3|2016

INTERNÍ AUDITOR

ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ
ROČNÍK 20, ČÍSLO 3–2016 (81)

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

The Institute of Internal Auditors

INTERNÍ AUDIT A INFORMAČNÍ TECHNOLOGIE

INTERNÍ AUDIT A INFORMAČNÍ TECHNOLOGIE

INTERNÍ AUDIT A INFORMAČNÍ TECHNOLOGIE

Slavnostní vyhlášení 1. ročníku Ceny za inovaci v interním auditu proběhne dne 12. října 2016 na národní konferenci ČIIA v Českých Budějovicích.

Z celkem osmi předkladatelů soutěžních projektů byli odbornou porotou vybráni tito finalisté:

Česká spořitelna, a. s.
s projektem
„Karta rizik“

MONETA Money Bank, a. s.
s projektem
„Guest Reviewer“

OKD, a. s.
s projektem
„Integrace vybraných funkcí společnosti do interního auditu“

Děkujeme za účast v soutěži všem předkladatelům projektů: Česká spořitelna, Krajská správa a údržba silnic Vysočiny, Masarykův onkologický ústav, Ministerstvo financí, MONETA Money bank, OKD, Státní fond životního prostředí, Státní úřad inspekce práce.

CENA ZA INOVACI V INTERNÍM AUDITU

více informací na **www.interniaudit.cz**

OBSAH

Vážené čtenářky, vážení čtenáři,

letošní rok je díky některým akcím ČIIA ve znamení problematiky auditu ve vztahu k IT. Zejména se jedná o konferenci na téma „CYBER SECURITY“, kterou v červnu uspořádal ČIIA ve spolupráci s ISACA CRC za podpory EY a o říjnovou národní konferenci ČIIA „AUD**IT**“ zaměřenou na aktuální témata z oblasti auditu informačních technologií s důrazem na kybernetickou bezpečnost. Tato konference je realizována pod záštitou ředitele Národního bezpečnostního úřadu. Další témata dotýkající se IT jsou součástí i jiných akcí ČIIA. Naše redakční rada navrhla téma časopisu „Interní audit a IT“ již v průběhu minulého roku v rámci přípravy témat jednotlivých čísel pro tento rok. Ne náhodou byl i tento záměr schválen. Z výše uvedeného je jasně cítit, že se ČIIA problematikou IT a auditu systematicky intenzivně zabývá. V letošním roce pak zvláště silně. Tímto rovněž navazujeme na celosvětový trend a potřebu vnímat kybernetická rizika i interními auditory.

Toto číslo časopisu není ani rekapitulací konference červnové ani místem pro uveřejnění problematiky, která je součástí konference podzimní. Není to ani možné, neboť vměstnat tuto problematiku do jednoho čísla profesního časopisu nelze. Přesto zde najdete články, které problematiku z uvedených akcí doplňují, případně rozvíjejí nebo se jedná o relativně samostatná témata.

Opět přinášíme zajímavý rozhovor, tentokrát s panem Harringtonem. Po rozhovoru s panem Chambersem uveřejněném v minulém čísle časopisu jde o další „úlovek“, který se Petrovi Hadravovi podařilo získat.

Věřím, že vás obsah tohoto čísla zaujme a nenechá vás klidnými pod tíhou inspirace pro vaši každodenní práci.

Jan Kovalčík
vedoucí redakční rady

Vydává
Český institut interních auditorů, z. s.
Karlovo nám. 3
120 00 Praha 2
tel.: +420 224 920 332
+420 224 919 361
e-mail: ciia@interniaudit.cz
www.interniaudit.cz

Redakce INTERNÍ AUDITOR
Karlovo nám. 3
120 00 Praha 2
Registrace: MK-ČR-E-12322
ISSN 1213-8274

Redakční rada:
Vedoucí – Jan Kovalčík, Petr Hadrava, Daniel Häusler, Ludmila Jiráňová, Andrea Lukasíková, Šárka Nováková, Petra Škvorová, Ivana Šťastná, Eva Štěpánková, Kateřina Zonygová

Foto: archiv ČIIA, fotobanka 123RF
Neprodejné, určeno pro Český institut interních auditorů
Náklad: 1 400 výtisků
Pre-press: Viktor Beránek
Tisk: REPRO servis s. r. o.
Distribuce: Mail Step a. s.

Zákon o kybernetické bezpečnosti a směrnice NIS

Adam Kučínský
Cyber Security/Policy Specialist, Auditor
Národní bezpečnostní úřad – Národní centrum kybernetické bezpečnosti

Již více než rok a půl je v České republice účinný zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), upravující pravomoci a povinnosti státu a některých dalších subjektů v oblasti kybernetické bezpečnosti.

Důvod vzniku regulace je prostý, informační a komunikační systémy se staly nedílnou součástí života společnosti a pro zabezpečení některých klíčových činností a služeb jsou tyto systémy nepostradatelné.

K podobnému závěru dospěla i Evropská unie, a proto byla 6. července 2016 přijata směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, tzv. směrnice NIS.

Směrnice NIS i zákon o kybernetické bezpečnosti regulují stejnou oblast, v některých případech se překrývají a v některých případech NIS na základě povinné transpozice zákon rozšíří. Pro srovnání je nutné začít u aktuálně účinného zákona.

1. Současný zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti ukládá povinnosti pěti skupinám subjektů (v § 3). Jedná se o:

a) poskytovatele služby elektronických komunikací a subjekty zajišťující síť elektronických komunikací,

b) orgány nebo osoby zajišťující významnou síť,

c) správce informačního systému kritické informační infrastruktury,

d) správce komunikačního systému kritické informační infrastruktury,

e) správce významného informačního systému.

Pro přesné stanovení, které subjekty se pod těmito pojmy skrývají, je třeba nahlédnout vedle zákona o kybernetické bezpečnosti i do jiných právních předpisů.

V případě *poskytovatelů služby elektronických komunikací* a subjektů zajišťujících síť elektronických komunikací je nutné využít zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Tyto subjekty určovány nejsou a při jejich identifikaci se vychází z definic uvedených v § 2 písm. f) a n) zmíněného zákona o elektronických komunikacích.

> „Česká republika již má fungující rámec kybernetické bezpečnosti“

Orgánem nebo osobou zajišťující významnou síť je subjekt, zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře. Jde tedy většinou o některého ISP (Internet Service Provider). Podobně jako u předchozí skupiny povinných osob určování jako takové neprobíhá a subjekty se identifikují samy na základě definice.

Kritickou informační infrastrukturu (dále také KII) určuje Národní bezpečnostní úřad (NBÚ) podle kritérií stanovených nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Proces určování, resp. posuzování, zda systémy naplňují stanovená kritéria, probíhá ve spolupráci s daným správcem systémů s využitím analýz dopadu incidentů a dalších podkladů. Samotný akt určení, potom probíhá podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a závisí zde na povaze subjektů – organizační složky státu jsou určeny na návrh NBÚ usnesením vlády, ostatní subjekty pak opatřením obecné povahy vydaným NBÚ. Obecně se jedná o takové informační a komunikační systémy, jejichž narušení by mohlo mít závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb, zdraví nebo ekonomiku. Pro představu jsou to

ANKETA

VÝBORY PRO AUDIT

1. Jakým způsobem ve Vašich podmínkách zajišťujete interní audit v oblasti IT?

2. Jaký je Váš názor na zajištění dostatečné pozornosti na problematiku IT ze strany interního auditu, včetně kvalifikovaných auditorů?

3. Na jaké oblasti IT se v rámci výkonu interního auditu v současné době nejvíce zaměřujete a která oblast vyžaduje dle Vašeho názoru největší pozornost?

Pavel Šrámek
ředitel ÚIA Skupiny Metrostav
Metrostav a.s.

1. Útvar IA byl v letošním roce rozšířen s o specialistu pro oblast IT.

2. Viz odpověď ot. 1.

3. Vypracování pravidel v rámci Skupiny Metrostav a posouzení souladu v jednotlivých společnostech Skupiny – hledisko ekonomické i bezpečnostní.

například systémy, na kterých jsou zcela nebo významně závislé prvky „fyzické" kritické infrastruktury, např. elektrárny, přenosové soustavy elektrické energie, banky apod.

Poslední skupinou povinných subjektů jsou *správci významných informačních systémů* (dále také VIS). Správcem VIS muže být pouze orgán veřejné moci. V souladu s tím, jsou jako VIS určeny pouze systémy ve státní sféře, přičemž z regulace jsou prozatím vyloučeny systémy spravované obcemi. V delším horizontu je pracováno s variantou rozšíření a zahrnutí obcí, aktuální novela zákona s tím však nepočítá. VIS musí naplnit kritéria stanovená vyhláškou č. 317/2014 Sb. Zjednodušeně to jsou takové informační systémy, které jsou svou funkcí důležité, nicméně dopady jejich narušení nedosahují závažnosti určené krizovým zákonem pro kritickou informační infrastrukturu. Narušení bezpečnosti informací v těchto informačních systémech by mohlo omezit či ohrozit výkon působnosti daného úřadu. Posouzení naplnění kritérií pro VIS provádí sám správce systému, který by v případě naplnění těchto kritérií měl daný systém prohlásit VIS a začít plnit povinnosti. V první řadě tedy nahlásit kontaktní a některé další údaje stanovené vyhláškou č. 316/2014 Sb. NBÚ. Velmi často jsou takto určovány systémy spisové služby, ekonomické a další systémy, kde by v případě narušení mohlo dojít k ochromení činnosti daného úřadu. Demonstrativní výčet VIS uvádí příloha č. 1 výše zmíněné vyhlášky č. 317/2014 Sb.

Aby tedy byl informační systém určen jako KII nebo VIS, musí splňovat určitá kritéria stanovená legislativou. Jednak to jsou kritéria určující míru závažnosti důsledků narušení těchto systémů (u KII se nazývají průřezová, u VIS dopadová) a dále kritéria odvětvová (u VIS oblastní), která vymezují pouze některé klíčové oblasti, které jsou pro stát, resp. pro zajištění jeho společenských a hospodářských funkcí, důležité. Z každé skupiny kritérií musí systém splnit alespoň jedno.

2. Směrnice NIS

Návrh směrnice je na půdě Evropské unie řešen již od roku 2013. Finální podoba směrnice však byla schválena až 6. července 2016 a o třináct dní později byla publikována v úředním věstníku EU.[1] Dvacátým dnem od její publikace se směrnice stává účinnou. Od 8. srpna 2016 tak začíná běžet 21 měsíců transpoziční lhůty pro implementaci směrnice do národního práva členských států Unie. To znamená, že do května 2018 by měly být požadavky směrnice zapracovány v českém právním řádu. Ač se transpoziční lhůta v délce 21 měsíců může zdát poměrně dlouhá, vzhledem k blížícím se volbám v říjnu 2017 a vzhledem ke standardní délce legislativního procesu tomu tak nemusí být. NBÚ jako národní autorita v oblasti kybernetické bezpečnosti proto započal přípravu transpozice směrnice již před jejím zveřejněním. Návrh novely zákona o kybernetické bezpečnosti, který zapracovává směrnici do českého právního řádu, již byl dokončen a rozeslán do mezirezortního připomínkového řízení ještě před oficiálním zveřejněním směrnice ve Věstníku EU 15. července 2016.

Směrnice NIS podobně jako současný zákon stanovuje určitá práva a povinnosti v kyberprostoru. Netýká se plošně všech subjektů, ale definuje dvě skupiny povinných osob – provozovatel základní služby (PZS) a poskytovatel digitálních služeb (PDS). Tyto subjekty jsou rozdílné nejen kritérii a způsobem určení, ale také mírou regulace. Zatímco u PDS platí tzv. zásada maximální harmonizace, tedy pravidlo znemožňující ukládání povinností nad rámec požadavků směrnice, u PZS toto omezení není a členským státům je umožněno ukládat povinností více.

2.1 Poskytovatelé digitálních služeb

Poskytovatel digitálních služeb je subjekt poskytující služby online tržiště, internetového vyhledávače nebo cloud computingu. Za online tržiště se považují platformy, umožňující uzavírání online smlouvy. Podle recitálu[2] 15 směrnice se za tržiště nepovažují různé srovnávače cen apod. Cloud computing definuje návrh novely zákona jako službu, která umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které lze sdílet. Internetový vyhledávač pak v zákoně definován není. Představu o tom, o jaké subjekty jde, si každý jistě udělá. V recitálu 16 směrnice je dále uvedeno, že se za internetový vyhledávač nepovažuje vyhledávací funkce v rámci konkrétních internetových stránek ani srovnávače cen.

Omezujícím kritériem pro všechny PDS je skutečnost, že z regulace jsou vyloučeny malé a mikropodniky. Mikropodnikem se zde rozumí podnik s méně než 10 zaměstnanci, ročním obratem nebo bilanční sumou menší než 2 miliony euro. Malým podnikem je pak podnik s méně než 50 zaměstnanci nebo ročním obratem či bilanční sumou pod 10 milionů euro.[3] PDS nebudou určováni – jejich identifikace vychází přímo z naplnění definice.

2.2 Provozovatelé základních služeb

Provozovatelé základních služeb jsou subjekty klíčové pro fungování společenských a ekonomických činností. PZS musí poskytovat službu, která je nezbytná z hlediska zachování kritických společenských nebo ekonomických činností, přičemž poskytování

[1] Úřední věstník Evropské unie Svazek 59 19. července 2016, Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

[2] Recitál je text předcházející samotným ustanovením směrnice – slouží jako interpretační pomůcka.

[3] Definice malého a mikropodniku viz Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků, Annex , Article 2 (Úř. věst. L 124, 20. 5. 2003).

Petr Grešl
auditor
Rogit s.r.o.

1. Naší společnosti se osvědčil, jako externímu dodavateli, přístup zadavatelů formou přizvané osoby dle standardu 1210_A1. Díky tomuto přístupu přinášíme jako externí dodavatel know-how interním auditorům a díky vzájemné spolupráci na auditech zvyšujeme jejich odbornost v této oblasti. Základním benefitem pak je, že jsou například schopni provést ověření realizace doporučení nebo pokrýt některé oblasti IT samostatně.

2. V současné době došlo k výraznému posunu v této oblasti díky zákonu 181/2014 Sb., o kybernetické bezpečnosti, kde je audit striktně vyžadován. Tato oblast začíná být jednou z prioritních a audity v této oblasti se budou vykonávat každoročně.

3. Obecně je všude kladen důraz na bezpečnost informací, nicméně z našeho pohledu jako externího dodavatele auditních služeb je nutné také věnovat pozornost řízení IT v obecné rovině. Jen tak je možné zajistit efektivitu, účelnost a hospodárnost vynaložených prostředků do IT. Bezpečnost je pouze jedním aspektem.

této služby je závislé na sítích a informačních systémech a incident by mohl vést k významnému narušení poskytování této služby.[4] Směrnice rámcově stanovuje dopadová kritéria, která by PZS měl naplnit pro své určení. Podle směrnice mají členské státy povinnost při posouzení systému zvážit alespoň hledisko (I) počtu uživatelů závislých na dané službě, (II) závislost dalších odvětví stanovených v příloze II směrnice, (III) možný dopad incidentů na ekonomické a společenské činnosti nebo na veřejnou bezpečnost, (IV) podíl daného subjektu na trhu, (V) zeměpisný rozsah zasažené oblasti a (VI) možné alternativy služby. Zváženy mají být rovněž další okolnosti specifické pro jednotlivá odvětví.[5] Odvětví, ve kterých se mohou vyskytovat PZS, uvádí příloha č. II směrnice. Jedná se o energetiku, dopravu, bankovnictví, infrastrukturu finančních trhů, zdravotnictví, dodávky a rozvody pitné vody a digitální infrastrukturu. Zahrnutá odvětví mohou být členskými státy rozšířena stejně jako dopadová kritéria. V návrhu novely zákona o kybernetické bezpečnosti jsou tak přidána ještě odvětví chemický průmysl a veřejná správa, která byla identifikována jako bílá místa při uvádění zákona o kybernetické bezpečnosti do praxe. PZS budou určováni opatřením obecné povahy, které bude vydávat NBÚ obdobně jako u KII. Zatímco odvětví, ve kterých budou PZS určováni, uvádí již návrh novely zákona, detailnější rozpracování dopadových kritérií stanoví prováděcí vyhláška.

„Návrh novely zákona o kybernetické bezpečnosti, který zapracovává směrnici do českého právního řádu, již byl dokončen a rozeslán do mezirezortního připomínkového řízení“

Podle výše nastíněného znění dopadových a odvětvových kritérií lze tedy dovodit, že PZS jsou obdobou KII. PZS se s KII v některých kritériích překrývá, v některých však bude PZS širší. KII je založena na krizovém zákoně a určována je podle kritérií uvedených v nařízení vlády, která jsou od kritérií stanovených směrnicí částečně rozdílná. Subjektů určených jako KII se navíc vedle povinností uložených ZKB týkají také povinnosti vyplývající z krizového zákona. Z těchto důvodů je kategorie PZS regulována samostatně. Pokud bude některý subjekt splňovat kritéria jak pro PZS, tak i pro KII, pak bude určen jako KII.

3. Povinnosti nově regulovaných subjektů

Jak bylo uvedeno výše, návrh novely zákona o kybernetické bezpečnosti zavádí dvě nové povinné osoby – PZS a PDS.

Ohledně povinností je možné uvést, že pro PZS se nebudou příliš lišit od povinností uložených KII (kromě těch, které vyplývají pro KII z krizového zákona). Podle navrhované novely zákona budou tedy PZS muset:

- nahlásit kontaktní údaje,
- přijmout bezpečnostní opatření (standardizace),
- detekovat a oznamovat incidenty, včetně případných přeshraničních dopadů,
- poskytovat NBÚ součinnosti pro posouzení naplnění určujících kritérií,
- řídit se případnými opatřeními k reakci na kybernetické bezpečnostní incidenty.

Vzhledem k tomu, že PZS a KII je svojí významností na velmi podobné úrovni, nepředpokládá se v této kategorii výrazný nárůst povinných osob. PZS budou určováni zejména tam, kde jsou současná kritéria pro KII nedostačující, např. v odvětví zdravotnictví.

Pokud jde o povinnosti týkající se PDS, zde je regulace mírnější. Povinnost zavedení organizačních a technických opatření, která jsou „vhodná, přiměřená a odpovídající míře existujícího rizika“, je možné vykládat různě, a je zde tedy značný prostor pro zavedení různé úrovně zabezpečení.

Shrnutí

Závěrem lze říci, že kromě zavedení nové kategorie povinných osob – PDS není směrnice NIS pro Českou republiku příliš přelomová. Česká republika již má fungující rámec kybernetické bezpečnosti a povinnosti a opatření zaváděné směrnicí, jsou již dnes z velké části zavedeny a plněny (vedle výše uvedených jde například o přijetí národní strategie, určení jednotného kontaktního místa, ustanovení týmu CSIRT apod.). Směrnice je tak významná zejména pro státy, které podobnou regulaci ještě nezavedly, a bude zajímavé sledovat, jakou cestu zvolí.

Tento článek je první ze série příspěvků týkajících se problematiky kybernetické bezpečnosti z pohledu garanta. V dalších číslech na něj naváží příspěvky věnující se tématům současných požadavků na bezpečnostní opatření a auditu shody se zákonem.

[4] Článek č. 5, odst. 2 směrnice.

[5] Článek č. 6, odst. 1 směrnice.

Prostor k vyjádření.

Bohuslav Poduška
ředitel útvaru interní audit
Česká spořitelna, a.s.

1. V rámci útvaru IA České spořitelny máme útvar IT auditu s týmem vysoce specializovaných IT auditorů. Interní audit v oblasti IT zajišťujeme hlavně vlastními silami, ale některé hodně specifické oblasti řešíme outsourcingem.

2. IT je ze strany útvaru IA naší společnosti věnována velká pozornost. Vzhledem ke skutečnosti, že působíme ve finanční oblasti, je ověřování procesů v IT (auditů v oblasti IT) věnována přibližně jedna pětina kapacity útvaru IA.

IT auditoři provádějí, buď specializované IT audity (tzv. technologické audity) nebo se podílejí, např. jako členové auditorských týmů a jako konzultanti, na ověřování bankovních procesů, v místech, kde se proces dotýká IT. Zajištění dostatečné kvalifikace IT auditorů, ale nejen IT auditorů, je proces náročný zejména na finanční zdroje. Specializovaná IT školení jsou finančně nákladná a v mnoha oblastech samotná školení nestačí k získání a udržení znalostí a dovedností, aniž by se danou oblastí člověk každodenně prakticky zabýval (např. penetrační testování). Podle našeho názoru je třeba ekonomicky vyvážit činnosti, které zajistíme vlastními silami, včetně nároků na odbornost a proškolení IT auditorů, a naopak činnosti vysoce specializované (např. penetrační testy), které nakupuje-

Sběr bezpečnostních auditních záznamů z činností vykonaných nad elektronickou dokumentací

Ing. Daniel Kardoš, Ph.D.
auditor bezpečnosti informací
oddělení bezpečnosti ICT
Ministerstvo práce a sociálních věcí ČR

Zveřejněním informací americké elektronické špionáže šokoval svět Snowden v roce 2013. Dalším rozsáhlým příkladem narušení bezpečnosti informací je únik interních dokumentů společnosti Mossack Fonseca, známý jako Panama Papers.

Pokud se nepovedlo ochránit informace o americké špionážní činnosti, je zcela naivní se domnívat, že únikům informací lze zabránit. To samozřejmě nevylučuje, že je možné snížit pravděpodobnost narušení bezpečnosti informací pomoci implementace různých opatření. Jako účinný nástroj bezpečnosti informací se v současnosti jeví použití automatizovaného systému záznamu auditní události. Ukazuje se, že vytváření záznamu vybraných auditních událostí, tj. událostí, které chceme zaznamenávat pro potřeby následného auditu, je velmi účinný analytický a kontrolní nástroj bezpečnosti informačních a komunikačních systémů. Slouží pro potřeby zpětné, reaktivní analýzy bezpečnostní události.

Musíme se smířit s tím, že nelze zcela zabránit úniku informací. Pokud ale budeme vytvářet dostatečně detailní záznamy o činnosti uživatelů a o činnosti samotného informačního systému, budeme schopni alespoň analyzovat to, co se stalo. Budeme schopni z auditního záznamu zjistit „kdo“, „co“ a „kdy“ v systému udělal. Auditní záznamy mohou sloužit také jako technický prostředek pro posouzení shody s politikou nebo stanovenými interními zásadami organizace, pro řízení přístupu uživatelů k aplikacím. Samotné řízení přístupu se skládá z identifikace, autentizace a autorizace uživatele. Identifikace znamená předložení identifikátoru, při přihlašování do informačního systému se nejčastěji uživatel identifikuje uživatelským jménem. Pak následuje autentizace uživatele k ověření, zdali je uživatel tím, za koho se vydává, což se při přihlášení projevuje většinou nutností zadat heslo. Posledním krokem řízení přístupu je autorizace, to jest umožnění identifikovanému a ověřenému uživateli v informačním systému vykonávat činnosti, ke kterým je oprávněn. Politika řízení přístupu by měla očekávat neočekávané. Při neočekávané události jsou automaticky shromažďované auditní záznamy primárním analytickým prostředkem řízení bezpečnosti přístupu. Proto, aby to bylo technický možné, má většina informačních systémů tuto funkcionalitu v sobě zakomponovanou. Většina informačních systémů je dnes vybavena technickými prostředky na úrovní hardware a software umožňujících automatizovaně vytvářet auditní záznamy. Tyto systémy se staly silným a účinným nástrojem nejenom interních auditorů informační bezpečnosti, ale také manažerů bezpečnosti informací.

> „Ukazuje se, že vytváření záznamu vybraných auditních událostí, tj. událostí, které chceme zaznamenávat pro potřeby následného auditu, je velmi účinný analytický a kontrolní nástroj bezpečnosti informačních a komunikačních systémů“

Oblast vytváření auditních záznamů v rozsahu kybernetické bezpečnosti upravuje § 21 vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti. Vyhlášku stanovil Národní bezpečnostní úřad, podle § 28 odst. 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti k provedení § 6 písm. a) až c), § 8 odst. 4, § 13 odst. 4 a § 16 odst. 6 zákona. V § 21 vyhlášky jsou ve čtyřech odstavcích stanoveny požadavky na „Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů“.

Na základě § 21 je správce informačního systému kritické informační infrastruktury, správce komunikačního systému kritické

me. Pro rozvoj odbornosti IT auditorů je prospěšné členství v profesních organizacích, u IT zejména v ISACA. Získávání profesních certifikací, např. CISA, CISM a dalších, napomáhá odbornému rozvoji IT auditorů.

3. V současné době se nejvíce zaměřujeme na oblast řízení IT, včetně outsourcingu, oblast kybernetické bezpečnosti, bezpečnosti a funkčnosti IT systémů a klíčových aplikaci.

Velkou pozornost podle našeho názoru vyžaduje / bude vyžadovat oblast cloud computingu, využívání „chytrých“ zařízení a oblast agilního vývoje IT aplikací.

Miroslava Bulubas Milecova
Manager Audit Leasing & Austrian subsidiaries
UniCredit Bank Austria

1. Okrem specialneho auditneho timu, ktory sa zaobera vyhradne IT auditom, IT work program a vybrane testy v oblasti IT (napriklad access rights management) su sucastou kazdeho procesneho auditu a auditu dcerskych spolocnosti.

2. Myslim si ze je potrebne venovat velmi vysoku pozornost IT problematike a overovaniu kontrol v tejto oblasti. Vzhladom k tomu, ze kapacity specialistov, IT auditorov, su obmedzene a zaroven z dovodu ze

informační infrastruktury a správce významného informačního systému povinen používat nástroj (informační systém) pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.

„Auditní záznamy mohou sloužit také jako technický prostředek pro posouzení shody s politikou nebo stanovenými interními zásadami organizace, pro řízení přístupu uživatelů k aplikacím“

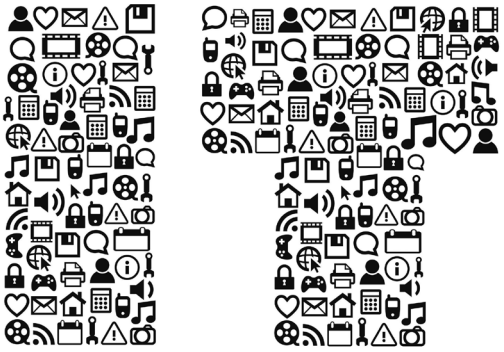
Pomocí nástroje musí správce zajistit:
a) sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost, nebo neúspěšnost činnosti a
b) ochranu získaných informací před neoprávněným čtením nebo změnou.

Nástroj musí zaznamenávat:
a) přihlášení a odhlášení uživatelů a administrátorů,
b) činnosti provedené administrátory,
c) činnosti vedoucí ke změně přístupových oprávnění,
d) neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
e) zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému,
f) automatická varovná nebo chybová hlášení technických aktiv,
g) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a
h) použití mechanizmů identifikace a autentizace, včetně změny údajů, které slouží k přihlášení.

Dále správce musí zajistit:
Jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

Správce informačního systému kritické informační infrastruktury a správce komunikačního systému kritické informační infrastruktury musí výše uvedené záznamy o činnosti uchovávat nejméně po dobu třech měsíců.

„Tyto systémy se staly silným a účinným nástrojem nejenom interních auditorů informační bezpečnosti, ale také manažerů bezpečnosti informací“



[thor83] © 123RF.COM

Kdo je správcem informačního systému kritické informační infrastruktury, správcem komunikačního systému kritické informační infrastruktury nebo správcem významného informačního systému, stanovuje nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení vlády č. 315/2014 Sb., vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, a usnesení vlády č. 390/2015 ke 2. aktualizaci Seznamu prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu.

V rámci působnosti zákona o kybernetické bezpečnosti je vytváření výše uvedených automatizovaných auditních záznamů minimem. Nad rámec těchto povinnosti je možné se dobrovolně inspirovat technickými normami upravujícími jak organizační, tak technická opatření k vytváření automatizovaných auditních záznamů. ■

IT je urcite oblast v ktorej si v dnesnej dobe musi kazdy auditor neustale prehlbovat vedomosti, sme pristupili k rozsireniu auditneho program v pripade procesnych auditov o povinnu „IT“ cast. V nasej banke a dcerskych spolocnostiach pravdepodobne neexistuje process, ktory by nebol podporeny IT aplikaciou a preto vnimame vybrane IT kontroly ako sucast procesnych auditov. Napriek zvysenej pozornosti priestor na zlepsenie stale existuje a hoci zlepsujeme interne vedomosti v oblasti IT auditov, pocitujeme zaroven nedostatok kvalifikovanych IT auditorov a problem ziskat ich, ci uz externe alebo interne.

3. Zameriavame sa prevazne na procesy riadenia pristupovych prav (identity and access management), dodrziavanie principu minimalnych privilegii, klasifikaciu a ochranu dat, ale aj change management, business continuity a disaster recovery. Na zaklade nasich analyz rizik, najvacsiu pozornost si vyzaduje cyber security, network management a mainframe security.

Bezpečnost při využívání osobních mobilních zařízení

Jan Andraščík, CISA, CISM, CRISC, CMDSP
Senior konzultant
oddělení ICT poradenství Deloitte
Česká republika

Jan Andraščík je Senior konzultantem v oddělení ICT poradenství Deloitte Česká republika. Během své kariéry byl součástí několika projektů napříč různými sektory v oblastech poradenství informační bezpečnosti, penetračního testování, stejně jako několika projektů řízení rizik a bezpečnostních auditů napříč Evropou a Asií. Specializuje se na technickou bezpečnost operačních systémů, databází, sítí a aplikací; a řízení zranitelností nástroji QualysGuard, Nessus, Acunetix či Greenbone. V současné době se specializuje na bezpečnosti mobilních zařízení, BYOD a Internet věcí. Je držitelem certifikací CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control), CMDSP (Certified Mobile Device Security Professional) a ISO 22301:2012 Business Continuity Manager.

1. Úvod

Svět, ve kterém žijeme, nám neustále přináší technologické novinky, kterým se musíme přizpůsobovat. Tyto nové technologie nám mohou usnadnit naše životy, zlepšit efektivitu naší práce, zvýšit výsledky hospodaření společností, ve kterých pracujeme, apod.

Jednou z novinek u nás, avšak na západ od nás již hojně vyžívané, je fenomén BYOD. BYOD je zkratkou anglického „Bring Your Own Device“, což v překladu znamená „Přines si vlastní zařízení“. Jak již ze samotného překladu vyplývá, využití tohoto přístupu umožňuje zaměstnancům používat svá vlastní zařízení k vykonávání pracovních činností. Ačkoliv v západních zemích je BYOD chápáno komplexně – tedy společnosti umožňují zaměstnancům přinášet teoreticky jakékoliv zařízení, v České republice jsme v BYOD přístupu stále ještě v počátcích, a BYOD je tak často spojováno pouze s mobilními zařízeními, typicky s mobilními (chytrými) telefony a tablety.

Zaměstnanci rádi využívají mobilní zařízení, neboť je mohou používat prakticky kdekoliv a kdykoliv, a s internetovým připojením, které je na těchto zařízeních běžné, mohou vzdáleně přistupovat k systémům společnosti.

> „Využívání mobilních zařízení ve společnostech nabývá stále většího významu“

2. Využívání mobilních zařízení a jejich rizika

Využívání mobilních zařízení ve společnostech nabývá stále většího významu. V západním světě podporují mobilní zařízení nepřeberné množství obchodních procesů napříč různými průmyslovými odvětvími. I v České republice se již mobilní zařízení dostávají do každodenního života zaměstnanců.

Dle zkušeností autora již v České republice existuje mnoho společností, které se rozhodly využívat mobilní zařízení jako taková pro podporu svých business procesů. Ať je to čistě pomocí možnosti připojení mobilního zařízení k firemní e-mailové schránce, nebo pokročilejší způsob s možností připojení k vybraným informačním systémům. Díky tomu je možné zvýšit produktivitu zaměstnanců, a tím dosahovat vyšších zisků.

Dalšího zvýšení produktivity je možné dosáhnout využitím přístupu BYOD, který je možné považovat také za benefit pro zaměstnance, neboť jim přináší svobodu rozhodnuti nad tím, jaká zařízení chtějí pro své pracovní činnosti používat. Tímto přístupem je tak možné zvýšit spokojenost zaměstnanců, a tím případně i jejich produktivitu, neboť budou mít možnost pracovat se systémy, které znají, a nebudou se muset učit zacházet s novým typem systému.

Ačkoliv je používání mobilních zařízení již v České republice rozšířené, dle zkušeností autora jen několik společností umožňujících tento způsob práce aktivně řeší bezpečnost takto používaných mobilních zařízení.

2.1 Rizika využívání mobilních zařízení ve společnostech

S využíváním mobilních zařízení souvisí mnoho rizik, která je nutné při plánování jejich používání brát v úvahu. Tato rizika nemusejí souviset pouze s chybami vyskytujícími se v samotných operačních systémech jednotlivých platforem, ale často souvisejí přímo s chováním uživatelů.

Mobilní zařízení jsou ze své podstaty přenosná, a na rozdíl od klasických stolních počítačů je tak není lehké kontrolovat. Stolní počítače jsou mimo softwarovou ochranu chráněny také fyzicky. Typicky je tak zabráněno přístupu neoprávněných osob k těmto počítačům. To však u mobilních zařízení zajistit nelze. Mobilní zařízení jsou téměř vždy po ruce svým uživatelům, v příruční tašce, v kapse apod., a není tak možné efektivně zajistit jejich fyzickou bezpečnost. Mohou tak být snadným cílem k odcizení či zmanipulování.

Samotné odcizení však není tím rizikem, kterého by se měly společnosti obávat, rizikem je až následná akce, kterou je možné se zařízením provést po jeho odcizení, ať už je to přístup k citlivým informacím ve firemním e-mailu, přístup k citlivým souborům uloženým na zařízení, ale i přístup k potenciálně citlivým interním systémům apod.

Štěpánka Kochmanová
interní auditor
Magistrát města Plzně

1. Částečně vlastními zdroji (např. oblast správy přístupových oprávnění), specifické oblasti dodavatelsky.

2. Problematice IT je zcela jednoznačně na straně IA naprosto nezbytné věnovat dostatečnou pozornost. Resp. celé oblasti tzv. kyberbezpečnosti.

3. Z pohledu ÚSC je priorita ochrana osobních údajů a archivace dat IS.

Milan Novák
interní auditor
Vojenská zdravotní pojišťovna ČR

1. Interní audit v oblasti IT je u VoZP ČR zajišťován interním auditem pojišťovny, ale i kvalifikovanými externími auditorskými společnostmi.

2. VoZP ČR, stejně tak jako ostatní zdravotní pojišťovny, je správcem množství osobních údajů mnohdy citlivého charakteru (např. databáze čerpání zdravotní péče pojištěnci, a tedy informace o jejich zdravotním stavu). Navíc specifické postavení VoZP ČR spočívá i v tom, že jsou u ni povinně pojištěni vojáci Armády ČR, jejíž některé složky podléhají nejvyšší-

Například v případě e-mailových zpráv to může být získání citlivých interních údajů – v případě pracovníka oddělení lidských zdrojů to mohou být osobní údaje zaměstnanců, údaje o výši jejich platů, v případě vysoké managementu to naopak mohou být informace týkající se hospodaření společnosti, účetní závěrky a další, a to ještě před jejich zveřejněním. Pokud takové informace případná nepovolaná osoba získá, může jich snadno zneužít ke spekulacím na burze, případně může jinak dojít k poškození společnosti z legislativního pohledu.

„S využíváním mobilních zařízení souvisí mnoho rizik“

Citlivé informace nemusejí být ukládány pouze v e-mailovém klientu, ale mohou být uloženy přímo v úložišti zařízení nebo na jeho paměťové kartě, v takových případech hrozí stejná rizika jako při zneužití informací z e-mailového klienta.

Aby společnosti podporovaly své zaměstnance, mohou jim z mobilních zařízení umožnit přístup k interním produkčním systémům. Zpřístupněné systémy mohou být prakticky jakékoliv – od běžných systémů pro schvalování dovolených přes schvalování finančních výdajů až po komplexní ERP systémy. V případě nekorektně zabezpečených mobilních přístupů mohou přístupy do produkčních systémů představovat značné riziko, neboť v případě zneužití mobilních zařízení by případný útočník mohl získat citlivá data společnosti z těchto systémů, případně je i upravovat či mazat, stejně jako je toho schopen oprávněný uživatel.

Dalším bezpečnostním rizikem při komunikaci se systémy společností může být nezabezpečená komunikace. Mobilní zaměstnanci mohou využívat mobilního přístupu do společnosti například skrze veřejné bezdrátové sítě restaurací či letišť. Avšak při používání takovýchto veřejných sítí existuje riziko, že veškerá komunikace směřující ze zařízení zaměstnance do systémů společnosti může být monitorována případnými útočníky, a mohou tak být získány např. přihlašovací údaje zaměstnance k systémům, které mohou být následně zneužity. Určitým bezpečnostním rizikem mohou být i přídavná zařízení, která zaměstnanci připojují ke svým mobilní zařízením pomoci Bluetooth. Aktuálně to mohou být jíž pomalu se rozšiřující tzv. „wearables“ či česky „nositelnosti“, což jsou zařízení, která mohou lidé nosit na svých tělech – typicky se jedná o chytré hodinky či náramky, ale může se jednat například i o chytré šperky, oblečení apod.

„Nositelnosti“ obvykle nemají žádné či velice omezené možnosti zabezpečení, i když mohou obsahovat citlivé informace. Je možné na ně získávat SMS zprávy, v omezené míře e-mailové zprávy či jiné citlivé informace, např. zdravotní informace uživatele apod.

Dále nejsou-li ve společnostech stanovena adekvátní pravidla používání mobilních zařízení pro pracovní účely, nemají společnosti prakticky žádnou kontrolu nad používáním mobilních zařízení v pracovním procesu – nemohou vynucovat bezpečnostní pravidla ani nemohou žádným způsobem kontrolovat zacházení s mobilními zařízeními. Je tak možné, že uživatelé budou moci za užití žádných či minimálních bezpečnostních opatření přistupovat k systémům společnosti, a ohrozit tak jejich fungování. Zaměstnancům též bude umožněno instalovat nekontrolovaně aplikace. Obzvláště u některých platforem tak bude existovat zvýšené riziko instalace škodlivé aplikace – malware, či dokonce spyware, což umožní případným útočníkům získat přístup k datům na zařízení, případně získat kontrolu nad zařízením.

Bez adekvátní kontroly tak společnostem hrozí, že uživatelé nebudou svá zařízení žádným způsobem zabezpečovat nebo je zabezpečí nedostatečně, a data tak nebudou chráněna takovým způsobem, který by společnosti vyhovoval. Zároveň bude možné, že uživatelé budou používat takové mobilní platformy, které jsou nedostatečně zabezpečené, nebo budou používat jejich zastaralé verze, čímž dále sníží celkovou bezpečnost dat na zařízeních.

„Stanovené bezpečnostní požadavky je následně nutné vynucovat na zařízeních zaměstnanců“

Aktuálně jsou mezi uživateli nejznámější platformy Apple iOS, Google Android, Windows Phone a BlackBerry, ačkoliv absolutně nejrozšířenější jsou však pouze Google Android a Apple iOS.

Každá z mobilních platforem je svými vlastnostmi specifická, a to jak z hlediska funkcionality, tak z hlediska svého zabezpečení. Některé platformy jsou tak vhodnější pro osobní použití, zatímco jiné jsou vhodnější pro pracovní použití, ačkoliv současné úrovně zabezpečení nejpoužívanějších platforem se již blíží porovnatelné výši, a to i díky aktivitám výrobců samotných zařízení.

mu stupni utajení, a proto IT musí být technologicky schopno zajistit tento požadavek. Existenci potencionálního rizika zneužití citlivých dat zaměstnanci je nutné brát jako možnou variantu selhání lidského faktoru. Z tohoto důvodu je role auditorů kvalifikovaných právě pro oblast IT nezastupitelná, stejně jako je nezastupitelná činnost auditorů společnosti v průběžném ověřování systému k zajištění oprávněnosti jednotlivých uživatelů.

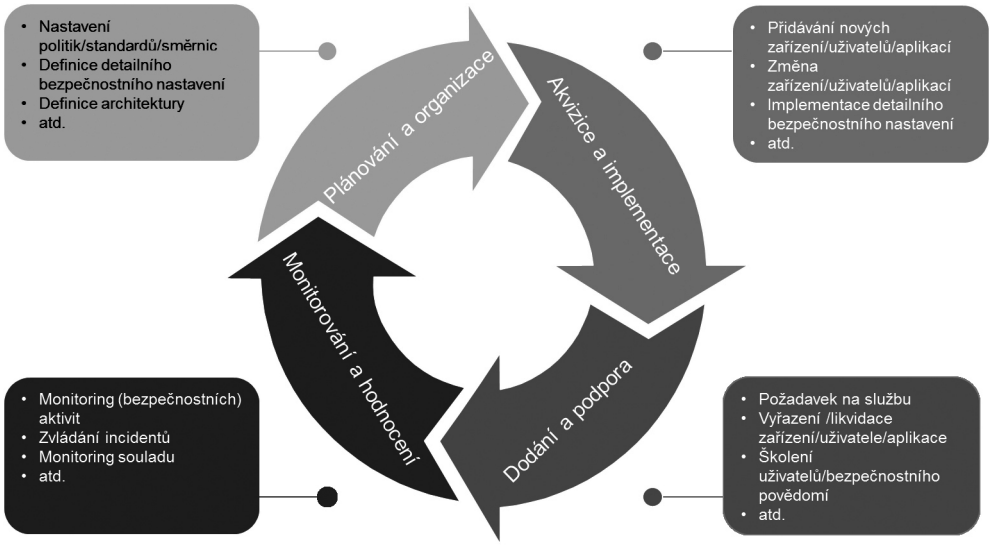
3. Z hlediska interního auditu VoZP ČR je pozornost zaměřena na zajištění systému používání IT jeho uživateli, tj. zaměstnanci. Jedná se především o nastavení přístupových oprávnění, systém rozhodování o stanovení oprávnění pro jednotlivé zaměstnance, evidenci oprávnění do jednotlivých modulů, systém ukončení uživatelských oprávnění v souvislosti s ukončením pracovního poměru, schopnost systému generovat historii vstupů daného zaměstnance do systému, nastavení pravidel pro aktualizaci a změny přihlašovacích podmínek do IT, jak je zajištěn systém zálohování dat a jejich ochrana proti havarijním stavům, systém nastavení vstupů do místností s uložením serverů, nastavení systému nahlížecích funkcí a funkcí operačních apod. Externí, specializovaný audit IT by měl být zaměřen především na testování systému proti napadení, tedy testování odolnosti systému proti neoprávněným vstupům, proti stažení dat, a to jak samotnými zaměstnanci, tak útoky z venčí, tedy měl by identifikovat možné cesty a procesy v IT, které nejsou dostatečně ochráněny.

Zaměříme-li se pouze na nejpoužívanější platformy – Android a iOS, můžeme porovnat jejich úrovně zabezpečení. Ve svých posledních verzích již oba dva systémy šifrují kompletně svůj souborový systém, což snižuje riziko odcizení dat při krádeži zařízení, avšak pouze v případě, kdy uživatel používá heslo k zamčení zařízení. Zároveň dochází k podepisování celého systému, což jej činí obtížněji napadnutelným při jeho startu.

V případě aplikací jsou jednotlivé aplikace spouštěny v tzv. sandboxu, kdy není systémem aplikacím umožněno přímo přistupovat k funkcím systému, kromě povolených funkcí. Získání přístupu k povoleným funkcím se však u obou platforem liší. Zatímco u iOS může uživatel povolit přístup k jednotlivým funkcím v momentě, kdy si je aplikace vyžádá, a má možnost je následně i odebrat, v případě Android musí uživatel při instalaci povolit aplikace využívání všech funkcí, které si žádá. Pokud uživatel nesouhlasí s využitím některých funkcí, nelze aplikaci nainstalovat. Zároveň není možné omezit využívání systémových funkcí v případě, že si to uživatel nepřeje. V systému Android je zároveň možné udělit aplikaci práva správce zařízení, zatímco u systému iOS je tato možnost velice omezena. Do systému iOS zároveň není možné instalovat aplikace jiným způsobem než prostřednictvím Apple AppStore, zatímco systém Android umožňuje instalaci odkudkoliv, pokud to uživatel vyžaduje, což dále zvyšuje možná rizika. Dále je rozdíl v uvádění aplikací do oficiálních distribučních kanálů – zatímco společnost Apple aktivně testuje veškeré uváděné aplikace i jejich aktualizace, společnost Google nechá vývojáře zveřejnit jakoukoliv aplikaci, a pokud se projeví jako škodlivá, dokáže ji společnost Google automaticky smazat ze všech zařízení, kam byla nainstalována.

3. Zabezpečení mobilních zařízení ve firemním prostředí

Aby společnosti mohly umožnit svým zaměstnancům používat vlastní mobilní zařízení, je vhodné zajistit takovou úroveň zabezpečení těchto zařízení, aby bylo možné ochránit data společnosti, ale zároveň aby toto příliš neomezovalo vlastníky zařízení. Předně je tak nutné stanovit bezpečnostní politiky pro používání vlastních mobilních zařízení. Tyto politiky by měly stanovovat, jaké skupiny uživatelů smí používat jaké typy mobilních zařízení, jaký způsob zabezpečení bude u jednotlivých zařízení využíván, měly by tak popisovat kompletní životní cyklus zařízení – od jeho zapojení do prostředí společnosti až po jeho vyřazení. Příklad procesů životního cyklu mobilních zařízení je zobrazen níže:



Stanovené bezpečnostní požadavky by měly vycházet z analýzy rizik společnosti. Běžně se na základě výsledků analýzy rizik a jako základní bezpečnostní opatření stanovuje požadavek na šifrování zařízení a s tím spojené heslo k odemčení zařízení, pro které se stanovuje politika. Ačkoliv nejpoužívanějším heslem k odemčení bývá čtyřmístní číselný PIN, ideálně je používat hesla silnější, neboť čtyřmístný PIN je možné prolomit ve velmi krátkém čase, a získat tak přístup k datům zařízení. Dle rizikového profilu je vhodné také vymezit okruh aplikací, které by uživatel neměl pro svou práci používat – typicky se jedná např. o cloudová úložiště typu Dropbox, One Drive apod. Dle typu společnosti a typu používaných dat je možné rozhodnout také o dalších omezeních, jako je např. omezení fotoaparátu, omezení hlasových asistentů, omezení zálohování do cloudového úložiště a vynucení šifrovaného zálohování do lokálního PC apod. Zároveň, aby bylo možné adekvátně kontrolovat jejich zavedení, je nutné stanovit požadavky na samotná zařízení – je vhodné omezit výběr pouze na některé platformy a také na jejich některé verze (ideálně na některé z nejaktuálnějších).

Takto stanovené bezpečnostní požadavky je následně nutné vynucovat na zařízeních zaměstnanců. K tomuto účelu slouží typicky systémy Mobile Device Management, známé pod zkratkou MDM. Systém MDM umožňuje využívat funkce dané mobilní platformy k její správě. Po instalaci klienta MDM na mobilní zařízení tak správce MDM může získat kontrolu nad zařízením. Systém MDM tak společnostem umožňuje vynutit bezpečnostní nastavení, umožňuje omezit aplikace, které může uživatel na svém

Tomáš Mrkos
interní auditor, Ministerstvo obrany

1. Vlastním interním auditem.

2. S ohledem na současný zákon o kybernetické bezpečnosti a požadavky na bezpečnost v kybernetickém prostředí obecně, ne zcela dostatečný především v otázce kvalifikace interních auditorů.

3. Kybernetická bezpečnost v dikci zákona o kybernetické bezpečnosti. Největší pozornost si podle mého názoru zasluhují akvizice v souvislosti s výstavbou IT systémů (datová úložiště, utajované systémy, rozhraní v rámci veřejné správy i prostředí internetu).

Josef Černý
specialista interního auditu
Metrostav a.s.

1. V útvaru interního auditu máme specialistu na ICT technologie. Interní audity v oblasti IT máme zaměřeny na zabezpečení oblasti ICT (bezpečnost informací, pravidla správy ICT, pravidla uživatelů, TOPO a zneužití prostředků ICT zaměstnanci), na funkčnost aplikací k podpoře procesů, a na zabezpečení dostupnosti služeb ICT (technické interní audity).

2. Systémy ICT obsahují významné informace pro potřeby prováděných zjištění interním auditem a jsou významným zdrojem auditní stopy k za-

zařízení používat, případně umožní nainstalovat tzv. kontejner, v rámci kterého bude docházet k vynucování většiny bezpečnostních požadavků a samotné mobilní zařízení bude dotčeno pouze minimálně.

V případě využití kontejneru je tak možné, aby uživatel přistupoval ke svým pracovním e-mailovým zprávám pouze v rámci daného kontejneru, zároveň může umožnit zpřístupnit některá sdílená úložiště, a usnadnit tak přístup k souborům na cestách. Aby však byla zajištěna bezpečnost takto uložených dat, bývá celý kontejner šifrován a dále umožňuje omezit okruh aplikací, pomocí kterých bude možné otevřít soubory uložené v rámci kontejneru. Toto umožní pouze minimální zásah do uživatelského komfortu a omezí běžné používání mobilního zařízení zcela minimálně.

> „Bezpečnost mobilních zařízení nebude už jen okrajovou záležitostí“

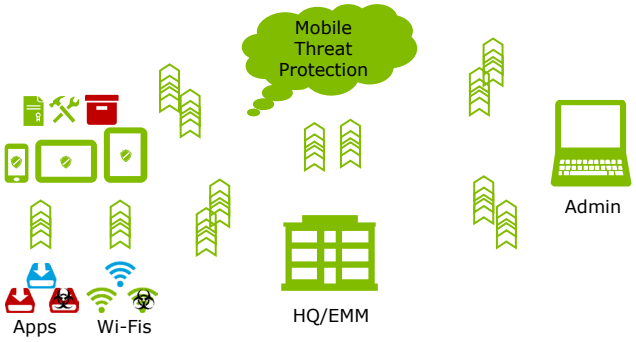
Systém MDM také umožňuje monitorovat dodržování bezpečnostních zásad a následně omezit funkcionality povolené společností v případě, kdy dojde k porušení některé z bezpečnostních zásad. Např. v případě, kdy uživatel na své zařízení nainstaluje aplikaci, která není povolena, např. Dropbox, MDM zjistí přítomnost nepovolené aplikace a může zakázat či omezit přístup ke kontejneru s daty společnosti, případně pokud dojde ke hrubému porušení bezpečnostních zásad, dokáže smazat celý kontejner a odebrat veškeré přístupy k systémům společnosti či v nejhorším případě smazat kompletně mobilní zařízení.

Fungování systému MDM je obecně znázorněno na následujícím schématu:

Administrátor systému nastaví bezpečnostní požadavky v rámci systému MDM, který následně bezpečnostní požadavky vynutí na mobilních zařízeních, nastaví některá výchozí nastavení, např. připojení k firemní Wi-Fi síti, e-mailový účet uživatele, a také nainstaluje kontejner. Zároveň nainstaluje aplikaci, která je nutná pro práci v rámci společnosti a také jednu aplikaci zakáže. Následně bude systém MDM mobilní zařízení monitorovat a v případě nesouladu některého nastavení, může omezit funkčnost firemních aplikací.

Nastavení MDM je však statické a nedokáže aktivně odolávat nově vznikajícím hrozbám. Např. administrátor nastaví seznam zakázaných aplikací, které by měl MDM zakázat, avšak nové aplikace přibývají každý den, a administrátor by tak musel pravidelně sledovat všechny nové aplikace a aktualizovat seznam zakázaných aplikací tak, aby splňoval bezpečnostní požadavky společnosti. K tomuto účelu již nyní existují systémy Mobile Threat Protection, zkráceně MTP, které dokáží dynamicky upravovat bezpečnostní nastavení mobilních zařízení dle aktuálních podmínek. V takovémto případě administrátor nastaví seznam zakázaných aplikací a následně v rámci systému MTP vybere, jaké typy aplikací mají být zakázané. MTP bude monitorovat nové aplikace i nové aktualizace a v případě, že některé z nich budou odpovídat nastavení, budou automaticky přidány do seznamu zakázaných aplikací. Mimo jiné dokáže MTP reagovat na rizika v bezdrátových sítích.

Fungování systému MTP je obecně znázorněno na následujícím diagramu:



Situace odpovídá předešlému diagramu. Systém MDM vynutil bezpečnostní nastavení, nainstaloval kontejner a aplikaci a monitoruje soulad zařízení s požadavky. Správce MTP nastavil typ aplikací, které by neměly být používány. Zatímco je uživatel na cestách, připojí se do bezdrátové sítě, kterou MTP identifikuje jako potenciálně nebezpečnou. Pomocí systému MDM tak zakáže přístup ke kontejneru společnosti. Mezitím je publikována nová aplikace, která odpovídá profilu zakázaných aplikací. Aplikace je systémem MTP identifikována a následně přidána do seznamu

jištění důkazů o prováděných činnostech. Systémy ICT jsou součástí podpory většiny řídicích procesů v organizaci a nástrojem k zajištění komunikace v procesním řízení společnosti.

3. Interní audit se zaměřuje na prověření bezpečnosti systému ICT proti narušením z vnějšího prostředí, na prověření dostupnosti aplikací a informací pro plynulé provádění procesů v organizaci a na prověření zajištění Business Continuity. Pro potřeby ujištění o kontrolní činnosti prověřuje oblasti využitelných dat.

Jaroslav Chlouba
vedoucí interního auditu
Pojišťovna VZP, a.s.

1. Není v silách interního auditu v naší společnosti obsáhnout celou problematiku IT do většího detailu, takže čas od času je nutno využít služeb najatých specialistů.

2. Co se týká pozornosti interního auditu ve vztahu k problematice IT je zajištění její pozornosti neoddiskutovatelné z mnoha důvodů. Mezi nejvýznamnější patří určitě pořizovací náklady – a to jak HW, tak i SW. Neméně významná je také otázka využívání IT a personálních kapacit. V řadě

zakázaných aplikací v prostředí MDM. MTP tak umožňuje systému MDM dynamicky reagovat na vznikající hrozby, čímž zvyšuje celkovou úroveň bezpečnosti používaných mobilních zařízení.

> „Zabezpečení mobilních zařízení je odsouváno nebo řešeno pouze minimálně“

4. Audit zabezpečení mobilních zařízení

V případě auditu bezpečnosti mobilních zařízení by se měl auditor zaměřit jak na kontrolu příslušných politik, tak na jejich následné vynucení pomocí technologických nástrojů.

Politiky a jejich bezpečnostní požadavky by měly reflektovat rizika identifikovaná v rámci analýzy rizik. Obsah politik by měl korespondovat s životním cyklem mobilních zařízení. Politiky by též měly zohledňovat právní požadavky – v případě BYOD patří mobilní zařízení zaměstnancům, a je proto obtížné omezovat jejich používání, respektive aplikovat omezení přístupu k systémům společnosti formou smazání celého mobilního zařízení. Zároveň by politiky měly specificky definovat nakládání s informacemi o poloze uživatele zařízení, neboť v případě zapojení mobilního zařízení uživatele do systému MDM mohou být polohová data automaticky sbírána systémem. V takovém případě může společnost neoprávněně shromažďovat osobní údaje uživatele. V ideálním případě by též politiky měly stanovovat různé skupiny uživatelů s různými druhy oprávnění a přístupů – typicky je možné se setkat se skupinou nejvyššího vedení, která má přístup k nejcitlivějším informacím, a měla by proto mít nejvyšší úroveň zabezpečení, dále jsou to zaměstnanci s přístupem k citlivým údajů, což jsou běžně pracovníci HR oddělení, pracovníci finančního oddělení, oddělení prodeje apod., třetí skupinou bývají ostatní uživatelé.

Bezpečnostní požadavky na jednotlivé skupiny by měly obsahovat požadavky na mobilní platformy a jejich verze, povolené či zakázané aplikace a detailní bezpečnostní nastavení pro dané platformy.

Soulad s bezpečnostními politikami je následně nutné ověřit v nastavení jednotlivých skupin systému MDM. V tomto případě je však nutné klást důraz na to, co společnost považuje za MDM řešení. Mnoho společností se domnívá, že zabezpečení poskytované technologií Exchange ActiveSync běžně používanou e-mailovými servery je srovnatelné se zabezpečením poskytovaným systémy MDM. Avšak poskytovaná úroveň ochrany je v tomto případě zcela minimální a nemůže aktuálně systém MDM nahradit.

5. Závěr

Zabezpečení mobilních zařízení je stejně komplexní, ne-li komplexnější záležitostí než zabezpečení běžných stolních počítačů či laptopů, a i přesto společnosti věnují vysoké úsilí zabezpečení počítačů, zatímco zabezpečení mobilních zařízení je odsouváno nebo řešeno pouze minimálně. Mobilní zařízení jsou součástí našich životů a čím dál více operací bude možné provádět právě z nich. Společnosti by se tak měly připravit, že bezpečnost mobilních zařízení nebude už jen okrajovou záležitostí. ■

[stokkete] © 123RF.COM

případů se ani kvalifikovaný interní auditor neobejde bez pomoci specialisty na oblast IT formou outsourcingu.

3. Kromě již uvedených finančních otázek ve vztahu k hospodárnému a efektivnímu využívání IT a potřebného servisu, nabývá na významu v poslední době také zajištění bezpečného provozu a ochrana dat před zneužitím.

Ludmila Jiráňová
vedoucí interního auditu a kontroly
ČHMÚ

1. Interní audit v každém roce prověřuje oblast IT dle plánovaných auditů. Jedná se o osm oblastí od spolehlivosti IT až po kybernetický zákon.

2. Problematika IT je v ČHMÚ na předních místech. Pozornost v oblasti IT je důležitou součástí při poskytování výsledků z našich odborných činností – meteorologie, hydrologie a čistoty ovzduší. Máme čtyři interní auditory IT, kteří prověřují spolehlivě zadaná témata interních auditů.

3. Zaměřujeme se v současné době na kybernetický zákon – nastavení pro ČHMÚ, dokumentace a postupy. Byl jmenován Výbor kybernetické bezpečnosti. ■

Změny v přístupu útočníků za posledních pět let a další výhled (1. díl)

Jiří Slabý
Senior Manager IT & Security Consulting
Deloitte Czech Republic

Lidská společnost se stále více spoléhá na online prostředky, které tak nabývají na hodnotě a stávají se lákavým cílem pro útočníky všeho druhu. S tím roste význam zabezpečení těchto prostředků i související infrastruktury. Historie je v mnoha případech zdrojem poučení pro lepší přípravu na budoucnost.

S trochou nadsázky lze říci, že neuplyne týden, aby se neobjevila nová kritická zranitelnost, a měsíc, aby se nějaký incident neobjevil na předních stránkách novin. To, že se bezpečnost dostává do hlavního zpravodajství, je dobrá zpráva. Jednotlivci i organizace tak častěji vnímají bezpečnost jako důležitý faktor, a nikoliv jako nutné zlo. Již dávno neplatí, že cílem útočníků jsou jen systémy umístěné v temných sálech velkých korporací, nýbrž každý jednotlivec, který pracuje s internetem a využívá nějaké služby. Zde jsou podle nás nejzajímavější události v oblasti kybernetické bezpečnosti minulých pěti let v ČR a zbytku demokratického světa[1].

Posledních pět let u nás a ve světě

Následující souhrn obsahuje jen několik málo nejzajímavějších a nejzásadnějších bezpečnostních událostí daného roku u nás a ve zbytku západního světa. Je však na místě upozornit, že kritéria jako „nejzajímavější", „největší", „nejzásadnější" apod. jsou kritérii subjektivními. Neexistuje jednotné měřítko, podle kterého by se závažnost nebo zajímavost útoků měla posuzovat. Nejčastěji používaným měřítkem je velikost dopadu útoku na organizaci nebo jednotlivce, měřená penězi. Avšak i tak je velice zavádějící, neboť vždy se jedná o hrubý odhad, jak veliký finanční dopad měla ztráta daných dat na chod organizace.

Prezentovaný seznam je výběrem autorů.

Rok 2010

Svět

O zranitelnosti SCADA systémů se dlouho teoretizovalo, ale v červnu 2010 byl zachycen vzorek malwaru Stuxnet, který byl velmi přesně zacílen na sabotování íránského jaderného programu. Šlo navíc o první – oficiálně nepotvrzený – malware vytvořený státem, v tomto případě USA.
Závěr a přelom roku pak patřil WikiLeaks a s tím souvisejícím DDoS útokům skupiny Anonymous na společnosti Visa, Mastercard, Paypal a další.

ČR

V ČR byl rok 2010 poměrně klidný. Velké banky se potýkaly se skimmingem i phishingovými kampaněmi[2], Česká pošta před vánočními svátky čelila DDoS útoku na aplikaci zajišťující hromadné online objednávky[3].

Rok 2011

Svět

Tento rok probíhal ve znamení krádeží dat a hackingu skupin Anonymous a Lulzsec. Asi největším útokem bylo ukradení milionů identit uživatelů herní konzole Playstation od Sony a hacknutí e-mailů od největšího poskytovatele e-mailu zdarma, společnosti Google. V tomto případě jsou podezírání hackeři z Číny.[4]

ČR

U nás jsme tento rok zaznamenali vlnu případů phishingu, napadeno bylo mnoho finančních institucí a pozor si museli dát například i zákazníci internetových providerů.
Česká spořitelna a Raiffeisenbank se potýkaly se zvýšeným počtem podvodných e-mailů, které se snažily vylákat z klientů využívajících internetové bankovnictví údaje o platebních kartách. Útočníci se snažili přimět adresáty kliknout na odkaz falešného internetového bankovnictví, a následně vložit údaje o jejich platební kartě.[5, 6]

Rok 2012

Svět

Počátek působení špionážního malware Turla se datuje do roku 2012 a sahá až do dnešních dnů. Tento malware se zaměřuje především na počítačové systémy vlád a velvyslanectví. Jeho působení není destruktivní, ale vykazuje prvky špionáže, neboť se zaměřuje na citlivé informace, které předává útočníkům. Celý kybernetický útok se dá rozdělit na tři hlavní části: V první části je

[1] Článek čerpá z mnoha veřejně dostupných zdrojů. Je však vhodné zmínit, že například o bezpečnostních incidentech v Číně existují jen strohé záznamy (pokud vůbec), a prezentovaný stav tedy odráží spíše realitu západního světa.

[2] HORÁČEK, Filip. Na bankomatech České spořitelny opět byly falešné čtečky – iDNES.cz [online]. c2010 [cit. 201604-05]. Dostupný na World Wide Web: http://ekonomika.idnes.cz/na-bankomatech-ceske-sporitelny-opet-byly-falesne-ctecky-pz0-/ekonomika.aspx?c=A100816_182730_ekonomika_fih

[3] ŠŤASTNÝ, Jiří. Hackeři útočí na Českou poštu, firmy nemůžou podávat on-line objednávky - iDNES.cz [online]. c2010 [cit. 2016-04-05]. Dostupný na World Wide Web: http://ekonomika.idnes.cz/hackeri-utoci-na-ceskou-postu-firmy-nemuzou-podavat-on-line-objednavky-13o-/ekonomika.aspx?c=A101209_200754_domaci_js

[4] 2011 CyberAttacks Timeline – HACKMAGEDDON [online]. c2011 [cit. 2016-04-05] Dostupný na World Wide Web: http://www.hackmageddon.com/2011/06/22/2011-cyberattacks-timeline/

[5] FIŠER, Miloslav. Raiffeisenbank čelí phishingovým podvodům – Novinky.cz [online]. c2011 [cit. 2016-04-05] . Dostupný na World Wide Web: http://www.novinky.cz/internet-a-pc/221377-raiffeisenbank-celi-phishingovym-podvodum.html

[6] MERAVÁ, Tereza. Podvodníci zaútočili na klienty UPC. Rozesílají jim falešné e-maily – iDNES.cz [online]. c2011 [cit. 2016-04-05]. Dostupný na World Wide Web: http://mobil.idnes.cz/podvodnici-zautocili-na-klienty-upc-rozesilaji-jim-falesne-e-maily-1d8-/mobilni-operatori.aspx?c=A111111_100559_mob_operatori_mer

využit spear phishing a watering hole útok pro infikování cíle trojským koněm Wipbot. V druhé části již zmíněný trojský kůň vytvoří v systému zadní vrátka, čímž připraví skrytou cestu pro infikování systému trojským koněm Turla. Zde nastává třetí část útoku, kdy Turla začíná dlouhodobě shromažďovat důležitá data. Turla se aktivuje vždy při zapnutí počítače.

ČR

Známé hackerské hnutí Anonymous v lednu 2012 zablokovalo pomocí DDoS útoku stránky České protipirátské unie (ČPU). Důvodem bylo prohlášení ČPU, ve kterém schvalovala zablokování stránek služby Megaupload.[7]

Další DDoS útok od hnutí Anonymous směřoval na stránky Ochranného svazu autorského (OSA); důvodem byl nesouhlas Anonymous s mezinárodní obchodní dohodou ACTA, jejímž účelem je vytvoření mezinárodního systému pro vynucování duševního vlastnictví.[8]

DDoS útokům skupiny Anonymous se nevyhnula ani Občanská demokratická strana (ODS). Útočníci nejprve provedli klasický DDoS útok a následně prolomili zabezpečení stránek a obsah nahradili svým vlastním. Podařilo se jim ukrást 30 000 jmen členů ODS. Tento seznam rozeslali médiím se vzkazem politikům, aby odmítli mezinárodní obchodní dohodu proti padělání ACTA.[9]

V únoru hacktivisté napadli web poslanecké sněmovny pomocí DDoS útoku; správci sítě se rozhodli web odpojit, a ten byl nedostupný až do časných ranních hodin.[10]

Jako událost s bezpečnostním přesahem je třeba vnímat i počin umělecké skupiny Ztohoven „Morální Reforma", kdy byli schopni v krátkém časovém úseku rozeslat poslancům PS PČR přes 500 podvržených SMS.[11]

> „V srpnu a září 2013 pak některé banky v ČR zasáhl zatím asi nejsofistikovanější útok"

Rok 2013

Svět

K události, která nenávratně změnila svět (nejen) IT bezpečnosti, došlo v květnu 2013, kdy bývalý systémový inženýr americké Národní bezpečnostní agentury (NSA) a senior advisor pro CIA Edward Snowden zveřejnil přes 1,7 milionu tajných dokumentů NSA. K jejich ukradení použil svůj administrátorský účet a SSH klíče svých kolegů.[12] Snowdenovy dokumenty jsou stále zpracovávány, nicméně světu odhalily dlouhodobé masové sledování a odposlouchávání ze strany západních tajných služeb ve spolupráci s komerčními poskytovateli služeb a infrastruktury.

V říjnu 2013 došlo k uzavření největšího mezinárodního ilegálního obchodního portálu Silk Road a zatčení jeho majitele a provozovatele Rosse Ulbrichta. Tento portál používal systém TOR zajišťující anonymizaci uživatele při pohybu na internetu. Aféra měla bohužel za následek pouze zrod řady následovníků a upozornila veřejnost na existenci „darknetu". K dopadení Ulbrichta nakonec zřejmě přispělo sledování a korelace pohybu bitcoinů, které mají (nepřesně) pověst naprosté anonymity.

Dne 20. března 2013 proběhlo v Jižní Koreji několik kybernetických útoků, které byly pojmenovány „DarkSeoul". Tyto útoky cílily na řadu vládních webových stránek, jako například na webové stránky ministerstev, vojenských velitelství, amerických sil v Jižní Koreji a hlavních bankovních institucí v regionu. Odhaduje se, že bylo zasaženo okolo 40 vládních a firemních webových stránek. Při využití speciálního malware bylo možné provést útok typu DDoS. Pro tento útok se předpokládalo využití až 11 000 osobních počítačů, které byly nakaženy škodlivým kódem.

Od června 2013 bylo ruskou skupinou Dragonfly napadáno velké množství webových stránek organizací činných v odvětví energetiky. Nejvíce zasaženy byly organizace nacházející se v USA a západní Evropě. Internetové stránky byly infikovány škodlivým malware a přesměrovaly návštěvníky na stránky, které obsahovaly Lightsout exploit kit. Tento kit kontroloval software, který návštěvník používal. Toho bylo využito k získání kontroly nad napadeným počítačem. Z napadených počítačů v několika zemích získala skupina řadu informací, které mohou v budoucnu ohrozit operátory energetické rozvodné sítě, řadu podniků zabývajících se výrobou energie, provozovatele ropného potrubí a poskytovatele průmyslových zařízení.

Za největší krádež roku 2013 je v neposlední řadě považován únik až 110 milionů záznamů osobních údajů a kreditních karet zákazníků sítě obchodních domů Target.

ČR

V březnu do ČR nečekaně přišly masivní DDoS útoky a zastihly cíle nepřipravené. Po zpravodajských serverech byl úspěšně napaden největší lokální portál Seznam.cz a následující den také stránky řady českých bank, což v jednom případě vedlo i k výpadkům POS terminálů.

Poměrně primitivní útok v řádu jednotek Gbps byl veden zřejmě z Ruska a nikdo se k němu nepřihlásil, motivace zůstává nejasná. Dle délky výpadků lze usuzovat, že s tímto typem hrozby a v daném rozsahu chyběly praktické zkušenosti na všech úrovních

[7] WIFT. Útok Anonymous na web České protipirátské unie a co je to vlastně DDoS? – Útok na web ČPU a její reakce | Diit.cz [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://diit.cz/clanek/utok-anonymous-na-web-ceske-protipiratske-unie-a-co-je-to-vlastne-ddos

[8] NÝVLT, Václav – KUŽNÍK, Jan. Anonymous napadli servery OSA, web české vlády i Evropského parlamentu – iDNES.cz [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://technet.idnes.cz/anonymous-napadli-servery-osa-web-ceske-vlady-i-evropskeho-parlamentu-1mp-/sw_internet.aspx?c=A120126_134112_sw_internet_nyv

[9] Hackeři zveřejnili osobní data tisíců členů ODS – ČT24 – Česká televize [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.ceskatelevize.cz/ct24/domaci/1181108-hackeri-zverejnili-osobni-data-tisicu-clenu-ods

[10] PELECH, Tadeáš. Web sněmovny byl nepřístupný – jak se bránit DDoS? | Computerworld.cz [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://computerworld.cz/analyzy-a-studie/web-snemovny-byl-nepristupny-jak-se-branit-ddos-44521

[11] Morální Reforma [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://ztohoven.com/mr/index-cs.html

[12] ESPOSITO, Richard – COLE, Matthew. How Snowden did it – NBC News [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.nbcnews.com/news/other/how-snowden-did-it-f8C11003160

infrastruktury, nicméně následné rychlé korektivní kroky CSIRTu i zasažených institucí tento typ útoků výrazně ztížily.

V červenci pronikl do hlavních zpráv bezpečnostní incident Penzijní společnosti Komerční banky, kdy bylo možné bez zvláštních nástrojů a zcela otevřeně získat osobní údaje přibližně 50 000 občanů z databáze kontaktů. Zranitelnost byla objevena náhodou a urychleně odstraněna, avšak bohužel pro KB až po zveřejnění.[13] Tento incident podtrhuje důležitost bezpečného životního cyklu softwaru, dohledu nad dodavateli a pravidelného penetračního testování.

V srpnu a září pak některé banky v ČR zasáhl zatím asi nejsofistikovanější útok, napadající dvoufaktorovou autentizaci a autorizaci pomocí SMS zpráv. Prvním krokem bylo získání přihlašovacích údajů do internetového bankovnictví. Útočníci poté pomocí velmi kvalitního phishingu přesvědčili oběti k instalaci „bezpečnostní aktualizace" na svůj smartphone. Tento malware (Hesperbot) ve skutečnosti zachytával autorizační SMS zprávy a přeposílal je útočníkům. Výše ztrát, kterou cílové banky zaznamenaly, nebyla sdělena. Údajně však byli útočníci výjimečně rychlí ve vyklízení účtů, na které si prostředky převáděli. Následnou analýzou tohoto malware bylo zjištěno, že mohl být snadno použit pro útoky na další banky na českém a slovenském trhu.[14, 15, 16]

> „V dubnu 2014 byla objevena jedna z doposud nejzávažnějších chyb v zabezpečení v historii internetu"

Rok 2014

Svět

V dubnu 2014 byla objevena jedna z doposud nejzávažnějších chyb v zabezpečení v historii internetu. Chyba s názvem Heartbleed v protokolu OpenSSL umožní útočníkům zachytávat datový přenos po do té doby důvěryhodném zabezpečeném protokolu HTTPS. Heartbleed otřásl především důvěrou veřejnosti v bezpečnost open source, přestože nikde nedocházelo k zatajování detailů o chybě. Dále došlo k několika mohutným krádežím dat – JPMorgan Chase (86 milionů záznamů zákazníků), Home Depot (56 milionů záznamů zákazníků), iCloud („citlivé" fotografie a videa některých celebrit) a Sony (obrovský objem interní komunikace).

ČR

U nás byl rok 2014 ve srovnání se světem relativně klidný. Pokračovaly phishingové kampaně a skimming; incidenty však nijak nevybočovaly z běžné praxe a již se ani v tak hojné míře neobjevovaly v masmédiích.

Rok 2015

Svět

V únoru byla oznámena krádež osobních údajů klientů americké zdravotní pojišťovny Anthem.[17] V červnu obvinily USA Čínu z kybernetického útoku, při kterém byla ukradena data čtyřem miliónům zaměstnanců vládních organizací s bezpečnostní prověrkou. Cílem útoku byl vládní personální úřad (OPM) a ukradena byla citlivá data jako jména, čísla smluv sociálního pojištění a data narození osob, které byly „jen" v evidenci tohoto úřadu. V červenci skupina „The Impact Team" získala a posléze zveřejnila data 37 milionů uživatelů internetové seznamky „pro nevěrné" Ashley Madison. Na tomto příkladu je nejjasněji vidět, že uživatelé služby utrpí mnohem větší škodu než cíl útočníka.

Kampaň Carbanak/Anunak, která byla objevena a popsána v únoru 2015, údajně způsobila bankám celkové ztráty ve výši jedné miliardy dolarů. Ponecháme-li stranou spornou výši škody a její rozsah, výjimečná je přesnost provedení, kdy útočníci při podvodných transakcích věrně napodobovali chování konkrétních uživatelů, aby transakce nevypadaly neobvykle, a vyhnuly se tak odpovídající kontrole.[18]

ČR

I Českou republiku zasáhla vlna ransomware. Zajímavá je perfektní lokalizace podpůrného „ekosystému", včetně nastavení cen odpovídajících lokální příjmové rovině (v řádech tisíců korun). Platba probíhá vesměs v bitcoinech. Phishing se začal vyskytovat na sociálních sítích a kvalita standardního e-mailového phishingu trvale rostla. Na přelomu roku se útočníkům z rasistické skupiny White Media podařilo proniknout na soukromý e-mailový účet premiéra Bohuslava Sobotky a zveřejnit několik e-mailů z jeho schránky. Podle poskytovatele služby Seznam.cz se nejednalo o hackerský útok jako takový, protože na e-mailovém účtu nedošlo k žádné podezřelé aktivitě. Útočník už heslo musel znát, když se na e-mailový účet připojoval. Je tedy pravděpodobné, že útočníci premiérův počítač předem napadli.[19]

Pokračování příště

[13] SLÍŽEK, David. Chyba v bankovnictví Komerční banky umožňovala přístup k datům o klientech – Lupa.cz [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.lupa.cz/clanky/chyba-v-bankovnictvi-komercni-banky-umoznovala-pristup-k-datum-o-klientech/

[14] Komerční banka. ČBA varuje před novou formou hackerských útoků – Komerční banka [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.kb.cz/cs/o-bance/tiskove-centrum/tiskove-zpravy/cba-varuje-pred-novou-formou-hackerskych-utoku-1712.shtml

[15] PELANTOVÁ, Petra – Euro. Jak vysát konta. Hackeři dál útočí na české banky [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://euro.e15.cz/archiv/jak-vysat-konta-hackeri-dal-utoci-na-ceske-banky-1040752

[16] PERMAN, Tomáš. ESET odhalil trojana, který ohrožoval klienty českých bank [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/article/eset-odhalil-trojana-ktery-ohrozoval-klienty-ceskych-bank/

[17] PERLROTH, Nicole. Anthem Hacking Points to Security Vulnerability of Health Care Industry – The New York Times [online]. c2015 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0

[18] GReAT. The Great Bank Robbery: the Carbanak APT – Securelist [online]. c2015 [cit. 2016-04-05]. Dostupný na World Wide Web: https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

[19] MIKULKA, Milan. Ochranu hackeři neprolomili. Znali heslo, nebo skenovali Sobotkův počítač, brání se Seznam – Aktuálně.cz [online]. c2016 [cit. 2016-04-05]. Dostupný na World Wide Web: http://zpravy.aktualne.cz/domaci/utocnici-skenovali-premieruv-pocitac-nebo-znali-heslo-k-jeho/r~9fd7924cb55311e5928a002590604f2e/

Školení auditorů v Českém hydrometeorologickém ústavu

Milan Rybák
System & GIS specialist
Český hydrometeorologický ústav

Před čtyřmi roky jsem byl požádán vedoucím interního auditu k vytvoření školení pro interní auditory Český hydrometeorologický ústav (ČHMÚ). Všichni interní auditoři jsou uživatelé PC a občas provádějí interní audit na oblasti IT. Spolupráce se rozvinula. Školím interní auditory pravidelně každý rok v dubnu a říjnu. Prezentace probíhá v délce asi tří hodin, plus dotazy. Vybral jsem pár základních informací, které je nutné určitě vědět a průběžně si opakovat. Říkám „opakování je matka moudrosti".

Školení auditorů v ČHMÚ podle Zákona o kybernetické bezpečnosti

Věnujeme se především těmto tématům:

A/ Aktuální bezpečnostní hrozby.

1) Probereme si rizika politiky BYOD (Bring Your Own Device) a mobilním útokům.
2) Co jsou Embedded zařízení a jakým způsobem mohou být infikována.
3) Dalším bodem bude Windows, což je stále jedna z nejcíleněji-ších platforem vzhledem k majoritnímu rozšíření.
4) Koukneme také na exploity – hlavně se zaměříme na děravé doplňky internetových prohlížečů:

– Flash,
– Adobe Reader,
– Java.

Dále rizika sociálního inženýrství a dolování peněz z neznalých uživatelů.
A nakonec cílené útoky na společnosti.

B/ Pověry v informačních technologiích.

- Antivirus je mrtvá technologie.
- Nejlepší antivirus je žádný antivirus.
- Linux/Mac je bezpečný systém.
- Windows je nebezpečný OS.
- Brouzdání po bezpečném internetu.

Skutečnost:

- Bezpečný internet = nebezpečná pohádka, kterou byste neměli krmit ani malé děti.
- Apple OS X byl v posledních letech několikrát velmi úspěšně napaden; např. virus Flash back infikoval 600 000 počítačů s Apple OS X během 14 dnů.
- Linux repository = zdrojem všech distribucí Linuxu, včetně dalšího sw. Byl úspěšně napaden v srpnu 2011.

Trvalo 17 dní, než si toho správce vůbec povšiml. V té době každý správce linuxových serverů a pracovních stanic nevědomky instaloval exploity.

- => Bezpečný operační systém ani jiný software neexistuje! (Viz další kapitola.)

C/ Efektivní obrana?

Principy:

1) Poučení zaměstnanců.
2) Pravidla pro zacházení s daty.
3) Stanovení základních pravidel bezpečnosti.
4) V případě infiltrace motivovat zaměstnance k řešení této situace.
5) Chránit koncové stanice bezpečnostním softwarem.
6) Ukládání logů operačních systémů => možnost zpětné analýzy.
7) Každý článek bezpečnosti spolu souvisí.

Ukážeme si možnosti uživatelů, jak se bránit proti těmto hrozbám na příkladu nejrozšířenějšího operačního systému Windows.

1) Nevypínat základní bezpečnostní prvky OS (UAC, firewall…)
2) Nastavit bezpečné (= komplexní) uživatelské (min. 9 znaků) i administrátorské heslo (min. 12 znaků).
3) Nepoužívat vestavěné anonymní účty (např. Administrator).
4) Nepracovat v účtu s admin právy, pouze v účtu s omezenými právy (v OS Windows je to účet skupiny Users).
5) Nesvěřovat svůj účet ani heslo jiné osobě.
6) Práce s poštou a poštovními klienty typu MS Outlook: číst i odesílat veškeré zprávy ve formátu čistého textu.
7) Nepoužívat nechráněné protokoly typu http, ftp, telnet aj. pro zadávání kritických hesel ani pro citlivou komunikaci (např. s bankou).
8) Používat plně aktualizovaný Windows + bezpečnostní systém + všechny síťové programy.
9) Zablokovat ve firewallu veškerou příchozí komunikaci.
10) Nepřipojovat k internetu operační systém s citlivými daty (účetnictví, databáze, hesla).
11) Zakázat nebezpečné funkce Windows (autorun, autoplay...)
12) Nastavit všechny používané i-prohlížeče do bezpečného režimu, tj.:
    a/ nastavit Vysoké zabezpečení,
    b/ povolit Chráněný režim.

Bezpečnost svou a své výpočetní techniky má každý ve svých rukou.

V ČHMÚ se pravidelně opakují v interních auditech oblasti IT a to během tří let na všech pracovištích:

- Spolehlivost IT (řízení incidentu, řízení problému, řízení změny a hodnocení spolehlivosti IT).
- Rozvoj SW (pořizování, evidence, vyřazení nebo převod, oprava, stažení, kontrola).
- Umisťování dat na internet.

K naplnění požadavků **Zákona o kybernetické bezpečnosti v ČHMÚ** povede ještě dlouhá cesta. Výbor kybernetické bezpečnosti pracuje naplno a výsledky se projednávají na poradách vedení. Výsledky se dostanou do plánu interních auditů nebo budou vypsány audity mimořádné. **Bezpečnost zaměstnanců i pracovních výsledků je na předním místě v činnostech ČHMÚ.** ■

Audit kybernetické bezpečnosti ve veřejné správě

Ing. Lucie Veselá, CIA
ředitelka odboru Interní audit,
Ministerstvo financí ČR

Mgr. Stanislav Klika
senior manažer, BDO Audit s.r.o.

Dne 1. ledna 2015 nabyl účinnosti zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále také „zákon o kybernetické bezpečnosti"). Zákon zavádí do českého právního řádu povinnost vykonávat tzv. audit kybernetické bezpečnosti. Cílem tohoto článku je nastínit možné přístupy k sladění úkolů interního auditu[1] orgánů veřejné správy v oblasti správy a řízení bezpečnosti informací (Information Security Governance) s tímto specifickým druhem ujištění.

> „Stěžejním kritériem pro vymezení vztahu auditu dle ISO norem k internímu auditu dle IPPF jsou podmínky pro zajištění jeho nezávislosti a objektivity"

Zájem organizací o bezpečnost jejich dat, informací a informačních systémů roste s jejich vzrůstající závislostí na těchto fenoménech a s jejich stále větším napojením na sítě elektronických komunikací[2]. Parlament České republiky schválením zákona o kybernetické bezpečnosti vyjádřil potřebu tuto oblast regulovat na zákonné úrovni.

Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Kybernetickým prostorem se podle tohoto zákona rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací[3]. Zákon ukládá správcům informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému v rozsahu nezbytném pro zajištění kybernetické bezpečnosti zavést a provádět bezpečnostní opatření pro zmíněné systémy, které spravují, a vést o bezpečnostních opatřeních bezpečnostní dokumentaci[4]. Bezpečnostním opatřením se rozumí i kontrola a audit kritické informační infrastruktury a významných informačních systémů[5]. Zákon o kybernetické bezpečnosti obsah a rozsah bezpečnostních opatření blíže nevymezuje a odkazuje na prováděcí právní předpis. Tím je vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Vyhláška stanoví, že v rámci kontroly a auditu kybernetické bezpečnosti se posuzuje soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a provádí a dokumentují pravidelné kontroly dodržování bezpečnostní politiky[6]. Pojem „audit kybernetické bezpečnosti" je legislativní zkratkou a zahrnuje shora uvedené činnosti.

[mindscanner] © 123RF.COM

Vyhláška stanoví, že správci informačního systému kritické informační infrastruktury a správci komunikačního systému kritické informační infrastruktury určí role manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, garanta aktiva a auditora kybernetické bezpečnosti.[7] Vyhláška nepožaduje, aby byl auditor kybernetické bezpečnosti zaměstnancem příslušného správce. Je tedy možné pro zajištění této role najmout externistu.

[1] V režimu zákona č. 320/2001 Sb., o finanční kontrole.

[2] Poptávka organizací po systematickém řízení rizik vztahujících se k informacím a informačním systémům se odráží v rozmanité nabídce různých rámců (pojetí) řízení, které lze pro účely zvládání těchto rizik využít (např. COBIT, normy řady ISO/IEC 27000 atd.). Tyto rámce se liší přístupem, včetně důrazu na různé procesy a kontroly, šíří svého záběru a samozřejmě i mírou obecnosti. Zmíněné rámce řízení mohou pro auditory také představovat východisko (kritérium) pro plánování a provedení auditu.

[3] § 2 písm. a) zákona o kybernetické bezpečnosti.

[4] § 4 odst. 2 ve spojení s § 3 písm. c) až e) zákona o kybernetické bezpečnosti.

[5] § 5 odst. 2 písm. m) zákona o kybernetické bezpečnosti.

[6] § 15 odst. 1 vyhlášky o kybernetické bezpečnosti. Uvedené povinnosti jsou adresovány správcům podle § 3 písm. c) až e) zákona o kybernetické bezpečnosti. Proto se domníváme, že povinnost v rámci auditu kybernetické bezpečnosti určit opatření a zohlednit výsledky kontrol v plánu rozvoje bezpečnostního povědomí a v plánu zvládání rizik není určena auditorovi kybernetické bezpečnosti, a to také s ohledem na požadavek jeho nezávislosti.

[7] § 6 odst. 2 vyhlášky o kybernetické bezpečnosti.

Na správce významného informačního systému jsou kladeny nižší požadavky a nemusí definovat roli auditora kybernetické bezpečnosti, a tedy ani provádět audity kybernetické bezpečnosti prostřednictvím této role[8]. Auditor kybernetické bezpečnosti musí svoji roli vykonávat nestranně a výkon jeho role musí být oddělen od ostatních bezpečnostních rolí. Jiné záruky nezávislosti auditora kybernetické bezpečnosti vyhláška nestanoví. Vyhláška dále předepisuje kvalifikační předpoklady pro auditora kybernetické bezpečnosti: auditor musí být pro tuto činnost proškolen a prokázat odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let[9]. Správci informačního systému kritické informační infrastruktury a správci komunikačního systému kritické informační infrastruktury jsou povinni v rámci systému řízení bezpečnosti informací nejméně jednou ročně zajistit prostřednictvím auditora kybernetické bezpečnosti provedení auditu kybernetické bezpečnosti[10]. Auditor kybernetické bezpečnosti v rámci auditu hodnotí také správnost a účinnost zavedených bezpečnostních opatření[11]. Vyhláška podrobněji postupy auditu kybernetické bezpečnosti neupravuje. Vzhledem k tomu, že právní úprava kybernetické bezpečnosti vychází zejm. z řady norem ISO/IEC 27000, tyto normy více přiblížíme.

Řada norem ISO/IEC 27000 je dílem Mezinárodní organizace pro normalizaci ISO a Mezinárodní elektrotechnické komise (IEC). Předmětem úpravy ISO/IEC 27000 je řízení bezpečnosti informací. Jádro tvoří norma ISO/IEC 27001:2013 – Systémy řízení bezpečnosti informací – Požadavky a jak plyne z názvu, upravuje strukturu a vlastnosti systému řízení bezpečnosti informací (Information Security Management System – ISMS). ISMS je definován jako část celkového systému řízení organizace, založená na řízení rizik. Způsob řízení ISMS je zaměřen na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací (bližší informace jsou uvedeny v normě ISO/IEC 27000 – Přehled a slovník ISMS). Aby organizace mohla tvrdit, že její procesy jsou ve shodě s normou ISO/IEC 27001:2013, musí splnit všechny její požadavky. Norma ISO/IEC 27001 je založena na modelu PDCA[12] (Plan – Do – Check – Act), tedy na cyklu plánuj – dělej – ověřuj – jednej. Smyslem PDCA je zajistit stálé zlepšování systému řízení. Z pohledu normy ISO/IEC 27001 fáze „plánuj" představuje ustavení ISMS, včetně vymezení jeho rozsahu, hranic, identifikace a zhodnocení rizik a výběr příslušných opatření k jejich zvládání. Zavádění a provoz ISMS včetně realizace bezpečnostních opatření odpovídá fázi „dělej" a fáze „ověřuj" se uskutečňuje prostřednictvím monitorování a přezkoumávání ISMS. Pomyslný cyklus je završen fází „jednej" údržbou a zlepšováním ISMS.

Pravidla pro provádění auditů ISMS lze nalézt v normě ISO/IEC 27007: 2011 – Směrnice pro auditování systému řízení bezpečnosti informací. S touto normou však při auditování ISMS vystačit nelze. Text zmíněné normy totiž obsahuje velké množství odkazů na normu ISO 19011:2011 – Směrnice pro auditování systémů managementu, která pro auditory ISMS představuje východisko pro uplatňování principů a postupů auditování.

> „Interní audit může prověřovat i fungování funkce auditu kybernetické bezpečnosti"

Abychom mohli definovat audit dle ISO/IEC 27007:2011 a ISO 19011: 2011 v kontextu jiných ujišťovacích funkcí organizace, a to zejména ve vztahu k internímu auditu podle Mezinárodního rámce profesní praxe interního auditu (IPPF), je nutné popsat nejen základní principy plynoucí z norem ISO/IEC 27007: 2011 a ISO 19011: 2011, ale také pochopit, jak se vyvíjel přístup Mezinárodní organizace pro normalizaci ISO k auditování systémů managementu. První normy ISO (např. 10011) upravující audit systému managementu vznikly v návaznosti na vydání normy ISO 9001 upravující systém řízení kvality v roce 1987. Cílem ISO 9001 je dosahování kvality (jakosti) – slovy této normy – stupně splnění požadavků souborem inherentních charakteristik. Přístup podle ISO 9001 lze tedy popsat jako zaměření úsilí organizace na dosahování shody s požadavky. Tím byla do značné míry určena i orientace a východiska auditu upraveného již zmíněnými doprovodnými normami a obecně budoucí zaměření auditu dle ISO norem[13].

Podstatná je skutečnost, že rizikově orientovaný přístup se do úpravy auditu systémů managementu ISO dostává jen pozvolna a ani v poslední verzi ISO 19011: 2011 není důsledně akcentován (s riziky však více „pracují" normy řady 27000). Ani jiné aktivity charakteristicky spjaté s interním auditem, jak je definován v IPPF, nejsou normami ISO upraveny. Tak například ISO auditor může (ale také nemusí, pokud to nebylo stanoveno jako cíl plánu konkrétního auditu) poskytovat doporučení ke zlepšení procesů, a to na základě své auditní (ujišťovací) činnosti. Oproti tomu výsledkem činnosti interního auditora pracujícího podle IPPF musí být přidaná hodnota organizaci při zaměření se na tři hlavní vzájemně propojené oblasti: řízení rizik, řídicí a kontrolní

[8] § 6 odst. 3 vyhlášky o kybernetické bezpečnosti.

[9] § 6 odst. 6 vyhlášky o kybernetické bezpečnosti.

[10] § 3 odst. 1 písm. f) vyhlášky o kybernetické bezpečnosti.

[11] § 15 odst. 2 vyhlášky o kybernetické bezpečnosti.

[12] Podobně jako např. řada ISO 9000 upravující systém řízení kvality, řada ISO 14000 upravující systém řízení vztahu k okolí a norma ISO 45001 upravující řízení bezpečnosti a ochranu zdraví při práci.

[13] Dalším přírůstkem do skupiny norem upravující systémy managementu byla v druhé polovině devadesátých let norma 14001 upravující systém řízení vztahu k okolí. Tu opět následovaly normy, jejichž předmětem byl audit systému řízení vztahu k okolí inspirované úpravou auditu systému řízení kvality. V roce 2001 pak byla vydána norma ISO 19011: 2002 – Směrnice pro auditování systémů řízení kvality a systémů řízení vztahu k okolí, která nahradila předchozí samostatné standardy pro audit systémů managementu a jejímž cílem bylo zajistit větší kompatibilitu postupů při auditování. Posledně jmenovanou normu nahradila v roce 2011 norma ISO 19011: 2011, se stejným názvem, která je stále platná (připravuje se však další revize). Je vhodné doplnit, že uvedené normy upravují jak tzv. „interní" audity (audity první stranou), které provádí organizace sama, tak tzv. „externí" audity – tedy audity druhou a třetí stranou – prováděné externími subjekty. V prvním případě jde o audity v rámci dodavatelského řetězce, v druhém případě jde o audity za účelem získání certifikace souladu s příslušnou ISO normou.

[Leo Wolfert] © 123RF.COM

procesy a řízení a správu organizace. Interní auditor tohoto cíle dosahuje jak v návaznosti na výstupy z provedených auditů, tak jako poradce a klíčový partner řídicích a kontrolních orgánů organizace. Jednou z dalších nevýhod auditování dle ISO norem je, jak bylo naznačeno výše, jejich vývojem podmíněná závislost na jednotlivých rámcích systémů managementu podle ISO (a to i přes snahy o větší obecnost norem pro auditování).

Stěžejním kritériem pro vymezení vztahu auditu dle ISO norem k internímu auditu dle IPPF jsou podmínky pro zajištění jeho nezávislosti a objektivity. ISO 19011: 2011 stanoví pouze, že auditoři mají provádět svou práci nestranným způsobem, tj. ve všech případech být spravedliví a nepodjatí a vnímat veškeré vlivy narušující jejich úsudek v rámci provádění auditu (srov. 4 Principy auditování, a) Integrita). Všude, kde je to proveditelné, mají být auditoři nezávislí na auditované činnosti a mají ve všech případech jednat způsobem, který vylučuje předpojatost nebo konflikt zájmů. U interních auditů mají být auditoři nezávislí na provozních manažerech auditovaných funkcí (srov. 4 Principy auditování, e) Nezávislost). Pro účely ISO norem postačí, když osoba, která audit provádí, nebyla předtím odpovědná za činnost, která je předmětem auditu, nejsou požadována jiná opatření na zajištění nezávislosti. Naproti tomu IPPF stanoví celé spektrum nástrojů k zajištění jak funkční, tak organizační nezávislosti. Funkce auditu dle ISO/IEC 27007: 2011 a ISO 19011: 2011 sice disponuje určitou úrovní nezávislosti, avšak tato omezená míra nezávislosti není dostatečnou zárukou pro zajištění skutečně objektivního ujištění adresovaného řídicím a kontrolním orgánům organizace. Z pohledu modelu tří linií obrany tak audit ISMS dle ISO/IEC 27007: 2011 a ISO 19011: 2011 spadá do druhé linie obrany[14].

Ze shora uvedeného dále plyne, že interní audit musí řídicím a kontrolním orgánům organizace podávat ujištění i o fungování funkce auditu ISMS dle ISO/IEC 27007: 2011 a ISO 19011: 2011. To by současně mělo přispět k naplňování standardů 2110.A2, 2120.A1 a 2130.A1. Funkce interního auditu by zásadně neměla přebírat odpovědnosti patřící funkcím druhé linie obrany. Vždy by se měla vyvarovat převzetí manažerské odpovědnosti za řízení rizik. Pokud však některé odpovědnosti funkcí druhé linie obrany převezme, musí být přijata opatření snižující riziko ztráty objektivity ujištění podávaného interním auditem. Platí také, že funkce interního auditu by měla navázat úzkou spolupráci s funkcemi druhé linie obrany, včetně funkce auditu ISMS dle norem ISO/IEC 27007: 2011 a ISO 19011: 2011. Interní audit se v zájmu zamezení duplicity činností může také za určitých podmínek spolehnout na výsledky práce jiných poskytovatelů ujištění.

Shora uvedené poznatky je třeba nyní konfrontovat s legislativní úpravou auditu kybernetické bezpečnosti a interního auditu. Útvar interního auditu podle zákona o finanční kontrole je nadále odpovědný za poskytování nezávislého a objektivního ujištění o fungování zavedených informačních systémů a o spolehlivosti jimi shromažďovaných, zpracovávaných, uchovávaných a předávaných informací. To může znamenat, že interní audit může

[14] Uvedeným závěrům dle našeho názoru není na překážku označení ujišťovací činnosti vykonávané podle ISO/IEC 27007: 2011 a ISO 19011: 2011 termínem „audit". Pokud bychom vyšli např. z definice auditu použité Davidem N. Ricchiutem v jeho knize Audit (Auditing), pak bychom na audit nahlíželi jako na „systematický proces objektivního získávání a vyhodnocování informací o ekonomických činnostech a událostech, s cílem zjistit míru souladu mezi těmito informacemi a stanovenými kritérii a sdělit výsledky zainteresovaným zájemcům". Jak některé funkce v rámci druhé linie obrany, interní audit dle IPPF, tak i tzv. statutární audit by naplňovaly výše uvedené znaky auditu. Všechna tato pojetí auditu se však také vzájemně liší, zejména již zmíněnou mírou nezávislosti, předmětem poskytovaného ujištění nebo adresáty, kterým je toto ujištění poskytováno. I česká legislativa upravuje „audity" různého zaměření, účelu a poskytovatelů. Proto lze již na tomto místě předjímat, že právní normy týkající se auditu kybernetické bezpečnosti stanovené zákonem o kybernetické bezpečnosti budou existovat samostatně vedle norem upravujících interní audit stanovených zákonem 320/2001 Sb., o finanční kontrole.

prověřovat i fungování funkce auditu kybernetické bezpečnosti. Kromě spolupráce těchto dvou funkcí mohou existovat i další možnosti, jak zajistit povinnosti stanovené zákonem a vyhláškou o kybernetické bezpečnosti, a to zejm. s ohledem na skutečnost, že postupy auditu kybernetické bezpečnosti nejsou vyhláškou o kybernetické bezpečnosti upraveny a vyhláška neodkazuje na použití mezinárodních standardů.

„Může například nastat situace, že vedoucí orgánu veřejné správy pověří zajištěním role auditora kybernetické bezpečnosti zaměstnance zařazeného v útvaru interního auditu“

Může například nastat situace, že vedoucí orgánu veřejné správy pověří zajištěním role auditora kybernetické bezpečnosti zaměstnance zařazeného v útvaru interního auditu. Ustanovení § 29 odst. 4 zákona o finanční kontrole stanoví, že útvar interního auditu nelze pověřovat úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů. Pokud by tedy nastala zmíněná situace, je nutné, aby vedoucí orgánu veřejné správy a vedoucí útvaru interního auditu přijali účinné zásady a postupy pro zajištění nezávislosti a objektivity interního auditu. Těmi rozumíme především přímou podřízenost útvaru interního auditu vedoucímu orgánu veřejné správy a jeho organizační oddělení od řídicích a výkonných struktur, nezávislost v plánování činnosti, podávání zpráv vedoucímu orgánu veřejné správy[15] a výkon auditu dle IPPF. Tyto postupy je pak nutné promítnout do dokumentace předepsané zákonem a vyhláškou o kybernetické bezpečnosti[16]. ■

[15] § 29 odst. 1, § 30, § 31 odst. 1 zákona č. 320/2001 Sb., o finanční kontrole.

[16] Např. § 6 odst. 1 vyhlášky o kybernetické bezpečnosti.

[dizanna] © 123RF.COM

Přehled řady norem ISO/IEC 27000

ISO/IEC 27000: 2016 – Přehled a slovník	**Stanoví základní pojmy používané při řízení bezpečnosti informací, přehled řady norem ISO/IEC 27000 a úvod do ISMS a základní popis PDCA.**
ISO/IEC 27001: 2013 – Systémy řízení bezpečnosti informací – Požadavky	**Stanoví (závazné) požadavky na ISMS.**
ISO/IEC 27002: 2013 – Soubor postupů pro řízení bezpečnosti informací	**Popisuje vhodná (doporučená) bezpečnostní opatření.**
ISO/IEC 27003: 2010 – Směrnice pro zavádění systému řízení bezpečnosti informací	**Obsahuje doporučení pro postup zavedení ISMS.**
ISO/IEC 27004: 2009 – Měření řízení bezpečnosti informací	**Upravuje pravidla pro sledování účinnosti ISMS.**
ISO/IEC 27005: 2011 – Řízení rizik bezpečnosti informací	**Upravuje pravidla pro řízení rizik bezpečnosti informací.**
ISO/IEC 27006: 2015 – Pravidla certifikace ISMS	**Upravuje pravidla při udělování certifikací ISMS.**
ISO/IEC 27007: 2011 – Směrnice pro auditování systému řízení bezpečnosti informací	**Upřesňuje pravidla pro provádění auditů ISMS. Doplňuje normu ISO 19011: 2011 – Směrnice pro auditování systémů managementu.**
ISO/IEC TR 27008: 2011 – Směrnice pro auditory o řízení (kontrolách) bezpečnosti informací	**Poskytuje návod k přezkoumávání implementace a fungování kontrol bezpečnosti informací.**

Interview with IIA 2015–2016 Chairman of the Board Lawrence J. Harrington, CIA, QIAL, CRMA

Performed by Petr Hadrava, Internal Audit Manager, MetLife

Larry Harrington is global chairman of The IIA, and chief audit executive (CAE) for Raytheon Company, which specializes in defense, civil government, and cybersecurity markets throughout the world. Prior to joining Raytheon in 2004, he led the internal audit function for several Fortune 100 companies, where he also served in other areas, including finance, human resources, and operations.

Committed to corporate diversity, Harrington has been a member of Raytheon's Executive Diversity Leadership Team since 2010, guiding the company's strategy to advance its culture of diversity and inclusion. Further, he was a key driver in the development of a diversity strategy for The IIA during his service on the North American Board of Directors.

Over the last 25 years, Harrington has held numerous leadership roles with The IIA that have positioned him well for his term as global chairman. A member of the Global Board of Directors since 2009, he has served as senior vice chairman of the Board, and as vice chairman of both the Professional Guidance and the Global Services Committees. He is also past chairman of the North American Board of Directors and the Professional Issues Committee, and past president of The IIA's Greater Boston Chapter.

Harrington earned a bachelor's degree in accounting from Bentley University, and has completed Harvard's Advanced Management Program. He has continually invested in himself by achieving professional certifications to grow his internal audit competencies and learn about the business functions within the scope of his internal audit responsibilities. He is a frequent speaker at seminars on auditing, change management, people development, and motivation.

For his term as The IIA's global chairman, Harrington chose the theme, "Invest in Yourself." Throughout the year, he is urging internal auditors to enhance their value by undertaking professional development opportunities. From reading topical and timely material, to adding professional certifications, to attending conferences and workshops in internal auditing and on the business functions they audit, internal auditors can improve their own professional skills and opportunities and better serve their organizations and stakeholders.

Petr: Today it is a great pleasure for me to meet with Larry Harrington, the Global Chairman of The IIA. Good afternoon Larry, welcome to the Czech Republic. It is great to have you here.

Larry: This is my first time here, and I have to tell you Prague is absolutely beautiful city. People are very friendly, and my wife and I have been enjoying the city for the weekend. The weather was supposed to be not so nice, but The IIA made the difference and the sun came out and it turned out to be a beautiful weekend.

Petr: That's nice to hear! Are you visiting only the Czech Republic or is your visit here a part of a wider tour?

Larry: We are on a tour across more countries. We started in Oslo speaking at the conference and then we went to Frankfurt, from Frankfurt to Copenhagen, from Copenhagen to Prague, and we will finish with a speech in Amsterdam. My chairmanship ends in July 2016, and this is my last tour. When I finish my chairman's year, I will have been to almost two dozen countries, and, within the United States, in almost two dozen Chapters. I have talked to almost twenty five thousand internal auditors during this year.

Petr: So it will be great to listen to your insight today. I hope you will have a lovely stay here in the Czech Republic, and that you will like Prague and that the weather will be nice. And now let's start discussing the main topic of our interview. You as the Global IIA Chairman chose the theme: "Invest in yourself."

Larry: Yes, that's correct.

Petr: I was searching the internet before our interview for your name and for this theme. I found a very interesting discussion on youtube when you were speaking very passionately about this theme. What was the main driver for you to choose this topic?

Larry: Each Chairman selects a theme. And if we recall some of the past themes they are 'Assess our roles', 'Think of the possibilities', 'Say it right' and 'Mind the gap'. I saw how the themes were interrelated to each other, but I also saw that for each of those to be successful one has to invest in themselves to improve your relevance, to be able to learn how to communicate effectively, to think of all the possibilities for creating a good brand. I picked the theme to build on each of the previous themes but focused a little different.

The last fifteen years of studies by the IIA has shown the average investment that an auditor puts into himself has not changed. Yet during these fifteen years we've watched technology explode; we've watched technology change industries and change companies. CEOs today are trying to keep up with all this transformation,

and they have said in certain studies that they struggle with having enough people who understand the need for transformation. We have the skills to drive transformation. Internal auditors are such a unique profession because we see every function in the company, and we look at risk across multiple industries, and so we see how fast business is changing. We can be the change agents that CEOs need to drive change.

I will give you an example. In the Middle East all the budgets were based on US$60-barrel oil. It dropped to US$30-a barrel. I was invited by the governments to speak to internal auditors across the Middle East because they want internal auditors to help them transform, because their revenue is not going to double, and they can't cut expenses into half, so they want internal audit to bring to the table Lean Six Sigma and leading practices. They asked me to come and talk to the profession about how we learn to invest in ourselves and grow the skills that we need in order to help our countries. In the Middle East we were successful.

When I talk to folks from governments, since 2008 almost every country's debt has increased. Interest rates will go back to historical levels at some point. When they do the debt payments are going to consume so much of government spending that either governments around the world will have to dramatically raise taxes, which will have a big effect on the economy, or they will have to cut back, which will also have a dramatical effect. Internal auditors working for government, whether it is local, state or the federal level, bring our skills to evaluate programs that are effective or ineffective or help bring leading practices. Regardless whether it is a non-profit, a for-profit organization or government, internal auditors today have to know so much more, and we can't do that unless we start to invest in ourselves.

You see today that the chairman of AT&T, one of the largest telecommunication companies, has said to all of his employees they must invest in themselves as well, not just what the company does. He has described how fast the telecommunication industry is changing, and if you do not adapt you will become extinct.

And so when you look at it from all different dimensions, investing in yourself is critical. And yet, as a profession we are not investing enough. We as individuals, we are not investing enough. As individuals we rely heavily on what our company does and does not do, and yet today not only do we need to learn internal audit skills, we need to understand risks and business and tools like Six Sigma and Lean and we must become greater at understanding technology and cyber and all of those things that are impacting our company. If we don't, we will not be as relevant as we need to be. Thinking about the possibilities we can bring to our companies is limitless, and helping them close the gaps will help our organizations be successful.

At the end of the day internal auditors are the good people. People often don't look at us as the good guys. We have to work to change our brand, and by helping people see that we grow sales, we can help grow profits. We can help our governments be sustainable.

Petr: Yes, I think internal auditors are in a great position, and you mentioned that. We are expected to have end-to-end mindset, and we can assess the process from the holistic point of view. We are not limited as employees working for a particular department and not caring too much what other departments are doing.

Larry: Absolutely. We can bring leading practices from other industries into whatever industry we are in so that we bring, not only that end-to-end mindset, but also bring business-to-business knowledge and lessons learned and we can really help organizations transform.

Petr: Yes. You also mentioned something I think is critical to us which is being proactive in the sense that if the company is not ready to pay for those conferences and lessons for the internal auditors we should not give up. I think our approach should not be, "The company does not want to pay for it so I do not care. I am not going to invest my time, my money." I expect this is not correct and acceptable approach.

Larry: This is so important. You made a great point. Look at your industry. You are in financial services. Look at how the regulations have changed, everything that you do and how you need to transform. When I talk to some small audit functions they say, "Oh, I do not have a budget for trainings and development." But EY does free webinars, PwC does free webinars, all the service providers do free webinars.

As I travel around the globe what really shocks me is how few people go to the IIA website on a regular basis. On the IIA website we have leading practices. We have Centre of Excellence for Chief Audit Executives. We have a Centre of Excellence for government auditors. We have just created a Centre of Excellence for financial services industry. When PwC puts on the White Paper it is on our website. When EY puts up a White Paper it is on our website, and it's all there for free.

The CBOK (The Common Body of Knowledge) is an example. As I have travelled around the globe for the last year, less then 10% of the people on all the audiences have downloaded even one report from the CBOK. I say to people it doesn't have to be expensive. You have so much free stuff if you want invest your time, and also you can read a business book and understand who are the leaders who have transformed the business.

As young professionals particularly, it is so important to understand that the world is changing, and at the end of the day you can be in front of the change or behind the change. Where do you want to be? Take it from the surfing point of view. Do you want to be in front of the wave, enjoy the ride, or not? So that is why it is so exciting. It is an exciting time for internal auditors. We have to be able to tie the head and heart together and help them understand that we must each of us take control of our own destiny before someone else does. We must have a desire to achieve a continuous learning mindset and to recognize that we can help change the world, but we can only do that with knowledge.

Petr: I think it is our task, the task of internal auditors, to convince the management that we are there for them, that we want truly to help them, that we are not going to look into the past to much, but we are going to focus into the future and show them that we are in the same boat and that their concern is my concern.

Larry: Absolutely. You just hit on another great point. Internal auditors are often accused of looking through the rear view mirror always auditing what happened the last year. Todays' studies show that people want insight and foresight, and that means internal audit has to understand the risk and how risks are changing. We must audit the right things. To be world class you have to be auditing the right things and for auditors to audit the right

things you need to have the right relationships, the right knowledge, the right concerns around the risks and ultimately it is our job to show value every day and the more value we show the more management is going to utilize internal audit and the more they are going to invest in internal audit.

I will give you another idea. This is an investment one should make. Invest 8 hours and read the book written by Richard Chambers: 'Lessons Learned on the Audit Trial'. You will take away some nuggets of gold that you can use in your own career. One of the things that I suggest to people is this. Companies have strategic plans. They look at the industry; they look at the strengths, weaknesses, opportunities, threats; they look at the competitors, their strategies and out of that comes the strategic plan. Out of that come goals and objectives for the CEO, for all of the direct reports and they flow down. So why wouldn't you as an individual have a strategic plan? Why wouldn't you know your strengths, your weaknesses, your opportunities and threats? Why wouldn't you know who the competition is that could get the next job that you want to have and why wouldn't you be investing in yourself so that you can be successful? We need people to thing about themselves as a business and as a business you only have one product. It is called "your knowledge" and you only have one customer. That's who you are working with. That's a pretty high risk business with one customer and one product. So expanding your knowledge, expanding your brand, expanding your reputation is crucial. Bad things will happen in good organizations and imagine that you somehow lose your job. Do you want to be one of three hundred looking for a new job or do you want to have such a brand that you are employed in a second because of your reputation? That's the message we want to get across to people.

Petr: Could you elaborate more how we can invest in ourselves? I am sure there are hundreds and hundreds of possibilities.

Larry: I will give you some easy tips. Number one – going to the IIA website at least monthly and downloading the leadership documents, reading them and sharing them across the internal audit function and utilizing them with your Audit Committee and your management. These documents often provide great talking points for you and your management. Number two – attend the free IIA webinars. Number three – read business books. Number four – get your CIA, get your CISA, get Certified Fraud Examiner certification or other certifications. There are number of them available! Invest in yourself and build your credentials. Utilize the resources of local IIA chapters or institutes who hold training programmes, offer newsletters and other things. This is just to demonstrate what you can do.

I will give you another example. Often when I speak let's say there are ten tables with six people at each table. I will ask if anybody is here with their fellow team members from their work. It happens at one table six hands up. So I say, "You all work together! There are 94 people you don't know. Why are you sitting together? You see each other in the office every day." So another thing we can do is to expand our network, expand our relationships. We all learn from other people if we take the time to build those relationships. And when you are out at the conference or lesson, spend the time with people you don't know. Ask them about the best audits they have done. Ask them about their risk assessment. Learn from each other.

For 75 years the IIA has had one slogan: 'Progress through sharing'. We share everything as a profession. But if you have a small network, how much are you sharing and getting from others? So these are all very inexpensive tips. You can certainly go for advanced degree. You can do lots of symposiums and seminars, but those cost money. There are so many things you can do for free! And what they take is your time.

People say to me sometimes, "Larry I have a work life balance issue." Do you drive to work? If yes, you can listen some of these on iPod, iPad or while you exercise. You have to make the decision. You have to make a commitment in yourself. And then we can find the way to balance those, and we can find them in a very inexpensive way.

Petr: In my opinion if you consider something as a priority your always find time to do it.

Larry: That's correct. That's why every New Year's Eve people make resolutions that on January 1 will give up on. I see you wearing a ring so you must be married. How many children do you have?

Petr: Yes, I am married and have two children.

Larry: Who do they rely on? If you are not investing in yourself, if you do not make yourself more valuable, how does that affect your family? I really try hard, and my message is to convey to people to make it very personal. You are the most important thing in the world, not your company, not your friends. How are you going to succeed in this difficult world if you are not investing in yourself? If the company lays you off tomorrow, they are not going to worry one minute about it. But your wife and your children will be worried about it, and you will have to find another job. It is so important for people to understand that they must control their own destiny.

Petr: As you mentioned expanding the network is very important. Three years ago the auditors in the market did not know what other auditors in other insurance companies were doing in terms of internal audit. They were not sure what risk assessment of others was saying, what audits are being and planned to be performed. With the help of the Czech IIA we introduced regular insurance auditors' roundtable meetings in the effort to close this gap as much as possible. During the roundtable meetings we are sharing the best practices and thoughts just to ensure that we are not missing anything important. This is very valuable.

75th anniversary this year at the global conference — I also would also remind internal auditors that in order for you to understand the products and the things around you, you may need to attend some conferences that are unrelated to internal audit but are all about the business. Because if you do not understand the business, how do you audit the business?

I share with people that when I worked in the consumer products industry I sent one of my auditors to a supply chain conference. Two thousand people – 1,999 supply chain experts and one internal auditor. And she came back with all sorts of connections

Larry: Perfect and how much did that cost?

Petr: Time.

Larry: And did you get any value out of these meetings?

Petr: Yes, absolutely.

Larry: That is the message we need to convey to people. The IIA is the centre of providing that information for you at so little cost, and as a member of the IIA you have access to the websites. You get all the free stuff if you take the time to visit and download the materials.

Petr: You also mentioned the importance of expanding the network. What about the conferences? I guess this is a great place to meet with people you have not met before, listen to and share the ideas, experience and real-life examples.

Larry: Absolutely. But I have a little different twist. While the IIA has great conferences — in fact in New York we celebrate our

and business cards. She was out there with one thing in mind. The company was doing certain things. She wanted to find out how this is done in other companies, what are the lessons learned. She learned so much that when she came back within a month the supply-chain folks hired her out of internal audit because she showed the connection between the business and internal audit, and her inquisitiveness and her network was invaluable to the company. So I also suggest that you think about how you learn more about the industry, and the business, and the challenges, and you will not always learn that at the internal audit conference.

Richard Chambers talks a lot about auditing at the speed of risk to understand how risk is affecting your industry. So understanding the financial services, government, commercial product is critical. Going to some of those programs will really help you understand what your competitors are fearing the most, what they see coming. And it allows you to understand what could impact your company, and what skills and what audits maybe you could do to make a difference.

Petr: Yes, this is actually a great point. I agree that those business Subject Matter Experts are the best partners to learn from.

I discussed this with Richard Chambers recently, that very often we can hear from the executives that internal auditors they are nice guys but they don't understand the business risks, strategic risks, they don't feel comfortable auditing risk management. What are the best ways for internal auditors to improve in these areas?

Larry: I will give you some simple ideas. 1. Build your network. Meet regularly with the heads of different functions in the company. Ask them what magazines they read, and read those magazines. You could read the magazines a month or two after they read them. You don't have to buy those yourselves. As a team you can leverage them so maybe you take one function, I take a different function, and as we read that material, we share with each other those ideas making the most sense and bringing the most value for us. You don't even have to always look for outside programmes if you build your relationships – have a lunch, have a breakfast, have a regular meetings so that you understand what each of those key functions are facing every day, which ones are exceeding goals, which ones are struggling with goals and why.

We ultimately want to make sure that our audit plan is aligned against the key strategies of the company going forward, because if we can help the company achieve its goals and objectives, that means we are helping the company to be successful. And the more successful we can help the company to become the more valuable we are. Auditing something twelve months ago that doesn't change anything. It has no value to the company. So building those relationships of trust is important. What will happen is that someone will call you and say, "I may have a problem. Do you think you could send the team, and help me figure it out?" The more calls you get to come and look at things that are unexpected is a reflection upon your competency and your abilities.

Petr: So it is again about sharing, sharing knowledge, sharing best practices.

Larry: Absolutely. It is about building brand, demonstrating the value that we can bring and the trust. The audit reports should not just be about things they did wrong. We should be known as folks who also talk about the things that have been done well.

Another thing is that we have to understand that we are overhead. People don't like overhead. If we contribute to the success of the organization, people will invest in us; people will build our function; people will come to us when they have a problem. The leading internal audit organizations are spending 20–30% of their time on unplanned audit activities because people trust in them and come saying, "We have a problem here. Bring some resources; help us figuring it out; help us transform that." That's when you know that you made a difference.

Petr: One of the last questions. What innovations can you see coming in the next 5, 10 years? What will need to change within internal audit departments or within the work we do to ensure that we remain relevant?

Larry: Those that are under the age of thirty, who are called Millennials, their brains are developed differently than someone like me. They are used to technology. It is intuitive to them. I see that the biggest change going forward is greater use of tools to analyze big data in order to be involved in cyber and other kinds of themes. What it is going to require is a leader. As an older leader, you will have to welcome them in. You will have to give them opportunities. You will have to showcase to them some of the skills that you have, and learn the skills they have. You will have to empower them and take risk with them to do some of the things that are intuitive to them. Technology will transform internal audit. It is transforming companies. We have to be able to be more nimble; we have to be able to look at big data differently; we have to look at cyber differently, and that means as internal auditors and internal audit leaders we must embrace the younger folks to which the technology has become so intuitive.

As leaders today, and Richard Chambers talks about this in his book, as leaders we must embrace diversity and inclusion, people with different skills. And we must recognize that we give them opportunities because they can help us use the skills and technology that is changing to be able to add that insight and foresight. Anybody can use a rear view camera and decide what was wrong a year ago. For auditor to look into the future, you have to use technology, and you have to connect the dots, and you have to be able to utilize programming techniques that allow you to connect those dots. This is the area that is going to change the most in the next several years.

Also the younger folks do not want to go and sit three days at the conference. They want just-in-time learning. So as a profession we will have to figure out how we provide just-in-time learning. How do we create a library of speakers to enable you to choose three speakers who talk about that topic of your audit, and you review those just before the audit starts so that it is just in time. We will have to transform how we provide the learning opportunities, because they are so used to Googeling the right answer. They are used to getting it when they need it and not three month before because there happens to be seminar in July, September or November. So we will have to transform how to provide knowledge transfer to people.

Petr: And this is also again about keeping up with the speed of risk.

Larry: That's correct. Absolutely.

Petr: That's it for today. It was a great pleasure for me to have this interview with you. What would be your final words and message to the readers of the IIA Journal?

Larry: Take pride in being an internal auditor. We have the greatest job than anyone in any company. Take pride in what you do. Invest in yourself, and add value that no one else in the company can add.

Petr: Thank you so much for your insight and all the best.

Larry: Thank you Petr, and have a nice day. ■

Co je nového v IPPF?

Dr. Antonín Šenfeld, CIA
manažer operačních rizik
AXA ČR/SK

V červnu nám IIA přichystala tři zbrusu nové prováděcí směrnice:

- IG 1010 – Přijetí Definice interního auditu, Etického kodexu a Standardů ve statutu interního auditu
- IG 2500 – Monitorování
- IG 2600 – Předávání informace týkající se přijetí rizika

České překlady těchto směrnic naleznete v příloze tohoto vydání časopisu, což činí zbytečným zde podrobným způsobem probírat jejich obsah. Nicméně mi dovolte vás upozornit na několik zajímavých věcí, a tím vás motivovat k jejich přečtení.

IG 1010 – Přijetí Definice interního auditu, Etického kodexu a Standardů ve statutu interního auditu

Tato prováděcí směrnice poskytuje praktický návod, jak do statutu interního auditu zahrnout požadavek souladu svých činností se stěžejními prvky Mezinárodního rámce profesní praxe interního auditu. Projednání statutu interního auditu s vedením a orgány společnosti tato směrnice považuje za výbornou příležitost pro vysvětlení jednotlivých prvků povinností, které interním auditorům ukládá IPPF.

IG 2500 – Monitorování

Pod tímto poměrně stručným názvem naleznete návody ke správnému nastavení procesů, které bývají souhrnně označovány termínem „follow-up" – následná kontrola plnění doporučení. Tato směrnice zdůrazňuje potřebu nastavení follow-up procesu se zřetelem k požadavkům a očekáváním jak managementu, tak vedení a orgánů společnosti. Směrnice poskytuje několik variant provádění follow-upů:

- Pravidelná čtvrtletní aktualizace stavu aktuálně „splatných" auditních doporučení.
- Samostatné follow-up zakázky u auditů s významnými zjištěními.
- Follow-up v průběhu další auditní zakázky plánované do stejné oblasti.

Je na rozhodnutí vedoucího interního auditu, jaký způsob zvolí, a to zejména se zřetelem k očekávané úrovni rizika souvisejícího s nezavedením auditního doporučení.

Závěrem tato směrnice zmiňuje způsoby, jakými předávat informace o výsledcích follow-upu. Za nejlepší praxi je považováno, pokud je interní audit schopen vyčíslit pozitivní zlepšení (finančního i nefinančního charakteru), kterého bylo dosaženo díky zavedení nápravného opatření.

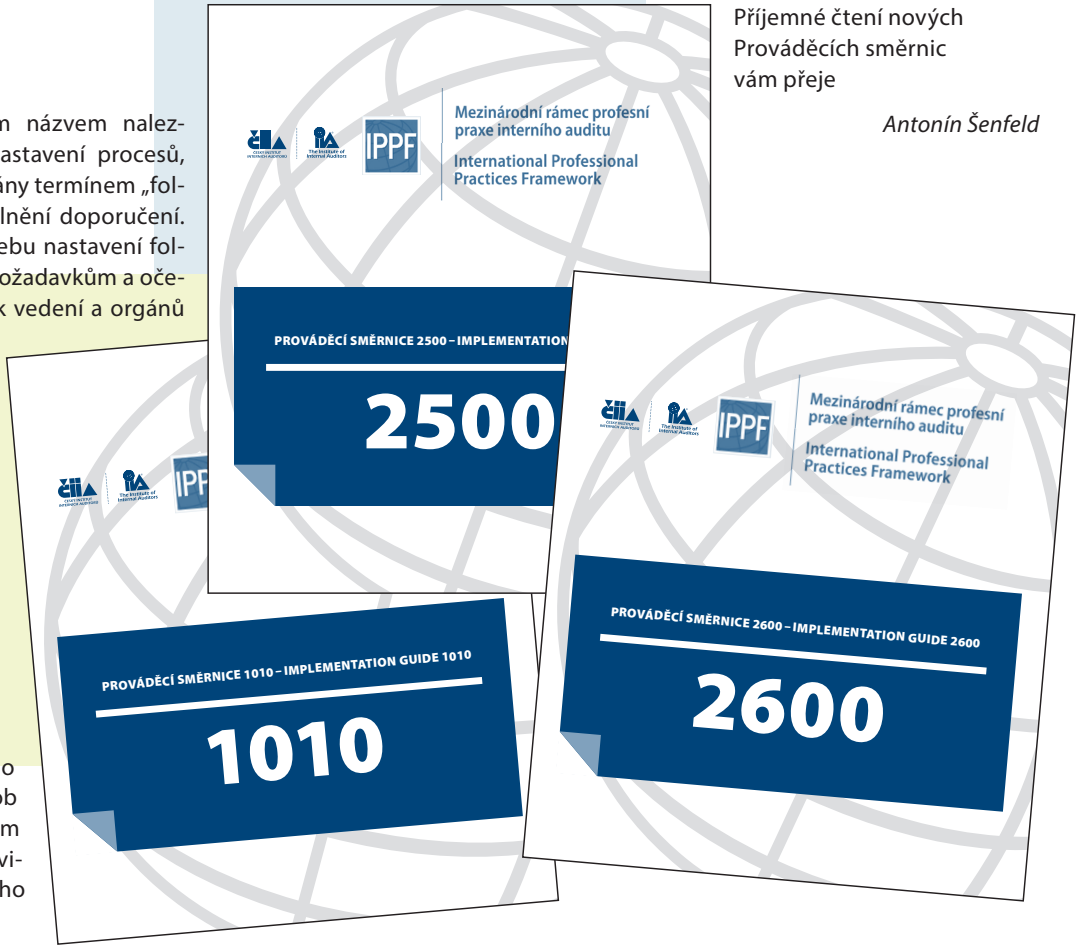
IG 2600 – Předávání informace týkající se přijetí rizika

Tato prováděcí směrnice tematicky navazuje na předchozí směrnici 2500 a zabývá se situacemi, kdy management včas (nebo vůbec) nezavede nápravné opatření, které souvisí s nálezem vysoké rizikovosti, a vystaví tak organizaci nepřijatelnému riziku.

Směrnice poskytuje výčet ostatních činností, které by internímu auditu měly poskytnout ucelený obrázek nejen o aktuálních rizicích, ale také o nově vznikajících rizicích (emerging risks). Za velmi důležité směrnice považuje projednání nepřijatelného rizika s členy managementu s cílem sdílení názorů, pochopení pohledu managementu a dosažení dohody o řešení. Teprve až v případě nedosažení dohody přichází ke slovu eskalace rizika vedení a posléze i orgánům společnosti. Závěrem je uveden přehled jednotlivých typů rizik s vysokou závažností. ■

Příjemné čtení nových Prováděcích směrnic vám přeje

Antonín Šenfeld



Týden v Novém Yorku

Mgr. Tomáš Pivoňka, CIA, CRMA
ředitel útvaru Interní audit ČEZ, a.s.
prezident ČIIA

Na začátku července jsem strávil více než týden v New Yorku. Zúčastnil jsem se tam série akcí Mezinárodního institutu interních auditorů (IIA). Šlo o Global Council a Valnou hromadu IIA, Mezinárodní konferenci IIA a jednání Výboru pro propagaci profese IIA (IIA Global Advocacy committee), jehož jsem členem. Všechny akce byly ve znamení oslav 75 let existence IIA.

Global Council a Valná hromada IIA

Global Council je poradním orgánem Boardu IIA. Je složen ze zástupců jednotlivých národních institutů. Diskuze na Global Council byly vedeny dva dny a jejich hlavním tématem byl Globální strategický plán (strategie) IIA pro roky 2015–2020 a jeho naplňování. Tento plán stojí na následujících čtyřech pilířích: Profesionalita, Propagace profese, IIA jako Globální lídr profese a Budování kapacit. Jednání Global Council jsem se účastnil poprvé a byl to pro mě velký zážitek (vidět zástupce 160 zemí společně pracovat na naplňování strategie IIA). Bez nadsázky mohu říci, že až tady jsem si uvědomil, že IIA je skutečně globální organizací.

Foto 1: Gala večer na Global Council – *zleva:* president ČIIA Tomáš Pivoňka, Angela Witzany (současná prezidentka IIA), Richard Chambers (CEO IIA), Larry Harrington (minulý prezident IIA) a Ladislau Ventura (prezident IIA Angola)

Foto 2: Zástupci z luhů českých na mezinárodní konferenci

Hlavním bodem Valné hromady IIA bylo, podobně jako u Sněmu ČIIA, schválení Výroční zprávy a volba členů Rady a prezidentky IIA, kterou byla zvolena Angela Witzany a my jsme ji měli možnost přivítat na mezinárodní konferenci Praze v minulém roce. Součástí Global Council bylo i setkání prezidentů institutů IIA ze střední a východní Evropy. Na tomto setkání bylo dohodnuto, že budu těmito instituty nominován do Rady Evropské konfederace institutů interního auditu (ECIIA). Velmi jsme si s kolegy užili i gala večer uspořádaný k 75. výročí IIA (viz fota 1 a 3).

Mezinárodní konference IIA

Konference se nesla opět v duchu oslav 75. výročí IIA. Hlavními tématy pak byla vhodně zvolena aktuální témata – geopolitické otázky a rizika podnikání a kybernetická bezpečnost. Osobně mě nejvíc zaujalo vystoupení Iana Bremmera (geopolitolog, profesor na Universitry of New York), a to už jen proto, že nějakou dobu ho sleduji na Twitteru (pro zájemce o geopolitiku vřele doporučuji). Velmi milé bylo na konferenci (tak daleko od domova) potkat kolegy z České republiky a spořitelny ☺ (viz foto 2).

Výbor pro propagaci profese IA

Na jednání výboru byl dohodnut tříletý akční plán, který směřuje k naplnění jednoho ze čtyř pilířů Globálního strategického plánu IIA pro roky 2015–2020, kterým je Globální propagace profese. Na jednání výboru jsem prezentoval i aktivity ČIIA v oblasti propagace IA, zejm. pak oslavy 20 let ČIIA jako případovou studii. Tato prezentace byla přijata velmi pozitivně s řadou doplňujících dotazů.

Foto 3: Prezidenti IIA ČR, Bulharska a Maďarska mají rádi blondýnky ☺

Foto 4: Zavěrečné foto z Global Council (kdo najde prezidenta ČIIA, obdrží dárek ☺)

Bludičky, permoníci a von Däniken

PhDr. Václav Peřich
člen Čestného presídia ČIIA od roku 1996

Zhruba před dvěma dekádami se u jednoho panonského jezera sešla skupina lidí diskutujících o možnostech doplnit některé ze standardů pro vnitřní řízení a kontrolu ve veřejných institucích. Sjeli se z různých kontinentů, a ačkoliv je spojoval společný zájem o zlepšení chodu veřejného sektoru, jejich profesní zkušenost byla také rozmanitá. Izraelský právník představil poznatky, které v jeho zemi udělali po přijetí prvního zákona o interním auditu z roku 1992, skandinávští ekonomičtí experti prezentovali působivé analýzy velkých objemů dat o fungování programů veřejné podpory v sociální oblasti, britští a američtí počítačoví odborníci referovali o úskalích informatizace různých veřejných agend. Diskuze probíhala v živém, a vlastně nadějném ovzduší. Všechna vystoupení podávali zaujatí a přesvědčiví odborníci, většinou přímí autoři nebo spolutvůrci těch technických řešení či odborných materiálů, které byly prezentovány.

Nálada se však poněkud pozměnila, když došlo na téma možného využívání tehdy prudce se rozvíjejícího internetu. Nepochybně bylo velmi lákavé integrovat územně rozprostraněné informační sítě veřejných institucí pomocí tohoto rychle a slibně se šířícího prostředí, avšak část přítomných odborníků s internetovými zkušenostmi vyrukovala s řadou varování. Tvrdili, že internet vytváří záludné a těžko hájitelné prostředí, které se osvědčilo v síti akademických a vzdělávacích institucí, ale je příliš riskantní pro organizace s cennými daty bez možnosti komunikovat po vlastní separátní síti. Samozřejmě se ozvali zastánci internetu a argumentovali mimo jiné tím, že jde o problematiku technicky řešitelnou správným uplatněním šifrovacích algoritmů a technik.

> „Hrozby virtuálního světa představují nikoli permoníci či bludičky, nýbrž hackeři“

Tato diskuze neskončila ukončením oficiálního denního programu. Ovládla potom ještě neformálně vedenou debatu po večeři. Všechny nás velmi zaujal a také pobavil jeden Brit, ostatně obdivovatel G. K. Chestertona a J. R. R. Tolkiena, líčící prostředí internetu jako tajuplný paralelní svět s řadou zvláštností a odlišností. Poukazoval zejména na to, jakou rychlostí se celá ta veliká soustava sítí rozvíjí, jak masivně přibývá uživatelů a kapacity přenosů. „Nemůžeme toutéž rychlostí postihnout všechny způsoby nových a záludných hrozeb, které tam vzniknou. Jaké škody už nadělaly za deset let počítačové viry i na samostatně pracujících počítačích, co teprve na tak rozvětvené síti…“ tvrdil.

A navázal malebným výkladem rozvíjejícím myšlenky Ericha von Däniken o mimozemšťanech. Všechny legendy a pohádky o kouzelnících, skřítcích a magických formulích jsou prý jen naivně tradovanou vzpomínkou na zkušenost našich předků s mimozemšťany. Vysoce inteligentní a technologicky skvěle vybavení návštěvníci z vesmíru tehdejší lidi oslňovali svými technickými kousky, pro jaké nebylo jiné než čistě magické vysvětlení. Všichni „ETs“ pak z nějakých důvodů naši planetu opustili a zůstalo po nich jen něco nevysvětlených úkazů a ty legendy i pohádky o proměnách kamení ve zlato, o létajících lidech, o vílách tančících na vodě a o zaklínadlech, u nichž už si nikdo nemohl pamatovat, že to nebylo ABRADA-KABRA, ale obyčejný povel či klávesová zkratka k nějaké aplikaci. Vypravěč to byl skvělý, a navíc dobrý společník. A nejspíš své alegorické výklady nemyslel nijak vážně, ale jako starý a zkušený informatik si určitě vážné starosti s budoucím vývojem dělal.

Nejednou jsem si na něj vzpomněl, jak by například reagoval osvícenský vzdělanec, kdyby byl svědkem naší hlasové aktivace zdánlivě nečinného iPhonu a následného telefonického hovoru, nebo zadání povelu pro 3D tiskárnu, aby „vytiskla“ model Guggenheimovy galerie v Bilbau. Nepokoušely by se o něj myšlenky na magii nebo podivné bytosti? Nám všem je však jasné, že hrozby virtuálního světa představují nikoli permoníci či bludičky, nýbrž hackeři – vzpomínka na onoho starého skeptika se mi totiž vybavila úplně stejně, když jsem si v brožuře IIA z letošního července přečetl konstatování prezidenta významné společnosti pro IT bezpečnost RSA Amita Yorana, že odvětví kybernetické bezpečnosti selhává[1]. Brožura ten výrok uvádí v souvislosti se statistikou incidentů za poslední dobu, podle které rychle vzrůstají jak počty incidentů, tak způsobené škody. Např. průměrná výše škody na jedno prolomení ochrany dat se zvýšila ze 3,52 milionů USD v roce 2014 na 3,79 milionů USD v roce 2015, přičemž v jednotlivých případech škody dosahovaly i u renomovaných firem desítek milionů USD. Tyto mimořádně závažné incidenty byly vyvolány vcelku banálními útoky vpašováním malweru do fingované zprávy od obvyklého dodavatele napadené společnosti.

To nejsou moc povzbudivé zprávy pro interního auditora působícího u organizace, jejíž agendy jsou z velké části provozovány s podporou informačních technologií napojených na veřejné sítě. Přitom pro společnosti existují ještě záludnější hrozby spojené s informačními technologiemi v širším slova smyslu. Prezident IIA Richard Chambers v červnu na svém blogu uveřejnil velmi zajímavý příspěvek k falšování emisí dieslových motorů s titulem: „Zvýší tento skandál povědomí o hodnotě interního auditu?“ Aniž by sám blíže rozebíral téma „diesel scandal“, upozorňuje na stanovisko dvou investorských skupin (PIRC a ISS), z něhož lze vyčíst, že obě významné investorské skupiny poukazují u postižených

[1] Global Perspectives: Issue 4, Internal Audit as Trusted Cyber Adviser, IIA Altamona Springs, 2016-July, 15p.

organizací na absenci funkce silného interního auditu, který by byl náležitě zasvěcen do všech oblastí strategického směřování společnosti, a tedy příslušných rizik. V té souvislosti je pak srozumitelnější důraz většiny posledních publikací IIA na zapojení manažerů interního auditu do strategického plánování a do spolupráce s klíčovými manažery a odborníky informačních technologií nejen ve firemním informačním systému, ale také ve všech útvarech společnosti, jejichž činnost je pro organizaci důležitá. Obdobně je kladen důraz také na co nejtěsnější spolupráci s partnery (stakeholders), když se zvažuje vyhodnocování rizik v povaze vzájemných kontaktů nebo při navazování produktových řetězců. Ilustrovat to může např. skutečnost, že v září 2015 německý list Bild am Sonntag uvedl s odvoláním na interní vyšetřování Volkswagenu, že automobilka již v roce 2007 obdržela dopis od dodavatelské firmy Bosch, ve kterém byla upozorněna, že software dodaný automobilce není určen pro běžný provoz automobilů, a varovala před možným nezákonným využíváním tohoto softwaru. Není moc pravděpodobné, že by firemní struktury zabývající se řízením rizik nebo interním auditem o tomto dopise cokoli věděly stejně jako o podvodném zlepšováku falšujícím výsledky testů. Není na místě spekulovat co by – kdyby. Rozhodně je však na místě vytrvale usilovat o náležité postavení interního auditu v komplexním hodnocení rizik, včetně těch, která vyplývají z pokusů snižovat firemní náklady používáním informačních technologií. Rovněž je nutné dát prostor interním auditorům při hodnocení rizik ve spolupráci se zainteresovanými partnery (stakeholdery).

> „Odvětví kybernetické bezpečnosti selhává“

A na závěr si neodpustím další doporučení pro přemýšlení. Společnost Ernst & Young v roce 2013 vydala v edici ***Insights on governance, risk and compliance*** sice stručnou, avšak velmi hutně připravenou příručku (dostupnou na webu) s názvem **Ten key IT considerations for internal audit – Effective IT risk assessment and audit planning** (Deset klíčových uvážení o informačních technologiích pro interní audit – Efektivní hodnocení IT rizik a plánování auditu). Těch osmadvacet stránek není ani tak počtení jako spíše návod k postupnému probírání jednotlivých otázek, které před interním auditorem vyvstávají ve snaze postihnout nejen tradiční otázky bezpečnosti dat, správného nastavení přístupových práv a odolnosti informačního systému jako celku, nýbrž také nové výzvy dané přesouváním informačního obsahu na cloudová řešení, různorodost vztahů se zainteresovanými partnery nebo obtíže při nastavení priorit mezi úsporami a riziky ve složitém prostředí. Uvažování je to sice poměrně nesnadné, ale v porovnání se skeptickými vzdechy nad záludností kyberprostoru přináší střízlivou a zvládnutelnou perspektivu. ■

[Michael Borgers] © 123RF.COM

Čeho si Petr povšiml (nejen) v legislativě

Ing. Petr Kheil
metodika interního auditu, řídicího a kontrolního systému, včetně jeho vyhodnocování
Česká spořitelna, a.s.

Pokud se ohlédnu za nedávno publikovanými dokumenty pro oblast našeho zájmu, mohu za společného jmenovatele označit problematiku kybernetické bezpečnosti. K tomu jsem vybral následující materiály:

Basilejský výbor pro bankovní dohled publikoval pomůcku k počítačové odolnosti pro infrastrukturu finančního trhu **„Guidance on cyber resilience for financial market infrastructures"** *(www.bis.org/cpmi/publ/d146.htm)*. Cílem této pomůcky je upozornit na kybernetická rizika a na možnosti k posílení odolnosti proti kybernetickým útokům v organizaci. Tento dokument může současně posloužit jako příspěvek k celkovému rámci řízení rizik organizace. Přesto, že tento dokument je určen pro subjekty na finančním trhu, může se stát, podle mého názoru, inspirací pro subjekty v ostatních sektorech.

Společnost Deloitte publikovala stručný materiál k úloze interního auditu v rámci kybernetické bezpečnosti **„Cybersecurity and the role of internal audit: An urgent call to action"** *(www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html)*. Stěžejní částí materiálu je přehledný „rámec" pro hodnocení oblastí kybernetické bezpečnosti interním auditem.

V tuzemském prostředí, v knihovně připravované legislativy k projednání vládou ČR, byl publikován **návrh změny zákona o kybernetické bezpečnosti a zákona o svobodném přístupu k informacím**. Cílem předloženého návrhu je transpozice Směrnice EU 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v EU.

Z dalších informačních zdrojů by naší pozornosti neměl uniknout následující výběr:

Pro interní auditory ze sektoru veřejné správy byla na internetu IIA publikována užitečná pomůcka **„A Comparison of Authoritative Guidance Frameworks"** *(www.global.theiia.org/standards-guidance/leading-practices/Pages/The-IIA-and-INTOSAI-A-Comparison-of-Authoritative-Guidance.aspx)*. Těžištěm této pomůcky je přehledné porovnání standardů INTOSAI se standardy IIA.

Na internetu COSO byla publikována informace o připravené aktualizaci rámce COSO ERM z roku 2004. Nově má tento koncept v záhlaví dodatek **„ERM – Aligning Risk with Strategy and Performance"**, který vyjadřuje podstatu a filozofii změn. K celému záměru zřídil COSO zvláštní internetové stránky *http://erm.coso.org/Pages/default.aspx*, kde je možno získat dokumentaci a další související informace. V období od 15. 6. 2016 do 30. 9. 2016 je k předloženému návrhu organizován celosvětový průzkum.

Otázky interního auditora

Vážení čtenáři,
stále máte možnost soutěžit s Interním auditorem a odpovídat na otázky z profese interního auditu. Správné odpovědi na otázky z příslušného čísla jsou zveřejněny vždy v dalším čísle časopisu Interní auditor. Odpovědi je možné vyplnit na webu – www.interniaudit.cz, a to do **30. listopadu 2016**. Výherce bude následně vylosován na nejbližším jednání Redakční rady. Vylosovaný výherce z čísla 3/2016 obdrží jednodenní seminář v ČIIA zdarma dle vlastního výběru.

1. Co z následujícího tvrzení nejlépe popisuje účel interního auditu?
a) přidávat hodnotu společnosti
b) pomáhat managementu s implementací systému řízení rizik
c) zkoumat a hodnotit účetní systém
d) monitorovat interní kontroly pro externí auditory

2. Nejpřesvědčivější informace ohledně hodnoty aktiv získáme
a) dotazem na management
b) pozorováním procesů
c) fyzickým zkoumáním
d) externě vypracovanou dokumentací

3. Jaká je přímá odpovědnost jednotlivých uživatelů EUC?
a) nákup HW a SW
b) vedení seznamu používaných EUC
c) strategické plánování v oblasti EUC
d) fyzické zabezpečení vybavení

Správné odpovědi z čísla 2/2016...

1. Obchodování s futures s cílem snížení nebo kontrolování rizika se nazývá:
a) pojištění
b) hedging
c) krátké prodeje
d) faktoring
(správná odpověď je b)

2. Riziko, že cenné papíry nebudou moci být rychle prodány za přiměřenou cenu, se nazývá:
a) riziko defaultu
b) úrokové riziko
c) riziko nákupní síly
d) likviditní riziko
(správná odpověď je d)

3. Hlavním zaměřením tzv. „balanced scorecard" je:
a) zaměstnanci
b) struktura společnosti
c) strategie
d) systémy
(správná odpověď je c)

Výherce z minulého čísla:
Ing. Olga Mertlová, Ph.D.
Státní fond dopravní infrastruktury
GRATULUJEME

Prostor pro vaše odpovědi.

Noví členové

- Ing. Alexandra Ábelová, 1to1design s.r.o.
- Ing. Jindřich Bláha, MBA, Česká pošta, s.p.
- Andy Broughton, Wolters Kluwer ČR, a.s.
- Jakub Daněk, Deloitte Audit s.r.o.
- Ing. Věra Fousková, Zlínský kraj
- Jana Harantová, DiS., Krajské ředitelství policie Plzeňského kraje
- Igor Húževka, Slovenská pošta, a.s.
- Bc. Bronislava Johannes, DiS., Individuální členka
- Ing. Gabriela Kazimourová, Wüstenrot – stavební spořitelna a.s.
- Bc. Alena Knollová, Městský úřad Beroun
- Ing. Michal Kolařík, Česká pošta, s.p.
- Ing. Libor Kožíšek, Státní pozemkový úřad
- Ing. Ivana Kubaštová, Státní pozemkový úřad
- Ing. Petra Kunešová, Správa železniční dopravní cesty, státní organizace
- Ing. Arnošt Linzmaier, Individuální člen
- Bc. Jan Maršík, Individuální člen
- Mgr. Jan Musil, Povodí Odry, státní podnik
- Mgr. Barbora Pompe, MONETA Money Bank, a.s.
- Ing. David Radošovský, Česká pošta, s.p.
- Miloslava Samcová, Město Soběslav
- Ing. Ivica Sekerková, Slovenská pošta, s.p.
- Ing. Ivo Středa, CIA, MONETA Money Bank, a.s.
- Ing. Jana Viktorie Šeinerová, Plzeňská teplárenská, a.s.
- Ing. Lenka Šiklová, Město Chrudim
- Ing. Markéta Štrajtová, Správa železniční dopravní cesty, státní organizace
- Mgr. Stanislav Švára, Individuální člen
- Ing. Lukáš Trcala, Ministerstvo dopravy ČR
- Ing. Jiří Večeřa, Ministerstvo pro místní rozvoj ČR
- Bc. Hana Vlasáková, Česká pošta, s.p.
- Ing. Alena Wišová, Podpůrný a garanční rolnický a lesnický fond, a.s.

ČIIA na sociálních sítích

Tereza Bubníková
manažer dlouhodobého vzdělávání a certifikace ČIIA

Sociální média jsou v současné době neopominutelnou součástí nejen života jednotlivců, ale i podstatná informační platforma pro kteroukoli společnost. Proto bychom vás rádi pozvali, abyste se připojili do naší „rodiny" na sociálních sítích. Vedle využití těchto médií jako dalšího informačního kanálu se snažíme **vytvořit i prostor pro odbornou diskuzi a aktivní prostředí, jehož prostřednictvím můžete být v kontaktu s ČIIA i mezi sebou každý den**.

> „Prostor pro odbornou diskuzi"

Na sociální síti **LinkedIn** fungujeme hned dvěma způsoby. Prvním jsou **stránky společnosti Český institut interních auditorů**, kde vás pravidelně informujeme o všem podstatném, co se na ČIIA děje a nemělo by vám uniknout. *https://www.linkedin.com/company/český-institut-interních-auditorů-z-s-*
Současně se můžete na LinkedIn připojit do naší **diskuzní skupiny**. Zde vás zveme k aktivní účasti, sdílejte s námi své postřehy, názory, komentáře, ptejte se a diskutujte navzájem. Pro přihlášení do skupiny je nutné nejprve požádat o přístup do skupiny. Po schválení se již směle můžete vrhnout do diskuzí.
https://www.linkedin.com/grp/home?gid=8483240&trk=my_groups-tile-flipgrp

Rádi bychom vás také pozvali, abyste se stali našimi **odběrateli na sociální síti Twitter:** *https://twitter.com/IIACzech*. Zde vám přinášíme nejnovější aktuality a nejrychlejší postřehy, komentáře a novinky a sdílíme s vámi zajímavé příspěvky tak dynamicky, jak jen to moderní technologie umožňují.

Vaše podpora na sociálních sítích je pro nás důležitá! Vaše komentáře, „lajky" i sdílení aktivit nám poskytují jedinečnou zpětnou vazbu. Prostřednictvím sociálních sítí nám můžete dát jasně najevo, co vás zajímá, o čem byste se chtěli dozvědět víc, co je pro vás aktuální. Využijte tuto možnost podílet se na dění v ČIIA a být s námi v kontaktu každý den, a to rychle a jednoduše z pohodlí svého domova, kanceláře, nebo kdykoli skrze aplikace v chytrých telefonech. **ČIIA není jen institut, ČIIA jste vy, naši členové a přátelé**.

ČIIA Vám nabízí služby v oblasti hodnocení kvality

Tereza Bubníková
manažer dlouhodobého vzdělávání a certifikace
ČIIA

V současné době se potřeba kvalitního a nezávislého interního auditu stává ve všech sférách závažnější a závažnější. Hodnocení kvality interního auditu poskytuje internímu auditu zpětnou vazbu ohledně jeho fungování vůči vlastní organizaci, očekávání dalších stran zúčastněných ve fungování organizace i dobré praxi interního auditu.

Požadavek na toto hodnocení kvality vychází ze standardů č. 1300 a 1310, které nám říkají, že jednou z povinností vedoucího interního auditu je vypracovat a pravidelně aktualizovat **Program pro zabezpečení a zvyšování kvality interního auditu**, který musí zahrnovat jak interní, tak externí hodnocení. **A právě zde přichází ČIIA s nabídkou svých služeb v oblasti hodnocení kvality.**

Pokud program ještě vůbec nastaven nemáte, nebo ho potřebujete aktualizovat, tým expertů Českého institutu interních auditorů vám připraví a nastaví **na míru Program pro zabezpečení a zvyšování kvality** pro vámi řízený audit tak, aby umožnil hodnocení souladu činnosti interního auditu s Definicí interního auditu a se Standardy, a také hodnocení, zda se audit řídí Etickým kodexem.

Externí hodnocení vyplývá z již zmíněného standardu 1310 a specifikuje ho standard 1312: „Externí hodnocení musí být provedeno minimálně jednou za pět let odborně způsobilým a nezávislým externím hodnotitelem nebo externím hodnoticím týmem." Z interpretace potom vyplývá, že „externí hodnocení mohou být provedena **formou plně externího hodnocení nebo ve formě sebehodnocení s nezávislou externí validací**."

Pokud vám více vyhovuje možnost **Externího hodnocení kvality** interního auditu, zaměříme se na všechny klíčové oblasti fungování interního auditu. Základní osou pro nás je Mezinárodní rámec profesní praxe IA. Vedoucí interních auditů, v jejichž firmách jsme zatím hodnocení prováděli, oceňovali v referencích především profesionální přístup našeho hodnotitelského týmu (např. Ing. Ladislava Slancová, ředitelka Odboru interního auditu NKÚ, nebo Ing. Blanka Adámková, vedoucí odboru interní audit a řízení rizik České pošty) a také přínos hodnocení pro rozvoj interního auditu (např. Ing. Jindřiška Čechová, ředitelka odboru interního auditu SZIF, nebo Ing. Martin Dořičák, vedoucí odboru interního auditu Českého telekomunikačního úřadu).

Pokud je pro Vás vhodnější forma **Nezávislé validace sebehodnocení kvality** interního auditu, pak se zaměříme na vámi provedené sebehodnocení, budeme předpokládat, že jste při něm prošli všechny mezinárodní standardy pro profesní praxi interního auditu, definici interního auditu a etický kodex a vyjádřili se k tomu, jak váš útvar naplňuje jednotlivé požadavky. Náš tým expertů s bohatými zkušenostmi potom poskytne nezávislou validaci vašeho sebehodnocení.

Tým expertů ČIIA je zkrátka připraven vám pomoci jak se samotným nastavením programu kvality interního auditu, tak s oběma typy externího hodnocení.

Noví certifikovaní *(nejen)* interní auditoři

V současné době evidujeme celkem **323** certifikací:

291	CIA
11	CGAP
2	CCSA
5	CFSA
14	CRMA

V měsících období

červen–srpen 2016

nám řady certifikovaných rozšířila (CIA):

Ing. Jana Dlouhá, CIA

GRATULUJEME!

Upozornění: Kompletní certifikační program je nutné dokončit do čtyř let od podání registrace.

Certifikace interních auditorů ve veřejné správě

Počet certifikovaných auditorů ve VS dle oblastí do 31. 7. 2016

Oblasti	Počet VIAA	Počet VIAJ	Počet VIAS	Počet VIAK	Počet IA dle oblastí
Ministerstva, Úřad vlády	35	21	50	27	**133**
Krajské úřady	3	3	3	9	**18**
Úřady měst a obcí	9	15	27	12	**63**
Policie a Hasiči	7	9	10	4	**30**
Vysoké školy	1	0	7	3	**11**
Zdravotnictví, lázně	4	2	7	2	**15**
Ostatní	32	23	28	18	**101**
Celkem IA ve VS	**91**	**73**	**132**	**75**	**371**

Přehled o počtu žádostí a vydaných certifikátů

Počet žádostí od 1. 1. 2016	62
Počet vydaných certifikátů	61
Celkový počet žádostí od r. 2011	492
Celkem vydaných certifikátů od r. 2011	469

Upozornění pro certifikované

	VIAS	VIAK
Hlášení CPE do konce roku 2016 pro vydané certifikáty v roce	2013	2012, 2014

Zefektivněte své finance a ušetřete na bankovních službách

V profesním životě trávíte čas zdokonalováním procesů a zefektivňováním práce vaší společnosti. Máte ale stejný přístup i ve svém soukromém životě? Snažíte se například hledat možnosti, díky kterým zefektivníte své osobní finance, aniž byste zbytečně přepláceli? Jak ušetřit za bankovní služby od běžného účtu až po hypotéku vám poradí v UniCredit Bank.

Často cestujete a nechcete platit za každý výběr hotovosti z bankomatu? Sjednejte si bezpoplatkový běžný účet U konto od UniCredit Bank. Při splnění jednoduché podmínky aktivního využívání konta s kreditním obratem 12 000 korun měsíčně jej získáte zcela zdarma.

Stačí, když si na účet necháte posílat svou výplatu a máte bez poplatku vše od vedení účtu, přes transakce, až po výběry z jakéhokoliv bankomatu doma či kdekoliv na světě. Ty oceníte zejména, když často cestujete. Ať soukromě, nebo pracovně. S U kontem si zdarma vyberete hotovost v Londýně stejně jako v New Yorku nebo Pekingu.

ZÍSKEJTE LEPŠÍ SAZBU PŘI REFINANCOVÁNÍ HYPOTEČNÍHO ÚVĚRU

Významnou položkou osobního rozpočtu je bezpochyby bydlení. Pokud jste své bydlení pořídili na hypoteční úvěr již před několika lety, určitě jste za poslední dva roky zaregistrovali prudký pokles jejich úrokových sazeb. Lepší sazbu a nižší splátky můžete získat i vy, stačí pečlivě ohlídat termín refixace vaší hypotéky.

Během refixace si můžete v bance vyjednat výhodnější podmínky a snížit si úrokovou sazbu až o několik procentních bodů proti situaci před několika lety. V UniCredit Bank vám dnes nabídneme sazbu od 1,49 % p.a., kterou si můžete zafixovat na tři nebo pět let dopředu. Rozdíl ve splátce rozhodně pocítíte. Na stejně výhodné podmínky ale dosáhnou i klienti, kteří teprve řeší svůj první úvěr na byt nebo dům.

Pokud se vám nová nabídka vaší současné banky nebude líbit, přejděte s celou hypotékou za lepšími podmínkami jinam. Přejít s hypotečním úvěrem do jiné banky je dnes stejně jednoduché jako změnit poskytovatele běžného účtu, složitá administrativa je dávno minulostí.

V UniCredit Bank dokonce můžete od loňského roku refinancovat hypotéku po internetu. Stačí zaslat všechny podklady ke svému stávajícímu úvěru nafocené telefonem, klidně večer po práci z klidu domova, a banka vše vyřídí za vás. Na pobočku zajdete jen k podpisu smlouvy. Celý proces nezabere víc než pět pracovních dnů.

PODNIKÁTE V AUDITU? VYUŽIJTE VÝHODNÉ PODNIKATELSKÉ ÚČTY

Pokud podnikáte a máte vlastní auditorskou praxi, můžete v UniCredit Bank také získat konto, se kterým ušetříte na poplatcích. Pro auditory nabízí banka speciální Konto PROFESE Plus. Samozřejmostí je prestižní zlatá platební karta, nadstandardní úroková sazba na běžném účtu a při splnění podmínek aktivního využívání účtu i vedení konta zdarma stejně jako u běžného U konta. Ušetřit můžete i díky široké nabídce financování podnikatelů – od kontokorentu až po bankovní záruky.

Jako auditor se pro vaši firmu nespokojíte s prvním řešením. Hledáte to nejefektivnější a snažíte se procesy neustále zlepšovat. Stejně tak se nespokojte s tím, co dnes využíváte pro své osobní finance.

Dobré bankovní služby nejsou samozřejmost. Vezměte je do vlastních rukou a chtějte od své banky víc. Přijďte si s námi promluvit o tom, jak ušetřit na běžném účtu, úvěrech i jak investovat na nejbližší pobočku UniCredit Bank.

Více informací o službách UniCredit Bank *www.unicreditbank.cz*

English Annotation

Adam Kučínský

– Cybersecurity Act and the NIS Directive

This article is the first one from the series of articles about cybersecurity from the sponsor point of view. It deals mainly with the legal structure.

Daniel Kardoš

– Collection of data gather from security audits of the electronic documentation

The article deals with the audit data creation in the framework of the cybersecurity act. In an comprehensive manner it summarizes the possibilities of the access conrol and audit trail creation and the liabilities of the administrators.

Jan Andraščík

– Security of the use of personal mobile devices

The author deals in his article with the security of the use of personal mobile devices. He explains the trends in this area, describes the risks connected with the use of the mobile devies. One chapter is devoted to the protection of the mobile devices in the company environment. Shortly it mentions security audits of the mobile devices.

Jiří Slabý

– Changes in the approach of the perpetrators for the last five years and further development (1st part)

The article introduces interesting world and national security events.

Milan Rybák

– Training of the auditors in the CHMU

The cybersecurity act, quick IT development and the security of human resources and data are to be discussed regularly at the internal auditors' training.

Lucie Veselá, Stanislav Klika

– Cybersecurity audit in the public sector

The aim of the article is to introduce possible approaches to the IT security governanci in the public sector and coordination with other internal audit tasks.

Petr Hadrava

– Interview with IIA 2015–2016 Chairman of the Board Lawrence J. Harrington, CIA, QIAL, CRMA

The interview is focused on the theme of the 2015–16 IIA Chairman of the Board being "Invest in Yourself". Such investment is critical to remain relevant and value adding for the company.

Antonín Šenfeld

– What is new in the IPPF?

The author informs about new Implementation Guides issued by the IIA and introduces their interesting content.

Tomáš Pivoňka

– A week in the New York

Information about the IIA activities in relation to the celebration of the 75th anniversary of the IIA.

Václav Peřich

– Ignes Fatui, Knockers and von Däniken

The author deals in his article with the threats and risks which are connected with the current wolrd in the form of the new technologies, and with the importance of their management and security. In this connection it shows the necessity of strong internal audit with correct position.

Tereza Bubníková

– IIA in the social networks

Information about the CIIA activities in the social networks LinkedIn and Twitter.

www.erstecorporatebanking.cz

„ČÍM JEDNODUŠŠÍ SMLOUVA, TÍM PEVNĚJŠÍ OBCHODNÍ VZTAH.“

Ing. Ladislav Denk
Jednatel
VÁHALA a spol. s r.o.

1933
VÁHALA

ERSTE
Corporate Banking

V zahraničí jsem se naučil, jakou váhu má důvěra a dané slovo. Nejlepší smlouva, jakou jsem kdy uzavřel, neměla 50 stran, ale je napsána ručně na kusu papíru. Obchodujeme na ni již více než 10 let. Vybíráme si proto partnery, pro které je také podání ruky ta nejpevnější smlouva.

Pro podnikání založené na důvěře kontaktujte **Erste Corporate Banking**.