Digitalizace ve vzdělávání
Národní pedagogický institut ČR

Nastavení procesů

Kyber ve škole

Checklist pro vedení školy

Úvod

Zajistit bezpečné a funkční digitální prostředí ve škole není jednoduché. Škola musí dobře nastavit pravidla, mít kvalifikovaný tým, propracovanou strategii a dbát na technickou i organizační stránku věci. Tento checklist slouží jako praktická pomůcka pro vedení školy. Díky němu snadno zkontrolujete, zda máte vše potřebné pro správu digitální infrastruktury, ochranu dat, bezpečnost uživatelů i efektivní využívání technologií ve vaší škole.

Tento checklist vychází ze zkušeností odborníků na kybernetickou bezpečnost a následujících dokumentů:

- Standard konektivity škol
- Průvodce ke Standardu konektivity škol
- Bezpečná digitální infrastruktura školy
- Příručka pro ředitele k IT správě

Checklist slouží i jako rozcestník – pod podtrženými částmi textu se skrývají odkazy na dokumenty, které danou tematiku více rozebírají, například na kurzy Národního pedagogického institutu nebo přímo na vzory, které jsme pro vás připravili.

Obecné nastavení, tým a strategie

- Máme ICT koordinátora/metodika (viz Edu.gov.cz/ITsprava).
- Máme správce ICT, kterého můžeme požádat o pomoc v případě, že nám něco nefunguje (viz Edu.gov.cz/ITsprava).
- Máme k dispozici ICT experta (firmu nebo zaměstnance), který se stará o celou naši školní digitální infrastrukturu (viz Edu.gov.cz/ITsprava). Amatéři nebo samouci naši infrastrukturu nespravují.
- Nejsme závislí na jednom technikovi, jsme připraveni na jeho případný odchod.
- Máme metodika prevence.
- Máme digitální strategii školy, příp. jiný dokument (ICT plán), který definuje naše směřování.
- Máme plán reakce pro případ kybernetického incidentu.
- Splňujeme Standard konektivity.

Pravidla pro uživatele

- Máme bezpečnostní ICT směrnici, která uživatelům určuje pravidla pro chování na internetu.
- Uživatelé nepoužívají pro soukromé účely pracovní účty a obráceně.
- Uživatelé používají silná hesla. Hesla se nelepí na obrazovku.
- Používáme vícefaktorové ověřování všude tam, kde je to možné. Minimálně u administrátorských účtů a ideálně také u zaměstnaneckých účtů.
- Účty administrátorů a účty běžných uživatelů jsou odděleny (nelze mít účet, který používá učitel pro svou práci, mezi administrátorskými účty).
- Uživatelé se automaticky odhlašují při odchodu od zařízení.

Vnitřní síť, wi-fi, aktualizace

- Máme funkční a pravidelně aktualizovaný firewall.
- Software, aplikace a operační systémy na všech zařízeních pravidelně aktualizujeme.
- Vnitřní síť je správně šifrovaná (viz Standard konektivity).
- Vnitřní síť je segmentovaná – např. administrátorská, žákovská, učitelská, pro síťové prvky.
- Antivirovou ochranu sítě pravidelně aktualizujeme s aktuální databází malwaru.
- Wi-fi sítě pro učitele (příp. administrátory), žáky a hosty jsou oddělené.
- Vstup do wi-fi sítě je kontrolovaný a dohledatelný.
- Routery a další síťové prvky jsou mimo fyzický dosah uživatelů.

Zařízení uživatelů a účty

- Anonymní účty jsou zakázány (neexistuje jeden účet pro všechny).
- Všichni uživatelé mají své uživatelské účty, které jsou centrálně spravovány.
- Správně zařízení evidujeme, abychom měli přehled, kde se nacházejí a v jakém jsou stavu.
- Žádný uživatel (žák, pedagog, nepedagog, host) nemá na zařízení žádná administrátorská oprávnění.
- Každý uživatel má přidělenou správnou sadu oprávnění.
- Antivirová ochrana zařízení je pravidelně aktualizována.
- Opětovné zapojení zařízení, které se používá mimo školu, je bezpečné.
- V případě, že škola zvolila přístup BYOD, je ošetřeno bezpečné zapojení mobilních zařízení do sítě školy.
- Bezpečnostní ICT směrnice školy ošetřuje nakládání s nepoužívanými účty a daty (např. v případě odchodu žáka či zaměstnance), zejména specifikuje, po jaké době se účet a data po odchodu mažou/deaktivují.
- Všechny účty mají nastavenou délku a složitost hesla a intervaly pro změnu hesla a zamykání účtů při neúspěšných pokusech o přihlášení.
- Přístup do BIOS je omezen heslem a operační systém je možné zavést pouze z pevného disku.
- Disk v noteboocích a PC je šifrován.
- Cizí USB disky jsou zakázány nebo musí před vložením proběhnout jejich kontrola.

Server a zálohování

- O server se správně staráme – je na bezpečném, větraném a suchém místě (viz Průvodce ke Standardu konektivity).
- Jsou nastavené automatizované denní zálohy klíčových dokumentů a dat.
- Při zálohování aplikujeme pravidlo 3-2-1 (vytvoření nejméně tří kopií dat – uložení kopie na nejméně dva typy médií – udržování alespoň jedné kopie zálohy mimo pracoviště).
- Máme plán pro obnovu dat v případě útoku a seznam osob, které nám s tím pomohou.
- Pravidelně testujeme, zda zálohování i obnova fungují (min. jednou ročně).

Školení, osvěta, vzdělávání

- Všichni uživatelé jsou pravidelně (min. jednou ročně) proškolováni ohledně bezpečných hesel, ochrany proti phishingu a dalších metod podvodů a na téma digitální stopy a umělé inteligence. Ke školení mohou sloužit například kurzy NPI nebo e-kurz Dávej kyber! pro učitele na osveta.nukib.cz.
- Pravidelně organizujeme testovací phishingové kampaně (detekce zranitelností).
- Kyberbezpečnost i kyberprevence je součástí našeho ŠVP dle aktualizovaného RVP.

Komunikace a ochrana osobních údajů

- Dodržujeme GDPR, uchováváme jen taková data, která dle zákona můžeme mít.
- Sociální sítě školy spravují pouze určení zaměstnanci, pro publikaci si stanoví pravidla.
- Pro komunikaci s rodiči i žáky máme oficiální jednotný kanál (školní informační systém, LMS).
- Pro interní komunikaci ve škole používáme také oficiální jednotný kanál (školní informační systém, interní komunikační systém).
- Učitelé nevytvářejí neoficiální komunikační kanály s žáky ani rodiči (facebookové skupiny, WhatsApp skupiny aj.).
- Pečlivě zvažujeme, které fotografie sdílíme a přes jaké kanály.
- Uživatelé využívají AI nástroje s rozumem – nevkládají do nich žádné osobní a citlivé údaje ani fotografie žáků.