AUDITOR KYBERNETICKÉ BEZPEČNOSTI

Školící materiál – vybrané části

Pro více informací nás neváhejte kontaktovat.

Platná legislativa

- Zákon nepředstavuje nic jiného, než srozumitelný manuál proaktivní bezpečnosti. Největší změny jsou v přístupu k ochraně aktiv. Bezpečnost je nutné vnímat jako součást komplexního systému řízení organizace.
- Splnění legislativních požadavků nemusí nutně znamenat investice do nových bezpečnostních produktů a technologií.
- Zákon vyžaduje **implementaci a pravidelné audity systému ISMS** (Information Security Management System), tedy řízení informační bezpečnosti.
- **Klíčovým pilířem je správné nastavení bezpečnostní politiky a následně její uplatňování napříč organizací.**

Platná legislativa

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

- Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti
  - **§6, písmeno c** vymezuje povinnost dotčené organizace k ustanovení role Auditora kybernetické bezpečnosti
  - ***Auditor kybernetické bezpečnosti*** *je osoba provádějící audit kybernetické bezpečnosti, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let. Auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu rolí uvedených v odstavci 2 písm. a), b) nebo d).*

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

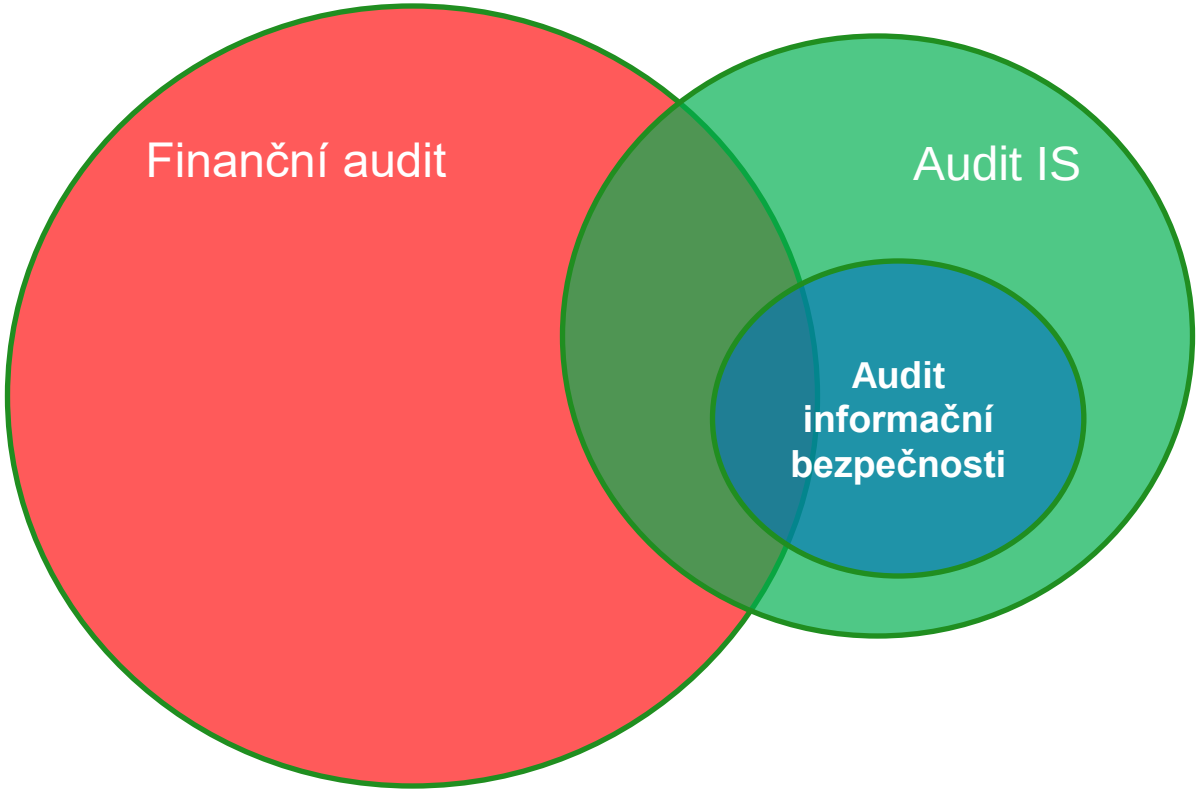
- Změna nař. o kritériích pro určení prvku kritické infrastruktury

Typy auditu kybernetické bezpečnosti

- Metodika BSI se zabývá dvěma typy – **Průřezovým auditem a částečným auditem IS**.
- Cyklus průřezového auditu je doporučen na 3 roky.

- **Co je Audit informační/kybernetické bezpečnosti** - specifický druh auditu informačního systému, který se zaměřuje na bezpečnost:
  - **bezpečnost:** důvěrnost, integrita, dostupnost
  - **kvalita:** efektivita, účinnost
  - **důvěryhodnost:** spolehlivost, soulad s legislativou
- Audit je nedílnou součástí systémové bezpečnostní politiky, zahrnující:
  - plán obnovy a havarijní plán,
  - implementace bezpečnostního systému,
  - monitoring (průběžné sledování účinnosti bezpečnostního systému)
  - řešení bezpečnostních incidentů,
  - …audit (následné sledování účinnosti bezpečnostního systému)
- Audit **hodnotí úroveň bezpečnosti neinvazivním způsobem**, pasivní sběr informací o konfiguraci a nastavení zařízení a následné vyhodnocení těchto informací a vyvození závěrů
- Měl být vždy **prováděn za asistence odborníků** – informatiků v auditované společnosti (nejlépe administrátorů)

Vztahy mezi různými druhy auditů



Typy auditu – různě cílené

- **Audity první stranou** (spíše známé jako **interní** audity) „sebe ověření“

- **Audity druhou stranou** jsou prováděny externími subjekty, které mají vůči dané organizaci nějaké zájmy

  Např. odběratel může na základě dohody provádět či objednat audit svých dodavatelů (na základě dohody)

- **Audity třetí stranou** jsou prováděny externí organizací, která je zcela nezávislá na auditované organizaci. Výsledky auditů třetí stranou jsou využívány pro udělování certifikací souladu s danou normou (např. soulad řízení bezpečnosti informací s normou ISO/IEC 27001) tzv. certifikační audity nebo slouží jako nezávislé vyjádření pro různé regulační orgány (např. v rámci dohledu nad finančními institucemi apod.).

Typy auditů – průřezový audit

- Průřezový audit má holistický přístup a širokou škálu testů a zkoušek.
- V průřezovém auditu se testují na základě namátkové kontroly nebo vybraných vzorcích všechny vrstvy IS.
- Objektem testování v průřezovém auditu je vždy celá organizace.
- Cílem průřezového audit je získat komplexní představu o stavu informační bezpečnosti organizace.

Typy auditů – částečný audit

- Částečný audit IS je omezen na určitý úsek organizace a je zahájen, když je to nutné, manažerským týmem IS.
- Testy provedené částečným auditem jsou mnohem hlubší, než v případě průřezového auditu IS.
- Částečný audit IS se spouští v případě specifické potřeby, například po rozsáhlé restrukturalizaci organizace, při výskytu bezpečnostního incidentu, nebo v případě zavádění nových obchodních procesů a nových technologií.
- Částečný audit IS je vhodný zejména pro audit kritických podnikových procesů.
- Skutečnost, že částečný audit je omezen na určité obchodní procesy nebo informační postupy, umožňuje provést náročnější testy.
- V závislosti na rozsahu zkoušek definované oblasti, může mít smysl zkoumat vybrané vzorky nebo zcela přezkoumat všechna platná bezpečnostní opatření.

Obecný audit informační bezpečnosti

- **Rozdíl od certifikačního auditu:** hlavním kritériem hodnocení není konkrétní ISO norma, ale bezpečnostní politika dané organizace

- **Důležité primární hledisko dekompozice auditu:**
  - **Hledisko prvků bezpečnosti**: důvěrnost, dostupnost, integrita, prokazatelnost, pravost, spolehlivost
  - **Hledisko komponent informatiky**: hardware, software, infrastruktura, data, dokumentace,
  - **Hledisko procesů a služeb informatiky** (respektují současně kontrolní cíle a životní cyklus služeb: plánování, návrh a pořízení, implementace a testování, provozování a údržba, monitorování a zlepšování; např. podle ITIL nebo COBIT).

Druhy obecných auditů

- Personální audit
- Provozní audit
- Technologický audit

Průběh auditu

- Specifické životní cykly auditu
  - Certifikační audit informační bezpečnosti
  - Obecný audit informační bezpečnosti

Průběh:

- Plánovat a připravit audit
- Etapy auditů: plánování, realizace
- Vyhodnotit a porovnat získané výstupy
- Vypracovat auditní zprávu a realizovat nápravná opatření

Auditní techniky

- Verbální (pohovory)
- Vizuální kontrola systémů, umístění, prostor a objektů
- Pozorování (pozorování skutečností a zařízení mimochodem v rámci kontroly na místě)
- Analýza souborů (včetně elektronických dat)
- Technické testy (např. testování poplašných systémů, přístupových systémů, aplikací)
- Analýza dat (například soubory protokolu, hodnocení databáze, atd.)
- Otázky psané (dotazníky)

Auditní techniky

- Sledování po směru
  - audit sledující tok procesu, služby
- Sledování proti směru
  - audit zpětně vyhledává záznamy o realizované činnosti

- Tvorba záznamu zjištění:
  - hledání objektivního důkazu, že systém funguje, jak je předepsáno, podle požadavku
  - odebrané vzorky jsou požadovaným důkazem

Auditní techniky

Klasifikace neshod je obsahem Bezpečnostní politiky organizace

Zjištěné skutečnosti	*Klasifikace zjištění IA*
Selhání v dodržování kritických postupů – vliv na výsledek činnosti nebo na funkce SM	**Systémová neshoda**
Menší nedostatky SM, které bezprostředně neohrožují jeho funkci, selhání jednotlivce	**Nesystémová neshoda**
Izolované nebo nahodilé malé nedostatky, nejlepší praxe	**Doporučení**
Kritéria jsou plněna, postupy dodržovány	**Bez neshody**

Auditní týmy

- Auditní tým IS je nezávislý a objektivní.
- Tým poskytuje organizaci s podporou dosáhnout svých cílů na základě vyhodnocení přes metodický a cílený přístup a poskytuje podporu pro zlepšení.
- Základním požadavkem pro jakýkoli audit, a tedy i pro audit IS, je neomezené právo získat a zobrazit informace.
- To může zahrnovat i právo prohlížet citlivé či utajované informace týkající se řízení informační bezpečnosti.
- Nedílným předpokladem jsou morální a odborné kvality všech členů auditního týmu.

Auditní týmy

- **Auditor** – osoba s odbornou způsobilostí provádět audit – je nezávislá na prověřované činnosti
- **Tým auditorů** – jeden nebo více auditorů, kteří provádějí audit, podporovaný technickými experty, jsou-li potřební
- Jeden z auditorů týmu auditorů je ustanoven **vedoucím auditorského týmu**. Tým auditorů může zahrnovat i auditory ve výcviku
- **Technický expert** – osoba, která poskytuje specifické znalosti a odborné posudky k předmětu auditu
- **Pozorovatel** – člen týmu, nezasahuje do auditu

Obsah auditorské zprávy

Základní údaje:

- Cíle auditu
- Rozsah auditu, zvláště identifikaci auditovaných organizačních a funkčních jednotek nebo procesů a časový úsek, ve kterém audit proběhl
- Identifikace klienta
- Identifikaci vedoucího auditora a jeho týmu
- Data a místa, ve kterých proběhla šetření v místě zákazníka
- Kritéria auditu
- Nálezy auditu
- Závěry auditu

Obsah auditorské zprávy

Doplňkové údaje:

- Plán auditu
- Seznam lidí, kteří spolupracovali na straně zákazníka s auditory
- Přehled realizovaných akcí/procesů auditu a případné okolnosti, které vedly ke snížení spolehlivosti závěrů auditu.
  - Neshoda – nesplnění požadavku (klasifikace)
  - Záznam o neshodě – formulář IA, kde jsou vedeny údaje o zjištěných neshodách
  - Check list (dotazník) – pomocný dokument při auditu pro záznam zjištění provedených na místě
- Potvrzení o tom, že bylo dosaženo definovaných cílů auditu.
- Přehled oblastí, které byly zahrnuty v plánu a nebyly auditovány
- Popis nevyřešených rozdílných názorů mezi auditorským týmem a auditovanou stranou.
- Přehled doporučení ke zlepšení, pokud byly součástí cílů auditu.
- Odsouhlasený plán realizace nápravných doporučení (pokud existuje).
- Prohlášení o zachování mlčenlivost o získaných údajích (u externího auditora).
- Seznam příjemců auditorské zprávy a způsob jejího doručení.

Odborná a morální způsobilost auditorů, nezávislost

Auditor by měl být:

- morální - spravedlivý, pravdomluvný, čestný a diskrétní;
- nezaujatý - schopný přijímat alternativní myšlenky nebo jiné úhly pohledu;
- diplomatický - taktní při jednání s lidmi;
- pozorný - aktivně sleduje okolní prostředí a činnosti;
- vnímavý - je schopný vnímat a pochopit různé situace;
- všestranný - přizpůsobivý ke způsobu posuzování různých typů systémů;
- vytrvalý - vytrvalost v překonávání zábran, zaměřen na dosažení cíle;
- rozhodný - dosahuje závěrů na základě logických úvah a analýz;
- samostatný - pracuje nezávisle přičemž spolupracuje s ostatními.

Odborná a morální způsobilost auditorů, nezávislost

Auditor by měl:

- znát podrobně požadavky normy (norem), podle které je vybudován systém řízení ve společnosti
- znát předpisy platné ve společnosti a požadavky specifikované na produkty firmy
- být schopen správně aplikovat požadavky normy a dalších předpisů
- mít odpovídající schopnosti pro jednání s lidmi na všech úrovních
- mít odpovídající zkušenosti v činnostech a na pracovištích, která bude prověřovat (je velmi důležité při volbě auditora zohlednit i znalost příslušného prověřovaného oddělení)
- umět vhodně klást otázky, které umožní získat dostatek důkazů z prověřované činnosti
- být schopen identifikovat a jasně definovat neshodu, umět přednést zjištěné neshody přesvědčivým způsobem
- měl by si průběžně zvyšovat kvalifikaci pomocí školení a průběžného sběru zkušeností
- měl by být schopen akceptovat filozofii systémů řízení a principy zabezpečování kvality

Komunikace s gestorem

- Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení **Národního bezpečnostního úřadu gestorem problematiky** kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Přílohou usnesení je Statut Rady pro kybernetickou bezpečnost. Na základě přijatého usnesení vzniklo **Národní centrum kybernetické bezpečnosti** (NCKB), jako součást Národního bezpečnostního úřadu, se sídlem v Brně.
  - Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům.

- Více na http://www.nbu.cz/cs/e-komunikace/