Technické zajištění on-line bezpečnosti na školách

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Na úvod aneb co s metodikou

V metodickém materiálu se čtenář seznámí s problematikou online bezpečnosti z hlediska aspektu více technického. V první části se čtenář seznámí s principy fungování informačních technologií, a to zejména běžně používaných ve školním prostředí. Rovněž bude uvedena řada nejběžnějších pojmů týkajících se síťových informačních technologií doplněná o jejich vysvětlení. Druhá část metodického materiálu bude věnována konkrétní problematice zabezpečení informačních technologií ve školách. V neposlední řadě budou uvedeny praktické tipy nejen pro správce sítě ve školách, učitele vyučující informatiku, ale i pro ostatní pedagogické pracovníky, kteří tak mohou poradit nejen dětem, ale i rodičům.

Metodický materiál je koncipován tak, aby v něm potřebné a využitelné informace našel jak začátečník, tak i středně pokročilý i pokročilý uživatel informačních technologií.

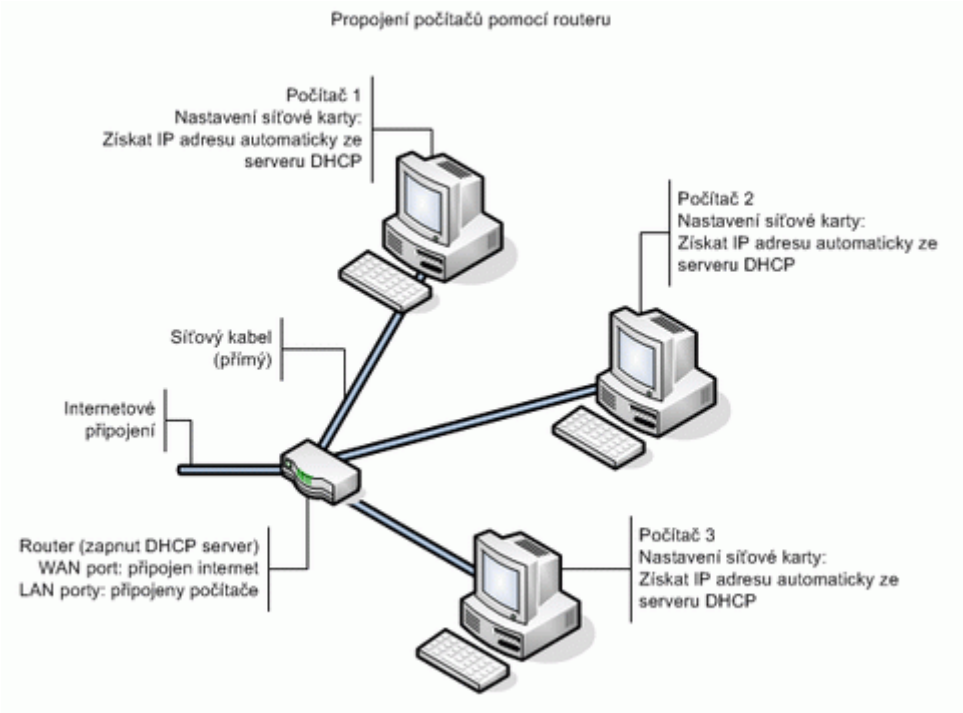
Jak tedy funguje školní síť?

Školní počítačová síť **LAN** se sestává z řady vzájemně propojených počítačů přes tzv. **router** nebo zařízení s názvem **switch** nebo také **hub**. Tato síť je následně připojena k další síti resp. k internetu, který budeme označovat pojmem **WAN**.

Router

Router (česky "směrovač"), je síťové zařízení, které "spojuje dvě sítě" a přenáší mezi nimi data - tato funkce se nazývá routování. Tím se liší od switche, který spojuje počítače v jedné síti. Router se převážně používá pro spojení místní sítě (LAN) se sítí vnější (WAN) - nejčastěji Internetem (pak realizuje i funkci NAT). Internetové routery jsou v dnešní době často kombinovány s DSL modemy nebo WiFi přístupovými body (AP, Access Point). Nejjednodušší routery, se základními funkcemi a jedním portem WAN (bodem připojení vnější sítě) a 4-portovým **switchem**, se dají pořídit i do 1500Kč. I tak levné routery mohou v sobě obsahovat i jednoduchý firewall.

V okamžiku, kdy propojíme veškeré hardwarové prvky sítě, budeme ještě potřebovat, aby se prvky spolu "domluvily" - musí tedy používat společný protokol. Zatímco dříve byl populární protokol firmy Novell (IPX/SPX), dnes se komunikuje zásadně pomocí "internetového" komunikačního protokolu **TCP/IP** (popularita Internetu udělala TCP/IP skoro universálním protokolem).



Model připojení přes router

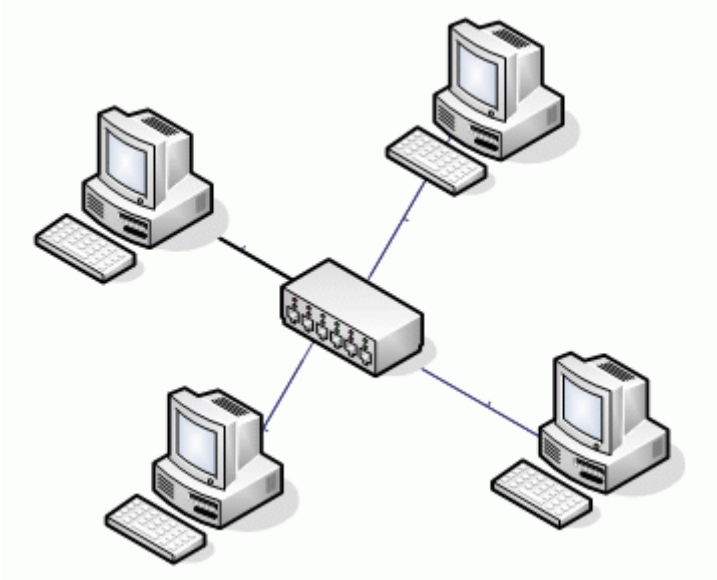
Hub / Switch

Jedná se o zařízení, která fyzicky spojují kabely síťových prvků (tiskáren, modemů, počítačů. IP kamer...) dohromady - nacházejí se ve všech uzlech sítě. I když připojíte počítač k zásuvce rozvodu LAN na zdi kanceláře, tento rozvod, dříve nebo později, skončí zapojený v některém hubu nebo switchi. **Hub** i **switch** (přepínač) dělají v podstatě totéž, ovšem každý trochu jinak (poznámka: v dnešní době už téměř nenarazíte na Hub, protože ceny switchů se pohybují již kolem několika málo stovek korun).

Hub je ze síťového hlediska pasivním prvkem. Směruje veškerý datový tok od všech počítačů do jednoho místa a jednotlivé síťové karty pak rozhodnou, jestli jsou data určena pro ně nebo nikoli. Při intenzivní síťové komunikaci mezi několika počítači dochází na síti často k tzv. kolizím (typicky: data vysílají dvě a více stanic společně) a data musí být vyslaná znovu - to komunikaci zpomaluje. Síťová komunikace probíhá systémem Half Duplex (komponenty buď data vysílají, nebo je přijímají - ne však současně).

Oproti tomu **switch** (přepínač) posílá data jen těm počítačům, kterým jsou určena (části sítě, které spolu komunikují - tzv. segmenty - podle potřeby spojuje "přepíná"). Z toho vyplývá, že switch pracuje daleko efektivněji a při jeho použití není zbytečně zatížena celá síť. Pro použití v malé školní síti dostačí 100Mbps switch, Gigabitové Ethernetové switche jsou trochu nákladnější záležitostí a v domácích podmínkách je ve většině případů nevyužijete (s gigabitovou sítí musíte mít pochopitelně kompatibilní všechny články sítě).

Další parametr u switchů bývá Full Duplex a Half Duplex. Při Full Duplexu je zařízení schopno ve stejném okamžiku přijímat a odesílat a to dokonce plnou rychlostí (u 100Mbps switche je to 100Mbps + 100Mbps), zatímco při Half Duplexu je pásmo rozdělené mezi vysílání a příjem.



Model připojení přes switch

LAN

Lokální počítačová síť (**LAN** - Loacal Area Network) je počítačová síť pokrývající, jak už název naznačuje, místní (lokální) oblast - například dům, kancelář (nebo kanceláře), budovu (nebo maximálně skupinu budov). Poznámka: v tomto článku se budeme zabývat lokálními sítěmi LAN - pokud se u nějakého prvku setkáte s konektorem označeným jako WAN (Wide Area Network, rozlehlé sítě), bude se nejspíše jednat o připojení k Internetu (ten je ve své podstatě největší sítí WAN).

Uspořádání sítě

Síťové prvky jsou u jednoduchých sítí uspořádané typicky do tvaru "hvězdice" (Star). U rozsáhlejších sítí, které obsahují několik **segmentů,** se topologie podobá "stromu" (Tree). V místech, kde se sbíhají kabely, jsou typicky umístěné tzv. huby nebo, a to je běžnější, přepínače (Switche), nebo případně směrovač (Router).

Síťová karta

Integrovaná síťová karta je dnes běžnou součástí základní desky. Odpovídající zdířku RJ-45 sítě Ethernet najdete nejčastěji na zadním panelu ATX základní desky. Zdířka je typicky umístěná těsně nad USB porty. Každá síťová karta má svou MAC adresu.

MAC adresa

MAC je unikátní "podpis" síťového prvku a... vstup do hackingu

Už dříve bylo požadavkem správců síti to, aby každá prvek sítě LAN měl své vlastní jedinečné a neměnitelné* číslo přidělené už v průběhu výroby. Důvodem je zvýšení bezpečnosti počítačových sítí - některé služby kontrolují nejen IP adresu cílového zařízení, ale i dodatečný hardwarový identifikátor zařízení sítě Ethernet, takzvanou MAC adresu (často nazýván fyzickou adresou zařízení).

MAC adresa bývá některými poskytovateli internetu použita pro identifikaci a tím zpřístupnění internetu (např. UPC), proto je dobré vědět, jak ji zjistit. Postup je jednoduchý - otevřete příkazový řádek (*„Start“ > „Spustit“*, do pole napište *cmd* a stiskněte *„OK“*). Do příkazového řádku napište příkaz: *IPconfig /all* a na obrazovce se vypíší vlastnosti všech síťových adaptérů v počítači. Vaši MAC adresu najdete v řádku *Fyzická adresa*

WAN

Termín WAN se používá pro množinu dvou a více lokálních sítí. V praktické oblasti tak lze říci, že jde o připojení k internetu, kde má každé zařízení v síti svou IP adresu.

IP adresa

IP adresa je jednoznačná identifikace konkrétního zařízení (typicky počítače) v síťovém prostředí TCP/IP (ať se jedná o lokální síť nebo Internet). V současné době je převážně používán protokol IP verze 4 (IPv4). U tohoto protokolu je IP adresou 32 bitové číslo,

zapisované po jednotlivých bajtech, oddělených tečkami. Pro snazší zápis se hodnoty jednotlivých bajtů se zapisují v desítkové soustavě, např.: **192.168.1.24**

IPv4

- **32 bitové adresy** zařízení (cca 4 miliardy různých IP adres, dnes nedostačující)

  Dnes je připravena nová verze IPv6, která řeší nedostatek unikátních síťových adres v IPv4 a řeší některé bezpečnostní a výkonnostní problémy (hierarchické směrování).

IPv6

- **128 bitové adresy**
- podpora bezpečnosti
- podpora pro mobilní zařízení
- funkce pro zajištění úrovně služeb (QoS - Quality of Service)
- fragmentace paketů - rozdělování
- zařízení IPv6 je schopné komunikovat se sítí IPv4 (to neplatí naopak)

  Protokolem IPv6 se v lokálních sítích nebudeme zabývat - prvkům sítě LAN se obvykle totiž přidělují **interní IP**adresy, platné pouze v rámci dané lokální sítě (viz. další odstavec). Tady problém s adresami není - vaše IP adresa na lokální síti bude nejspíše použitá v desítkách tisících počítačových sítí.

Veřejná / neveřejná IP adresa, router

Jelikož ne každý síťový prvek může mít světově unikátní IP adresu, přistoupilo se k myšlence vyhrazení části adresového prostoru IPv4 pro privátní sítě (jeden z rozsahů těchto adres začíná typicky čísly 192.168.xxx.yyy). Takových lokálních sítí jsou tisíce a k internetu jsou připojené vždy pomocí nějakého routeru. **Důležité**: v konfiguraci interní sítě je tento prvek označený jako "**brána**" (**Gateway**) - tudy totiž prochází komunikace směrem ze sítě LAN k internetu.

Na "lokální straně" routeru (LAN) má každé zařízení svou unikátní privátní **IPv4 adresu**, tato adresa je ale **unikátní pouze v rámci této lokální sítě**. Pomocí této adresy mohou zařízení spolu komunikovat v síti přímo, tedy bez účasti routeru (využívá se switch). Na druhé "straně" je router (WAN) připojený nejčastěji přímo k internetu, zde má svou vlastní, světově unikátní IP adresu.

NAT - Network Address Translation

Pokud router provádí tzv. překlad adres (**NAT**) mezi vnitřní (privátní) sítí LAN a internetem, pak je komunikace počítačů interní sítě s internetem bezproblémová. Poznámka: podmínkou správného fungování NAT je, že komunikaci mezi počítačem umístěnném na vnitřní síti a internetem **musí vždy zahájit počítač na vnitřní síti**. Router v této situaci si zapamatuje obě komunikující strany a dovoluje hladký přenos mezí klientem (počítačem na síti) a internetovým serverem (v průběhu komunikace provádí proces, který vede k "zamaskování" / skrytí interní síťové adresy klientského počítače - někdy se mluví o IP "maškarádě").

Problém nastává, když potřebujete, aby nějaký počítač byl přímo dostupný z prostředí Internetu - takové zařízení musí mít svou vlastní jedinečnou internetovou IP adresu (taková adresa je pak **veřejně přístupná na internetu**). Na takovém počítači pak může běžet internetový server, herní server, IP kamera... Jelikož veřejné IP adresy jsou vzácné, přidělují se veřejné IP adresy jen vzácně (obvykle je to spojeno s vyššími poplatky za připojení k internetu).

Poznámka: tato situace se změní s hromadným nástupem protokolu IPv6, kde se předpokládá, že většina zařízení (pokud to nebudou vyžadovat bezpečnostní důvody) bude přístupná přímo z prostředí internetu.

Výhody veřejné IP adresy oproti neveřejné jsou zejména tyto:

- přímá dostupnost počítače z Internetu,
- možnost provozování veřejných serverových služeb, např. webové stránky, FTP
- vyžadováno některými síťovými hrami

Nevýhody jsou:

- větší riziko napadení nezabezpečeného počítače,
- ztráta anonymity
- riziko pro nezkušené uživatele

Bezdrátové školní sítě

Dnes je již běžným standardem, že každá škola má vlastní bezdrátovou síť, kam se mohou studenti přihlašovat pomocí svých zařízení. Důležité je, aby tyto sítě byly rovněž zabezpečené, a to pomocí registrace MAC adresy jednotlivých zařízení v síti. Každý student, který se chce připojit do školní sítě, si tak musí registrovat své zařízení u správce sítě. Problémem je však možnost klonování MAC adresy, kdy se i jiné zařízení touto funkcí může vydávat za jiné. Řešením je zvýšení odpovědnosti nejen za své jméno a heslo (viz níže), ale i za privátnost své MAC adresy.

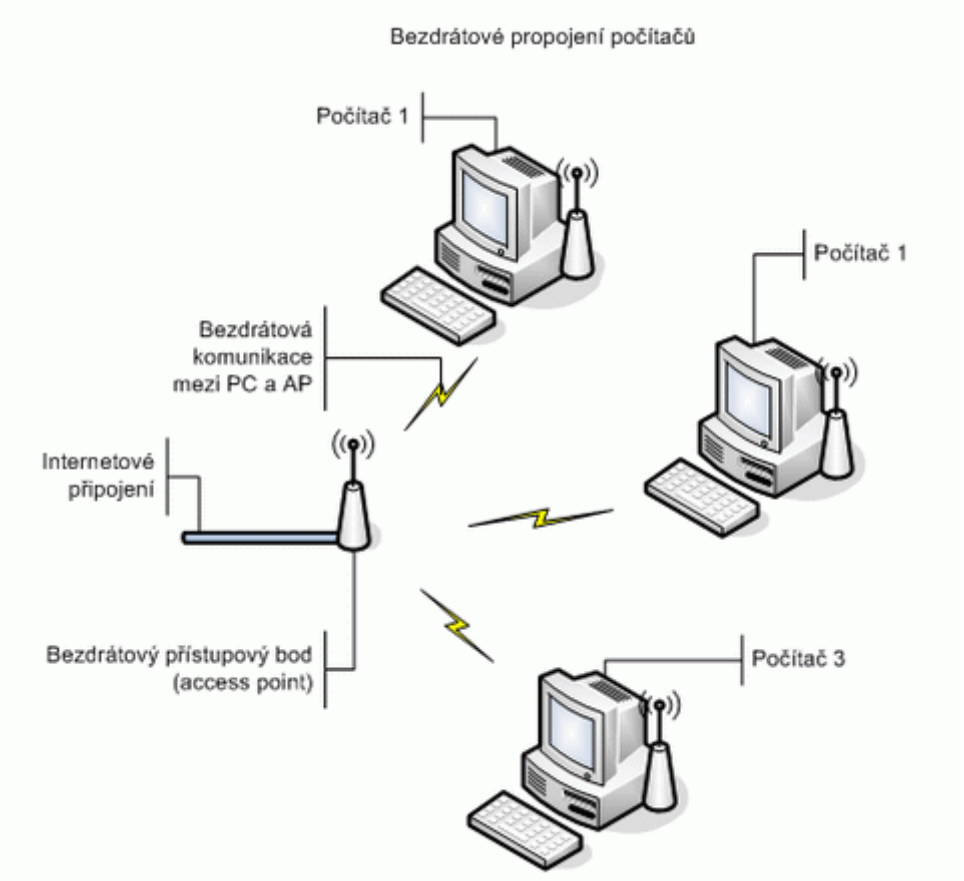


Schéma zapojení bezdrátovou technologií

Zabezpečení pracovních stanic (PC)

Pro náš klidný spánek a kvalitní zajištění ochrany počítače je důležité mít k dispozici technické prostředky, které nám v boji s neviditelným nepřítelem pomohou. Ostatně, jak jinak detekovat desítky miliónů škodlivých virů, než s pomocí antivirového programu? Nebo jak zastavit automatizované útoky prostřednictvím internetu, než s pomocí firewallu?

Základními stavebními kameny bezpečnosti jsou následující aplikace

- Antivirový program. Jeho používání je alfou i omegou celé informační bezpečnosti. Antivirový program je nutné používat správně a především zajistit, aby byl vždy v aktuální verzi. Nutné je dbát jak na aktuálnost virových databází (velcí světoví výrobci v současné době vydávají nové databáze každý den, v případě nutnosti i několikrát denně), tak na aktuálnost samotného programu. Mění se totiž způsoby infiltrace operačních systémů a technologie používané počítačovými viry, přičemž několik let starý antivirový program by si s nimi nemusel umět poradit.
- Filtr spamu. Spam (nevyžádaná elektronická pošta) dnes není jen o záplavě nechtěných zpráv v e-mailové schránce. Je mnohem nebezpečnější: slouží k podvodům, nelegální přípravě půdy pro další útoky. Kromě toho neřešený spam lavinově generuje další množství spamu (aneb útočníci mají prostředky, jak zjistit, že jste zprávu otevřeli). Proto je více než kdy jindy nutné zajistit kvalitní filtrování nevyžádané pošty.

Jak fungují spamfiltry

Ohledně filtrování spamu se nedá říci jedno jediné absolutně platné obecné pravidlo. Protože kdyby existovalo, první, kdo by ho porušil, by byli rozesílatelé spamu. Filtry spamu se snaží každou zprávu analyzovat z desítek různých úhlů pohledu.

A jejich společným vyhodnocením pak dochází k závěru, zdali jde či nejde o spam. Díky této „hloubkové kontrole“ mají filtry poměrně vysokou úspěšnost a zachytávají značné procento spamu.

Pod pojmem „desítky úhlů pohledu“ si lze představit třeba vyhodnocování frekvence některých slov v textu, zkoumání, zdali e-mail nemá zfalšovanou adresu odesílatele (korektní zpráva něco podobného nemá zapotřebí), „umí“ číst i text v obrázcích, sleduje, zdali odkazy nevedou na známé stránky podvodníků apod. Je toho opravdu hodně a každý e-mail je

během zlomku sekundy podrobený takovémuto „křížovému výslechu“, z něhož vychází s verdiktem vinen či nevinen. Spam či korektní pošta.

Žádný počítačový program sice není neomylný, nicméně dnešní filtry se vyznačují opravdu solidní úspěšností – čímž každý den šetří mnoho času strávených nad tříděním a mazáním nesmyslných zpráv. Nehledě na to, že už prosté otevírání spamu může být nebezpečné: jsou třeba škodlivé kódy, které se zcela automaticky spustí po pouhém otevření e-mailu. Stejně tak se rozesílatel spamu může jednoduše dozvědět (třeba pokud se do e-mailu stahuje obrázek z jeho serveru), že konkrétní osoba spam otevírá – a následně ji tak „zasype“ další lavinou nevyžádané pošty.

- Personální firewall. Jedná se o počítačový program, který slouží coby pomyslná brána mezi jednotlivým počítačem a okolním prostředím (lokální síť nebo internet). Funguje tak, že přes něj prochází VEŠKERÁ komunikace, která je následně tříděna a filtrována. Hrozby, které personální firewall dokáže eliminovat, spadají do oblasti útoků síťových červů, brání počítač před napadením hackery, infiltrací škodlivého kódu z web stránky, zabraňuje neoprávněnému získání práv po síti, snižuje riziko bezpečnostního incidentu vinou lidské chyby, znesnadňuje odcizení informací…
- Záplatování. Aktualizovat je nutné nejen antivirové programy, ale také ostatní software (operační systém, kancelářské aplikace, chatovací programy aj.) – počítačové viry a hackeři vůbec totiž mnohdy využívají různých zpravidla již známých a popsaných bezpečnostních problémů. Jinými slovy: hřeší na lidskou neznalost nebo pohodlnost.

Několik tipů, jak se aktivně bránit

Kromě technických prvků je dobré dodržovat při ochraně počítačů jistá „organizační“ opatření.

- Používejte antivirový program. Jedná se o základní stavební prvek každé bezpečnosti.
- Používejte antispywarový program. Hledání spyware má odlišné zákonitosti, než odhalování virů, takže je k němu zapotřebí přistupovat odlišně. Většina antivirových programů umí vyhledávat i spyware – ale raději si to ověřte.

- Používejte firewall. To je brána mezi počítačem/sítí a internetem, která kontroluje veškerý provoz. (Ideální je používat „komplexní bezpečnostní řešení“, které obsahuje antivirus/antispyware, firewall i filtr spamu – tedy „vše v jednom“, kdy odpadají problémy se správou, kompatibilitou nebo špatným nastavením.)
- Mějte na počítači svůj vlastní účet. Sdílený účet rovná se sdílená odpovědnost rovná se žádná odpovědnost.
- Vypínejte po sobě programy. Počítačové programy, které nepotřebujete, vypínejte – zvláště odcházíte-li od veřejného počítače, neboť by mohly obsahovat některé informace (třeba seznam navštívených stránek aj.).
- Neukládejte jména a hesla. Jejich ukládání je sice na jedné straně jednodušší, na druhé straně může ke jménům a heslům získat přístup útočník: třeba fyzicky (stačí, aby zasedl k počítači a má dveře dokořán otevřené) nebo vzdáleně (instalace programu, který zkontroluje obsah pevného disku).
- Aktualizujte a záplatujte operační systém i aplikace. Hackeři nejčastěji využívají známých chyb k průnikům do systému – proč by taky hledali chyby nové, když těch starých (a nezáplatovaných) jsou mraky…
- Používejte legální software. Používání pirátských kopií s sebou nese celou řadu rizik: od omezení přístupu k aktualizacím (= větší zranitelnost) přes nejasný původ (= častá virová nákaza) až po problémy s kompatibilitou s bezpečnostními programy.
- Zálohujte. Nepočítejte s tím, že se vám bezpečnostní průšvih vyhne. Dříve nebo později si najde i vás. Pak je otázkou, jak na něj budete připraveni.
- Snažte se problémům předcházet. Nejlepší je takový, který vůbec nevznikne. Aneb nenavštěvujte stránky, o kterých máte předem pochybnosti, nespouštějte podezřelé přílohy u e-mailů (antivirový program považujte až za poslední záchrannou brzdu) apod.

Možnosti rodičovské kontroly

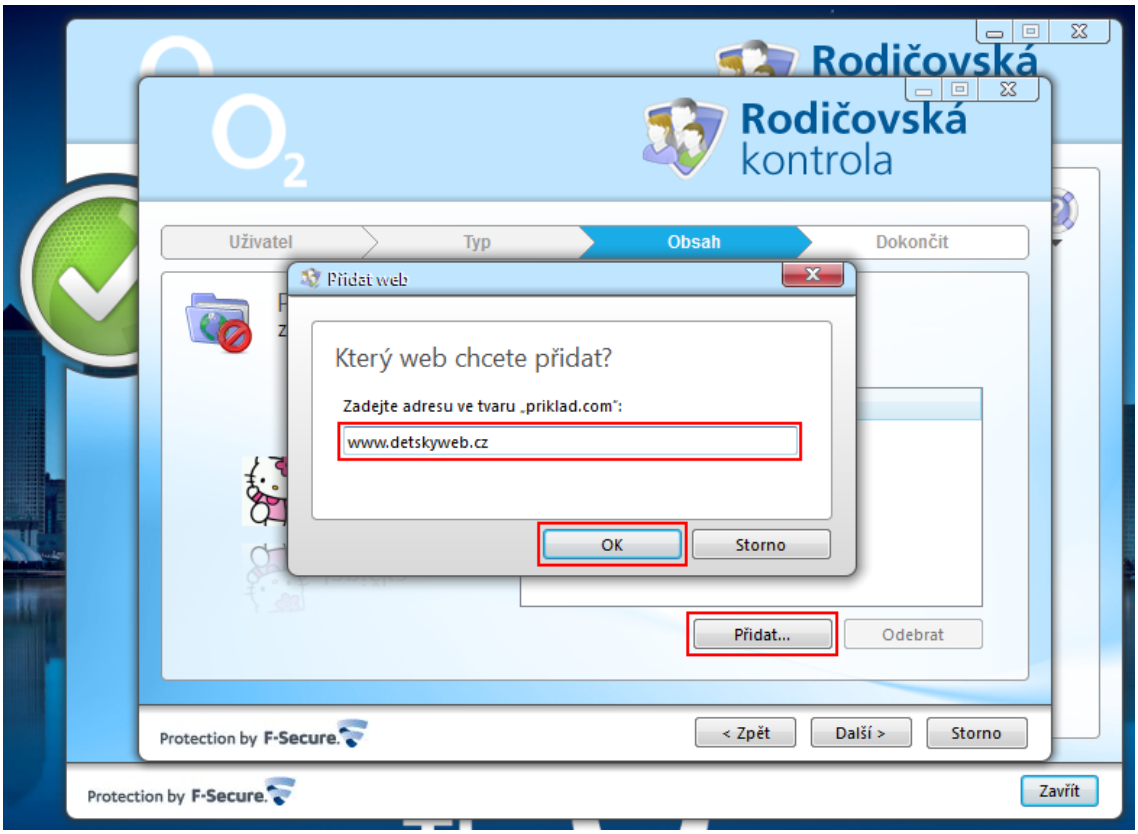
- Jedním z užitečných pomocníků pro bezpečnější pohyb dětí v kybernetickém prostoru jsou programy tzv. rodičovské kontroly (parental control). Jedná se o programy, které vynucují pravidla pro chování na počítači.

  Ovšem pozor, nesmíme zapomínat, že jsou to jen a jen počítačové programy! A že ani stoprocentně nastavené nebudou garantovat absolutní jistotu bezpečí. Navíc je internet plný návodů, jak je obejít. A kromě toho: dětí se k internetu bezpochyby připojuje z různých míst. Z knihovny, skrze mobil, od kamarádů... Přesto jsou programy rodičovské kontroly užitečnými pomocníky.

  Z technického hlediska je můžeme rozdělit na tři kategorie:

- Filtrování obsahu. Veškerý obsah, který vstupuje do počítače, je kontrolován na základě několika parametrů. Jedná se vlastně o něco podobného jako v případě personálních firewallů nebo antivirových programů, ale na trochu jiné úrovni. Zatímco tyto mají pevně definovaná pravidla (blokování nežádoucího provozu, hledání určitých řetězců v souborech apod.), tak v případě rodičovské kontroly je to trochu odlišné: hledá nevhodná slova v e-mailech a www stránkách, analyzuje obrázky apod.

- Monitorování aktivity na počítači. Ne vše se samozřejmě podaří zablokovat na vstupu do počítače. A ne všechen nevhodný obsah přichází po internetu – ale třeba i po CD půjčených od spolužáků apod. Proto je potřeba věnovat pozornost také kontrole počítačů. Ta přitom funguje na podobném principu jako filtrování obsahu, neboť vyhledává nežádoucí nebo přinejmenším podezřelé objekty.
- Omezování přístupu ke zdrojům. Toto je další metoda, která se v oblasti rodičovské kontroly používá a která vychází z předpokladu, že nejlépe se nevhodný obsah bude blokovat tak, že se k němu odepře přístup. Jinými slovy: v počítači existuje databáze nevhodných zdrojů (seznam www stránek určených pro dospělé apod.) a počítač při přihlášení nepovolané osoby (dítěte) odmítne příslušnou stránku zobrazit. Tato metoda je velmi účinná, ale na druhé straně je velmi závislá na kvalitě použité databáze nebo nastavených pravidlech. A ta bude těžko kdy obsahovat všechny nevhodné zdroje.



Postaveno (především) na důvěře

Přistupovat k problematice dětí a informační bezpečnosti je ošidné. Zvláště ve chvíli, kdy jsou děti technicky zdatnější, než jejich rodiče. Přesto to neznamená, že bychom na celou problematiku měli rezignovat – naopak, musíme „začít od sebe“. Ale jak?

- Vzdělávejte se. Vyhledávejte zdroje informací, zkoušejte nové věci, snažte se pochopit fungování počítačových programů.
- Komunikujte s dětmi. Informujte se navzájem o výhodách používání počítače stejně jako o nebezpečích, která tato činnost s sebou nese.
- Nastavte pravidla. Nadefinujte jasná pravidla, která je třeba za každých okolností dodržovat. Např. nesdělujte osobní informace či adresu.
- Zajistěte dodržování pravidel. Každé pravidlo je účinné pouze v případě, že se dodržuje.
- Mějte počítač ve společné místnosti. Neposkytujte dětem možnost porušovat pravidla tím, že jim dáte počítač k neomezenému fyzickému i časovému přístupu.
- Využijte technologické nástroje. V mnoha počítačových programech můžete najít – pokud budete hledat – užitečné pomocníky. Třeba filtry nevyžádané pošty (spamu), rodičovskou kontrolu přístupu (k internetu) apod.
- Mějte věci pod kontrolou. Máte-li mít zodpovědnost, mějte i pravomoci. Mějte administrátorský přístup k počítači, rozhodujte o to, jaké programy se budou či nebudou instalovat apod.
- Nenechte děti volně se setkávat s internetovými přáteli. Každé podobné setkání v sobě nese velké riziko – klidně jej umožněte, ale přijměte odpovídající opatření.
- Kontrolujte historii navštívených stránek na internetu. Stejně tak kontrolujte různé další výpisy: s kým dítě komunikuje, kdo mu posílá e-maily apod.

Jak poznám, že se něco děje

Ne všemu se dá předem zabránit, ale existují mnohé varovné příznaky, kterých je dobré si všímat a které mohou ledasco napovědět. Patří k nim zejména:

- Dítě se začne chovat „jinak“ (= divně). Co dříve bez problémů akceptovalo nebo vyhledávalo (např. vaši pomoc u počítače) je mu najednou na obtíž a je to nežádoucí. Najednou chce být z nějakého důvodu samo, stáváte se překážkou.
- Dítě v určeném čase náhle bez zjevné příčiny MUSÍ být u počítače. Všechno ostatní jde v tu chvíli stranou, cíl je jediný.
- Dítě začne používat neobvyklé programy a odmítá vás seznámit s jejich účelem.
- Dítě za sebou znenadání začne „zametat stopy“ a mazat třeba historii navštívených www stránek, má evidentně důvod nebo potřebu něco skrývat.

- Dítě se zdráhá povídat si o tom, co na počítači dělá a s kým komunikuje. Na počítači najednou chce trávit veškerý volný čas.

Technické zabezpečení offline

Každá škola by měla mít zpracován svůj plán online bezpečnosti, podle kterého bude postupovat při eradikaci jednotlivých hrozeb internetu, ale i při preventivních aktivitách. Příklad takové plná níže.

Plán online bezpečnosti

Školní plán prevence a řešení elektronického násilí

KROK 1: Inovace školního řádu

- Integrujte pravidla užívání mobilních technologií a internetu v prostorách školy a v době výuky do školního řádu.
- Začleňte pravidla pro zveřejňování osobních údajů včetně fotografií dětí na školních webových stránkách.

KROK 2: Školní specialista bezpečného internetu

- Určete školního specialistu/konkrétní kontaktní osobu ve škole pro řešení krizové situace (výchovný poradce, metodik prevence, ICT informatik, školní psycholog),
- kontaktní osobě zajistit odbornou přípravu v oblasti online bezpečnosti
- kontaktní osobu zveřejnit dětem a rodičům
- kontaktní osoba získá oporu pro zápis intervence /rozhovoru – připravit oporu pro zápis

KROK 3: Místní záchranná síť pro řešení elektronického násilí

Zajistěte konkrétní spolupracující osoby v subjektech, které v lokalitě řeší kyberkriminalitu a elektronické násilí.

- Za OSPOD – doplňte jméno
- Za PPP
- Za Policii místní složku
- Krizové linky
- Česká školní inspekce

Subjekt	Jméno, příjmení	Tel.	činnost
Náš mentor			
OSPOD			
Policie ČR			
PPP			
ČŠI			
NCBI			
NCBI – Horká linka	Ing. Ladislav Kos Ing. Michal Horčic		Nezákonný obsah, šikanující obsah, pomoc s falešnými profily na FB
SLB – rodičovská linka	www.pomoc-online.cz		Psychická krize spojená s internetem

KROK 4: Zajistěte technické řešení online bezpečnosti

- Definujte konkrétní osobu, která zajistí technické řešení online bezpečnosti (informatik)
- Rozhodněte, jakým způsobem bude školní internet přístupný pro žáky, s jakými omezeními, zajistěte filtrování přístupu na nevhodné a nezákonné stránky
- Zapojte rodiče do prevence elektronického násilí, zajistěte rodičovský seminář, informujte je o školní kontaktní osobě pro řešení elektronického násilí

KROK 5: Zařaďte téma etického a bezpečného užívání mobilních technologií a internetu do ŠVP

- 1. Stupeň - Člověk a jeho svět
- 2. Stupeň – Informační a komunikační technologie
- Jednorázové preventivní aktivity - Projektové dny/vyučování
- Připojte se k soutěži k Mezinárodnímu dni bezpečného internetu - každoročně únor
- Externí primární prevence (NCBI, E-bezpečí, Nebuď oběť)

Pro výuku využijte metodické materiály pro pedagogické pracovníky dostupné na www.saferinternet.cz a www.bezpecne-online.cz.

Začlenění problematiky do školního řádu

Jak již bylo uvedeno v prvním kroku příkladného plánu online bezpečnosti, je potřeba se zabývat zapracování této problematiky do školního řádu. Příkladné kapitoly mohou vypadat následovně.

Základní pojmy

“Uživatelem” se v těchto pravidlech rozumí každý, kdo používá počítač, terminál nebo jakékoli jiné zařízení připojené do počítačové sítě školy. Pod pojmem “počítačová síť” nebo

zkráceně “síť” se rozumí souhrn technických a softwarových prostředků výpočetní techniky potřebných k propojení uživatelů. “Legální software” je software získaný v souladu se zákony, včetně autorského práva. Termín “výpočetní technika” se v těchto pravidlech používá pro označení počítačové sítě a prostředků výpočetní techniky, včetně jejich programového vybavení. Pod pojmem “školní počítačová síť“ nebo “školní síť“ se rozumí počítačová síť školy XY. “Hostem” se rozumí uživatel připojený z prostor školní jídelny, služebního bytu, mateřské školky a městské knihovny.

Správa sítě

- 1. Host si zodpovídá za svou výpočetní techniku sám.
- 2. Školní počítačová síť je hiearchicky uspořádaná síť propojených počítačů.
- 3. Školní síť jako celek spravuje správce sítě, jehož jmenuje ředitel školy. Správce sítě zajišťuje celkovou funkčnost sítě, vede evidenci jejích uživatelů a může podle potřeby datový provoz v síti monitorovat. Účelem monitorování je optimalizace provozu výpočetní techniky, zjišťování abnormálních stavů a prevence proti nim a odhalování případů porušování pravidel používání sítě.
- 4. Za provoz výpočetní techniky ve školní síti zodpovídají zaměstnanci příslušného pracoviště (kabinety, třídy, učebny, kancelář), případně určení zaměstnanci (sborovny, chodby).

Práva uživatelů

- 1. Uživatelé mají právo využívat školní síť za předpokladu dodržování pravidel počítačové sítě.

Povinnosti uživatele

- 1. Každý uživatel se před započetím práce s výpočetní technikou seznámí s pravidly používání školní sítě.

- 2. Uživatel smí používat výpočetní techniku pouze v souladu se vzdělávacím posláním školní sítě.
- 3. Uživatel pracuje s výpočetní technikou pouze pod tím uživatelským jménem, které mu bylo přiděleno, a heslo ke svému uživatelskému jménu volí a udržuje v tajnosti tak, aby zabránil jeho zneužití. Uživatel plně zodpovídá za škody, ke kterým by došlo zneužitím jeho uživatelského jména v důsledku nedbalé manipulace s heslem.
- 4. Přístupová práva uživatele jsou dána jeho uživatelským jménem. Uživatel se nesmí pokoušet získat přístupová práva či privilegovaný stav, který mu nebyl přidělen, a nesmí se snažit získat přístup k chráněným informacím a datům jiných uživatelů. Pokud uživatel jakýmkoli způsobem (včetně hardwarové nebo softwarové chyby systému) získá privilegovaný stav nebo přístupová práva, která mu nepatří, je povinen tuto skutečnost neprodleně ohlásit administrátorovi domény.
- 5. Uživatel nesmí provádět takové změny výpočetní techniky, které by mohly mít vliv na provoz sítě. Tato činnost je vyhrazena jen správci školní sítě.
- 6. Uživatel nesmí vyvíjet takovou činnost, která by ostatním uživatelům škodila nebo bránila v řádném využívání sítě.
- 7. Uživatel nesmí používat a šířit nelegální software a bez souhlasu kopírovat a distribuovat části operačního systému a instalovaných programů. Uživatel, s výjimkou hosta, bez souhlasu správce sítě neprovádí jakékoliv instalace programů nebo jejich částí.
- 8. Každý uživatel plně odpovídá za veškeré informace, které ve školní počítačové síti zveřejnil. Pro používání elektronické pošty a vystavování informací na počítačích platí stejná etika jako pro používání klasické pošty. Je výslovně zakázáno používat počítačovou školní síť k šíření materiálů, jejichž rozšiřování nebo veřejné vystavování je v rozporu se zákonem, a obtěžovat ostatní nevyžádanou poštou. Při komunikaci je zakázáno používat vulgární výrazy.
- 9. Uživateli, který tato pravidla hrubě a úmyslně poruší, bude omezen nebo zakázán další přístup do školní sítě. Tím se nevylučuje další postih vyplývající z porušení povinností zaměstnance nebo žáka školy.

Informační tabule přímo v učebně

Podmínky užívání ICT ve škole musí samozřejmě definovat školní řád. Ale kdo z žáků dokonale jeho stanovy zná? Proto je doporučeno v počítačové učebně mít vyvěšenou informační tabuli, kde jsou pro uživatele uvedeny stručné informace, co je při využívání ICT ve škole možné a co naopak není.

Tyto informace by měli být v souladu s podmínkami přijatelného užití definované CESNETem, z nichž vyplývá, že uživatelé nesmějí tuto síť využívat pro činnosti, které:

- umožňují nebo snaží se získat neoprávněný přístup ke zdrojům připojených sítí
- porušují práva duševního vlastnictví
- nepříznivě působí na provoz sítě nebo jejích jednotlivých služeb, brání uživatelům v přístupu k těmto službám, ohrožují činnost sítě nebo nadměrně omezují její výkon
- plýtvají kapacitou sítě
- ničí integritu informací uložených v počítačích a ostatních síťových prvcích
- omezují soukromí uživatelů.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.