Plánování zabezpečení školní ICT infrastruktury, bezpečnostní audit

# anotace

Proč je zabezpečení školní ICT infrastruktury tak důležité a proč je stále tato oblast spíše přehlížená? Bezpečná a kvalitní ICT infrastruktura se se stává v souvislosti s neustále rostoucím přílivem technologií do škol stále důležitější. Statisticky se blížíme k poměru 1 počítač či tablet na jednoho studenta. Školská zařízení začínají v současnosti stále častěji využívat digitální zdroje (digitální obsah, digitální nástroje, digitální hodnocení, administrativní aplikace apod.). To způsobuje, že se ve školských institucích, respektive v jejich datových a cloudových úložištích začíná shromažďovat mnohem více dat, informací a zdrojů, než tomu bylo v letech minulých. Tento nárůst s sebou nese odpovědnost pro školská zařízení zajistit, aby tyto digitální zdroje a prostředí byly bezpečné. Častější využívání moderních digitálních technologií a digitálních zdrojů přináší také větší rizika, na která je třeba být připraven. Jedním z nezbytných kroků, které je třeba pro zvýšení bezpečnosti ICT infrastruktury ve školských zařízeních udělat, je provedení bezpečnostního auditu. K tomu může dobře posloužit následující bezpečnostní checklist, podle kterého mohou ředitelé škol či školní správci sítí provést vyhodnocení úrovně bezpečnosti své ICT infrastruktury a dle výsledků učinit nezbytná opatření, která povedou ke zvýšení bezpečnosti a nastavení kvalitních bezpečnostních politik.

# Bezpečnostní checklist

Je důležité zavádět bezpečnostní politiky, které jsou nastaveny tak, aby co nejvíce chránily školní ICT prostředí a důležité zdroje před neoprávněnými přístupy. Tento bezpečnostní checklist je navržen tak, aby pomohl rychlé orientaci ve školním ICT prostředí a rychlému vyhodnocení zabezpečení školní ICT infrastruktury. Výsledné informace by měly vést k tomu, aby odhalené nedostatky byly co nejdříve odstraněny.

Checklist obsahuje čtyři klíčové oblasti pro nastavování bezpečnostních politik ve školských zařízeních. Otázky v checklistu jsou formulovány tak, aby na ně mohl respondent odpovědět pouze třemi možnými způsoby:

1. Ano
2. Částečně
3. Ne.

Účelem bezpečnostního auditu je odhalení a identifikace slabých míst v ICT infrastruktuře, která by mohla být zneužita ke kybernetickým útokům.

## oblast 1 - Plánování bezpečnostních politik

* **Má školské zařízení sestavený zvláštní tým pro nastavování bezpečnostních politik, který by měl být složen z následujících zástupců?**
* Zástupce vedení školy
* Zástupce z řad pedagogů
* ICT správce / odborník
* Právník
* Zástupce externích poskytovatelů služeb
* **Má školské zařízení vytvořený plán zvládání rizik? Plán by měl obsahovat následující segmenty:**
* Popis rolí a odpovědnosti členů týmu
* Seznam důležitých kontaktů, na které je možné se obrátit v případě ohrožení
* Identifikace možných rizik
* Soupis odpovídajících strategií zmírňujících rizika ohrožení
* Jasná komunikační pravidla a postupy, které určují, co je komu třeba sdělit a v jakém časovém rámci
* Plán kontinuálního vzdělávání pedagogů v oblasti kybernetické bezpečnosti

## oblast 2 - Prosazování bezpečnostní politiky

* **Má školské zařízení jasně definovanou bezpečnostní politiku, se kterou byli seznámeni všichni uživatelé ICT ve školských zařízeních (pedagogové, žáci, studenti, ostatní zaměstnanci školských zařízeních)? V případě využívání outsourcingových služeb i vně školská zařízení?**
* **Je v bezpečnostní politice jasně definováno následující?**
* Kdo má a nemá přístup k síti a za jakých podmínek
* Definice zakázaných činností v ICT infrastruktuře
* Informace o monitorování pohybu v ICT prostředí
* Důsledky při porušování nastavených pravidel
* Zveřejnění osoby zodpovědné za prosazování bezpečnostní politiky
* Kontaktní informace pro hlášení škodlivých a podezřelých aktivit
* Zásady vzdáleného přístupu
* Pokyny pro vyžádání, schválení a odmítnutí vzdáleného přístupu

## oblast 3 – Komunikace a profesní rozvoj v oblasti bezpečnostních politik

* **Zajišťuje školské zařízení dostatečným způsobem vzdělávání pedagogů, žáků, studentů, dalších zaměstnanců, rodičů v oblasti bezpečného používání moderních digitálních technologií a bezpečnostních politik? Poskytuje školské zařízení následující možnosti?**
* Další profesní vzdělávání pedagogů
* Osobní konzultace pro veřejnost
* Webináře, online kurzy
* Besedy, přednášky, projektové dny
* Poskytuje školské zařízení všem uživatelům dostatečné množství rad a doporučení pro správnou etiku v ICT prostředí? Tato doporučení by měla být dostupná i online a obsahovat zejména:
* Informace o dostatečné ochraně svého hesla
* Doporučení používat alfanumerická hesla o délce nejméně 12 znaků
* Vždy se odhlašovat z pracovního/žákovského PC
* Nepřihlašovat se do více než jedné stanice na jednou
* Neotvírat žádné přílohy, které uživatel nezná
* Neotvírat žádné přílohy s příponou EXE
* Nereagovat na emaily vyžadující sdělení citlivých/ soukromých údajů
* Jakékoliv podezřelé aktivity, e-maily, vždy oznámit

## oblast 4 – Bezpečné nastavení ICT infrastruktury / Best practices

* **Provádí školské zařízení pravidelné hodnocení bezpečnosti ICT infrastruktury a pravidelnou kontrolu a identifikaci každého zařízení v rámci školního ICT prostředí?**
* **Je věnována dostatečná pozornost zejména těmto oblastem?**

**A) brána firewall**

* Jsou nainstalovány nejnovější aktualizace?
* Jsou aktivovány účinné filtry, které jsou v souladu s bezpečnostní politikou?
* Jsou nevyužité porty a protokoly blokovány?
* Je IPsec nakonfigurován pro šifrovanou komunikaci v obvodové síti?
* Jsou využívány autentizace a autorizace uživatelských účtů?
* Jsou aktivovány systémy detekce a prevence narušení?

**B) router/směrovač**

* Jsou nainstalovány nejnovější aktualizace?
* Jsou přiřazeny statické IP adresy?
* Používají se pouze zabezpečené směrovací protokoly, které používají ověřování?
* Je využívána nejbezpečnější metoda vzdáleného přístupu, obvykle SSH (Secure Shell)?
* Je vypnut Telnet a další nebezpečné metody vzdáleného přístupu?
* Jsou velké ping pakety screenovány?
* Je omezen vzdálený přístup pouze na známá a prověřená zařízení?
* Jsou pro vzdálená i místní připojení používána dostatečně silná hesla?

**C) bezdrátové síťové zařízení**

* Je pro ověření vstupu do bezdrátové sítě využíván protokol IEEE 802.11, ke kterému se mohou připojit pouze schválené přístroje?
* Jsou využívány nejsilnější šifrovací metody, zejména WPA2 a WPA3?
* Je ve veřejné síti povoleno připojení pouze k internetu, nikoliv k interním datům?

# Legenda k vyhodnocení bezpečnostního auditu

**Převažuje odpověď ANO.**

Úroveň bezpečnosti Vašeho ICT prostředí je vysoká, nicméně něco jako 100% ochrana neexistuje a z tohoto důvodu je nutné neustále své ICT prostředí monitorovat, aktualizovat a připravovat na nové hrozby.

**Převažuje odpověď ČÁSTEČNĚ.**

Vaše bezpečnostní politika je vedena správným směrem, nicméně některým oblastem bude nutné věnovat větší a důkladnější pozornost, to je totiž jediný způsob, jak zvýšit úroveň vašeho zabezpečení. Sestavení kvalitního plánu zvládání rizik by mělo být Vaším prvním krokem ke zvýšení bezpečnosti.

**Převažuje odpověď NE.**

Vaše ICT prostředí ve vztahu k nízké úrovni zabezpečení může být kdykoliv snadným cílem kybernetických útoků. Prvním a velice důležitým krokem pro Vás bude sestavení odborného týmu, který se otázkou nastavování bezpečnostních politik bude intenzivně zabývat a prvním úkolem tohoto týmu bude identifikace možných rizik a zavádění odpovídajících strategií zmírňující rizika ohrožení.