Bezpečnost ICT

směrnice
Gymnázia a Jazykové školy s právem státní jazykové zkoušky Zlín

Zlín 2018

schválila: Mgr. Alena Štachová,
ředitelka školy

OBSAH

SEZNAM POUŽITÝCH POJMŮ A ZKRATEK

Active Directory	Je řešení adresářových služeb pro správu síťových prostředků. Active Directory využívají administrátoři počítačových sítí pro různé účely. Nastavují za jeho pomoci pravidla a politiku sítě, instalují programy na veliké množství PC stanic zároveň či řeší kritické situace v síti.
Administrátor	Osoba pověřená správou jednoho, nebo více ICT zařízení, která je schválena ředitelkou školy a má nejvyšší úroveň oprávnění pro ICT zařízení ve své správě.
Administrátorský účet	Uživatelský učet, jenž má nevyšší možná oprávnění v rámci daného operačního systému nebo aplikace.
Aplikace	Programové vybavení výpočetní techniky organizace (např. MS Word).
Autentizace	Je proces ověření proklamované identity subjektu.
Bezpečnost informací	Je zajištění následujících atributů chráněných informací: důvěrnosti (ochrana před neoprávněným čtením), integrity (ochrana před neoprávněnými úpravami nebo zničením) a dostupnosti (zajištění adekvátního přístupu a ochrana před jeho neoprávněným zamezením).
Cloud	Externí internetové datové uložiště (např. One Drive, Google drive, Dropbox apod.).
Fyzická bezpečnost	Fyzická bezpečnost znamená používání fyzických a technických ochranných opatření k zamezení neoprávněného přístupu k majetku a informacím organizace.
Hardware	Označuje veškeré fyzicky existující technické vybavení výpočetní techniky či síťových prostředků.
Operační systém	Základní programové vybavení počítače (tj. software), který je zaveden do paměti počítače při jeho startu a zůstává v činnosti až do jeho vypnutí (např. MS Windows 10).
Osobní údaj	Veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické,

	ekonomické, kulturní nebo společenské identity této fyzické osoby.
Počítačová síť organizace	Síťové prostředky a výpočetní technika ve správě, nebo v majetku organizace, které realizují spojení a výměnu informací.
Pověřenec pro ochranu osobních údajů	Mgr. Dana Stesková, zástupce v době nepřítomnosti: Mgr. Sylva Mikelová
Přístupový údaj	Sada informací potřebných pro přihlášení do operačního systému nebo aplikace. V základní podobě jsou tvořeny uživatelským jménem a heslem.
Režimová opatření	Ucelený soubor opatření, pokynů, příkazů, zákazů a omezení představující soupis instrukcí pro vstup, odchod, pohyb v objektu a přistup k informacím organizace.
Síťové prostředky	Technická zařízení používaná k zajištění provozu, správy a bezpečnosti sítě organizace. Jedná se zejména o Routery, servery, switche, firewall apod.
SLA – Service Level Agreement	Je dohoda o úrovni poskytovaných služeb. SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi. SLA definuje rozsah, úroveň a kvalitu služby.
Správce ICT	Osoba odpovědná za provozování a správu počítačové sítě a prostředků ICT organizace. Disponuje administrátorskými účty k operačním systémům a některým aplikacím.
Uživatel	Zaměstnanec využívající výpočetní techniku organizace
Uživatelské jméno	Je jednoznačný identifikátor uživatele v systému. Jedná se o unikátní jméno zpravidla složené z písmen (případně i číslic).
Uživatelský účet	Jednoznačná identifikace uživatele v rámci operačního systému nebo aplikace. Uživatelský účet umožňuje plnou práci, ale bez možnosti instalovat aplikace do výpočetní techniky nebo měnit nastavení operačního systému nebo aplikace. Uživatelský účet se standardně skládá z uživatelského jména a hesla.
VPN	Virtuální privátní síť (zkratka VPN, anglicky Virtual Private Network) je v informatice prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly

	propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě.
Výpočetní technika	Soubor počítačů, notebooků, tabletů nebo smartphonů organizace. Obecně všech zařízení, která disponují vlastním operačním systémem.
Zvláštní kategorie údajů	Osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

POZNÁMKA

Role definované tímto dokumentem předpokládají, že je bude vykonávat i žena. Avšak z důvodu zjednodušení textu jsou použity názvy jednotlivých rolí v mužském rodě. Bude-li danou roli zajišťovat žena, předpokládá se automatické přechylování názvů jednotlivých rolí bez nutnosti úpravy směrnice.

1 PŮSOBNOST DOKUMENTU

Tento dokument stanovuje bezpečnostní pravidla pro zpracování, uchování a předávání dat organizace, obsahující osobní údaje v souladu s požadavky 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 a o zrušení směrnice 95/46/ES (dále jen GDPR).

Dokument je platný pro všechny zaměstnance organizace. Bezpečnostní pravidla, definovaná tímto dokumentem, jsou platná pro zpracování dat, obsahujících osobní údaje ve všech operačních systémech a aplikacích, které jsou ve správě organizace a provozované buď na výpočetní technice Gymnázia a Jazykové školy s právem státní jazykové zkoušky Zlín, nebo na technice a aplikacích poskytnutých smluvním dodavatelem.

2 ÚVOD

Dokument stanovuje 3 různé úrovně bezpečnostních požadavků na zajištění ochrany osobních údajů. Nejnižší úroveň, označená jako Úroveň bezpečnosti 1, definuje minimální bezpečnostní požadavky na zajištění ochrany osobních údajů pro všechny organizace. Úrovně bezpečnosti 2 a 3 obsahují zvýšené požadavky na bezpečnost v některých oblastech. Jestliže tedy organizace implementuje opatření vyšší úrovně bezpečnosti, musí mít implementovány všechny požadavky nižších úrovní.

Popis jednotlivých úrovní bezpečnosti je následující:

- **Úroveň bezpečnosti 1** – minimální bezpečnostní požadavky platné pro všechny organizace bez rozdílu svého zaměření. Jsou zde zařazeny organizace, které používají pouze koncové počítače a nemají serverová řešení. Většinu svých agend zpracovávají v základních aplikacích pro Windows (např. MS Office) nebo v rámci on-line dodavatelských řešení, tzv. pomocí webového prohlížeče. Síťová infrastruktura existuje jen pro připojení do sítě Internet, případně sdílený tisk a obsahuje pouze několik jednotek pracovních stanic nebo notebooků.

- **Úroveň bezpečnosti 2** – Organizace, které mají vlastní server nebo síťové zálohovací řešení. Tato zařízení jsou umístěna ve standardních kancelářích zaměstnanců organizace. Síťová infrastruktura je již větší, může obsahovat desítky počítačů nebo notebooků. Zaměstnanci mohou mít možnost ukládat svá pracovní data na síťové disky. Využívají se aplikace, které jsou dostupné také ze síťového prostředí organizace apod.

- **Úroveň bezpečnosti 3** – Organizace disponuje vlastní serverovnou, ve které jsou umístěny technologické prvky síťové infrastruktury, jako jsou aplikační servery, záložní servery, NAS servery apod. Síťová infrastruktura je již rozlehlejší a zahrnuje mnoho koncových zařízení, a to jak stolních počítačů, tak i notebooků. Zaměstnanci plně využívají vnitřní infrastrukturu pro ukládání dat (síťové disky), přístupy k aplikacím či sdílení dokumentů (intranet) apod.

Jednotlivé úrovně bezpečnosti jsou vždy vyznačeny samostatným podnadpisem: „**Úroveň 1**“ nebo „**Úroveň 2**“ nebo „**Úroveň 3**“.

3 ORGANIZACE BEZPEČNOSTI

Ředitelka školy je odpovědná za ustanovení zaměstnanců do jednotlivých rolí, ve kterých budou odpovědni za řízení bezpečnosti osobních údajů. Jedná se především o ustanovení role pověřence pro ochranu osobních údajů, správců ICT, administrátorů a jednotlivých garantů aplikací. Schvaluje také přidělení administrátorských účtů vybraným zaměstnancům.

4 BEZPEČNOSTNÍ PRAVIDLA UŽIVATELŮ

Úroveň 1, 2 a 3

Zaměstnanci jsou povinni dodržovat následující bezpečnostní pravidla při zpracovávání osobních údajů:

1. Svěřenou výpočetní techniku využívají **pouze pro plnění pracovních povinností.**

2. Dodržují zásady pro tvorbu přístupového hesla k operačním systémům, nebo aplikacím.

3. Zachovávají jedinečnost a důvěrnost přístupového hesla, tj. nikomu heslo nesdělují a nikde a nijak si jej nezaznamenávají.

4. Při přihlašování k operačním systémům nebo aplikacím dbají na to, aby nebylo možné heslo odpozorovat další osobou.

5. V případě jakéhokoliv podezření na kompromitaci hesla nebo dokonce jeho zneužití heslo okamžitě změní.

6. Před opuštěním pracoviště **zabezpečují výpočetní techniku uzamčením pracovní plochy nebo odhlášením** (např. pomocí kláves ⊞+L nebo ctrl+alt+del). Odborné učebny informatiky (407, 411 a 421) **poslední opouští učitel a místnost uzavře**.

7. Dodržují pravidlo „prázdného stolu“, to znamená, že všechny dokumenty obsahující osobní údaje, které v danou chvíli nezpracovávají, jsou uloženy v uzamykatelných skříních.

8. Při používání přenosné výpočetní techniky a datových nosičů v majetku školy (notebooků, flash disků, externích HDD, DVD apod.) mimo prostory organizace:

- nepředávají tuto techniku a nosiče třetím osobám,
- učiní všechna dostupná opatření, která mohou zabránit ztrátě či odcizení výpočetní techniky (neponechávají je bez dohledu, nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.),
- v případě přenosných datových médií používají pouze zařízení, která jsou zašifrována,
- nepoužívají výpočetní techniku na veřejných místech pro práci s daty organizace,
- ztrátu či odcizení okamžitě nahlásí svému nadřízenému.

9. Neinstalují software na výpočetní techniku organizace. Pokud potřebují k práci instalaci software, požádají správce ICT, který instalaci provede po schválení ředitelkou školy.

10. Nepoužívají soukromé datové nosiče (např. CD, flash disky, externí HDD).

11. Nenavštěvují rizikové internetové stránky.

12. Důsledně ověřují doručenou elektronickou poštu a v případě podezření, že se jedná o závadný e-mail (spam, podvodný e-mail apod.), **takovou zprávu neotvírají, nereagují na ní a tuto skutečnost neprodleně ohlásí správci ICT**. Správce ICT **neprodleně informují** také při každém jiném problému s elektronickou poštou (problémy s odesíláním mohou být také způsobeny napadením počítače nebo schránky).

13. Nezasahují do výpočetní techniky a její konfigurace, vyjma situací, kdy toto bude schváleno přímo správcem ICT.

14. Nekopírují, neukládají, nepřenáší osobní údaje a data z aplikací organizace na pevných discích počítačů, jiných datových nosičích, vyjma stanovených úkolů a povinností či po schválení ředitelkou školy. Na cloudové úložiště je zakázáno ukládat jakékoli osobní údaje!

15. Soubory, obsahující osobní údaje, adresované mimo doménu Gymnázia a Jazykové školy s právem státní jazykové zkoušky Zlín, zasílají pouze chráněné (prostřednictvím datových schránek, nebo prostřednictvím elektronické pošty minimálně v archivním souboru (např. ve formátu „zip“) opatřeném heslem, přičemž heslo zašlou adresátovi jiným komunikačním kanálem, např. prostřednictvím SMS).

16. Soubory, obsahující zvláštní kategorie osobních údajů, zasílají pouze prostřednictvím datové schránky.

17. Netisknou data z aplikací organizace pro jiné než pracovní účely.

18. Pokud dojde k úniku, kompromitaci nebo ztrátě dat obsahujících osobní údaje, je každý zaměstnanec povinen **neprodleně hlásit tento incident nadřízenému vedoucímu zaměstnanci, který tuto skutečnost hlásí neprodleně pověřenci pro ochranu osobních údajů**.

5 BEZPEČNOSTNÍ PRAVIDLA SPRÁVCE ICT

Správce ICT je odpovědný za dodržování bezpečnostních pravidel při zpracovávání a ochraně osobních údajů v rámci počítačové sítě a na výpočetní technice organizace. Je povinen dodržovat následující bezpečnostní pravidla při plnění pracovních úkolů správce ICT:

1. Spolupracuje s organizací na tvorbě a aktualizaci analýzy rizik.

2. Spravuje antivirový systém na všech výpočetních prostředcích organizace a to především:

- provádí jeho instalaci,
- kontroluje funkčnost aktualizací,
- kontroluje výstupy programu.

3. Pro zaměstnance organizace připravuje a instaluje výpočetní techniku, kterou nastaví dle definovaných bezpečnostních požadavků (např. způsoby přihlášení, oprávnění uživatelského účtu, uzamykání počítače při neaktivitě apod.) a následně ji předává určeným zaměstnancům k použití.

4. Vytváří a nastavuje zaměstnancům uživatelská oprávnění do počítačové sítě a aplikací v rozsahu schváleném ředitelkou školy.

5. Na základě požadavku ředitelky školy zřizuje nebo ruší přístupy do operačních systémů organizace.

6. Zajišťuje fyzickou bezpečnost datových úložišť, nosičů a dat organizace.

7. Poskytuje zaměstnancům organizace technickou podporu při využívání výpočetní techniky.

8. Provádí kontrolní činnost k zajištění bezpečnosti osobních údajů zpracovávaných ve výpočetní technice organizace.

9. Provádí bezpečnou likvidaci datových nosičů organizace, zejména pak pevných disků, flash disků, paměťových karet, CD a DVD disků apod.

10. V případě nutnosti odeslat výpočetní techniku či jejich komponenty obsahující osobní údaje mimo organizaci (oprava u servisní organizace, výpůjčka, pronájem, vyřazení, likvidace apod.), musí před odesláním vymazat z pevného disku veškeré osobní údaje nebo musí vyjmout paměťová média.

11. Provádí zálohování zpracovávaných dat a klíčových síťových prostředků organizace tak, aby při selhání např. hlavního datového úložiště, bylo možné provést obnovu dat s minimální ztrátou uložených dat vzhledem k okolnostem havárie.

6 ŘÍZENÍ RIZIK

Úroveň 1, 2 a 3

Organizace provádí v pravidelných intervalech (alespoň jedenkrát za rok) analýzu rizik v souladu s metodikou pro analýzu rizik na základě požadavků čl. 24 a 32 GDPR.

Analýza rizik GDPR má za cíl určit možné hrozby a zranitelnosti při zpracování osobních údajů, včetně identifikace a stanovení rizik, která mohou vzniknout působením těchto hrozeb na účely zpracování osobních údajů.

7 ŘÍZENÍ AKTIV

Úroveň 1, 2 a 3

Ředitelkou pověřená osoba eviduje veškerý hardware a aplikace používané organizací.

Používání soukromých přenosných paměťových zařízení (externí pevné disky a flash disky) pro ukládání nebo zpracování osobních údajů je zakázáno.

Paměťová zařízení, která ke své práci potřebují zaměstnanci, jsou evidována. Evidenci paměťových zařízení provádí správce ICT nebo jiná ředitelkou pověřená osoba.

Veškerá výpočetní technika organizace disponuje aktuálním operačním systémem a aplikacemi, jež mají nastavené automatické aktualizace.

Při přidělení výpočetní techniky jinému zaměstnanci správce ICT provádí kompletní reinstalaci. Ředitelka nebo jí pověřená osoba určí, jakým způsobem naložit s daty, která jsou na výpočetní technice uložena.

8 ŘÍZENÍ PŘÍSTUPŮ

Úroveň 1 a 2

Každý zaměstnanec využívající výpočetní techniku organizace, používá pro připojení k operačním systémům a aplikacím jedinečné uživatelské jméno a heslo.

Společné, projektové či jinak sdílené uživatelské účty k operačním systémům a aplikacím obsahující osobní údaje jsou zakázány.

Všem zaměstnancům organizace jsou standardně přidělovány základní uživatelské účty.

Přístup ke sdíleným složkám je zaměstnancům povolen pouze na základě zadání jejich uživatelského jména a hesla. Správce ICT definuje způsoby přístupu k těmto složkám a na základě schválení ředitele nastaví příslušná přístupová oprávnění jednotlivým uživatelům.

Administrátorské účty jsou striktně řízeny. Správce ICT na základě souhlasu ředitelky školy nastavuje přístupy tak, aby administrátorským účtem disponovali jen zaměstnanci, kteří jej ke své práci prokazatelně potřebují (správci ICT apod.).

Zaměstnanci s administrátorskými účty jsou prokazatelně seznámeni s faktem, že jsou majiteli administrátorského účtu a jsou si vědomi vyšších bezpečnostních a uživatelských nároků spojených s tímto typem účtu.

Zaměstnanci s administrátorskými účty jsou pro běžnou práci povinni používat standardní uživatelský účet. Administrátorský účet jsou oprávněni použít pouze v opodstatněných případech k výkonu činností, pro které je toto oprávnění nezbytné.

Správce ICT vede seznamy zaměstnanců, kteří disponují administrátorskými účty. Ředitelka školy, ve spolupráci se správcem ICT, pravidelně tyto seznamy přezkoumává z hlediska aktuálnosti a potřebnosti.

Při nástupu zaměstnance jsou správcem ICT, na základě pokynů ředitelky školy, nastupujícímu zaměstnanci přiděleny uživatelské účty a přístupové údaje k operačním systémům a aplikacím organizace.

Při vzniku potřeby změnit přidělená přístupová opatření, žádá zaměstnanec ředitelku školy o povolení požadovaných přístupových oprávnění.

V případě ukončení pracovního poměru zaměstnance jsou na základě pokynu ředitelky školy veškerá přístupová oprávnění zaměstnance odebrána správcem ICT.

Na veškeré výpočetní technice organizace je nastaveno uzamykání uživatelského účtu po 5 minutách jeho neaktivity.

Mobilní zařízení organizace (notebooky, tablety) jsou chráněna proti neoprávněnému přístupu heslem.

Pravidla pro hesla uživatelů jsou stanovena následovně:

- minimální délka je 8 znaků, obsahující alespoň jednu číslici a velké písmeno,
- maximální platnost hesla je nastavena na 12 měsíců s vynucenou změnou (tj. nelze ji odložit).

Administrátorské účty a správce ICT pro přihlašování k síťovým prostředkům používá heslo splňující alespoň následující pravidla:

- minimální délka 15 znaků, obsahuje alespoň jednu číslici, malé a velké písmeno,
- maximální platnost hesla je nastavena na 6 měsíců s vynucenou změnou (tj. nelze ji odložit).

Úroveň 3

Pro řízení přístupů k operačním systémům se využívá řešení adresářových služeb pro správu síťových prostředků (např. Active Directory).

Organizace má vytvořené uživatelské role s předem definovanými oprávněními pro operační systémy a aplikace. Na základě takto vytvořených rolí s definovanými oprávněními jsou prosazována pravidla pro správu veškeré činnosti všech uživatelů počítačové sítě organizace.

Pokud je to možné, tak síťové aplikace, síťové disky apod. jsou napojeny na řešení adresářových služeb, která slouží pro přímé řízení přístupových oprávnění uživatelů na základě členství v předem definovaných skupinách.

9 FYZICKÁ BEZPEČNOST

Úroveň 1

Gymnázium a Jazyková školy s právem státní jazykové zkoušky Zlín má **definovaná režimová opatření pro provoz budovy organizace**. Jsou popsána v samostatném metodickém pokynu (MP12 – Zajištění bezpečnosti žáků, posluchačů a zaměstnanců GJŠ Zlín).

Zaměstnanci, zacházející s písemnostmi, obsahujícími osobní údaje, mají dostatek uzamykatelných úložných prostor pro ukládání těchto dokumentů, které aktivně využívají.

V organizaci je stanoven **klíčový režim** (tzn. klíče, přidělené zaměstnancům, jsou evidovány). Duplikáty klíčů jsou uloženy v uzamykatelné skříňce.

Úklid prostor organizace je prováděn **pouze vlastními zaměstnanci**.

Úroveň 2

Servery a jiná klíčová síťová zařízení jsou umístěny takovým způsobem, který maximálně zabraňuje nepovolaným osobám s těmito zařízeními jakkoliv manipulovat nebo je poškodit.

Úroveň 3

V rámci klíčového režimu pro vstup do jednotlivých místností využívá Gymnázium a Jazyková škola s právem státní jazykové zkoušky Zlín **systém generálního klíče**.

Všechny klíčové síťové prostředky jsou umístěny v serverovně. Základní zabezpečení vyplývá z povahy a umístění dané místnosti.

Okruh osob, oprávněných ke vstupu do serverovny, je omezen jen na správce ICT.

10 NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

Úroveň 1

Data, obsahující osobní údaje, ukládají zaměstnanci do určených adresářů na interní pevný disk přidělené výpočetní techniky. **Ukládat osobní údaje na soukromá paměťová média a do cloudu je zakázáno.**

Soubory, obsahující osobní údaje, jsou primárně zasílány mimo organizaci prostřednictvím datové schránky. Pokud tak nelze učinit, musí zaměstnanec tento soubor uložit do souboru typu ZIP apod. zabezpečeného heslem, který je odeslán příjemci elektronickou poštou. Heslo je příjemci zasláno jiným komunikačním kanálem např. SMS. Pro zašifrování souboru je možné využít kvalifikovaný certifikát.

Soubory, obsahující zvláštní kategorie osobních údajů, jsou zasílány pouze prostřednictvím datové schránky.

Zaměstnanci, zpracovávající dokumenty obsahující osobní údaje, mají možnost zabezpečeného tisku na osobních tiskárnách umístěných v kanceláři zaměstnance, nebo na společných tiskárnách, umístěných mimo místnost zaměstnance přiložením identifikačního čipu k tiskárně.

Pro ukládání osobních údajů na přenosná paměťová zařízení (flash a externí pevné disky) nebo notebooky **je vždy využito šifrování**.

Paměťová zařízení, obsahující zálohy dat organizace, jsou uchovávána v uzamykatelných skříních a nejsou používána pro jiný účel.

Úroveň 2 a 3

Data obsahující osobní údaje, která nejsou uložena v aplikaci (např. soubory MS Word, MS Excel apod.), ukládají zaměstnanci do určených adresářů na interní pevný disk přidělené výpočetní techniky nebo dle potřeby na síťové disky organizace.

Organizace má nastavený automatizovaný systém zálohování důležitých částí počítačové sítě včetně síťových prostředků.

11 BEZPEČNOST SÍTĚ

Úroveň 1

Wi-Fi síť organizace je používána jen pro přístup do sítě Internet. Je chráněna standardními prostředky včetně přístupového hesla. Heslo pro přístup do sítě Wi-Fi je pravidelně měněno 1x za 6 měsíců. Minimální požadavky na kvalitu hesla jsou definovány v kapitole Řízení přístupů (Úroveň 1).

V nastavení přístupových údajů k administraci routerů musí odpovědná osoba změnit továrně nastavené přístupové údaje. Kvalita nového hesla splňuje požadavky pro heslo správce ICT (Úroveň 2).

Mobilní zařízení organizace s vlastním operačním systémem jsou vybavena antivirovou aplikací.

Zaměstnanci mohou využívat soukromá mobilní zařízení pouze pro práci s obsahem pracovní e-mailové schránky. Jiné využití soukromých mobilních zařízení pro pracovní účely (např. připojení do vnitřní sítě organizace, administrace aplikací apod.) je zakázáno.

Úroveň 2

Pokud je Wi-Fi síť používána pro přístup k interní síti, a tedy i aplikacím organizace, je identita zaměstnance před zpřístupněním této sítě ověřena prostřednictvím zadání přístupových údajů. Bez ověření identity zaměstnance nejsou interní síť, aplikace nebo síťové disky zpřístupněny.

Přístup k zálohám síťových prostředků a síťovým aplikacím je striktně omezen jak na logické, tak i fyzické úrovni pouze na oprávněné osoby.

Všechny vzdálené přístupy k síti organizace (pomocí např. vzdálené plochy nebo VPN) povoluje ředitelka školy.

Všechny způsoby vzdáleného přístupu k síti organizace splňují následující:

- vytvořené spojení v rámci vzdáleného přístupu je šifrované (bez ohledu na povahu přenášených dat) a předchází mu autentizace (minimálně heslem, lépe uživatelským certifikátem),
- každý vzdálený přístup je jednoznačně identifikovatelný (uživatel) a je zaznamenán,
- uživatelé nesmí „propůjčovat“ své oprávnění vzdáleného přístupu třetím osobám, byť zaměstnancům organizace,
- připojení probíhá prostřednictvím bezpečného kanálu (HTTPS, VPN, pomocí VPN mimo veřejnou síť poskytovatele apod.).

Správce ICT vede evidenci zaměstnanců a výpočetní techniky s povoleným vzdáleným přístupem. Tyto seznamy jsou v pravidelných intervalech (jedenkrát za rok, vždy k termínu zahájení školního roku) přezkoumávány ředitelkou školy.

Úroveň 3

V organizaci je využíváno vhodné logické dělení sítě na jednotlivé segmenty (tzv. segmentace sítě). Správce ICT nastavuje samostatné segmenty sítě.

Síťové zásuvky organizace jsou připojeny dle jejich využití. Nepoužívané zásuvky jsou správcem ICT v rozvaděči odpojeny.

Správce ICT přezkoumává v pravidelných intervalech (alespoň 1x za měsíc) důležité bezpečnostní logy firewallu. Například využití sítě (jednotlivých portů), neúspěšné pokusy o vzdálené přihlášení, pokusy o skenování sítě apod.

12 DODAVATELÉ SLUŽEB ICT

Úroveň 1, 2 a 3

Organizace identifikovala dodavatele aplikací a služeb ICT s možností přístupu k datům organizace (i vzdálený přístup např. pomocí VPN) a uzavřela s nimi smlouvy, resp. dodatek smlouvy o zpracování osobních údajů v souladu s požadavky čl. 28 GDPR.

Správce ICT eviduje jednotlivé vzdálené přístupy dodavatelů a kontroluje jejich oprávněnost.

V rámci smluvního vztahu s dodavatelem si organizace stanoví předmět dodávané služby. V rámci klasifikace úrovně dodávky musí být minimálně stanoveny následující podmínky:

- stanovení předmětu a kvality služby,
- stanovení service level agreement SLA (pokud je předmětem dodávky služba),
- stanovení požadavků na bezpečnostní opatření pro dodavatele a zároveň dodavatelského řetězce (pokud rizika závisí nejen na dodavateli, ale i na jeho subdodavatelích),
- definice stížností, reklamací (stanovení postupů),
- eskalační procedura (v případě, že nelze s dodavatelem dohodnout řešení, mělo by být určeno, na kterou hierarchicky vyšší řídící úroveň se řešení problému přesune),
- nastavení kontrolních mechanizmů v rámci předmětu dodávané služby,
- hodnocení a kontrola bezpečnostních opatření.

Za řízení dodavatelů je odpovědná ředitelka školy.

O všech změnách, dohodách a kontrolách s dodavateli musí být proveden záznam.