PRŮVODCE KE STANDARDU KONEKTIVITY ŠKOL

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Praha, březen 2024

Č.j. MSMT-27467/2023-1

Obsah

Úvod

Českou společnost, a tedy i vzdělávací systém čekají velké výzvy i příležitosti ve spojitosti s tzv. dvojitou – digitální a zelenou transformací[1]. Rychlá digitalizace v posledním desetiletí změnila náš způsob života a pravděpodobně jej bude měnit i nadále. Až 90 % pracovních pozic bude v blízké době vyžadovat alespoň základní digitální dovednosti[2]. V budoucnosti bude čím dál akutnější nedostatek ICT specialistů s pokročilými digitálními dovednostmi, především z oblasti umělé inteligence nebo kyberbezpečnosti.

Cílem vzdělávání je proto v následující dekádě základními a nepostradatelnými kompetencemi vybavený a motivovaný jedinec, který dokáže v co nejvyšší míře využít svůj potenciál v dynamicky se měnícím světě ve prospěch jak svého vlastního rozvoje, tak ve prospěch rozvoje celé společnosti s ohledem na druhé. Poslední roky pro školy představovaly velkou zatěžkávací zkoušku. Pandemie Covid-19 ukázala sílu digitálních technologií, ale i silné či slabé stránky digitalizace. V reakci na globální situaci v pandemii přinesla Evropská komise finanční nástroj, díky kterému v souladu s Národním plánem obnovy Ministerstvo školství, mládeže a tělovýchovy (dále jen „MŠMT") investuje do digitalizace škol (více viz https://edu.cz/digitalizujeme). Počet digitálních zařízení ve školách tak rapidně roste a bude dále růst. Impulzem pro digitalizaci ve vzdělávání je také přechod škol na výuku dle inovovaných školních vzdělávacích programů posilujících informatické myšlení a digitální kompetence.

Ve všech výše popsaných výzvách je nezbytné školy podporovat, a to i ohledně jejich digitální infrastrukturu, která by měla být funkční a bezpečná. Funkčností se v tomto smyslu rozumí především možnost efektivního využívání digitálních technologií ve výuce v souladu s inovovanými školními vzdělávacími programy. Bezpečností se rozumí primárně schopnost čelit hrozbám vnějšího online světa.

MŠMT publikovalo Standard konektivity škol (dále také „Standard"), který je dostupný na webových stránkách https://edu.cz/digitalizujeme. Dokument definoval základní technická kritéria cílového stavu školní síťové infrastruktury a přijatelnosti aktivit projektů naplňující požadavky na školy v 21. století, mj. i strategický cíl IROP 4.1 v oblasti zajištění vnitřní konektivity škol a připojení k internetu – rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu.

Cílem Průvodce ke Standardu konektivity škol je blíže školám vysvětlit problematiku digitální infrastruktury školy. Zároveň jim přiblížit důležitost kvality a funkčnosti digitální infrastruktury a pomoci procesu digitalizace vzdělávání. Dokument je určen pro ředitele, ICT koordinátory, správce IT i zřizovatele.

1 https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

2 World Economic Forum. The Future of Jobs. [online]. [cit. 09. 04. 2021]. Dostupné z: *http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf*

K dispozici jsou i následující metodické materiály:

- **Prokázání a kontrola naplnění Standardu konektivity škol.** Jedná se o dokument pro všechny školy/příjemce, které mají prokázat naplnění parametrů uvedených ve Standardu konektivity škol, dostupný na https://www.edu.cz/digitalizujeme/standard-konektivity-skol#prokazani
- **Bezpečná digitální infrastruktura školy.** Dokument, který představuje základní principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro školy. Zároveň je určen IT správcům či administrátorům, dostupný na https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/
- **Bezpečná školní ICT infrastruktura.** Jedná se o edukační videa, která jsou dostupná na https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/
- **IT správa.** Příručka ke správě ICT ve škole a příklady dobré praxe (rozhovory i videa), které jsou dostupné na https://www.edu.cz/digitalizujeme/it-sprava/.

Nevíte, jak si Vaše škola stojí na poli digitální infrastruktury? Zda je dostatečná, funkční a bezpečná? Obraťte se na specializované IT guru, kteří Vám rádi pomohou a zdarma prověří stav digitální infrastruktury vaší školy. Více informací naleznete na https://www.edu.cz/digitalizujeme/it-guru/.

Další informace o metodické podpoře naleznete na https://www.edu.cz/digitalizujeme/metodicka-podpora/.

V případě dotazů nás kontaktujte na digitalizujeme@msmt.cz.

Věříme, že Vám tento dokument a další metodická podpora poskytnutá MŠMT a Národním pedagogickým institutem ČR pomůže a bude pro Vás inspirací na cestě digitalizace Vaší školy.

Průvodce dokumentem

Průvodce ke Standardu konektivity škol je rozdělen na dvě části, stejně jako Standard konektivity: vnější konektivita a vnitřní konektivita školy.

Jednotlivé části obsahují oblasti, u kterých je vždy vysvětleno:

Proč? je důležité se jimi zabývat,

- Co? je třeba ze strany školy zajistit
- Jak? návodné otázky, které by měly být položeny.

Technické požadavky, které je třeba pro bezpečnou a funkční digitální infrastrukturu zajistit.

- minimální úroveň – bez zajištění této úrovně nelze považovat digitální infrastrukturu školy za funkční ani bezpečnou;
- úroveň Standardu konektivity škol
- doporučená úroveň a další doporučení

KONEKTIVITA ŠKOLY K VEŘEJNÉMU INTERNETU (WAN) – VNĚJŠÍ KONEKTIVITA ŠKOLY

Proč?

Pro fungování školy v 21. století je nutné zajistit dostatečně kvalitní a bezpečné připojení k internetu. Pandemická situace ukázala vzrůstající nároky na kvalitu nejen vnitřní, ale i vnější rychlosti a kapacity připojení ke světové síti. Toto připojení nesmí zůstat otevřené všemu, je tedy nutné vnitřní svět školy chránit ochrannou zdí, a to tzv. firewallem, tedy virtuální ochranou mezi sítí internet a vnitřní sítí školy.

Co je třeba zajistit

- Přístup na internet, který je realizován optickým vláknem, telefonní linkou nebo bezdrátovým spojením (nebo jejich kombinací) v odpovídající rychlosti a kvalitě.
- Na straně školy je mezi vnitřní a vnější sítí umístěn firewall, který primárně chrání vnitřní síť a zajišťuje bezpečné spojení s „vnějším světem“.
- Záložní řešení konektivity pro případ, že by došlo k výpadku přístupu k internetu (např. datové simkarty apod.).

OBLAST 1: RYCHLÁ A BEZPEČNÁ PŘÍPOJKA

Proč?

Nároky na připojení v posledních letech nebývale rostou. Jedním z požadavků poslední doby je přenos celé výuky nebo její části do virtuálního prostředí. K zamyšlení proto patří nejen současná rychlost připojení školy, ale také budoucnost rychlosti ve střednědobém horizontu. Jak ale přijít na to, jakou rychlost připojení škola potřebuje nebo bude potřebovat v budoucnu? S touto otázkou vám rádi poradí konzultanti IT guru (https://www.edu.cz/digitalizujeme/it-guru/) nebo kolegové z BCO (Broadband Competence Office, https://www.bconetwork.cz/).

Návodné otázky:

- Jakou rychlost přípojky k internetu potřebuji? Bude přípojka stačit i v horizontu 5 let a více s ohledem na plánovaný rozvoj digitální infrastruktury školy?
- Potřebuji symetrickou přípojku (stejnou rychlost stahování – download a nahrávání dat – upload)?
- Jaké služby mi poskytovatel konektivity nabízí?

Technické požadavky

Minimální požadavek

- Minimální požadavek je stanoven ve Standardu konektivity (parametr 1.2.1).

Standard konektivity škol

- Parametr 1.2.1 Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student nebo 0,5 Mbps/koncové uživatelské zařízení a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.
- Parametr 1.2.8 Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.
- Parametr 1.2.9 Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.

Doporučení nad rámec Standardu konektivity škol

- Směřovat ke kapacitě konektivity školy 1 Gb/s
- Symetrická přípojka (stejný download jako upload).
- Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.
- Antivirová kontrola internetového provozu.

Další doporučení

- Nejlepší možnou variantou je optické připojení, protože poskytuje nejvyšší rychlost připojení.
- V případě že není možné optické připojení, doporučujeme snažit se o připojení v co největší možné rychlosti, a to např. bezdrátovou profi technologií, která zajistí kvalitní spojení na co nejbližší bod páteřní sítě internetového poskytovatele. I těmito technologiemi nebývá problém se připojit rychlostmi kolem 100 Mb/s.
- V případě škol v lokalitách se sníženou dostupností připojení, je možné využít běžných tarifů od internetových poskytovatelů, využití telefonních linek, které již také dosahují dostatečných kapacit.

- Pokud nevíte, jakou rychlost přípojky zvolit, obraťte se na konzultanty IT guru (https://www.edu.cz/digitalizujeme/it-guru/).
- Pokud si nevíte rady, jaké máte možnosti přípojek ve svém území, spojte se se svým zřizovatelem nebo koordinátorem Broadband Competence Office (BCO, viz https://bconetwork.cz/).
- Metodické materiály a další informace k vnější konektivitě naleznete na stránkách BCO https://bconetwork.cz/.

OBLAST 2: FIREWALL

Proč?

Koncová zařízení a síťové prvky se dostávají do kontaktu s vnější sítí – internetem, a právě odtud hrozí naprostá většina rizik. Firewall je virtuální ochrannou zdí školy před tímto vnějším světem.

Návodné otázky:

- Potřebuji firewall?
- Co vůbec firewall dělá?

Potřebuji firewall?

- Ano, firewall je nutný na všech typech škol, které využívají připojení k internetu[3].

Firewall – co dělá?

- Firewall je prostředníkem mezi vnějším světem a sítí školy.
- Správně nastavený firewall neumožní neoprávněný vstup do školní sítě a umožní bezproblémový přístup školní sítě k internetu.
- Firewall propustí do vnitřní sítě školy pouze oprávněný provoz a neoprávněné aktivity zastaví.
- Firewall na základě pravidel filtruje provoz (přístup) do jednotlivých částí sítě školy.

3 Tato zařízení jsou škálovatelná dle požadavků školy a jsou jednoduchá na pořízení.

Technické požadavky

Minimální požadavek

- Pořídit a správně nastavit firewall tak, aby nebyl umožněn neoprávněný vstup do školní sítě a zároveň byl zajištěn bezpečný vstup do sítě Internet.
- Firewall je správně nastaven tak, aby jednotlivé skupiny uživatelů měly přístup do určité části sítě.
- Firewall je pravidelně/automaticky rekonfigurován na základě zaznamenaných útoků.

Standard konektivity škol

- Parametr 1.2.5: Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.

OBLAST 3: IPV ADRESA

Proč?

Veřejná IP adresa školy slouží k jednoznačné identifikaci lokální sítě školy v rámci internetu. V současné době je nejrozšířenější IPv4, z důvodu nedostatku adres je IPv4 postupně nahrazován protokolem IPv6. Veřejná IP adresa je pro školu důležitá z těchto důvodů:

- Umožňuje IT správci vzdálený monitoring IT infrastruktury, připojení na jednotlivé prvky (routery, servery apod.)
- Umožňuje zaměstnancům organizace bezpečné připojení do školní sítě zvenku. V případě více budov umožňuje bezpečné propojení a rozšíření vnitřní sítě mezi oddělenými pracovišti.
- Umožňuje přístup k online systémům školy hostovaných na vlastním hardwaru (např. školský informační systém, stravovací systém apod.)

Návodné otázky

- Nabízí váš poskytovatel internetu minimálně jednu veřejnou IP adresu v rámci tarifu?

Technické požadavky

Minimální požadavek

- Minimální požadavek je definován Standardem konektivity škol (parametr 1.2.2).

Standard konektivity škol

Parametr 1.2.2: Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.

Doporučení nad rámec Standardu konektivity škol

Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.

OBLAST 4: ZABEZPEČENÍ VNĚJŠÍ SÍTĚ, ŠIFROVÁNÍ

Proč?

Nepřetržité připojení školy k internetu má za následek její vystavení nehostinnému prostředí a rychle se vyvíjejícím hrozbám. Zaměstnanci a žáci mohou navíc svými činy, ať už úmyslně nebo neúmyslně, interní síť ohrozit, proto je zabezpečení jednou z klíčových činností k ochraně dat organizace. Pro bližší informace k tematice doporučujeme pročíst materiál Bezpečná digitální infrastruktura školy.

Návodné otázky

Jakým způsobem je síť školy zabezpečena proti vnějším hrozbám a úniku dat?

Dochází k pravidelnému monitorování síťového provozu a vyhodnocování anomálií?

Je škola schopna včas identifikovat a zaznamenat kybernetické útoky?

Technické požadavky

Minimální požadavek

Minimální požadavek je definován Standardem konektivity škol (parametry níže).

Standard konektivity škol

Parametr 1.2.3 Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.

Parametr 1.2.4 Síťové zařízení podporující rate limiting, antispoofing, access listy – zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.

Parametr 1.2.6 Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).

- Parametr 1.2.7 Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem.

Doporučení nad rámec Standardu konektivity škol

- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).
- Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.

VNITŘNÍ KONEKTIVITA ŠKOLY (LAN A WLAN)

V případě vnitřní konektivity řešíme zabezpečení a kvalitu digitální infrastruktury uvnitř školy, počínaje koncovými zařízeními v majetku školy nebo vlastními zařízeními zaměstnanců a žáků jako jsou počítače, notebooky nebo mobilní telefony, ale i další digitální zařízení jako routery, tiskárny, servery atd. Na těchto zařízeních nakládáme na školách s osobními údaji a dalšími citlivými daty, příkladem jsou matriční záznamy, docházkový a klasifikační systém, účetnictví nebo osobní korespondence. Tyto dokumenty jsou vystaveny nebezpečí i „ze světa“ prostřednictvím internetu, a to i když máme data uložená „pouze“ na vlastním počítači nebo tzv. vnitřní síti. Proto je nutné vnitřní IT provoz chránit a mít ho nastavený tak, aby odolal vnějším i vnitřním hrozbám. Tyto hrozby mohou být automatizované a univerzální nebo cílené a mířit na soukromá a citlivá data vás nebo vašich žáků. Následky mohou být ekonomické až likvidační, zároveň mohou narušovat soukromí zaměstnanců a žáků nebo ohrožovat vývoj a psychiku jedince. Za žádných okolností tedy nelze toto riziko podceňovat.

OBLAST 1: BEZPEČNÁ SPRÁVA KONCOVÝCH ZAŘÍZENÍ

Proč?

Uživatel přistupuje k vnitřní síti nebo internetu pomocí jednotlivých koncových zařízení (notebook, stolní počítač, tablet, mobil apod.). Z vnějšku je tak i se svým zařízením vystaven rizikům. Na druhou stranu, jakmile se připojuje k síťovým zařízením školy, působí tato koncová zařízení jako riziko. V každém případě tedy musí být zabezpečená samotná zařízení. Čím dál větší výzvou je zvládnutí správy s ohledem na vzrůstající počet těchto zařízení a různorodosti hrozeb. Řešením může být tzv. centrální řízení účtů (viz níže).

Zároveň se ve školní síti pohybují různí uživatelé, kteří by měli mít přidělená správná oprávnění. Cílem je zajistit například to, aby žáci nemohli do adresářů učitelů nebo vedení školy a učitel měl přístup do adresářů, které potřebuje k výkonu své práce, nebo aby se nestalo, že se neoprávněná osoba dostane do klasifikačního systému a provede nežádoucí úpravy. Vše musí být správně zabezpečeno a v souladu s GDPR.

Co je potřeba zařídit:

- Nastavit systém pro pravidelné aktualizace software koncových zařízení – zejména aktualizace operačního systému zařízení tak, aby byly pravidelně řešeny minimálně kritické opravy operačního systému.
- Vhodně zvolený způsob logování (přihlašování do sítě školy) tak, aby se případné incidenty daly zpětně dohledat.
- Vhodně zvolený způsob logování (přihlašování do sítě školy) tak, aby se nepovolaní uživatelé nedostali do částí sítě, které jim nepřísluší.

- Účty administrátorů a účty běžných uživatelů jsou odděleny (nelze mít účet, který používá učitel pro svou práci mezi administrátory).
- Žádný koncový uživatel (žák, pedagog, nepedagog, host) nemá na koncovém zařízení žádná administrátorská oprávnění.
- Každý uživatel má přidělenou správnou sadu oprávnění.
- Vhodně zvolená antivirová ochrana zařízení.
- Bezpečné zapojování mobilních zařízení v majetku školy, které uživatelé používají i mimo školní síť (například zapůjčené zařízení).
- V případě, že škola zvolila přístup BYOD[4], je ošetřeno bezpečné zapojení mobilních zařízení do sítě školy.
- V interní směrnici školy je ošetřeno nakládání s nepoužívanými účty a daty (např. v případě odchodu žáka či zaměstnance), zejména by mělo být specifikováno, po jaké době se účet a data po odchodu mažou/deaktivují.
- Počet anonymních účtů by měl být minimalizován, příp. eliminován.
- U všech účtů by mělo být řešeno nastavení: délky, složitosti a intervaly vypršení hesla, neopakovatelnosti hesel při změně a zamykání účtů při neúspěšných pokusech o přihlášení.
- Přístup do BIOS[5] je omezen heslem a zavedení operačního systému je umožněno pouze z pevného disku. Disk v noteboocích a PC by měl být šifrován.

Návodné otázky

- Potřebuji centrální řízení účtů? Jsme schopni zajistit aktualizaci, zabezpečení a funkčnost každého koncového zařízení ve škole ručně?
- Jaký způsob řešení centrálního řízení účtů je pro naši školu vhodnější? Univerzální cloudový balíček pro školství, serverový systém nebo kombinace?
- Je zajištěn přístup do sítě tak, aby nebylo možno zneužít administrátorský účet?
- Dostane se každý uživatel v síti jen tam, kam smí?
- Řešíme účty zaměstnanců/žáků, kteří již ve škole nejsou?

4 Z anglického Bring Your Own Device, tzn. žáci ve výuce pracují s vlastními digitálními zařízeními (např. mobilem, tabletem nebo počítačem).

5 BIOS (z angl. Basic Input/Output Setup) slouží k nastavení/detekci komponent a spolupráce základní desky s operačním systémem. Zdroj: https://it-slovnik.cz/pojem/bios/?utm_source=cp&utm_medium=link&utm_campaign=cp

Co je to centrální řízení účtů?

Důvodem pro zavedení centrální správy účtů v organizaci je snaha zvýšit bezpečnost, produktivitu a zároveň snížit náklady a opakující se úkony při správě stejných účtů v rozličných aplikacích napříč organizací. Každému uživateli v síti je umožněno přihlásit se pomocí jeho unikátního přihlašovacího jména a hesla na jakoukoliv jemu povolenou stanici či do aplikace.

Centrální řízení účtů umožňuje:

- Jednotnou správu účtů uživatelů a správců s možností nastavení konkrétních oprávnění pro přístup k systémům či jen k datům v rámci sdílených úložišť apod.
- Rozdělovat účty do skupin s různými oprávněními přístupu.
- Nastavit více-faktorovou autentizaci pro určitou skupinu účtů (doporučeno pro administrátorské účty).
- Mít přehled o jednotlivých stanicích.

Server nebo univerzální cloudové balíčky pro školství?

Centrální řízení účtů lze vyřešit dvěma způsoby, které mají své výhody a nevýhody a dají se i vzájemně kombinovat:

a) **Univerzální cloudové balíčky pro školství** (např. MS Office 365 Education nebo Google Workspace for Education[6]),
   - Pro školy jsou zdarma. Je však i tak třeba počítat se správou.
   - Škola nemusí mít v budově fyzické servery, o ty se stará poskytovatel služby.
   - Data a informace školy mohou být však reálně uložena na serverech, které jsou někdy mimo ČR nebo EU (nutno ověřit u poskytovatele služby). Je tedy vhodné zvážit i otázky ochrany osobních údajů dle GDPR.
   - Je nutné počítat s náklady spojenými s aktivací služeb a vyškolením odpovědného pracovníka.
   - Základním předpokladem pro dobrou funkčnost cloudových služeb je kvalitní konektivita.
   - Pokud se škola rozhodne využívat cloudové balíčky, tak je řádově snížen nárok na úložiště a správu serveru. Cloudový balíček může ulehčit online spolupráci v týmu a pomoci rozvíjet digitální gramotnost žáků a učitelů.
   - Poskytovatel služeb musí splňovat nároky na ochranu osobních údajů dle GDPR.

6 Více viz https://spomocnik.rvp.cz/clanek/22586/PLATFORMY-A-SYSTEMY-PRO-SKOLNI-KOMUNIKACI-A-SPOLUPRACI.html

b) Vlastní serverové prostředí

- Data a informace školy jsou uloženy na serveru, který se fyzicky nachází v budově školy.
- O server se musí starat kompetentní personál, zejména je třeba zajistit:
  - Musí být umístěn na čistém, nejlépe bezprašném místě, kde se nebude přehřívat (nejlepší je klimatizovaná místnost).
  - Musí být uložen na bezpečném místě, ke kterému má přístup jen omezený počet lidí.
  - Pokud není umístěn v rozvaděči (racku), nesmí existovat překážky před ventilačními otvory.
  - Je doporučen minimálně jeden server pro doménový řadič[7], který zvládne běh nejméně jednoho virtuálního stroje[8] (virtualizován může být například email, školní informační systém apod.). Server musí mít minimálně dva zrcadlené disky.
  - Data serveru je nutné pravidelně zálohovat.
  - Doporučeno zvážit druhý záložní server pro případ vyřazení prvního serveru z provozu.

Technické požadavky

Minimální požadavek

V případě, že má škola správce, který zvládne pravidelně aktualizovat a spravovat koncová zařízení ručně, je možné v závislosti na charakteristice školy fungovat bez centrálního řízení účtů. Centrální řízení účtů je však doporučeno (viz výše).

- Pozn.: Ruční správa vyžaduje pravidelnou činnost na týdenní bázi v závislosti na charakteristice činnosti školy.

Standard konektivity škol

Parametr 2.2.1 Systém správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).

7 Doménový řadič (Active Direcotry) zajišťuje v počítačové síti autentizaci a autorizaci uživatelů, počítačů i další služby. Řadič domény výrazně ulehčuje administraci počítačové sítě. Dalo by se říci, že pro administrátora je při větším počtu koncových zařízení nezbytná, viz: https://cs.wikipedia.org/wiki/Active_Directory

8 Virtuální stroj je v informatice software, který vytváří virtualizované prostředí mezi platformou počítače a operačním systémem, ve kterém koncový uživatel může provozovat software na abstraktním stroji. Zjednodušeně řešeno, je to virtuální počítač běžící v jiném počítači (server). Virtuálních strojů může na serveru běžet více, záleží na tom, jak je server dimenzován. Virtualizované stroje se poté při poruchách jednodušeji přenáší na jiné servery a virtualizace odděluje jednotlivé služby, ke kterým lze potom přistupovat jednotlivě a nastavovat pro každé jednoduše vlastní zabezpečení. Důležitá je také záloha virtuálních strojů.

- Parametr 2.2.2 Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém.

Doporučení nad rámec Standardu konektivity škol

- Podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].
- Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.
- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktivní zapojení do federovaného systému www.eduroam.cz)).
- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).
- Zavedení více-faktorové autentizace.
- Podpora vzdáleného přístupu (VPN).
- Nástroje pro centrální správu a audit ICT prostředků.
- Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).

OBLAST 2: BEZPEČNÉ UKLÁDÁNÍ A SPRÁVA DAT ŠKOLY

Proč?

Jak bylo řečeno, ve školním prostředí pracujeme často s citlivými daty, při jejichž zneužití hrozí až fatální následky a nemalé náklady. Podobnou hrozbou je ztráta těchto dat, a proto je potřeba je vždy zálohovat. Doporučuje se aplikovat pravidlo 3 – 2 – 1 (Vytvoření nejméně tří kopií dat – Uložení kopie na nejméně dva typy médií – Udržování alespoň jedné kopie zálohy mimo pracoviště).

Při práci s daty také musíme dodržovat platné zákony a nařízení, zejména týkající se ochrany osobních údajů, nebo vnitřní předpisy. Více informací k této problematice najdete v publikaci Bezpečná digitální infrastruktura školy.

Co je třeba zařídit:

- Bezpečné uložení dat žáků a zaměstnanců školy tak, aby nedošlo k jejich úniku nebo zneužití.
- Uchovávání pouze takových dat, které je v souladu s pravidly pro ochranu osobních údajů dle GDPR.
- Pravidelné zálohování výše uvedených dat.
- Správné nastavení oprávnění pro čtení, ukládání a mazání dat na společných složkách/discích/prostředí.

Technické požadavky

Minimální požadavek

- Záložní datové úložiště (NAS) je doporučené, a to pro zálohování důležitých dat a souborů a pro uložení společných dat.
- Základní datové úložiště se dvěma pevnými disky může být postačující (nutné konzultovat s odborníkem).
- Je možné využít i univerzálních cloudových balíčků (viz výše), avšak s nastavením šifrovaného ukládání a oprávnění k přístupu/úpravě jen vybraným uživatelům.

Standard konektivity škol

- Parametr 2.2.3 Systémy zálohování a obnovy dat serverové infrastruktury na externí uložiště (NAS).
- Parametr 2.2.4 Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.

OBLAST 3: PEVNÁ LAN – PŘIPOJENÍ KONCOVÝCH ZAŘÍZENÍ DO SÍTĚ ŠKOLY

Proč?

Zabezpečení koncových zařízení uživatelů (viz výše) je jen jedna stránka věci. Tato zařízení se musí bezpečně připojovat i do sítě tak, aby byla funkční a využitelná pro výuku i nepedagogickou práci. Práce s koncovými zařízeními nemá učiteli přidělávat potíže a starosti, ale má pomoci rozvíjet informatické myšlení a digitální kompetence žáků.

Pokud koncová zařízení nejsou do sítě zapojena správně, jednak nepomáhají vzdělávacím cílům a jednak může být ohroženo zařízení samotné, školní síť nebo i ostatní zařízení v síti.

Co je třeba zařídit:

I Funkční připojení koncových zařízení do sítě školy a vhodně je využívat ve výuce a při práci.

Technické požadavky

Minimální požadavek

M Aktivní prvek – switch s managementem[9] - minimálně variantu 100/1000 Mb/s.

M Minimální konektivita koncových počítačových systémů 100/1000 Mb/s fullduplex, ostatní systémy 100 Mbit/s.

Standard konektivity škol

S Parametr 2.3.1 Minimální konektivita koncových uživatelských zařízení 1000 Mb/s fullduplex.

S Parametr 2.3.2 Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex.

S Parametr 2.3.3 Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí – VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].

S Parametr 2.3.4 Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).

S Parametr 2.3.5 Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.

9 Switch – Síťový přepínač, častěji i v našem prostředí označovaný anglicky switch, je v informatice aktivní prvek v počítačové síti, který propojuje jednotlivé prvky do hvězdicové topologie. Přepínač obsahuje větší či menší množství síťových portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Jednoduše řečeno, switch je základní prvek počítačové sítě. Switche pracují na různých maximálních rychlostech 100 Mb/s, 1000 Mb/s, 10000 Mb/s a dále. V současné době bychom měli směřovat k tomu, aby port pro koncové zařízení měl rychlost 1000 Mb/s (1 Gb/s) a „páteřní trasy“ směřovat k 10000 Mb/s (10 Gb/s). Dále viz: https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%BD_p%C5%99ep%C3%ADna%C4%8D. Přídomek „s managementem“ znamená možnost upravovat nastavení přepínače pomocí příkazové řádky nebo webového rozhraní (HTTP).

Doporučení nad rámec Standardu konektivity škol

- Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.

OBLAST 4: ŘEŠENÍ BEZDRÁTOVÝCH SÍTÍ (WLAN) – WI-FI

Proč?

V současnosti se většina zařízení připojuje k síti bezdrátově pomocí Wi-Fi. Připojování školních nebo vlastních přenosných zařízení (BYOD) je stále častější. K bezdrátové síti Wi-Fi se často mohou připojovat učitelé, žáci i návštěvníci a u všech skupin existuje riziko poškození celé sítě (například zavlečením viru), ať už úmyslně nebo neúmyslně. Zároveň musí být Wi-Fi síť spolehlivá, aby se mohl internet využívat pro vzdělávací cíle. Proto je nutné, aby každá skupina uživatelů měla svoji vlastní oddělenou Wi-Fi síť. Wi-Fi ve škole by měly být správně nastaveny a spravovány. V případě incidentu by měl být jeho původce dohledatelný. Dalším důležitým parametrem je odpovídající pokrytí a kapacita dle plánovaného počtu připojených zařízení. Před budováním Wi-Fi sítě tedy doporučujeme zpracování studie proveditelnosti ze strany potenciálního dodavatele[10].

Co je třeba zařídit:

- Kvalitní a kontrolovaný přístup koncových zařízení do Wi-Fi sítí školy.
- Fyzická nepřístupnost některých zařízení (např. Wi-Fi router) běžným uživatelům.
- Dohledatelnost uživatelů v případě incidentu pomocí registrace.
- Dohledatelnost počítačových systémů v případě incidentu.
- Vytvoření více Wi-Fi sítí, tedy více SSID[11] (např. pro hosty, zaměstnance, žáky).
- Adekvátní nastavení přístupů pro skupinu uživatelů (např. žáci by neměli mít přístup do stejné Wi-Fi sítě jako pedagogové).
- Dostatečné pokrytí a kapacita Wi-Fi sítě dle plánovaného počtu zařízení. Sledování využití pokrytí a kapacity Wi-Fi sítě a reagování na případné přetížení sítě.

10 Roli při budování Wi.Fi sítě například hraje i síla zdiva.

11 Název sítě Wi-Fi, neboli SSID (Service Set Identifier), je název, který vaše síť používá k oznamování své přítomnosti jiným zařízením. Více viz https://cs.wikipedia.org/wiki/Wi-Fi.

Návodné otázky

- Kdo bezdrátovou síť Wi-Fi využívá a kde? Používá se i ve výuce?
- Je povolen přístup na síť Wi-Fi i s vlastním zařízením?
- K čemu by uživatelé Wi-Fi sítě ne/měli mít přístup?

Technické požadavky

Minimální požadavek

- V případě, že je Wi-Fi využíváno pro zařízení učitelů a pro zařízení školy přidělené žákům. Každá skupina uživatelů má vlastní síť Wi-Fi, tedy SSID (název sítě).
- Pokud je Wi-Fi používaná i pro připojení soukromých zařízení žáků a dětí (tedy koncept BYOD), musí být síť Wi-Fi pro tato zařízení oddělena od školní sítě. Připojování zařízení je logováno[12].
- Veškerý provoz u organizací spravovaných zařízení musí být zabezpečen minimálně AES šifrováním a standardem WPA2-Enterprise. Zabezpečení WPA2-PSK technologií se ve větších organizacích nedoporučuje; zabezpečení WEP technologií je nedostatečné.
- Doporučená je centralizovaná správa Wi-Fi sítě[13].

Standard konektivity škol

- Parametr 2.4.1 Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i žáků.
- Parametr 2.4.2 Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.
- Parametr 2.4.3 Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky školy a externí zařízení (hosty).
- Parametr 2.4.4 Podpora mechanismu izolace uživatelů.
- Parametr 2.4.5 Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.

12 Je třeba zajistit logování (zaznamenání dat za účelem jejich analýzy), aby byl případný útočník-škoditel dohledán.
13 Centralizovaná správa wifi sítě – software/hardware, který umožní centrální správu všech wifi zařízení. Od základního nastavení po logování provozu a dohled nad wifi sítí.

Doporučení nad rámec Standardu konektivity škol

- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.
- Centralizovaná architektura správy Wi-Fi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení).
- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému www.eduroam.cz).
- Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].

DALŠÍ ZDROJE INFORMACÍ

Bezpečná školní ICT infrastruktura – edukační videa. Edu.cz. Dostupné z: https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/

Bezpečnost – Systém podpory profesního rozvoje učitelů a ředitelů. Úvod - Systém podpory profesního rozvoje učitelů a ředitelů [online]. Dostupné z: https://www.projektsypo.cz/bezpecnost

KOPECKÝ, K., Základy počítačové bezpečnosti. Podpora kompetencí vedoucích pedagogických pracovníků při implementaci digitálních technologií do života školy/školského zařízení. [online]. Dostupné z: http://www.klus.upol.cz/wp-content/uploads/2021/02/pc_bezpecnost_kopecky.pdf

Bezpečná školní ICT infrastruktura (BEZIT). Edu.cz. Dostupné z https://www.edu.cz/bezpecna-skolni-ict-infrastruktura-bezit-jako-prevence-pred-kybernetickou-kriminalitou/**.**

Akademie CZ.NIC: https://akademie.nic.cz/

Osvětové materiály o kybernetické bezpečnosti a prevenci
https://osveta.nukib.cz/mod/page/view.php?id=1043

Portál o digitalizaci škol: https://edu.cz/digitalizujeme

Příklad auditní zprávy k digitální infrastruktuře školy: https://revize.edu.cz/files/auditni-zprava-2023-online.pdf