MINIMÁLNÍ BEZPEČNOSTNÍ STANDARDY PRO VÝUKU NA DÁLKU

aneb bezpečná digitalizace českého školství

Minimální bezpečnostní standardy pro výuku na dálku

autor: Mgr. Tomáš Hamberger

anotace: S ohledem na stále rostoucí počet účastníků distančního vzdělávání a s ohledem na rostoucí množství nově vznikajícího digitálního obsahu je nutné pro všechny tyto aktivity definovat minimální bezpečnostní standardy, prostřednictvím kterých bude zajištěno bezpečné vzdělávací prostředí pro všechny účastníky, tedy jak pro pedagogy, tak i pro žáky a studenty. Dále bude nezbytné, jasně definovat kybernetická rizika a hrozby, která mohou nastat v souvislosti s distančním vzděláváním. Mezi nejčastější rizika a hrozby v rámci distančního vzdělávání můžeme zařadit zneužití osobních údajů, zneužití a prolomení hesla a podobných přístupových údajů, odcizení a zneužití autorského obsahu, narušování a trolling[1] virtuálních tříd nebo videokonferenčních setkání. Většina kybernetických útoků je vedena samotnými žáky, kteří zneužívají nízké digitální gramotnosti některých pedagogů. Je nezbytné, aby bylo všem pedagogům umožněno prohlubovat své dovednosti a znalosti nejen ve smyslu používání moderních technologií a vzdělávacích platforem, ale i ve smyslu minimalizace kybernetických hrozeb s těmito technologiemi a platformami spojených. Většina výrobců a poskytovatelů těchto moderních digitálních technologií a vzdělávacích a výukových platforem využila zkušeností z první vlny distančního vzdělávání a své technologie a vzdělávací platformy vybavila velkým množstvím bezpečnostních prvků, které uživatelům slouží především k minimalizaci kybernetických rizik. Běžně lze již tedy vytvářet předsálí k videokonferencím, aniž by docházelo k samovolnému a nekontrolovanému vstupu do videokonferenčních místností, lze již účastníkům vypínat mikrofon nebo je lze zcela vyloučit z videokonferenční místnosti a tak dále. Nejdůležitější ovšem je, aby o těchto funkcích a možnostech byli dostatečně poučení pedagogové. A právě přispět k informovanosti pedagogů v rámci této problematiky si klade za cíl tato metodika k bezpečnostním standardům pro výuku na dálku. Tyto bezpečnostní standardy pro výuku na dálku se zaměřují na nejčastěji využívané technologie a digitální platformy v českém regionálním školství v rámci distančního vzdělávání.

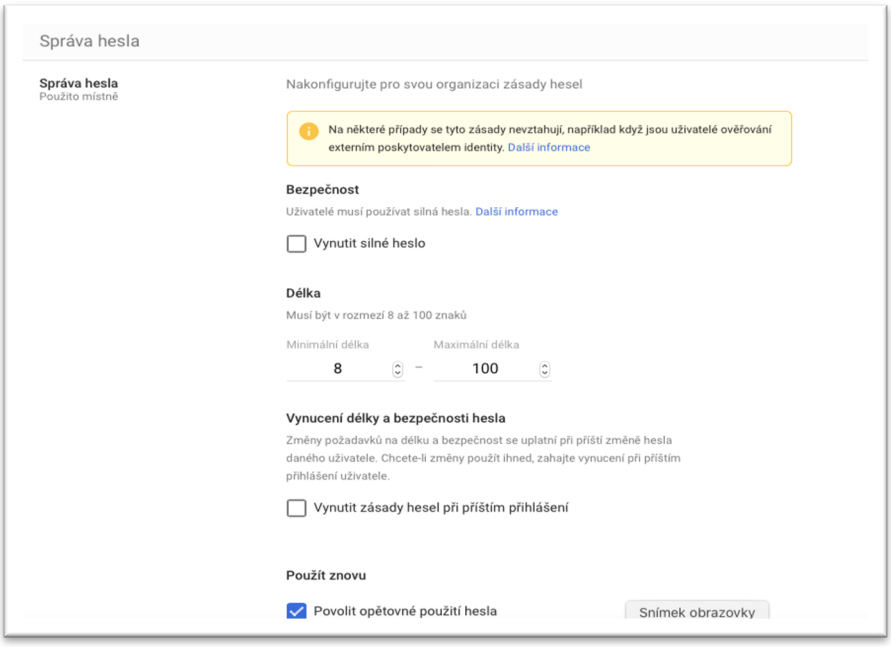
[1] Trolling dostupné z: https://cs.wikipedia.org/wiki/Troll_(internet)

Google Suite, rizika a bezpečnostní prvky: mezi nejpoužívanější aplikace této digitální vzdělávací platformy patří Gmail, Google Disk, Google Meet a Google učebna. Předností této platformy je neomezené cloudové úložiště, které hostuje uživatelská data v síti serveroven patřící přímo společnosti Google. Další nesporná výhoda je, že dostupnost většiny aplikací je pro účely vzdělávání bez poplatků, tedy zdarma. Nedílnou součástí této platformy jsou také funkce pro blokování spamu, antivirovou kontrolu a prověření dokumentů, jež testují data ještě předtím, než si uživatel stáhne příslušnou zprávu.

Rizika:

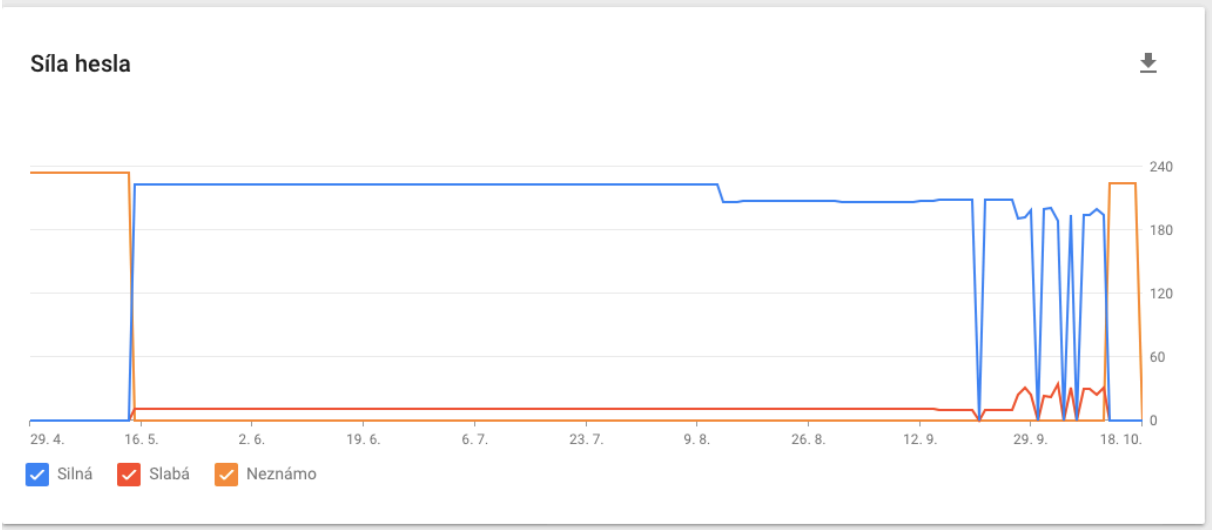
1. Zneužití, prolomení hesla k uživatelskému účtu: bezpečnostní pravidla Google Suite vyzívají každého uživatele ke zvolení dostatečně silného hesla o minimálně 8 znacích, avšak doporučení této metodiky je heslo o minimálně 12 znacích. Platforma Google Suite se rozděluje na uživatelská a administrátorská oprávnění, a právě v rámci administrátorských oprávnění lze dohlížet na kvalitu hesel a umožňuje administrátorovi s touto bezpečnostní politikou efektivně pracovat. Administrátor školní domény Google Suite tak může nastavovat různou úroveň bezpečnostních prvků, například si může na uživatelích vynutit vyšší minimální počet znaků u hesel, může povolit či zakázat opětovné použití hesla (viz recyklace hesla), může nastavit platnost hesla od 30 dnů až po neomezenou platnost. Viz obrázek číslo 1.

obr.č.1



Je umožněno také uživatelům nastavit dvoufázové ověřování při přihlašování k uživatelskému účtu. Administrátor platformy Google Suite má také k dispozici pravidelné přehledy o úrovni bezpečnosti dané platformy, tyto přehledy přinášejí také informace o úrovni síly hesel uživatelů dané platformy. Viz obrázek 2.

Obr.č.2



Obecně ale stále platí, že zásadní odpovědnost v rámci prevence kybernetických hrozeb je na každém jednotlivém uživateli. Žádný bezpečnostní a vynucovací prvek totiž nezajistí to, že například žák své heslo nesdělí jinému žákovi, který toho posléze může zneužít.

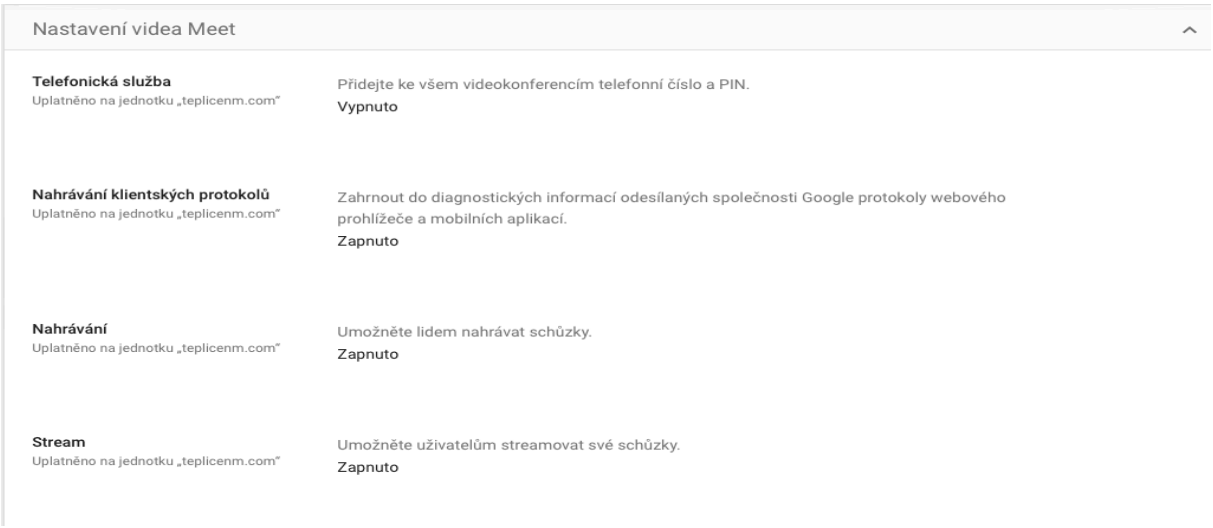
2. Narušování a trolling videokonferenčních setkání:

Nastavení kvalitní bezpečností politiky videokonferenčních setkání lze opět rozdělit do dvou úrovní. Do úrovně uživatelské a úrovně administrátorské. V rámci administrátorských oprávnění doporučuji nastavit následující opatření pro videokonferenční setkání:

- vypněte telefonickou službu, tak aby uživatelé neviděli telefonní číslo jako další možnost přihlášení ke schůzce,
- vypněte žákům/studentům možnost nahrávat schůzky,
- vypněte žákům/studentům možnost streamovat své schůzky. Viz obrázek 3.

V rámci své školní platformy můžete také žákům/studentům zakázat uskutečňovat videohovory a hlasová volání.

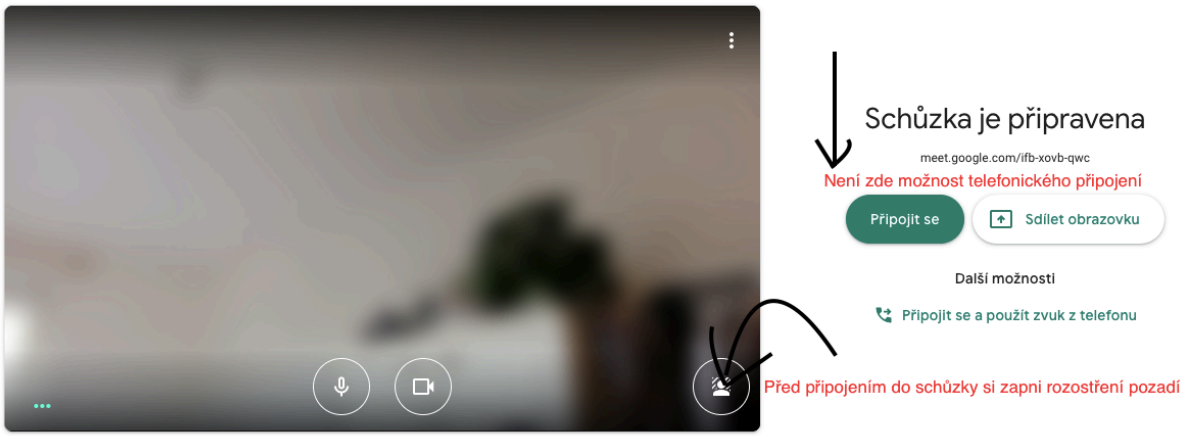
obr.č. 3



Na úrovni uživatelských oprávnění a funkcí doporučuji používat následující:

- před připojením do schůzky si rozostřete své pozadí, doporučuji i u žáků, jelikož tím můžeme minimalizovat výskyt kyberšikany. Běžně se stává, že jsou někteří žáci vystaveni posměškům a urážkám od ostatních účastníků videokonferenční schůzky. Děje se tak, že lze vidět v jakých sociálních podmínkách někteří žáci žijí, jaké mají podmínky pro výuku z domova apod. Tím, že použijeme funkci rozostření pracovního pozadí, tak eliminujeme vznik této formy kyberšikany. Viz obrázek 4.

obr.č. 4

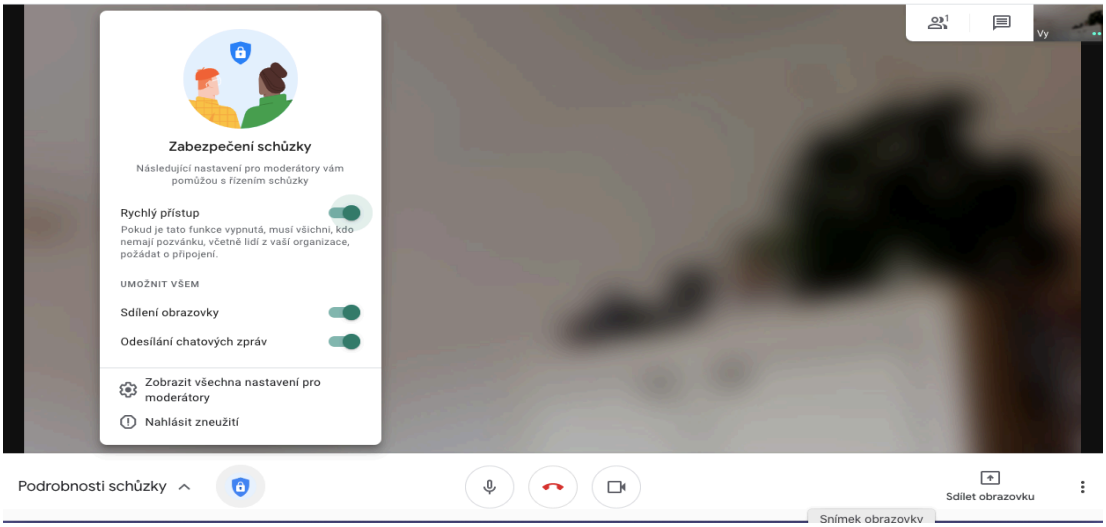


V samotné videokonferenční místnosti má pak její správce/zakladatel k dispozici další bezpečnostní prvky. Nutno zmínit, že k plnému využívání, nejen bezpečnostních prvků, doporučuji pracovat v internetovém prohlížeči Google Chrome. Nově tedy nalezneme

v aplikaci Google Meet ikonu zámečku. Po kliknutí na ikonu zámečku se správci objeví další bezpečnostní prvky, mezi které patří:

- povolení/zákaz rychlého přístupu, v případě zákazu rychlého přístupu do videokonferenční místnosti musí všichni, kdo nemají pozvánku k videokonferenci požádat o připojení, lze tímto minimalizovat připojování cizích účastníků k videokonferencím,
- dále lze účastníkům zakázat/povolit sdílení své obrazovky, tímto lze předejít ke sdílení nevhodného obsahu,
- lze také zakázat/povolit zasílání chatových zpráv, které mohou odvádět pozornost žáků/studentů od výuky. Viz obrázek 5.

obr.č.5

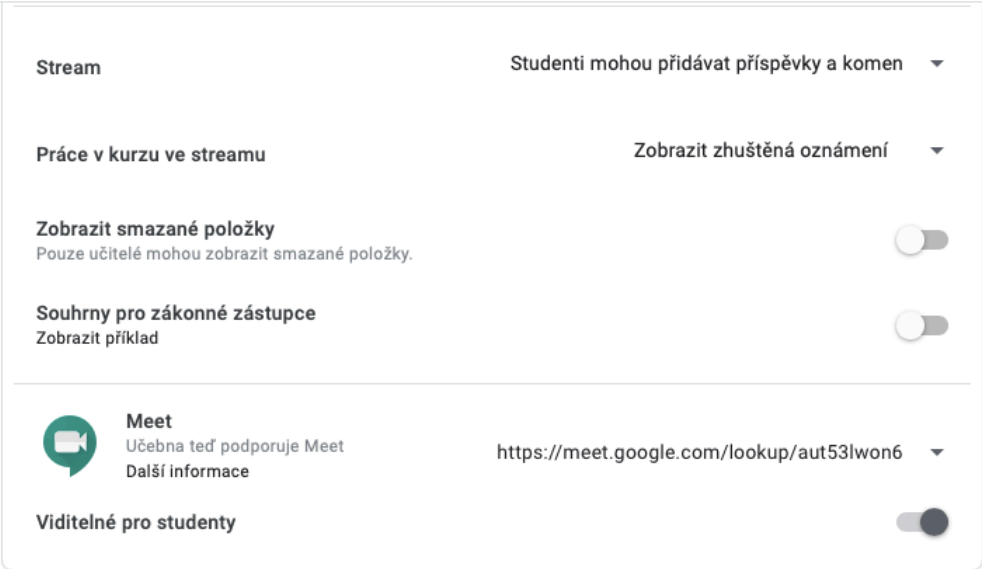


Dalšími bezpečnostními prvky aplikace Google Meet, které můžeme využít k minimalizaci kybernetických hrozeb jsou možnosti ztlumit účastníka schůzky nebo odebrat účastníka ze schůzky a tím mu znemožnit opětovné připojení. K těmto opatřením by pedagogové měli přistoupit pouze v případech hrubého a opakovaného narušování videokonferenčních schůzek žáky/studenty.

3. Zneužití sdílených dokumentů a dokumentů v Google Učebně: jakýkoliv uživatel, který vytvoří dokument v rámci platformy Google Suite se automaticky stává jeho vlastníkem a záleží pouze na něm, jaký rozsah oprávnění poskytne ostatním uživatelům. Pokud pedagog chce, aby jeho dokument mohli žáci upravovat a měnit, poskytne jim oprávnění editora v opačném případě jim udělí roli čtenáře, což žákům/studentům nedovolí cokoliv v dokumentu změnit, vymazat nebo zneužít. Obecně platí, pokud jakýkoliv dokument nesdílíte s ostatními, nikdo jiný s e k němu nedostane. To samé platí i pro Google Učebnu,

prostřednictvím které například žáci/studenti odevzdávají své domácí práce a projekty. Žáci/studenti mezi sebou své práce, hodnocení apod. nevidí a nemohou tedy nic a nikomu změnit, zneužít nebo vymazat. Google učebna vytváří prostor i pro online setkávání žáků/studentů se svými učiteli. Žáci/studenti se mohou z Google Učebny připojit k videokonferenční místnosti, která je vytvořená pro každou Google učebnu. Riziko zde spočívá v tom, že se zde žáci/studenti mohou sházet i mimo vyučování, což by někomu nemuselo vadit, ale kdo chce mít absolutní přehled nad děním v rámci platformy Google Učebna, lze využít funkci, při které lze dočasně skrýt možnosti připojení do Google Meet dokud to opět nezviditelní správce Google učebny. To většinou udělá pedagog se začátkem distanční výuky. Funkci nalezneme v nastavení každého jednotlivého kurzu v rámci Google Učebny. Viz obrázek 6.

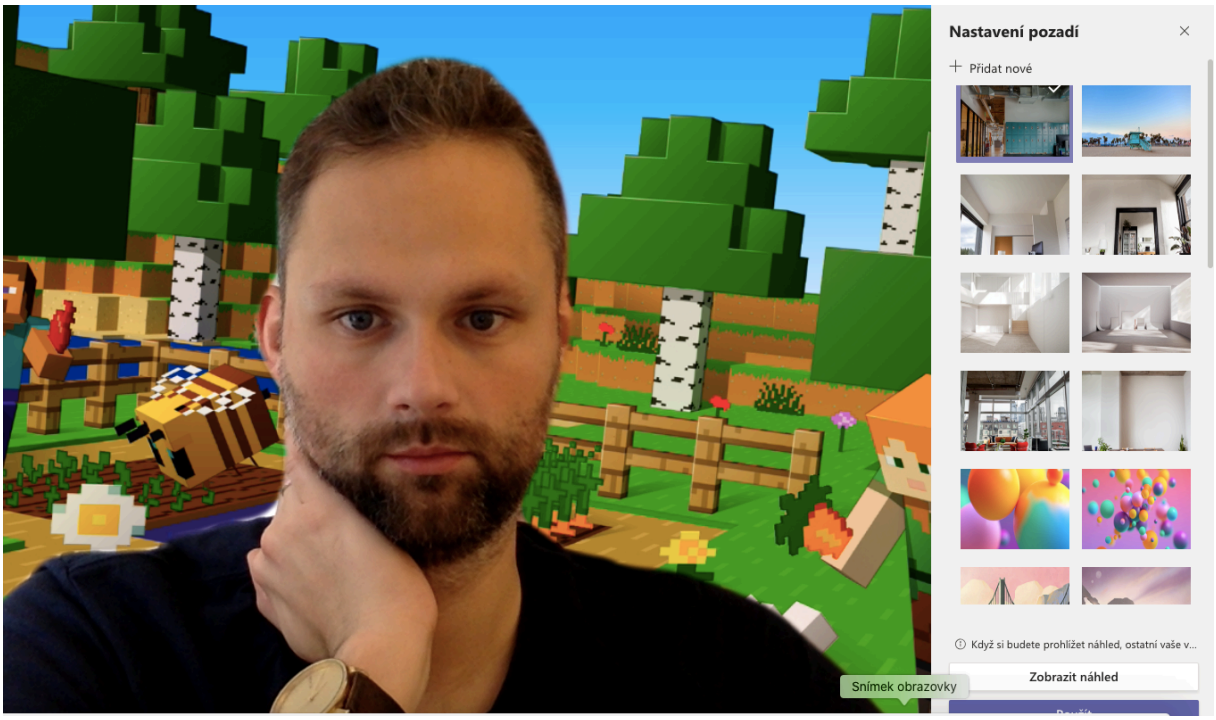
obr.č.6



Microsoft 365, rizika a bezpečnostní prvky: tento poskytovatel především cloudových služeb a kancelářského softwaru je stejně, jako v případě Google Suite, pro účely vzdělávání zcela zdarma. Platforma nabízí totožné aplikace jako Google Siute, které se liší pouze názvem. Principy, možnosti a funkce jsou podobné a tím pádem jsou podobná i kybernetická rizika. Nejčastěji používanou aplikací MS 365 v rámci distančního vzdělávání je MS Teams, který podobně jako Google Meet umožňuje uživatelům textovou komunikaci, video hovory, ukládání souborů a integraci dalších aplikací do tohoto prostředí. MS Teams umožňuje pedagogům distribuovat a klasifikovat žákům/studentům jejich domácí práce a projekty podobně jako Google Učebna. Není tedy nutné opakovat všechna rizika, jelikož jsou totožná

jako pro platformu Google Suite. Upozorníme ale i zde na riziko vzniku kyberšikany v rámci video hovorů prostřednictvím aplikace MS Teams. Riziko lze i v případě této platformy minimalizovat aktivováním funkce zobrazit efekty pozadí, kdy máme možnost nastavit tapetu pozadí pro video hovory, abychom zvýšili ochranu svého soukromí při zachování zapnutí webové kamery. Viz obrázek 7.

obr. č. 7



Ve vztahu k těmto poměrně novým vzdělávacím platformám musíme ale zmínit, že neexistuje žádný bezpečnostní prvek nebo funkce, která by zajišťovala absolutní bezpečnost uživatelů. Pedagog už nemůže dohlédnout na to, jestli si jej v rámci video hovoru například žák/student nenahrává na mobilní telefon nebo jestli žák/student poskytne své přihlašovací údaje jiné osobě. Je tedy nutné věnovat se tomuto tématu i rámci výchovných předmětů a snažit se ve třídách nastavit zdravé klima, ve kterém nebudou chtít žáci/studenti poškodit pedagoga tím, že budou například nevhodným způsobem narušovat online vyučování.

Doplňující doporučení k MS Teams[2]. Viz obrázek 8.

Oblast zásad	Podoblast	Zásadami	Globální hodnota pro primární a sekundární studenty	Hodnota pro pedagogy
zásad týmů		Vytvoření soukromých kanálů	Vypnuto	Zapnuto
zásad schůzky	Obecné	Povolit okamžitou schůzku ve kanálech	Vypnuto	Zapnuto
		Povolení doplňku outlooku	Vypnuto	Zapnuto
		Povolithttps://docs.microsoft.com/microsoftteams/meeting-policies-in-teams#allow-channel-meeting-schedulingplánování schůzek s kanálem	Vypnuto	Zapnuto
		Povolit plánování soukromých schůzek	Vypnuto	Zapnuto
		Povolit okamžité schůzky v soukromých schůzkách	Vypnuto	Zapnuto
	Účastník a hosté	Umožněte anonymním lidem zahájit schůzku	Vypnuto	Zapnuto
		Role s právy prezentujícího na schůzkách	Všichni v organizaci, ale uživatel může přepsat	Organizátori, ale uživatelé můžou přepsat
		Automaticky připustit uživatele (zásady pro jednotlivé organizátory)	Všichni v organizaci	Pouze organizátor
	režimu videofiltry	režimu videofiltry	BlurandDefaultBackgrounds	AllFilters
Zásady dynamických událostí		Povolit plánování	Vypnuto	Zapnuto
zásad zasílání zpráv		Vlastníci můžou odstranit odeslané zprávy.	Vypnuto	Zapnuto
		Odstranění odeslaných zpráv	Vypnuto	Zapnuto
		Úpravy odeslaných zpráv	Vypnuto	Zapnuto
		Chat	Vypnuto	Zapnuto

[2] Dostupné z: https://support.microsoft.com/cs-cz/office/zajištěn%C3%AD-bezpečnosti-studentů-při-použ%C3%ADván%C3%AD-teams-pro-výuku-na-dálku-f00fa399-0473-4d31-ab72-644c137e11c8

Další rizika a hrozby v rámci školní digitální infrastruktury:

1. Útoky na nezabezpečené webové stránky provozované na internetovém protokolu http.

Řešení: Provozovat školní webové stránky na zabezpečeném protokolu HTTPS, který zajišťuje autentizaci a důvěrnost přenášených dat.

2. **Narušení standardní činnosti počítačového systému mallwarem či jiným nepřátelským softwarem.**

Řešení: Kvalitní antivirový program. Pravidelné aktualizace. Pravidelné vzdělávání pedagogů.

3. **Pokus o neautorizovaný přístup ke školní internetové síti, ke školní evidenci dat a osobních údajů, ke školním emailům.**

Řešení: Kvalitní bezpečnostní politika hesel. Pravidelné vzdělávání pedagogů.

4. **Sociální inženýrství a další podvodná jednání za účelem získaní citlivých informací nebo peněz (key-logger, podvodné faktury).**

Řešení: Pravidelné vzdělávání pedagogů.

Proces zabezpečování školní digitální infrastruktury:

1. Definovat reálná rizika a hrozby

2. Vykonat bezpečnostní audit

3. Sestavit plán zvládání rizik

Doporučené oblasti pro bezpečnostní audit:

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 14 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, emaily vždy oznámit

oblast 4 - Bezpečné nastavení digitální infrastruktury

- 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?

Plán zvládání rizik by měl zahrnovat následující segmenty:

- Popis rolí a odpovědnosti členů týmu / zaměstnanců školy / externích poskytovatelů služeb ad. + seznam důležitých kontaktů, na které je možné se obrátit v případě ohrožení.
- Identifikace možných rizik a zavádění odpovídajících strategií zmírňující rizika ohrožení.
- Příprava na nové, dosud nepopsané, způsoby provádění kybernetických útoků a neustálá aktualizace plánu zvládání rizik.
- Postupy ověřování, zda k incidentům skutečně došlo.
- Jasné komunikační pravidla a postupy, které určují, co je komu třeba sdělit a v jakém časovém rámci. Z komunikace musí být zřejmé, k jakému incidentu došlo a jaké kroky jsou podnikány ke zmírnění incidentu.
- Možné využití komunikačních šablon, které mohou být použity v případě ohrožení. Komunikační šablony mohou být vytvořeny pro nejrizikovější incidenty z důvodu úspory času.
- Aktivní bezpečnostní audit, který dokáže určit, jak k incidentu došlo, dokáže identifikovat zranitelnost a potencionální pokračující riziko.
- Jasně definované strategie, které zajistí, že riziko nebude pokračovat.
- Nastavený systém evaluace s cílem zlepšovat bezpečnostní opatření.
- Plán kontinuálního vzdělávání zaměstnanců/pedagogů ad. v oblasti kybernetické bezpečnosti.
- Soulad se zákonem o kybernetické bezpečnosti.

- Dalším krokem je konkrétní popsání incidentů, které mohou nastat, a vypracování podrobných akčních plánů ke každé rizikové situaci.

Závěr: při sestavování těchto bezpečnostních standardů jsem čerpal především ze svých zkušeností, které jsem nabyl jako učitel informatiky a metodik ICT na základní škole. Popsal jsem problematiku používání moderních digitálních technologií na základních i středních školách, která se vyskytuje nejčastěji a opakovaně. Jelikož se termíny jako jsou bezpečnostní audit či plán zvládaní kybernetických rizik vyskytují v českém vzdělávacím prostředí minimálně, mají tyto bezpečnostní standardy přispět k popularizaci této problematiky a pomoci, aby se v českém vzdělávacím prostředí staly povinnou normou. Pedagogové pak mohou tyto standardy využít jako svého průvodce ve stále více robustnější digitální infrastruktuře, do které se většina pedagogů vydává dnes a denně vzdělávat a vyučovat dnešní mládež.