

# **Bezpečnostní témata ve výuce na střední škole**

Safety and Security Topics  
in Tuition in Secondary Schools

Lukáš Jakubík

---

Diplomová práce  
2015



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

## **ZADÁNÍ DIPLOMOVÉ PRÁCE**

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Lukáš Jakubík**  
Osobní číslo: **A13372**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **kombinovaná**

Téma práce: **Bezpečnostní témata ve výuce na střední škole**  
Téma anglicky: **Safety and Security Topics in Tuition in Secondary Schools**

Zásady pro vypracování:

1. Provedte analýzu požadavků několika rámcových vzdělávacích programů pro výuku oborů ve vztahu k bezpečnosti.
2. Teoreticky pojednejte o potřebném obsahu vzdělávacích materiálů.
3. Analyzujte míru požadavků na vědomosti a schopnosti ve vztahu k současnému pojetí bezpečnostních rizik ve společnosti.
4. Připravte studijní materiály z oblasti bezpečnosti a teoretické informatiky pro studenty středních škol.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **BALABÁN, Miloš, Jan DUCHEK a Libor STEJSKAL.** Kapitoly o bezpečnosti. Vyd. 1. Praha: Karolinum, 2007, 428 s. ISBN 978-80-246-1440-3.
2. **DOSEDĚL, Tomáš.** Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, ix, 190 s. ISBN 80-251-0106-1.
3. **BRABEC, František.** Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001, 400 s. ISBN 80-86445-04-6.
4. **ANDRESS, Jason a Russ ROGERS.** The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Amsterdam: Elsevier, 2011, xviii, 171 s. ISBN 978-1-59749-653-7.
5. **SAK, Petr a Jiří MAREŠ.** Člověk a vzdělání v informační společnosti. Vyd. 1. Praha: Portál, 2007, 290 s. ISBN 978-80-7367-230-0.
6. **ZOUNEK, Jiří a Petr SUDICKÝ.** E-learning: učení (se) s online technologiemi. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2012, xix, 226 s. ISBN 978-80-7357-903-6.

Vedoucí diplomové práce:

**doc. Mgr. Milan Adámek, Ph.D.**

Ústav bezpečnostního inženýrství

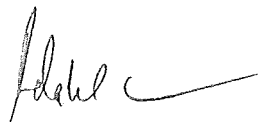
Datum zadání diplomové práce:

**12. ledna 2015**

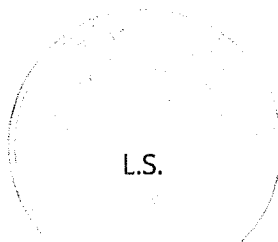
Termín odevzdání diplomové práce:

**15. května 2015**

Ve Zlíně dne 6. února 2015



doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



doc. RNDr. Vojtěch Křesálek, CSc.  
*ředitel ústavu*

### **Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejména § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### **Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor;
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Brně 15. května 2015

Lukáš Jakubík

## **ABSTRAKT**

Tato práce je přehledem požadavků v oblasti informačního bezpečí a bezpečnosti v prostředí edukace na středních školách, v konkrétních studijních oborech. Opírá se o moderní vzdělávání, pojednává o motivaci, dobré praxi. Přináší několik studijních materiálů a prezentací pro žáky gymnázii a středních škol – bezpečnost komunikace, šifrování, elektronický podpis.

## **KLÍČOVÁ SLOVA**

bezpečnost IT, ochrana dat, moderní vyučování, katalog požadavků, RVP

## **ABSTRACT**

This thesis is an overview of the requirements in the area of information security and safety in education in secondary schools in specific fields of study. It relies on modern education, discusses the motivation, good practice. It brings some study materials and presentations for pupils grammar schools and high schools – communication security, encryption, electronic signature.

## **KEYWORDS**

IT security, data protection, modern teaching, state requirements catalog, RVP

## **PODĚKOVÁNÍ**

Děkuji mému vedoucímu doc. Milanu Adámkovi, děkanovi, jeho životní příběh, začátky v učitelství jsou pro mě nevídanou inspirací.

A ďakujem aj Júlíi, že mi bola spolužiačkou, že ma v tomto štúdiu sprevádzala.

*Mým studentům, minulým i těm příštím.*

# OBSAH

<b>I</b>	<b>TEORETICKÁ ČÁST.....</b>	<b>10</b>
<b>1</b>	<b>MODERNÍ VZDĚLÁVÁNÍ A JEHO ASPEKTY.....</b>	<b>11</b>
1.1	Učení.....	11
1.2	Motivace.....	12
1.3	Maslowova hierarchie potřeb.....	14
1.4	Edukace.....	17
1.5	Edukační prostředí.....	19
1.6	Edukační konstrukty.....	20
<b>2</b>	<b>KURIKULÁRNÍ DOKUMENTY.....</b>	<b>22</b>
2.1	Znalostní společnost.....	22
2.2	Národní ústav pro vzdělávání.....	23
2.3	Rámcový vzdělávací program.....	23
2.4	Školní vzdělávací program a reálná situace.....	25
<b>3</b>	<b>OBSAH VZDĚLÁVÁNÍ A STAV JEHO OVĚŘOVÁNÍ.....</b>	<b>28</b>
3.1	Státní maturita.....	29
3.2	Cermat a jeho odraz ve společnosti.....	29
3.3	Katalogy požadavků.....	31
<b>II</b>	<b>PRAKTICKÁ ČÁST.....</b>	<b>33</b>
<b>4</b>	<b>ANALÝZA POŽADAVKŮ.....</b>	<b>34</b>
4.1	RVP pro gymnaziální vzdělávání.....	35
4.2	RVP pro informační technologie.....	37
4.3	RVP pro bezpečnostně právní činnost.....	40
<b>5</b>	<b>STUDIJNÍ MATERIÁLY.....</b>	<b>43</b>
5.1	Moderní a bezpečné edukační prostředí.....	44
5.2	Počítačová bezpečnost.....	47
5.3	Firewall.....	47
5.4	IDS, IPS.....	48
5.5	Kryptografie pro SŠ.....	49
5.5.1	Symetrická kryptografie.....	50
5.5.2	Asymetrická kryptografie.....	50
5.5.3	Praxe.....	52
5.6	Elektronický podpis pro SŠ.....	54
5.6.1	Pojmy.....	54
5.6.2	Praxe.....	55
5.6.3	Vydávání důvěryhodného certifikátu.....	55
<b>6</b>	<b>ZÁVĚR.....</b>	<b>57</b>
<b>7</b>	<b>BIBLIOGRAFIE.....</b>	<b>59</b>
<b>8</b>	<b>PŘÍLOHY.....</b>	<b>61</b>
8.1	Počítačová bezpečnost.....	62
8.2	Firewall.....	66
8.3	IDS, IPS.....	70
8.4	Elektronický podpis.....	72



## ÚVOD

Vstoupili jsme do doby, kdy svět kolem nás netvoří už jen zdi, lidi kolem, prostor, kam naše oko dohlédne. Nenápadně, pomalu, ale zcela jistě a čím dál více nás zasahuje i svět virtuální – takový, kde zdi neplatí, lidi kolem nás už neznáme. Nechceme předpovídat cokoli hrůzostrašného, jen chceme přimět k zamyšlení, zda-li opravdu víme, co za nebezpečí na nás číhá? Uvědomujeme si rizika?

Necháme to bez odpovědi, na teď, ať si každý domyslí, co ho na Internetu děsí.

My, vysokoškoláci jsme už velcí, dospěli jsme, ale co ty děti, co ti mladší? Nás asi učil život, možná jsme s technologiemi a jejich překotným rozmachem společně rostli, dospívali. Naučili nás na telefony, takové, co musíme mít s sebou, naučili nás nechodit do banky, prý se to dá z Internetu, a emailovat už umíme. Nastěhovaly se k nám domů.

Ale znova se ptáme, jak se to učí děti? Kde? Kým? Je vzdělávací systém nastaven tak, aby se vedle matematiky, dějepisu, stovek knih z češtiny věnovala patřičná pozornost také bezpečnostním tématům, těm co souvisí s informačními technologiemi? Převzaly si děti ze škol také to, co je ochránit od všech hrozeb – vlastní rozum, rozum v hrsti, se kterým se neztratí ani ve světě změn.

Od škol očekáváme, že naučí vše, co je potřeba, že je tam dětem fajn, že tam chodí rády. A také proto se v této diplomové práci věnujeme rozsáhlému kontextu vzdělávání, motivace, něco málo z psychologie až po ta bezpečnostní témata – od ochrany dat, chování uživatelů, bezpečnosti sítí, přes ochranu komunikace šifrováním až po samotný elektronický podpis. Například tyto témata jsme hledali v závazných dokumentech ministerstva školství. Bud' jsme našli, nebo jsme to patřičně vytkli a také nabídli řešení vlastní.

Součástí této diplomové práce jsou 2 studijní texty a řada prezentací k dalšímu použití v edukaci těch bezbranných, určitě moc pilných středoškoláků.

## **I. TEORETICKÁ ČÁST**

## 1 MODERNÍ VZDĚLÁVÁNÍ A JEHO ASPEKTY

Vzdělávání je proces celoživotní, setkáváme se s ním od narození až do vysokého věku, provází nás na každém kroku, v každé životní etapě, učíme se z každého podnětu. Bylo nepřesné říct, že se učíme jen ve škole od učitelů, vliv na naše vědomosti, názory a postoje má každá životní situace, možná každý rozhovor s kamarádem.

My zde budeme rozvádět možnosti moderního vzdělávání, základní pojmy jako učení, výchova ale také motivaci, neméně se věnujeme modernímu vyučování jako takovému, aby ve výsledku bylo dosaženo *vzdělanosti* – kvalitního vzdělání.

### 1.1 Učení

Podle Pettyho knihy Moderního učení [2008, s. 35] *je učení skrytý a nezjevný duševní proces*, který učitel nijak přímo neřídí, nemůže ho zcela ovládat. Žáci si postupně vytvářejí osobní verzi probírané látky a požadovaných znalostí. Učení je jakýmsi způsobem přibližování, proto zpočátku bývá porozumění žáka nedokonalé a nepřesné. Proto je důležité dát mu čas a dostatek prostoru k zafixování, nasledovat řadu didaktických postupů.

Během učení se vytváří několik verzí učiva, jakoby si vzdělávaný sám zkoušel vytvořit vlastní verzi probírané látky a dosadit ji do kontextu dosavadních zkušeností z jeho světa. Ostatně toto je nejlepší forma získávání nových znalostí – vycházet od známého k neznámému. Chceme vsazovat učivo do reality, příkladů, ke kterým se vytváří vztah, posléze si vytváříme vzpomínky. V procesu učení dělají žáci pokroky – opravují své chyby a získávají další znalosti a dovednosti, korigují svoji verzi učiva, a tak se stále přibližují ideálnímu porozumění.

Tento proces vyžaduje tzv. *korigovanou praxi*, nestačí když učitel jen opravuje žáka – žák sám musí opravovat svou verzi porozumění. *Učení je také proces, při němž žák řeší problémy a přitom jeho úkolem je vytvořit si osobní správnou verzi porozumění určitým dovednostem a znalostem* [Petty, 2008, s. 35].

## 1.2 Motivace

Každá rozsáhlejší psychologická, pracovní ale i pedagogická literatura popisuje také motivační atributy v jakékoliv lidské činnosti, jakým způsobem člověka, zaměstnance, žáka podporovat v dosahování lepších výsledků, vnitřně startovat jeho motory k lepší práci, mluvíme o *správné motivaci*.

Je nelehký úkol vzdělávaného přesvědčit o smyslu a účelu získání nových vědomostí, jak ho průběžně povzbuzovat, vést k pokroku, udržet a neztratit. Petty [2008, s. 35, 37, 54, 62] uvádí jako *silný motivační faktor pocitové prožívání*. Motivovaný, v našem případě řekněme žák, cítí, jak v hodině něčeho dosáhl, že se mu za jeho práci dostalo uznání. Provází ho také existenční obavy, že pociťuje stres, strach z neúspěchu. Později v životě, ve vyšším věku, v jiných životních situacích se za motivační považuje také konečné dosažení vyšších cílů, nalezení smyslu naší činnosti. Když to ukážeme na výsledcích vzdělávání – jakého vzdělání jsem dosáhl, k čemu konkrétnímu učivo v životě bude, jaké zvýšení pracovních dovedností poskytne, v čem rozvine mojí osobnost?

*Motivace je možná pouze tehdy, když mezi výkonem a výsledkem existuje jasně vnímatelný a použitelný vztah, a je-li výsledek považován za nástroj uspokojení potřeb* [Armstrong, 2002, s. 164].

Dále můžeme motivační faktory rozlišit na vnější – tedy peníze nebo odměny a vnitřní – vlastní pocity a uspokojení ze seberealizace, ze získání dobrého pocitu, že člověk vykonal to, k čemu má schopnosti a jistý potenciál. Více o hierarchii potřeb v Maslowově pyramidě v kapitole 1.3.

Často se bohužel setkáváme s nízkou mírou aktivity až lhostejností účastníků vzdělávání, někdy také na straně vzdělavatelů, že v tomto procesu nevidí smysl, užitečnost, začíná se objevovat letargie až nechuť. Ovšem plejáda těchto pocitů, pořád jsme na úrovni značně emocionální, je už za hranou demotivace a člověka, který v nabízeném nevidí smysl, účel, přidanou hodnotu, lze do procesu získat jen stěží. Nemá vnitřní motivaci.

Za účinnou motivaci se považuje *pochvala*, základní psychologická potřeba člověka, uznání. Rozlišuje se ale pochvala za dosažený úspěch a pochvala udělená za snahu. První je znakem postupu, často opomíjená součást jakékoliv dokončené činnosti, ta

druhá může být zrádná v tom smyslu, že jenom snaha k naučení nestačí. K dosažení stanovených vzdělávacích cílů je potřeba více než snaha spíše efektivní úsilí. Podle Armstronga [2002, s. 164] je efektivní úsilí podmíněno schopnostmi, tedy že přece jenom vzdělávaný, motivovaný člověk má předpoklady a osobnostní charakteristiky stanovených cílů dosáhnout. Je důležité také kriticky zhodnotit a dát vědět, které znalosti jsou nezbytné pro další pokrok, průběžně je ověřovat, motivovat k výkonům pod hrozbou špatné známky. Poté další včasná a častá pochvalu za snahu motivuje i méně šikovných. Pochvala jako taková nebo jiné ocenění se musí dostavit co nejdříve poté, jak bylo úspěchu dosaženo, nesmí však přetrvávat nezdravě dlouho v podvědomí, že by motivovaný usoudil, že takto a tolik už stačí, víc není nic potřeba.

Míru poskytované chvály a oceňování vyrovnává *konstruktivní kritika*. Chvála nepůsobí sama o sobě, rozhodující roli tu hraje emocionální reakce na ní. Pro vznik správného motivačního efektu je podstatné, aby si žáci vážili úsudku učitele, věřili tomu, že pochvalu myslel vážně a sami připisovali oceněné práci jistou hodnotu [Petty, 2008, str. 63]. Ve většině učebních prostředí se zpětnou vazbou je patrná jistá konkurence, vzájemné srovnávání. Nelze proto některé jedince jen chválit, jiné jen kritizovat, protože jakýkoliv emocionální projev vždy ovlivňuje naslouchající publikum jako celek. Žáci silně prožívají nespravedlnost, když nejsou dodržena stejná pravidla, když kritiku cítí jako nezaslouženou a neúměrnou, snad nepřekonatelnou, proto musí být výhradně konstruktivní, vést k dosažitelným cílům. Žák by si z vyřčené kritiky měl být vědom svého pochybení a způsobu, jak to napravit, kritika se musí týkat obsahu a provedené činnosti nikoliv činitele, nesmí být jakkoliv osobní.

Motivační faktory v širším kontextu, si lze zapamatovat podle Pettyho [2008, s. 53-54] mnemotechnické pomůcky, prvních písmen slova FOCUS:

- Fantazie – zajímavost a zábavnost hodin, atraktivita a spektrum činností souvisejících s výkladem, osobní rozměr a souvislost s životem, návaznost na současné, skutečné události ve světě, zapálenost učitele pro téma, vládnoucí dobré vztahy;
- Ocenění – průběžné a včasné pochvaly, povzbuzení, známky, odznáčky;

- Cíle – dosažitelnost vytčených cílů, touha je dosáhnout, přiměřený strach z důsledků, pokud nebudou splněny, výzva k odpovědnosti za své studium;
- Úspěch – vyhovující úroveň obtížnosti a tempo, program vyučování, který odpovídá dosavadním zkušenostem žáků;
- Smysl – reálná užitečnost, další přesah do života, finanční a osobní hodnota získání nové dovednosti.

Zde je nutno shrnout, že motivace není samo spásná, protože nedokáže přebít některé negativní činitele v obecně nepředvídatelném *edukačním prostředí*, ať už jde o školu, rodinu, pracoviště nebo jiný okruh lidí se stejným sociokulturním postavením (dělníci, vojáci, sportovci, lékaři...), kteří proces učení nemalou mírou ovlivňují a celé prostředí různě negativně působí na všechny aspiranty o vědění.

Někteří se mylně domnívají, že motivace má svůj smysl sama o sobě. Motivace napomáhá procesu učení: zvyšuje pozornost, duševní úsilí i odhodlání čelit obtížím. Jestliže je prostředí hlučné, rozptylující, může být obtížné udržet pozornost, pak snaha a odhodlání opadnou, i když byla motivace sebevětší.  
[Petty, 2008, s. 52]

### 1.3 Maslowova hierarchie potřeb

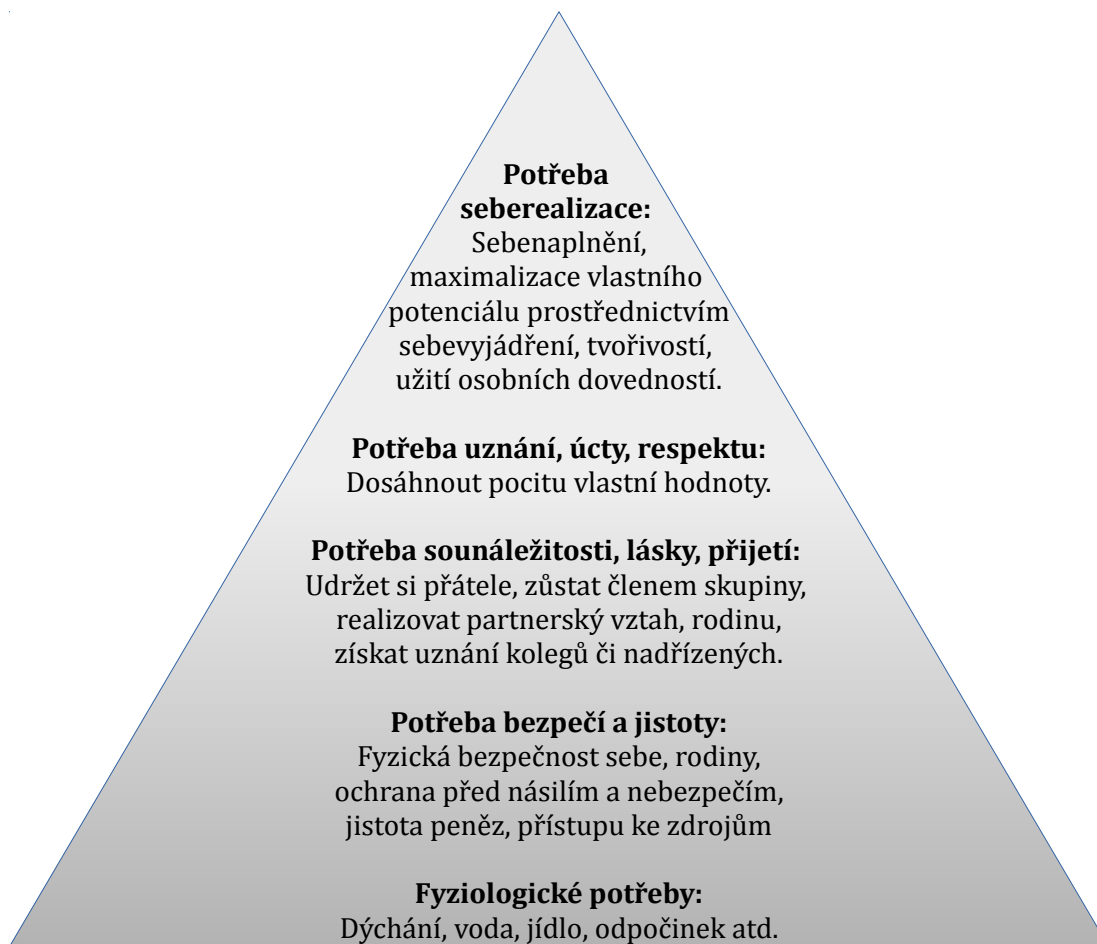
Abraham Maslow (1908 – 1970) byl americký psycholog, který stál kolem roku 1954 za teorií *hierarchie lidských potřeb*. Jde o obecně vyjmenované lidské potřeby, jejich kategorie, které musí být naplněny, uspokojeny postupně tak, aby se dosáhlo vyšších cílů. Jsou uspořádány hierarchicky tak, že alespoň částečné uspokojení nižších potřeb, vede k realizaci méně naléhavých vyšších potřeb, viz obrázek 1. Maslow stanovil pět kategorií potřeb:

1. fyziologické procesy,
2. potřebu bezpečí,
3. potřebu sounáležitosti,
4. potřebu uznání,
5. potřebu seberealizace.

Z čehož máme skupinu nedostatkových potřeb (1., 2., 3., 4.), tedy deficitní, omezující, které musíme naplňovat z vnějších zdrojů a skupinu růstovou (5.), která

nás může posunout dál, vytváří nové produkty, realizuje naše záměry. Toto můžeme uplatňovat v jakékoliv naší tvůrčí činnosti v průběhu života. Např. i vzdělávání začíná odstraněním hladu, nastavením klidu, sjednocením určitého kolektivu, průběžným oceňováním snah až po úspěšný průběh učení, konečné získání nových dovedností. Jak bylo uvedeno v kapitole 1.1, učení je tvořivý proces, proto ho lze chápat i jako jistou seberealizaci té nejvyšší růstové potřeby, aby došlo k sebenaplnění.

Maslowova teorie motivace tvrdí [Armstrong, 2002, s. 163], že v případě uspokojení nižší potřeby se stává dominantní potřebou potřeba vyšší a pozornost jedince je pak soustředěna na uspokojení této vyšší potřeby. Potřeba seberealizace však nemůže být uspokojena nikdy. Maslow uvedl, že *pouze neuspokojená potřeba může motivovat* a aktuálně dominantní potřeba je největším motivátorem toho-kterého chování jedince – hladový se jde najíst. Nižší potřeby naopak pořád existují, i když jako motivátory dočasně usnou, a lidé se k dříve uspokojeným potřebám soustavně vracejí, aby je oslabily, dokrmily. Naopak vyšší potřeby jejich naplněním na své intenzitě spíše sílí, chceme být chváleni víc a víc, realizujeme se a tvoříme bez zastavení.



Obr. 1: Maslowova pyramida potřeb, inspirováno [Petty, 2008, s. 51] a doplněno.

Maslow do jisté míry pyramidu sám zpochybnil z toho důvodu, že lidi jsou neskutečně individuální a mají různé priority, své osobní potřeby, které nelze kategorizovat ani uspořádat hierarchicky. Ne všechny potřeby mají stejnou důležitost pro každého jednotlivce.

Podle Armstronga [2002, s. 162] je základem motivačních teorií přesvědčení, že neuspokojená potřeba vytváří napětí a stav nerovnováhy. K opětovnému nastolení rovnováhy je potřeba rozpoznat cíl, který tuto potřebu uspokojí. Situace je o to komplikovanější, že chování lidí závisí od prostředí, ze kterého vyšli, na výchově a dosavadním životě i na jejich současné situaci. Obecně platí, že nejsme schopni nalézt jednotný cíl/prostředek na uspokojení té které potřeby pro všechny jedince. A taktéž platí, že čím déle některá potřeba přetrvává, tím se nabízí více cílů/prostředků, kterými ji lze naplnit – uznání partnerem, rodinou, kýmkoliv. Z



druhé strany jeden prostředek dokáže uspokojit i více potřeb – atraktivní auto dopravuje, zajišťuje jistotu přijetí i možnost zapůsobit na okolí.

Zde bychom chtěli poukázat na souvislost s tématem této diplomové práce, a to hledání bezpečnostních témat kdekoliv v životě lidské společnosti, posléze jejich výuku. Podle Maslowa jsou jisté obavy o bezpečí sebe a rodiny v pyramidě již druhou nedostatkovou potřebou. Různá rizika, hrozby nás doprovází v každodenním životě a my zde nabízíme pohled na bezpečnost, jak jí máme vnímat, co všechno do ní může spadat a jak to do svého života převzít nebo se nechat poučit. Samozřejmě se v praktické části nevěnujeme základním principům ochrany zdraví nebo sebeobrany, ale už např. prvotní povědomí o bezpečnostní složkách, uniformovaných nebo i těch tajných zpravodajských (toto předkládáme jako studijní materiál v kapitole 5.3), ve většině společnosti pocit bezpečí zcela určitě navozuje, by navozovat mělo. Např. také otázka peněz a jejich zabezpečení, pochopení principu bankomatů a platebních terminálů je důležitým bezpečnostním tématem, ne každý si je rizik s falšováním vědom, i když se nám může stát při každé manipulaci s hotovostí. Skimming (úprava bankomatu) byla realizována také v ČR, klient banky tak může přijít o svou kartu zcela nepozorovaně.

## 1.4 Edukace

Pokud bychom hledali větší přesah uvedené teorie vzdělávání, hledali bychom odraz v životě celé společnosti, určitě bychom mohli mluvit o obecnějším *pedagogickém pojmu, a to edukaci*. Pokusme se v dalším textu přesně poukázat na vzdělávání v oblasti bezpečnosti, výklad a pochopení bezpečnostních témat, celkovou výchovu k odpovědnému občanovi, člověku, jenž by měl odolat bezpečnostním hrozbám, jak se má chovat bezpečně. Že tyto cíle dosáhneme právě vhodným edukačním působením, vychází už ze samotné definice edukace, zaměříme se na její výklad.

*Edukace je v širším slova smyslu výchova, výchova a vzdělání v rozsahu celého života. Jak vyjmenovává Vlčková [2005] jde o záměrné, cílevědomé a systematické působení na rozvoj jedince, permanentní a celoživotní proces. Je ovlivněn mnoha faktory, zejména edukátory, které v životě potkáváme, edukačním prostředím, ve*

kterém se vyskytujeme. Proto je edukace vždy konkrétní povahy, v určité společnosti, na úrovni této společnosti. Můžeme od ní očekávat mnohostrannou orientaci, s cílem dosáhnout plný rozvoj osobnosti, je součástí života každého z nás, proto je univerzální. Edukací se člověk připravuje na mnohé sociální role, jako občan, pracovník, partner, rodič, uživatel čehokoliv; rozvíjí se jeho fyzické i duševní schopnosti, nabývá vědomosti, dovednosti, kvalifikaci (známe jako vzdělávání, vzdělanost), návyky, schopnosti, vhodné postoje (chápeme jako výchovu). Může uspokojit svoje potřeby a zájmy, tehdy je edukace velmi účinná a rychle posouvá ku předu k *edukačním cílům*.

*Edukační cíl je ucelená představa (ideál) předpokládaných a žádoucích rysů jedince, které lze získat edukací, určuje směr edukačního působení.* [Vlčková, 2005]

Jak tedy lidi něco naučit, o čem dosud neměli tušení?

Podle Prokeše [2000] je předmět obecných pedagogických věd mnohem širší než jen činnost pedagogů ve školách, jak jsme je popisovali výše až manuálovou formou, jak by měli svojí práci dělat. Může jít o přenos dovedností jako je např. jazyk z matky na dítě, trénink, koučink, zlepšování a zvyšování vlastních schopností a celkově působení na lidi, za účelem změn jejich postojů, poučit je, připravit na neznámé, potenciálně nebezpečné hrozby. Těmto činnostem říkáme výchově-vzdělávací, dobré působení vzdělanějšího, obecně tedy *edukační procesy*.

Obecným předmětem jakékoliv edukace ať už dětí, dospělých, a to formou hravou, nucenou, povinnou, placenou, další a další je vzdělávání chápáno jako tzv. *edukační realita*. *Jde tedy o takovou souhrnnou realitu, v níž probíhají nějaké edukační procesy nebo jsou vyvíjeny nějaké edukační konstrukty.* [Prokeš, 2000]

V kapitole 1.6 i praktické části se věnujeme právě těmto edukačním konstruktorům, jako jsou knihy, testy a další učební pomůcky ve smyslu doporučených, ale také povinných materiálů, jenž se používají k dosažení normativních cílů – získat určité vzdělání nebo alespoň povědomí, a to v rovině obecné, tak konkrétní, v našem případě bezpečnostní. Co rámcové vzdělávací programy nabízejí v oblasti bezpečnostních témat, které oblasti jsou státem považovány za nezbytné, které jsou jen doporučené a nakonec, které jsou přehlíženy. Tomuto věnujeme hlubší analýzu v praktické části.

Domníváme se, že naše studium bezpečnostních systémů a technologií poskytnuté fakultou odpovídá požadovanému pemu znalostí a dovedností, aby mohly být předány dál. Znalosti pedagogiky získané v předešlém studiu a nyní z dlouhé praxe pedagoga nás opravňuje být tzv. *edukačními činiteli*.

## 1.5 Edukační prostředí

Nedospělí jsou vychováni světem dospělých, ve kterém se pohybují, kterému jsou vystaveni. Děti se učí od rodičů, žáci od učitelů, kamarádů, zaměstnanci od kolegů. Přijímají se také jisté hodnoty, už od raného dětství ve formě vědomých ale i zcela nevědomých zkušeností, prožitků, jak to bylo v televizi, co dělali kamarádi, rodiče nebo kdokoli v užší rodině. Mluvíme o tzv. *edukačním prostředí*.

Čím je prostředí kvalitnější, tím se dosahuje lepších edukačních cílů. Nemusí jít nutně o předávání vědomostí, stačí mít dobrý pocit, bezpečí a vzájemnosti, který si z tohoto místa odnášíme, ovlivňuje nás po zbytek života. Ostatně jsme v edukačním prostředí škol strávili čtvrtinu až třetinu svých životů a zásadně změnilo naše další chápání životních událostí. Jestli na nás působili lidé vzdělaní, znalí, s jistou mírou entusiasmů pro svoji práci, odnesli jsme si mnohé. Jestli jsme naopak nedostávali žádné větší podněty, zakrněli jsme. Proto je důležité nejen mířit na obsah, ale také na formu předávaných znalostí, formu materiálů, vysvětlování, ověřování. Neméně podstatné je vystupování, chování, vzájemné vztahy v edukačním prostředí, kde musí být všechny negativní společenské jevy razantně potlačeny – šikana, strach, obavy, strádání a další.

Stranou edukačnímu prostředí stojí také podle Prokeše (2000):

- *sociální prostředí* – o stavu rodiny, o vztazích s kamarády, o životní úrovni, zaměstnanosti, takový ten pohled, když se doma rozhlédnu;
- *ekonomické prostředí ve školství* – stav financí ve školství (podíl HDP), počet žáků ve školách, počet a komplexní nabídka oborů vzdělávání, prostředky na pomůcky, na kantory;
- *politické prostředí* – řízení školství, závaznost kurikulárních dokumentů, soukromé školství, placené vysokoškolské studium, ohodnocení a prestiž učitelů a jiné.

## 1.6 Edukační konstrukty

V kapitole 1.4 jsme popisovali *edukaci* a *edukační realitu*, při níž se všichni *edukační činitelé* v jistém prostředí vzájemně obohacují, předávají si znalosti a zkušenosti. Krom takovéhoho lektorského působení je na snaze opřít se také o nějaké *edukační konstruktory*.

Edukační konstrukty jsou podle Prokeše [2000] všechny teorie, modely, plány, scénáře, předpisy a jiné teoretické výtvoř, které nějakým způsobem určují či ovlivňují reálné edukační procesy. Mezi příklady edukačních konstruktů patří:

- Učební osnovy různých vyučovacích předmětů, učební plány různých druhů a stupňů škol, vzdělávací programy a standardy vzdělávání, didaktické testy, školní vysvědčení, různé certifikáty atp. Tedy popisují, předpisují, zavádějí, normují či hodnotí reálné edukační procesy.
- Učebnice školní, učebnice pro samouky, výukové filmy, výukové počítačové programy.
- Instrukce k obsluze různých zařízení, kuchařky s předpisy na zhotovování pokrmů, rady lékaře pacientovi... a mnohé další komunikáty verbální i neverbální, které mají nějakou edukační (poučovací) funkci.
- Veškeré výtvoř pedagogické teorie, knižní monografie, články v pedagogických časopisech, referáty na konference, disertace a diplomové práce zaměřené na pedagogickou problematiku...

Tedy nejde jenom o samotné ukázkové edukační materiály, které by se mohli bezpečnostních témat týkat a jsou obsahem této práce, ale také širší kontext jejich vymezení a kodifikace v různých osnovách, předpisech, plánech – co se v řízeném procesu vzdělávání očekává, kdo to vyžaduje, kdo to zkontroluje. O těchto aspektech pojednáváme v praktické části práce.

Tážeme se, jestli je ministerstvo, nebo jiná centrální organizace, schopna požadavky na bezpečnost zohlednit a edukační konstrukty, učebnice, návody, doplňkové materiály vytvořit?

Jisté snahy jsou zjevné z neziskového sektoru a vysokoškolského prostředí, setkáváme se s projekty překladu ucelených knih<sup>1</sup> od správce národní domény firmy CZ.NIC, náhled obsahu je na obr. 1.6.1.

#### **4. Hackeři a crackeři – 81**

##### **4.1 Hackeři – 81**

- 4.1.1 Kdo je to hacker? – 82
- 4.1.2 Černé, bílé a šedé klobouky – 84

##### **4.2 Hackeři chtějí váš počítač – 86**

##### **4.3 Nástroje hackerů – 86**

- 4.3.1 Skenovací nástroje – 87
- 4.3.2 Prolamování hesel – 88
- 4.3.3 Rootkit – 90

##### **4.4 Voláme bílé klobouky! – 92**

#### **5. Jak poslat SPAM na věčnost – 99**

##### **5.1 E-mail a SPAM – 100**

- 5.1.1 Co je to SPAM? – 100
- 5.1.2 Není SPAM protizákonný? – 101

##### **5.2 Spoofing – 103**

- 5.2.1 Falešné adresy – 103
- 5.2.2 SPAM proxy a relay – 105

##### **5.3 Ťuk ťuk - jak spammeři poznají, že jste doma – 106**

- 5.3.1 Skryté sledování – 107
- 5.3.2 Scavengery a crawlery – 108
- 5.3.3 Je vaše e-mailová adresa na prodej? – 109

##### **5.4 Sociální inženýrství – 109**

##### **5.5 Aby se SPAM do příchozích zpráv nedostal – 110**

##### **5.6 SPIM – 111**

#### **6. Kyberšikana – 115**

##### **6.1 Šikana se přesouvá do digitálního světa – 116**

##### **6.2 Útoky na online reputaci – 117**

- 6.2.1 Frontální útoky – 117
- 6.2.2 Útoky na identitu – 118

##### **6.3 Ochrana reputace – 119**

- 6.3.1 Vygooglujte se – 119
- 6.3.2 Pokud potřebujete, obraťte se na odborníky. – 120



Obrázek 1.6.1: Obsah a přebal knihy z produkce NIC.CZ na téma bezpečnosti

1 <http://knihy.nic.cz>

## 2 KURIKULÁRNÍ DOKUMENTY

### 2.1 Znalostní společnost

Podle *Lisabonské strategie Evropské unie* z roku 2004, převzato ze [Skalková, 2007], která představuje program komplexní ekonomické, sociální a ekologické Evropy, akcentuje přechod *ke společnosti založené na znalostech*, důležitost zvyšování úrovně a přípravy pro život v informační společnosti, význam celoživotního vzdělávání, prioritu investic do lidských zdrojů.

*Formální vzdělávání* jako takové, jenž všichni známe a byli jsme mu povinně podrobeni, vystaveni se realizuje ve vzdělávacích institucích, jejichž funkce, cíl, obsah prostředky a způsoby hodnocení jsou definovány a legislativně omezeny – takové vzdělání poskytuje škola. Druhá skupina tzv. *neformální vzdělávání* vede k ucelenému pojetí, rozvoji osobnosti, realizuje se mimo formální vzdělávací systém – nabízí se mimo škol, za úplatu v kurzech, školeních ale i online zdarma a kvalitně<sup>1</sup>. A třetí skupiny tvoří *informální vzdělávání*, jako proces získávání vědomostí, osvojení dovedností a postojů z každodenních zkušeností, z prostředí a kontaktů. Krátce jsme tyto úvahy již rozvíjeli v kapitole 1.5 o edukačním prostředí, kde ho představujeme z psychologické stánky věci.

Dobrou úroveň všech typů a forem vzdělávání si člověk buduje *gramotnost*.

Podle *Zprávy o stavu země. Strategické volby, před nimiž stojí*. Univerzity Karlovy [Potůček, 2004 převzato z Skalková, 2007], kde již před 10 lety charakterizovali problémy ČR a snažili se naznačit možná řešení. Vycházeli z předpokladu, že v znalostní společnosti, či společnosti vědění, budou mít zásadní roli ve vytváření ekonomické prosperity procesy spjaté s věděním – učením, tvorbou, kreativitou a rozšiřováním vědomostí skrz ICT, aplikovat vědění a inovace. Ano, už tehdy se počítačové znalosti vyzdvihovali a země byla zaostalá v jazykových kompetencích – neznalost cizích jazyků, angličtiny v dospělé populaci zcela zarážející.

---

1 <http://www.coursera.org>  
<http://www.khanacademy.org>

I z tohoto důvodu se řadu setkáváme v akademickém prostředí s cizojazyčnými zdroji, které nepřekládáme, pojmy se snažíme uvědomit v kontextu – viz obr. 5.5.1.1

## 2.2 Národní ústav pro vzdělávání

Ministerstvo školství, mládeže a tělovýchovy (MŠMT) zřídilo k 1. červenci 2011 pod názvem *Národní ústav pro vzdělávání, školské poradenské zařízení a zařízení pro další vzdělávání pedagogických pracovníků* (NÚV)<sup>1</sup> nástupnickou organizaci předešlých organizací působících ve školství:

- Národního ústavu odborného vzdělávání (NÚOV),
- Výzkumného ústavu pedagogického v Praze (VÚP)
- a Institutu pedagogicko-psychologického poradenství ČR (IPPP ČR).

Tato organizace je v dikci MŠMT a vzhledem na uvedenou šířku původního členění, je nutné uvést, že stojí také na pilířích institucí, které v 50. letech minulého století podporovali ekonomické a učňovské vzdělávání, pohltilo také *Institut pedagogicko-psychologického poradenství ČR* a *Národní informační centrum pro mládež* (NICM). Na základě těchto pestrých zkušeností je tvorba rámcového vzdělávacího programu v dobrých rukou – formálně řečeno jinak – NÚV vydává zcela zásadní kurikulární dokument ve vztahu k požadavkům na vzdělávání a to *rámcový vzdělávací program* (RVP).

V dalším textu na NÚV ještě poukážeme při potřebě širších souvislostí v získávání gramotnosti žáků v různých studijních oborech. Jakou mírou jsou požadavky uvedené v RVP inovativní, moderní a spjaté s realitou, požadovanou kvalifikací.

## 2.3 Rámcový vzdělávací program

Stát vydává prostřednictvím ministerstva školství, řadu dokumentů, ze kterých je jedním z nejdůležitějších a závazných předpisů pro obsah vyučování, jeho formu a průběh právě *rámcový vzdělávací program* (RVP) pro konkrétní typ a obor studia. Posledních patnáct let se setkáváme se s rozsáhlou reformou školství, zavádění a revize RVP mají dopad na celé *kurikulum*.

---

1 <http://www.nuv.cz/>

Pokud *kurikulum* definujeme jako seznam všech vyučovaných předmětů a jejich časové dotace pro pravidelné vyučování na daném typu vzdělávací instituce [Prokeš, 2000], tak RVP je zásadní kurikulární dokument. Mezi další kurikulární dokumenty patří obecně všechny učební plány, osnovy, standardy, didaktické texty, ale také metodické příručky. Některé dokumenty ministerstvo zveřejňuje, některé hledáme dosud marně! Je zajímavé poznamenat, že právě kurikulum zavedlo ty předměty, které důvěrně všichni známe, které se ve školách vyučují. Zdůvodňuje se zde potřeba matematiky, jazyků atd., naopak například pomyslné předměty „vyjednávání“, „sociální a životní situace“ nebo „ochrana zdraví, lidského organismu“, „chov malých domácích zvířat“ – to vše obecně chybí a ještě dlouho chybět budou. Opravdu víme, jak se věci vyřizují, jak se má k nám chovat doktor, policista, soudce, jak sjednat dobrou kupní smlouvu, proč? V občanské nauce bylo přece vyjmenování evropských institucí a pramenů práva.

Prokeš [2000] uvádí, že by bylo nevhodné ztotožňovat *kurikulum* s *učivem*, protože se v něm navíc popisuje koncepce, cíle i cílové standardy celého vzdělávacího procesu pro zvolený typ a obor studia, dokonce délka a rozsah vzdělávání. Kurikulum je tedy už na začátku statická norma, kterou někdo naplánoval pro celý národ. Jeho obsah je později přejímán všemi pedagogy do druhého běhu změn – do procesu vyučování Tito kreativní rétorové ho podle svých individuálních vloh a svými způsoby předávají už do třetího běhu, do třetího kola změn – žákům, aby si učivo zpracovali, zapamatovali. Že jde při učení o proces plný chyb a nepřesností jsme uváděli už v kapitole 1.1. Proto nelze zcela očekávat, že prvotní norma a závěrečné zisky budou stejné. Každý účastník může hrozby vnímat různě, být o nich poučen všelijak, ale ve výsledku chceme zaručit stejnou míru získaných znalostí – proto nabízíme studijní materiály, učební texty, ze kterých se lze připravovat samostatně podle vlastní rychlosti vzdělávaného.

Další zajímavé historické a mezinárodní konsekvence ke kurikulu lze nalézt v Prokešovi [2000], zejména srovnání českého školství se západní Evropou, co do délky a rozsahu vzdělávání – nejsme ve škole ti, co jsou tam nejdéle.

Naposled ministerstvo iniciovalo jistou snahu o stejnost, zavedení *vzdělávacích standardů*, jejichž cílem je napomoci pedagogům, rodičům i žákům při naplňování vzdělávacích cílů z RVP. Standardy jsou tvořeny indikátory, které konkretizují

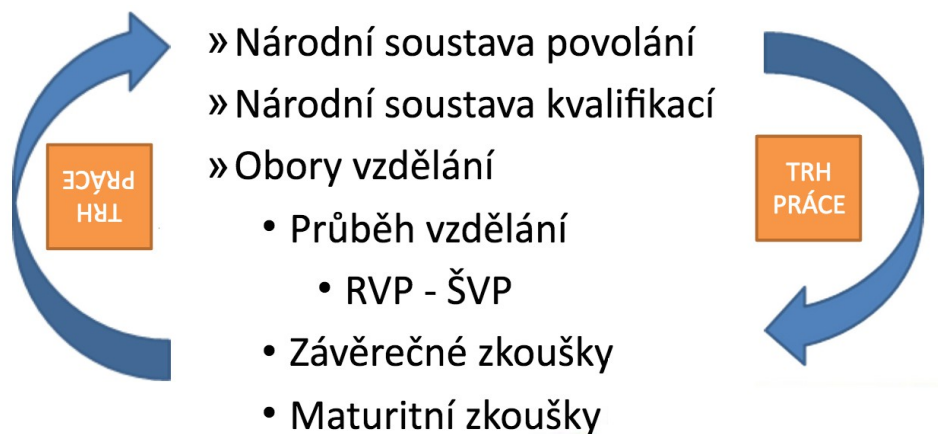


očekávané výstupy a stanovují pro ně konkrétní úroveň obtížnosti, s ilustrativními úlohami. V roce 2012 byly ovšem vydány a konkretizovány jen pro úzké skupiny předmětů základních škol: český a anglický jazyk, matematiku. Úzce s tvorbou standardů souvisí i polemika kolem *národních testů a srovnávání*, ale tomuto se zde již nebudeme věnovat. Věříme, že na hrubou orientaci v spleti norem pro vzdělávání tento výčet pojmů a jejich vysvětlení postačuje.

RVP také stanovuje závazné požadavky na vzdělávání, zejména výsledky, kterých má žák v jeho závěru dosáhnout a klade základní podmínky realizace vzdělávání. Každý poskytovatel vzdělávání toho kterého typu a oboru studia musí z RVP vycházet [převzato z RVP]. Tuto shodu kontroluje školní inspekce.

## 2.4 Školní vzdělávací program a reálná situace

V návaznosti na rámcové programy si poskytovatelé vzdělávání, všechny druhy škol, vytvářejí své vlastní, konkrétní *školní vzdělávací programy* (ŠVP). Přehled vzájemných vztahů a jistou hierarchii ukazuje obr. 2.4.1. Popisuje také ověřování vzdělávání, kterému se ve vztahu k zadání této práce věnujeme komplexně až v kapitole .



Obrázek 2.4.1: Souvislosti RVP, ŠVP s ověřováním znalostí a trhem práce [NUV]

Podle někdejšího 10. ministra školství Ondřeje Lišky (\*1977) v letech 2007–2009 jde o inovativní dvouúrovňový model, kde stát vytvořil obecnou část (RVP) a školy si druhou úroveň (ŠVP) vytvářejí samy podle svých představ. Už tehdy se podle ministrových slov nevstřícně projevovala nesystematičnost podpory učitelů v

tomto úsilí, jistá vyšší zátěž kladená na kantory navrch svých dřívějších povinností. Ministr uvedl ke kreativitě: „Přitom když se zeptáte nositelů Nobelových cen, co je přivedlo k bádání, k jejich oboru, tak vám v naprosté většině řeknou, že to byl jejich vyučující na základní, střední nebo vysoké škole, který je pro to nadchl. [...] Děti nejsou hloupější než dřív, ale já se obávám, že je nedokážeme nadchnout. Namísto toho jejich tvůrčí a inovační potenciál utlumujeme a zabíjíme.“ [Kundra, 2009]

Na vyváženou je potřeba dodat, že ministr Liška také kriticky zhodnotil chybějící vizi, která by motivovala ke změnám. Z důvodů politických změn ve spojitosti s pádem vlády skončil ve funkci za několik měsíců. Následující 11. ministryně školství Miroslava Kopicová (\*1951) v roce 2010 rozběhla 14 let starou vizi *státní maturity*. K tomuto centralizovanému způsobu ověřování znalostí a dalším standardům vysvětlujeme podrobnosti v kapitole 3.3.

Současný 15. ministr Marcel Chládek (\*1968) uvedl za očekávané metody společné práce skupinovou výuku, sdílené prostředí. Jinak ve svých krocích rozhodujícího úředníka pozastavil testování 5. a 9. tříd a snaží se podporovat střední odborné školství. Chtěl by rozdělit financování regionálního školství na dvě části, a to zvlášť základní a zvlášť střední školy. Základní školy by dostaly prostředky na třídu, nikoliv jenom žáky, tím mohou prosperovat malotřídky. Mohly by se zvýhodňovat taktéž svazky škol – školy učící stejný obor se na některých aktivitách záměrně spojují a vytvářejí jistou přidanou hodnotu pro žáky.

Anna Putnová (\*1960), někdejší předsedkyně výboru poslanecké sněmovny pro školství, dlouholetá děkanka, skvělý člověk, jak ji osobně známe z komunikace v úřední školní věci<sup>1</sup>, u kulatého stolu dodala: „v únoru 2013 byla hotova tato koncepce, vycházelo z nových oborových normativů – projevuje se náročnost studia a zároveň profilace budoucích absolventů“ [Moravec, 2014], co bylo myšleno jako opravdová rozdílná finanční nákladnost některých typů oborů, zejména těch, které mají větší potřebu pomůcek a nástrojů. Ne nutně tolik proklamované odborné školství, které, musíme uznat, pro nezájem skomírá. Poslankyně Putnová, tedy v dobrém poradila, aby se ve školství pořád a pořád nevymýšleli nové

---

1 Návrh novely školského zákona, kdy paní předsedkyně, věcně a dokonce osobně, uvedla na pravou míru s vysvětlením stav věci osobním dopisem. S takovou vstřícnou reakcí jsme se v školství už dlouhou nesetkali. Tímto paní poslankyni vyjadřujeme svůj vděk.

strategie, velké plány, ale stačilo by dokončit navrženou, sepsanou a bohužel, založenou koncepci – když se znova změnila garnitura.

Z vlastní praxe můžeme uvést, že potřeba tvorby ŠVP, motivace, nebyla edukátorům dostatečně vysvětlena, a proto nebyla inovace přechodu od osnov k rámcovému a školnímu programu v zásadě zcela dobře přijata. Oproti osnovám co do rozsahu jde u ŠVP o desítky stran obsáhle dokumenty, které musí obsahovat penzum povinných informací z RVP, upravených na poměry a realitu školy. Ne však do takové míry, aby se dalo mluvit o skutečné kreativitě a inovaci kurikula, jak jsme uváděli při trvalých cílech edukace v kapitole 1.4. Dalo by se říct, že právě pomocí ŠVP si škola má dělat v očích veřejnosti reklamu, co všechno žákům nabízí, v jaké míře bude ve výuce zastoupena matematika, jak bude provázána s dalšími předměty, které učební metody a prostředky se použijí, jak bude hodnocena apod. Toto však rodiče často neví, že vůbec existuje a školy od sebe tak výrazně odlišuje, ve výsledku samotný rozsah dokumentu spíše veřejnost i odborníky z té které školy vůbec neláká, možná odstrašuje. Střední škola s desítkou oborů, i těch dobíhajících a už nenabízených, musí povinně udržovat třeba až dvacet samostatných ŠVP, a staré verze archivovat.

ŠVP může být co do obsahu kdykoliv revidováno samotnou školou jako celek, pokud projde schválením školskou radou, nesmí se však uškodit zájmům žádného z žáků, že by některé učivo neabsolvoval nebo na některém předmětu a jeho obsahu byl jakkoliv krácen. Nedodržení návaznosti ŠVP na RVP, neodůčení obsahu ŠVP může vést k odvolání ředitele školy.

V této práci se v praktické části pokoušíme analyzovat obsah několika rámcových vzdělávacích programů několika typů vzdělávacích oborů, ve kterých by se mohly bezpečnostní témata objevovat z principu, ze životních potřeb bezpečností a informačního bezpečí např. na Internetu, více v kapitole 4.

### 3 OBSAH VZDĚLÁVÁNÍ A STAV JEHO OVĚŘOVÁNÍ

V této kapitole popisujeme východiska, kdo a jak stanovuje, nebo v minulosti stanovoval, kritéria hodnocení dosaženého vzdělání. Přibližujeme metody ověřování znalostí, protože tyto jsou stěžejním důkazem stavu edukace. Učíme (se) to, co se zkouší, porovnáváme se podle toho, jakého hodnocení jsme dosáhli. Výsledkem středoškolského vzdělávání je maturita – v tuto chvíli *povinná státní maturita*.

Protože v praktické práci chceme srovnat požadavky některých rámcových vzdělávacích programů (RVP) (viz kapitola 2.3), musíme najít tento klíč, vhodný oficiální materiál, podle kterého se vyhodnocuje nebo vyhodnocovalo, dosažené vzdělání v maturitních předmětech. Váhu a smysl gramotnosti v ICT jsme již vysvětlili v evropském i místním českém kontextu (viz kapitola 2.1), a proto můžeme s radostí říct, že Informatika a komunikace patřili také do povinně volitelně části státní maturity. Současný stav neblahých úvah informatiku znovu odsunul do oblastí nepovinných, centrálně nezkoušených, ale pozitivní dopad toho, že kdysi byla v oficiální nabídce státních maturit, je znát už napořád.

Není však snadné nalézt ty správné jednotné požadavky na obsah jednotlivých předmětů, či vzdělávacích oblastí v kontextu testů, v popisu toho, co se bude zkoušet. Ano, připouštíme, že obsah vyučování je dán Rámcovým vzdělávacím programem, ze kterého zejména čerpáme a jeho realizací ve Školním vzdělávacím programu, který si musí školy sestavovat samy.

Věříme, že uvedený komplexní přehled podle témat bezpečnosti a ochrany dat pomůže učitelům/tvůrcům Školního vzdělávacího programu lépe integrovat, doplnit vzdělávací obsah na jejich škole tak, aby možná co nejlépe reflektoval dobrou bezpečnostní praxi a uvědomělé chování budoucího občana, který se bude orientovat v oblastech ochrany dat, komunikace a vlastního např. finančního, duševního i fyzického majetku a na té které škole získá kvalitní středoškolské vzdělání.

Kdo takové požadavky stanovuje v prostředí školy, lze zkratkovitě chápat – učitel. My však potřebujeme v celkovém kontextu dlouhodobé vzdělanosti a gramotnosti

najít oficiální normativy, které toto vyjmenovávají, formálně kontrolují – maturita, či už interní, školní nebo centrální, státní.

### 3.1 Státní maturita

Asi pět let zpátky (2010) panovala v oblasti ověřování výsledků vzdělávání na středních školách značná nejistota, ministerstvo nařídilo spuštění státních maturit. Prakticky jsou prováděné jako *zkoušky společné části maturitní zkoušky* a stará známa maturita ve škole se přejmenovala na *profilovou část*. Tedy dnešní žáci jsou i po několika novelizacích a změnách prováděcí vyhlášky pořád zkoušeni zčásti interně – ve škole, kde se učili, těmi, kdo je naučili. Státní část maturity je prováděná formou písemné zkoušky, kterou nazýváme *didaktické testy*. Tedy státní maturita jako taková není čistě ani maturitou, ani zcela centralizovanou zkouškou.

### 3.2 Cermat a jeho odraz ve společnosti

Organizace Centrum pro zjišťování výsledků vzdělávání (Cermat) vznikla jako ústřední orgán kontroly výsledků vzdělávání v dikci ministerstva školství. Má svého ředitele, obory a řadu pracovníků metodických, technických a školících. Není nadřízenou organizací v hierarchii školství školám, nepodléhá inspekci.

Cermat se snažil nalézt výchozí rámec požadavků, které bude ověřovat, které mají školy plnit, samy zkoušet – s předstihem dvou let před samotnou maturitní zkouškou vydává Katalogy požadavků pro jednotlivé předměty, viz v dalším textu, původně pro nižší a vyšší úroveň státní maturity, dnes už jen jeden typ.

Na vysvětlení musíme uvést, že původní záměr zavést dvě úrovně obtížnosti za účelem lepší rozlišitelnosti zvládnuté maturity se dnes už neuplatňuje. Jeho záměrem bylo na všech typech škol, které maturitní studium nabízejí, umožnit žákům se svobodně rozhodnout mezi nižší (*základní úrovní*), anebo prokázat zvládnutí většího obsahu učiva ve *vyšší úrovni*. Pozitivní dopad takového rozhodnutí měl abiturientům zajistit snadný vstup na vysoké školy, že by jim snad mohlo odpustit konání přijímacích zkoušek. Bohužel, se tak nedělo. Sekundární smysl dvojí náročnosti byl ve volbě podle typu školy, odborné školy a učiliště by standardně konaly nižší laťku, gymnázia by mohly prokázat svojí vyšší náročnost

probíraného, ale kdo by si přidával starosti?! Z důvodu společenského odrazu, reakcí společnosti, který uvádíme níže, nakonec došlo k zrušení víceúrovňové obtížnosti.

V textu práce se k obtížnosti požadavků jako obecného pojmu, co by se mělo umět z bezpečnosti a ochrany dat vracíme také v (1) analýze Katalogu z informatiky a (2) v samotných studijních materiálech. Tyto materiály se snažíme vypracovat s co nejvyšší pochopitelnou úrovní pro středoškoláky, kdyby jen přece, v překotných změnách ve školství, opět jednou požadavky stouply, jsou tak již připraveny.

Cermat, jako původní organizace, která zastřešuje státní maturity od jejich spuštění před pěti lety, bojuje s nezdařením udržení dobrého *public relations*. Velmi těžko nalézáme zdroje chvály a uznání, které by organizace od společnosti obdržela. Ať už jde o publicistické zprávy, televizní zpravodajství, diskuse a tiskové konference, většinou se setkáváme s negativním vyzněním zpráv – co se nepovedlo, kolik to stálo, kolik změn bude potřeba. Společnost toto vyznění vnímá a obáváme se, že nikoliv pozitivně. Je však nutné zmínit, že v oblasti školství se zdá být každý odborníkem.

Negativní zkušenosti můžeme doložit po jednotlivých ročnících běhu státních maturit tak, že nejsou srovnatelné úrovně náročnosti, že příliš mnoho žáku neuspělo, že úroveň byla příliš lehká, že státní hodnotitelé nebyli neomylní apod. Jednotlivé výtky jsme studovali a jejich zpravodajské podání Cermatu na popularitě nikterak nepřidává. Vydání tiskové zprávy, nebo promluva ředitele, o nepravdivosti tvrzení médií, není dostačující.

Tedy sumárně lze říct, že se nedaří najít jednu společnou úroveň požadovaných vědomostí, zejména v matematice, ověřit ji konzistentně, srovnatelně.

Nebo řekněme to z druhé strany ve prospěch Cermatu, nelze si na svých kritériích trvat. Tedy se Cermat raději nevyjadřuje, výsledky nijak zvlášť nepublikuje. Podle našeho názoru zbytečně vede spory s *aktualne.cz* nebo testovací firmou Scio. Uvedený zpravodajský online deník jako první reálně výsledky jednoho ročníku zpracoval a zveřejnil tabulky kvality vzdělávání na jednotlivých středních školách podle počtu úspěšných maturantů – jak objektivně. Takto analytický výstup Cermat neposkytuje. Naopak Scio spíše zpochybňuje vedení a realizaci testování, že by testování dokázal udělat levněji. Poznamenejme, že poslední běh maturit stál

přibližně 300 miliónů korun a otestování jednoho žáka připadá asi 2000 Kč. Tuto cenu také považujeme za vysokou, v případě, že jde o zatrhávání testů, jistou část peněz stojí počítačové zabezpečení a odměna hodnotitelů na školách.

### 3.3 Katalogy požadavků

Katalogem požadavků Cermat směřuje na sjednocení obsahu požadovaného obsahu, který bude ověřován, testován u státní maturity. Sada těchto katalogů se vydává vždy s dvouletým předstihem před konáním konkrétní společné části maturitní zkoušky. Katalogy se vydávají pro všechny maturitní předměty, jenž jsou zkoušeny ve společné části.

Vyznění obsahu a konkrétních inovativních požadavků katalogu informatiky se v zajetých kolejích typické středoškolské informatiky – sedíme u počítačů, wordujeme – potkalo s velkou nevolí! Podle našeho odborného IT vzdělání a podle našeho názoru, se při jejich vzniku konečně našel autor, který tyto katalogy připravoval ze stejného IT přesvědčení – dělat informatiku, ne kancelář, nebál udělat zajetému přítrž a konečně opravdu věnovat ICT patřičnou pozornost.

Při podrobném zkoumání zejména *Katalogu požadavků zkoušek společné části maturitní zkoušky: Informatika: vyšší forma zakončení: platný od školního roku 2011/2012* [Cermat, 2012], duše informatika zaplesá. Protože informatika v současnosti není maturitním předmětem, není zkoušení uvedených požadavků závazné, může však inspirovat. V následující tab. 1 jsme vybrali ty témata, které co nejvíce splňují bezpečnostní charakteristiku v úzkém slova smyslu.

**4.1 Bezpečný počítač**

Žák dovede:

- vysvětlit potřebu aktualizací operačního systému a aplikačních programů, aktualizaci provést a nastavit způsob jejího provádění;
- s porozuměním používat antivirový program, firewall a další bezpečnostní nástroje;
- vysvětlit problematiku a způsoby šíření počítačových virů a červů, malware a spyware; popsat nejčastější metody útoků přes webové stránky a elektronickou poštu a bránit se proti nim;
- vysvětlit problematiku spamu a používat obranu proti němu, rozpoznat hoax;
- rozlišit nebezpečí podvodů (tzv. technik sociálního inženýrství), rozpoznat základní rysy takového podvodu;
- zdůvodnit důležitost komplexního přístupu k bezpečnosti IT.

**4.2 Obecné bezpečnostní zásady a ochrana dat**

- aplikovat zásady vytvoření bezpečného hesla pro identifikaci přístupu;
- popsat základní způsoby zabezpečení dat před jejich zneužitím;
- chránit svá data před ztrátou, zálohovat svá data;
- vysvětlit pojmy integrity dat, hash, autenticita, šifrovací algoritmus a klíč;
- popsat principy šifrování pomocí symetrické kryptografie a oblasti jejího nasazení;
- popsat principy šifrování pomocí asymetrické kryptografie a oblasti jejího nasazení, pojmy privátní a veřejný klíč a princip elektronického podpisu;
- prakticky provádět šifrování souborů.

**4.3 Etické zásady a právní normy související s informatikou :**

- respektovat při práci s informacemi etické zásady; - charakterizovat principy stanovené v zákonech o svobodném přístupu k informacím a o ochraně osobních údajů;
- vysvětlit podstatu ochrany autorských práv a základní ustanovení zákona o právu autorském ve vztahu k software a k šíření digitálních dat (hudby, videa, ...)
- aplikovat normy pro citování z knih a z on-line zdrojů;
- vysvětlit pojem licence k užití programu a charakterizovat jednotlivé nejčastěji používané druhy licencí;
- objasnit principy obsažené v licencích GNU/GPL a Creative Commons; - uvést příklady běžných proprietárních programů a Open Source programů; - podat přehled o způsobech ochrany software proti nelegálnímu šíření, uvědomovat si protiprávnost prolomení těchto ochrany a rozpoznat související rizika.

Tabulka 1: Vybraný seznam bezpečnostních požadavků z katalogu pro někdejší vyšší úroveň státní maturity z informatiky [Cermat, 2012].



## **II. PRAKTICKÁ ČÁST**

## 4 ANALÝZA POŽADAVKŮ

V této kapitole jsme provedli rozsáhlou komparativní analýzu shody několika rámcových vzdělávacích programů (RVP) s požadavky, které jsme vysvětlili a předložili v předešlé kapitole.

K analýze jsme vybrali RVP pro studijní obory, jenž spějí k maturitě a souvisí zejména s informačními, komunikačními; bezpečnostními technologiemi, buď názvem oboru, jeho účelem nebo obecným cílem. Zohlednili jsme také současný zájem žáků při vstupu do středoškolského vzdělávání, jejich preference, podle naplněnosti škol, zvolili jsme tedy k analýze:

1. RVP pro gymnaziální vzdělávání,
2. RVP pro informační technologie,
3. RVP bezpečnostně právní činnosti.

Při hodnocení obsahu jednotlivých kurikulárních dokumentů jsme přihlédlí také na zkušenosti z praxe učitele, z prostudované literatury:

- DOSEDĚL, Tomáš, 2004. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1,
- BRABEC, František, 2001. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001. 400 s. ISBN 80-86445-04-6,

základních učebnic a studijních materiálů:

- KALUŽA, Jindřich a Ludmila KALUŽOVÁ, 2012. *Informatika*. Havlíčkův Brod: Ekopress, 2012. 130 s. ISBN 978-80-86929-83-5,
- ROUBAL, Pavel, 2012. *Informatika a výpočetní technika pro střední školy - Teoretická učebnice*. Brno : Computer press, 2012. 104 s,

doplňkových a přehledových kapitol (pro bezpečnostně právní činnost):

- BALABÁN, Miloš, DUCHEK, Jan a Libor STEJSKAL, 2007. *Kapitoly o bezpečnosti*. Vyd. 1. Praha: Karolinum, 2007. 428 s. ISBN 978-80-246-1440-3.

Analýza je provedena, věříme, odborně z důvodu našeho (a) specifického bezpečnostního zaměření studia, (b) dosažené kvalifikace vysokoškolského vzdělání. Zaměřujeme se na majoritní vzdělávací proud absolventů s maturitou, které ostatně dává základ dalšímu možnému studiu na vyšším stupni škol, ať už vyšších odborných (DiS.) nebo přímo vysokých školách veřejného (Bc., Ing., Mgr.) a státního charakteru (policejní, vojenská). Uvažujeme krátce také potenciální růst až do rigorózního řízení ve vztahu k právu a obecné bezpečnosti u policejního sboru, nebo v kontrolních orgánech (JUDr.).

Samozřejmě, je přehánějící tvrdit, že by středoškolské vzdělání poskytlo obsahový základ k státním závěrečným/rigorózním zkouškám, nelze však ani vyvrátit, že kvalitní a erudované působení na žáky již na střední škole může velice stimulovat k příštím studiu vyššího stupně vzdělávání, poskytnout k němu nezbytnou motivaci, že by se žák chtěl dozvědět víc. Uvedenou kvalifikaci/titul žák také dosáhne ve vybraných typech zaměstnání vyššího výdělku a zařazení.

V dalším uvádíme přehledovou formou obsahovou část „Učiva“ vyjmenovaných RVP ve vztahu k bezpečnostním tématům. V případě malého pokrytí tématy v RVP je uvedeno v záhlaví tabulek „výběr“. Komentář je uveden průběžně.

#### 4.1 RVP pro gymnaziální vzdělávání

Digitální technologie	komplet
<b>informatika</b> – vymezení teoretické a aplikované informatiky	
<b>hardware</b> – funkce prostředků ICT, jejich částí a periférií, technologické inovace, digitalizace a reprezentace dat	=kódování ≠ šifrování
<b>software</b> – funkce operačních systémů a programových aplikací, uživatelské prostředí	+šifrování souborů
<b>informační sítě</b> – typologie sítí, internet, síťové služby a protokoly, přenos dat	+HTTPS
<b>digitální svět</b> – digitální technologie a možnosti jejich využití v praxi	
<b>údržba a ochrana dat</b> – správa souborů a složek, komprese, antivirová ochrana, firewall, zálohování dat	
<b>ergonomie, hygiena a bezpečnost práce s ICT</b> – ochrana zdraví, možnosti využití prostředků ICT handicapovanými osobami	

<p><i>Nejvíce pokrývá katalog požadavků, ale je natolik obecným seznamem učiva, že nelze hledat shodu podle jednotlivých bodů.</i></p> <p><i>Doporučujeme v teorii informace vysvětlit, co je kódování a že se nejedná o šifrování, jak si žáci pletou. Na tomto lze stavět nepovinné zařazení šifrování souborů nebo komunikace (HTTPS).</i></p>	
---	--

<b>Zdroje a vyhledávání informací, komunikace</b>	<b>komplet</b>
<p><b>internet</b> – globální charakter internetu, multikulturní a jazykové aspekty, služby na internetu</p> <p><b>informace</b> – data a informace, relevance, věrohodnost informace, odborná terminologie, informační zdroje, informační procesy, informační systémy</p> <p><b>sdílení odborných informací</b> – diskusní skupiny, elektronické konference, e-learning</p> <p><b>informační etika, legislativa</b> – ochrana autorských práv a osobních údajů</p>	<p>+sociální inženýr</p> <p>+hacker</p> <p>+cracker</p> <p>+rizika</p> <p>neověřených zdrojů</p>
<p><i>Charakteristika učiva je obecná, bezpečnostní témata se hledají stěží, jen v závěru o ochraně dat, krátce lze mluvit o informačních systémech kolem nás.</i></p> <p><i>Doporučujeme zcela určitě začlenit termíny sociální inženýr, hacker, cracker, protože se v komunikaci objevují jako bezpečnostní rizika.</i></p>	

<b>Zpracování a prezentace informací</b>	<b>komplet</b>
<p><b>publikování</b> – formy dokumentů a jejich struktura, zásady grafické a typografické úpravy dokumentu, estetické zásady publikování</p> <p><b>aplikační software pro práci s informacemi</b> – textové editory, tabulkové kalkulátory, grafické editory, databáze, prezentační software, multimedia, modelování a simulace, export a import dat</p> <p><b>algoritmizace úloh</b> – algoritmus, zápis algoritmu, úvod do programování</p>	<p>+ export do PDF</p> <p>+UAC</p> <p>+hrozby malware a skriptů</p>
<p><i>Množství učiva je překotné, nelze ho vůbec zvládnout v krátké době.</i></p> <p><i>Doporučujeme doplnit například export dat a textů do PDF při publikování, vysvětlit smysl ochrany User Acces Control (UAC) vo Windows aplikacích a také v tom nuceném programování poukázat alespoň na hrozby malware, skriptů v prohlížeči internetu nebo souborů např. PDF.</i></p>	

## 4.2 RVP pro informační technologie

Vzdělávání v informačních a komunikačních technologiích	výběr
<b>1 Práce s počítačem, operační systém, soubory, adresářová struktura, souhrnné cíle</b> - hardware, software, osobní počítač, principy fungování, části, periférie - základní a aplikační programové vybavení - operační systém, jeho nastavení - data, soubor, složka, souborový manažer - komprese dat - prostředky zabezpečení dat před zneužitím a ochrany dat před zničením - ochrana autorských práv - algoritmizace - nápověda, manuál	+ochranu uživatele, +šifrování souborů, +malware
<b>3 Práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu</b> - počítačová síť, server, pracovní stanice - připojení k síti a její nastavení - specifika práce v síti, sdílení dokumentů a prostředků - e-mail, organizace času a plánování, chat, messenger, videokonference, telefonie, FTP...	+šifrování
<b>4 Informační zdroje, celosvětová počítačová síť Internet</b> - informace, práce s informacemi - informační zdroje - Internet	+sociální inženýr
<p><i>Plusem je výklad celého spektra ICT technologií, přechod základním HW až po SW a jeho nastavování, krátce programování. Velký rozsah síťových pojmů, dokonce telefonie – vše oblasti, kde se bezpečnostní problematika může objevit.</i></p> <p><i>Minusem je absence určitějšího cíle, například řešit a edukovat o životě uživatele v operačním systému a počítačové síti po zbytek života, jak ho potkáváme už v současnosti. Téměř se nekomprimuje, už vůbec nepoužívají manuály, organizátory a plánovače, FTP. Toto učivo bude nezbytně zastarávat.</i></p> <p><i>Zcela chybí kapitola Bezpečnosti podle katalogu požadavků!</i></p> <p><i>V uvolněných blocích by bylo možné učit kryptografii, alespoň obecně a v síťových kapitolách ukázat elektronický podpis, ne-li další bezpečnostní pojmy.</i></p>	

Hardware	výběr
<b>1 Bezpečnost a ochrana zdraví při práci, hygiena práce, požární prevence</b> - řízení bezpečnosti práce v podmínkách organizace a na pracovišti - pracovněprávní problematika BOZP - bezpečnost technických zařízení	

*V této oblasti jen krátké pojednání o BOZP, žádné čtečky otisků, prstů, nic dalšího, škoda i když se v předmětu nabízí obrovský rozsah učebních hodin.*

*Ve zbytku se probírá primární cíl předmětu, o všech základních částech počítače (CPU, HDD...), síťové prvky a počítačové periferie.*

*Pokud by to bylo možné, doporučujeme zařadit biometriky, protože s HW úzce souvisejí a IT odborník se s jejich instalací může potkat*

<b>Základní programové vybavení</b>	<b>výběr</b>
<b>1 Instalace, konfigurace a správa operačního systému</b> - konfigurace OS (nastavení uživatelských účtů, přizpůsobení uživateli a požadavkům organizace, konfigurace přístupu ke službám OS, konfigurace přístupu k datům)	
<b>2 Operační systémy</b> - druhy, systémové požadavky, vlastnosti, použití, aktualizace - zabezpečení a ochrana systému a dat - viry, spyware	
<i>Obecné principy ochrany uživatele, jeho OS a SW</i> <i>Ve zbytku se pojednává o konfiguraci konkrétních síťových služeb jako DHCP, SQL, SMTP a síťových zařízení včetně serveru</i>	

<b>Počítačové sítě</b>	<b>výběr</b>
<b>2 Komunikace v síti</b> - referenční modely, protokoly	
<b>11 Bezpečnost v počítačových sítích</b> <i>(bez obsahu)</i>	
<i>Ve zbytku se v 10/12 celků probírají базové principy počítačových sítí od topologií, přes jednoduché návrhy, všechny pasivní i aktivní prvky, adresaci, bezdrátové spojení i diagnostika celé sítě</i>	

<b>Aplikační programové vybavení</b>	<b>výběr</b>
<b>1 Výběr a instalace software</b> - druhy SW, shareware, freeware - autorská práva - licence	

<b>8 E-mailový klient</b> <i>(bez obsahu)</i>	
<b>9 Webová klient</b> <i>(bez obsahu)</i>	
<i>Ve zbytku 10/13 celků se věnuje pozornost zejména práci v editorech textu a tabulek a databází, obecné zpracování zvuku, grafiky, multimédii a prezentacím, řeší se také uživatelská podpora a základní datové formáty souborů</i>	

<b>Programování a vývoj aplikací</b> <i>(nic)</i>	výběr
<i>Velmi nevhodné pojetí, protože právě programováním malwaru lze způsobit rozsáhlé škody v IT prostředí. Praktika dobrého programátora by byly vhodné.</i>  <i>Sumárně v 5/5 celků pojednává o algoritmizaci a diagramovém zápisu, obecném strukturovaném imperativním paradigmatu a poté objektovém programování. Velká část se věnuje také databázovým technologiím (nijak specifikovány) a tvorbě webu</i>	

### 4.3 RVP pro bezpečnostně právní činnost

<b>Bezpečnostní příprava</b>
<b>1 Bezpečnostní sbory</b> - policejní právo a jeho normy - právní úprava činnosti bezpečnostních sborů upravující organizaci a úkoly
<b>2 Policie ČR</b> - Organizační struktura služby pořádkové policie - povinnosti policistů - etika policejní práce - oprávnění policistů podle zákona o Policii ČR - policejní cely - donucovací prostředky - součinnost a spolupráce s orgány státní správy a samosprávy na úseku ochrany a bezpečnosti - doklady totožnosti občana - problematika pobytu občanů na území ČR - zbraně a střelivo - úkoly obecní policie a obvodních oddělení Policie ČR na úseku ochrany životního prostředí
<b>3 Organizační struktura služby dopravní policie</b> - doprava a společnost - rozdělení působnosti Ministerstva vnitra ČR a Ministerstva dopravy ČR a Ministerstva financí ČR na úseku silniční dopravy - prevence a bezpečnost silničního provozu - pozemní komunikace - pravidla provozu na pozemních komunikacích - podmínky provozu silničních vozidel na pozemních komunikacích - provozování silniční dopravy - přestupky související s provozem na pozemních komunikacích - správní evidence na úseku silničního provozu - řidičské průkazy a řidičská oprávnění
<b>4 Organizační struktura služby cizinecké a pohraniční policie</b> - cestovní doklady - pobyt cizinců na území ČR - azyl a dočasná ochrana - doklady totožnosti cizince - česká a Schengenská víza - azyl a dočasná ochrana - evropské právo a Schengenské acquis - mezinárodní terorismus
<b>5 Ochrana člověka za mimořádných událostí</b> - živelní pohromy - havárie s únikem nebezpečných látek - radiační havárie jaderných energetických zařízení - zásady poskytování první pomoci
<b>6 Střelecká příprava</b> - zbraně a jejich historický vývoj - charakteristika některých zbraní - zákon o zbraních a střelivu - bezpečnostní opatření při zacházení se zbraněmi - teorie střelby - konstrukce nábojů - hlavní části náboje do palných zbraní - praktická manipulace se zbraní (suchý nácvik) - školní střelba dle pravidel sportovní střelby - čištění a údržba zbraní - zásady



<b>Prevence a odhalování kriminality</b>
<b>1 Kriminologie</b> - Kriminologie, obecná část - kriminologický výzkum - fenomenologie kriminality - etiologie kriminality - osobnost pachatele - viktimologie - kontrola a prevence kriminality - trestní represe a penologie - kriminologické prognózování - Kriminologie, zvláštní část - recidiva kriminality - druhy kriminality
<b>2 Kriminalistika</b> - kriminalistická nauka o stopách - kriminalistická identifikace - kriminalistická technika - kriminalistické metody identifikace osob a věcí - Kriminalistická dokumentace - kriminalistickotechnická dokumentace - základy kriminalistické fotografie - Kriminalistické učení o trestné činu - kriminalistická charakteristika trestného činu - poznání trestného činu a vyšetřovací situace - Kriminalistická taktika - vybrané problémy kriminalistickotaktických metod - kriminalistická taktika - Obecné otázky metodiky vyšetřování jednotlivých trestných činů
<b>Pedagogicko-psychologické vzdělávání</b>
<b>Učivo</b>
<b>3 Profesní etika</b> osobnostní charakteristika pracovníka bezpečnostně právní činnosti profesionální deformace a její prevence
<b>4 Psychologie a její aplikace</b> - psychologie, policejní, kriminální a forenzní psychologie - psychické jevy - psychologie osobnosti
<b>5 Sociální psychologie a její aplikace</b> - socializace osobnosti - sociální skupiny - jedinec ve skupině - vnímání druhých lidí - jednání v davu a hromadné chování - jednání s lidmi – verbální a neverbální řeč, konflikt a spolupráce, asertivita, altruistické chování - postoje veřejnosti k bezpečnostním složkám - mediální obraz bezpečnostních složek
<b>6 Psychologie obětí</b> - viktimologie a její předmět - dopad trestného činu na oběť - jednání s obětí trestného činu - problém poskytování pomoci
<b>7 Forenzní a penitenciární psychologie</b> - Forenzní a penitenciární psychologie - forenzní psychologie a její předmět - kriminalistická psychologie – psychologie výslechu, výpovědi, zvláštnosti výslechu - penitenciární a postpeniterciární psychologie

<b>Právní vzdělávání</b>
<b>Učivo</b>
<b>5 Pracovní právo a služební poměr</b> - účastníci pracovněprávních vztahů - vznik, změny a skončení pracovního poměru - pracovní kázeň - pracovní doba, dovolená, mzda a bezpečnost práce - vznik, změny a skončení služebníhopoměru - služební kázeň - doba služby, dovolená, služební příjem a bezpečnost práce
<b>6 Správní řízení</b> - základní zásady správního řízení - správní orgány a účastníci řízení - průběh správního řízení - rozhodnutí ve správním řízení - opravné prostředky
<b>7 Přestupkové právo</b> - právní úprava přestupků - obecná ustanovení zákona o přestupcích - druhy přestupků - řízení o přestupcích
<b>8 Trestní právo hmotné</b> - vznik, změna a zánik trestně právních vztahů - trestný čin - skutková podstata trestného činu - okolnosti vylučující protiprávnost - vývojová stadia trestného činu - trestná součinnost a účastenství - tresty a ochranná opatření - odpovědnost mládeže za protiprávní činy - rozbor vybraných skutkových podstat trestných činů
<b>9 Trestní právo procesní</b> - základní zásady, subjekty a stadia trestního řízení - vyšetřování trestných činů - procesní úkony k zajištění osob a věcí - dokazování - řízení před soudem
<b>10 Soudy, státní zastupitelství, advokacie</b> - organizace a úkoly soudů, státního zastupitelství, advokacie a notářství

## 5 STUDIJNÍ MATERIÁLY

I když se pohybujeme v prostředí s vysokou mírou investic, školství je chudé. Většinu prostředků spotřebují platy a provoz škol, úřadů, na úrovni 135 mld. korun ročního rozpočtu kapitoly MŠMT<sup>1</sup>, náklady školství představují 3,5 % HDP. MŠMT v kapitole ostatních neinvestičních výdajů (ONIV), do kterých spadají zejména učebnice a školní potřeby, stanovila 7 mld., na podporu technického vzdělávání 42 mil. korun. Tyto prostředky jsou použity na nákup všech možných knih do regionálního školství, už od základního školství, kde je stát garantuje. Ve středním školství se zavedl komerční přístup k věci, knížky jsou přece v knihkupectvích. Záleží tedy na interním nastavení a usnesení školy, z čeho se budou její žáci vzdělávat, které učebnice doporučí k studiu. Určitě se najdou školy, které knihy svým žákům zapůjčují, jsou však v minoritě.

Z našich zkušeností s výukou informatiky doporučujeme pro SŠ učebnici:

- ROUBAL, Pavel, 2012. *Informatika a výpočetní technika pro střední školy - Teoretická učebnice*. Brno : Computer press, 2012. 104 s.

Z pohledu kvalitního zpracování bezpečnosti IT na úrovni pro SŠ:

- DOSEDĚL, Tomáš, 2004. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
- McCARTHY, Linda a Denise WELDON-SIVIY. *Bud' pánem svého prostoru: Jak sebe a své věci chránit, když jste online*. Praha: CZ.NIC, 2014. 316 s. ISBN 978-80-904248-6-9. Dostupné z:  
<https://knihy.nic.cz/files/nic/edice/bpsp.pdf>
- <http://www.bezpecnyinternet.cz/>

Z pohledu ucelené publikace o fyzické bezpečnosti, zejména pro obor bezpečnostně právní činnost na SŠ:

- LUKÁŠ, Luděk a kol., 2011. *Bezpečnostní technologie, systémy a management*. Zlín: Verbum, 2011. 316 s. ISBN 978-80-87500-05-7.

---

1 [http://www.msmt.cz/uploads/odbor\\_13/Kniha\\_2015\\_text.pdf](http://www.msmt.cz/uploads/odbor_13/Kniha_2015_text.pdf)

Tato diplomová práce se snaží přispět k spektru těch spolehlivých studijních materiálů v oblasti bezpečí a bezpečnosti, proto jsme zpracovali několik studijních textů a prezentací, aby byly její součástí v přílohách a v elektronickém archivu<sup>2</sup>.

## 5.1 Moderní a bezpečné edukační prostředí

Školní inspekce navrhuje změnu vyučovacích metod na více inovativní. Proto v této kapitole postupně uvádíme argumenty odborníků na edukátory, na moderní edukační prostředí, abychom dospěly k jednomu konkrétnímu příkladu.

Závěry inspekce prezentovaly zjištění: „Čím starší děti, tím horší přístup ke škole a zhoršující se výsledky“ a to potvrzuje i prezident Asociace profese učitelství Jan Korda: „Neumíme učit tak, abychom děti motivovali, nevnímají smysl. Způsob vzdělávání a obsah vzdělávání, musíme změnit, abychom učili pro život. Aby děti věděly, proč se to učí.“

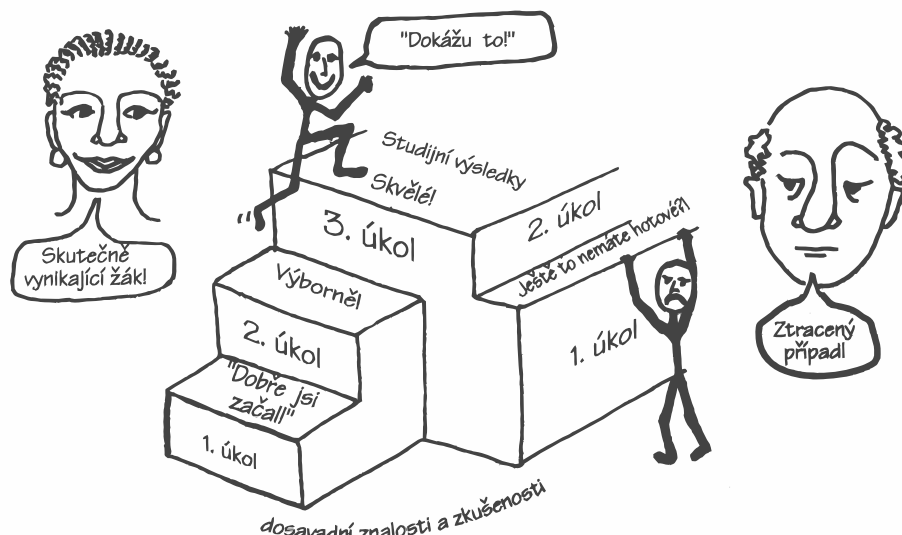
Petr Fiala (\*1964), někdejší 13. ministr školství, u kulatého stolu uvedl: „Učitelské povolání musíme jednoznačně definovat a musíme si říct [...] ne každý je vhodný, aby byl dobrým učitelem, že nestačí jenom mít dobré, odborné znalosti, ale jsou k tomu potřeba i určité osobnostní předpoklady, je potřeba, abych to řekl úplně jednoduše, aby ten člověk měl vztah k dětem, měl je rád, chtěl jim něco předávat, měl radost z toho, že je nějakým způsobem vede.“ [Fiala, 2013]. Škola je tak dobrá, jak dobří jsou její učitelé.

*E-learningu* se obsáhle věnuje Zounek (2012), který uvádí známé, že učení není pouhý mechanický proces, kde se přesouvají znalosti od zdroje ke konzumentovi, ale právě akt transformace, jakési vystavení se problémům, úkolům, testům vytváří nové znalosti, které jsou výsledkem aktivity učícího se jedince. A dále se potvrzuje, co jsme výše naznačili, že sociální prostředí v tomto sehrává svoji roli, ať už jsme ve třídě nebo někde na internetu.

Učení je sice záležitostí individuální, ale současně učení probíhá v určitém prostředí, v němž jsou přítomni i další lidé – učící se jedinec je členem nějaké komunity či skupiny. Student může být členem řady různých komunit, a v jejich rámci jsou rovněž vytvářeny a šířeny znalosti. Příkladem je skupina studentů určitého kurzu. V takovém kurzu mohou být zadávány úkoly, práce další postupné

2 <https://digilib.k.utb.cz/discover>

kroky vedoucí k vědě (viz kapitola 2.1) a ten správný motivující přístup (viz kapitola 1.2) je ilustrován na obr. 5.1.1.



Obrázek 5.1.1: Motivační přístupy ve vztahu k obtížnosti úkolů, vlevo postupná zátěž, vpravo nezdolatelný první úkol [Petty, 2008, s. 57]

Podle jednoho mezinárodního srovnání (NUV, 2015) je používání počítačů ve školách zcela podceňováno. Podíl učitelů, kteří se domnívají, že využívání ICT ve výuce pomáhá u žáků vzbuzovat větší zájem o studium, je v České republice ve srovnání s ostatními zeměmi jeden z nejnižších, přesto tento názor zastávají dvě třetiny českých učitelů. Obdobně nízký je v České republice podíl učitelů, kteří si myslí, že využívání ICT ve výuce zlepšuje studijní výkony žáků (53 %). Tři čtvrtiny českých učitelů naopak zastávají názor, že využívání ICT při výuce a studiu ve škole vede ke zhoršení písemného projevu žáků (průměrný podíl takových učitelů v rámci zemí ICILS činí 67 %). Nadprůměrný je též podíl učitelů, kteří se domnívají, že využívání ICT ve výuce jen vede ke kopírování materiálů z veřejných zdrojů.

Ve vzdělávací praxi se lze potkat s řadou systémů a inovativních metod, jak využít počítače, jak se dá zlepšit interakce s tabulí. Nabízíme krátké seznámení s jedním, jenž se jmenuje Edmodo, a je zdarma dostupný online<sup>1</sup>. Určitě může nabídnout lepší interakce s žáky než prezentace mailem.

1 <http://edmodo.com>



Ilustrace 5.1.2: Promo na e-learningový portál [edmodo.com].

Edmodo je americký pohled na e-learning, Iniciativa několika programátorů a učitelů, která přesahuje až zdarma za hranice států i do České republiky, je to systém, vyučovací prostředí dostupné online. Zvolili jsem si tento e-learningový systém, protože jsme dostali výborné reference na jeho používání v americkém středním školství. Odborníky v oblasti e-learningu určitě napadne, proč zde nedoporučujeme Moodle? Jsme toho názoru, že v době, kdy Facebook vládne, se právě Edmodo přístupem k práci hodně inspirovalo, Moodle možná zmizí v nenávratně pro jeho velkou zkostnatělost.

Edmodo umožňuje registraci a personifikaci profilů učitelů a žáků, kde se později sbírá řada ocenění *badges*, odznáček. Systém je pro veřejnost uzavřen, vyžaduje účet a vstupní kód, tím pádem velmi dobře chrání edukační prostředí, jak jsme ho popsali v kapitole 1.5.

Dokonce Google se svým vyhledáváním zůstává nevpuštěn, vyžaduje se tu povinná registrace pro vzdělávací účely a vstupní *group code* do třídy. Po registraci přijde na komunikaci na *zdi*, *společné nástěnce*, *kam píšou všichni*. Přítomné je lajkování, diskuse. Pro učitele Edmodo umožňuje tvořit víc druhů kvízů a zadávat domácí úkoly. Nejde jen o aktivní webovou stránku, ale celou databázi na sběr dat, protože úkoly lze uložit na server. Další funkce nabízí Edmodo v anketách a urgentních oznámeních, rozesílá maily, no chrání soukromí všech zúčastněných – studenti dokonce nevidí svá příjmení navzájem, nelze tvořit stovky přátel, bohudík, o to

máme edukační nezájem. Na Edmodu lze udělovat hodnocení, sbírat odznaky a navzájem studenty motivovat (viz kapitola 1.2). Myslíme si, že systém je silně intuitivní a spíš má jen ty nezbytné funkce, které tak akorát *stačí na podporu edukace*.

Velkou výhodou je vazba M:N, kdy student jednou registrací získá přístup do všech relevantních kurzů a zároveň jsou všechny kurzy nabízené klidně všem studentům, vždy podmíněno znalostí vstupního kódu. Jedna integrální součást školy, paráda. Učitelé se mohou navzájem spolupodílet na kurzech, tvořit další, dokonce je sami aktivně studovat.

Edmodu částečně chybí stromová struktura témat, nelze zde snadno udělat běžný, statický e-learning se strukturou a hierarchií informací... zde existující Zed' na to není vhodná. Edmodo však umožňuje sdílení ucelených materiálů přes složky, soubory dáváme do různých složek, složky do různých skupin. Vyzdvihujeme však tento přístup z pohledu toho, že soubory lze adresně poslat té které skupině, tomu studentovi nebo kantorovi, který jej bude potřebovat. Správa souborů v systému není ideální, nelze jej přejmenovat, ale to se snad časem spraví, komentáře lze vložit jen přes Zed', kterou ale nelze přeuspořádat. Uzavíráme tento popis vlastností Edmoda spíše jako místa, kde se potkávají zájmy související se studiem, od testování přes diskuse až po několik málo materiálu, odkazů a domácích úkolů k tomu – doplňující vyučovací prostředí.

## 5.2 Počítačová bezpečnost

Malware, spware, viry a červy, skrytý trojský kůň nebo všemocný nebezpečný rootkit – to vše se může uživatele kdykoliv nastěhovat do počítače.

Vysvětlení pojmů nabízíme v příložené prezentaci Počítačová bezpečnost.

## 5.3 Firewall

Bázové ochranné prvky sítí firewally, rovněž s *Network Address Translation* (NAT) nalézáme v domácích směrovačích, můžeme je konfigurovat, proto je dobré o nich něco znát. Odpovědné nastavení bezpečnostní politiky vlastního počítače nutí uživatele použít k antiviru, antimalwaru také firewall, vybrali jsme ty lepší.

Jejich přehled a srovnání nabízíme v příložené prezentaci Firewall.

## **5.4 IDS, IPS**

V počítačových sítích se také setkáváme s možnostmi ochrany celého prostředí, pomocí síťových prvků *Intrusion Detection System* (IDS) a *Intrusion Prevention Systems* (IPS).

Vysvětlení pojmů nabízíme v příložené prezentaci IDS, IPS.



## 5.5 Kryptografie pro SŠ

Podle Katalogu požadavků na znalosti z informatiky [Cermat, 2012] a podle Roubalové učebnice Informatiky [Roubal, 2012] patří i povědomí o principech šifrování a utajování dat k obecným znalostem ze střední školy, zejména do života.

*Kryptografii* chápeme jako praktický návrh ochranných utajovacích algoritmů, tedy postupů jak data zašifrovat. *Kryptoanalýza* se snaží tyto algoritmy prolamovat, různým zkoumáním složitosti návrhu šifrovacího algoritmu, jestli není rychlý způsob jeho odhalení. Naopak *útok hrubou silou* (angl. Brute Force Attack) zkouší na zašifrované data všechny možné klíče – aby jednou uspěl. V bezpečném světě očekáváme kvalitní šifrovací algoritmy a útoky hrubou silou tak neefektivní, hlavně kvůli množství všech kombinací klíčů, že by po desetiletích až staletích ztratili smysl. Kryptografie a kryptoanalýza dohromady tvoří vědní obor *kryptologii*.

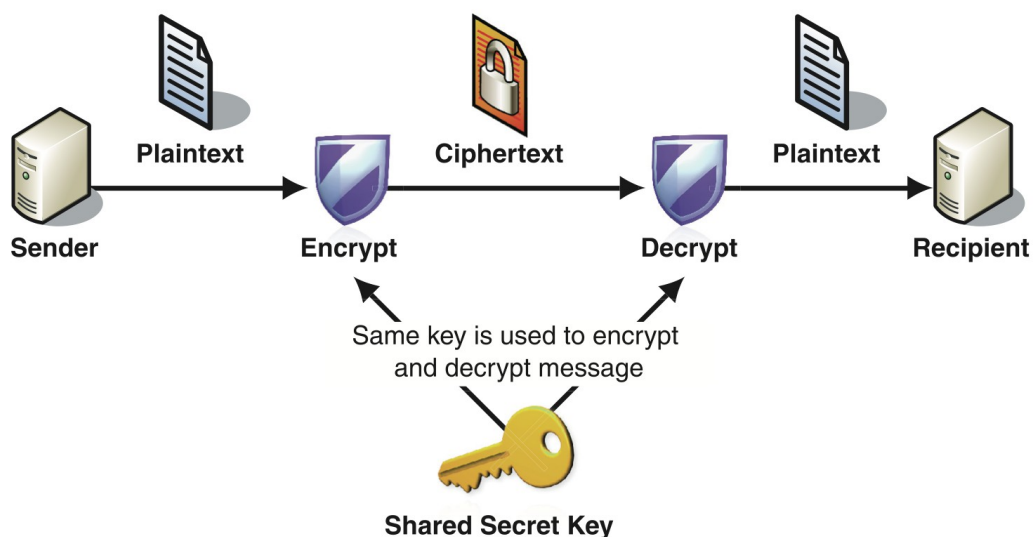
K zašifrování otevřené zprávy/textu/dat používáme *tajný klíč*, pomocí kterého nastavuje *šifrovací algoritmus* tak, aby vznikla tajná zpráva. Pomocí tajného klíče zprávu opět dešifrujeme a získáme původní text. Klíče nesmí být jednoduché, protože *jen složité a dlouhé klíče*, ostatně jako hesla, prodlužují útok hrubou silou.

Někdy se bohužel setkáváme s nevhodným označením „zakódovat“, který není správný. Data *šifrováním utajujeme* a *dešifrováním odtajňujeme*. Kódování dat je jejich převod do jiného tvaru/do jiných znaků, ale každý si je může vrátit zpátky změnou kódování – s tímto se setkáváme zejména při nastavení *znakové sady* v prohlížeči Internetu. Někdo tomu říká „rozsypal se čaj“, tehdy je potřeba vrátit se ke znakové sadě UTF-8 nebo Win1250 pro naše znaky.

Zpět ke kryptografii, podle toho jestli tajný klíč máme jenom jeden a ten stejný, nazýváme ji *symetrická kryptografie*. Pokud se v utajování zpráv objevují klíče dva, že to taky jde viz dále, postupu říkáme *asymetrická kryptografie* – není mezi šifrováním a dešifrováním symetrie. Pozor, symetrická kryptografie je zásadní a velmi důležitá k ochraně dat v řadě organizací, i v našich počítačích, je velice rychlá. Naopak s asymetrickou kryptografií se setkáváme v neznámém prostředí, když potřebují tajně komunikovat sobě ne zcela známe osoby, je pomalejší, protože je výpočetně náročnější.

### 5.5.1 Symetrická kryptografie

Symetrickou kryptografii chápeme jako zámek na truhlici, od kterého má klíč jak Alice, tak i Bob. V truhlici si nechávají svoje společné tajemství



Obrázek 5.5.1.1: Symetrická kryptografie [Microsoft, 2005]

Odesílatel (sender) svoji otevřenou zprávu (plaintext) zašifruje (encrypt) pomocí sdíleného tajného klíče (shared secret key) na tajnou šifrovanou zprávu (ciphertext).

Takovou zprávu lze přenést i nebezpečným/nedůvěryhodným prostředím. Poté se na ní během dešifrování (decrypt) použije symetricky/stejně sdílený tajný klíč (shared secret key) a získáme původní otevřenou zprávu (plaintext) na straně příjemce (recipient).

### 5.5.2 Asymetrická kryptografie

Jak jsme vysvětlovali výše, lze šifrování chápat jako analogii se zámkem, ke kterému mají klíč jen dva milenci, oba stejný. V sedmdesátých letech britská tajná služba objevila způsob, jak šifrovat s dvěma klíči. Tento postup nezávisle objevili také američtí výzkumníci Rivest, Shamir a Adleman.

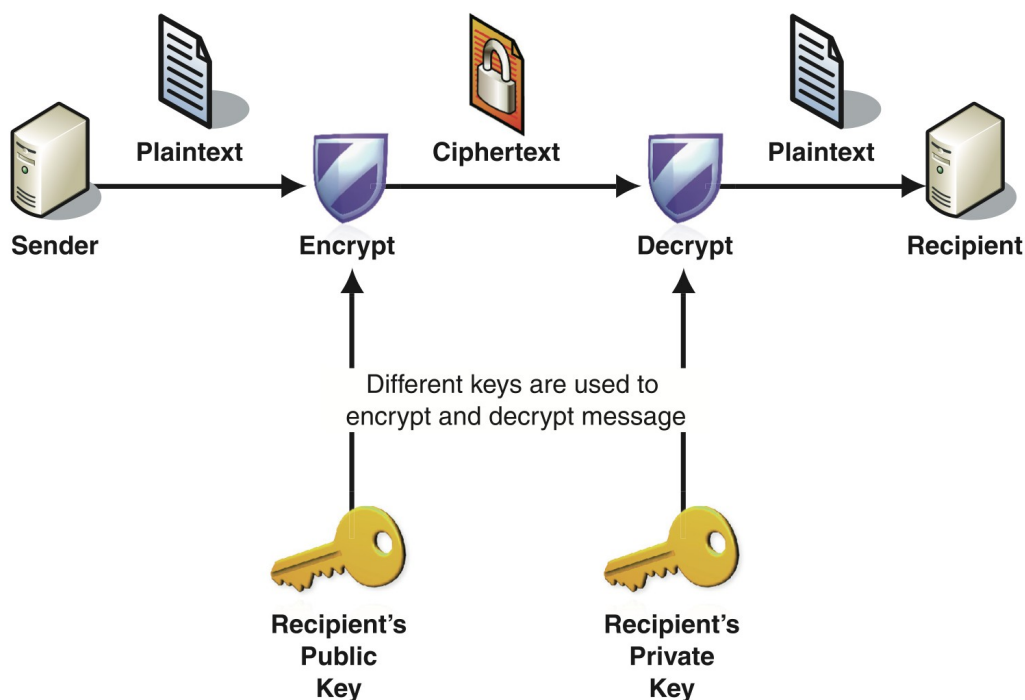
V asymetrické kryptografii, však není možné mít tak obrovské množství zámků a stejných klíčů, kterých by byla potřeba, aby byla každá vzájemná komunikace chráněná novým, unikátním klíčem. Tedy co spojení, to zámek a dva klíče – možná

je to z pohledu uživatele nijak závratné, ale z pohledu veřejného serveru zcela neudržitelné.

Příběh o sdíleném zámku a dvou klíčích k němu můžeme takto upravit:

1. Alice navrhne nový zaskakující zámek a jeho kopie distribuuje odemknuté po celém světě, klíč k němu si ponechá.
2. Bob dá tajemství do truhlice, zaklapne Alicin zámek, a pošle ji zpět Alici.
3. Alice si každou doručenou truhlici odemkne svým klíčem.

Bob by v případě správ pro sebe potřeboval svůj nový zámek, který by nechal odemknutý u všech kamarádů, všude možně po světě.



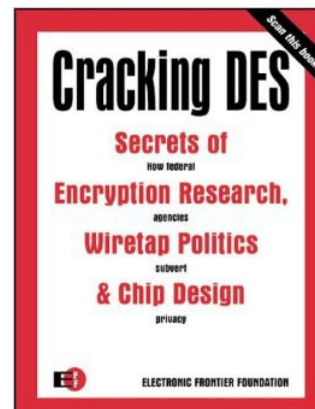
Obrázek 5.5.2.1: Asymetrická kryptografie [Microsoft, 2005]

Odesílatel (sender) svoji otevřenou zprávu (plaintext) zašifruje (encrypt) pomocí příjemcova veřejného klíče (recipient's public key) na tajnou šifrovanou zprávu (cipher-text).

Takovou zprávu lze přenést i nebezpečným prostředím. Poté se na ní během dešifrování (decrypt) použije tajný klíč příjemce (recipient's private key) a získáme původní otevřenou zprávu (plaintext) na straně příjemce (recipient).

### 5.5.3 Praxe

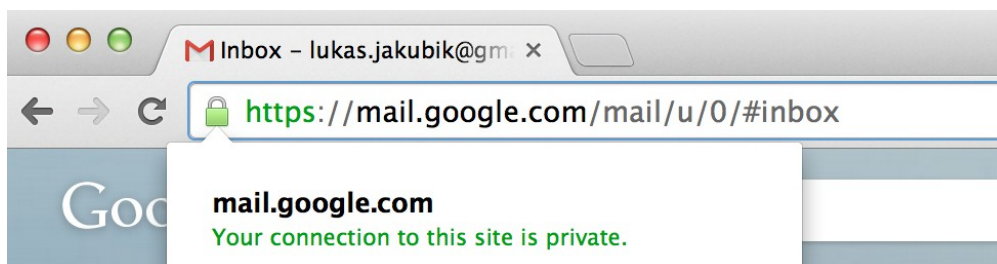
Symetrickou kryptografií můžeme uplatnit při jakémkoliv nastavování hesla, zřejmě se v útrobách chránícího systému skrývá některý ze šifrovacích algoritmů, který poté naše tajemství chrání. Na trhu profesionálních šifrovacích algoritmů se můžeme potkat s Luciferem, oficiálně nazván v 70. letech jako DES (Data Encryption Standard), dnes je už ale málo bezpečný, existují totiž přístroje, které jej dokážou hrubou silou úspěšně dešifrovat za méně jako sto let, třeba už za rok.



Na trhu kryptografie a to i pro ty nejtajnější informace vlád se používá šifrovací algoritmus Rijndael, pod zkratkou AES (Advanced Encryption Standard).

Asymetrický algoritmus se jmenuje RSA podle příjmení jeho objevitelů.

S asymetrickou kryptografií se setkáváme v reálném počítačovém životě mnohem častěji, než by se laikovi mohlo zdát. Používá se k ochraně komunikace mezi uživatelem a servery, protože její obsah musí být v nebezpečném prostředí Internetu chráněn, skryt, utajen zcela běžně. Nechceme, aby někdo viděl, co si čteme, co zadáváme, s kým si online chatujeme. Že se používá asymetrická kryptografie, můžeme pozorovat na URL adrese s prefixem protokolu HTTPS na obr. 5.5.3.1 s typickým zámečkem a několika důležitými informacemi o spojení.

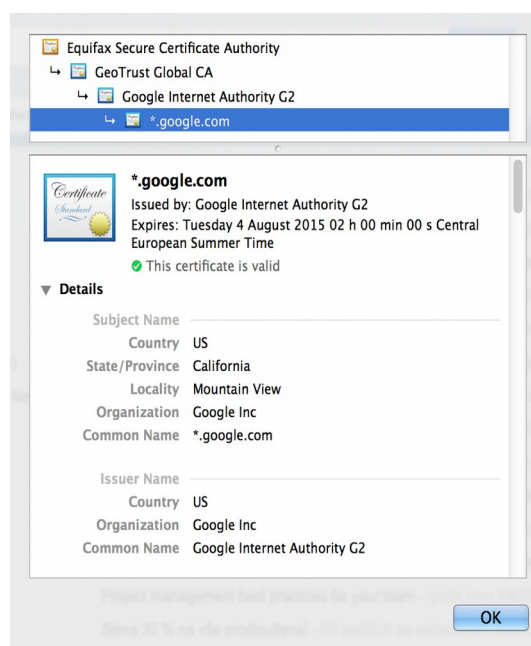


Obrázek 5.5.3.1: Komunikace s Gmailem přes protokol HTTPS

Je nutné však poznamenat, že asymetrické metody se použijí jen na začátku spojení, když se obě strany snaží se navzájem představit, vyměnit si šifrovací trivia. Domluví se na dalším sdíleném klíči, aby se ve výsledku po zbytek spojení domlouvali chráněni symetrickou kryptografií, protože je rychlejší na výpočet.

Další kontrolní informace lze najít v detailech o certifikátu na obr. 5.5.3.2. Vysvětlení, jak tyto certifikáty vznikají, hledejte v materiálu o elektronickém podpisu a certifikačních autoritách.

Principiálně \*.google.com přijímá data zašifrované jeho veřejným klíčem, který nechává viset na svých stránkách, ale podle čeho se mají uživatelé rozhodnout, že jde opravdu o klíč Googlu a nikoliv nějakého útočníka? Jde o tzv. *útok muže uprostřed* (Man in the Middle Attack).



Obrázek 5.5.3.2: Detailů certifikátu \*.google.com

Tím pádem bychom zašifrovali údaje sice bezpečně, ale dešifroval by si je útočník, který má k vyvěšenému podvrženému klíči svůj vlastní soukromý. A proto certifikát, jak je uveden na obrázku v postupné hierarchii certifikačních autorit, jistou vysokou mírou spolehlivosti garantuje, že opravdu komunikujeme s Google a nikoliv útočníkem.

## Zdroje

Microsoft, 2005. *Web Service Security: Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0* [online]. Microsoft, 2005, [cit. 2015-05-01]. Dostupné z: [http://download.microsoft.com/download/8/d/6/8d608524-0763-48b5-840b-0ae446996a14/MS\\_WSS\\_Dec\\_05.pdf](http://download.microsoft.com/download/8/d/6/8d608524-0763-48b5-840b-0ae446996a14/MS_WSS_Dec_05.pdf)

DOSEDL, Tomáš, 2004. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

KHANACADEMY, 2015. *Journey into cryptography* [online]. 2015, [cit. 2015-05-01]. Dostupné z: <https://www.khanacademy.org/computing/computer-science/cryptography/>

## 5.6 Elektronický podpis pro SŠ

Už v Katalogu požadavků na vyšší znalosti z informatiky [Cermat, 2012] se i na střední škole objevil požadavek pochopit principy *elektronického podpisu*, porozumět mu zejména do budoucnosti.

Začal se masivně používat ve veřejné správě – na úřadech, soudech, obecně v komunikaci státu směrem k občanovi. Pomocí něho je již možné podávat vlastní daňové přiznání elektronicky, přímo z domu za předpokladu, že je dokument opatřen *zaručeným elektronickým podpisem* občana. Také napsat a podat žádost do elektronické podatelny úřadu nebo státní instituce, nebo naopak obdržet rozhodnutí úřadu nebo soudu v hezky, informaticky v PDF (printable document format), souboru, který bude opatřen právě elektronickým podpisem. Takovéto dokumenty jsou i v elektronickém světě dlouhodobě platné, nedají se snadno falšovat.

Další mezistupeň zvýšení důvěryhodnosti elektronické komunikace ve vztahu k státu, doručovat a mít doručeno aj bez použití pošty a to zdarma, bylo zavedení *datových schránek*, které jsou zákonem postaveny na roveň listinnému rozhodnutí, jen je nenacházíme v schránce, nechodí na doručenkou, zůstanou v elektronické datové schránce. O takovouto schránku můžeme požádat dnes na poště.

### 5.6.1 Pojmy

Terminologicky je věc, jak už to bývá, složitější, možná malinko nepřehledná. Je nutné si ujasnit pojmy *digitální podpis*, pak *elektronický podpis* a nakonec *zaručený elektronický podpis založený na certifikátu kvalifikované certifikační autority*, o tomto pojednává zákon č. 227/2000 Sb., zákon o elektronickém podpisu.

Pro naše potřeby stačí pochopit zásadní vztah k předešlým znalostem z kryptografie, že digitální podpis je typický produkt operací s klíči nad nějakými chráněnými daty. Doporučujeme si připomenout pojem veřejného a soukromého klíče, jak se *šifruje* a *dešifruje* tajemství – veřejným, poté soukromým klíčem. A po těchto operacích je poté možné pochopit *podepsání* a *ověření digitálního podpisu* – nejprve soukromým klíčem, druhou operaci veřejným klíčem.

Co je zde nové a v asymetrické kryptografii se nevysvětluje je *certifikát veřejného klíče*. Tedy, že existuje takový postup, datová struktura, která po připojení k veřejnému klíči vytvoří uvedený certifikát, seznam vlastností kdo je majitelem klíče, od kdy a do kdy je platný, za jakých podmínek a s jakými algoritmy se používá atd. Technicky se provádí pomocí X.509 struktury, ale některé zejména linuxové a geek<sup>1</sup> prostředí používají GPG klíče, které si navzájem ověřují. Cílem certifikátu veřejného klíče je zvýšit povědomí o majiteli tohoto klíče, kterému chceme psát (šifrovat) nebo jeho dopis s podpisem zkontrolovat (ověřit) – víme o koho jde.

### 5.6.2 Praxe

Pokud bychom chtěli zkusit možnosti elektronického podpisu v praxi, být na chvíli geekem, můžeme si to nejlépe zkusit při doručování elektronické pošty. Abychom si podpis takříkajíc ohlíдали, svůj soukromý klíč měli pořád ve své moci a ne někde na serveru, musíme použít samostatný program na obsluhu pošty – emailového klienta – vybíráme Mozilla Thunderbird, protože si certifikáty drží ve svých souborech, naopak Microsoft Outlook je integruje do registrů operačního systému.

Můžeme zvolit produkt certifikační autority Comodo, který je dostupný zdarma, ale nefunguje ve smyslu českého zákona o elektronickém podpisu, nebo investovat do komerčního osobního certifikátu už ověřené kvalifikované certifikační autority PostSignum.

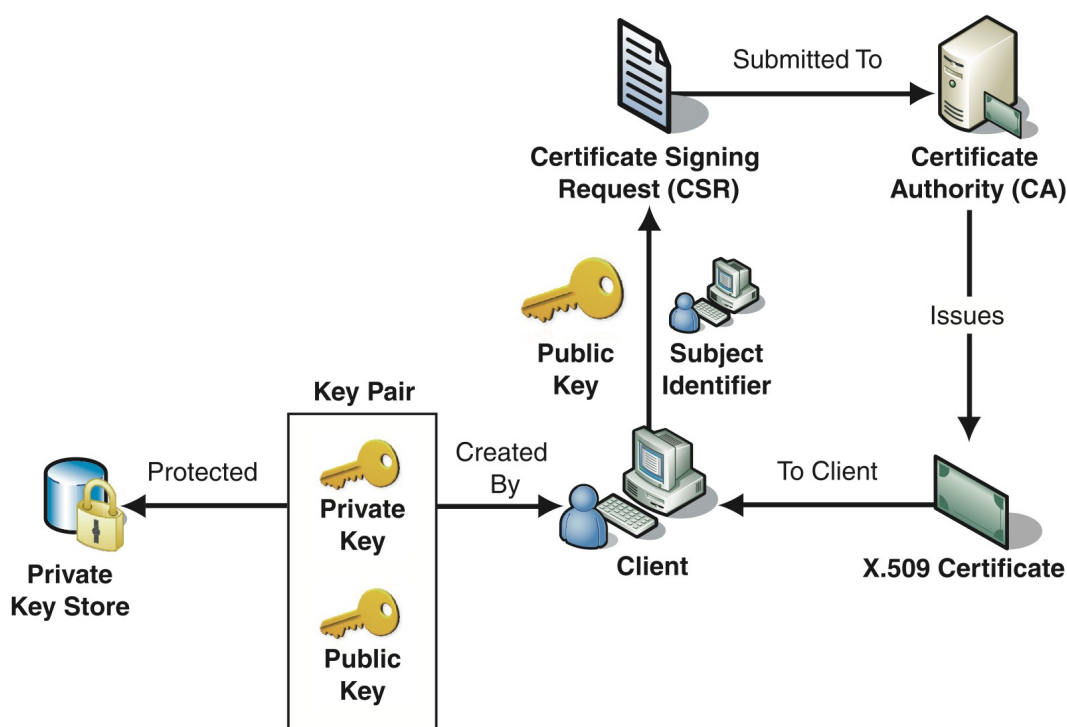
Zajímavosti z tohoto procesu jsou v příložené Presentaci o elektronickém podpisu.

### 5.6.3 Vydávání důvěryhodného certifikátu

Právě díky požadavku na certifikáty vydané důvěryhodnými *certifikačními autoritami* se tato důvěra buduje, snaží vybudovat. Stát bezpečnostní prověrkou určil některé subjekty býti schopnými vydávat certifikáty, být tzv. *kvalifikovanými* certifikačními autoritami. Na následujícím obr. 5.6.3.1 je zobrazen postupný proces vydávání X.509 certifikát certifikační autoritou.

---

<sup>1</sup> Geek [gí:k] je spíše novodobý termín z angličtiny, označuje osobu většinou z oblasti informačních technologií, která je pro svůj obor zapálená, dokáže vyřešit i obtížné problémy v rámci oboru. Také se tímto termínem označují lidé se silným západem pro jakékoli téma nebo jsou zaměřeni na malou část nějakého oboru [Wikipedie].



Obrázek 5.6.3.1: Vydávání certifikátu X.509 pro klienta od autority [Microsoft, 2005]

Žadatel si vytvoří a uchová svůj klíčový pár – soukromého a veřejného klíče, které se používají v asymetrické kryptografii. Dále předloží svojí pravou identitu (občanský průkaz a další doklady) *registrační autoritě*, která vytvoří požadavek na certifikát aj s uvedením požadovaných vlastností a údajů. V praxi je to tatáž autorita, nejčastěji paní za okénkem pošty (PostSignum certifikační autorita v rámci České pošty). Takto vygenerovaná žádost je někde v bezpečném prostředí certifikační autority, samozřejmě, technicky vzato mimo okénka, někde na serveru autority, převedena a zabezpečena na výsledný certifikát vydávající autoritou, ke kterému připojuje vlastní certifikát. Klient tak obdrží soubor, pomocí kterého pak může ve vlastní počítači vytvářet už zmíněný *zaručený elektronický podpis založený na certifikátu kvalifikované certifikační autority*.

#### Zdroje

KALUŽA, Jindřich a Ludmila KALUŽOVÁ, 2012. *Informatika*. Havlíčkův Brod: Ekopress, 2012. 130 s. ISBN 978-80-86929-83-5.

Microsoft, 2005. *Web Service Security: Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0* [online]. Microsoft, 2005, [cit. 2015-05-01]. Dostupné z: [http://download.microsoft.com/download/8/d/6/8d608524-0763-48b5-840b-0ae446996a14/MS\\_WSS\\_Dec\\_05.pdf](http://download.microsoft.com/download/8/d/6/8d608524-0763-48b5-840b-0ae446996a14/MS_WSS_Dec_05.pdf)



## 6 ZÁVĚR

*You must realize, that fear is not real.  
It is a product of thoughts you create.  
Do not misunderstand me, danger is very real,  
but fear is a choice.*

*- After Earth, 2013*

Možná je opravdu strach v nás jen myšlenkou, i když hrozby jsou reálné, strach a obavy z nich jsou jen naší volbou. Můžeme se s ní poprat, můžeme s ní něco dělat!

Snažili jsme se v této diplomové práci rozebrat a znova poskládat bezpečnostní témata ve výuce středních škol, v prostředí těch bezbranných, kteří věci neznají, snaží se je zjistit, většinou to tak bývá. Učení je náročný proces, během kterého si přebudováváme znovu a znovu naši vlastní představu o učivu, sami si ji korigujeme a vylepšujeme, až časem bude odpovídat požadavkům na správnost - dosáhneme pochopení. Toto si mnozí učitelé neuvědomují, jen hrnou a hrnou novou frontální výuku na své žáky a pak je otestují. Pak jsou všichni překvapení, jak to je jen možné? Jste se neučili?!

Řešení je snadné, stačí si opakovat, procvičovat, dokola a neustále. Zažívat nové výzvy, zkoušet si věci, dělat zajímavé úkoly, protože mohou motivovat – podle Maslowa – je potřeba seberealizace a tvořivosti tou nejvyšší z potřeb správného sebe naplnění, třebaže jde jen o žáky, oni se svými úspěchy pochlubí... a přitom se tolik naučili.

Z pohledu změn v učení se přikláníme k názoru inovovat, opustit vykládání a přejít k procvičování, děláním, jak jen to bude možné. Protože při úkolech a všech činnostech obecně lze zažívat radost i zklamání, protože každý emoční vjem je mnohem trvalejší, než slyšené slovo, odvykládané učivo. Vymýšlejme takovéto úkoly. Nebojme se ani žáky stimulovat odměnami, nejen známkami, ale čímkoliv, co se namane, i nálepka udělá kouzlo, pochvala zavazuje k příštím výkonům. Nebojme se žáky provokovat, oni jsou ve škole proto, aby poslouchali a plnili, co jim bylo tím chytřejším přikázáno. Třebaže se cítí zrovna těmi nejchytřejšími oni sami, že jsme

je rozčílili. Ve většině případů si vzpomínáme na ty zlé učitele, kteří pořád něco požadovali. Věříme, že tímto způsobem nás vychovali více, do života, tam je zlých lidí hromada, umíme se s tím nějak srovnat.

Pojednali jsme v začátku této práce také o tom, že vzdělávání je jen částí edukace, druhou neviditelnou část tvoří výchova – neustále vystavování stejným problémům formuje osobnost, mění postoje a vnímání hodnot. Tyto cíle jsou v bezpečnosti nanejvýš důležité, je potřeba začít myslet jinak – obezřetně, v předstihu, tušit problémy a rizika předem. A toto je velice nesnadný úkol ve výuce bezpečnosti, jak neznalého vůbec poučit o všech hrozbách, aby se jen nenaučil odvykládat, ale aby chápal některé souvislosti, širší kontext a přesah.

Jak jsme uvedli v praktické části ve své analýze, je zřejmým cílem rámcových vzdělávacích programů provazovat jednotlivé tematické kapitoly do jednoho celku, opakovat, na různých místech, v různých předmětech se dozvědět to samé. A to není na škodu, opakované vystavování podobným tématům má i během 4letého života středoškoláka výchovný charakter.

Našli jsme výborný zdroj společných požadavků na úroveň získaných vědomostí – katalogy požadavků od Centra pro zjišťování výsledků vzdělávání. I když v oblasti informatiky v současnosti nejsou tím výchozím platným dokumentem, jsou pořád lepší než nic. Informatika a bezpečnost IT, vůbec snaha chránit data, uživatele, jejich komunikaci a také znát kryptografické pojmy je podle nich jasně daným požadavkem státu na bezpečnostní témata ve výuce na střední škole.

Přehled pojmů z IT bezpečnosti, pár zábavných slidů o detekci hrozeb, ale i zcela vážnou kryptografii jsme zpracovali do studijních materiálů.

## 7 BIBLIOGRAFIE

1. ANDRESS, Jason a Russ ROGERS, 2011. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Amsterdam: Elsevier, xviii, 171 s. ISBN 978-1-59749-653-7.
2. ARMSTRONG, Michael, 2002. *Řízení lidských zdrojů*. Havlíčkův Brod: Grada, 856 s. ISBN 80-247-0469-2.
3. BALABÁN, Miloš, DUCHEK, Jan a Libor STEJSKAL, 2007. *Kapitoly o bezpečnosti*. Vyd. 1. Praha: Karolinum, 2007. 428 s. ISBN 978-80-246-1440-3.
4. BRABEC, František, 2001. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001. 400 s. ISBN 80-86445-04-6.
5. CERMAT, 2012. *Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika: vyšší forma zakončení: platný od školního roku 2011/2012*. Praha: Centrum pro zjišťování výsledků vzdělávání, 2012.
6. DOSEDĚL, Tomáš, 2004. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
7. FIALA, Petr, 2013. In: *Otázky Václava Moravce*. TV, ČT24, 2013-03-03. Dostupné z: <http://www.ceskatelevize.cz/porady/1126672097-otazky-vaclava-moravce-2-cast/213411030510303/video/>
8. KALUŽA, Jindřich a Ludmila KALUŽOVÁ, 2012. *Informatika*. Havlíčkův Brod: Ekopress, 2012. 130 s. ISBN 978-80-86929-83-5.
9. KUNDRA, Ondřej a Erik TABERY, 2009. Chci změnit školu, ne děti. *Respekt*. 2009, roč. XX, č. 5. s. 50-53. ISSN 0862-6545.
10. Microsoft, 2005. *Web Service Security: Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0* [online]. Microsoft, 2005, [cit. 2015-05-01]. Dostupné z: [http://download.microsoft.com/download/8/d/6/8d608524-0763-48b5-840b-0ae446996a14/MS\\_WSS\\_Dec\\_05.pdf](http://download.microsoft.com/download/8/d/6/8d608524-0763-48b5-840b-0ae446996a14/MS_WSS_Dec_05.pdf)

11. MORAVEC, Václav, 2014. In: *Otázky Václava Moravce*. TV, ČT24, 2014-06-29.  
Dostupné z: <http://www.ceskatelevize.cz/porady/1126672097-otazky-vaclava-moravce/214411030510629-otazky-vaclava-moravce-2-cast/>
12. NUV, 2015. *Čeští žáci zabodovali v ICT gramatnosti*. IN: *Vzdělávání*, čtvrtletník Národního ústavu pro vzdělávání, 1/2015. Dostupné z: [http://www.nuv.cz/uploads/Periodika/VZDELAVANI/15/1\\_15.pdf](http://www.nuv.cz/uploads/Periodika/VZDELAVANI/15/1_15.pdf)
13. PETTY, Geoffrey, 2008. *Moderní vyučování*. Vyd. 5. Praha: Portál, 380 s. ISBN 9788073674274.
14. POTŮČEK, M., 2004. *Zpráva o stavu země. Strategické volby, před nimiž stojí*. Praha, FSK Univerzity Karlovy, CESES, 2004.
15. PROKEŠ, Josef, 2000. *Školní pedagogika [učební text]*. [Cit. 2015-05-08].  
Dostupné z: <http://www.fi.muni.cz/~qprokes/pedagogika/index.html>
16. ROUBAL, Pavel, 2012. *Informatika a výpočetní technika pro střední školy - Teoretická učebnice*. Brno : Computer press, 2012. 104 s.
17. SAK, Petr a Jiří MAREŠ, 2007. *Člověk a vzdělání v informační společnosti*. Vyd. 1. Praha: Portál, 2007, 290 s. ISBN 978-80-7367-230-0.
18. SKÁLOVÁ, Jarmila, 2007. Kategorie vzdělání a pojetí vzdělávání v soudobé učící se informační společnosti. In: SAK, Petr a Jiří MAREŠ. *Člověk a vzdělání v informační společnosti*. Vyd. 1. Praha: Portál, 2007, str. 91-131. ISBN 978-80-7367-230-0.
19. VLČKOVÁ, Kateřina, 2005. *Základní pedagogické kategorie a pojmy* [materiál k výuce]. [Cit. 2015-05-08]. Dostupné z: [http://is.muni.cz/elportal/estud/lf/ps05/mpmp071/ped\\_kategorie.doc](http://is.muni.cz/elportal/estud/lf/ps05/mpmp071/ped_kategorie.doc)
20. ZOUNEK, Jiří a Petr SUDICKÝ, 2012. *E-learning: učení (se) s online technologiemi*. Vyd. 1. Praha: Wolters Kluwer Česká republika, xix, 226 s. ISBN 978-80-7357-903-6.

## 8 PŘÍLOHY

Součástí této práce jsou následující autorské prezentace k výuce na SŠ:

- Počítačová bezpečnost
- Firewall
- IDS, IPS
- Elektronický podpis

Doporučujeme také použít studijní text:

- Kryptografie pro SŠ
- Elektronický podpis pro SŠ

## Počítačová bezpečnost

Lukáš Jakubík

## Softwarové hrozby

- **Všeobecně malware** (z angl. malicious)
  - Počítačový program určený ke vniknutí nebo poškození počítačového systému
- **Spyware**
  - Bez vědomí uživatele shromažďuje a odesílá data
    - Keylogger
- **Bootsektorové viry**
  - Nacházejí se v bootovacích oblastech disket, CD
  - Namísto zavedení OS se sami kopírují do paměti

## Softwarové hrozby II.

- **Viry**
  - Malý program, který se umí vložit do jiného programu a s ním se šířit
    - 1982 „Elk Cloner“ vir na Apple
    - 1986 „Brain“ pákistánský vir šířen na disketách světem
- **Červy**
  - Program, který je schopen se šířit sám, bez hosta
    - 2000 „I Love You“ – VBS skript přiložen do emailové správy a spuštěn automaticky emailovým klientem

## Softwarové hrozby III.

- **Trojský kůň**
  - Malware umístěn do systému pod zástěrkou jiné funkcionality
    - Password-stealing (PWS)
    - Dropper
    - Proxy Trojan
- **Makrovir**
  - Napadají dokumenty Microsoft Word a Excel
  - Využití Visual Basic for Application
    - W97M/Melissa

## Softwarové hrozby IV.

- **Rootkit** („sada nástrojů pro správce“)
  - 2005 Sony vydává audio CD se skrytým softwarem
    - Extended copy protection (XCP)
  - Šlo o rootkit bránící kopírování CD
  - Po vložení CD se nainstaloval přehrávač CD v PC, společně s aplikací, která skrývala některé systémové soubory a znemožnila zkopírování CD
  - Toto skrývaní souborů s předponou \$sys\$ mohl využít i jiný útočník

## Společenské hrozby

- **Sociální inženýrství**
  - způsob získávání důležitých informací od uživatelů bez jejich vědomí
- **Druhy útoků**
  - I. Přímý přístup
  - II. Důležitý uživatel
  - III. Bezmocný uživatel
  - IV. Pracovník technické podpory
  - V. Obrácená sociotechnika

## Společenské hrozby II.

- **Kevin Mitnick (\*1963)**
  - Označen jako nejlepší hacker v dějinách
  - Ukradl několik tisíc souborů s daty a nejméně 20 000 čísel kreditních karet, tisícovky megabajtů chráněného SW
  - Naboural se do počítače Velitelství vzdušné obrany Severní Ameriky a další
  - Používal důmyslné techniky k ovlivňování lidí
  - Jedna z nejhledanějších osob v historii FBI
  - Soudním výrokem mu byl zakázán jakýkoliv přístup k PC
  - Kniha *Umění klamu*



## Bezpečnostní software

- **Antivirové programy**
  - Kontrolují data na základě virové databáze
  - Neznámé hrozby pomocí inteligentní heuristiky
    - Alwil Avast!
    - AVG Internet Security 2012
    - Norton AntiVirus 2012
    - ESET Smart Security 5





## Bezpečnostní software II.

### • Firewall

- Odděluje provoz mezi dvěma sítěmi – propouští data jedním nebo druhým směrem podle předem definovaných pravidel
- Jako součást OS – jen vstupní filtry (nutný základ)
- Jako samostatná aplikace (hodně dotazů)
- Podniková proxy brána (omezení obsahu)
- UTM (profesionální řešení)
  - SonicWALL UTM Firewall

## Hrozby z Internetu

### • Adware

- Znepříjemňuje práci na PC neustálou reklamou
- Příznaky: vnucování stránek, pop-up okna atd.

### • Falešné produkty

- Falešné antispywarové a jiné bezpečnostní produkty
- Instalujeme např. na základě odkazů ze spamu

### • Dialer

- Mění způsob přístupu na Internet, používán u vytáčeného připojení, změna na zahraničního ISP

## Hrozby z Internetu II.

### • Phishing

- První kontakt je většinou přes důvěryhodný e-mail
- Obsahuje překrytý URL odkaz na podvržené stránky
- Snaha o získání citlivých informací

### • Pharming

- Přesměrování na podvodné stránky formou změny DNS záznamu – těžko detekovatelné uživatelem
- Pokročilá snaha o získání citlivých informací
- Často vyžaduje pomoc trojského koně

## Hrozby z Internetu III.

### • Tracking cookie („sledovací cookie“)

- Identifikuje uživatele a připraví pro něj upravenou webovou stránku, podle jeho předešlé historie

### • Exploit („bezpečnostní díra“)

- Využívají známých bezpečnostních děr v operačních systémech
- Využívá se poté k dalšímu spouštění škodlivého software
- Ochrana je v neustálé aktualizaci všeho softwaru



## Hrozby z Internetu IV.

- **Hijacker („únosce“)**
  - Přímo napadá Internet Explorer, e-mailový klienty, případně i operační systém
  - Mění nastavení – získává plnou kontrolu nad systémem
- **Backdoor („zadní dvířka“)**
  - Po spuštění postiženého souboru se ukryje v systému a vyčkává na kontakt zvenčí
  - Tvůrce viru má poté přístup na postižený PC

## Cracking

- Cracking je zásah do spustitelného programu
- Často za účelem prolomení ochrany proti neoprávněnému použití
  - Crackování her
  - Odemčení nepřístupných funkcí
- **Nástroje pro crackery**
  - Disassembler (zpětně analyzuje spustitelný soubor)
  - HEX editor (umožňuje editaci binárních dat)
  - Debugger (odhaluje chyby, zefektivňuje crack)

## Cracking II.

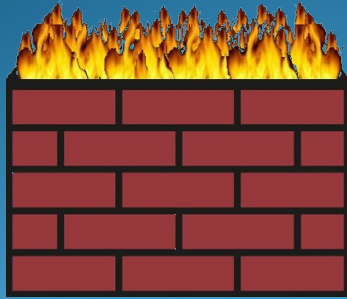
- **Anticracking ochrany**
  - Snaha omezit šíření a crackingové úpravy spustitelných souborů
    - Registrační číslo
    - Klíčový soubor
    - Kontrola originálního CD a ochrany na něm
    - Hardwarový klíč
    - Zmatečný kód
    - Závislosti mezi soubory aplikace
    - ...

## Odkazy

- <https://sites.google.com/site/intomatika/antivirove-programy>
- <http://www.antivirovecentrum.cz/firewally.aspx>
- <http://programujte.com/clanek/2006080803-cracking-2-cast/>
- <http://programujte.com/clanek/2006080401-cracking-1-cast/>
- <http://www.spyware.kvalitne.cz/>
- <http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx>
- <http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm>
- <http://www.avg.com/cz-cs/caste-dotazy.num-2334>
- <http://owebu.blogger.cz/Bezpecnost/Nebezpeci-na-internetu-Exploit-Hijacker-a-BHO>
- <http://zivotopis.osobnosti.cz/kevin--mitnick.php>

# Firewall

Porty, NAT, rozdělení



- Lukáš Jakubík

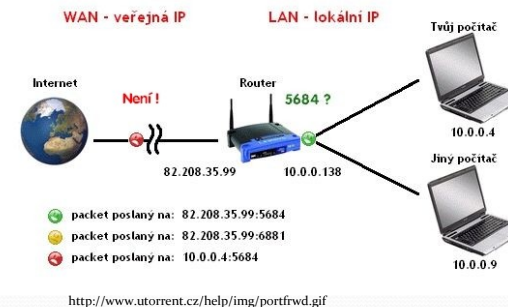
## Port

- **Síťový port** je číslo, které slouží u protokolů TCP, UDP k rozlišení komunikace na dané IP adrese
  - portem se rozumí "dveře" nebo "brána" do počítače
  - na portu aplikace poslouchá a čeká na komunikaci
  - je daný číslem v rozsahu 0-65535
  - *IP adresa:port* 192.168.0.1:80
- typické porty
  - pro **ssh** 22, pro **smtp** 25, pro **web** 80, pro **https** 443
  - od 50000 volné, jinak rozdělení a registraci určuje IANA (Internet Assigned Numbers Authority)

## NAT

- **NAT** (network address translation) je proces překladač vnější adresy na adresu z vnitřní sítě
  - nastavuje se v směrovači, NAT tabulka, pravidla typu *vnější IP adresa směrovače:port » vnitřní IP adresa:port*
  - typicky je potřeba
    - pro přístup k nějaké službě vevnitř sítě (web, mail, ssh)
    - pro přímý download (utorrent)
    - pro spojení počítačových her v síti apod.
  - v minulosti se pomocí NAT řešil nedostatek IPv4 adres

## NAT tabulka



<http://www.utorrent.cz/help/img/portfwd.gif>

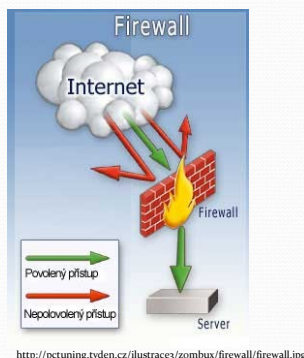
25 - ADVANCED PORT FORWARDING RULES				
Remaining number of rules that can be created: 25				
Name	Application Name	Port	Traffic Type	
utorrent	<< Application Name >>	Public Port 5684 ~ 5684	TCP	
IP Address 10.0.0.4	<< Computer Name >>	Private Port 10000 ~ 10000		

- první paket se směrovačem podle NAT tabulky doručí na tvůj počítač
- druhý paket směrovač zahodí jako nedoručitelný, protože pro něj nemá pravidlo v NAT
- třetí paket je ztracen již po cestě jako nesmyslný (má neveřejnou adresu)



## Co to je firewall?

- Ohnivzdorná zeď, ale propustná, síto, co stojí mezi místní sítí (LAN) a světem (WAN)
- **Kontrolní bod**, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje
- Typy firewallů
  - **hardwarově samostatné zařízení** (i počítač) / **síťový**
  - **softwarový nástroj** v OS koncového počítače / **osobní**



## Principy firewallu

- Základním posláním je chránit počítače umístěné v síti za firewallem **před útokem zvenčí** pomocí
  - zavíráním portů, skrýváním počítačů (NAT tabulka)
  - aktivní kontrolou hlaviček paketů
  - aktivní kontrolou dat v paketech
- Některé pokročilejší firewally dokážou chránit i vnitřní počítače před únikem dat zevnitř ven
- Firewall **je řízen pravidly**, které bývají přednastaveny, ale nakonec vždy záleží na obsluze, co zakáže, nebo co (omylem) povolí

## Historie vývoje firewallů

- 1. Nestavové paketové filtry
- 2. Stavové paketové filtry
- 3. Aplikační brány (proxy firewally)
- 4. UTM (Unified Threat Management)

## Paketové filtry

- **Paket** je blok dat přenášených v počítačových sítích, obsahuje hlavičku (režijní informace) a data
- **Paketový filtr** kontroluje pakety, z jaké adresy a portu přicházejí a na jakou adresu a port jdou
  - doručení paketu ovlivňují striktní pravidla v firewallu
  - výhodou je rychlá kontrola paketů
  - nevýhoda je nízká bezpečnost a často minimální přizpůsobitelnost, omezena jen na IP adresy a porty

## Stavové paketové filtry

- **Stavové paketový filtry** navíc dokážou uchovat stav
  - po ustavení komunikace *IP:port* <>> *IP:port* si uloží stav a tuto komunikaci dále nekontrolují
  - mají režim, který nepovolí jinou komunikaci
  - výhodou může být ještě rychlejší kontrola
  - nevýhodou zůstává malá nastavitelnost a práce s pakety jen na síťové vrstvě

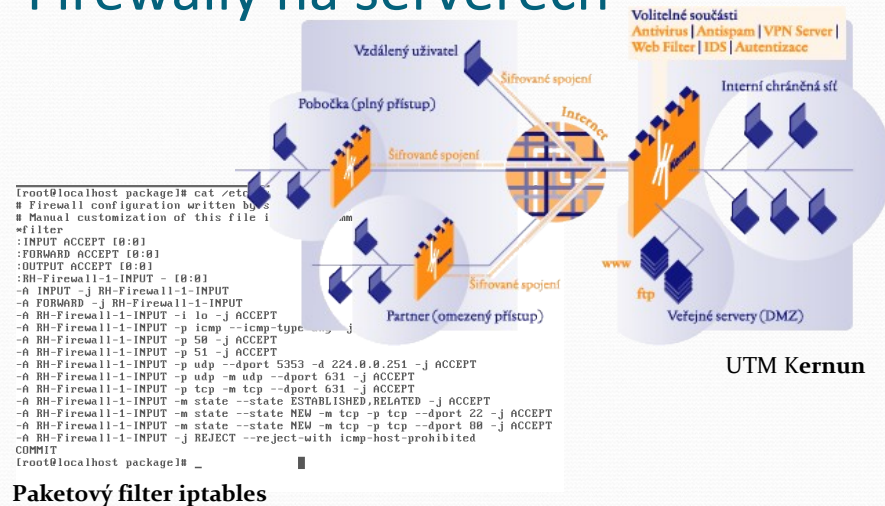
## Aplikační brány

- **Proxy** je server, přes který jsou směrována data klientů
  - za účelem ochrany anonymity, nebo bezpečnosti
  - často i kvůli agregaci dat a filtrování obsahu
- **Aplikační brána** je firewall, který kontroluje pakety již na aplikační vrstvě pomocí svojí proxy
  - vynucená kontrola jdoucí až do vnitřku paketů, na data
  - možno zakázat jednotlivé příkazy, nebo akce uživatele
  - výhodou je vysoké zabezpečení, mnoho možností nastavení a filtrování
  - nevýhodou jsou vysoké požadavky jak na hardware, software, tak i na obsluhu

## UTM

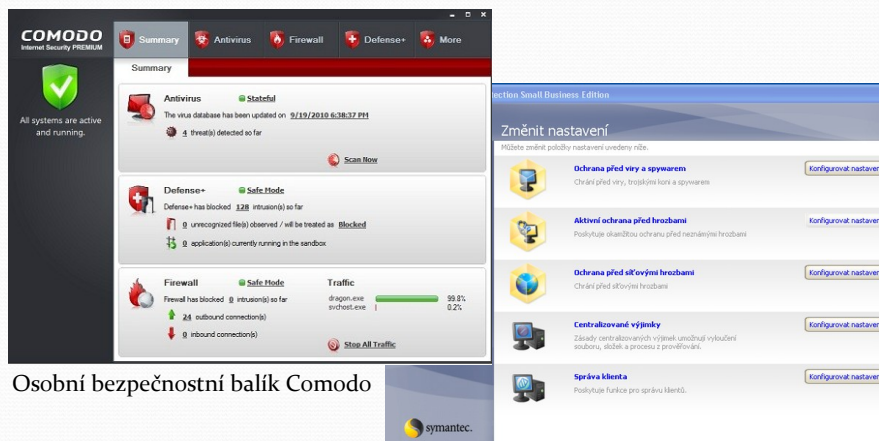
- **UTM (Unified Threat Management)**
  - komplexní řešení pro korporace, sjednocující vícero bezpečnostních prvků v jednom balíku
    - firewall
    - antivirus
    - anti-spam
    - antispyware
    - filtrování obsahu
    - detekce (IDS nebo IPS)
    - QoS (quality of service)
    - DMZ (demilitarized zone)
    - VPN...

## Firewally na serverech





# Firewally na stanicích



Osobní bezpečnostní balík Comodo

Klientská část firewallu Symantec Endpoint Protection

# Symantec Endpoint Protection

- Jde o firewall s antivirem, byznys řešení na vícero PC, z dálky nastavitelný
- Obsahuje i IDS, který může kromě detekce útoku zvnějška zamezit i odnosu citlivých dat z firmy

Konfigurovat pravidla brány firewall

Pravidla brány firewall povolují, blokuji a protokolují provoz sítě.

Název pravidla	Hostitelé	Porty a protokoly	Akce	Síťové adaptéry
<input checked="" type="checkbox"/> Povolit ovladač NDISUIO.SYS	Všichni hostitelé	Všechny porty a protokoly	Povolit	Všechny síťové a...
<input checked="" type="checkbox"/> Povolit protokol RDP (Remote Desktop Protocol)	Všichni hostitelé	Místní porty TCP 3389; příchozí prov...	Povolit	Všechny síťové a...
<input checked="" type="checkbox"/> Blokovat protokol IPv6 (sít Ethernet typu 0x86dd)	Všichni hostitelé	typ sítě Ethernet 34525; příchozí i od...	Blokovat	Všechny síťové a...
<input checked="" type="checkbox"/> Blokovat vzdálený port UDP 3544 protokolu IPv6 over IPv4 (Tere...	Všichni hostitelé	Vzdálené porty UDP 3544; příchozí i o...	Blokovat	Všechny síťové a...
<input checked="" type="checkbox"/> Povolit bezdrátový provoz protokolu EAPOL	Všichni hostitelé	typ sítě Ethernet 0x888E; příchozí i o...	Povolit	Všechny síťové a...

# Zdroje

- Wikipedia contributors. *Port number* [Internet]. Wikipedia, The Free Encyclopedia; 2015-01-13, 15:52 UTC [cit. 2015-05-17]. [http://en.wikipedia.org/w/index.php?title=Port\\_number&oldid=407674054](http://en.wikipedia.org/w/index.php?title=Port_number&oldid=407674054)
- Přispěvatelé Wikipedie. *Firewall* [Internet]. Wikipedie: Otevřená encyklopedie; 2015--01-15, 01:34 UTC [cit. 2015-05-17]. Dostupné na: <http://cs.wikipedia.org/w/index.php?title=Firewall&oldid=6351294>
- Řešení pro prostředí s vysokými požadavky na bezpečnost [Internet]. TNS, aktualizované 2008-07-17 [cit. 2015-05-17]. Dostupné na: <http://www.tns.sk/prod/firewall.html>
- Wikipedia contributors. Symantec Endpoint Protection [Internet]. Wikipedia, 2015-01-12, 18:55 UTC [cit. 2015-05-17]. [http://en.wikipedia.org/w/index.php?title=Symantec\\_Endpoint\\_Protection&oldid=407514757](http://en.wikipedia.org/w/index.php?title=Symantec_Endpoint_Protection&oldid=407514757)

Product	Product score	Level reached	Protection level	Recommendation	Report	Award
Comodo Internet Security 4.0.141842.828 FREE	100 %	10+	Excellent – 100 %	GET IT NOW! <sup>1</sup>		
Online Solutions Security Suite 1.5.14905.0	99 %	10+	Excellent	GET IT NOW! <sup>1</sup>		
Outpost Security Suite Free 7.0.4.3418.520.1245.401 FREE	97 %	10+	Excellent	GET IT NOW! <sup>1</sup>		
Outpost Security Suite Pro 7.0.1.3376.514.1234.401	97 %	10+	Excellent	GET IT NOW! <sup>1</sup>		
Kaspersky Internet Security 2011 11.0.1.400	92 %	10+	Excellent	GET IT NOW! <sup>1</sup>		
Malware Defender 2.6.0	90 %	10	Very good	N/A		
Privatefirewall 7.0.21.1 FREE	86 %	9	Very good	N/A		
BitDefender Internet Security 2011 14.0.24.330	84 %	10+	Very good	GET IT NOW! <sup>1</sup>		
ZoneAlarm Extreme Security 9.1.008.000	59 %	7	Poor	Not recommended		
Rising Internet Security 2010 22.33.00.01	55 %	8	Poor	Not recommended		
PC Tools Firewall Plus 6.0.0.88 FREE	51 %	7	Poor	Not recommended		
Norton Internet Security 2011 18.1.0.37	40 %	6	Very poor	Not recommended		
Jetico Personal Firewall 2.1.0.7.2412	28 %	4	None	Not recommended		
Dr.Web Security Space Pro 6.0.2.07290	14 %	3	None	Not recommended		
CA Internet Security Suite Plus 2010 6.0.0.285	12 %	3	None	Not recommended		
F-Secure Internet Security 2010 10.00.246	9 %	2	None	Not recommended		
Trend Micro Internet Security Pro 2010 17.50.1647.0000	9 %	2	None	Not recommended		
FortKnox Personal Firewall 6.0.205.0	7 %	2	None	Not recommended		
ZoneAlarm Free Firewall 9.2.076.000 FREE	7 %	2	None	Not recommended		
ESET Smart Security 4.2.64.12	6 %	2	None	Not recommended		
avast! Internet Security 5.0.418.0	3 %	1	None	Not recommended		
Avira Premium Security Suite 10.0.0.542	3 %	1	None	Not recommended		
AVG Internet Security 2011 10.0.1153	3 %	1	None	Not recommended		
McAfee Internet Security 2010 11.0.378	3 %	1	None	Not recommended		
G Data InternetSecurity 2011 21.1.1.0	2 %	1	None	Not recommended		

<http://www.matousec.com/projects/proactive-security-challenge/results.php>

# IDS, IPS bezpečnost



Lukáš Jakubík

## IDS – systém detekce narušení

- ◆ IDS (intrusion detection system) je systém, sada nástrojů, metod a zdrojů jak identifikovat a hlásit nežádoucí síťové aktivity
- ◆ nedetekuje samotné narušení, **pouze hlásí narušující aktivity**, nezabrání narušení, jen nás varuje
- ◆ není samostatné ochranné opatření, potřebuje další součásti k ochraně
  - ◆ *I ten sebelepší alarm v autě vyžaduje, aby někdo vstal z postele a podíval se z okna, proč houká.*
  - ◆ *Jak na pozorovanou událost pravděpodobně vedoucí k odcizení auta vlastně reagovat?*



## Narušení bezpečnosti

- ◆ **bezpečnost není stav, ale proces**
- ◆ rozlišuje se mezi útokem a narušením
  - ◆ **útokem** se myslí pokus o narušení
  - ◆ kdežto **narušení** je aktivní posloupnost odpovídajících událostí, které se záměrně snaží uškodit takovou měrou, že **systém se stává nepoužitelným**
- ◆ *firewall lze srovnat se zamčenými dveřmi*
- ◆ *IDS s alarmním systémem*
- ◆ *a IPS s hlídacími psy*
- ◆ *Jak ochrání alarm náš majetek?*



## IPS – systém prevence narušení

- ◆ IPS (intrusion prevention system) je monitorovací systém v síti, který **reaguje na narušující události podle předdefinovaných pravidel**
- ◆ IPS někdo považuje za nástupce IDS, jiní jako nutný doplněk k detektorům IDS
- ◆ IPS musí dokázat prosadit zabezpečení, reagovat na narušení
- ◆ *Rozmístění alarmů a senzorů na všechny okna, dveře, nákup bojových psů, je zbytečný, když je garáž otevřena a psy ze své ohrady ani nevyběhnou.*



## IDS a IPS v praxi

- ♦ jsou nesrovnatelně efektivnější než člověk, avšak jen reagují na narušení, nedokáží průniku předejít
- ♦ všechno se zaznamenává
- ♦ nenahrazují člověka, odborníka, který je nastavuje a narušení vyhodnocuje
- ♦ principiálně se detekce dělá pomocí
  - ♦ databáze vzorků útoků, známých exploitů
  - ♦ statistického vyhodnocování
  - ♦ stavové, behaviorální analýzy
- ♦ příkladem IDS+IPS je **Snort**



## Zdroje

- ♦ ENDORF, Carl – SCHULTZ, Eugene – MELLANDER, Jim. Detekce a prevence počítačového útoku. Praha: Grada Publishing 2005. ISBN 80-247-1035-8
- ♦ Wikipedia contributors. *Intrusion detection system* [Internet]. Wikipedia, The Free Encyclopedia; 2011-01-15, 18:32 UTC [cit. 2015-05-18]. [http://en.wikipedia.org/w/index.php?title=Intrusion\\_detection\\_system&oldid=408058101](http://en.wikipedia.org/w/index.php?title=Intrusion_detection_system&oldid=408058101).
- ♦ Obrázky převzaty z
  - ♦ [http://www.astickerheaven4u.com/catalog/SnoopySleepingOnDoghouse\\_thumb.jpg](http://www.astickerheaven4u.com/catalog/SnoopySleepingOnDoghouse_thumb.jpg)
  - ♦ [http://1.bp.blogspot.com/\\_mfvHDMw0Zlw/SwbZikviKvI/AAAAAAAAAK4/eIYw3EiOWTk/s320/snoopy-is-joe-cool-peanuts-254005\\_1024\\_768.jpg](http://1.bp.blogspot.com/_mfvHDMw0Zlw/SwbZikviKvI/AAAAAAAAAK4/eIYw3EiOWTk/s320/snoopy-is-joe-cool-peanuts-254005_1024_768.jpg)
  - ♦ <http://kruse-jensen.com/html/video2.html>
  - ♦ <http://www.fanpop.com/spots/peanuts/>





## Elektronický podpis

Lukáš Jakubík

## Motivačně

Celá osobní komunikace, nyní přenesena do světa Internetu, stojí na důvěryhodnosti v email

### • Věříte tomu, co vám přijde emailem?!



Vytvořit email s podvrženou identitou (*fake email*) není tak těžká věc – freeSMTP serverů je dost

### • Věříte tomu, co čtete, že mohl napsat váš známý?!



Dostat se k heslu (*keylogging*) nebo využít slabou chvíli (*social engineering*) majitele účtu jde snadno

### • Používejte elektronický podpis!

... sken podpisu není to, oč tu kráčí



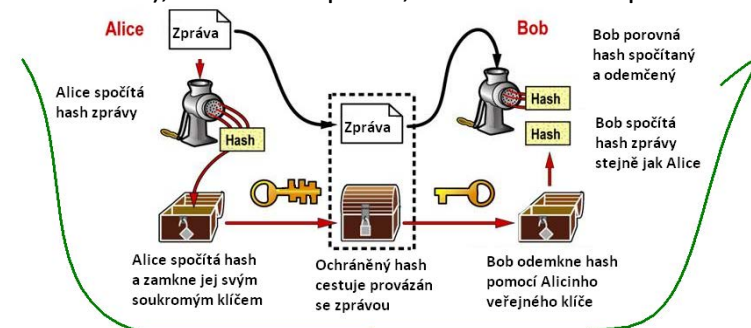
## Principy z kryptografie

- Potřebujeme data chránit  
**důvěrně (šifrovat, utajovat)**  
**důvěryhodně (podepisovat, razítkovat)**
- Běžně známe symetrické metody (společný klíč) které jsou však nepoužitelné při větším počtu lidí
- Využívají se spíše **asymetrické metody** (klíčový pár veřejného a soukromého klíče), protože veřejný můžeme zveřejnit a rozšiřovat i neznámým lidem

klíč/činnost	šifrování	podepisování
veřejný	kdokoliv zašifruje	kdokoliv ověří
soukromý	jen my odšifrujeme	jen my podepíšeme

## Digitální podpis

- Je mechanismus zajišťující **nepopiratelnost dat** (důkaz pravosti zprávy), že ji napsala právě Alice
- Hash** je otisk dat, chrání **integritu** (důkaz, že se nic nezměnilo), že nikdo nepřidal, nezměnil nic v zprávě





## Elektronický podpis

- Je digitální podpis s integritou, který má navíc i vlastnost **autenticity** (je jednoznačně jasné komu patří, kdo podepsal)
- Je kodifikován ve směrnici EU 1999/93/ES v místním zákonu č. 227/2000 Sb. o elektronickém
- Jako **kvalifikovaný elektronický podpis** již plně nahrazuje rukou psaný podpis v rámci zemí EU
- Souvisí s certifikátem, který musí být vydán akreditovanou kvalifikovanou certifikační autoritou



## Certifikát a certifikační autorita

- Certifikát je důvěryhodný dokument potvrzující nějakou skutečnost (občanský průkaz s fotografií)
- Elektronický certifikát je jistý datový soubor, který se používá na **důvěryhodné provázání identity a veřejného klíče** (certifikát s emailem a klíčem)
- Certifikát vydává certifikační autorita, která ověřila data v něm a stvrzuje je tím, že certifikát podepíše
- Bohužel, každý si může udělat vlastní certifikát i celou certifikační autoritu  
... jen málo jich je skutečně důvěryhodných

## Certifikační autorita Comodo

- Komerční bezpečnostní společnost s celým spektrem produktů a služeb
- Jedna z posledních světových autorit, které vydávají **emailové certifikáty pro běžné použití zdarma**
- Standardně předinstalovaná a důvěryhodná ve **většině emailových klientů**



## Certifikační autorita PostSignum

- jedna z **kvalifikovaných certifikačních autorit**
- vlastněná Českou poštou, akreditovaná MV
- vydává kvalifikované certifikáty již od září 2005
- dostupná **na poště**, kde je i CzechPOINT
- přiděluje i identifikátor sociálního zabezpečení
- probojovala se na seznam kořenových certifikátů Microsoftu, tedy jí vydané certifikáty by měli být **taky rozeznány jako důvěryhodné**



## Certifikační autorita po vás chce

- doma vygenerovaný veřejný klíč – na USB nebo zaslaný
- elektronickou žádost podepsanou soukromým klíčem
- 2 doklady totožnosti
- kopu papírů (2 smlouvy, 2 formuláře, 2 povolení...)
- 400 Kč

• *8 fyzických podpisů  
jeden elektronický*



o

## Praxe

- na elektronické podepisování emailů je potřebný emailový klient s podporou S/MIME ~ Thunderbird
- musíme si vytvořit soukromý a veřejný klíč
- požádat certifikační autoritu o vydání certifikátu, kde bude naše emailová adresa a náš veřejný klíč
- certifikát (záloha.p12) **nikdy nikomu nesvěříme**, jen svému emailovému klientu, který chráníme heslem
- posíláme, přijímáme a ověřujeme podpisy zvesela

## Certifikační autorita je



- Dostupná
  - ale plexisklem chráněná
- Vytížená
  - ale v pořadí dosažitelná
- Ochotná
  - ale předpisově striktní
- Milá a znalá!
  - nato jak je placená

Děkuji za vaši účast a pozornost

### Použité zdroje

DOSTÁLEK, L. – VOHNOUTOVÁ, M. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. Brno: Computer Press, 2009. 534 str. ISBN 978-80-251-2619-6

NEVOSÁD, L. *Jak jsem si pořídil elektronický podpis České pošty* [online]. Lupa.cz, 19. 9. 2005. [cit. 2015-02-15]. Dostupné z: <http://www.lupa.cz/clanky/jak-jsem-si-poridil-elektronicky-podpis-ceske-posty/>

*Digital signature* [online]. Hill associates, revize 24 August 2009. [cit. 2015-02-15]. Dostupné z [http://wiki.hill.com/wiki/index.php?title=Digital\\_signature&oldid=10140](http://wiki.hill.com/wiki/index.php?title=Digital_signature&oldid=10140)