Jak na bezpečnou online výuku?

O2 Chytrá škola

Pedagogická fakulta

V tomto textu se zaměříme se na to, jakým způsobem zabezpečit online výuku. Zopakujeme si bezpečností pravidla, vysvětlíme si, jakým komunikačním nástrojům bychom měli dávat přednost a které při realizaci online vzdělávání naopak omezit.

Zajištění technického personálu

Na úvod je třeba upozornit na to, že abychom mohli online výuku skutečně zabezpečit, je nutné mít k dispozici personál, který je schopen online vzdělávací systémy bezpečně nakonfigurovat, nastavit systém uživatelských účtů a rolí a zajistit případnou podporu v situacích, kdy dojde k bezpečnostnímu incidentu. Tuto úlohu může hrát např. ICT koordinátor či další pracovník disponující IT znalostmi a dovednostmi. Ne každá škola však takového pracovníka k dispozici má, řada škol dokonce expertní pracovníky sdílí s jinými školami a zaměstnává tyto osoby pouze na částečný úvazek či dokonce dohodou o provedení práce.

Výběr vhodného nástroje pro realizaci e-learningu

V první pandemické vlně velká část škol zvolila pro synchronní komunikaci (videokonference) v rámci e-learningových forem vzdělávání takové nástroje, které znali (a používali) buď samotní učitelé, nebo jejich žáci. K frekventovaným nástrojům využívaným pro komunikaci pak patřily především *Facebook Messenger, WhatsApp, Skype, Zoom* či u žáků oblíbený *Discord*. Školy však často nerespektovaly, že tyto nástroje mají definován minimální věkový limit pro používání – a to zpravidla 13 let, u WhatsApp dokonce 16 let. Navíc od roku 2019 je v České republice (v souladu s opatřeními GDPR) posunuta hranice využívání těchto služeb dokonce na 15 let věku (Zákon č. 110/2019 Sb.).

Tyto nástroje by tak bez souhlasu rodičů neměli žáci mladší 15 let ke komunikaci používat. Omezení používání těchto nástrojů má své důvody - v těchto prostředích poskytujeme osobní údaje dětí třetím stranám (jméno, příjmení, email či dokonce telefonní kontakt…), řada z těchto nástrojů má přístup k telefonnímu seznamu v mobilu dítěte, dítě dále může kontaktovat kdokoli zvenčí (např. dospělý uživatel stejné služby), škola nemá pod kontrolou správu uživatelského účtu dítěte apod. Další problém, který se s využíváním těchto služeb pojí, je podvádění - pro registraci do dané služby žák podvrhne (často i na pokyn učitele) své datum narození apod. A asi nemůžeme považovat za žádoucí učit dítě lhát.

Podle školského zákona má škola povinnost zajistit, aby byli žáci (a pedagogové) v rámci výuky v bezpečí, proto by měla volit co nejvíce bezpečné systémy, ve kterých má účty žáků

a přístup do vzdělávacího prostředí pod kontrolou. Proto by měly využívat zejména takové systémy, které opatření spojená s GDPR dodržují a které poskytují škole **jednotné vzdělávací prostředí (JVP)** s jednotným přístupem ke vzdělávacímu obsahu a komunikaci. V tomto případě je pak vhodnou volbou používání produktů Google GSuite či Microsoft (Teams, Office365).

Nastavení uživatelských rolí a pravidel pro celé JVP

Základem bezpečnosti výuky je dodržování minimálních bezpečnostních standardů v kombinaci se správným ***nastavením uživatelských rolí a pravidel pro celé JVP***. V praxi to znamená, že oddělíme uživatelské role učitele a žáka, pro které nastavíme přístupová práva.

Jedním z problémů využívání videokonferenčních systému bylo, že žáci mohli díky nesprávně nastaveným rolím např. *sdílet nevhodný obsah, vypínat mikrofon učitele (mute), případně ho dokonce vyhodit z výuky (kick)*. Tyto problémy nastávaly také v situaci, kdy žáci vstoupili do dané videokonference dříve než učitel – získali pak vyšší oprávnění a opět mohli narušovat výuku, či dokonce zakázat učiteli do místnosti vstoupit. Z tohoto důvodu doporučujeme používat ***funkci předsálí*** – žáci před samotnou videohodinou zůstávají ve virtuálním předsálí a do hodiny se dostanou teprve tehdy, až jim učitel povolí přístup.

Nastavení uživatelských účtů a hesel v rámci JVP

Pro zajištění bezpečné online výuky je velmi důležité správně nastavit uživatelské účty žáků – podle ***názvu účtu by totiž v souladu s bezpečnostními standardy nemělo být možné poznat, o účet kterého žáka se jedná***. Název účtu, např. karelnovak@ebezpecnaskola.cz je tedy z hlediska bezpečnosti zvolen chybně. Toto opatření je důležité proto, aby nemohl být žák kontaktován uvnitř vzdělávacího prostředí osobami zvenčí - např. pomocí e-mailové komunikace (GMail, Outlook), ale také např. přímo prostřednictvím vzdělávacího prostředí (např. z MS Teams mimo doménu školy). Proto je také vhodné omezit komunikace s žáky na komunikaci uvnitř školní domény – osoby z vnějšího světa tak nebudou moci žáky tímto způsobem kontaktovat. Toto opatření je obdobné, jako když zakážeme cizím osobám přístup do školní budovy a školních tříd.

Při generování uživatelských účtů školy svým žákům ve většině případů vygenerovaly bezpečné heslo dodržující přísné bezpečnostní standardy. Bohužel však řada z nich také svým žákům umožnila, aby si heslo změnili a nastavili si místo něj heslo jiné - např. univerzální (které žáci využívají např. pro vstup do oblíbené hry Fortnite či do prostředí Steam). Tím se samozřejmě zabezpečení účtu snížilo a v několika případech máme zdokumentováno, že se přes žákovský účet do vzdělávacího prostředí skutečně přihlásila jiná osoba. Proto je důležité vysvětlit žákům, proč by měli mít pro přístup k různým službám různá hesla (splňující bezpečnostní standardy, tj. minimálně 8 znaků, používat fráze, kombinovat písmena, číslice apod.). K logickým bezpečnostním standardům také patří, že bychom neměli své přihlašovací údaje prozrazovat dalším osobám.

Využívání cloudu

V případně online výuky je velmi užitečné využívat cloudových řešení (často integrovaných přímo do jednotných vzdělávacích prostředí), která umožňují např. pravidelně zálohovat data spojená s výukou a zajistit jejich obnovu v případě bezpečnostního incidentu (např. malware, ransomware apod.). Pozor - **do komerčních cloudových řešení NEPATŘÍ citlivé údaje spojené s žáky, např. zprávy z pedagogicko-psychologických poraden či další podobné materiály o dítěti** (zdravotní dokumentace, vyšetření apod.).

Ochrana osobních údajů

Z hlediska bezpečnosti online výuky je také důležité zajistit, aby byly chráněny osobní údaje žáků i pedagogů. Ty mohou z online prostředí unikat celou řadou cest:

1. Školy zveřejní záznam z online výuky na školním webu (video, screenshot)
V první vlně přechodu na online výuku řada škol sdílela v dobré víře záznamy z výuku na svých školních webech. Školy tím chtěly především ukázat, že se jim přechod na e-learning daří a že se např. aktivně naučily využívat nástroje Google či Microsoftu. Bohužel prostřednictvím záznamů z výuky unikaly také osobní údaje žáků - např. jméno a příjmení v kombinaci s tváří dítěte a dalšími informacemi, např. o ročníku, který dítě navštěvuje. Zde je třeba opět upozornit na to, že škola může zveřejňovat takové údaje, u kterých nedochází k jednoznačné identifikaci konkrétních dětí - např. projení tváře a jména a příjmení dítěte (např. u fotografií tříd).

2. Záznam z výuky unikne - např. od žáků či prostřednictvím dalších osob.
Druhá vlna uzavření škol s sebou přinesla řadu fenoménů, ke kterým patří např. trollování výuky (tzv. video bombing) jinými osobami, kterým se podařilo proniknout do výuky. Trollové pak výuku narušovali, provokovali učitele, sdíleli nevhodný obsah, nadávali či uráželi jak učitele, tak i ostatní studenty apod. Hodiny si aktivně nahrávali a záznamy pak sdíleli prostřednictvím sociálních sítí (především pak prostřednictvím služby YouTube a TikTok).

Do výuky se tito trollové dostávali především díky samotným žákům, kteří jim *dobrovolně poskytovali přihlašovací údaje do videolekcí*, nešlo tedy o žádné složité hackerské útoky, u kterých dochází k prolomení zabezpečení. Řada z trollů dokonce na svých profilech v rámci sociálních sítí sdílela výzvy pro žáky, aby jim poskytli přihlašovací údaje do online hodin.

Prevencí před těmito typy útoků je především:

1. Nesdílet s žáky přihlašovací údaje do online hodin (např. kód dané hodiny a vstupní heslo).

2. Využívat uzavřené systémy (jednotná vzdělávací prostředí), ve kterých lze snadno spravovat uživatelská oprávnění. Např. definovat, že po přihlášení do hodiny budou mít

všichni žáci vypnuté mikrofony, nebudou moci lekci nahrávat, nebudou moci aktivně sdílet obrazovku apod.

3. Využívat funkce předsálí (viz výše v textu).

4. Zamykat probíhající výuku. Při virtuálním uzavření videochatu učitelem se totiž do hodiny nedostanou další uživatelé, pokud jim to sám učitel nedovolí.

Samozřejmě je také nutné chránit pedagogy, a to především jasně definovanými pravidly výuky (tj. jasně definovat např. zákaz nahrávání výuky, průběh realizace výuky, případné sankce apod.). Technicky bohužel pedagogy chránit nelze (možností je omezit využívání webové kamery učitelem, což ale snižuje efektivitu výuky a motivaci žáků).

Znovu tedy opakujeme – nahrávání **výuky nejde technickými prostředky zabránit** - existují stovky nástrojů, které umožňují nahrávat celou obrazovku či její výřez. A pokud snad nemáme k dispozici daný program, vždy můžeme nahrát obrazovku třeba mobilním telefonem či tabletem. Přesto však můžeme vypnout funkci nahrávání přímo v daném vzdělávacím prostředí - a to právě vhodným nastavením.

Na co nesmíme zapomenout

Z hlediska bezpečnosti je také velmi důležité **posilovat školní klima** a podporovat pozitivní vztahy jak mezi samotnými žáky, tak i žáky a pedagogy. Minimalizujeme tím riziko vážnějších útoků a omezíme tím nežádoucí aktivity žáků především na běžné zlobení. Žáci, kteří budou mít se svými pedagogy dobré vztahy, nebudou aktivně usilovat o narušování online výuky. Stejně tak je důležité dodržovat doporučení MŠMT pro online výuku, které limituje množství synchronní e-learningové výuky na 3 hodiny denně a které obsahuje řadu doporučení (např. s ohledem na množství a důležitost učiva, hodnocení žáků apod.). Omezíme tak rozvoj frustrace, která může být jedním ze spouštěčů kyberšikany a dalších forem agrese.

Nesmíme zapomenout také na dodržování obecných bezpečnostních pravidel, ke kterým patří např. *pravidelné aktualizace, aktivní antivirový program a funkční firewall*, *neotvírání podezřelých emailových příloh z neznámých zdrojů* (téměř čtvrtina pedagogů v rámci výzkumu Český učitel ve světě technologií 2020 realizovaného Univerzitou Palackého v Olomouci a společností O2 potvrdila, že jejich škola zažila útok pomocí ransomware, při kterém došlo k zašifrování školních data), *neotvírání podezřelých flashdisků bez antivirové kontroly, nereagování na žádosti o přihlašování se do různých podvodných stránek* (phishing), *nepřeposílání kódů potvrzujících finanční transakce* (mplatby) apod. Samozřejmostí je samozřejmě bezpečné heslo pro přístup k online službám, případně přímo dvojfázové či vícefázové ověřování přihlášení (např. pomocí mobilního telefonu).

Připravil doc. Kamil Kopecký, E-Bezpečí | Pedagogická fakulta Univerzity Palackého v Olomouci ve spolupráci s O2 Chytrá škola

JAK NA BEZPEČNOU ONLINE VÝUKU?

NĚKOLIK DOPORUČENÍ PRO PEDAGOGY

Podporujme dobré klima ve školní třídě.

Nastavme si s žáky jasná pravidla pro realizaci online výuky a dbejme na jejich dodržování.

S žáky pravidelně udržujme kontakt, poskytujme jim zpětnou vazbu, dejme jim prostor ke komunikaci.

Pro realizaci online výuky používejme jednotná vzdělávací prostředí a jednotné aplikace.

Nezapomeňme oddělit uživatelské role pedagogů a žáků. Nastavme správná oprávnění.

Do přihlašovacích údajů nepatří jméno a příjmení žáků.

Používejme bezpečná hesla obsahující fráze kombinující číslice, písmena další znaky.

Využívejme funkce předsálí, vstupujme do videkonferencí před svými žáky a poté jim umožněme přístup.

V případě potřeby online videolekce uzamkněme. Zamezíme tak přístupu nežádoucích osob.

Chraňme osobní údaje - jak pedagogů, tak i žáků. Nesdílejme veřejně záznamy z výuky.

Pro zálohování vzdělávacího obsahu využívejme cloud. Pozor, do cloudu nepatří citlivé údaje žáků.

Dodržujme obecná bezpečnostní pravidla: Pravidelně aktualizujme, používejme antivir a firewall atd.

E-BEZPEČÍ
www.e-bezpeci.cz