách, tak je rozpoznali u svých klientů. Zpětnou vazbu k vašim znalostem z oblasti kybernetické bezpečnosti vám poskytne i závěrečný test, který si můžete zkusit udělat i elektronicky a já vás ubezpečuji, že se nejedná o sofistikovaný kybernetický útok využívající psychologický moment vaší zvědavosti a soutěživosti.

Ladislav Mejzlík
editor tohoto čísla

Co byste měli vědět o malware

Ladislav Mejzlík

Malware je obecným názvem pro velké množství nejrůznějších programů, jejichž škodlivost je dána spíše záměrem autora programu než jeho vlastnostmi, protože malware nemusí způsobovat přímou škodu (může například jen zabírat místo nebo čas uživatele počítače), ale do počítače byl nainstalován bez vědomého souhlasu uživatele. Proto by jako malware neměl být označován software, který sice obsahuje chyby (a ty mohou způsobit škodu), ale byl napsán pro legitimní účely a uživatel vědomě souhlasil s jeho instalací.

Malware byl a je vytvářen z různých důvodů. Zpočátku tyto programy vznikaly jako experiment nebo žert a většinou bez záměru způsobit nějakou škodu, případně měly pouze uživatele obtěžovat. U tvůrců malware se často objevuje i touha sobě (nebo jiným) dokázat, že něco takového dovedou. S postupem času se však malware dostal do oblasti počítačové kriminality a stal se nejen nástrojem šedé ekonomiky na vydělávání peněz (např. vyděračský ransomware), ale i formou vydírání, pomsty nebo zbraně v konkurenčním nebo politickém boji nejen mezi firmami, ale i státy.

I když jsou mezi jednotlivými druhy malware jasné rozdíly, tak se často různě míchají a zaměňují nebo považují za synonyma. Typické je zaměňování počítačových virů a červů. Rozdíl mezi virem a červem je v tom, že virus potřebuje k fungování jiný spustitelný program, který napadá a prostřednictvím kterého se replikuje. Naproti tomu červ je spíše způsob šíření malware, který je soběstačný a může se sám spouštět, kopírovat a odesílat kopie sebe sama prostřednictvím e-mailů. Tyto dva způsoby je možné kombinovat, takže některé z nejnebezpečnějších počítačových virů jsou ve skutečnosti červi.

Milníky v historii malware

Creeper byl experimentální počítačový program napsaný Bobem Thomasem v BBN v roce 1971. Jeho původní verze byla navržena pro pohyb mezi sálovými počítači DEC PDP-10, na kterých se používal operační systém TENEX, a to pomocí sítě ARPANET. Tato samoreplikující se verze Creeperu je obecně považována za historicky první počítačový virus. Program nebyl aktivně škodlivým softwarem, protože nezpůsobil žádné poškození dat. To jediné co dělal, bylo, že se na monitoru objevila zpráva: „Jsem Creeper: chyťte mě, pokud to dokážete“. Reakcí na Creeper byl podobný program **Reaper** vytvořený v roce 1972 Rayem Tomlinsonem pro pohyb po síti ARPANET, jehož úkolem bylo naopak odstranění samoreplikujícího se Creepera.

Malware (složení anglických slov **mal**icious a soft**ware**) je v informatice označení pro škodlivé programy, které v počítači provádí činnost, se kterou by uživatel nesouhlasil, kdyby o jeho skutečných záměrech věděl.

První skutečný vir, který mohl nějak uškodit, naprogramovali v roce 1986 bratři Basid a Amjad Farooq Alvi z Pakistánu a pojmenovali jej **Brain** (mozek). Objevil se 19. ledna 1986. Útočil na spouštěcí sektor disket, čímž zabránil spuštění operačního systému z nich, čímž na tehdejších počítačích způsobil relativně rozsáhlé škody. Tím fakticky odstartovala éra virů, které se od té doby dále rozvíjely.

Morrisův červ byl první počítačový červ, který ke svému šíření využíval internet. Byl vytvořen tehdy 23letým studentem Cornellovy univerzity Robertem Tappanem Morrisem a vypuštěn 2. listopadu 1988 prostřednictvím počítače MIT. Morris byl prvním člověkem obviněným v USA z porušení zákona o zneužívání výpočetní techniky a s ní spojených podvodech (Computer Fraud and Abuse Act z roku 1986). Byl odsouzen k tříletému podmíněnému trestu, 400 hodinám veřejně prospěšných prací a pokutě ve výši 10 tis. dolarů, Podle slov autora nebyl červ vytvořen pro destruktivní účely, ale jako nástroj pro změření počtu počítačů připojených k internetu. V současnosti je Robert Morris respektovaným informatikem a docentem na MIT.

Zdrojový kód Morrisova červa v muzeu

Éra **ransomware** (z anglického *ransom* – výkupné) byla zahájena v roce 2013 virem CryptoLocker. CryptoLocker infikoval v původní verzi asi půl milionu počítačů ve 150 zemích. Některé z jeho klonů, například TorrentLocker nebo CryptoWall, byly speciálně navrženy pro cílení na počítače v Austrálii.

WannaCry (také WannaCrypt, WanaCrypt0r, Wanna Decryptor) je ransomware (vyděračský software) napadající počítače se systémem Microsoft Windows. Jeho útoky od pátku 12. května 2017 až do současnosti jsou považovány za nejničivější a nejagresivnější svého druhu. WannaCry po nakažení počítače zašifruje data na pevném disku a žádá platbu 300 dolarů v Bitcoinech na odblokování souborů (po vypršení lhůty pro zaplacení výpalného se jeho cena zvýší až na 2 000 dolarů). Většina typů ransomwaru se do počítače dostane e-mailem, prostřednictvím kliknutí na odkaz nebo reklamami.

Malware WannaCry má obrovský dopad nejen na osobní počítače soukromých uživatelů, ale nakazil například Národní zdravotnickou službu (NHS) ve Spojeném království, takže musely být zrušeny mnohé naplánované operace. Virus způsobil i několik hodin dlouhou odstávku mobilní sítě O2 Telefónica ve Španělsku, taktéž i problémy s dopravou, když byly napadeny železniční počítače Deutsche Bahn a aerolinky LATAM Airlines. Mezi další významné firmy napadené virem WannaCry patří Renault, FedEx nebo Sberbank. Virus byl zaznamenán i na Slovensku, kde zasáhl Fakultní nemocnici v Nitře a v ČR nemocnici v Benešově, ostravskou a olomouckou fakultní nemocnici nebo Karlovarskou krajskou nemocnici.

Deset virů, které způsobily největší škody[1]

1. Mydoom – 38 mld. dolarů

Tento malware, známý také jako Novarg, je technicky vzato červ šířený hromadnými e-maily, které v okamžiku jeho největšího šíření představovaly 25 % všech na světě odeslaných e-mailů. Mydoom vyhledal v infikovaných počítačích všechny e-mailové adresy, na které odeslal své kopie. Navíc napadené počítače propojil do sítě nazývané botnet, které prováděly distribuované útoky (DDoS) na cílové weby nebo servery. Mydoom stále existuje a generuje cca 1 % všech phishingových e-mailů, což není málo vzhledem k 3,4 miliardám phishingových e-mailů odeslaných každý den. Ačkoli byla vypsána odměna 250 tis. dolarů, vývojář tohoto počítačového červa nebyl nikdy dopaden.

2. Sobig – 30 mld. dolarů

Počítačový virus Sobig z roku 2003 měl v rychlém sledu několik verzí pojmenovaných Sobig.A až Sobig.F, přičemž Sobig.F byl nejškodlivější. Tento malware se vydával za legitimní počítačový software v příloze e-mailům. Autor červa nebyl nikdy dopaden.

3. Klez – 19,8 mld. dolarů

Klez infikoval v roce 2001 přibližně 7,2 % všech tehdy existujících počítačů, (cca 7 milionů). Klez odesílal falešné e-maily s vymyšleným jménem odesílatele a kopíroval se a šířil po síti každé oběti. Virus přežíval po celá léta a každá jeho verze byla destruktivnější než ta předchozí.

4. ILOVEYOU – 15 mld. dolarů

Virus ILOVEYOU z roku 2000 byl založen na rozesílání falešného „milostného" dopisu v e-mailu s přílohou, která vypadala jako neškodný textový soubor. Stejně jako Mydoom i tento červ zasílal své kopie na každou e-mailovou adresu ze seznamu kontaktů infikovaného počítače. Krátce po jeho vypuštění 4. května 2000 se rozšířil na více než 10 milionů počítačů. Virus vytvořil vysokoškolský student na Filipínách jménem Onel de Guzman, který prostřednictvím něj chtěl ukrást hesla, aby se mohl zdarma přihlásit k online službám, které chtěl použít. Vzhledem k absenci zákonů týkajících se kybernetické kriminality byl propuštěn.

5. WannaCry – 4 mld. dolarů

WannaCry z roku 2017 je ransomware, který převezme kontrolu nad počítačem a drží jej jako rukojmí. WannaCry pronikl do 200 000 počítačů ve 150 zemích a způsobil obrovské ztráty, protože podniky, nemocnice a vládní organizace byly vyřazeny z provozu, musely zaplatit výkupné či složitě obnovovat své systémy od nuly. V září 2020 zasáhl WannaCry americký řetězec nemocnic Universal Health Services, který má více než 400 poboček. Jednalo se údajně o největší počítačový útok v historii, který si vynutil přerušení zdravotní péče včetně zrušení operací a nouzový provoz nemocnic prostřednictvím papírových záznamů.

6. Zeus – 3 mld. dolarů

Počítačový virus Zeus byl vypuštěn v roce 2007 a o tři roky později představoval podle odhadů 44 % veškerého bankovního malware. Virem bylo v té době zasaženo 88 % všech společností z žebříčku Fortune 500, celkem 2 500 organizací a 76 000 počítačů ve 196 zemích. Botnet Zeus byla skupina programů, které společně pracovaly na ovládnutí počítačů tak, aby mohly být společně řízeny. V roce 2010 bylo zatčeno více než 100 členů zločinecké skupiny, která stála za vznikem a šířením viru.

7. Code Red – 2,4 mld. dolarů

Počítačový virus Code Red, který byl poprvé zpozorován v roce 2001, byl dalším červem, který pronikl do 975 000 hostitelů. Zobrazoval slova „Hacked by Chinese!" napříč infikovanými webovými stránkami a běžel zcela v paměti každého stroje. Ve většině případů nezanechal žádné stopy na pevných discích ani jiných úložištích. Napadl weby infikovaných počítačů a pak zaútočil na web amerického Bílého domu www.whitehouse.gov způsobem zvaným DDoS (distributed denial of service). Bílý dům musel změnit svoji IP adresu, aby se proti Cod Red ubránil.

8. Slammer – 1,2 mld. dolarů

Červ SQL Slammer stál v roce 2003 odhadem 750 milionů dolarů a napadl 200 000 uživatelů. IP adresy vybíral náhodně a pak se odesílal na další počítače. Svoje oběti použil k zahájení DDoS útoku na několik internetových hostitelů, což výrazně zpomalilo internetový provoz. Červ Slammer zasáhl hlavně banky v USA a Kanadě a na mnoha místech vyřadil bankomaty z povozu. Zákazníci torontské Imperial Bank of Commerce zjistili, že nemají přístup k finančním prostředkům. Útok se opakoval v roce 2016, kdy se šířil z IP adres na Ukrajině, v Číně a v Mexiku.

9. CryptoLocker – 665 mil. dolarů

CryptoLocker je ransomware z roku 2013, který během čtyř let napadl více než 250 tis. počítačů a zašifroval jim soubory. Na napadených počítačích se zobrazila červená zpráva se žádostí o výkupné a informacemi o tom, jak jej zaplatit.

10. Sasser – 500 mil. dolarů

Sasserův červ napsal 17letý německý student informatiky Sven Jaschan, který byl zatčen v roce 2004 na základě vypsané odměny 250 tis. dolarů a který byl zřejmě autorem dalších virů (například Netsky.AC). Odsouzen byl pouze k podmíněnému trestu, protože byl v době napsání malware nezletilý.

[1] Zdroj: Gerencer, T.: The Top 10 Worst Computer Viruses in History, online, Hewlett Packard 2020.

Glosář typů malware a hackerských útoků

Typ malware	Charakteristika
Virus	Jako virus se v oblasti počítačové bezpečnosti označuje program, který se dokáže šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Zatímco některé viry mohou být cíleně ničivé (např. mažou soubory na disku), mnoho jiných virů je relativně neškodných, příp. pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba. Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji. Některé viry mohou být takzvaně polymorfní (každý „potomek" se odlišuje od svého „rodiče").
Červ (worm)	Počítačový červ je v informatice specifický program, který je schopen automatického rozesílání kopií sebe sama na jiné počítače. Poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a využívá je ke svému vlastnímu šíření. Kromě svého vlastního šíření, které má rozhodující vliv na úspěšnost červa, vykonává obvykle tento program v počítači nějakou sekundární činnost, která je červem nesena jako „náklad" (kód, který tvoří náklad, se nazývá anglicky payload).
Trojský kůň (trojan horse)	Trojský kůň je uživateli skrytá část programu nebo aplikace s funkcí, se kterou uživatel nesouhlasí (typicky je to činnost škodlivá). Název pochází z antického příběhu o dobytí Tróje. Trojský kůň může být samostatný program, který se tváří užitečně – například hra, spořič obrazovky nebo nějaký jednoduchý nástroj. Někdy se trojský kůň vydává za program k odstraňování malware (dokonce i jako takový může fungovat a odstraňovat konkurenční malware). Tato funkčnost slouží ale pouze jako maskování záškodnické činnosti, kterou v sobě ukrývá.
Spyware	Spyware (nebo také špehovací software, špionážní software) je program, který využívá internetové stránky k odesílání dat z počítače (či mobilního telefonu nebo jiného zařízení) bez vědomí jeho uživatele. Někteří autoři spyware se hájí, že jejich program odesílá pouze data typu přehled navštívených stránek či nainstalovaných programů za účelem zjištění potřeb nebo zájmů uživatele a tyto informace využívá pro cílenou reklamu. Existuje ale i spyware odesílající hesla a čísla kreditních karet nebo spyware fungující jako zadní vrátka. Protože lze jen těžko poznat, do které skupiny program patří, a vzhledem k postoji k reklamě řada uživatelů nesouhlasí s existencí a legálností jakéhokoliv spyware. Spyware se často šíří jako součást shareware, a to jako adware nebo bez vědomí uživatelů (ale s vědomím autorů programu). Jakmile si takový program nainstalujete a spustíte, nainstaluje se do systému také spyware. Často se to týká například klientských programů pro peer to peer sítě umožňující stahování hudby a videa od ostatních uživatelů.
Ransomware	Ransomware (nebo také vyděračský software, vyděračský program) je složením anglických slov ransom (výkupné) a software. Jedná se o druh škodlivého programu, který blokuje počítačový systém nebo šifruje data v něm zapsaná a pak požaduje od oběti výkupné za obnovení přístupu. Některé formy ransomware šifrují soubory na pevném disku (kryptovirální vydírání), jiné jen zamknou systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení.
Adware	Adware (z angl. reklamní software, zkratka advertising-supported software) je označení pro produkty znepříjemňující práci nějakou reklamní aplikací. Ty mohou mít různou úroveň agresivity – od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti. Další nepříjemností může být např. změna domovské stránky v internetovém prohlížeči, aniž by o to uživatel měl zájem. Většinou ale nejsou tyto programy přímo nebezpečné jako spyware a bývají spojeny s nějakým programem, který je zadarmo. To se dělá z důvodu toho, že díky těmto reklamám mohou vývojáři financovat dál svůj program. Nebo když se jedná o placený produkt, může se díky těmto reklamám prodávat program se slevou. Některé produkty nabízejí uživateli za poplatek možnost reklamy odstranit. Řada lidí si plete pojmy spyware a adware.
Crimeware	Crimeware je v informatice název pro druh malwaru, který je vytvořen pro automatizaci počítačové trestné činnosti. Crimeware (na rozdíl od spyware a adware) je určen k páchání krádeží identity prostřednictvím sociálního inženýrství nebo k získání přístupů k různým placeným službám a bankovním účtům uživatele za účelem provádění neoprávněných transakcí a využívání uživatelových finančních prostředků k obohacení kyberútočníka. Crimeware může také případně ukrást a zneužít citlivá a důvěrná firemní data. Představuje rostoucí hrozbu v zabezpečení sítě, jelikož mnoho škodlivého kódu je zaměřeno právě na krádeže důvěrných informací. Za crimeware je tedy možné považovat všechny softwarové nástroje kyberzločinců, které jim usnadňují útoky a zefektivňují jejich provádění a zároveň se zaměřují zejména na finanční zisk nebo krádež citlivých informací. Crimeware často provádí (ro)boti, kteří automatizovaně provádějí útoky na uživatele ku prospěchu útočníka.

Typ malware	Charakteristika
Backdoor	Zadní vrátka (anglicky backdoor) je v informatice název metody, která umožňuje obejít běžnou autentizaci, která za běžných okolností brání uživateli v neoprávněném využívání počítačového systému. Pokud jsou zadní vrátka v softwaru či hardwaru zabudována, mohou být využívána i k seriózním účelům (např. univerzální heslo pro servisní přístup), avšak často jsou zneužívána, takže jsou klasifikována jako bezpečnostní riziko, resp. zranitelnost. Nemohou totiž být bezpečná, ale přesto o jejich implementaci usilují také například vlády.
Rootkit	Rootkit je sada počítačových programů, pomocí kterých lze maskovat přítomnost zákeřného softwaru v počítači, například přítomnost virů, trojských koní, spywaru a podobně. Rootkit maskuje přítomnost zákeřných programů skrýváním adresářů, v nichž jsou instalovány, volání API, položek registru Windows, procesů, síťových spojení a systémových služeb tak, aby přítomnost zákeřného softwaru nebyla běžně dostupnými systémovými prostředky odhalitelná. Tyto programy umožňují skrývat běžící procesy, soubory a systémové údaje, takže pomáhají útočníkovi zůstat skrytý (upravují operační systém tak, aby nebyly běžnými prostředky uživatele zjistitelné). Rootkity existují pro mnoho operačních systémů.
Keylogger	Keylogger (někdy také Keystroke Logger) je software, který snímá stisky jednotlivých kláves. Antivirem bývá považován za virus. V případě software se jedná o určitou formu spyware, ale existují i hardwarové keyloggery. Keylogger neohrožuje přímo počítač, ale slouží ke zjišťování hesel jiných lidí. Některé z nich bývají v operačním systému Microsoft Windows proti svému zničení chráněny pomocí Archivace a Skrytí souborů, takže je není možné pomocí Průzkumníku najít (je nutné použít vyhledávání).
Phishing	Phishing (někdy převáděno do češtiny jako rhybaření) je podvodná technika používaná na internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. Je příkladem techniky sociálního inženýrství používané k oklamání uživatelů za využití slabých míst současných bezpečnostních technologií (jejich implementací). K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů, úřadů státní správy nebo od IT administrátorů. Principem phishingu je typicky rozesílání e-mailových zpráv nebo instant messages, které často vyzývají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s tou oficiální. Stránka může například napodobovat přihlašovací okno internetového bankovnictví nebo e-mailové schránky. Uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří je mohou zneužít (např. mu z účtu ukrást peníze nebo z jeho e-mailu rozesílat další podvodné e-maily). Obdobně může prozradit jiné citlivé (osobní) údaje, které pak útočníci mohou zneužít (např. vzít si půjčku na jméno oběti).
Hacking	Hacking je záměrná změna běžného chování počítače a připojených systémů. Obvykle je prováděn pomocí skriptů nebo programů, které manipulují s přenášenými daty s cílem získat přístup k informacím ze systému. Hackeři napadají počítače pomocí virů, červů, trojských koní, ransomware, rootkitů nebo neautorizovanými změnami v nastavení DNS serverů nebo útoků na ně tak, aby je vyřadily z provozu, případně využívají chyb a bezpečnostních děr v operačním systému a legálních programech instalovaných na počítači uživatelem. Hackerské skripty si často může na internetu kdokoli volně stáhnout a podle své potřeby upravit. Trpělivý a dobře motivovaný člověk se dokáže naučit tyto skripty využívat a může se pokusit získat například vaše osobní údaje, včetně přihlašovacích údajů do vašeho e-mailu, banky nebo jiných přístupových údajů.
Útoky na DNS	První skupinu tvoří Denial of Service (DoS) (česky odepření služby). Je to typ útoku na internetové služby nebo stránky, jehož cílem je danou službu znefunkčnit a znepřístupnit ostatním uživatelům; může k tomu dojít přehlcením požadavky či využitím nějaké chyby, která sice útočníkovi nedovolí službu ovládnout, ale umožní mu ji rozbít. Podtypem útoku DoS je tzv. Distributed Denial of Service (DDoS), při kterém je pro přehlcení cílové služby požadavky využito velké množství počítačů. Druhou možností je přímo úprava lokálních DNS záznamů nebo DNS údajů na serveru či napadení celého serveru, což je velmi nebezpečné, protože to může ohrozit velký počet uživatelů internetu.
Cookies	Jako cookie (anglicky koláček, oplatka, sušenka) se v protokolu HTTP označuje malé množství dat, která WWW server pošle prohlížeči a ten je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies nepředstavují žádné nebezpečí pro počítač jako takový. Přesto mohou být nebezpečné pro ochranu soukromí. Navštívený web si totiž může ukládat do cookies jakékoliv informace, které o návštěvníkovi zjistí, a může tak postupně zjišťovat zájmy konkrétního návštěvníka – které stránky navštěvuje, jaké informace vyhledává, jak často daný web navštěvuje apod. Těchto informací se dá posléze i bez vědomí návštěvníka využívat pro cílenou reklamu, statistické vyhodnocování chování návštěvníků apod. Cookies lze zneužít zejména tehdy, pokud útočník získá přístup k počítači uživatele, neboť cookies na počítači nejsou nijak chráněny. Pak lze předstírat např. cizí identitu.
Útok jako skrytý prostředník (Man-In-the-Middle)	Při tomto typu kybernetického útoku útočník tajně předává a případně mění komunikaci mezi dvěma stranami, které se domnívají, že spolu komunikují přímo a nezprostředkovaně. Jedním z příkladů útoku MITM je situace, při které útočník naváže nezávislá spojení s oběťmi a předává mezi nimi zprávy, aby se domnívaly, že mezi sebou mluví přímo prostřednictvím soukromého spojení, i když ve skutečnosti je celá konverzace řízena útočníkem. Útočník musí být schopen zachytit všechny relevantní zprávy předávané mezi oběma oběťmi a vkládat nové. To je za mnoha okolností jednoduché – například útočník v dosahu příjmu nešifrovaného přístupového bodu Wi-Fi se může vložit do komunikace s uživatelem jako man-in-the-middle a získat kontrolu nad připojením k WiFi a jeho obsahem.

Osm nejtypičtějších kybernetických útoků

Richard Clarke, bývalý odborník vlády Spojených států pro boj proti terorismu, jednou řekl: „Pokud utratíte více za kávu než za bezpečnost IT, budete hacknuti. A co víc, zasloužíte si být hacknuti." Pokud nechráníte sebe a své podnikání před počítačovou kriminalitou, je jen otázkou času, kdy se stanete obětí útoku. V roce 2015 činily celosvětové škody působené počítačovou kriminalitou 3 biliony dolarů. Prognózy říkají, že do roku 2021 se tato částka zdvojnásobí. Nejlepší způsob, jak se chránit, je vědět o různých typech kybernetických útoků. Poté můžete tyto informace použít a podniknout kroky k zajištění zabezpečení svých sítí.

Kybernetické útoky mohou mít různou podobu. Některé se zaměřují na lidský faktor uživatelů jako je nedbalost, nepozornost, fluktuace zaměstnanců nebo jiné lidské chyby. Jiné útoky se zaměřují spíše na bezpečnostní díry v samotných informačních systémech.

Toto je osm obvyklých typů kybernetických útoků (podle americké společnosti Alpine Security):

- útoky na prolomení hesla (Password Cracking Attacks),
- útoky s využitím sociálního inženýrství (Social Engineering Attacks),
- útoky na sociální média (Social Media Attacks),
- malwarové útoky (Malware attacks),
- útoky odmítnutí služby (Denial-of-Service Attacks),
- útok jako skrytý prostředník (Man-in-the-middle Attacks),
- odposlouchávání komunikace (Eavesdropping Attack, nebo Sniffing, či Dnooping Attack),
- útok prostřednictvím stahování (Drive-by Download Attack).

Kybernetické útoky v ČR

Prudký rozvoj informačních technologií doprovází podobně rychlý růst tzv. kyberkriminality. Zatímco v roce 2011 policie řešila 1 502 těchto trestných činů, v roce 2018 jich bylo již 5 654. Podle společnosti PwC se kybernetickým útokem v posledních letech setkala přibližně čtvrtina tuzemských firem.

Dušan Navrátil z Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) varoval před internetem věcí (IoT): „Útočit dnes může lednička, kávovar i plynoměr," řekl s tím, že velkým problémem jsou útoky na řízení technologických procesů. Monitorující a řídicí systémy výrobních technologií v průmyslu bývají zastaralé, a když se připojí na internet, případnému útoku se nedokážou ubránit. Takto se například v Německu před časem udál útok na vysokou pec, která v jeho důsledku vyhasla a zatuhla. Moderní technologie, automatizace a digitalizace dnes umožňují efektivnější správu celých budov, současně však využívání množství nejrůznějšího softwaru představuje pro tyto budovy stále větší riziko. Dnes hackeři už nejsou „geekové" v mikinách, hackerství se stává velkým byznysem. Nástroje pro kybernetické útoky se upgradují jako operační systémy a výkupné se platí anonymně v bitcoinech.

NÚKIB zveřejňuje každoročně na svých webových stránkách zprávu o stavu kybernetické bezpečnosti České republiky, ve které se můžete dočíst o nejvýznamnějších cílech kybernetických hrozeb a slabých místech, u kterých hrozí únik dat. Cílem zprávy je uceleně zhodnotit aktuální stav kybernetické bezpečnosti v naší zemi. Upozornit zejména na velké hrozby a jejich aktéry (zdroje), nejohroženější cíle a opatření k předcházení a reakci na kybernetické útoky a také na trendy, které odborníci sledují.

Oblíbeným cílem útoků v ČR (ale i v Evropě) se stávají nejen firmy, ale také zdravotnická zařízení. Podle informací bezpečnostních institucí takových útoků přibývá. V Česku v roce 2020 hackeři zaútočili například na nemocnici v Benešově, ostravskou a olomouckou fakultní nemocnici nebo Karlovarskou krajskou nemocnici.

Počátkem března 2021 došlo v ČR k rozsáhlému a sofistikovanému útoku na Microsoft Exchange servery, před kterým varovala jak společnost Microsoft, tak i NÚKIB a další bezpečnostní instituce a firmy, a informovala o tom široce i česká média. Útočníci při svém útoku řetězili čtyři různé zranitelnosti, čehož výsledkem byl přístup k obsahu e-mailových schránek a instalace malwaru zajišťujícího dlouhodobý přístup do prostředí napadené instituce. Podle Microsoftu za útokem s velkou mírou jistoty stojí Čínská APT skupina HAFNIUM, která operuje z VPS pronajatých v USA. V originálním blogpostu lze najít další technické podrobnosti a indikátory útoku. Jedním z cílů útoku se údajně stal i informační systém Ministerstva práce a sociálních věcí.

Ladislav Mejzlík

Doc. Ing. Ladislav Mejzlík, Ph.D., *absolvoval obor Ekonomické informace a kontrola na VŠE v Praze, kde pracoval na Katedře finančního účetnictví a auditingu v letech 2006–2014 jako vedoucí katedry. V letech 2014 a 2018 byl dvakrát zvolen děkanem Fakulty financí a účetnictví VŠE v Praze. Od roku 1993 je auditorem a v letech 2010–2014 byl dvakrát zvolen prvním viceprezidentem Komory auditorů ČR. V letech 2004–2010 zastupoval ČR v European Accounting Association a od roku 2004 zastupuje Fakultu financí a účetnictví VŠE v Praze v Národní účetní radě. Odborně se specializuje na oblast využití informačních a komunikačních technologií v účetnictví a auditingu a na regulaci a harmonizaci účetnictví v mezinárodním měřítku. Je členem poradní komise Ministerstva financí ČR pro účetnictví.*

Základní pravidla kybernetické bezpečnosti

Oto Křivanec

Tomáš Matějíček

Dnes prakticky každý používá telefon, počítač nebo jakékoliv chytré zařízení, které je připojeno k internetu. Denně prostřednictvím těchto zařízení sdílíme různá data o sobě, o firmě, kterou vlastníme nebo v ní pracujeme, o našich blízkých i kolezích. Jen menšina z nás ale přemýšlí o tom, jak moc jsou tato data zneužitelná. Měli bychom se zamyslet nad tím, jak se chovat správně, abychom používali naše počítače a další zařízení bezpečně a minimalizovali riziko úspěšného kyberútoku.

Pro potřeby tohoto článku budeme používat pojem počítač, ale myslete na to, že stejně tak riziková jsou i mobilní zařízení a všechna ostatní „chytrá" zařízení připojená k internetu.

V tomto článku vám přinášíme několik základních doporučení, které vám pomohou ochránit se před kybernetickými hrozbami. Nejdříve se ale pojďme zaměřit na motivace kybernetických útočníků, což nám pomůže lépe pochopit celou problematiku.

Motivace kybernetických útočníků

Už dávno nejsou tzv. hackeři pouze vtipálci nebo politicky motivovaní aktivisté, kteří napadají servery vlád nebo velkých korporací. Rozhodně si nepředstavujme podivné týpky v kapucích schované v temných sklepích, kteří provádějí kyberútoky, protože je to baví. Zločin se přesouvá z „ulice" do kyberprostoru, je organizovaný a má globální dosah. Za kyberútoky stojí skupiny, které fungují „podnikatelsky", mají propracované postupy a naplno se touto činností živí. Jejich primární motivací jsou peníze, přičemž chtějí minimalizovat své náklady a maximalizovat výnosy. Logicky používají metody, které stojí málo peněz a mají dobré výsledky. Proto jsou pro první fázi útoku tak často využívané e-maily. Poslat hodně e-mailů je levné. Útočník potřebuje vytvořit jen dobrý, respektive účinný text a ten pak recyklovat a rozesílat. Cílem může být, aby oběť otevřela přílohu obsahující malware – škodlivý program, pomocí kterého útočník získá přístup k zařízení, nebo aby oběť navštívila podvodnou internetovou stránku, pomocí které z vás „tahá" vaše heslo do banky, sociální sítě, e-mailové schránky atp. V okamžiku, kdy útočník získá přístup k zařízení, snaží se napadnout další zařízení v síti a pak maximálně monetizovat (zpeněžit) získaná data, která buď mohou být cenná pro někoho jiného, nebo pro napadenou organizaci. Takovými daty jsou uložené přístupové údaje, e-mailová korespondence, osobní údaje klientů, smlouvy, informace o zakázkách nebo cenné know-how, jednoduše data, která lze prodat. V druhém případě, kdy jde o data, která jsou důležitá pro majitele napadeného zařízení, což může být například účetnictví nebo systém řízení výroby. Útočník data zašifruje a vyžaduje výkupné. Také se snaží nalézt zálohy, aby znemožnil obnovení dat bez platby výkupného. Útočníci se nezdráhají kombinovat obě varianty, kdy vám řeknou, když nám nezaplatíte, tak nezískáte přístup k vlastním datům, a ty nejcennější navíc zveřejníme.

Možná vás napadá, jestli byste za data byli ochotni zaplatit. Z etického pohledu je to velmi sporné, protože v případě zaplacení výkupného za data podpoříte útočníka k dalším útokům. Z pragmatického pohledu, když vám odcizení dat znemožní například pokračovat ve vašem podnikání, přichází otázka vaší připravenosti na podobné útoky. V nejlepším případě jste připraveni tak dobře, že útočit na vás je náročné natolik, že se to útočníkům nevyplatí. Když máte alespoň dobře vyřešené zálohování, tak nemusíte nic platit, protože si obnovíte celou infrastrukturu ze záloh, aniž byste k dešifrování dat potřebovali klíče od útočníků. Připravenost je vhodné testovat, ideálně simulovaným útokem a přinejmenším pravidelným testováním obnovy zálohovaných dat. Pokud na takový případ ale nejste připraveni, můžete zkusit s útočníkem alespoň smlouvat o ceně. Nemají stanovenou jednotnou cenu za odcizená data, jen odhadují a zkoušejí. Tak trochu dobrou zprávou je, že si tito útočníci zakládají na své pověsti. Tedy, že když jim oběť zaplatí výkupné, úspěšně data obnoví. Pokud by vznikl dojem, že oběti data nezískají ani po zaplacení výkupného, nikdo by jim už nezaplatil. Kyberútočníci pracují s důvěrou obětí.

Ani se ke slečně nepřibližujte, ještě ji zavirujete nebo něco horšího a já mám na starosti její kybernetickou bezpečnost.

Kresba: Ivan Svoboda

Jak se chovat bezpečně?

Nyní se tedy pojďme věnovat několika pravidlům, jejichž dodržováním byste se měli stát odolnějšími vůči kybernetickým útokům.

Zapojte kritické myšlení

Jedním z nejdůležitějších pravidel je rozhodně kritické myšlení. Při práci s počítačem je potřeba přemýšlet. Kyberútočníci kromě technických metod útoků hojně využívají technik sociálního inženýrství a manipulují své oběti falšováním identity, naléhavostí nebo výhružkami. Cílem je, aby oběť provedla nějakou akci (otevření přílohy, kliknutí na odkaz) bez toho, aby o ní dlouze přemýšlela. Ale opatrnost při čtení e-mailů nestačí, kritické myšlení bychom měli aplikovat i na sebe, například když se registrujeme do online systému a píšeme heslo, které už jsme použili na mnoha jiných místech, a také na svého IT správce, protože jen málokomu důvěřujeme tak moc jako lidem od IT.

Nenechte se překvapit phishingem

Velmi častým typem útoku je phishing. Existují různé formy tohoto útoku. Mohou to být podvodné sms, podvodné zprávy na sociálních sítích i třeba podvodné volání. Nejčastěji to jsou ale podvodné e-maily, které nás vyzývají k rychlé akci – např. ihned nainstalovat aktualizaci, kliknout na odkaz, otevřít přílohu nebo obnovit heslo.

Platí zde ověřené pravidlo *dvakrát měř, jednou řež* – když vám přijde podezřelá zpráva, měli byste se zamyslet, co je na ní podezřelého. Zastavit se, když dostanete zprávu tzv. mimo normál a rozmyslet si, zda a jak na ni budete reagovat. Bohužel častější je, že lidé nejdříve kliknou a pak přemýšlejí. Je potřeba to obrátit.

Když vám přijde podezřelý e-mail, tak ve většině případů není rizikové otevřít samotnou zprávu, hrozba bývá ukryta v příloze nebo na odkazované webové stránce. Když pravidelně aktualizujete operační systém, poštovního klienta (typicky Outlook) i antivirový program, nemusí být problém si takový e-mail otevřít, přečíst a rozhodnout se, zda jde o podvodný e-mail nebo ne. Phishingové e-maily můžete poznat hned podle několika znaků. V hlavičce zkontrolujte celou adresu odesílatele, zda není něčím nestandardní. Stejně tak zkontrolujte, komu byl e-mail zaslán, tedy příjemce. Podvodné e-maily jsou často směřovány na více lidí nebo dokonce na cizího příjemce, než je vaše e-mailová adresa. Pokud vám text zprávy nedává smysl nebo z textu pociťuje manipulaci, urgenci či nátlak na provedení určité akce, je potřeba být ve střehu a přílohu raději neotevírat. Stejně tak je vhodné zkontrolovat, kam směřuje odkaz, ještě před tím, než na něj kliknete, zda nejde o nesmyslnou adresu (obvykle extrémně dlouhou) či adresu s překlepem apod.

Neotevírejte bez rozmyslu přílohy a odkazy v e-mailech. Kontrolujte e-mailovou adresu odesílatele i příjemce a zpozorněte, když odkazovaná stránka požaduje zadání hesla, nebo když zpráva vytváří časovou tíseň či vás žádá o něco neobvyklého. Nepovolujte makra Microsoft Office (Word, Excel…) když si nejste naprosto jistí, že je to v pořádku.

Když si nejste jistí, můžete kontaktovat údajného odesílatele telefonicky a ověřit, zda vám tuto zprávu skutečně odeslal.

Mějte silná hesla

Čím delší heslo, tím lepší. Nepoužívejte stejné heslo do více systémů a pokud je to možné, aktivujte více faktorové ověřování například pomocí potvrzení SMS kódů, nebo ještě lépe potvrzení přes aplikaci. Hesla si pište na bezpečné místo, ideálně používejte specializovanou aplikaci pro správu hesel (např. LastPass, 1Pass nebo Bitwarden). Heslo, které si musíte pamatovat, můžete tvořit jako větu. Heslo nikomu nesdělujte (ani lidem z IT). Heslo zadávejte tak, aby ho nikdo nemohl odpozorovat.

Udržujte software vždy aktuální

Každý software obsahuje chyby a některé z nich jsou objeveny až po mnoha letech. Určité chyby je možné zneužít k tomu, aby útočník podstrčil vlastní škodlivý program vašemu počítači či serveru a ten ho spustil. Když je taková chyba výrobcem zjištěna a opravena, je vydaná bezpečnostní aktualizace, která nás chrání před zneužitím této chyby. Odkládáním instalace aktualizace se zbytečně vystavujeme riziku, že tuto chybu někdo zneužije proti nám.

Zálohujte automaticky

Zálohování patří k notoricky podceňované a odkládané činnosti, proto je důležité tento proces automatizovat a současně neztratit kontrolu. Nejjednodušším způsobem, jak zajistit kvalitní zálohování našich dat je využít takzvaného cloudového úložiště aplikace jako např. Microsoft OneDrive, Google Drive nebo Dropbox. Tyto aplikace mohou data automaticky na pozadí synchronizovat na servery poskytovatele dané služby. Zároveň vás upozorní, když dojde k nějakému problému se synchronizací, a vy problém můžete bez zbytečného odkladu vyřešit. Získáváme tak zálohovací systém, který funguje autonomně, ale můžete ho kontrolovat. Nebojte se využívat cloudové služby renomovaných firem, které poskytují řádově vyšší úroveň zabezpečení, než jaký je možné v rámci obvyklého rozpočtu většiny organizací realizovat vlastními silami.

Mnohé firmy, které provozují vlastní server, mají každou noc nastavené automatické zálohování. V případě zálohování serveru je velmi důležité zvolit takovou technologii, která zajistí, že případný útočník nebude moci zašifrovat zálohy vašich serverů.

Pro zálohy jako takové platí, že je neděláme kvůli zálohování samotnému, ale kvůli případné budoucí obnově. Proto nestačí kontrolovat, že se záloha provedla, ale je nutné ověřit, že jde obnovit a obsahuje vše, co očekáváme.

Chraňte si svá zařízení i fyzicky aneb šifrujte všude, kde je to možné

Ztráta zařízení je sama osobě velmi nepříjemná záležitost, nicméně ztráta dat uložených na daném zařízení může být ještě horší, resp. může mít horší následky. Šifrováním uložených dat získáváte ochranu, ať už vám někdo zařízení zcizí, anebo ho jen necháte po určitý čas bez dozoru a někdo se pokusí ukrást či modifikovat uložená data.

Nezapomínejte však, že šifrování značně degraduje, pokud máte slabé heslo pro přihlášení do počítače nebo pokud odejdete od nezamčeného počítače. Připravený útočník, a může se jednat i o takzvaného insidera (někoho zevnitř organizace), potřebuje jen pár vteřin k tomu, aby získal kontrolu nad nezamčeným počítačem.

Spolupracujte s IT odborníky a buďte vůči nim zdravě kritičtí

Na konec výčtu bychom doplnili poslední pravidlo nebo spíše doporučení. Využíváme různé technologie doma i v práci a není naším úkolem stát se IT expertem, abychom si všechny zařízení bezpečně nastavili. Když chceme mít dobrý pocit, že jsme udělali pro svou kybernetickou bezpečnost dost, musíme přemýšlet o tom, co na počítači děláme, a k tomu spolupracovat s odborníky. Správný IT správce se zajímá nejen o spravovaná zařízení, která udržuje aktuální a v chodu, ale také o business a procesy klienta, se kterým pomocí technologií hledá způsoby, jak business rozvíjet. Rozhodně by to neměl být někdo, kdo infrastrukturu udržuje „pouze“ v chodu a řídí se heslem „když to funguje, tak na to nesahej“. V této myšlence je schovaná past, že IT infrastruktura zůstane v historii a neadaptuje se na aktuální potřeby a hrozby.

Důležité je, abychom vůči IT správci zůstali zdravě kritičtí. Není tím myšleno, že byste ho měli podezřívat a kontrolovat, ale měli byste se ho ptát, jaká jsou možná řešení, jestli je můžete vidět a testovat. Je to opět aplikace kritického myšlení. Není od věci se poptat, co antivir v poslední době zachytil, jakým způsobem je nastavené zálohování a jak dlouho by v případě potřeby trvala kompletní obnova dat. Jednoduše být u toho, stejně jako při stavbě domu, kdy si jezdíte prohlížet, jak stavba postupuje a zda je to podle vašich představ. IT správce by také neměl mít problém nechat otestovat spravované IT nezávislým IT expertem. Jen tak se dozvíte, v jaké kondici je vaše IT struktura. Podobně jako účetní účtuje, ale audit dělá auditor.

Závěrem

V otázce kybernetické bezpečnosti je důležité zdůraznit, že neexistuje jedno sofistikované řešení, které by nás uchránilo před všemi kybernetickými útoky. Kybernetická bezpečnost je budována jako kombinace více opatření, jejichž účinnost se vzájemně nesčítá, ale násobí. Celková bezpečnost takového systému je pak dána (ne)bezpečností toho nejslabšího článku, kterým však bývá obvykle právě člověk.

Řešením není ani naprostá izolace od internetu a všech technologií. S kybernetickými riziky se musíme naučit žít, chránit se před nimi a minimalizovat je tak, jako jsme se to v historii naučili i v případě jiných rizik, která přinesl pokrok. Řiďte se proto uvedenými pravidly a zvyšte tak svou kybernetickou bezpečnost.

Oto Křivanec
Tomáš Matějíček

Ing. Oto Křivanec *absolvoval obor informatika na Fakultě informatiky a statistiky VŠE v Praze a v současnosti je studentem doktorského studia oboru účetnictví a finanční řízení na katedře finančního účetnictví a auditingu Fakulty financí a účetnictví VŠE v Praze. Pracuje zároveň jako daňový poradce ve společnosti Mepatek s.r.o.*

Tomáš Matějíček *je partner ve společnosti Mepatek s.r.o. a certifikovaný etický hacker. Informačním technologiím se profesně věnuje více než 15 let. Kromě počítačové bezpečnosti se soustředí také na problematiku efektivity správy informačních technologií.*

Objednali jsme si penetrační test kybernetické bezpečnosti našeho informačního systému, při kterém se tady panu kolegovi z počítačové firmy podařilo v naší účtárně ukrást dva šanony.

Kresba: Ivan Svoboda

Jak probíhá běžný kybernetický útok

V tomto článku se podíváme na čtyři scénáře kybernetických útoků, se kterými se můžete poměrně běžně setkat. Zásadní rozdíl spočívá v tom, zda útočník směruje útok přes uživatele nebo server.

První scénář: uživatel přijme e-mail

Jde o klasický příklad, kdy uživatel přijme phishingový e-mail, jehož text ho navede k rozkliknutí odkazu, který ho přesměruje na webovou stránku vypadající jako např. internetové bankovnictví, sociální sítě nebo přihlašovací stránka do webového e-mailového serveru. Vše vypadá v pořádku a uživatel zadá své přihlašovací údaje. Stránka je ale podvodná, takže zadané přihlašovací údaje zachytí útočník, který oběti řekne, že nastala chyba, že zadala údaje špatně nebo oběť přesměruje na reálnou správnou stránku. To už není až tak podstatné, protože útočník získal údaje, které potřeboval.

Podobně to může být situace, kdy útočník zašle e-mail s informací, že vám brzy vyprší platnost hesla a máte si ho co nejdříve obnovit, jinak nebudete mít přístup ke službám. Případně že s vámi někdo sdílí soubor a když kliknete na odkaz a přihlásíte se, můžete si soubor zobrazit.

Útočník počítá s tím, že oběť používá stejné heslo na více místech, anebo že se díky získanému heslu dostane k cíli. Příkladem může být získání přihlašovacích údajů do e-mailové schránky. V té si útočník může dohledat další přihlašovací údaje nebo si případně ve službách pomocí schránky hesla resetovat. E-mailová schránka se stane vstupní branou do dalších služeb.

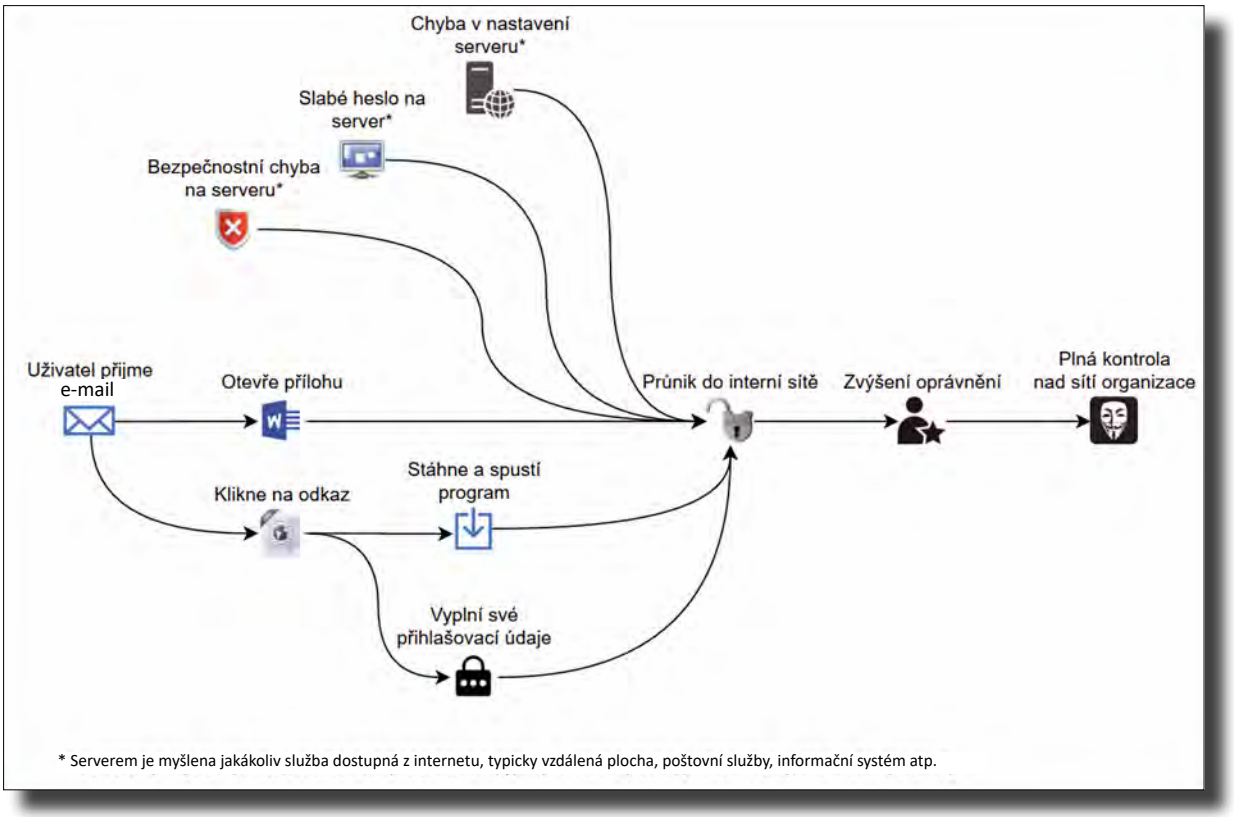
Další variantou je, že odkazovaná stránka kromě přihlášení nabízí stažení programu (např. důležité aktualizace) nebo nějakého dokumentu. Oběť si stáhne program nebo dokument, který obsahuje škodlivý program, který útočníkovi umožní ovládat počítač oběti.

Druhý scénář: chyba nastavení serveru

Jde o situaci, kdy organizace provozuje vlastní server, který je, ať už nedopatřením nebo z neznalosti, chybně nastaven. Obecně se jedná o chybu při správě systému. Chyba může být i velmi triviální, například mohlo zůstat nezměněné výchozí heslo nebo je chybně povolen přístup k interním službám z internetu. Tyto chyby se dají detekovat automaticky pomocí tzv. robotů. Ty prohledávají internet a detekují právě chyby v nastavení. V okamžiku, kdy chybu robot identifikuje, převezme si ji lidský operátor, který se pokusí chybu zneužít.

Třetí scénář: slabá hesla

V tomto scénáři útočník využívá tzv. slovník, seznam nejpoužívanějších hesel, který může být obohacen o osobní informace získané ze sociálních sítí oběti.



Útočník za pomoci slovníku automaticky zkouší jedno heslo za druhým, dokud se ho nepodaří odhalit. Snaží se zneužít tendenci uživatelů používat jednoduchá hesla nebo stejná hesla ve více službách. Pokud útočník odhalí heslo, dostáváme se opět do bodu, kdy pomocí přístupů pronikne do sítě.

V souvislosti s velkým nárůstem práce z domova kvůli koronavirové pandemii se narychlo otevírály vzdálené přístupy, které jsou často slabě zabezpečené. Tím útočníkům vzniklo nové pole působnosti, ve kterém mohou zkoušet, zda účty mají slabá hesla.

Čtvrtý scénář: bezpečnostní chyba na serveru

Tato situace nastává v případě, kdy je bezpečnostní chyba v softwaru, který server používá. Takovou chybu může být možné zneužít k tomu, aby útočník podstrčil vlastní škodlivý program vašemu počítači či serveru a ten ho spustil. Útočníci obvykle zneužívají již známé chyby, ke kterým už existuje oprava – aktualizace. Ke zneužití chyby se využívá tzv. exploit, což je malý program, který se spojí se serverem takovým způsobem, aby se chyba projevila.

Existuje celá řada známých zranitelností, které nemají exploit, tedy nejsou zneužívané. Výrobce softwaru má dostatek času na výrobu aktualizace a uživatelé na instalování aktualizace. Jsou ale situace, kdy exploit vznikne ještě dříve, než je k dispozici aktualizace, pak se jedná o tzv. zero-day exploit, proti kterému není obrany. V takové situaci musí výrobce i správce velmi rychle reagovat, výrobce musí, co nejdříve vydat aktualizaci a správce ji nainstalovat anebo aplikovat dočasné opatření k minimalizaci rizika (např. zablokovat přístup ke službě z internetu).

Útok na uživatele versus útok na server

Pokud útočník směřuje útok na server a na služby, které na serveru jsou, hledá chyby, pomocí kterých získá určitou úroveň přístupu na daný server. Nemusí to být vždy hned administrátor, může se jednat o nějaký omezený systémový účet. Cílem útočníka je zvýšit si oprávnění tak, aby na serveru fungoval jako správce a měl přístup ke všemu.

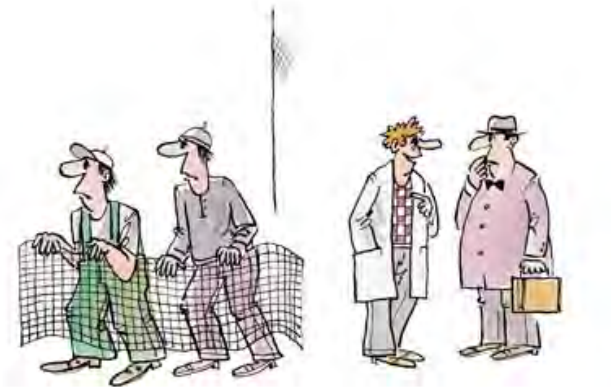
V případě, kdy se útočník soustředí na uživatele a jeho počítač pomocí phishingového e-mailu, usiluje o to, aby získal identitu uživatele. Když útočník získá identitu uživatele, získá oprávnění, které má daný uživatel. Pokud má uživatel omezená oprávnění, útočník je stejně omezen. Samozřejmě se snaží najít na síti maximum cest, jak si oprávnění zvýšit. V tomto spočívá velká slabina celé řady organizací, které z nějakého důvodu požadují, aby jejich uživatelé měli administrátorská oprávnění. Pokud se takový uživatel stane cílem útoku, výrazně útočníkovi usnadní průnik do celé sítě. Proto je vhodné minimalizovat oprávnění uživatelů.

Od průniku po plnou kontrolu sítě

Když se útočník dostane dovnitř sítě, vidí tiskárny, kamery, zařízení, ostatní počítače a servery. Typicky zde najde nějakou chybu v nastavení, slabé heslo nebo bezpečností chybu softwaru a v principu se vrací na začátek a znovu rozbíhá proces průzkumu a útoky na prostředky, které vidí nově. Opět hledá servery, chyby v nastavení, slabá hesla apod. Tomuto procesu se říká „lateral movement“. Útočník se posouvá v infrastruktuře více do hloubky a získává vyšší oprávnění. Cílem je získat plnou kontrolu nad celou sítí a všemi zařízeními, které v ní jsou. Útočník potřebuje, aby si ho nikdo nevšiml a on mohl na síti nějakou dobu fungovat. Na zkopírování citlivých dat potřebuje dostatek času. Nemůže si je zkopírovat plnou rychlostí během pracovní doby, toho by si pravděpodobně někdo všimnul. Potřebuje si to rozplánovat a rozfázovat. Statistiky uvádějí, že doba do objevení útočníka v síti je 197–280 dní. Během celé doby má útočník trvalý přístup do sítě a může se vracet a prozkoumávat nové informace a těžit data.

V okamžiku, kdy útočník už vytěžil všechna data, stáhnul si všechna hesla, zkopíroval všechny e-maily apod., přichází poslední fáze, a to šifrování. Šifrování dat na síti má dva účely. Útočník si takto připraví podmínky pro vydírání a zároveň skryje stopy po své předchozí činnosti, které by někdo mohl analyzovat. Pak už následuje vydírání a komunikace s uživateli. V tu dobu už získal ze sítě všechno, co potřeboval, a většinou je to také okamžik, kdy se o úspěšném útoku dozvídají lidé z dané organizace.

Tomáš Matějíček



Nařídil jsem našim síťovým analytikům, aby podstatnou část sítě upgradovali na vyšší úroveň bezpečnosti.

Kresba: Ivan Svoboda

Legislativa a regulace kybernetické bezpečnosti

Vzhledem ke složitosti kybernetického prostoru je i legislativa týkající se kybernetické bezpečnosti relativně rozsáhlá. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vytvořil základní právní předpis Zákon č. 818/2014 Sb. Tento zákon je dále upřesněn dvěma prováděcími vyhláškami a směrnicí Evropského parlamentu. Ze schématu na straně 19 je patrné, že právní normy jsou propojené a částečně vycházejí z norem ISO/IEC 27k a metodiky COBIT v.5.

Zaměřme se nyní na jednotlivé právní předpisy, které regulují kybernetickou bezpečnost v České republice.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále „zákon o kybernetické bezpečnosti“)

Předmětem zákona je úprava práv a povinností osob, jakož i pravomoci a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti**.** Zákon se věnuje zpracování příslušných předpisů Evropské unie (jedná se o transpozici směrnice NIS) a úpravě zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. Zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

Zákon je účinný od 1. ledna 2015, přičemž v roce 2017 byl tento zákon významně novelizován. Aktuální znění je účinné od 1. února 2020 a zahrnuje stanované základní úrovně bezpečnostních opatření, zlepšení detekce a zavedení hlášení kybernetických bezpečnostních incidentů. Také zavádí systém opatření k reakci na kybernetické bezpečnostní incidenty a upravuje činnosti dohledových pracovišť.

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 z 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)

Dne 6. července 2016 byla uveřejněna směrnice Evropského parlamentu a Rady (EU) 2016/1148 (dále jen „směrnice NIS“). Tato směrnice má za cíl harmonizovat právní úpravu členských států v oblasti bezpečnosti sítí a informačních systémů a zavést jednotný standard úrovně kybernetické bezpečnosti s cílem zlepšení fungování vnitřního trhu.

Vybrané povinnosti, které směrnice NIS ukládá, v České republice již řeší zákon o kybernetické bezpečnosti a jeho prováděcí předpisy.

Směrnice NIS mimo jiné rozšiřuje okruh subjektů, pro které budou stanoveny povinnosti v oblasti ochrany a prevence před kybernetickými bezpečnostními incidenty. Jedná se o tzv. provozovatele základní služby a poskytovatele digitálních služeb (internetové vyhledávače, cloud computing a online tržiště). Požadavky směrnice zapracovává novela zákona o kybernetické bezpečnosti formou zákona č. 205/2017 Sb. s účinností od 1. srpna 2017 (viz příslušná sekce stránek NÚKIB).

Vyhláška o kybernetické bezpečnosti

Tato vyhláška zapracovává směrnici NIS a upravuje obsah a strukturu bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatření, typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho vzor oznámení kontaktních údajů a jeho formu, způsob likvidace dat, provozních údajů, informací a jejich kopií pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné informační systémy, informační systémy základní služby nebo sítě elektronických komunikací, které využívá poskytovatel digitálních služeb.

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Dne 19. prosince 2014 vstoupila v platnost vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích.

V roce 2020 byla přijata novela vyhlášky, která má za cíl zpřesnit kritéria pro určení toho, zda je daný informační systém významný. Nabytí účinnosti celého znění vyhlášky je rozloženo do tří období (měnit se bude znění § 2, první období nastává 1. ledna 2021). Kompletní znění nabude účinnosti 1. ledna 2023.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Nařízení vlády je platné od 30. prosince 2010. Definuje průřezová a odvětvová kritéria pro určení prvku kritické infrastruktury. V příloze k nařízení vlády je definováno devět odvětví včetně jednotlivých odvětvových kritérií pro určení prvku kritické infrastruktury.

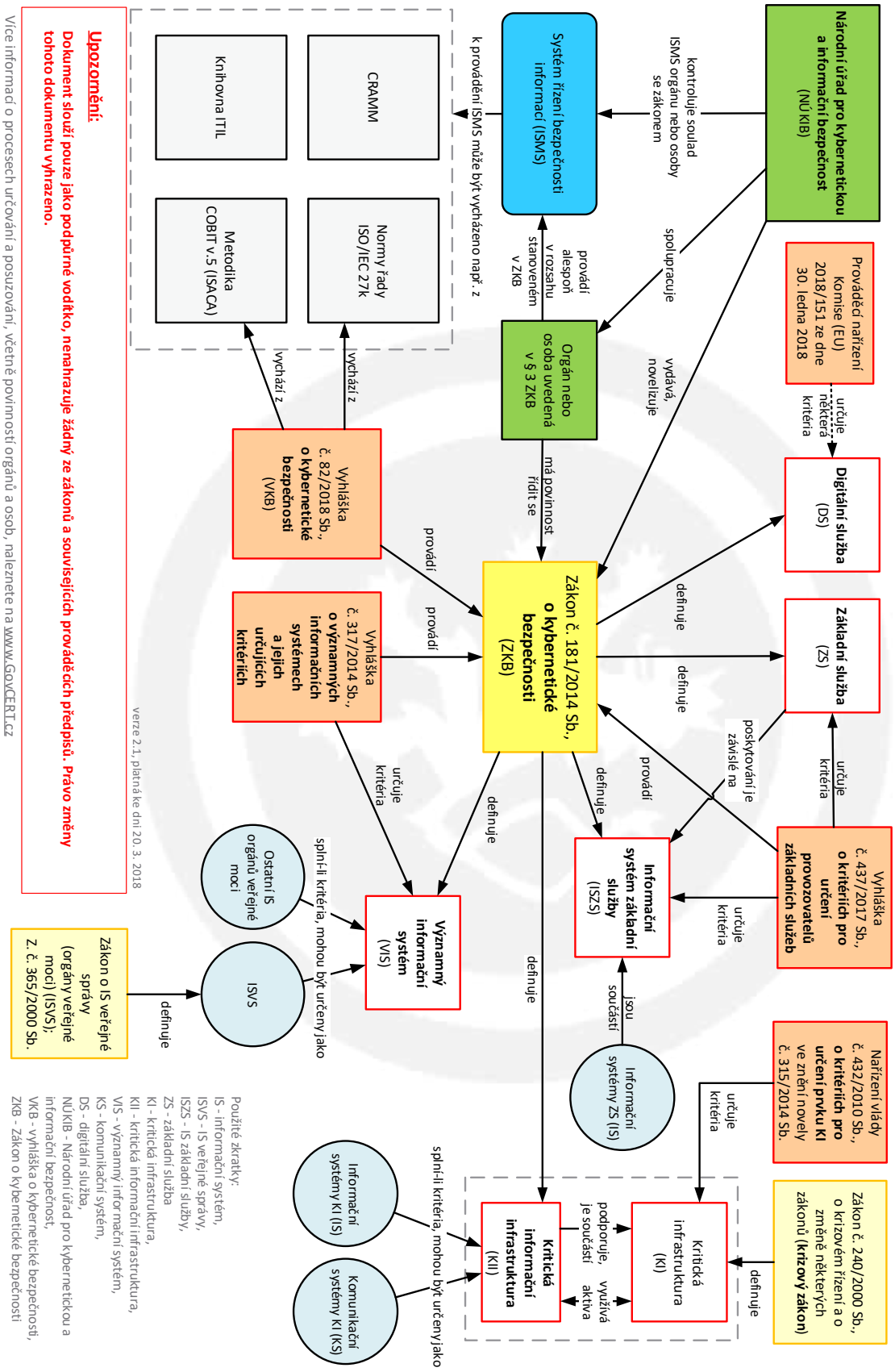
Toto nařízení vlády nabylo účinnosti 1. ledna 2011. V souvislosti se zahrnutím oblasti kybernetické bezpečnosti do odvětvových kritérií proběhla novela nařízením vlády č. 315/2014 Sb., s účinností od 1. ledna 2015.

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Dne 15. prosince 2017 byla ve Sbírce zákonů České republiky vydána nová vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

Vyhlášku zpracoval NÚKIB ve spolupráci s odbornou veřejností. Vyhláška zapracovává požadavky

Přehledové blokové schéma k zákonu a jeho prováděcím předpisům[1]



[1] Zdroj: https://www.nukib.cz/download/publikace/podpurne_materialy/ZKB_blokove_schema.pdf

směrnice NIS ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Vyhláška upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 zákona o kybernetické bezpečnosti. Vyhláška nabyla účinnosti dne 1. února 2018.

Prováděcí nařízení EK ke Směrnici NIS, které stanoví bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb

Dne 31. ledna 2018 zveřejnila Evropská komise prováděcí nařízení komise (EU) 2018/151, kterým se stanoví pravidla pro uplatňování směrnice NIS. Toto prováděcí nařízení obsahuje bližší upřesnění bezpečnostních opatření, které musí poskytovatelé digitálních služeb (§ 3 písm. h) podle ZKB) zohledňovat při řízení bezpečnostních rizik, jimž jsou vystaveny sítě a informační systémy, a dále bližší upřesnění parametrů pro posuzování toho, zda je dopad incidentu významný. Toto prováděcí nařízení je účinné od 10. května 2018 a je přímo aplikovatelné. Pro poskytovatele digitálních služeb je tedy závazné.

Oto Křivanec

Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti (č. 118/2014 Sb. ze dne 23. července 2014) upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon je implementací příslušný předpisů Evropské unie a upravuje zejména způsob zajištění bezpečnosti sítí elektronických komunikací a informačních systémů. V průběhu své účinnosti byl zákon již šestkrát novelizován, jeho aktuální verze je účinná od 1. ledna 2021.

Hlavní cíle zákona:

- stanovit základní úroveň bezpečnostních opatření,
- zlepšit detekci kybernetických bezpečnostních incidentů,
- zavést hlášení kybernetických bezpečnostních incidentů,
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty,
- upravit činnost dohledových pracovišť.

Vymezení pojmů (§ 2):

- *bezpečnost informací* je zajištění důvěrnosti, integrity a dostupnosti informací a dat,
- *významný informační systém (VIS)* je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,
- orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou *správce a provozovatel VIS,*
- *bezpečnostním opatřením* se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru,
- *informační systém základní služby* je informační systém, na jehož fungování je závislé poskytování základní *služby*, tj. služby, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví:
  - energetika,
  - doprava,
  - bankovnictví,
  - infrastruktura finančních trhů,
  - zdravotnictví,
  - vodní hospodářství,
  - digitální infrastruktura,
  - chemický průmysl.

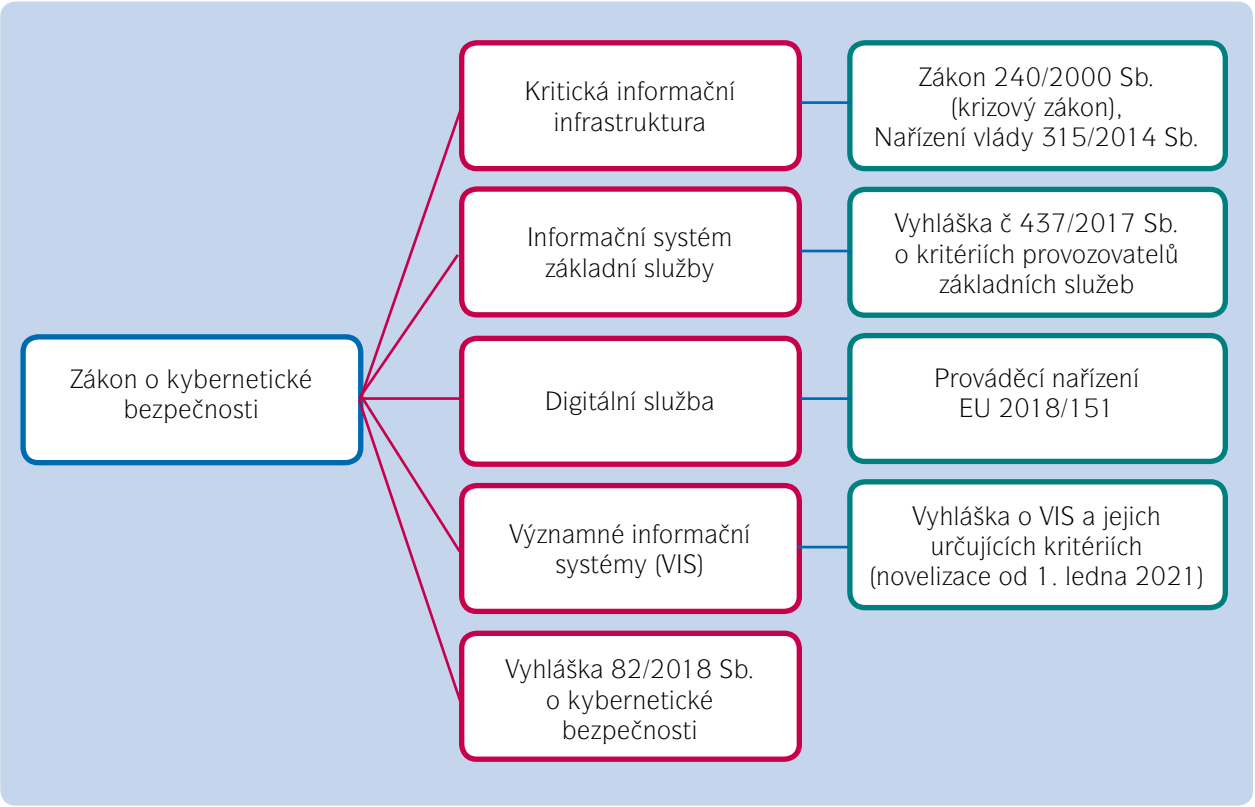
Národní CERT (Computer Emergency Response Team) (§ 17)

Národní CERT zajišťuje v rozsahu stanoveném zákonem sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti.

Jako provozovatele národního CERT vybral Národní bezpečnostní úřad (NBÚ) 17. srpna 2015 sdružení právnických osob CZ.NIC[1]. Výběrem národního CERT byl splněn úkol vyplývající ze zákona o kybernetické bezpečnosti a dokončena dělba kompetencí a práce mezi vládním CERT a národním CERT. Rozdíl mezi vládním a národním CERT je definován zákonem o kybernetické bezpečnosti. Zjednodušeně lze říci, že vládní CERT je určen pro řešení bezpečnostních incidentů v počítačových sítích státní správy, kritické informační infrastruktury a VIS dle zákona o kybernetické bezpečnosti. Národní CERT je pak bezpečnostní tým pro koordinaci řešení ostatních bezpečnostních incidentů v počítačových sítích provozovaných v České republice.

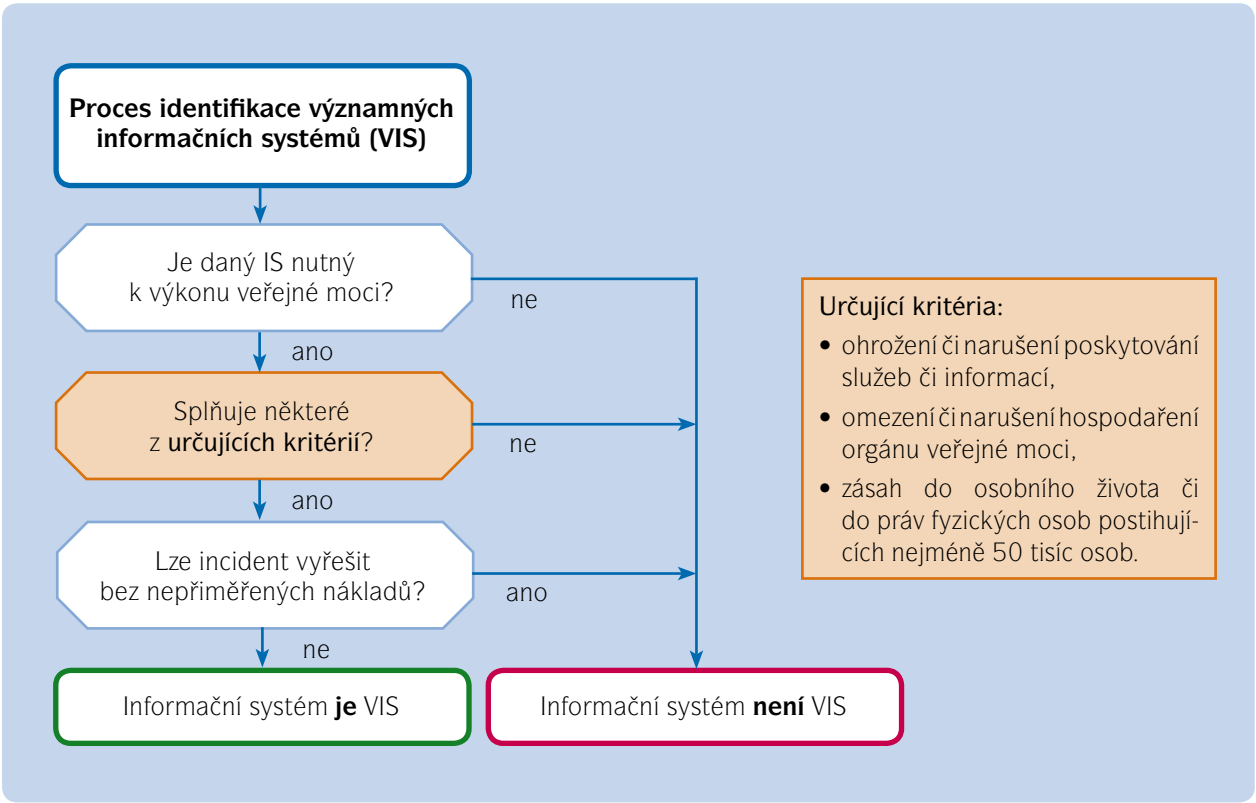
[1] https://www.nic.cz/page/2961/narodni-bezpecnostni-tym-csirt.cz-bude-i-nadale-provozovat-sdruzeni-cz.nic/

Oblasti působnosti zákona o kybernetické bezpečnosti



Co mimo jiné stanoví prováděcí právní předpisy:

- obsah bezpečnostních opatření,
- obsah a strukturu bezpečnostní dokumentace,
- rozsah bezpečnostních opatření pro orgány a osoby,
- proces hlášení a evidence kybernetického bezpečnostního incidentu,
- významné informační systémy (VIS) a jejich určující kritéria.



Hlavní povinnosti správce, kterého musí mít každý VIS

- Nahlášení VIS a kontaktních údajů do 30 dnů (tj. do konce ledna 2021 pro existující systémy),
  - implementace a provádění bezpečnostních opatření (specifikuje Vyhláška o kybernetické bezpečnosti),
  - hlášení kybernetických bezpečnostních incidentů (obdoba hlášení incidentů na ÚOOÚ),
- provádění opatření vyhlášených NÚKIB pro správce VIS.

Závěrem

Přesto, že by se mohlo zdát, že zákon o kybernetické bezpečnosti je primárně zaměřen na otázky bezpečnosti státu a jeho informační infrastruktury, v řadě ohledů se může týkat i soukromých subjektů, které provozují VIS. Východiskem implementace zákona je tedy posoudit, zda organizace takový VIS provozuje, protože pak se na ni vztahuje řada povinností uložených zákonem a s takovou situací se mohou u svých klientů setkat při své práci i auditoři.

Ladislav Mejzlík

.

Hugo a Sally se baví o detailním testování

1. Rozsah testu

Ahoj Sally. Chtěl bych se s tebou pobavit o tom našem novém asistentovi. Hodlám mu ze začátku svěřovat zejména detailní testování. Má pár let zkušeností s auditem a principy zná. Ale rád bych s ním prošel, na co si má dávat pozor.

To je dobrý nápad. Určitě bych s ním probrala otázku stanovení potřebného rozsahu testů.

Na to se mě už ptal. Z předchozí praxe byl zvyklý, že některé účty testoval určitým konstantním počtem položek. Třeba při inventuře vybral náhodně deset položek zásob, ve mzdách pět zaměstnanců a tak podobně.

Tak bude potřeba mu vysvětlit, že takhle to nefunguje. Počet testovaných položek při reprezentativním výběru vždy závisí na dvou finančních veličinách: celkové hodnotě testovaného účtu a prováděcí materialitě. Na účtu, který má zůstatek dvacetinásobku prováděcí materiality, musí otestovat mnohem více položek než na účtu, který má zůstatek třeba jen jejího dvojnásobku.

Jasně. Ale taky mu musím zdůraznit další důležitý faktor, a to je riziko. Musí chápat, že pro ověření dvou účtů se stejnou finanční hodnotou, které mají dle mého vyhodnocení různé riziko, je třeba testovat rozdílný počet položek.

Souhlasím. Rozsah detailního testování musí být vždy vázán na hodnotu testovaného účtu, prováděcí materialitu a riziko.

-SpM-

Kybernetická bezpečnost – zkušenosti a rady specialistů

Jan Huml

Jan Klouda

Kvalifikace hackerů a tím i sofistikovanost kybernetických útoků roste. Myslíte si, že s nimi specialisté na bezpečnost zvládají držet krok?

JH: Zabezpečení je ve všech svých činnostech vždy o krok pozadu – ukazuje nám to historie na všech příkladech v oblasti mechanické, technické, fyzické i režimové bezpečnosti. Kybernetická bezpečnost v tom není jiná. Bohužel sofistikovanost útoků je přímo úměrná prevenci, která se systému věnuje při jeho návrhu. Většinou se podaří systém napadnout skrze zařízení, které bylo vyvinuto s omezeným rozpočtem. Rozpočet na bezpečnost při návrhu systému je totiž vždy kompromisní, a kdyby záleželo pouze na bezpečnosti, nikdy nebude systém prakticky použitelný.

JK: Technologické schopnosti předcházet kybernetickým útokům jsou dobré. Úspěšný útočník tak musí být o krok napřed, aby překonal nastavené bariéry, nebo mu situaci usnadní nesprávně nastavené prvky kybernetické ochrany.

Nejsofistikovanější útoky s využitím nástrojů tajných služeb probíhají i na infrastruktuře izolované od vnějšího světa. To hezky ilustruje, že obrana proti kybernetickým hrozbám nespočívá jen v technologických opatřeních, ale také ve vhodném nastavení fyzické ochrany ohrožených prvků.

Některá rizika si firmy způsobují samy extensivním propojováním svých sítí včetně zahraničních poboček. Úspěšný kybernetický útok v jedné zemi se tak může ve skutečnosti projevit kdekoli na světě, nebo může mít fatální dopad na celou mezinárodní strukturu.

Myslíte si, že si je laická veřejnost obecně vědoma rozsahu rizik kybernetické bezpečnosti? Je tendence je spíš přeceňovat, či podceňovat?

JH: Veřejnost začíná o kybernetické bezpečnosti mluvit teprve s rozvojem běžně použitelné výpočetní techniky (mobilní telefony, domácí sítě) a hlavně s nástupem inteligentních budov a internetu věcí. Na nových sociálních sítích se bezpečnost řeší běžně, nicméně je stále věcí spíše okrajové části společnosti. Boom kybernetické bezpečnosti nás teprve čeká.

JK: Téma kybernetické bezpečnosti není nové a v médiích se pravidelně objevuje. Většina z nás má zkušenost s podezřením na phishingový útok předstírajícím komunikaci banky, čas od času se objeví zpráva o napadení provozních systémů či databází i velkých korporací.

Přesto někteří lidé kybernetickou bezpečnost podceňují, často s odkazem na tvrzenou nezajímavost obsahu jejich počítačů či mobilních telefonů.

Právě zabezpečení mobilních telefonů a zařízení typu Internet of Things (IoT) je jednou ze současných velkých hrozeb. Troufnu si říct, že většina lidí tuto hrozbu neřeší, neaktivuje ochranné prvky, neupdatuje firmware či neupgraduje hardware a software, který jej ovládá.

To, že často „přání je otcem myšlenky“, platí i zde.

Věnují podle vás firmy kybernetické bezpečnosti dostatečnou pozornost, kapacity a finanční prostředky? Liší se to podle velikosti nebo oboru?

JH: Určitě je viditelný rozdíl mezi korporátem a menšími společnostmi. Nadnárodní firmy běžně přistupují k ochraně dat a vlastních sítí a zařízení velmi odborně, většinou i prostřednictvím vlastního týmu IT security. Naopak střední a menší firmy toto začínají řešit až v případě, kdy dojde k napadení systému. Taktéž lze říct, že mobilní operátoři, jejichž podstatou je udržovat síť přístupnou všem uživatelům, mají velmi kvalitně zpracovanou bezpečnostní politiku a snaží se v maximální míře chránit infrastrukturu a přitom neomezovat uživatele. Bankovní sektor k tomu přistupuje ještě striktnější metodou. Je však třeba říct, že náklady na bezpečnost obecně jsou dlouhodobě poddimenzované.

Pane kolego, vedení naší firmy rozhodlo, že je třeba věnovat vyšší pozornost kybernetické bezpečnosti, a proto se rekvalifikujete z požárního technika na správce firewallu naší počítačové sítě.

Kresba: Ivan Svoboda

JK: Na kybernetickou bezpečnost se dá vynaložit tolik finančních prostředků a úsilí, kolik budete chtít, a stále bude co zlepšovat.

Ochota firem pořizovat prostředky kybernetické ochrany se liší nejen podle oboru, ale také podle ekonomické výkonnosti. Rozdíl je i mezi soukromou a veřejnou sférou.

Velké instituce typu bank, mobilních operátorů či energetických společností do kybernetické ochrany investují značné prostředky. Vědí, že jeden útok je dokáže zcela vyřadit z provozu, způsobit značné škody a poškodit jejich pověst. Mívají nastavené vysoké parametry úrovně kybernetické bezpečnosti, které chtějí dosáhnout. Tyto parametry odpovídají oborovým standardům, regulačním požadavkům, dostupnosti technologií a výsledkům analýz rizik odhalujících nejohroženější části infrastruktury.

Hugo a Sally se baví o detailním testování

2. Reprezentativní výběr

Náš nový asistent se mě ptal, jak velká může být neotestovaná část zůstatku nějakého účtu, respektive jakého procentuálního pokrytí populace musí testovanými položkami dosáhnout.

Bavíme se o testování relativně homogenní populace, kdy je možné využít reprezentativního výběru?

Ano. Položky v populaci jsou relativně stejně veliké a riziko chyby je u nich také podobné.

Kvalitu takového testu neměříme procentuálním pokrytím. Celý účet může mít tisíce položek a v testovaném vzorku jich bude třeba jen pár desítek. Vzorek běžně pokrývá jen pár procent zůstatku testovaného účtu. A hodnota položek, které nespadly do vzorku, běžně bývá i několikanásobek materiality. To není při dodržení správného postupu testování problém.

Jasně. Důležitý je dostatečný počet položek vzorku. Jsou na to vzorce a pomůcky.

Ano. Pokud je otestovaný dostatečně velký reprezentativní vzorek, potom výsledek vzorku vypovídá o celém zůstatku daného účtu. Hodnota zbytku, který nebyl zahrnut do vzorku, tak není podstatná.

Rozumím. Klíčové je vzorek skutečně vybírat z homogenní populace reprezentativně, což znamená, že všechny položky daného účtu musí mít šanci se do vzorku dostat.

A položky, které mají třeba výrazně vyšší hodnotu než zbytek, nezahrnovat do reprezentativního testování a otestovat samostatně jiným způsobem.

-SpM-

Jaký je váš názor na aktuálně probíhající „živelnou“ digitalizaci a práci na dálku v důsledku opatření proti šíření koronaviru? Zvyšuje to významně rizika kybernetické bezpečnosti?

JH: Většina středních a velkých společností byla na tento stav připravena již dříve, jelikož práce z domova byla často aplikovaná jako zaměstnanecký benefit. Pro tyto potřeby proto byly vytvořeny virtuální sítě s odpovídajícím (někdy i více faktorovým) ověřením. Například společnosti, které provozují callcentra, tak mohly snadno přesunout své operátory na režim home office s notebookem.

Určitě nyní zažíváme čtvrtou průmyslovou revoluci – práce z domova není považována za tabu, na kolegy doma se nedíváme jako na flákače, a stejně tak začínáme i více přemýšlet nad vlastní bezpečností. Čím dál častěji se skloňuje otázka zabezpečení domácích Wi-Fi a uživatelé mají i více prostoru to řešit.

Rizika, která se definují větším počtem vnějších vstupů do sítě, jsou samozřejmě měřitelná, a základním rizikem je vždy uživatel. Tady vidím obrovské rezervy, jelikož kybernetická bezpečnost se v rámci firem nevysvětluje a odehrává se většinou v rovině „nařízení“ někoho z IT. Všichni víme, že na IT se stále dívá spousta lidí skrz prsty. Obzvláště, když řekneme, že je to „bezpečák“ v IT – pro mnoho lidí je ta práce neuchopitelná a rizika neviditelná.

JK: Rostoucí míra digitalizace kybernetická rizika zvyšuje. Sama práce na dálku nicméně nové kybernetické riziko nepředstavuje, na rozdíl od nových technologií, které s tím souvisí.

Při rozumném užívání prověřených aplikací a systémů a instalaci antivirových programů by běžný uživatel neměl čelit nadměrným rizikům. Zvýšenou míru rizika představuje spíše neopatrné jednání uživatelů, instalace neprověřených softwarů zdarma z internetu či sdílení neprověřených souborů.

Kybernetické útoky probíhají neustále, 24 hodin denně. Pokusů o proniknutí do počítačů, počítačových sítí či průmyslové infrastruktury je ohromné množství. Riziko je permanentní.

Obecné riziko plynoucí z živelné digitalizace spočívá v menší ochraně informací například v průběhu telekonferencí, u kterých nemáte přehled, kdo další může poslouchat, či ve sdílení dokumentů a důvěrných informací nezabezpečenými a neschválenými kanály.

Firmy také často bojují s odporem zaměstnanců podřizovat své chování nastaveným bezpečnostním pravidlům. Odvolávají se přitom na komplikovanost a pomalost. Neuvědomují si ale, že kybernetická bezpečnost není o pohodlí, ale o bezpečnosti. Obcházení nastavených opatření z lenosti je velkým problémem. Extrémním případem může být třeba sdílení velkých souborů s firemními daty přes ulož.to, přestože existuje proprietární bezpečné řešení s funkcionalitou šifrování.

Jak podle vaší zkušenosti dnes vypadá (probíhá) typické napadení firemních počítačů?

JH: Pro každého útočníka je prvním krokem vždy hledání nejslabšího místa v obraně – tím se velmi často stává uživatel. Mým nejoblíbenějším testem, který zůstává v platnosti roky, je rozmístění USB disků náhodně po budově společnosti a sledování zvědavosti zaměstnanců. Málokdo se k povalující „flešce“ postaví skepticky a většina lidí se raduje ze získání nového disku. To se ale bavíme pouze o jedné formě útoku, při němž se vyžaduje má vlastní fyzická přítomnost.

Mnohem častější jsou útoky prostřednictvím škodlivého obsahu na internetových stránkách, popřípadě zasíláním infikovaných příloh. V obou případech je třeba bezpečnost rozdělit do několika rovin, které souvisejí se vzděláváním uživatelů, kontrolou škodlivosti příloh v e-mailech a nastavení odpovídajících pravidel činností na internetu.

JK: Tak, že neinformovaný nebo nepozorný zaměstnanec klikne, kam nemá.

Jaké jsou typické chyby jak při budování obrany proti útokům, tak zejména při reakci na ně?

JH: Nejčastěji se pořád setkáváme s nedostatečným zabezpečením přípojných bodů, neoddělením sítí pro návštěvy a zaměstnance a neřešením připojených zařízení do sítě – je to typický problém menších nebo rychle se vyvíjejících společností.

Druhou věcí je pak živelnost IT, které se snaží v maximální míře pokrýt potřeby s tím, že zabezpečení se dodělá někdy potom. To generuje nejen neznalost vlastní sítě a s tím evidované problémy, ale současně to otevírá větší množství vstupů do systému.

Za zmínku pak stojí i bezpečnostní politika související s filtrováním obsahu – většina uživatelů využívá pracovní zařízení i pro soukromé účely a spousta stránek je jen chytákem pro tyto útoky.

JK: Firmy často instalují opatření kybernetické bezpečnosti, aniž by měly dobře zanalyzovaná rizika, identifikované kritické prvky a připravené postupy pro případ úspěšného útoku. Bez znalosti rizik však může ochrana být neúčinná nebo předimenzovaná a nemusí vůbec řešit hlavní hrozby.

V předchozí odpovědi jsem zmiňoval, že incidenty často vznikají nevhodným chováním. To může spočívat třeba v užití infikovaného USB zařízení, jako je flash disk. Divili byste se, kolik firem si myslí, že má dobře připravenou kybernetickou ochranu a stále zaměstnancům užití USB zařízení povoluje. Přitom uzamčení USB portu je nesmírně jednoduché, je zadarmo a bez USB portu se dá krásně žít.

Firmám také často nedochází riziko propojenosti klíčových prvků jejich IT infrastruktury. Úspěšný útočník tak může ohrozit veškeré prvky najednou. Tomuto riziku se dá čelit například oddělením jednotlivých prvků,

virtualizací, důsledným řízením přístupových práv, oddělením procesů apod.

Stejně základním opatřením je řízení uživatelských práv na pracovních stanicích. Stále ještě existují firmy, které zaměstnancům přidělují plná administrátorská práva a zaměstnanci si tak mohou i na firemní zařízení nainstalovat, co chtějí. I řešení tohoto rizika je nesmírně jednoduché a je zadarmo. Administrátorská práva potřeba nejsou a v případě potřeby může vždy pomoci pracovník IT.

Při reakci na kybernetický útok bývá problém volit správné kroky ve správném pořadí. Míra dopadu útoku může také záležet na štěstí, jak se zasahujícímu týmu kybernetických specialistů podaří v průběhu útoku udělat klíčový krok, který útok může zcela zastavit. Vedle štěstí je to také o pohotovosti, třeba když pracovník IT rozpojí včas ty správné kabely a postup útoku tak zastaví. I takové věci se dějí.

Hovoříme-li o štěstí, mám na mysli štěstěnu dobře připraveného týmu. Spoléhat se jenom na náhodu je opravdu špatný nápad. Když totiž k útoku dojde, můžete třeba reálně vidět, jak vám před očima mizí jeden sdílený disk za druhým, jak je útočník postupně šifruje a tím je pro vás znepřístupňuje. Je to nesmírně krizová a kritická situace, ve které dobře připravený kybernetický tým má daleko větší šanci na šťastný zákrok a izolaci problému.

U složitějších systémů je důležité identifikovat napadené prvky a postupovat s velkou obezřetností, protože útočník může obranné činnosti identifikovat a třeba spustit útok, se kterým čekal na jinou vhodnou příležitost. Identifikace napadených prvků je důležitá také pro jejich důslednou izolaci od zbytku „zdravé infrastruktury". Je to podobné operaci rakoviny. I zde může pacient zemřít.

Čištění systému je až posledním krokem, který by měl následovat, až když si je napadená firma jista, že ví, co se přesně stalo. Stejně obezřetně je třeba přistupovat k aktivaci záložních systémů a zajistit jejich ochranu před nastalou hrozbou.

Mohou být firmám v boji proti kybernetickým útokům nějak nápomocny státní instituce jako Policie ČR, NÚKIB apod.? Kdy a jak by s nimi měly firmy spolupracovat?

JH: NÚKIB aktuálně spouští zajímavý vzdělávací program pro veřejnost, který určitě stojí za to sledovat. Jeho roli považuji za spíše strategickou v ochraně, vzdělávání a případně detekci hrozeb pro státní sektor. Stejně tak Policie ČR dělá dobrou práci hlavně při následném trestním řízení nebo v případě preventivního zásahu a omezení větších škod, pokud jde o útoky na kritickou infrastrukturu. Pro každou společnost je nejlepší obranou její vlastní znalost systému a architektury – zde je potřeba chápat, že útočník napadenou síť nezná a musí se ji předem naučit. V úvodu rozhovoru jsme se bavili o tom, že zabezpečení je pozadu. Pokud budeme do řešení útoku zapojovat jiné externí složky, pak jsme uměle vytvořili ten samý problém – zasahující odborník nebo státní složka se musí se situací nejdříve seznámit a útočník má před nimi náskok. Obecně platí, že jsou mnohem efektivnější zásahy soukromých společností, které se snaží v maximální míře chránit zájem zákazníka (napadené společnosti) a způsobit co nejmenší škody.

JK: Pomoc ze strany státu může být několikerá. Zaprvé sdílením informací o aktuálních hrozbách, což se do jisté míry děje již dnes. Pokud ale vezmeme například debatu kolem některých čínských dodavatelů, chybí nám konkrétní informace o hrozbách, proti kterým se chránit. Stát konstatuje nebezpečí. Ale chybí to „B": v čem a o kolik je problematická technologie rizikovější než jiná a v čem konkrétní hrozby spočívají, abychom je dokázali ošetřit či se rozhodnout o její vhodnosti.

Stejně tak by bylo dobré podpořit technologickou vybavenost a dovednosti Policie a zvýšit rychlost při šetření kybernetických útoků. Je ale také potřeba si uvědomit, že velké kybernetické útoky na infrastrukturu v Čechách nejsou zpravidla vedeny z území České republiky, ale ze zahraničí. Schopnost identifikovat konkrétního útočníka, který vám zašifroval datová úložiště, je prakticky nulová.

Obrovským problémem je nedostatek soudních znalců v potřebných oborech. Pro trestní řízení nebo soudní vymáhání vzniklé škody tak často nastává důkazní nouze, protože znalci nedokážou správně zhodnotit technologickou stránku věci nebo správně určit výši vzniklé škody. Soudy nemají potřebnou znalost a bez podpory znalce nemohou svá rozhodnutí důkazně podložit. I přes deklarovanou snahu o digitalizaci Česká republika stále ještě významně zaostává.

Je lepší si ve firmě budovat vlastní kapacity specialistů pro obranu před kybernetickými útoky, využívat externí specialisty nebo oba způsoby kombinovat?

JH: U čistě IT společností se vyplatí držet si včasnou reakci ve vlastní režii z důvodů, které jsme řešili v předchozí otázce. Znalost vlastního prostředí je výhodou, kterou je třeba využít proti útočníkovi.

Nicméně je třeba současně s tím říci, že provozní náklady tohoto útvaru budou extrémně vysoké – znalosti a trendy je třeba v tomto týmu udržovat na stejné úrovni, jako má útočník, a i včasná reakce musí být odpovídající kvality. Hodně pomáhá, když se společnost věnuje IT bezpečnosti stejně jako bezpečnosti fyzické: plánuje služby monitoringu sítě, provádí pravidelné penetrační testy a věnujeme se pravidelným aktualizacím. Vzhledem k omezenému rozpočtu všech společností je pak ideálním řešením udržovat maximální kvalitu vlastního personálu s ohledem na náklady a společně s tím

používat pro penetrační testy odborníky, kteří se pokoušejí v pravidelném intervalu tuto obranu prolomit.

JK: Nejlepší je oba způsoby podle velikosti firmy a jejích okolností kombinovat.

Pro velké organizace může být vhodné řešit nastavení vnitřních procesů a opatření vlastními silami, stejně jako třeba ošetření kybernetických hrozeb instalovaného software či nových produktů.

Pro zavádění moderních prvků kybernetické ochrany, vyšetřování kybernetických incidentů či penetrační testy na úrovni firemní infrastruktury má externí dodavatel výhodu nezávislosti a zkušenosti s aktuálními hrozbami. Zejména mezinárodní korporace mohou také těžit z expertízy zahraničních kolegů či sdílené infrastruktury zabezpečené centrálně.

Jak vidíte další vývoj v oblasti kybernetické bezpečnosti?

JH: Stejně jako v ostatních oborech je trendem umělá inteligence. Jiné činnosti pravidelně provádíme my (a stejně jako jiný uživatel se můžeme chytit do pasti) a jiné činnosti provádí finanční účtárna. Umělá inteligence nám pomáhá předpokládat, který krok uživatele je nestandardní, která služba se musí používat a jaká komunikace s tím souvisí. Využití umělé inteligence nám v budoucnu bude určitě pomáhat mnohem více.

Hugo a Sally se baví o detailním testování

3. Cílený výběr

S naším novým asistentem jsme se také bavili o cílených výběrech, které nejsou reprezentativní. Třeba, když 80 % zůstatku tvoří 20 % faktur a já úmyslně vyberu největší faktury nebo faktury několika největších dodavatelů. Co potom s neotestovanou částí účtu?

U cíleného výběru je neotestovaný zbytek zůstatku účtu důležitý, protože na něj na rozdíl od reprezentativního testu nelze vztáhnout výsledek testu těch vybraných položek.

Aha, takže k neotestované části nemám žádnou důkazní informaci. Pokud je tento zbytek materiální, musí se dále testovat.

Ano, ale pozor! Může být nutné dále testovat i v případě, kdy je testem nepokrytý zbytek zůstatku na jednom účtu menší, než je prováděcí materialita.

Máš na mysli situaci, kdyby bylo takových zbytků z cílených testů víc?

Přesně tak. Pokud by součet takto netestovaných zbytků účtů byl materiální, mohl by to být problém. Podle celkové hodnoty a výše odhadovaných rizik může být nutné alespoň část z těchto zbytků dotestovat.

Ale na to můžu klidně použít i reprezentativní vzorek, ne?

Ano. Často může stačit náhodně vybrat pár dalších položek.

-SpM-

To samé platí u systému včasné reakce – umělá inteligence bude například odstavovat klíčové síťové prvky, a tím izolovat útočníka.

JK: Kritická bude ochrana autonomních řešení, jako jsou automobily, a telekomunikačního spojení pro vzdálené aplikace, jako jsou chirurgické zákroky na dálku apod.

Stejně tak bude potřeba nastavit standardy kybernetické ochrany IoT zařízení a technologických celků jako je Smart City a čehokoli dalšího, co je tzv. „smart".

Úspěšný kybernetický útok v každé z těchto oblastí by měl závažné dopady na velké množství lidí a způsobil by značné škody.

Žádný z těchto problémů nemá jednoduché řešení. Zatímco výrobci autonomních aut budou zřejmě motivováni maximálně své produkty zabezpečit, u výrobců IoT zařízení jsem si skoro jist opakem. Samostatnou kapitolou pak jsou ona „smart" řešení kombinující technologie více výrobců. Rozhlédněme se kolem sebe a můžeme si sami udělat názor na rizika spojená s provozem takových celků například na úrovni obcí, měst nebo státu.

Samostatnou kapitolou je rozvoj kybernetické bezpečnosti ve státních IT systémech potýkajících se velkou roztříštěností, zastaralostí a neduhy vyplývajícími z veřejných zakázek. Přitom ochrana základních systémů státu by měla mít prioritu.

Stát by měl také více dbát na reálné zvýšení kybernetické bezpečnosti v rámci tzv. kritické informační infrastruktury. Dnes existující legislativní rámec v oblasti kybernetické bezpečnosti pravomoci státu dává. Ale ruku na srdce, kolik firem bere svou připravenost vážně, a kolik z nich jen jako papírové cvičení?

Kdybyste měl dát auditorům dobrou radu týkající se počítačové bezpečnosti, co by to bylo?

JH: Hlavní jsou informace a vlastní vzdělávání. (Ne)bezpečnost je po celou dobu své historie stejná – tkví v tom, co jako společnost akceptujeme jako hrozby a co jsme ochotni kvůli nim obětovat. Dokážu si představit, že firma pracující v cloudu dokáže obětovat všechny klientské stanice za předpokladu, že bude cloud v bezpečí. Na bezpečnost v IT lze proto aplikovat stejné myšlení – jsou tam stejné hrozby, stejná rizika i stejná filozofie ochrany. Jediné, co se mění, je prostředí, které je digitální. I v tomto prostředí však máme dveře, zdi a případně i pro nás důležité stroje. Jen je potřeba si porty, firewally a servery představit jinak. A stejně tak se dívat i na uživatele, útočníka a návštěvy.

JK:

- Nespoléhat na to, že vám se to stát nemůže.
- dentifikovat klíčové prvky, jejichž ztráta v případě kybernetického útoku může mít nejvážnější následky a připravit proces jejich nahrazení. Může se jednat o zálohování dat, záložní systémy apod.
- Oddělit jednotlivé kritické systémy tak, aby je útočník nemohl snadno zasáhnout jedním útokem.
- A testovat připravenost a odolnost nastavené ochrany včetně reakce na simulovaný úspěšný útok.

Udělejte si z kybernetické bezpečnosti silné vnitrofiremní téma a věnujte mu čas.

Jan Huml
Jan Klouda

Jan Huml *je od roku 2020 technickým ředitelem společnosti SECURITAS ČR s.r.o. a následně vyhlášen TOP IT osobností roku 2020 za výzkum v oblasti termálních kamer a popularizaci digitálních bezpečnostních technologií. V letech 2014–2019 budoval monitoring a divizi bezpečnostních technologií pro Českou poštu s.p. jako technický ředitel v České poště Security s.r.o. V bezpečnostním prostředí se pohybuje od roku 2012, ve volném čase se věnuje průmyslu 4.0 a modernizaci bezpečnostních technologií v souvislosti s IT.*

Jan Klouda *je členem představenstva a viceprezidentem společnosti Vodafone Czech Republic pro právní záležitosti, řízení rizik a korporátní bezpečnost. Je členem Akademické rady Compliance Academy, členem prezidia Asociace kritické infrastruktury České republiky a členem řídícího výboru Czech Institute of Directors. Spolupracuje též s katedrou podnikového a evropského práva na Fakultě mezinárodních vztahů Vysoké školy ekonomické. Získal certifikaci Certified Fraud Examiner americké Association of Certified Fraud Examiners a Professional Postgraduate Diploma pro oblasti governance, risk a compliance u britské International Compliance Association. Přednáškovou a vzdělávací činností podporuje osvětu v oblastech jako je compliance a corporate governance.*

Audit kybernetické bezpečnosti

Michal Wojnar

Petr Šimsa

Audit kybernetické bezpečnosti může připadat nezasvěcenému člověku jako velmi specifická oblast. Při bližším pohledu se však může jednat o širokou škálu nejrůznějších postupů od revize návrhu procesů a přezkoumání shody se standardy a normami, bezpečné architektury přes kontrolu nastavení pravidel monitoringu a reakce na incidenty a krizové situace.

Nezávislý audit má v oblasti kybernetické bezpečnosti zásadní místo pro celistvé zajištění bezpečnosti dat a poskytovaných služeb. Obecným cílem auditu kybernetické bezpečnosti je identifikace slabých míst – tzv. zranitelností a nedostatků v podobě nefunkčních opatření organizace. Nezávislý interní i externí audit je rovněž vyžadovanou součástí bezpečnostních standardů, certifikací a atestací typu ISO 27001 či SOC2 a je součástí řady zákonů a regulací.

Jaké tedy má firma možnosti v případě auditu kybernetické bezpečnosti?

IT audit jako součást auditu finanční závěrky

Při rostoucí úrovni digitalizace se rovněž zvyšuje závislost účetních transakcí a vedení účetnictví na informačních technologiích. Aby se auditor mohl spolehnout na výsledky, které dané systémy prezentují, potřebuje mít alespoň základní úroveň důvěry ve finanční systémy svého klienta. Proto je standardní praxí účast specialisty, IT auditora, který otestuje a ověří základní úroveň bezpečnosti a funkčnosti finančních systémů a návazných IT procesů. Pokud IT auditor shledá dostatečnou úroveň nastavených opatření, může se spolehnout na kompletnost, přesnost a další tvrzení o výkazech a transakcích zpracovávaných finančními systémy. V případě nedostatků v IT kontrolách je pak finanční auditor nucen využít detailnější, leč manuální a méně efektivní postupy pro snížení z nich plynoucích rizik. Při větších pochybnostech může omezit či v krajním případě odmítnout vydat výrok auditora. Nutno podotknout, že IT auditor se zde zaměřuje primárně na účetní a transakční systémy a bezpečnost je řešena primárně na aplikační úrovni.

Příklad oblastí ověřovaných v rámci tohoto auditu:

- řízení přístupů a oprávnění ve finančních systémech,
- řízení a nasazování změn,
- řízení IT provozu jako např. nastavení zálohování a řízení incidentů,
- testování manuální a automatických kontrol finančního prostředí organizace.

Audit systému řízení bezpečnosti informací a procesní audit

Kybernetická bezpečnost není pouze zodpovědností „ajťáka", ale celé společnosti. Perfektní technické zabezpečení může být jednoduše obcházeno pomocí neexistujících či špatně nastavených procesů řízení přístupů do systémů, změn nasazovaných do produkčních IT systémů či procesů reakce na bezpečnostní incidenty a mnoha dalších. Z tohoto důvodu je systematické řízení bezpečnosti a procesů včetně jejich nezávislého auditu jedním ze základních kamenů bezpečné organizace. Tento typ auditu má zpravidla širší záběr ve srovnání s předchozím typem auditu. Zde bychom rádi zdůraznili i nutnost se v rámci auditu zaměřit na oblast vzdělávání. U našich zákazníků se může jednat o hodnocení přínosu phishingových kampaní, případně vzdělávacích kurzů. Co do zkoumaných oblastí se na rozdíl od auditu v rámci finančního auditu, nezaměřuje pouze na finanční systémy a zpravidla netestuje finanční kontrolní prostředí.

Příkladem oblasti pro audit tohoto typu může být:

- řízení rizik kybernetické bezpečnosti,
- organizace bezpečnosti – role a zodpovědnosti,
- řízení přístupů a oprávnění v IT systémech,
- klasifikace informací a jejich ochrana,
- řízení informačních aktiv,
- řízení bezpečnosti u dodavatelů,
- řízení kontinuity a obnovy po havárii,
- monitoring a řízení incidentů,
- bezpečnost lidských zdrojů.

Nakecali jsme mu, že má ty výkresy zavirovaný, tak s nimi teď jde k doktorovi.

Kresba: Ivan Svoboda

Technologický audit kybernetické bezpečnosti

To, že v kybernetické bezpečnosti je zásadní zajistit technická opatření zabraňující úmyslnému útoku či neúmyslné chybě, není potřeba významně zdůrazňovat. Společně s předchozím typem auditu je základem zajištění bezpečného prostředí organizace a bezpečnosti dat.

Příkladem oblastí pro audit tohoto typu může být:

- konfigurace autentizace a autorizace přístupu do aplikace,
- nastavení šifrování uložených a přenášených dat,
- nastavení monitoringu IT prostředí a pravidel vyhodnocování událostí,
- architektura IT sítě organizace,
- audit a revize zdrojového kódu aplikace,
- audit zabezpečení IT infrastruktury,
- analýza technických zranitelností.

Audit souladu dle normy či předpisu

Kontrola ze strany regulátora, interní audit nebo přezkoumání souladu s danou regulací či standardy kybernetické bezpečnosti a snížení tak rizika budoucích sankcí, jsou nejčastějšími motivátory pro „compliance" orientovaný audit – tedy audit souladu s právním řádem nebo oborovými standardy. Tento audit má za úkol identifikovat oblasti nesouladu a předjímat tak pravděpodobnost budoucího negativního dopadu na organizaci, případně zpětně šetřit již proběhlé pochybení a nesoulad s předepsanými požadavky.

Příkladem oblastí pro audit tohoto typu může být:

- audit souladu s Obecným nařízením o ochraně osobních údajů ze strany Úřadu pro ochranu osobních údajů,
- audit souladu se Zákonem o kybernetické bezpečnosti ze strany Národního úřadu pro kybernetickou a informační bezpečnost,
- externí certifikační audit souladu se standardem ISO 27001: Systém řízení bezpečnosti informací.

Ofenzivně orientovaný audit

Pro někoho to zní téměř jako extrémní varianta auditu, nicméně ve světě a (naštěstí) velké řadě českých podniků již standardní praxe: penetrační testování. Tedy testování pro tyto účely najatým tzv. „etickým" hackerem, který má za úkol systematicky identifikovat zranitelnosti v IT a procesním prostředí organizace, které by mohl využít skutečný útočník.

Příkladem tohoto typu testování může být:

- testování zranitelností webové aplikace vystavené do prostředí internetu,
- testování IT sítě, kdy se tester snaží proniknout do interního prostředí skrze veřejnou či návštěvnickou Wi-Fi,
- Red Team cvičení, kdy tester svou činností realisticky napodobuje skutečného útočníka,
- fyzické testování, kdy se tester snaží proniknout do budovy či datového centra,
- testování za užití technik sociálního inženýrství, tedy když se tester nesnaží prolomit technickou zranitelnost IT systému, ale soustředí se na lidský prvek ochrany ve snaze zajistit kýženou akci – např. zasílání podvodných e-mailů ve snaze získat od uživatele jméno a heslo do IT systému.

Závěr

Ačkoliv v praxi se často stírají rozdíly mezi jednotlivými typy auditů a jednotlivé oblasti se kombinují dle požadavku klienta či regulátora, je potřeba tyto rozdíly vnímat stejně jako zaměření konkrétního auditního projektu. Nepochopení pak v praxi vede často k mylné myšlence všeobjímajícího, tzv. „kompletního" auditu bezpečnosti a mylnému pocitu auditované strany, že je úplně v bezpečí, jelikož audit další pochybení či zranitelnosti neidentifikoval. Zde je potřeba také silně vnímat fakt, že i přes zavádějící slovo „audit" se z valné většiny nejedná o ověřovací zakázky dle standardů ISAE či IFRS.

Audit kybernetické bezpečnosti tedy můžeme a priori označit jako zakázku poradenského charakteru. Variantně může nabývat formy interního i externího auditu s přihlédnutím na jednotlivá specifika (např. Certifikační audit ISMS lze provést jen akreditovaným nezávislým subjektem). Zde bychom rádi směrem nejen k laické veřejnosti apelovali na pochopení a adekvátní rozbor rozsahu dané zakázky objednatelem tak, aby byly splněny jeho cíle a naplněno očekávání.

Petr Šimsa a Michal Wojnar
experti na kybernetickou bezpečnost
z týmu Cyber & Privacy ve společnosti PwC

Petr Šimsa *se zaměřuje primárně na analýzu, implementaci a audit systému řízení bezpečnosti Informací (ISMS) a ochranu osobních údajů (PIMS) včetně zajištění souladu se Zákonem o kybernetické bezpečnosti, GDPR a dalšími regulacemi. Je držitelem odborných certifikací CIPT, ITIL, ISO 27 Lead Implementer a M365 Security Administrator.*

Michal Wojnar *se zaměřuje na poskytování služeb v oblastech implementace ISMS, bezpečnostní audity či analýzy kybernetických rizik včetně cloudových řešení. Dlouhodobě se věnuje problematice nastavení bezpečnosti organizace, strategii a motivaci týmů v celém spektru kyberbezpečnosti. Je držitelem odborných certifikací CISA, CISSP a CEH. Pravidelně se věnuje přednáškové činnosti, vzdělávání a konzultacím pro top management a je členem PV IS2 a redakční rady peer-reviewed žurnálu DSM.*

Rozhovor s Monikou Zahálkovou, výkonnou ředitelkou České bankovní asociace

Aktivity České bankovní asociace v oblasti digitalizace

Od listopadu 2020 jste výkonnou ředitelkou České bankovní asociace, která byla založena v roce 1992 a v současnosti má 37 členů, kteří reprezentují 99 % českého bankovního sektoru. Jaké jsou vaše hlavní úkoly a vize v této nové funkci?

Česká bankovní asociace je na trhu již téměř 30 let a stojí za ní velký kus práce. Za tuto dobu se nemalou měrou zasloužila o dobrou pověst českého bankovního sektoru a je také její zásluhou, že veřejnost bankám důvěřuje. A důvěra, jak všichni víme, je v bankovnictví klíčová. Na tuto práci chci jednoznačně navázat a i nadále se aktivně podílet na rozvoji českého bankovního sektoru a celé naší ekonomiky, jakožto i finanční gramotnosti Čechů. Navíc je mým záměrem vytvořit z ČBA svěží, dynamickou a moderní organizaci, která tak bude vnímána napříč celým bankovním trhem, veřejnou správou, ale i širokou a odbornou veřejností.

Banky dlouhodobě patří k lídrům trhu v oblasti inovací a digitalizace. Na požadavky klientů reagují rychle a pružně, jejich obsluhu přizpůsobují jejich stále náročnějším požadavkům. Pokud má být ČBA bankám důvěryhodným a rovnocenným partnerem, musí s nimi držet krok. Musí kopírovat jejich dynamický vývoj, sledovat nejnovější trendy, umět přijímat a využívat moderní technologie a též se aktivně podílet na přinášení inovativních řešení v oblasti bankovnictví. První kroky už jsme v této oblasti udělali. Spustili jsme nový čtrnáctidenní newsletter pro všechny, které bankovnictví zajímá. Také jsme uvedli nový diskusní pořad ČBA FOCUS. Do něj si zveme zajímavé osobnosti z bankovnictví, ale i třeba ze státní správy, a dáváme jim pod vedením zkušeného moderátora prostor pro objektivní diskusi nad aktuálními tématy. První díl už máme za sebou a zasvětili jsme ho digitalizaci českého státu a jak s ní pomáhají banky. Pořad je ke zhlédnutí na našem YouTube kanále nebo si ho můžete poslechnout jako podcast na Spotify. Další novinky chystáme i v oblasti vzdělávání, ale zatím je brzy cokoliv prozrazovat.

Ještě ve vaší předchozí funkci ředitelky Institutu členů správních orgánů CoID jsem absolvoval velmi zajímavý seminář o kybernetické bezpečnosti. Jaká je podle vašeho názoru znalost kybernetických rizik mezi členy top managementu českých firem a jakou prioritu dávají opatřením pro jejich minimalizaci?

Monika Zahálková *vystudovala Vysokou školu ekonomickou v Praze. Působila jako jednatelka CG Institutu a ředitelka Institutu členů správních orgánů (Czech Insstitute of Directors). Mezi lety 2018 až 2019 byla členkou představenstva mediálního domu Economia. Od listopadu 2020 zastává funkci výkonné ředitelky České bankovní asociace.*

V průběhu let se situace zlepšuje. Stále jsou sice organizace, které do kybernetické bezpečnosti investují méně, než by měly, v obecné rovině však tento typ hrozeb vnímají takřka všichni. Zejména korporace se zahraničním vlastníkem mají zkušenost s kybernetickými incidenty a umí si spočítat, že výpadek jejich služeb či provozu je stojí mnohem více, než kolik stojí nástroje na posílení kybernetické bezpečnosti. Vědí, že nejde jenom o náklady na odstranění útoku, ale také o hrozbu ztráty dat, únik osobních údajů, citlivých informací a další s tím související následky.

Zejména telekomunikační operátoři, finanční instituce a obecně společnosti zalistované na některém z kapitálových trhů či společnosti s diverzifikovaným portfoliem služeb a náročným investičním

profilem vědí, že jeden kybernetický útok může na dlouhou dobu zastavit jejich činnost či je z podnikání prakticky vyřadit. Také proto v jejich výročních zprávách vidíte velmi často zmínku o kybernetických hrozbách na jednom z prvních míst potenciálních rizik. Prakticky neznám žádného vysoce postaveného manažera z velké korporace, který by kybernetické hrozby bagatelizoval a nechtěl je řešit.

Prevence obecné finanční a kybernetické kriminality je jednou ze čtyř hlavních oblastí činnosti, které o sobě ČBA uvádí na svých webových stránkách. Co to konkrétně představuje?

Naše zaměření, nejenom v této oblasti, vyplývá z potřeb našich členů, ale také z potřeb veřejnosti. Na jedné straně tedy budujeme společně se státem odpovídající legislativní prostředí, regulační

Hugo a Sally se baví o detailním testování

4. Důkazní informace vs. podklad klienta

Jak si náš nový asistent vede při samotném provádění detailních testů?

Docela dobře. Jen jsme si museli vyjasnit, co představuje důkazní informaci při detailním testu.

V čem byl problém?

Testoval dohadné účty pasivní obsahující doúčtování za odebranou elektrickou energii a nevyfakturované dodávky služeb. Do spisu založil výpočty těchto odhadů provedené klientem a považoval to za dostatečnou důkazní informaci.

Samozřejmě, že dotazování je základní a klíčová auditorská technika. Ale získané vysvětlení klienta ve formě výpočtu je informací, která musí být ověřena, aby se stala důkazní informací.

Vysvětloval jsem mu, že ověření dohadu typicky znamená získat konečnou fakturu od dodavatele.

Ještě to s ním prober, protože pokud konečná faktura není k dispozici, tak je nutné ověřit výpočet klienta. Musí ho přepočítat a zároveň ověřit vstupní data a předpoklady. U elektřiny to třeba může být odečet stavu elektroměru a smlouva.

Proberu. A taky se ještě ujistím, že dobře chápe, že některé techniky získávání důkazních informací mohou být lepší než pouhý sběr formálních dokladů. Třeba fyzická inspekce pro ověření existence či znehodnocení majetku.

-SpM-

rámec, který umožňuje bankovnímu sektoru budovat prostředí důvěry, bez kterého nelze úspěšně finanční služby poskytovat. A to jak v oblasti standardní, řekněme fyzické, bezpečnosti, tak i na úrovni mezinárodní spolupráce při potírání kybernetické kriminality. Na straně druhé se společně snažíme působit na klienty, kteří se zejména v dnešní době, kdy se celá řada našich aktivit přesunula do kyberprostoru, stávají cílenými objekty velmi sofistikovaných útoků. Jde o to, abychom je dokázali nasměrovat k uvědomění, že jejich málo obezřetné chování a nízká ochrana jejich elektronických zařízení vede k tomu, že právě oni jsou v drtivé většině právě tím nejslabším článkem v zabezpečení jejich finančních prostředků.

Jak ČBA spolupracuje v této oblasti se státními institucemi, jako je Policie ČR, FAÚ, NÚKIB, ÚOOÚ apod.?

K mé velké radosti velmi úzce. Nerada bych v rozhovoru vyzdvihovala jednu konkrétní instituci. Obecně platí, že spolupráce s regulátory funguje nejenom ve formální, ale i neformální rovině. A to téměř každodenně. Pokud budu přeci jen konkrétnější, tak například s Policií ČR má asociace podepsáno memorandum o vzájemné spolupráci a nastavení komunikace nejenom v oblasti prevence. S institucemi, které jsou pro banky regulátory v oblasti kybernetické bezpečnosti, tedy s Českou národní bankou a s Národním úřadem pro kybernetickou bezpečnost, jsme také pravidelně v kontaktu. Obě tyto instituce s námi v minulých letech spolupracovaly např. při realizaci testů připravenosti bank na řešení masivnějších hackerských útoků zaměřených na bankovní sektor. Zástupci Finančního analytického úřadu, státního zastupitelství a Policie ČR jsou pravidelnými hosty zasedání Komise pro bankovní a finanční bezpečnost, na kterých se zástupci bank diskutují nejen legislativní změny a z nich vyplývající povinnosti v oblasti boje s praním špinavých peněz a financováním terorismu, ale i poznatky z proběhlých útoků – ať už na pobočky, bankomaty či elektronické platební systémy, nebo přímo na klienty. Nesmím také zapomenout zmínit, že ČBA ve spolupráci s FAÚ také pravidelně školí v oblasti praní špinavých peněz a kyberbezpečnosti zaměstnance bank.

Jak je ČBA aktivní v oblasti prevence finanční a kybernetické kriminality například formou vzdělávání, seminářů metodické podpory apod.?

Jak už jsem naznačila, prevence finanční a kybernetické kriminality je nedílnou součástí naší činnosti. Již přes dvacet let pořádáme odborný seminář „Prevence finanční kriminality“, kde si s odborníky v této oblasti vyměňujeme řadu užitečných poznatků. Ty se pak snažíme uplatnit nejenom v práci příslušných útvarů bank, ale také je přenést do vzdělávacích programů a projektů, které ČBA pravidelně připravuje pro širokou veřejnost, od dětí po seniory. Každoročně také měříme tzv. Index kyberbezpečnosti ČBA. Jeho cílem je zjistit, jak si Češi v oblasti kyberbezpečnosti stojí, a na základě těchto výsledků se pak zaměřit na jejich cílenou edukaci. V loňském roce dosáhli Češi ve zmíněném testu jen asi 60% úspěšnosti, v praktickém kvízu dokonce pouze 43 %. Z výsledků vidíme, že nejvíce jsou ohroženi mladí, kteří si nebezpečí nepřipouštějí a také nemají tolik životních zkušeností. Z těchto důvodů ve spolupráci s našimi členskými bankami každoročně organizujeme projekt Bankéři do škol, kdy se zaměstnanci bank vydají tuto problematiku formou interaktivních workshopů vyučovat do středních a základních škol po celé České republice. Projekt má velký úspěch a každý rok se nám do něj zapojuje stále více škol, i když loni nám to pandemie trochu zkomplikovala...

V oblasti finanční bezpečnosti, konkrétně pak fyzické bezpečnosti, také ČBA realizovala v minulosti projekt „Lekce komisaře Maigreta“. Cílem tohoto projektu bylo vytvořit školící videa pro zaměstnance bank, reagující na v té době vysoký nárůst případů loupežných přepadení na území ČR. Toto školení je v bankách využíváno dodnes.

Jak je tato oblast důležitá pro vás osobně, setkala jste se někdy s nějakým bezpečnostním incidentem, se kterým nás můžete obecně seznámit?

Ani já nejsem výjimkou a již jsem se, asi jako každý, s phishingovými útoky setkala. Tyto útoky mají mnoho podob, od podvodných e-mailů sepsaných špatnou češtinou, až po bohužel v poslední době i velmi sofistikované a cílené kriminální aktivity. I já jsem zjistila, že existují podvodné e-shopy plné atraktivního zboží s úžasnými slevami, jejichž jediným cílem je získat od vás údaje o vaší platební kartě za účelem jejího zneužití.

Našim programátorům se podařilo hacknout náš robotický vysavač tak, že nám teď při auditu pomáhá vést auditorský spis.

Kresba: Ivan Svoboda

V poslední době se objevuje nový fenomén tzv. vishing, který je obzvlášť zákeřný, protože pracuje s vašimi emocemi. Jedná se o útoky v podobě telefonických hovorů pachatelů, kteří se vydávají za pracovníky bank. Útočníci volají pod záminkou, že banka zjistila útok na klientův účet nebo platební kartu s tím, že je nutné s jeho pomocí provést jejich okamžité zablokování. Cílem těchto útoků je klienta nejprve dostatečně vyděsit, tedy vyvolat v něm pocit, že jsou aktuálně ohroženy jeho úspory a následně mu sdělit, že vše je možné s jeho okamžitou pomocí ještě zachránit. Klient tak po prvním šoku nabývá pocit spásy, že mu chce jeho banka pomoci a s volajícím začne spolupracovat. Ve snaze ochránit své finance pak prozradí všechny přístupové údaje. Ty přitom banky po svých klientech nikdy nevyžadují. Kromě toho banky samy, pokud například identifikují riziko možnosti zneužití platební karty klienta, tyto karty blokují a žádné údaje od klienta k jejich zablokování znát nepotřebují.

Osobně se zájmem sleduji projekt „Bankovní identita“, ve kterém je ČBA aktivní a který nabízí veřejnosti možnost elektronické identifikace prostřednictvím bankovní identity i do nebankovních informačních systémů, například i do Portálu občana apod. V jaké fázi se projekt aktuálně nachází?

Tento projekt považuji za jeden z nejvýznamnějších za několik posledních let. V loňském roce jsme po dvouletém úsilí dokončili jeho legislativní rámec a do začátku letošního roku jsme ve spolupráci s Ministerstvem vnitra, Ministerstvem financí a Správou základních registrů pracovali na implementaci. To vše vyústilo ve zdokonalení náročného akreditačního procesu, který banky, jakožto poskytovatelé bankovní identity, musí podstoupit v souladu se zákonem o elektronické identifikaci. Akreditaci získalo již pět bank, které nyní ověřují a registrují identitní prostředky svých klientů prostřednictvím státní Národní identitní autority NIA. To probíhá postupně. Denní kapacita systému umožňuje registrovat maximálně 50 tisíc identit. Přesto už jich je od začátku roku více než dva miliony převážně od dvou bank. S trochou zjednodušení tedy můžeme říct, že stejně snadno, jako se přihlašují do internetového bankovnictví, se nyní mohou prokazovat i ve světě ostatních, nebankovních online služeb přes dva miliony klientů.

Bankovní identitu mohou klienti používat při přihlašování na portály státu – samozřejmě jen tam, kde jim to stát umožní. Poslední novinkou je možnost podat daně prostřednictvím portálu Moje daně Ministerstva financí. Dalším připravovaným projektem je Sčítání lidu 2021. Za nejlepší rozcestník, kde si klienti mohou pomocí bankovní identity vyřídit nejrůznější záležitosti směrem ke státu online, považuji Portál občana, kam Ministerstvo vnitra postupně přidává další a další služby a šetří nám tak cesty na úřady.

Pokud tomu dobře rozumím, tak se funkce bankovní identity budou postupně otevírat i pro komerční využití společnostmi, které provozují informační systémy vyžadující spolehlivou elektronickou identifikaci uživatelů (například e-shopy apod.). Jak to bude fungovat?

Podle informací, které máme, se bankám podařilo dosáhnout shody na vybudování jednoho společného podniku Bankovní identita a.s. – BANK ID, jehož prostřednictvím banky firemnímu sektoru nabídnou jedno řešení pro spolehlivou, rychlou a bezpečnou online identifikaci jejich klientů či zákazníků a mimo to také elektronický podpis. Díky tomu tak bude například mobilní operátor či poskytovatel energií po uzavření smluvního vztahu s tímto „agregátorem“ moci vybudovat pouze jedno standardizované technologické rozhraní a jeho prostřednictvím tak spolupracovat se všemi bankami, které budou identitní služby poskytovat. Jsem optimista a věřím, že se bankám a společnosti Bankovní identita vše podaří připravit tak, abychom mohli bankovní identitu v soukromém sektoru používat již počátkem druhé poloviny letošního roku.

Co byste na závěr vzkázala či poradila auditorům s ohledem na bezpečnost využívání ICT osobně i u svých klientů?

V prvé řadě se řídit bezpečnostními doporučeními provozovatelů IT systémů, bank, mobilních operátorů, zkrátka všech institucí, jejichž výrobky a služby využíváme. Těch bezpečnostních opatření není moc, v principu se opakují, ale pokud je dodržujeme, ochráníme tím nejen naše data a soukromí, ale i data našich klientů, kteří nám je s důvěrou svěřili. A tuto důvěru bychom neměli zklamat.

Rozhovor vedl
Ladislav Mejzlík

Rozhovor s Markem Richterem, partnerem ve společnosti PwC Česká republika

Aspekty kybernetické bezpečnosti při auditu finančních institucí

Vždy, když dělám s někým rozhovor, tak mě zajímá, jaká byla jeho cesta k aktuální pracovní pozici, a proto mi to nedá a zeptám se i vás. Kudy vedla vaše cesta od absolvování oboru ekonomika a řízení na Vysokém učení technickém v Brně, k pozici partnera v auditu PwC?

Do pražské kanceláře, tehdy Pricewaterhouse, jsem nastoupil na podzim 1992, hned po absolvování vysoké školy. O auditu jsem nic nevěděl, na vysokých školách se v té době audit neučil. Při přijímacím pohovoru do PW mě zaujalo, že hned po nástupu do zaměstnání budu mít možnost hovořit s lidmi, kteří velké firmy vedou. To bylo nesmírně zajímavé a je to podle mě atribut, který do auditu láká absolventy i v současnosti.

„Divoká" devadesátá léta přinesla mimo jiné obrovskou vlnu zahraničních investorů, se kterými jsme intenzivně pracovali. Úžasné projekty jsme měli i s ryze českými firmami, které se v té době nadechovaly k expanzi. Mezi tím jsem si však odskočil do EY, kde jsem strávil i odbornou stáž v londýnské kanceláři se zaměřením na finanční služby. Přičichnout trochu k světu velkých financí bylo nesmírně zajímavé. Po návratu z Londýna jsem nastoupil už do PwC v Brně. I zde jsem se však hodně věnoval finančním institucím, včetně privatizací velkých bank a pojišťoven jak v ČR, tak i na Slovensku. Měl jsem však možnost pracovat i s klienty téměř ze všech oborů podnikání. Takže ta cesta byla poměrně přímá.

Přebral jste funkci vedoucího oddělení auditorských služeb pro sektor finančních institucí PwC po Petru Křížovi, který byl, mimo jiné, také prezidentem Komory auditorů ČR a prezidentem FEE (nyní Accountancy Europe). Jak vy osobně vidíte význam angažovanosti významných odborníků z praxe v činnosti a řízení profesních organizací účetních a auditorů?

Ten přínos je zásadní. Obecně lidé z praxe přinášejí jiné názory a pohledy na věc. A to nejen při řízení našich profesních organizací. Osobně to vidím například na fungování výborů pro audit, které jsou složeny z odborníků s různorodými zkušenostmi ať už z auditorské praxe nebo s praktickými zkušenostmi z daného oboru podnikání.

Toto číslo časopisu Auditor je věnováno kybernetické bezpečnosti. Jak vy osobně z pozice auditora vnímáte nárůst složitosti informačních a komunikačních technologií a rizik, které z jejich používání vyplývají?

Ing. Marek Richter *vystudoval VUT v Brně, obor ekonomika a řízení. Je členem Mezinárodní asociace certifikovaných účetních (ACCA) a auditorem registrovaným v Komoře auditorů České republiky. Je partnerem PwC a v současnosti vede oddělení auditu finančních institucí PwC.*

Informační technologie udělaly za posledních několik let obrovský skok kupředu. To znamená, že při auditech musí být nasazeno daleko více IT expertů, než bývalo potřeba dříve. Já pracuji s několika klienty, kteří mají několik desítek IT systémů nebo aplikací, které významně ovlivňují oblast finančního výkaznictví. Auditor musí ověřit efektivní fungování těchto systémů pro účely svého auditu. Finanční instituce digitalizují celé oblasti, jako je například platební styk nebo třeba spotřební úvěry. To pak dává auditorům možnost v daleko větší míře využívat digitální nástroje k otestování příslušných kontrol, transakcí nebo zůstatků. Firmy musí mít dobře ošetřeny oblasti jako je správné nastavení přístupových práv nebo řízení změn, musí mít vhodné struktury hesel. To je stále základ. Data jsou horké zboží. Zneužití nebo přímo krádež dat považuji za největší riziko.

A nejste vy náhodou silniční kontrola Kybernetické bezpečnosti?

Kresba: Ivan Svoboda

Myslíte si, že jsou si firmy těchto nových rizik a jejich možných důsledků dostatečně vědomy, nebo mají tendenci je spíše podceňovat?

Povědomí o těchto rizicích se významně zvýšilo. Představenstva si již jsou dobře vědoma, že např. zneužití klientských dat s sebou, mimo jiné, nese obrovské reputační riziko. Přispěly k tomu i hodně medializované a bohužel často úspěšné kybernetické útoky z poslední doby. Samozřejmě přístup se liší společnost od společnosti, byť v některých sektorech jsou kybernetická rizika vnímána vedením obzvlášť citlivě, a to i díky regulaci.

Ze zkušenosti vím, že od uvědomění si rizik k efektivním opatřením pro jejich minimalizaci může vést dlouhá cesta. Myslíte si, že firmy pro svou kybernetickou bezpečnost dělají dost?

Velké firmy mají vybudované vlastní týmy a využívají podle potřeby služby externích poradců. U menších firem je situace často odlišná. Bezpečnost něco stojí. U menších firem se často posuzuje investice do kybernetické bezpečnosti v krátkodobém časovém horizontu, což vede často k podhodnocení vynaložených prostředků v této oblasti. Náklady na posílení kybernetické bezpečnosti jsou u velkých firem významné. Všichni ale bojují s nedostatkem expertů, například manažer kybernetické bezpečnosti je na pracovním trhu velice nedostatkovým zbožím. A mimochodem, k posílení kybernetické bezpečnosti přispívají hodně i banky tím, že tlačí na klienty, třeba ze segmentu malých a středních firem, aby zlepšili zabezpečení svého IT prostředí využívaného pro internetové bankovnictví. Vždy můžete dělat více, ale osobně vnímám v této oblasti celkově posun dopředu.

Řídíte audity ve finančních institucích, které jsou z hlediska kybernetické bezpečnosti exponované, ale také jí věnují vyšší pozornost a podléhají přísnější regulaci. Máte srovnání i s jinými sektory?

V současnosti pracuji především s velkými finančními institucemi, především s velkými bankami a pojišťovnami. Zde je už několik let vnímána kybernetická bezpečnost jako klíčová oblast a kybernetická rizika jsou na rizikových mapách uváděna jako největší riziko jejich podnikání. Tomu odpovídá personální obsazení i finanční prostředky vynaložené na ochranu finančních institucí před kybernetickými hrozbami. Kybernetické hrozby a statistika kybernetických útoků jsou diskutovány na téměř každém jednání vrcholového vedení. Myslím si, že práce s kybernetickými riziky ve finančních institucích je ve srovnání s jinými odvětvími obecně na špičce. Finanční instituce jsou silně regulovány, to platí i pro oblast bezpečnosti. Někdy však může být „compliance“ vyvolaná regulačními pravidly na úkor toho, jaké služby by

technologie mohly poskytovat a jejich dalšího rozvoje. Prostě kapacity, které jsou věnovány „compliance“, chybí jinde.

Cítíte ve své práci nárůst objemu práce auditora věnované kybernetické bezpečnosti jak u klientů, tak i u vás osobně?

Oblast auditu IT a zmapování IT kontrol a jejich otestování je určitě rostoucí oblastí. Na mých auditech vynakládáme na tuto oblast i čtvrtinu celkového času týmu stráveného na zakázce. V rámci této práce se věnujeme i kybernetickým rizikům. Snažíme se pochopit, kde vidí v této oblasti klíčová rizika představenstvo, bavíme se s klienty o tom, jak se snaží tato rizika omezovat. Vyhodnocujeme případný dopad těchto rizik na auditovanou účetní závěrku. Navrhujeme doporučení na zlepšení. Ano, objem práce v této oblasti roste.

Zaregistroval jste akceleraci problému bezpečnosti ICT v souvislosti s nárůstem digitalizace a práce z domova v důsledku koronaviru?

Nepochybně přibylo útoků na zdravotnická zařízení. Zvýšilo se množství útoků vedených přes třetí strany (třeba právě přes firmy zajišťující dodávky bezpečnostních technologií a infrastruktury). To znamená, že pro manažery IT a kybernetické bezpečnosti se problematika zajištění bezpečnosti rozšiřuje i mimo jejich vlastní společnosti, musí si zajistit kvalitu a vysokou úroveň zabezpečení i v celém řetězci svých dodavatelů. Je to jako s kovidem, vir můžete chytit od kohokoli ve vašem okolí. Vím o tom, že některé menší společnosti měly problémy při přechodu na práci z domova, které postupně řešily. Většina mých klientů ale přešla na práci z domova poměrně hladce. I proto, že do oblasti IT bezpečnosti a digitalizace velice výrazně investovali dávno před vypuknutím pandemie. Kromě nutnosti posilovat kapacitu internetového připojení, jeho lepší zabezpečení a třeba nutnosti dovybavit zaměstnance laptopy, jsem osobně nějaké zásadní problémy nezaznamenal.

Problém kybernetické bezpečnosti se netýká jen auditorských klientů, ale také bezpečnosti auditora jako takového. Postupuje aktivně v ochraně svého IT systému i PwC a jak to pociťujete na práci svého auditorského týmu v době koronaviru?

Oblast bezpečnosti je pro nás zásadní. Systémy PwC jsou zabezpečeny s využitím nejnovějších poznatků. Samozřejmě v dnešní době i my pracujeme převážně z domova. Posilujeme dále oblast digitální komunikace a elektronické výměny dat s klienty. I v této době pokračujeme v inovacích, používáme čím dál více auditní nástroje pro pokročilé zpracování a vizualizaci velkých objemů dat, začínáme využívat umělou inteligenci, třeba pro hledání anomálií v hlavní knize, používáme nástroje pro automatizaci přípravy dokumentů (např. zpráv auditora).

Najímáte si v PwC na oblast bezpečnosti ICT odborníky nebo dáváte přednost budování vlastního týmu?

Máme vlastní tým. Náš tým IT auditorů a odborníků na kybernetickou bezpečnost má v Praze a Brně kolem 80 expertů a dále roste. V rámci poradenských projektů se členové tohoto týmu zaměřují i na samostatné projekty v oblasti kybernetické bezpečnosti.

Máte nějaké osobní zkušenosti s bezpečnostními incidenty v oblasti ICT, o které byste se s námi mohl podělit?

Bezpečnostní incident je vždy velice nepříjemná a stresující zkušenost. Jako řada jiných jsem zaznamenal několik phishingových e-mailů, které se podařilo s pomocí kolegů z centra sdílených služeb zaměřujících se v PwC na tuto oblast, úspěšně neutralizovat. Vidím, že mí klienti zaznamenávají zvyšující se počet útoků různé složitosti. A není to jen o útocích na počítače a „klasickou" IT infrastrukturu. V poslední době byly například v celé Evropě zaznamenány sofistikované útoky na bankomaty.

Co byste na závěr vzkázal či poradil auditorům s ohledem na kybernetickou bezpečnost?

Aby tuto oblast při auditech nepodceňovali. Pořád platí, že příležitost dělá zloděje. Společnost, která není řádně zabezpečena proti kybernetickým hrozbám, je snadný terč. Je proto nezbytné se s klienty o této oblasti bavit a tam, kde to je nutné, zvyšovat jejich povědomí o souvisejících rizicích. Už v případě útoku, který vyřadí IT systém i malé společnosti, jde o velké peníze a škody. Auditor může klientům pomoci těmto škodám předcházet.

Rozhovor vedl
Ladislav Mejzlík

Test: Jak jste připraveni na kybernetické hrozby?

Vyberte vždy jednu odpověď, která je z nabízených podle vašeho názoru nejsprávnější.

Test můžete vyplnit elektronicky na adrese ffu.vse.cz/test přičemž vaše odpovědi, které obdržíme do 30. dubna 2021, zařadíme do slosování o reklamní předměty. O výhře vás pak informujeme e-mailem, který zadáte na začátku testu.

1. Máte home-office a pro svou práci můžete použít jak vlastní počítač, tak i pracovní, který vám k tomuto účelu poskytl zaměstnavatel. Používání vlastního zařízení (počítače, mobilu apod.) k práci je obvykle:
a) méně rizikové než používání zařízení od zaměstnavatele
b) stejně rizikové jako používání zařízení od zaměstnavatele
c) rizikovější než používání zařízení od zaměstnavatele

2. Kterému z následujících subjektů víc hrozí, že se stane obětí kybernetického útoku?
a) malá firma
b) velká firma

3. Registrujete se do důležitého informačního systému a přemýšlíte, jaké heslo si zadat. Které z následujících hesel je nejbezpečnější?
a) 123456
b) drak
c) 10Ma1ych%C3rn0usku!
d) sppopzlszmpnkpncdzvsrbvnshasd
e) MilujiTe
f) He11oKitty
g) 1q2w3e4r

4. Kdo je pro vaši organizaci větší kybernetickou bezpečnostní hrozbou?
a) lidé uvnitř firmy
b) lidé z vnějšku firmy
c) nehraje to roli, může to být kdokoliv

5. Vyberte tvrzení, které je podle vás nejpřesnější:
a) Konkrétní personál (například IT pracovníci) musí umět rozpoznat známky kybernetického útoku.
b) Pokud firma používá vhodný antivirový software, personál nemusí umět rozpoznat známky kybernetického útoku.
c) Veškerý personál musí umět rozpoznat známky kybernetického útoku.

6. Písmeno „s“ v označení protokolu na začátku adresy URL (https:// místo http://) znamená, že:
a) tento web má speciální vysoké rozlišení
b) informace odesílané z tohoto webu a na tento web jsou šifrovány
c) web je aktualizován na nejnovější dostupnou verzi
d) přístup na tento web je omezen jen na přihlášené uživatele
e) nic z výše uvedeného

7. Který z následujících příkladů představuje útok nazývaný „phishing“?
a) odeslání e-mailu, jehož odesilatel je maskovaný tak, aby vypadal jako e-mail od někoho, koho příjemce zná
b) rozesílání odkazu na falešnou webovou stránku, která vypadá téměř stejně jako skutečný web, aby přiměl uživatele k zadání jeho přihlašovacích údajů
c) odeslání SMS zprávy, která obsahuje škodlivý odkaz maskovaný tak, aby vypadal jako oznámení, že daná osoba vyhrála nějakou soutěž
d) vše výše uvedené
e) nic z výše uvedeného

8. Skupina počítačů, které jsou vzájemně propojeny v síti a hackeři je používají ke krádeži informací, se nazývá:
a) ransomware
b) rootkit
c) DDoS
d) botnet
e) spam
f) phishing

9. Kybernetický útok, při kterém mají hackeři přístup k počítači někoho jiného tak, že zašifrují jeho soubory a data a požadují od uživatele výpalné za jejich dešifrování se nazývá:
a) botnet
b) rootkit
c) DDoS
d) spam
e) ransomware
f) phishing

10. Vypnutí funkce GPS na vašem chytrém telefonu zabrání jakémukoli sledování jeho polohy.
a) Je to pavda.
b) Není to pravda.
c) Záleží na operačním systému telefonu.

11. Které z následujících kybernetických rizik se používáním virtuální privátní sítě (VPN) minimalizuje nejvíce?
a) používání nezabezpečených Wi-Fi sítí
b) sledování komunikace
c) phishingové útoky
d) rozesílání spamu

12. V počítači se vám zobrazilo oznámení, že je k dispozici aktualizace pro důvěryhodnou aplikaci, kterou jste si instalovali a používáte ji. Který z následujících postupů je nejsprávnější?
a) Není třeba dělat nic, protože se aktualizace automaticky nainstaluje i přesto, že to neuděláte ručně.
b) Není třeba dělat nic, protože o instalaci se postará IT oddělení (specialista) vaší firmy.
c) Na nic nebudu klikat, protože oznámení může být součástí kybernetického útoku.
d) Není třeba se tím zabývat, protože aktualizace přinášejí pouze nové funkce nebo nový vzhled aplikací.
e) Okamžitě přeruším svou práci a nainstaluji aktualizaci.
f) Aktualizaci je třeba nainstalovat bez zbytečného odkladu, protože její absence může zvyšovat riziko kybernetického útoku na firmu.

13. Při odchodu z kanceláře najdete na chodbě USB flešku. Co uděláte?
a) Zvednete ji a zasunete do svého počítače, abyste zjistili, komu patří, a mohli mu ji vrátit.
b) Necháte ji ležet tam, kde je, aby se pro ni mohl pro ni vrátit ten, kdo ji ztratil.
c) Předáte ji na firemní recepci, aby zařídili vše potřebné.
d) Vezmete si ji domů a budete ji používat.

14. Váš počítač byl právě infikován ransomwarem a hacker požaduje 1 000 Euro, než vám jej znovu uvolní. Co uděláte?
a) Informujete o tom e-mailem vašeho firemního IT specialistu.
b) Pokusíte se toho zbavit antivirovým programem, než to někdo zjistí.
c) Zaplatíte požadované výkupné, protože je to nejrychlejší a nejjednodušší způsob, jak dostat své soubory zpět a pokračovat v práci.
d) Okamžitě odpojíte počítač od sítě.

15. Váš počítač již neobsahuje ransomware, takže můžete pokračovat ve své práci. Co uděláte jako první?
a) Co nejdříve si vytvoříte zálohu svých dat z počítače.
b) Pokračujte v práci jako obvykle, protože počítač je již „vyčištěný".
c) Konečně si prohlédnete tu nalezenou USB flešku, protože stále nevíte, komu patří.
d) Je to jedno, protože problém již byl vyřešen.

16. Po všech těch problémech už konečně jedete vlakem domů a po cestě z nádraží si uvědomíte, že jste ve vlaku zapomněli svůj mobil. Co uděláte?
a) Zavoláte na linku ztrát a nálezů, jestli ho někdo nenašel a neodevzdal.
b) Zavoláte na ztracený telefon a domluvíte si schůzku a předání telefonu s osobou, která jej našla.
c) Okamžitě telefon na dálku zablokujete.
d) Zavoláte svému mobilnímu operátorovi a poradíte se s ním na dalším postupu.

17. Večer si sednete k notebooku a začnete vyřizovat e-maily. V jednom z nich vám píše kamarád, že vám přeje všechno nejlepší k narozeninám a přikládá přání, na které když kliknete, tak uvidíte, co se bude dít dál. Co uděláte?
a) Na přílohu e-mailu nekliknete ani na email neodpovídáte a ihned jej smažete.
b) Kliknete na přílohu, abyste se podívali, co vám kamarád posílá k narozeninám.
c) E-mail přepošlete svým přátelům, aby věděli, jak hezké přání jste dostali.
d) Na e-mail příteli odpovíte s prosbou, aby vám takové e-maily neposílal.

Test připravil Ladislav Mejzlík

Řešení: 1c, 2a, 3c, 4a, 5c, 6b, 7b, 8d, 9e, 10b, 11a, 12f, 13c, 14d, 15a, 16c, 17a

Digitální platformy pro zprostředkování bankovních konfirmací

Někteří auditoři se při svých auditech již setkali s tím, že při žádosti o bankovní konfirmaci byli odkázáni na využití zprostředkující digitální platformy. Jedná se o novinku, která má nahradit dosavadní postupy pro získání bankovní konfirmace v listinné podobě s využitím služeb pošty, při kterých auditor získal od klienta kontaktní údaje na banku či jejího pracovníka a podepsaný konfirmační dopis, který sám následně poštou zaslal bance a opět poštou obdržel od banky listinnou odpověď. Místo toho je auditor požádán, aby žádost o bankovní konfirmaci podal elektronicky prostřednictvím digitální platformy, která tuto žádost předá bance a banka auditorovi opět prostřednictvím této platformy odpoví.

Proč k této digitalizaci celosvětově dochází? Důvodů je několik. Z pohledu banky se jedná o snahu zefektivnit a centralizovat celý proces vystavování odpovědí na konfirmační žádosti. Místo toho, aby bance přišly tisíce konfirmačních žádostí v listinné podobě na různé pobočky, chodí veškeré žádosti na centrální adresu a banka může vyčlenit pracovníky jen na tuto činnost a lze, s využitím dalších nástrojů, celý proces automatizovat. Jako klíčovou výhodu pro auditory všechny platformy uvádí spolehlivost těchto konfirmací a ochranu auditora před podvodnými odpověďmi. Pokud auditor zašle přes platformu konfirmační žádost bance, která s platformou spolupracuje, tak mu platforma zajišťuje, že jeho žádost skutečně obdrží daná banka a že odpověď banky nelze nijak před doručením auditorovi pozměnit. To konfirmace v listinné podobě zaručit nemohou. Další uváděnou výhodou pro auditora je zajištění auditní stopy, archivace celé komunikace, poskytnutí detailního přehledu o stavu všech zaslaných konfirmačních žádostí a také rychlejší dodání odpovědí oproti listinné podobě, protože i o upomínání se většinou stará automaticky přímo daná platforma. Žádosti lze také zasílat s předstihem.

Vyřizování konfirmací přes digitální nebo online portál má však několik nevýhod: tyto portály zatím nedisponují mutací v českém jazyce, je tedy nutné se spokojit s rozhraním v angličtině, případně v jiném ze světových jazyků. Dále za zprostředkování konfirmace platí auditor, přičemž platba klienta bance za vystavení konfirmace zůstává většinou ve stejné výši. Pro zaplacení zprostředkování konfirmace je nutné použít platební metody používané portálem (nejčastěji platební kartu). V neposlední řadě je nutné, aby měl auditor povědomí o elektronických dokumentech a jejich důvěryhodnosti, což dále souvisí s vyhodnocením důvěryhodnosti celé příslušné platformy (viz také článek *Využití online platforem pro cirkulaci auditních konfirmačních dopisů* v sekci Na pomoc auditorům v čísle 2/2021 časopisu Auditor).

S žádostí o využití online platformy se v Česku setkali zejména auditoři, jejichž klienti mají účet u ČSOB, která nově spolupracuje s platformou (webovým portálem) confirmation.com kanadské společnosti Thomson Reuters Company.

Platforma umožňuje posílat elektronické konfirmační žádosti všem bankám, které s confirmation.com spolupracují bez omezení na zemi, ve které má sídlo klient, banka nebo auditor. Zejména v USA je to často jediný bankou akceptovaný způsob pro poskytnutí konfirmace auditorovi. V České republice zatím smlouvu s confirmation.com podepsali kromě ČSOB i Deutsche Bank a HSBC. Dle našich informací ČSOB žádá klienty, aby využili tuto platformu pro zasílání konfirmačních žádostí, ale stále přijímá i klasické listinné žádosti. Platforma confirmation.com dle svého vyjádření aktivně vyjednává s dalšími významnými bankovními institucemi v České republice, aby se do její sítě zapojily. Lze tak očekávat, že v budoucnu budou tento způsob komunikace preferovat i ostatní banky, a je možné, že některé budou tuto formu i vyžadovat.

Platforma confirmation.com podle vlastního vyjádření splňuje přísné bezpečnostní standardy. Celý systém prochází ročně 450 různými bezpečnostními prověrkami a prověrkami pro ověření souladu s požadavky různých nařízení či standardů (SOC 1, 2 a 3; ISO 27001, TRUSTe Privacy policy, EU Privacy shield, GDPR compliance, PCI DSS Level 2 Compliance atd.). Veškerá komunikace včetně klientem poskytnutých podpisových vzorů, přiložených dokumentů a konfirmací je šifrovaná a zabezpečená před neautorizovaným přístupem. Technické řešení zajišťuje, že konfirmace se od třetí strany (banky) dostává přímo k auditorovi. Tím je systémově vyloučeno, že by s konfirmací mohl jakkoli manipulovat klient.

Portál confirmation.com umožňuje podávat různé druhy konfirmačních žádostí. Kromě bankovních ho lze využít i pro konfirmace pohledávek, závazků nebo právníků. Nicméně v České republice jsou do systému zatím zaregistrovány jen uvedené banky. Zasílání žádostí neregistrovaným subjektům je sice možné, ale auditor při něm ztrácí klíčovou výhodu, kterou je jistota identity odpovídající strany. Pouze pro subjekty registrované v platformě (spolupracující subjekty, in-network responder) je zodpovědností platformy ověřit jejich identitu včetně správnosti kontaktních údajů.

U bankovních konfirmací nabízí platforma confirmation.com dva typy: konsolidovaná konfirmace a konfirmace jednotlivých účtů (aktiv, závazků). V případě bankovních konfirmací pro ČSOB a většinu dalších

evropských bank je třeba žádat o tzv. konsolidovanou konfirmaci. Do žádosti v systému auditor vyplní hlavní účet klienta a banka pak prostřednictvím platformy konfirmuje všechny zůstatky všech účtů (aktivních i pasivních) a ostatní smluvní vztahy s tímto klientem. V případě žádostí o konfirmace zejména do mimoevropských bank je většinou třeba žádat o konfirmaci každého bankovního účtu či vztahu zvlášť, protože tyto banky konsolidované konfirmace nepřijímají. Detaily, jak u které banky postupovat, poskytuje platforma confirmation.com.

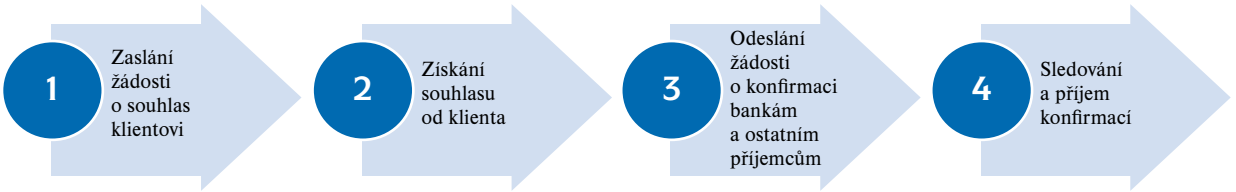
Postup žádosti o konfirmaci prostřednictvím platformy confirmation.com

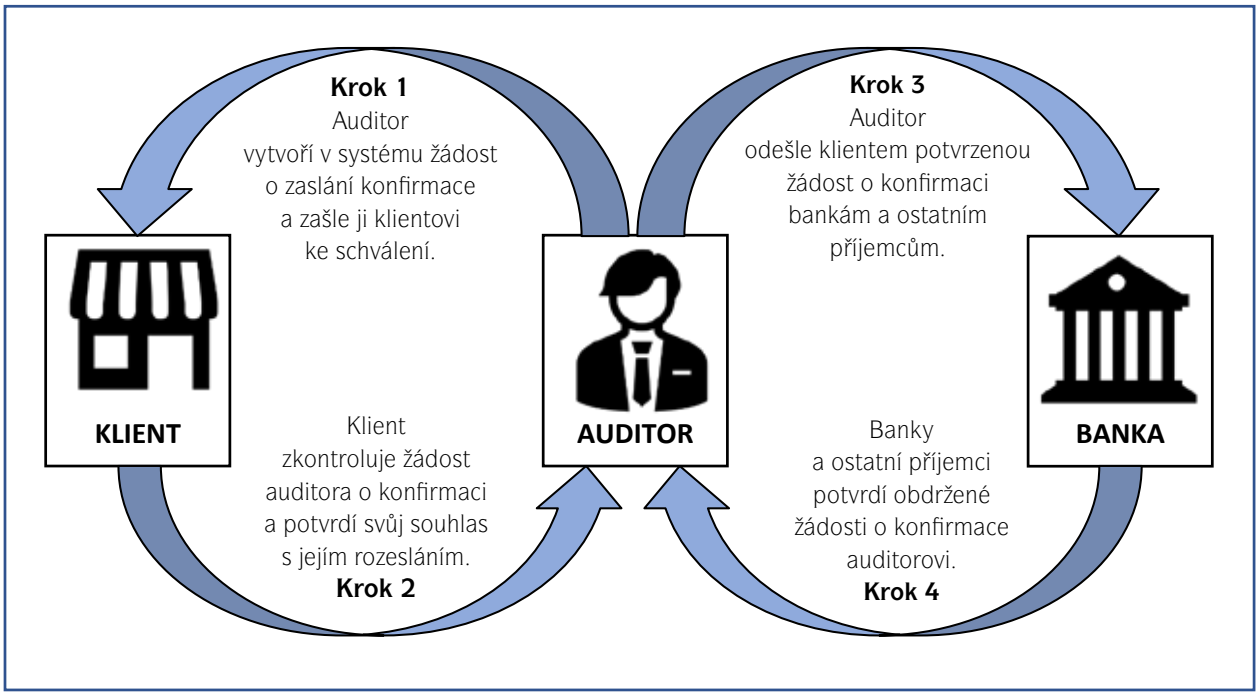
Auditor se zaregistruje na webové stránce www.confirmation.com. Vždy je nutné registrovat fyzickou osobu, tj. zaměstnance auditorské společnosti, auditora OSVČ. Identita auditora je pracovníky platformy vždy ověřena, k aktivaci účtu mohou být vyžadovány další podklady (například ev. číslo u KA ČR, kopie faktury za telefon, identifikace platební karty). Po aktivaci účtu vedou k bankovním konfirmacím od spolupracujících bank čtyři jednoduché kroky:

1) Auditor vytvoří klientův profil, identifikuje zodpovědnou osobu, přidá relevantní banky a hlavní účty a zašle prostřednictvím platformy žádost o autorizaci zodpovědné osobě klienta (nejčastěji člen statutárního orgánu, popř. finančního ředitele).
2) Klientovi je odeslán e-mail s odkazem pro schválení v prostředí confirmation.com. Klient žádost v prostředí platformy zkontroluje, elektronicky podepíše dle podpisového vzoru v bance (pomocí ipadu, note, myši, ale lze i vložit naskenovaný podpis v pdf, jpg, tif) a odešle zpět auditorovi.
3) Auditor pošle prostřednictvím platformy žádost bance (kontaktní informace banky jsou vyplněny automaticky bez zásahu auditora). K žádosti lze přiložit jakýkoliv dokument (například scan listinného konfirmačního dopisu s detaily auditorových dotazů na banku).
4) Banka požadavek přijme, ověří, zda poskytnutá autorizace od klienta (podpis) odpovídá platnému podpisovému vzoru, zpracuje a pošle odpověď zpět auditorovi přes rozhraní platformy. Auditor se přihlásí do systému a stáhne si dodané konfirmace spolu se záznamem auditní stopy celé komunikace.

Platforma confirmation.com poskytuje podporu, zatím pouze v anglickém jazyce, ve kterém je standardně celé rozhraní i pro Českou republiku. Dále jsou k dispozici e-learning, videa s ukázkami prostředí a funkcí a odpovědi na nejčastější otázky (opět primárně v anglickém jazyce).

Jak funguje koncept elektronických konfirmací pro auditory





Vybraní poskytovatelé platforem sloužících k důvěryhodné výměně dokumentů a dat

Název	Firma	Země	Odkaz	Popis
CONFIRMATION Part of Thomson Reuters	Confirmation jako součást Thomson Reuters	Kanada (USA)	www.confirmation.com	Zakladatel společnosti Brian Fox jako bývalý auditor PwC a EY budoval postupně platformu pro bezpečnou výměnu a potvrzení citlivých dat již od roku 2000. Nyní je společnost součástí kanadské skupiny Thomson Reuters a působí po celém světě.
auditi	Auditi GmbH ve spolupráci s DATEV eG	Německo	www.auditi.com/en/digital-confirmations	Poskytovatelem této služby je německá společnost Auditi GmbH založená v roce 2012 auditory a IT specialisty, která se zaměřuje na německý trh a od roku 2015 úzce spolupracuje s německým družstvem DATEV eG.
circit	Circit	Irsko	www.circit.io	Irská společnost zaměřující se na IT služby auditorům a sektoru SME nabízí globálně tuto službu pro důvěryhodnou výměnu elektronických dat mezi auditory a jejich klienty.
eConfirm.my	Extol Corporation jako součást AppAsia	Malajsie	econfirm.my	Autorem tohoto konceptu byl již v roce 1996 Malajsijský institut účetních (MIA), který pověřil vývojem této platformy pro elektronické bankovní konfirmace společnost Extol Corporation, která je nyní stoprocentní dceřinou společnost AppAsia Berhad.
ASD Auditing Software Distributor	Auditing Software Distributor SL	Španělsko	asdconfirmation.com	Poskytovatelem služby je španělská firma ASD, která je také dodavatelem dalšího SW pro auditory. Firma se zaměřuje na Španělsko, Portugalsko a Brazílii.

Další zdroje informací k elektronickým konfirmacím pro auditory

Elektronickými konfirmacemi pro auditory se zabývají i profesní organizace účetních a auditorů, jako například ICAEW, která již v polovině roku 2020 připravil stručnou příručku o hlavních faktorech elektronických konfirmací, které by měli auditoři znát a brát je zohledňovat je ve své auditorské praxi.

ICAEW poznamenává, že za okolností probíhající pandemie, se musí auditoři rozhodnout, zda budou organizovat zasílání konfirmací tradičním postupem poštou prostřednictvím vlastnoručně potvrzených podpisů, nebo elektronicky s využitím elektronického podpisu apod. I když je zřejmé, že druhý postup je za dané situace efektivnější, tak si mnoho auditorů není jistých, zda je to přípustné.

Příručka, kterou ICAEW vydala k řešení tohoto problému, se sice zaměřuje na auditorské postupy vyžadované ve Velké Británii, ale její zásady se mohou vztahovat analogicky i na jiné než auditorské zakázky, a to i mimo Velkou Británii v oblasti podávání zpráv. Účelem příručky je poskytnout praktická vodítka a v případě pochybností se auditorům doporučuje vyhledat konkrétní a podrobnější informace pro danou situaci.

Hlavní body příručky

- Stručně řečeno, nejsou již tradiční papírové dokumenty s vlastnoručními podpisy ve většině případů vyžadovány.
- Právní výbor ICAEW zohlednil právo EU, právní předpisy a judikaturu Velké Británie a uvedl, že k zasílání konfirmací lze použít elektronické dokumenty a elektronické podpisy, a to i v případech, kdy je vyžadováno originální potvrzení dokumentu.
- Vláda Spojeného království potvrdila, že se závěrem právního výboru ICAEW souhlasí a že elektronické podpisy jsou považovány za průkazné.
- Pokud v ústavních dokumentech účetní jednotky není uvedeno, jak musí být účetní závěrka podepsána, předpokládá se platnost elektronických podpisů, pokud nelze prokázat opak.

Oblasti, kterými se příručka se zabývá

Jaké jsou právní a regulační požadavky týkající se podpisů?

- Co by měl auditor zvážit, než se rozhodne použít elektronické podpisy?
- Co se rozumí „průkazným ověřením“?
- Jaké postupy řízení kvality v souvislosti s elektronickými potvrzeními a podpisy by měl firmy zavést?

Členové ICAEW mají přístup k příručce *Koronavirus (covid-19) – Úvod do používání elektronických podpisů k podepsání zprávy o auditu* na adrese: www.icaew.com/technical/audit-and-assurance/audit/covid-19-an-introduction-to-using-electronic-signatures-to-sign-an-audit-report

Martina Křížová Chrámecká,
Ladislav Mejzlík, Jiří Pelák

lidé a firmy

Daňař a daňová firma roku 2020

Slavnostní ceremoniál vyhlášení výsledků 11. ročníku soutěže Daňař & daňová firma roku se konal virtuálně v úterý 9. února. Online oznámení výsledků, během kterého bylo vyhlášeno v sedmi kategoriích 14 vítězů, se vysílalo z prostor společnosti Wolters Kluwer ČR, pořadatele soutěže. Vedle toho byly také vyhlášeny tři nejvstřícnější finanční úřady, nejžádanější zaměstnavatel v daních a byl zveřejněn žebříček největších poradenských firem mimo tzv. Velkou čtyřku.

Hlasování probíhalo od 2. listopadu 2020 do 8. ledna 2021. Do soutěže bylo nominováno celkem 48 daňových specialistů a osobností, největší počet nominovaných zaznamenala kategorie *daňové naděje roku*.

Poprvé se stala *nejžádanějším zaměstnavatelem v daních* společnost RSM CZ a.s., která se minulý rok umístila na pátém místě.

Daňovou osobností roku za státní sféru se stal Jiří Fojtík působící na Generálním finančním ředitelství.

Za komerční sféru získala titul *daňová osobnost roku* Ivana Pilařová, daňová poradkyně a účetní specialistka.

V kategorii *daňař roku* byli oceněni:

- v oblasti daň z přidané hodnoty Igor Pantůček z BDO Czech Republic s.r.o.,
- v oblasti správa daní Alena Wágner Dugová z Deloitte Legal s.r.o., advokátní kancelář,
- v oblasti daně z příjmů Pěva Čouková z Účetního portálu a.s.

V kategorii *daňové naděje roku* získali nejvíce hlasů:

- Vít Křivánek z BDO Legal s.r.o., advokátní kancelář,
- Barbora Čapská z Finančního úřadu pro Pardubický kraj,
- Klára Vandasová z RSM CZ a.s.

V kategorii *nejžádanější lektor v daních* byla oceněna Ivana Pilařová.

Nejvstřícnější územní pracoviště finančních úřadů byla zvolena širokou veřejností.

V pořadí podle počtu hlasů se jimi staly:

- Finanční úřad pro Jihomoravský kraj, územní pracoviště Brno I,
- Finanční úřad pro Jihomoravský kraj, územní pracoviště Brno–venkov,
- Finanční úřad pro Jihočeský kraj, územní pracoviště v Českých Budějovicích.

Poslední vyhlašovanou kategorií byla *ETL Global Největší poradenská firma roku 2020 mimo Velkou 4*. První místa získali podle celkového obratu za rok 2020 Grant Thornton Czech Republic a.s. a podle celkového počtu zaměstnanců skupina BDO.

-vk-

Co najdete v e-příloze č. 3/2021

Přístup k e-příloze Auditor

E-příloha Auditor vychází souběžně s tištěným časopisem Auditor v elektronické podobě. Pro auditory je ke stažení v uzavřené části webových stránek komory www.kacr.cz, kam se lze dostat pod přihlašovacím jménem a heslem.

OBSAH

-ab-

AUDITOR č. 3/2021

ročník XXVIII

REDAKCE
Komora auditorů ČR
Opletalova 55, 110 00 Praha 1
tel.: 224 212 670, 221 602 289
e-mail: redakce@kacr.cz

REDAKTORKA
Bc. Aneta Čermáková

REDAKČNÍ RADA
Ing. Jiří Pelák, Ph.D., předseda
doc. Ing. Ladislav Mejzlík, Ph.D.
Jarmila Melichová
Ing. Jiří Mikyna
Ing. Jan Molín, Ph.D.
prof. Ing. Libuše Müllerová, CSc.
Ing. Michal Šindelář, Ph.D.
Ing. Michal Štěpán
Ing. Petr Vácha, Ph.D.

Pravidla pro zveřejňování článků jsou uvedena na webu KA ČR (www.kacr.cz/desatero). Články prochází recenzním řízením redakční rady.

VYDÁVÁ
Komora auditorů České republiky
tel.: 224 212 670, 224 222 178
IČ 70901473

Vydávání povoleno MK ČR 6934

ISSN 1210-9096

INZERCE, SAZBA, DISTRIBUCE
Infomedia, spol. s r.o.
Otradovická 731/11, 142 00
Praha 4, tel.: 607 972 085
e-mail: infomedia@infomedia.cz

TISK
Wendy, spol. s r.o., Mělník

OBJEDNÁVKY A PŘEDPLATNÉ
Komora auditorů ČR
e-mail: kacr@kacr.cz

Vychází 10x ročně

Roční předplatné: 950 Kč

Pro členy KA ČR zdarma

www.kacr.cz