NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

ROZCESTNÍK PRO UČITELE STŘEDNÍ ŠKOLY

www.nukib.cz

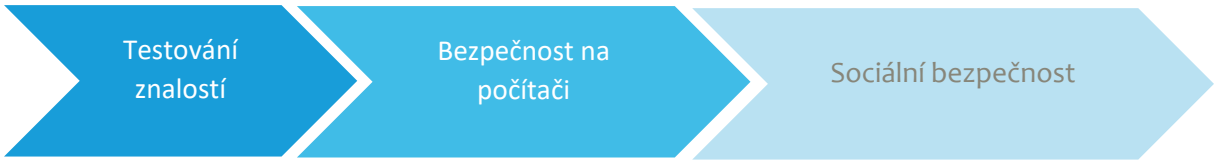
NAVIGACE

Kliknutím se přesunete na dílčí kapitolu.

ROZCESTNÍK UČITELE

Ještě než se pustíme do koncipování vlastní výuky, podíváme se na materiály, které nám dají jasnou představu, o co jde. Pro učitele, kteří nejsou s tématem dobře obeznámeni, lze doporučit materiál z Digifolia. Pro orientaci lze zvolit i Slideplayer, který vznikl na základě přednášky v roce 2015 a obsahuje základní pojmy a výklad k nim v oblasti problémového chování.

Materiál není určen jako pomůcka pro celý předmět nebo dokonce obor. Pokud máte na škole specializovaný předmět, doporučujeme kromě našeho výčtu hlavně využívat materiály CISCO Akademie, které obsahují dva moduly z dané oblasti.



Vyjdeme z klasické situace a noční můry každého učitele. Stojíte před třídou, je začátek roku a vy máte nějak naučit žáky bezpečnou práci na počítači – o které jsou pevně přesvědčeni, že ji znají mnohem lépe, než vy.

V první řadě je nutné si uvědomit, že bezpečnost neznamená pouze prevenci počítačové kriminality, ale patří k ní i chápání souvislostí a vidění virtuální reality jako celku. To žáci zpravidla neumí.

Ve druhé řadě pak to, že tento globální pohled bude jiný pro gymnazistu, který chce jít na studium Kybernetické bezpečnosti z pohledu sociologie, jiné pro budoucího technika a úplně jiné pro člověka, který půjde hned po škole do praxe mimo IT obor. To neznamená, že například zedník nemusí umět napsat správně životopis, poslat jej bezpečně mailem a rozpoznat manipulativní chování. Základní přehled potřebují v dnešní době všichni.

Materiál je členěn tak, aby z něj šly vybírat konkrétní celky, které potřebujeme posílit nebo naopak zeslabit a je doplněn občas i odkazy mimo IT bezpečnost, pokud tyto odkazy obsahují nějaké vhodné vysvětlení k dalšímu výkladu.

Testování dovedností Je v podstatě alfou a omegou úspěšné výuky kybernetické bezpečnosti. I když se to zdá jako ztráta času, je vhodné nenásilnou formou, třeba vypracováním soutěže, na začátku každého ročníku ověřit, kam se žáci posunuli a jestli nemusíme něco zopakovat.

Bezpečnost na počítači Základem je fakt, že každý žák by měl mít nějaké své zařízení, o které se stará a do kterého nahrává nejrůznější, vhodný nebo často i nevhodný, obsah. Měl by vědět, že zárukou bezpečnosti není cena mobilu, ale pravidelné aktualizace a péče o software. K tomu patří povědomí o fungování sítí, znalost toho, jak pracuje procesor a co to je třeba DNS.

Sociální bezpečnost Začíná znalostí bezpečného prostředí, pokračuje přes fakenews a pohyb po sociálních sítích a končí znalostí technik sociálního inženýrství. Existuje celá řada her, pomůcek a videí s touto problematikou. Bohužel do této oblasti patří i znalost trestního zákoníku s tím, že by žáci měli vědět, jaká sazba je za jakou protizákonnou činnost. Do této části jsou zařazeny i materiály pro metodu CLIL, které lze použít u těch žáků, kteří budou aspoň částečně rozumět. Není podmínkou, aby učitel celou hodinu souvisle mluvil, podstatné je, aby žáci hned na počátku hodiny text nepřeložili pomocí translátoru. V takovém případě většinou nepochopí, o co v textu jde.

TESTOVÁNÍ ZNALOSTÍ

SOUTĚŽE A AKTIVITY

Jde o úvodní aktivitu na začátku každého školního roku. Nemusí být vyloženě násilnou formou, tedy písemnou prací. Pokud žáky neznáme, je vhodné zadat téma a nechat je vypracovat prezentaci. Po zkušenostech z výuky bychom nedoporučili dávat témata typu „kyberšikana“, ale zaměřit se na viry, hoaxy a další, společensky neškodná témata. Vyhneme se tak překvapení, kdy žáci zkoušejí šokovat své okolí a na promítací ploše se objevují nejrůznější fotografie a videa, překračující hranice zákona.

SOUTĚŽE

Celorepublikově a pro všechny skupiny lze doporučit účast na Kybernetické soutěži pořádané klubem AFCEA. První kolo je zaměřeno na obecné, spíš teoretické znalosti tématu, které jsou ověřovány formou on-line otázek. Probíhá vždy na podzim, začíná v září a končí koncem října. K tomu patří i web s názvem Cybersecurity.

Pokud není zájem o zapojení do několikakolové soutěže, lze k mapování znalostí ve třídě využít například soutěž serveru „Kraje pro bezpečný Internet“ na tomto odkazu. Soutěž běží vždy v říjnu.

Žáci, kteří na střední školu právě nastupují, obvykle nepostoupí do vyššího kola soutěže. Pokud ano, pak je vhodné zařadit si žáka mezi nadané v dané oblasti a dále se mu věnovat – přinejmenším proto, aby nezačal z nudy prolézat školní síť.

MAPOVÁNÍ BEZ SOUTĚŽÍ

Pokud chcete zvolit atraktivnější formu testování, můžete se zaregistrovat na serveru Kahoot It! a založit vlastní test nebo využít testy už připravené.

Pokud budeme zadávat prezentace, osvědčilo se nechat žáky buď zvolit téma, nebo prostředek. Mohou tedy využít PowerPoint, Prezi, Google Site nebo Prezentace Google. Motivací jsou práce Web Rangers – do soutěže se není třeba hlásit, ale dá se tady najít kvalitní inspirace.

Výsledkem by měl být poznatek, jak žáci zvládají pojmy a postřehy. Určitě nejde o mapování klimatu třídy nebo o zjištění, kdo z žáků navštěvuje lechtivé stránky nebo nemá doma počítač. Pokud zjistíme problém výchovného typu, budeme další výklad a postup konzultovat se školním metodikem prevence. Tam, kde jsou potíže rázu závadového chování, je vhodné využít zdroje zaměřené na konkrétní problémy, například film „Na hory“ nebo další podle tématu.

TESTY

Samozřejmě nám nic nebrání udělat běžné testování pomocí třeba Google Forms, nebo si do třídy pozvat odborníka a požádat o mapování klimatu třídy a bezpečnostních slabin. Nic z toho nás ale nezbaví odpovědnosti za to, že by žáci měli zvládnout všechny oblasti práce v požadované kvalitě výstupů. Pokud rádi používáme techniku BYOD (každý žák má své zařízení), můžeme využít k testování a sledování šikovnosti třeba Quizlett.

BEZPEČNOST NA POČÍTAČI

PRÁCE S TECHNIKOU A FYZICKÝM ZABEZPEČENÍM A ÚVOD DO SÍTÍ

I v IT oborech je dobré si uvědomit, že ne každý se věnuje problematice jednotlivých koncových zařízení a je dobré si zopakovat základy práce na počítači. Opět nám mohou pomoci testy – například ze stránek učitele z Moravy, RNDr. Vladimíra Vaščáka. Najdete je na adrese Vascak.cz

Pokud učíme první ročník oboru, který má malou hodinovou dotaci (učební obor s dotací 1 hodina v každém ročníku), využijeme k obecné digitální hygieně materiál Sedua Sociální sítě pro začátečníky pro základy bezpečnosti v kyberprostoru. Dále lze žákům zadat eLearning ze serveru Kraje pro bezpečný internet. kde zvolíme některé z pokročilejších kapitol. Tímto v podstatě naše práce končí a pouze v jednotlivých tematických celcích vždy připomeneme zásady správného chování. Pokud ale máme žáky čtyřletých oborů nebo gymnázií, je nutné problematiku rozšířit tak, aby odpovídala jejich nárokům.

A CO TEDY S POČÍTAČEM?

Jednoduchou hru s ukázkou funkce Turringova stroje ukážeme na Doodle.
Tato ukázka se nám bude hodit i později při vysvětlování principů útoků. Pokud ji v hodině použijeme k samostatné práci, je možné výklad o historii počítačů a jejich bezpečnosti doprovodit článkem ze série „Úsvit hackera“. V článku Jak hacknout kasino je vidět nejen motivace, ale i způsob uvažování hackerů ještě před tím, než se stali hackery. Zabezpečení jednotlivých složek ukazuje simulovaná hra, která je k najití na serveru RVP. Další hry najdete v tomto článku. Je nezbytné jednotlivé balíčky stáhnout a naistalovat a musíme si tedy ověřit před výukou, že programy budou funkční.
Na střední škole se už nemusíme bát využít tutoriály různých redakcí. Většinou jsou psány napůl laicky a rozebírají témata popořadě. Třeba na Lupa.cz Samořejmě počítače nejsou jen s Windows, ale jde o nejběžnější systém.

V této fázi by už žáci měli souběžně s dovednostmi o prolomení základní obrany počítače povědomí i o tom, jak se na podobné pokusy dívá Trestní zákoník. Nejjednodušší pro učitele je navštívit stránky Policie ČR nebo pro ty zvídavější prostudovat velmi dobrou publikaci JUDr. Jana Koloucha Cybercrime, která je ke stažení na stránkách knihovny CZ.NIC. Jde ale o celkem obsáhlé, i když poutavé čtení.

JAK FUNGUJE SÍŤ?

Můžeme použít klasické, i když starší, video. Většinou se líbí. Jmenuje se

Válečníci sítě

Ukazuje přechod z vnitřní podnikové sítě do volného prostředí Internetu a zpět včetně základních bezpečnostních prvků včetně firewallu, portů a proxy serveru. Dobrým doplňkem tohoto videa je práce se serverem Paranoia.cz, která umožňuje otestovat většinu rizikových míst a podívat se na porty a domény pěkně z blízka. Už při ukázce práce je vhodné upozornit,

že server nemá HTTPS – pokud by byl zabezpečen, diagnostické nástroje by nefungovaly. Je zde i možnost testování pomocí Eicare – i když pouze jedné mutace. Na stránkách Eicare.org nebo na Wikipedii najdeme další informace.

ŠIFROVÁNÍ

V oblasti bezpečnosti počítačových sítí se už můžeme setkávat s nejrůznějšími materiály, které mohou a nemusí být pro žáky zajímavé. Více, než kdy jindy platí fakt, že je nutné nejprve dobře stanovit úroveň toho, co žáci umí a jsou schopni obsáhnout, a pak teprve začít s výkladem.

Pro úplně začátečníky se v nižších ročnících dají využít materiály z Khanovy akademie. Materiál je hodně obsáhlý, ale zábavný a poutavý. Lze z něj vybrat jen pár ukázek, které pak propojíme s jinými zdroji – povídání o Caesarově šifře spojíme s výkladem o Enigmě a přidáme další text z Úsvitu hacekrů nebo necháme žáky zahrát hru, která je sice dětská, ale je dobrým druhem alternativní výuky. Fungování sítě pak jenom zopakujeme a dodáme poučení o správném rozdělení rolí a přístupů.

Jiná věc je, pokud máte ostřílené vlky ze čtvrtého ročníku, ještě navíc se specializací nebo zaměřením na IT. Tam pak pomohou sofistikované materiály, které je nutné sladit se znalostmi z předmětu Počítačové sítě. Samozřejmě i pro tyto skupiny se materiály najdou, pěkný elaborát je například tady nebo tady.

Pořád je nutné mít na paměti, že se bavíme pouze o technické stránce věci. Nejsou zde zahrnuty softwarové úpravy, nastavení práv a hesel a další bezpečnostní záležitosti. Pohybujeme se v nejnižších vrstvách, kdy bez jejich řádného zabezpečení nemá smysl budovat nic nad nimi.

DETEKCE ÚTOKŮ NA SÍTI

Pokud tedy učíme ostřílené IT vlky, můžeme jim také třeba pustit video o detekci anomálií:

https://www.youtube.com/watch?v=_W9AYaHf7po

ale pak musíme počítat s tím, že jim ukážeme i některé nástroje, používané k průzkumu sítě. Jedná se například o AMAP, NMAP nebo program WireShark. K poslednímu můžeme najít pěkný článek na SWMAG. AMAP a NMAP si musí každý nastudovat sám – oba prográmky jsou vcelku triviální.

Pokud učitel má možnost a je si na 100% jistý, že žáci plně pochopili pojem „nepodmíněný trest“, může pustit video, které je na celou hodinu a velmi pěkně ukazuje všechny zde vyjmenované nástroje. Autorem je Tomáš Čejka.

https://www.youtube.com/watch?v=gorsF21-hqY

V případě NMAPu lze vyjít z manuálu, který je ve slovenštině.

Pro ty méně statečné existuje na Google Play i aplikace NMAP tutorial, která pracuje off line, ale opět se musí instalovat.

Protože svět se vyvíjí, je dobré sledovat třeba i oblast Internetu věcí. Vhodné stránky jsou třeba s3c.

Tím jsme se dostali ze světa hardware a sítí, tedy ze světa relativně bezpečného, kde si všechno nastavíme podle manuálů a ve většině případů nám to pak funguje, do světa sociálních manipulací, obtěžování a složitého nastavování přístupů oprávnění, hesel a práce s koncovými uživateli – tedy do světa takzvané „měkké bezpečnosti". A ta pravá práce nám začíná…

SOCIÁLNÍ BEZPEČNOST

JAK SI PORADIT S NOČNÍ MŮROU

Pokud učíte celý předmět „Kybernetická bezpečnost", pak je možné využít již připravený materiál – KISK MUNI nabízí hotový eLearning s velmi dobrým rozsahem. Nevýhodou je nutnost „přeložit" texty do podoby, srozumitelné středoškolákům, ale ve vyšším ročníku tento problém odpadá a lze si jednotlivá témata připravit na příslušný počet hodin. Kurz je tady. Není zaměřen technicky, ale poskytuje velmi pěkně uspořádaný průřez celým komplexem bezpečnosti a ochrany dat a informací. V IT zaměřených oborech jej tedy zkombinujeme s kurzy CISCO – obecný úvod a bezpečnostní moduly nastavování CISCO sítí a dostaneme ucelený průřez kompletní tématikou.

BEZPEČNOST NA INTERNETU

Pokud chceme prorazit s tímto tématem na střední škole a nebýt cílem opovržení a poznámek typu „To jsem viděl milionkrát", musíme zvolit neotřelý přístup. S běžnými filmy a servery nevystačíme.

V první řadě lze projít server E-bezpečí sekce Věda a výzkum a podívat se, co z toho zaujme. Další výklad pak bude vycházet z pokročilosti žáků, ale je dobré se zaměřit na zranitelnosti v rámci spíše technických dovedností.

Ve druhé řadě se nabízí praktická ukázka toho, jak vlastně fungují vyhledávače – klasicky přes Google Hacking. Materiál na přípravu najdete zde a je nutné si příkazy vyzkoušet, než necháte žáky řádit.

Další varianta je ta, že žákům ukážete nastavování vlastností adresního řádku. Pokud používáte Mozzillu, máte návod tady a odtud už je pouze krůček k poznatku, že do adresního řádku můžeme zadat příkaz...a podívat se někam, kam nemáme. Pozor na to, že hodina nesmí být návodná, jinak se žáci vyřádí na školní síti.

A pokud chceme být opravdu zvědaví, pak ve skriptech najdeme celá penetrační prostředí i s výkladem. To už je pouze pro opravdové nadšence.

HESLA

Pokud ale máte málo času, pak je nutné věnovat se jednotlivým bezpečnostním prvkům postupně. A současně musíte předpokládat, že žáci již něco znají – a obvykle viděli všechna ta pěkná a návodná videa z běžných serverů typu e-Bezpečí. Dá se ale předpokládat, že žáci nechodí dobrovolně na server Matematika.cz, kde je pěkný článek i s popisem běžných útoků.

Bohužel nejčastější útok na heslo je založen na pozorování – což se málokde uvádí. Povídání o tom, že na monitor by nemělo být vidět z chodby nebo z okna a k čemu slouží zamykání obrazovky a spořič můžeme spojit s výkladem o ergonomii počítačového pracoviště.

Ideální hodina pak vypadá tak, že žákům předáme vědomosti z článku, necháme je vytvořit „silné“ heslo a toto heslo pak necháme otestovat včetně označení slabin hesla, například na stránce https://howsecureismypassword.net/ a řekněme, že první, kdo vymyslí neprolomitelné heslo, může dostat jedničku. Pozor jen na to, že to obvykle netrvá moc dlouho. Seznam nejčastěji používaných hesel najdeme pomocí vyhledávače Google. Každý rok se aktualizuje a každý rok vedou stejná nebo hodně podobná hesla typu 123456.

SOCIÁLNÍ INŽENÝRSTVÍ

Začíná – bohužel pro nás – znalostí pojmů osobní údaje, citlivé údaje… a posouvá nás do úrovně komunikace. Na střední škole by už žáci měli umět rozlišit manipulativní text a k tomu mohou pěkně přispět články na serveru, který svým názvem evokuje Rusko a na první pohled není nijak výjimečný. Web Illinčev/psychologie má články v této kategorii ukazují pěkně manipulační techniky na webu i mimo něj. Doporučuji nenechat tam žáky příliš prolézat, spíše vybrat jedno nebo dvě témata a ta probrat podrobněji.

Podobnému tématu se věnuje i další portál, který má velkou část materiálů v češtině: The Web We Want – Evropský metodický projekt cílený na osvětu v rámci užívání Internetu a jeho služeb. Nabízí příručku pro teenagery (CZ) i pro učitele (EN), plány lekcí a pracovní listy ihned vhodné k realizaci.

SERVERY PLNÉ HAVĚTI

Najdeme na www.hoax.cz kde je celá škála věciček, o jejichž existenci řada lidí nemá tušení a to i přes osvětu, provedenou dříve. Tady můžeme ukázat hoaxy, nigerijské dopisy, malware a další věci, obvykle s ukázkami a vyjádřením odborníků.

K povídání o virech patří neodmyslitelně oblíbené techniky baiting, pretexting a phishing, které jsou pěkně ukázány ve videích firmy Eset.

https://www.youtube.com/playlist?list=PL-gT1FSSbRuyVj9lqr8IJEethJvarFlX6

koneckonců věta „Mě se to stát nemůže“ je opravdovým strašákem každého správce sítě.

Materiály, seřazené pro potřeby vzdělávání na serveru E-bezpečí najdete na tomto odkaze.

ANTIVIRY

Pěkný, vcelku komplexní materiál, najdeme v souboru *.pdf není ovšem k použití napřímo, je nutné jej pro potřebu výuky zpracovat.

Pokud máme žáky pokročilejší a se zvídavými dotazy, tak řadu informací najdeme – my i žáci – v Antivirovém centru.

METODA CLIL

Je technika výuky, která kombinuje české a anglické jazykové protředí. Pěkné ukázky této výuky jsou na stránkách učitele Pavla Hodála, který má na svém webu Ty brďo řadu ukázkových příprav.

Pro pokročilé žáky využijeme materiály Google.

A můžeme přidat i texty a kurzy z Akademie Microsoftu. Tady je ovšem nezbytné, aby učitel sám kurz nejprve prošel. Žáci třetích a čtvrtých ročníků středních škol už mohou s kurzem pracovat samostatně, ale učitel musí být v každém okamžiku k dispozici a musí vědět, co se v kurzu děje.

A některé souhrnné weby a projekty v oblasti kybernetické bezpečnosti:

Materiály, seřazené pro potřeby vzdělávání:

E-bezpečí - rozsáhlý projekt včetně virtuální sociální sítě

Buď safe online – soubory videí od Avastu

Kraje pro bezpečný Internet - rozsáhlé elearningové kurzy, zakončené testy. Využitelné do výuky, k mapování třídy i pro učitele.

Pokud už máme podezření, nebo dokonce jistotu, že ve třídě dochází k porušení zákona je po zmapování stavu ve třídě vhodné dohodnout přednášky s příslušným zaměřením. V této tabulce lze zvolit odpovídající organizaci a téma přednášky.

Další informace určitě poskytne vedení škol, které pilotují obor Kybernetická bezpečnost. Jsou to Smíchovská střední průmyslová škola a Střední škola informatiky, poštovnictví a finančnictví . Samostatný předmět Kybernetická bezpečnost učí např. i Střední škola technická a ekonomická Brno a další školy mají obor zařazen v rámci výuky do více předmětů.

PRO OPRAVDU ODVÁŽNÉ

Je nutné důkladně vysvětlit rozdíly mezi hackery. Nejen barvu klobouku, ale probrat zákon, jeho porušení a důsledky… a pak se můžeme mrknout na stránky Hacking kurzů a začít čarovat. Blogy tohoto serveru obsahují celou řadu zajímavých textů. Samotné lekce jsou ale placené.