ISO/IEC 27001:2022

07.06.2024

Antonín Šefčík

Obsah prezentace

1. Obsah ISO/IEC 27001:2022
2. Změny v procesech ISMS
3. Příloha A normy ISO/IEC 27001:2022
4. Vzor opatření z normy ISO/IEC 27002:2022
5. Nová opatření
6. Co dál

Obsah ISO/IEC 27001:2022

- Důraz na procesní přístup
- Harmonizovaná struktura (HS)
- Důraz na plánování změn v ISMS

Nová ISO/IEC 27001:2022

Rozsah normy rozšířen již v názvu - „Bezpečnost informací, **kybernetická bezpečnost a ochrana soukrom**í - Systémy řízení bezpečnosti informací - Požadavky “

- Norma byla vydána v říjnu 2022, jako ČSN vyšla v říjnu 2023
- Běží období k přechodu na novou normu do října 2024
- V kapitolách 1 – 10 došlo k minimálním změnám
- Hlavní změny se odehrály v příloze A, kde došlo k přeskupení bezpečnostních opatření do 4 oblastí/kategorií namísto původních 14 oblastí

Kapitoly 1 až 6 normy ISO/IEC 27001:2022

Doplnění těchto částí normy:

1. „4.3 Stanovení rozsahu systému řízení bezpečnosti informací“ byl doplněn bod „b) **který z těchto požadavků bude řešen prostřednictvím příslušného systému řízení bezpečnosti informací**“

2. „4.4 doplněn požadavek na **identifikaci nezbytných procesů a jejich interakcí v rámci ISMS**, které jsou nutné pro jeho zavedení a udržování

3. „6.2 Cíle bezpečnosti informací a plánování jejich dosažení“ byl doplněny body „d) že **(cíle) budou sledovány**“ a „g) že **(cíle) musí být k dispozici jako zdokumentované informace**“

4. Na závěr kapitoly „6 Plánování“ byl doplněn bod „6.3 Plánování změn - **Když organizace určí potřebu změn v systému řízení bezpečnosti informací, musí být změny provedeny plánovaným způsobem**.“

Kapitoly 7 až 10 normy ISO/IEC 27001:2022

Doplnění těchto částí normy:

4. „9.1 Monitorování, měření, analýza a hodnocení“ byl so bodu b) ke stávajícímu textu že organizace musí určit použitelné metody monitorování, měření, analýzy a hodnocení k zajištění platných výsledků doplněn text, že „**Zvolené metody by měly poskytovat srovnatelné a reprodukovatelné výsledky, aby byly považovány za platné**.“

5. „9.2 Interní audit“ a „9.3. Přezkoumání vedením organizace“ byla **rozčleněna na části „obecné“ a „Program interního auditu“ a „Vstupy a výsledky přezkoumání“.**

6. U nového bodu „9.2.2 Program interního auditu“ byl lehce upraven text na „**Při vytváření programu (programů) interního auditu musí organizace zvážit důležitost příslušných procesů a výsledky předchozích auditů**.“

7. U nového bodu 9.3.2 Vstupy přezkoumání“ byl nově přidán bod „**c) změny potřeb a očekávání zainteresovaných stran, které jsou relevantní pro systém řízení bezpečnosti informací**“.

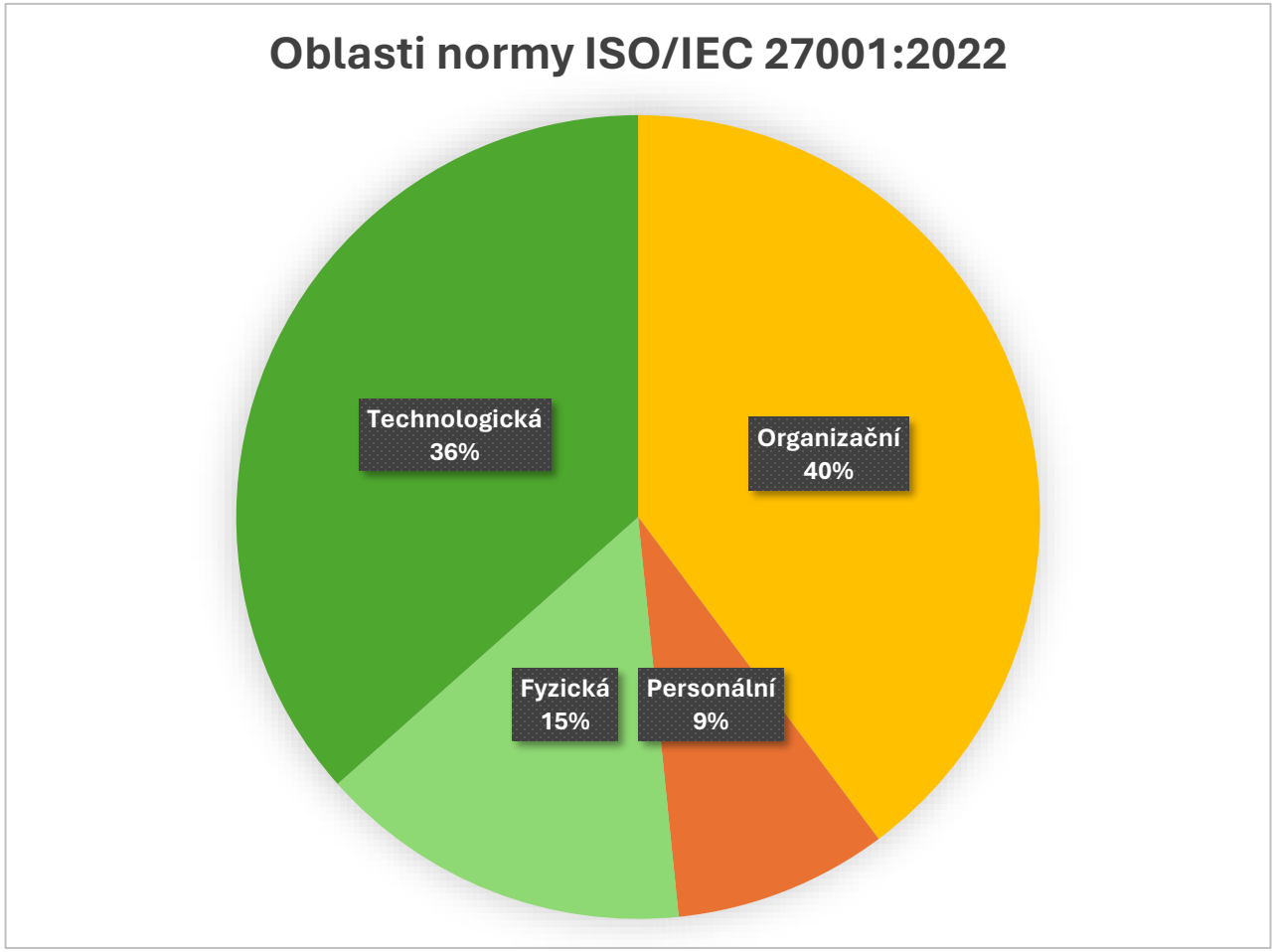
Příloha A nové normy ISO/IEC 27001:2022

Nová verze normy obsahuje celkem **93 opatření** rozdělených do celkem **4 oblastí**:

- 5. Organizační opatření - 37
- 6. Personální opatření - 8
- 7. Fyzická opatření - 14
- 8. Technologická opatření – 34

V nové normě bylo:

- přidáno 11 nových opatření
- 23 opatření přejmenováno, aby byla srozumitelnější
- zmenšen počet opatření (ze 114 na 93), žádná však nebyla vyloučena, jen se sloučila
- 57 opatření sloučeno do 24 opatření



Další změny v příloze A ISO/IEC 27001:2022

- Příloha A odkazuje na opatření z normy ISO/IEC 27002:2022, tentokrát bez přidaného „A“
- Byla upravena struktura opatření, kde se uvádí přímo název opatření a a vlastní obsah opatření a pro skupinu opatření již nepoužívá termín „cíl“

Table A.1 — Information security controls

5	**Organizational controls**	
5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined and allocated according to the organization needs.
5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.

Vzor opatření z ISO/IEC 27002:2022

Struktura popisu byla nově upravena:

- Název opatření
- Nové jsou atributy **s tagy**
- Definice opatření
- Účel
- Pokyny
- Další informace

5.5 Contact with authorities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience

Control

The organization should establish and maintain contact with relevant authorities.

Purpose

To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

Guidance

The organization should specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.

Contacts with authorities should also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g. applicable information security regulations).

Other information

Organizations under attack can request authorities to take action against the attack source.

Nová opatření ISO/IEC 27001:2022

1. **5.07 Správa hrozeb** - Informace související s hrozbami informační bezpečnosti by měly být shromažďovány a měly by se analyzovat, aby se vytvořila správa hrozeb
2. **5.23 Informační bezpečnost při používání cloudových služ**eb - Procesy získávání, používání, správy a ukončení cloudových služeb by měly být vytvořeny v souladu s požadavky organizace na bezpečnost informací
3. **5.30 Připravenost ICT zajištění kontinuity provozu** - Připravenost ICT by měla být plánovaná, implementována, udržována a testována na základě cílů kontinuity podnikání a požadavků na kontinuitu ICT
4. **7.04 Monitorování fyzické bezpečnosti** - Prostory by měly být nepřetržitě monitorovány, aby se předešlo neautorizovanému fyzického přístupu.)
5. **8.09 Řízení konfigurace** - Konfigurace, včetně bezpečnostních konfigurací, hardwaru, softwaru, služeb a sítí, by měly být vytvořeny, zdokumentované, implementovány, monitorovány a přezkoumávány
6. **8.10 Vymazání informace** - Informace uložené v informačních systémech a zařízeních by měly být vymazány, pokud již nejsou potřebné
7. **8.11 Maskování dat** - Maskování údajů by mělo být používáno v souladu s politikou organizace zaměřenou na řízení přístupu a obchodními požadavky, se zohledněním legislativních požadavků
8. **8.12 Prevence úniku dat** - Na systémy, sítě a koncová zařízení, které zpracovávají, uchovávají nebo přenášejí citlivé informace, by se měla aplikovat opatření k předcházení úniku dat
9. **8.16 Monitorovací činnosti** - V sítích, systémech a aplikacích by se mělo monitorovat neobvyklé chování a měla by být přijata vhodná opatření k vyhodnocení potenciálních incidentů informační bezpečnosti
10. **8.23 Filtrování webových stránek** - Přístup k externím webovým stránkám by měl být řízen, aby se snížilo vystavení škodlivému obsahu
11. **8.28 Bezpečné programování** - Na vývoj softwaru by se měly vztahovat zásady bezpečného kódování

5.7 Správa hrozeb

Opatření: Informace související s hrozbami informační bezpečnosti by měly být shromažďovány a měly by se analyzovat, aby se vytvořila správa hrozeb

Účel: Zajistit informovanost o prostředí hrozeb v organizaci, aby bylo možné přijmout vhodná opatření ke zmírnění dopadů

Pokyny:

Informace o stávajících nebo vznikajících hrozbách se shromažďují a analyzují **za účelem zavedení opatření a snížení dopadu těchto hrozeb**

Informace o hrozbách musí **zohlednit následující**:

a) Strategické zpravodajství: **výměna informací o měnícím se prostředí hrozeb** (např. typy útočníků nebo typy útoků)

b) **taktické zpravodajství o hrozbách**: informace o metodikách, nástrojích a technologiích útočníků

c) **operativní zpravodajství o hrozbách**: podrobnosti o konkrétních útocích, včetně technických ukazatelů

Informace o hrozbách **by měly být**:

a) **relevantní** (tj. související s ochranou organizace)

b) **zasvěcené** (tj. poskytující organizaci přesné a podrobné porozumění prostředí hrozeb)

c) **kontextuální, aby poskytovala situační povědomí** (tj. přidávala k informacím kontext na základě času, místa výskytu, zkušeností a výskytu v podobných organizacích);

d) **akční** (tj. může se na základě informací rychle a efektivně jednat)

Činnosti v oblasti **zpravodajství o hrozbách by měly zahrnovat:**

a) **stanovení cílů** pro tvorbu informací o hrozbách

b) **identifikaci, prověření a výběr interních a externích informačních zdrojů**, které jsou nezbytné a vhodné k poskytnutí informací potřebných pro tvorbu zpravodajství o hrozbách

c) shromažďování informací z vybraných zdrojů, které mohou být interní i externí

d) zpracování shromážděných informací za účelem jejich **přípravy pro analýzu** (např. překladem, formátováním, potvrzením informací);

e) analýza informací - jak souvisejí s organizací a jaký mají pro ni význam;

f) **jejich sdělování a sdílení relevantním osobám** ve srozumitelném formátu

Informace o hrozbách **by měly být analyzovány** a později využity:

a) k zavedením procesů pro začlenění informací získaných z informací o hrozbách do **procesů řízení rizik BI organizace**

b) jako **dodatečný vstup pro zavedení opatření**, jako jsou firewally, systém detekce narušení nebo řešení proti malwaru;

c) jako **vstup k testování** bezpečnosti informací

5.23 Informační bezpečnost při využívání cloudových služeb

Opatření: Procesy pro získávání, používání, správu a ukončení cloudových služeb by měly být stanoveny v souladu s požadavky organizace na bezpečnost informací

Účel: Specifikovat a řídit bezpečnost informací pro využívání cloudových služeb

Pokyny:

Stanovení a sdělení politiky cloudových služeb.

Definice a sdělení způsobu řízení rizik BI spojených s využíváním cloudových služeb.

Určit sdílenou odpovědnost zas cloudové služby mezi poskytovatelem a organizací.

Organizace by měla definovat:

a) požadavky na BI související s využíváním cloudových služeb
b) kritéria pro výběr cloudových služeb (včetně rozsahu)
c) role a odpovědnosti při využívání a správě cloudových služeb
d) rozdělení opatření BI mezi poskytovatelem cloudu a organizací
e) možnosti zabezpečení informací poskytované poskytovatelem cloudu
f) ujištění o opatřeních BI zavedených poskytovateli cloudových služeb
g) opatření, rozhraní a změny služeb, při využití více cloudových služeb
h) postupy řešení incidentů BI při využívání cloudových služeb
i) způsob monitorování, přezkoumávání a vyhodnocování průběžného využívání cloudových služeb (řízení rizik BI)

› způsoby změny nebo ukončení cloudových služeb

Provedení posouzení rizik ke zjištění rizik cloudových služeb.

Dohoda mezi poskytovatelem cloudové služby a organizací, by měla obsahovat následující ustanovení o ochraně dat a dostupnosti služeb:

a) poskytování řešení založených na průmyslově uznávaných standardech pro architekturu a infrastrukturu
b) řízení kontroly přístupu ke cloudu tak, aby splňovala požadavky organizace
c) zavedení řešení pro monitorování a ochranu před škodlivým softwarem
d) zpracování a ukládání citlivých informací organizace na schválených místech (např. v určité zemi nebo regionu)
e) poskytování specializované podpory v případě incidentu BI v cloudu
f) zajištění splnění požadavků organizace na BI v případě dalšího zadání cloudových služeb externímu dodavateli (případně zákaz jeho zadání)
g) podpora organizace při shromažďování digitálních důkazů s ohledem na zákony a předpisy pro digitální důkazy
h) podpora a dostupnost služeb po dobu opuštění cloudové služby
i) zajištění zálohování dat a informací o konfiguraci a bezpečná správa záloh
j) poskytování a vracení informací (konfigurační soubory, zdrojový kód a data)

Zvážení předběžného oznámení před provedením jakýchkoli podstatných změn majících dopad na zákazníka.

Zajištění a udržování kontaktů s poskytovatelem cloudu.

5.30 Připravenost ICT na zajištění kontinuity provozu

Opatření: Připravenost ICT by měla být plánována, implementována, udržována a testována na základě cílů kontinuity provozu a požadavků na kontinuitu ICT

Účel: Zajistit dostupnost informací organizace a dalších souvisejících aktiv během přerušení provozu

Pokyny:

Požadavky na kontinuitu ICT jsou výsledkem **analýzy dopadů na podnikání (BIA)**. Proces BIA by měl využívat typy dopadů a kritéria k posouzení dopadů v čase, které vyplývají z narušení obchodních činností, jež poskytují produkty a služby. Velikost a trvání výsledného dopadu by měly být použity k určení prioritních činností, kterým by měl být přiřazen **RTO.** BIA určí zdroje potřebné k podpoře prioritních činností. Pro tyto zdroje by měl být rovněž stanoven RTO. Podskupina těchto zdrojů by měla zahrnovat služby ICT.

BIA zahrnující služby ICT lze rozšířit o definování požadavků na výkon a kapacitu systémů ICT a **RPO**.

Na základě výstupů z BIA a posouzení rizik by organizace měla určit a vybrat strategie kontinuity ICT, které zohlední možnosti před narušením, během něj a po něm. Na základě strategií by měly být vypracovány, implementovány a testovány plány, které zajistí požadovanou úroveň dostupnosti služeb ICT.

Organizace by měla zajistit, aby:

a) byla vytvořena **odpovídající organizační struktura** pro přípravu na narušení, jeho zmírnění a reakci na něj, **podporovaná pracovníky** s potřebnou odpovědností, pravomocemi a kompetencemi

b) byly vypracovány **plány kontinuity ICT**, včetně postupů reakce a obnovy, které podrobně popisují, jak organizace plánuje zvládnout narušení služeb ICT:

   1) pravidelně vyhodnocovány prostřednictvím **cvičení a testů**

   2) **schváleny vedením**

c**) plány kontinuity ICT** obsahují následující informace o kontinuitě ICT:

   1) **specifikace výkonnosti a kapacity pro splnění požadavků a cílů kontinuity provozu**, jak je uvedeno v BIA;

   2) **RTO** každé prioritní služby ICT a postupy pro obnovení těchto složek;

   3) **RPO** prioritizovaných zdrojů ICT definovaných jako informace a postupy pro obnovení těchto informací.

RTO, **cílový čas/doba zotavení¨-** je plánovaná doba trvání a úrovně služeb, za/na kterou musí být obchodní proces po katastrofě nebo narušení obnoven…

RPO, cílový bod obnovení/zotavení - jedná se o nejdelší plánované období, během kterého mohla být data (transakce) ztracena z IT v důsledku incidentu.

7.4 Monitorování fyzické bezpečnosti

Fyzické prostory by měly být monitorovány dohledovými systémy, které mohou zahrnovat **strážce, poplašné systémy proti vniknutí nebo monitorovací video systémy**, ty mohou být spravovány buď interně, nebo poskytovatelem monitorovacích služeb

Přístup do budov, v nichž jsou umístěny kritické systémy, by měl být **nepřetržitě monitorován**, aby se odhalil neoprávněný přístup nebo podezřelé chování, a to prostřednictvím:

a) instalací **monitorovacích kamerových systémů**

b) instalací, v souladu s příslušnými platnými normami, a pravidelným testováním **kontaktních, zvukových nebo pohybových detektorů** pro spuštění poplachu proti vniknutí, jako např:

   1. **instalace kontaktních detektorů**, které spustí poplach při navázání nebo přerušení kontaktu
   2. **detektory pohybu založené na infračervené technologii**
   3. **instalace senzorů citlivých na zvuk rozbíjeného skla**

c) použití těchto alarmů k **pokrytí všech vnějších dveří a přístupných oken**. Neobydlené prostory by měly být vždy zabezpečeny alarmem; krytí by mělo být zajištěno i pro další prostory (např. počítačové nebo komunikační místnosti)

Systém by měl být pravidelně testován, aby se zajistilo, že funguje, jak má, zejména pokud jsou jeho součásti napájeny z baterií

Jakýkoli monitorovací a záznamový mechanismus by měl být použit s **ohledem na místní zákony a předpisy, včetně právních předpisů o ochraně osobních údajů**, zejména pokud jde o monitorování osob a **doby uchovávání zaznamenaných videozáznamů**

8.9 Řízení konfigurace

Opatření: Konfigurace, včetně bezpečnostních konfigurací hardwaru, softwaru, služeb a sítí, by měly být stanoveny, zdokumentovány, implementovány, monitorovány a přezkoumávány

Účel: Zajistit, aby hardware, software, služby a sítě fungovaly správně s požadovanými bezpečnostními nastaveními a aby konfigurace nebyla změněna neoprávněnými nebo nesprávnými změnami

Pokyny:

Organizace definuje a **zavede procesy a nástroje k prosazování definovaných konfigurací** (včetně bezpečnostních konfigurací) pro HW, SW, služby (např. cloudové služby) a sítě. Zavede i **role, odpovědnosti a postupy** pro zajištění změn konfigurace.

Definice **standardních šablon pro bezpečnou konfiguraci HW, SW, služeb a sítí**:

a) s využitím **veřejně dostupných pokynů** dle **potřebné úrovni ochrany**
b) s podporou BPI, dalších politik, norem a dalších bezpečnostních požadavků
c) zvážení **možností proveditelnosti a použitelnosti** konfigurací

Šablony by měly být pravidelně **revidovány a aktualizovány v závislosti na nových hrozbách nebo zranitelnostech** a **změn v HW a SW**.

Při vytváření standardních šablon je potřebné přihlédnout k:

a) **minimalizace** počtu **privilegovaných uživatelů**
b) **zakázání** nepotřebných, nepoužívaných nebo **nezabezpečených identit**
c) zakázání nebo omezení **nepotřebných funkcí a služeb**
d) synchronizace hodin
e) změna výchozích ověřovacích informací dodavatele (**výchozí hesla**)
f) **časový limit**, který automaticky odhlásí PC při nečinnosti
g) **ověřování splnění licenčních požadavků**

Správa konfigurací - zavedené konfigurace HW, SW, služeb a sítí by měly být zaznamenány a o všech změnách konfigurace by měl být veden protokol. Tyto záznamy by měly být bezpečně uloženy (konfigurační databáze nebo konfigurační šablony).

Změny konfigurací by se měly řídit **procesem řízení změn**.

Záznamy o konfiguraci mohou podle potřeby obsahovat:

a) **aktuální informace o vlastníkovi nebo kontaktním místě** pro aktivum
b) **datum poslední změny** konfigurace
c) **verzi šablony** konfigurace
d) **vztah ke konfiguracím** jiných aktiv

Sledování konfigurací - konfigurace by měly **být monitorovány pomocí komplexní sady nástrojů pro správu systému** (např. nástroje pro údržbu, vzdálenou podporu, nástroje pro správu podniku, software pro zálohování a obnovu) a měly by být **pravidelně kontrolovány za účelem ověření nastavení konfigurace, vyhodnocení síly hesla a posouzení prováděných činností**.

Konfigurace **lze porovnávat s definovanými cílovými šablonami**. Odchylky by měly být řešeny buď **automatickým vynucením definované cílové konfigurace**, nebo **manuální analýzou odchylky s následnými nápravnými opatřeními**.

8.10 Vymazání informací

Opatření: Informace uložené v informačních systémech, zařízeních nebo na jiných paměťových médiích by měly být vymazány, pokud již nejsou potřebné

Účel: Zabránit zbytečnému odhalování citlivých informací a dodržovat právní, zákonné, regulační a smluvní požadavky na vymazání informací

Pokyny:

Citlivé informace by **neměly být uchovávány déle, než je nutné**, aby se snížilo riziko jejich nežádoucího vyzrazení.

Při mazání informací v systémech, aplikacích a službách je třeba vzít v úvahu následující skutečnosti:

a) výběr metody vymazání (např. **elektronický přepis nebo kryptografický výmaz**)

b) **zaznamenání výsledků** vymazání jako důkazu

c) při využívání **služeb dodavatelů** výmazu informací **získání důkazů o výmazu** informací od nich

Pokud třetí strany ukládají informace organizace jejím jménem, měla by organizace zvážit začlenění požadavků na výmaz informací do smluv s třetími stranami

Metody výmazu - V souladu s politikou organizace týkající se uchovávání údajů a s přihlédnutím k příslušným právním předpisům a nařízením by citlivé informace měly být vymazány a to tak, že se

a) **konfigurace systémů tak**, aby bezpečně zničily informace, pokud již nejsou potřebné (např. po uplynutí stanovené doby)

b) **vymazáním zastaralých verzí**, kopií a dočasných souborů bez ohledu na to, kde se nacházejí

c) používání **schváleného bezpečného softwaru**

d) využívání **schválených certifikovaných poskytovatelů** služeb

e) používání **likvidačních mechanismů** vhodných pro typ likvidovaného **paměťového média** (např. demagnetizace)

V případě **využívání cloudových služeb** by organizace měla ověřit, zda je způsob vymazání poskytovaný poskytovatelem cloudových služeb přijatelný

Při odesílání zařízení mimo organizaci (např. prodejcům), by měly být citlivé informace chráněny **odstraněním pomocných úložišť** (např. pevných disků)

8.11 Maskování dat

Opatření: Maskování dat by mělo být používáno v souladu s tematickou politikou organizace týkající se řízení přístupu a dalšími souvisejícími tematickými politikami a obchodními požadavky s ohledem na platné právní předpisy

Účel: Omezit vystavení citlivých údajů včetně osobních údajů a dodržet právní, zákonné, regulační a smluvní požadavky

Pokyny:

Organizace by měla zvážit skrytí těchto údajů pomocí technik, jako je **maskování údajů, pseudonymizace nebo anonymizace.** Pseudonymizace nebo anonymizace mohou skrýt identifikační údaje, zamaskovat skutečnou identitu zadavatelů nebo jiných citlivých informací a odstranit příslušné vazby. Vždy je třeba ověřit, zda byly údaje odpovídajícím způsobem pseudonymizovány nebo anonymizovány.

Mezi **další techniky maskování údajů** patří např:

a) **šifrování** (vyžadující, aby oprávnění uživatelé měli klíč)

b) **nulování nebo mazání znaků** (nejsou vidět celé zprávy)

c) **různá čísla a data**

d) **záměna** (změna jedné hodnoty za jinou ke skrytí citlivých údajů)

e) nahrazení hodnot jejich **hashem**

Při **zavedení maskování dat** je třeba vzít v úvahu následující skutečnosti:

a) **neumožnit** všem uživatelům **přístup ke všem datům**

b) existují případy, kdy by **některé údaje neměly být pro uživatele viditelné u některých záznamů ze souboru údajů** (použít maskování údajů

c) použití **zastření** (používá se ve zdravotnických zařízeních)

d) případné **právní nebo regulační požadavky** (např. požadavek na maskování informací o platebních kartách během zpracování nebo uchovávání).

Při používání maskování, pseudonymizace nebo anonymizace údajů je třeba vzít v úvahu následující skutečnosti:

a) **úroveň síly maskování údajů, pseudonymizace nebo anonymizace** v závislosti na použití zpracovávaných údajů

b) **kontroly přístupu ke zpracovávaným údajům**

c) **dohody nebo omezení** týkající se používání zpracovávaných údajů;

d) **zákaz srovnávání zpracovávaných údajů s jinými informacemi** za účelem identifikace

e) **sledování poskytování a přijímání zpracovávaných údajů**

8.12 Prevence úniku dat

Opatření: Opatření pro prevenci úniku dat by se měla vztahovat na systémy, sítě a jakákoli jiná zařízení, která zpracovávají, ukládají nebo přenášejí citlivé informace

Účel: Odhalit a zabránit neoprávněnému vyzrazení a získání informací jednotlivci nebo systémy

Pokyny:

Organizace by měla zvážit následující opatření ke snížení rizika úniku dat:

a) **identifikaci a klasifikaci informací** za účelem ochrany před únikem

b) **sledování kanálů úniku dat** (např. e-mail, přenosy souborů, mobilní zařízení a přenosná paměťová zařízení)

c) **opatření k zabránění úniku** informací (např. karanténa e-mailů)

Nástroje pro prevenci úniku dat by měly být využívány k následujícím účelům:

a) **identifikaci a monitorování** citlivých informací (např. v nestrukturovaných datech v systému uživatele);

b) zjišťovat **odhalení citlivých informací** (např. při nahrávání informací do nedůvěryhodných cloudových služeb třetích stran nebo při jejich zasílání e-mailem);

c) **blokovat akce uživatele nebo síťové přenosy**, které odhalují citlivé informace (např. zabránění kopírování záznamů z databáze do tabulky)

Organizace by měla určit, zda je nutné **omezit možnost uživatele kopírovat a vkládat nebo odesílat** data do služeb, zařízení a paměťových médií mimo organizaci

V případě zálohování dat je třeba dbát na ochranu citlivých informací pomocí opatření, jako je **šifrování, řízení přístupu a fyzická ochrana paměťových médií**

Prevence úniku dat ze své podstaty zahrnuje sledování komunikace a online aktivit zaměstnanců, a tím i zpráv externích stran, což **vyvolává právní obavy**, které je třeba zvážit

8.16 Monitorovací činnosti

Opatření: Sítě, systémy a aplikace by měly být monitorovány z hlediska anomálního chování a měly by být přijímány příslušné kroky k vyhodnocení potenciálních incidentů v oblasti bezpečnosti informací

Účel: Odhalit anomální chování a potenciální incidenty v oblasti bezpečnosti informací

Pokyny:

Do systému monitorování by měly být zahrnuty následující informace:

a) odchozí a příchozí **síťový, systémový a aplikační provoz**

b) **přístupy** k systémům, serverům, síťovému vybavení, monitorovacímu systému, kritickým aplikacím atd.

c) soubory s konfigurací systému a sítě na **kritické nebo administrátorské úrovni**

d) **protokoly z bezpečnostních nástrojů** [např. antivir, IDS, systém prevence narušení (IPS), webové filtry, firewally, prevence úniku dat]

e) **protokoly událostí** týkající se činnosti systému a sítě

f) kontrola, zda je **spouštěný kód oprávněn běžet v systému** a zda do něj nebylo zasahováno (např. rekompilací za účelem přidání dalšího nežádoucího kódu)

g) **využití zdrojů** (např. procesoru, pevných disků, paměti, šířky pásma) a jejich výkonnost

Organizace by měla stanovit základní linii normálního chování, kdy přihlíží k následujícím skutečnostem:

a) přezkoumání využití systémů v **běžných obdobích a v období špičky**

b) **obvyklou dobu** přístupu, **místo** přístupu, **četnost** přístupu

Monitorovací systém by měl být nakonfigurován na základě stanovené základní linie, aby bylo možné identifikovat anomální chování, jako např:

a) neplánované ukončení procesů nebo aplikací

b) činnost typicky spojená se škodlivým softwarem

c) známé charakteristiky útoku

d) neobvyklé chování systému

e) úzká místa a přetížení

f) neoprávněný přístup

g) neoprávněné skenování podnikových aplikací, systémů a sítí

h) úspěšné a neúspěšné pokusy o přístup k chráněným zdrojům

i) neobvyklé chování uživatelů a systémů ve vztahu k očekávanému chování

8.23 Filtrování webových stránek

Opatření: Přístup k externím webovým stránkám by měl být řízen tak, aby se omezilo vystavení škodlivému obsahu

Účel: Chránit systémy před napadením škodlivým softwarem a zabránit přístupu k neautorizovaným webovým zdrojům

Pokyny:

Organizace by měla **snížit riziko přístupu svých zaměstnanců k webovým stránkám, které obsahují nezákonné informace nebo o nichž je známo, že obsahují viry nebo phishingový materiál**.

Technika pro dosažení tohoto cíle funguje tak, že se **zablokuje IP adresa nebo doména dotyčných webových stránek**. Některé prohlížeče a technologie proti škodlivému softwaru to dělají automaticky nebo je lze takto nakonfigurovat.

Organizace by měla určit typy webových stránek, na které by zaměstnanci měli nebo neměli mít přístup.

Organizace by měla z**vážit zablokování přístupu k následujícím typům webových stránek**:

a) **webové stránky, které mají funkci nahrávání informa**cí, pokud to není povoleno z oprávněných pracovních důvodů

b) **známé nebo podezřelé škodlivé webové stránky** (např. ty, které šíří malware nebo phishingový obsah);

c) příkazové a řídicí servery

d) škodlivé webové stránky **získané ze zpravodajských informací o hrozbách**

e) webové stránky sdílející **nelegální obsah**

Před zavedením tohoto opatření by organizace měla **stanovit pravidla pro bezpečné a vhodné používání online zdrojů**, včetně **případného omezení přístupu na nežádoucí nebo nevhodné webové stránky a webové aplikace**. Tato pravidla by měla být průběžně aktualizována.

Zaměstnanci by měli být **proškoleni o bezpečném a vhodném používání online zdrojů včetně přístupu na web.**

Školení by mělo zahrnovat:

› pravidla organizace,
› kontaktní místo pro vznesení bezpečnostních obav a
› proces udělování výjimek v případech, kdy je z oprávněných pracovních důvodů nutné přistupovat k omezeným webovým zdrojům

Zaměstnanci by měli být rovněž **proškoleni,** aby se ujistili, že **nepřehlédnou** žádné **upozornění prohlížeče, které hlásí, že webová stránka není bezpečná**, ale umožní uživateli pokračovat.

8.28 Bezpečné programování

Opatření: Při vývoji softwaru by se měly uplatňovat zásady bezpečného programování

Účel: Zajistit, aby byl software napsán bezpečně, a tím snížit počet potenciálních zranitelností v oblasti bezpečnosti informací v softwaru

Pokyny:

Organizace by měla zavést procesy, které zajistí **správnou správu bezpečného programování**. Měla by být stanovena a uplatňována **minimální bezpečná základní úroveň**. Tyto procesy a správa by navíc měly být rozšířeny tak, aby **zahrnovaly softwarové komponenty třetích stran a software s otevřeným zdrojovým kódem**.

Organizace by měla **sledovat reálné hrozby a aktuální rady a informace o zranitelnostech softwaru**, aby se mohla řídit zásadami bezpečného programování v organizaci prostřednictvím neustálého zlepšování a učení.

Plánování a před programováním - zásady bezpečného programování by se měly používat jak při **novém vývoji, tak při scénářích opakovaného použití**. Tyto zásady by se měly uplatňovat jak při **vývojových činnostech v rámci organizace, tak u produktů a služeb, které organizace dodává ostatním** (konfigurace vývojářských nástrojů, kvalifikace vývojářů, bezpečný návrh a architektura, kontrolované prostředí atd.).

Během programování by měly být zváženy **postupy bezpečného programování** specifické pro používané programovací jazyky a techniky; používané techniky, dokumentování kódu a odstraňování chyb a zákaz používání nezabezpečených návrhových technik.

Testování by mělo být prováděno v průběhu vývoje i po něm.

Přezkoumání a údržba programu - po zprovoznění programu provést **aktualizace, reagovat na známé zranitelnosti, zajistit ochranu zdrojového kódu** (např. pomocí nástrojů pro správu konfigurace).

Pokud je třeba softwarový balíček upravit, **je třeba zvážit :**

a) rizika ohrožení procesů integrity

b) zda je třeba získat souhlas dodavatele

c) možnost získat požadované změny od dodavatele jako standardní aktualizace programu

d) dopad v případě, že se organizace v důsledku změn stane odpovědnou za budoucí údržbu softwaru

e) kompatibilitu s jiným používaným softwarem

8.28 Bezpečné programování

Opatření: Při vývoji softwaru by se měly uplatňovat zásady bezpečného programování

Účel: Zajistit, aby byl software napsán bezpečně, a tím snížit počet potenciálních zranitelností v oblasti bezpečnosti informací v softwaru

Pokyny:

Organizace by měla zavést procesy, které zajistí **správnou správu bezpečného programování**. Měla by být stanovena a uplatňována **minimální bezpečná základní úroveň**. Tyto procesy a správa by navíc měly být rozšířeny tak, aby **zahrnovaly softwarové komponenty třetích stran a software s otevřeným zdrojovým kódem**.

Organizace by měla **sledovat reálné hrozby a aktuální rady a informace o zranitelnostech softwaru**, aby se mohla řídit zásadami bezpečného programování v organizaci prostřednictvím neustálého zlepšování a učení.

Plánování a před programováním - zásady bezpečného programování by se měly používat jak při **novém vývoji, tak při scénářích opakovaného použití**. Tyto zásady by se měly uplatňovat jak při **vývojových činnostech v rámci organizace, tak u produktů a služeb, které organizace dodává ostatním** (konfigurace vývojářských nástrojů, kvalifikace vývojářů, bezpečný návrh a architektura, kontrolované prostředí atd.).

Během programování by měly být zváženy **postupy bezpečného programování** specifické pro používané programovací jazyky a techniky; používané techniky, dokumentování kódu a odstraňování chyb a zákaz používání nezabezpečených návrhových technik.

Testování by mělo být prováděno v průběhu vývoje i po něm.

Přezkoumání a údržba programu - po zprovoznění programu provést **aktualizace, reagovat na známé zranitelnosti, zajistit ochranu zdrojového kódu** (např. pomocí nástrojů pro správu konfigurace).

Pokud je třeba softwarový balíček upravit, **je třeba zvážit :**

a) rizika ohrožení procesů integrity

b) zda je třeba získat souhlas dodavatele

c) možnost získat požadované změny od dodavatele jako standardní aktualizace programu

d) dopad v případě, že se organizace v důsledku změn stane odpovědnou za budoucí údržbu softwaru

e) kompatibilitu s jiným používaným softwarem

Co dál

1. Prostudovat normy ISO/IEC 27001 a ISO/IEC 27002
2. Provést srovnávací analýzu vůči svém ISMS a to zejména v oblasti procesů
3. Upravit procesy ISMS a úpravu zdokumentovat
4. Provést nové hodnocení rizik s důrazem na nová opatření
5. Zavést nová vybraná opatření
6. Provést interní audit

Děkuji za pozornost

ANTONÍN ŠEFČÍK

asefcik@ngss.cz

+ 420 601 307 992