Minimální rozsah dokumentace ke zdrojům/prostředkům/provozu ICT infr./GDPR

Cílem tohoto dokumentu je snaha o zvýšení IT bezpečnosti a stanovení minimálního rozsahu dokumentace. Kybernetická bezpečnost je komplexní oblast aktivit zahrnující technické a technologické prostředky, aplikace, sady pravidel nastavení hardware, software, procesů a činností a jejich používání s cílem zajistit maximální možnou ochranu dat.

Aby takto komplexní systém mohl fungovat, je naprosto nezbytné jeho činnost pravidelně a opakovaně testovat, ověřovat a na základě zjištěných skutečností jeho nastavení upravovat.

Takovýto dokumentovaný systém se nazývá Systém řízení bezpečnosti informací (anglicky "Information Security Management System“ – ISMS). Jeho nasazení a provozování má přesně stanovená pravidla, která jsou popsána např. řadou norem ISO/IEC 27000. Základem systému je definice aktiv, která je třeba chránit, definování a řízení rizik bezpečnosti informací a zavedení opatření k eliminaci rizik. Aktivy se rozumí zařízení, programy a informace, na kterých závisí chod instituce. Především se jedná o data v informačních systémech, dokumentech společnosti a jejich zálohách. Každé aktivum je popsáno a klasifikováno. Následně je zpracován návrh zabezpečení aktiva a určena osoba zodpovědná za realizaci navržených opatření. Přednostně jsou obvykle zabezpečována aktiva s nejvyšší stanovenou hodnotou.

Jednotlivá pravidla a definice sloužící k ochraně aktiv jsou prezentována sadou interních řídících norem, směrnic a pokynů.

Externí zdroje, např.:

- obecná legislativa (Zákon č. 89/2012 Sb. Občanský zákoník, Zákon č. 134/2016 Sb. Zákon o zadávání veřejných zakázek aj.),
- Zákon č. 181/2014 Sb.,
- Vyhláška č. 82/2018 Sb. a navazující předpisy,
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR),
- pokyny a směrnice zřizovatele,
- Standart konektivity 2022 ÚK

jsou do interních řídících dokumentů vhodně implementovány.

Pro potřeby obecného školního prostředí není nezbytně nutné zavedení celého systému řízení bezpečnosti informací, ale zavedení některých hlavních pravidel a principů je nezbytné zejména také s ohledem na směrnici o ochraně osobních údajů.

Prvním krokem předcházejícím úspěšnému nasazení síťových technologií a prostředků je kategorizace informací. V běžné praxi informace rozdělujeme na informace:

- veřejné (např. povinně zveřejňované informace);
- neveřejné (interní informace určené pro celou organizaci);
- chráněné (citlivé informace, u nichž není žádoucí šíření napříč celou organizací, protože jsou určeny jen pro vybraný okruh osob, osobní a personalizované informace a data).

S tímto rozdělením úzce souvisí technická podoba informací (papír, elektronické médium apod.), umístění, označování, doba a způsob uchovávání, definice způsobu přístupu k informacím, definice okruhu osob oprávněných informace číst, měnit a mazat.

Definice budou zakotveny do interní směrnice.

Dodavatel bude spolupracovat se školou a jeho GDPR zmocněncem na Interní směrnici dle „Obecného nařízení o ochraně osobních údajů - GDPR“, která primárně řeší pravidla ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů a pravidel pro oběh osobních údajů. Bude se jednat o samostatnou směrnicí a její obsah není s uvedeným nařízením EU v rozporu.

Obsah této Interní směrnice má přímý dopad na:

- nastavení segmentace sítě,
- nastavení systému pro jednotnou správu identit, která má za úkol řídit informace o uživatelích v počítačích, spravuje jejich autentizaci, role a hierarchie s cílem zvýšit zabezpečení a produktivitu a zároveň snížit náklady na správu,
- nastavení prostředků pro ukládání, zálohování a archivaci dat,
- atd.

Dále dodavatel zpracuje detailní popis technické infrastruktury zahrnující popis nastavení síťových prvků, serverů, datových úložišť, tiskáren a instalovaných systémů a aplikací. Popis obsahuje název, značku, technické parametry, kontakt na dodavatele, jeho technickou a servisní podporu, způsob monitorování, základní nastavení, správce prvku a další vybrané informace.

Vzor:

Název HW/hostitele	FIREWALL_DOLE_NAHORE
Značka + Model	ABC 35 XZZZ
Porty + Parametry	3G/4G WAN Connectivity GE RJ45 WAN / DMZ Ports: GE RJ45 Internal Ports: SFP : SFP+ : USB Ports: 1, Console (RJ45): 1, Interní uložiště: ANO IPS Throughput: x Gbps Firewall Throughput y Gbps … Ostatní parametry – viz: http://www.abc.cz/xx.pdf
Firmware	1.0.1.
Monitoring	Monitoring firewallu se provádí nepřímo – prostřednictvím monitoringu služby Zabbixx .Služba zasílá pravidelné zprávy o své činnosti formou e-mailů. Všechny tyto zprávy procházejí přes *internet*. Pokud by *internet* nefungoval, přestanou přicházet kontrolní zprávy a dohledový systém bezodkladně informuje IT správce. Rovněž probíhá pravidelná (minimálně 1x týdně) ruční kontrola logů přímo v operačním systému firewallu.
Servis/podpora	Podporu firewallu zajišťuje osoba v roli ADM. Podpora firewallu je zajišťována v rámci záruky od výrobce: XXX + 8x75 support 5y

	Kontakt na podporu: +420 999 999 999
Konec podpory	x.z.2027
Audit	Audit je řešen manuální kontrolou logů uložených ve firewallu.

V případě popisu serverů, síťových zařízení a stanic je součástí dokumentu také seznam spuštěných a seznam zakázaných služeb.

Nová dokumentace obsahuje minimálně zejména tyto části:

1. Správa a konfigurace
   1.1. Obsah správy systémů
   1.2. Personální obsazení
   1.3. Nástroje pro správu
   1.4. Zdroje informací o stavu sytému – log management
   1.5. Konfigurace komponent
   1.6. Zálohování konfiguračních souborů
2. Havarijní plánování / Disaster Recovery Plan
3. Správa uživatelských účtů
   3.1. Ochrana proti sdílení hesel mezi správci
      3.1.1. Úložiště hesel
      3.1.2. Zakládání administrátorských účtů na serverech a firewallech
      3.1.3. Změna administrátorských hesel
      3.1.4. Odblokování účtu po neúspěšné autentizaci
      3.1.5. Rušení administrátorských účtů na serverech a firewallech
      3.1.6. Řešení problému ztracených či zapomenutých hesel
   3.2. Jmenná konvence účtů
      3.2.1. Jmenná konvence účtů
      3.2.2. Jmenná konvence neprivilegovaných účtů
   3.3. Požadavky na obnovu hesel u privilegovaných účtů
   3.4. Záloha hesla administrátorského účtu
      3.4.1. Autentizační údaje k uživatelským účtům na serverech
   3.5. Požadavky na sílu a obnovu hesel u běžných neprivilegovaných účtů
4. Pracovní postupy
   4.1. Přístup k serverům a firewallům
   4.2. Start a zastavení systému
   4.3. Zálohování konfigurací
   4.4. Profylaxe a pravidelná údržba systému
      4.4.1. Kontrola systémových žurnálů
      4.4.2. Kontrola zaplnění disku
      4.4.3. Kontrola nepotřebných účtů
      4.4.4. Antivirová ochrana
      4.4.5. Vyhodnocení logů IDS - Intrusion Detection System (systém pro odhalení průniku)
      4.4.6. Revize topologie sítě
      4.4.7. Kontrola hardware a diskového pole
   4.5. Aktualizace systému a SW komponent
      4.5.1. Zjišťování dostupných aktualizací
   4.6. Aktualizace pravidel firewallů
   4.7. Záznamy do provozního deníku

Samostatným dokumentem je „Směrnice pro nastavení a provádění zálohování a archivace dat“, kdy důležitým obsahem je:

- Popis typu a rozsahu zálohovaných dat
- Popis technologie pro zálohování a archivaci
- Popis činností při zálohování a archivaci
    - Algoritmus pro zálohování (doby uložení, termíny provedení, způsob provedení, umístění záložních médií apod.)
    - Kontrola možnosti obnovení zálohy
        - Roční úplná kontrola
        - Průběžná
    - Algoritmus pro archivaci elektronických dat
- Odpovědnosti a pravomoci
    - Matice vlastníků dat
    - Matice odpovědností při zálohování
    - Matice odpovědností při archivaci
- Související dokumentace

Součástí provozu je správné a úplné vedení Provozního deníku, kam jsou administrátorem/administrátory zaznamenávány všechny provozní události IT systému, a to zejména:

- instalace a konfigurace komponent (HW, SW),
- nastavení práv a hesel uživatelů včetně administrátorů,
- provedené zálohy a archivace,
- provedené testy obnovení dat ze zálohy,
- provedené pravidelné kontroly, včetně jejich výsledků a návrhu opatření,
- zjištěné nedostatky a rozpory s předepsaným stavem,
- havárie systémů,
- bezpečnostní události a incidenty.

Ustanovení přílohy č. 16 a-d) bod 3.5. (2) h není tímto dokumentem dotčeno a platí souběžně.

Uchazeč/dodavatel je povinen zpracovat uvedenou dokumentaci v tomto minimálním rozsahu v součinnosti s danou školou.