Renata Štolfová

E-government a rizika plynoucí z využívání současných ICTs ve státní správě

Rozvoj e-governmentu v ČR. Informační a kybernetická bezpečnost aneb Je třeba se obávat kybernetické války?

(Diplomová práce)

Vedoucí diplomové práce: Mgr. Eva Lebedová

OLOMOUC 2009
Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně na základě uvedených pramenů a literatury.

V Olomouci dne 26. listopadu 2009 Podpis: ..............................
PODĚKOVÁNÍ

OBSAH

OBSAH ................................................................................................................................. 3
Seznam zkratek .......................................................................................................................... 4
ÚVOD ............................................................................................................................................ 6
1. E-GOVERNMENT ................................................................................................................... 17
   1.1. Vymezení pojmu ............................................................................................................... 17
   1.2. Rozvoj e-governmentu v České republice ....................................................................... 23
   1.3. Působení EU na rozvoj e-governmentu v ČR ................................................................. 34
   1.4. Vývoj právního ukotvení e-governmentu a vládních postojů k němu ......................... 39
   1.5. Praktické projevy e-governmentu v ČR ................................................................. 43
       1.5.1. Elektronický podpis ............................................................................................... 43
       1.5.1.1. Novelizace zákona o elektronickém podpisu – kvalifikované časové razítko a elektronická značka .......................................................... 47
       1.5.2. Elektronické doručování a podání ....................................................................... 49
       1.5.3. Czech POINT ........................................................................................................ 52
       1.5.4. Datové schránky ................................................................................................... 53
2. RIZIKA E-GOVERNMENTU A ZNEUŽITÍ ICTs PROTI STÁTU ........................................... 60
   2.1. Bezpečnost a zabezpečení ISVS ................................................................................ 61
   2.2. Informační bezpečnost ..................................................................................................... 66
       2.2.1. Hrozby informační bezpečnosti ............................................................................. 69
       2.2.2. Metody zajištění informační bezpečnosti .............................................................. 71
   2.3. Zneužití ICT prostředků k útokům proti státu .............................................................. 74
       2.3.1. Motivace k útokům v kybernetickém prostoru ......................................................... 78
       2.3.2. Metody kybernetických útoků ............................................................................... 80
       2.3.3. Příklady kybernetických útoků proti státu .............................................................. 81
           2.3.3.1. Kybernetická špionáž ......................................................................................... 82
           2.3.3.2. Kybernetický terorismus .................................................................................. 84
           2.3.3.3. Kybernetická propaganda a hacktivismus ......................................................... 86
   2.4. EU a její pojetí kybernetické a informační bezpečnosti .............................................. 88
ZÁVĚR ........................................................................................................................................ 95
ANOTACE .................................................................................................................................... 104
ANNOTATION .......................................................................................................................... 105
Prameny a literatura ................................................................................................................... 106
   Prameny ................................................................................................................................. 106
   Literatura ............................................................................................................................... 111
   Internetové odkazy ............................................................................................................... 126
ABSTRAKT ............................................................................................................................... 128
ABSTRACT ................................................................................................................................. 129
Seznam zkratek

3G Třetí generace (mobilní telefony třetí generace)
ARES Administrativní registr ekonomických subjektů
B2B Business to Business, vztah obchodníků mezi sebou
B2C Business to Customer, vztah obchodníků k zákazníkům
CERT Computer Emergency Response Team, tým pohotové počítačové reakce
CIA Central Intelligence Agency, Ústřední zpravodajská služba
CIP Competitiveness and Innovation Framework Programme, Rámcový program Konkurenceschopnost a inovace
ČR Česká republika
ČSN Česká technická norma (původně Česká státní norma)
DG Directorate-General, generální sekretariát Evropské komise
DoS Denial-of-Services, odepření služeb
EFTA European Free Trade Association, Evropské sdružení voleného obchodu
ENISA European Network and Information Security Agency, Evropskou agenturu pro síťovou a informační bezpečnost
ePUSA Elektronický portál územních samospráv
EU Evropská unie
EVA Elektronicky vlídná administrativa, Elektronická a Vaše administrativa
FBI Federal Bureau of Investigation, Federální úřad pro vyšetřování
G2B Government to Business, vztah státní správy k obchodníkům
G2C Government to Citizen, vztah státní správy k občanům
G2E Government to Employees, vztah státní správy ke svým zaměstnancům
G2G Government to Government, vztah orgánů veřejné správy mezi sebou
G2P Government to Public, vztah státní správy k veřejnosti
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT</td>
<td>Informační a komunikační technologie</td>
</tr>
<tr>
<td>ISSS</td>
<td>Internet ve státní správě a samosprávě</td>
</tr>
<tr>
<td>ISVS</td>
<td>Informační systém veřejné správy</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology, informační technologie</td>
</tr>
<tr>
<td>ITSEC</td>
<td>Information Technology Security Evaluation Criteria, Kritéria hodnocení bezpečnosti informačních systémů</td>
</tr>
<tr>
<td>KIVS</td>
<td>Komunikační infrastruktura veřejné správy</td>
</tr>
<tr>
<td>LPIS</td>
<td>Land Parcel Information System, informační systém evidující zemědělskou půdu</td>
</tr>
<tr>
<td>MI</td>
<td>Ministerstvo informatiky ČR</td>
</tr>
<tr>
<td>MPO</td>
<td>Ministerstvo průmyslu a obchodu ČR</td>
</tr>
<tr>
<td>MVČR</td>
<td>Ministerstvo vnitra ČR</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization, Severoatlantická organizace</td>
</tr>
<tr>
<td>NPPG</td>
<td>Národní program počítačové gramotnosti</td>
</tr>
<tr>
<td>NSIB</td>
<td>Národní strategie informační bezpečnosti</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Cooperation and Development, Organizace pro ekonomickou spolupráci a rozvoj</td>
</tr>
<tr>
<td>OSN</td>
<td>Organizace spojených národů</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure, infrastruktura veřejných klíčů</td>
</tr>
<tr>
<td>PSP</td>
<td>Policy Support Programme, program na podporu konkrétní politiky</td>
</tr>
<tr>
<td>TCSEC</td>
<td>Trusted Computer System Evaluation Criteria, Kritéria hodnocení zabezpečených počítačových systémů</td>
</tr>
<tr>
<td>WB</td>
<td>World Bank, Světová banka</td>
</tr>
<tr>
<td>Y2K</td>
<td>Year 2000, Rok 2000</td>
</tr>
</tbody>
</table>
ÚVOD

V závěru 20. století jsme se stali svědky ohromného pokroku a rozvoje v užívání informačních a komunikačních technologií (dále jen ICTs). Ty pronikly do reality každodenního fungování současné moderní či spíše post-moderní společnosti. ICTs, a zdůrazňeme zejména Internet či mobilní telefony, které v současnosti již dovedou s tímto médím také pracovat, se staly našimi věrnými společníky v širokém spektru činností.

Většina naší komunikace se děje jejich prostřednictvím v tzv. kybernetickém prostoru. V něm obchodujeme, nakupujeme, ukládáme v něm ohromné objemy dat a informací. Prostřednictvím kybernetického prostoru komunikujeme se svými blízkými a přáteli, ale také v profesních či obchodních záležitostech. Elektronická komunikace začala být využívána také k jednoduššímu navázání kontaktu mezi občany a veřejnou správou v souvislosti se zaváděním a rozvojem praktik e-governmentu de facto ve všech post-moderních společnostech. Státní správa i politici pak využití těchto ICTs často považují za efektivní a inteligentní způsob jak být v kontaktu se svými občany i voliči.

Rozvoj využívání vyspělých ICTs také přinesl poměrně významné změny do fungování současné post-moderní společnosti. Ustálil se pojem informační společnost. Informace jsou považovány za hlavní zdroj, sociálního, ekonomického i kulturního pokroku. Lze také říci, že post-moderní společnost se v tomto ohledu do jisté míry stala závislou na ICTs, které nám tyto informace zprostředkovávají.

Podobně jako jakákoli jiná závislost, tak i tato může být zdrojem zranitelnosti. ICTs mohou být zneužity k nezákonným činům, ale také k narušení bezpečnosti štátu. Komunikační a informační systémy a sítě mohou být narušeny neautorizovaným vstupem. Pokud se pak tyto ICTs stávají nedělitelnou součástí našeho obchodního, politického, ale také osobního života a státních bezpečnostních složek, může tato skutečnost znamenat určité riziko pro správný chod štátu.

Inspiráci k napsání této diplomové práce byly kybernetické útoky na Estonsko na jaře r. 2007. Tato pobaltiská země několik týdnů čelila soustředěnému a koordinovanému útoku proti svým klíčovým
infrastrukturám, hlavně bankovnímu sektoru a vládním komunikačním kanálům. Tyto útoky byly vedeny v kybernetickém prostoru, tedy za použití ICTs. Estonsko bylo paralyzováno a dočasně neschopné zajišťovat běžný chod a služby státu.

Kybernetické útoky v Estonsku vyvolaly zvýšený zájem vědců a pozorovatelů o problematiku kybernetické bezpečnosti i potenciální kybernetické války. Rozsah a úspěšnost těchto útoků vedla k určitému přehodnocení vnímání kybernetické války coby součásti sci-fi a předložila ji k vážnému zájmu a bádání široké veřejnosti i vědecké obce.

Estonsko je charakteristické svou pokročilostí v aplikaci ICTs do různých složek fungování a komunikace společnosti. Pro nás je relevantní zejména rozvoj praxe e-governmentu v rámci veřejné správy. Díky tomu je také někdy tato pobaltská republika přezdívána e-Stonia. Bezprecedentní útok vedený v kybernetickém prostoru ovšem znamenal citelný zásah do integrity toho státu, morálky jeho občanů i jejich důvěry v tento model.

Inspirativní pro tento text se stala právě pokročilost rozvoje služeb a možností e-governmentu aplikovaných v Estonsku. V naší práci proto představíme vývoj, hlavní překážky a úspěchy zavádění jeho praxe ČR od počátku 90. let do současnosti, kdy můžeme pozorovat největší a do určité míry až revoluční změny v oblasti zavádění nástrojů tohoto způsobu veřejné správy. Hovoříme o projektu tzv. datových schránek, který zásadně mění způsob komunikace občana se státní správou a úřady, a také o projektu základních registrů veřejné správy, jež by měly sjednotit a zefektivnit nakládání s údaji a daty spravovanými státními orgány a úřady.

Zaměříme se také na vliv EU a jejích iniciativ pro podporu a rozvoj využívání ICTs ve společnostech jejích členských i kandidátských států. Věříme totiž, že toto působení mělo na rychlost zavádění a aplikace e-governmentu v ČR zásadní vliv. Největší rozvoj je možné zaznamenat v první dekádě tohoto století, resp. posledních několika letech. Je zde patrná korelace s čerpáním finančních prostředků evropských fondů v rámci současného rozpočtového období Unie (2007-2013) pro zajištění prostředků zavádění e-governmentu. Nicméně nelze opomenout ani iniciativy eEurope a na ně navazující i2010, které povzbuzují členské i kandidátské země k rozvoji a využívání post-moderních ICTs, a to hlavně
k zajištění ekonomického pokroku, ale také větší demokracie skrze využívání praktik e-governmentu, který má přivést veřejnou správu blíže k občanovi.

Premisa zrychleného rozvoje zavádění nástrojů e-governmentu v posledních letech je také spojena se stále rychlejším zdokonalováním a zpřístupňováním sofistikovaných ICTs. Tento technologický rozvoj je ale také spojen se zvyšujícím se rizikem zneužití těchto ICTs proti veřejnosti a státu. Další část textu je proto věnovaná informační, resp. kybernetické bezpečnosti, kdy estonská zkušenost nám dala možnost pocítit a uvědomit si riziko, které se v této oblasti v současnosti vyskytuje.

Téma e-governmentu je rozpracováváno zejména v zahraniční literatuře, kde má také jeho praxe delší tradici než v ČR.1 Nicméně i v této oblasti jsme u nás spolu s jeho úspěšnými praktickými projevy v posledních letech zaznamenali výraznější posun. Čeští autoři se však spíše než na teoretická východiska zaměřují právě na praktický výkon e-governmentu. Odpovídá se tak pravděpodobně potřebám současnosti, kdy je nutné vymezen a zmapovat využívání a možnosti tohoto způsobu veřejné správy v ČR. Výrazná část publikací věnujících se e-governmentu má často charakter příruček či návodů, jak se v problematice elektronické správy pohybovat. V této oblasti nicméně lze očekávat další vývoj související s rozvojem e-governmentu, a který je již patrný také v některých studiích menšího rozsahu či diplomových pracích.

Od r. 2001 čtvrtletně vychází časopis E-government, který se zabývá tématem elektronizace a informatizace české veřejné správy i společnosti. Je zaměřen zejména na poskytování relevantních informací pracovníkům státní správy, nicméně dostupný je všem. V jeho rámci je také vydávána výroční publikace The Best obsahující výběr z nejlepších projektů v oblasti elektronizace veřejné správy daného roku.2


2 Časopis E-government je dostupný online na http://www.egovernment.cz/.
V oblasti kybernetické či informační bezpečnosti je možné největší rozvoj výzkumu a literatury sledovat od přelomu milénia. Je to opět spojeno s technologickým rozvojem a rozšířováním užití moderních a vyspělých ICTs do stále většího okruhu lidské činnosti, ať už civilní, tak i vojenské či obranné. Otázka zajištění bezpečnosti informačních a komunikačních sítí se také stala naléhavější v prostředí zvýšených rizik plynoucích z teroristických útoků a nekonvenčních způsobů vedení boje. Svoji roli měl ale také tzv. fenomen Y2K neboli obavy spojené s přelomem milénia.

Výzkum problematiky informační bezpečnosti má nicméně o něco delší tradici. Jeho vznik datujeme do období 80. let minulého století, kdy se ve větší míře začalo využívat ICTs pro spravování ohromného objemu dat, které státy, ale i soukromé firmy, banky a podobně začaly shromažďovat o svých občanech, zaměstnancích i zákaznících. Stanovení pravidel a východisek pro bezpečné nakládání s těmito cennými informacemi se stalo zásadní záležitostí.


Kybernetická bezpečnost se stala součástí výzkumu postmoderních nekonvenčních konfliktů, do jejichž charakteristiky řadíme také
kybernetické útoky, resp. kybernetické války. Rozvoj této disciplíny je patrné sledovat také v učebních programech některých vysokých škol v ČR (např. Fakulta sociálních studií Masarykovy univerzity a její obor Bezpečnostná a strategická studia, Policejní akademie, Matematicko-fyzikální fakulta Univerzity Karlovy a její Katedra softwarového inženýrství či České vysoké učení technické se svým Ústavem informatiky a telekomunikací ad.).

Při zpracování této diplomové práce vycházíme z česky i anglicky psaných titulů. Nezbytný zdroj relevantních informací představuje rovněž Internet, konkrétně webové stránky důležitých organizací a institucí zabývajících se (alespoň částečně) problematikou e-governmentu a kybernetické či informační bezpečnosti. Uvedeme zde hlavně příklady Organizace spojených národů (OSN), Organizace pro ekonomickou spolupráci a rozvoj (OECD), Severoatlantickou alianci (NATO) či EU. Pro sledování a rozbor konkrétních projevů a přístupů k e-governmentu v ČR byly relevantním zdrojem stránky Ministerstva vnitra ČR, dále stránky spojené s projekty CzechPOINT či datových schránek. Důležité informace čerpáme také ze serveru Informační systémy veřejné správy či ze stránek krajských i místních samospráv.


Autoři kolem V. Lídinského zpracovali téma e-governmentu do jakési příručky občana pro orientaci v základní problematice jeho nástrojů
a možností. Zohledňovány jsou opět právní normy a základní dokumenty s vysvětlením konkrétních praktických dopadů e-governmentu.

Problematikou e-governmentu v ČR a rozvojem elektronické komunikace se zabývá i Jiří Peterka. Čerpáme zde z jeho třech článků i2010 místo eEurope 2005, Ohlédnutí za zanikajícím Ministerstvem informatiky a Osm priorit státní informační politiky.

V oblasti informační bezpečnosti je českým expertem Josef Požár působící na Policejní akademii v Praze. V této práci pracujeme se dvěma jeho tituly. Nejprve se jedná o skriptum Základy teorie informační bezpečnosti kolektivu autorů kolem J. Požára a dále pak o knihu Informační bezpečnost, kterou již J. Požár vydal sám. Tento autor se ve svých pracích podrobně věnuje tématu informační bezpečnosti jak z pohledu teoretického, tak i technického. Jeho publikace se proto staly cenným zdrojem informací o typech a metodách hrozeb informační bezpečnosti, stejně jako o možnostech jejího zajištění a posílení.

K problematice informační bezpečnosti bychom ještě zmínili skriptum Romana Jaška Informační a datová bezpečnost. Jeho zájem je obrácen k problematice šifrování a přístupu firem k zabezpečení svých informačních systémů. Na podzim 2008 byl založen také odborný internetový magazín o bezpečnosti ICTs, ICT Security, který se věnuje aktuálním trendům i problémům souvisejících s využíváním současných ICTs.3


Otázkám kybernetických konfliktů se zevrubně věnují autoři Andy Jones, Gerald L. Kowacich a Perry G. Luzwick ve své knize *Global Information Warfare. How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages*. Sledují zde vývoj konceptu informační války a dále také přístup k němu v různých státech či regionech.

Jako jeden z nejčerstvějších příspěvků do diskuze o kybernetických výzvách současnosti představíme knihu editovanou Athinou Karatzogianni *Cyber-conflict and Global Politics*. Jednotliví autoři zde analyzují 14 konfliktů, jež využívají, resp. zněužívají možnosti kybernetického prostoru. Sledují také vliv post-moderních ICTs na současná bezpečnostní studia a tématu, na politiku, média i společnost obecně.

Z českých řad bychom rádi zmínili Martina Bastla, který působí na Fakultě sociálních studií Masarykovy univerzity a zabývá se strategickými studii, soudobými konflikty a souvisejícími bezpečnostními hrozbami. V této práci využíváme jeho článku *Budoucnost nekonvenčních forem boje*. V jeho pojetí je nekonvenční způsob boje přirozeným vývojem způsobu vedení válečného konfliktu. Ve svém textu Bastl pracuje se dvěma příklady, a to s kybernetickými konflikty coby poměrně novým typem konfliktů a dále s terorismem coby příkladem psychologicky vedené, nekonvenční války. Oblast kybernetického terorismu pak rovněž rozpracovává Michal Janoušek ve svém článku *Kybernetický terorismus: terorismus informační společnosti*. Kybernetický terorismus je zde vnímán jako extenze klasického terorismu do kybernetického prostoru využívající možnosti nabízené informační společnosti.

Přístupy EU k informační bezpečnosti, ale i k rozvoji e-governmentu analyzujeme zejména na základě oficiálních dokumentů Společenství i textů jednotlivých výzv v této oblasti. Zdůraznili bychom iniciativy eEurope a i2010 či Strategii pro bezpečnou informační společnost. Dialog, partnerství a posílení. K relevantním zdrojům informací patří také oficiální webové stránky Unie, především Evropské komise a jejího tematického portálu o evropské informační společnosti.©

---

4 Webová adresa - http://ec.europa.eu/information_society/
Texty dokumentů, sdělení a dalších je možné vyhledat v rámci Portálu EU5 a jeho sekce Eur-lex.

Podobně jako v případě sledování problematiky EU, také v oblasti rozvoje e-governmentu v ČR čerpáme z primárních zdrojů, tedy zákonních úprav a vyhlášek, ale také z textů různých strategií a iniciativ (např. Národní strategie informační bezpečnosti ČR, Státní informační a komunikační politika ad.). Je nutné zdůraznit zejména dva zákony, které přinesly dosud zřejmě nejpodstatnější změny a posuny v elektronizaci veřejné správy. Jedná se o Zákon č. 227/2000 Sb., o elektronickém podpisu a Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Texty zákonů i vyhlášek lze dohledat na webových stránkách nakladatelství ekonomické a právní literatury Sagit, dále také v relevantních odkazech na webových stránkách Ministerstva vnitra ČR či v rámci Portálu veřejné správy ČR. Významným zdrojem informací byla také programová prohlášení jednotlivých vlád od r. 2002,6 která jsou dostupná na webových stránkách Vlády ČR.


Tato práce je členěna tematicky do dvou základních částí. První z nich je věnovaná problematice e-governmentu, kdy se nejednáme zejména na vymezení tohoto pojmu. Z tohoto důvodu zde bude použito zejména metody analýzy a syntézy, neboť budeme vycházet z různých konceptů a uchopení tohoto fenoménu.

5 Webová adresa: http://europa.eu
6 Vlády předchozí, tedy Klausovy, Tošovského a Zemanova, se elektronizaci veřejné správy ve svých programových prohlášeních přišli nevěnovaly.

Pátá kapitola části o e-governmentu v ČR předkládá jeho nejzásadnější praktické projevy. Představíme si koncept elektronického podpisu a institut elektronického podání a doručování. Následovat bude prezentace projektů CzechPOINT a datových schránek. Sledovat budeme jejich základní charakteristiky a zhodnotíme jejich přínos pro rozvoj e-governmentu, stejně jako jejich úspěšnost, resp. neúspěšnost v tomto procesu.

E-government coby elektronická veřejná správa využívající možností ICTs je právě na základě spoléhání na tyto prostředky a technologie zranitelná a ohrozitelná. E-government lze také vnímat jako pozitivní využití ICTs. Existuje pak také možnost jejich zneužití proti státu i společnosti. Druhá část této diplomové práce je proto věnována rizikům souvisejícím s aplikací nástrojů e-governmentu, konkrétně pak informační a kybernetické bezpečnosti.

Nejprve přiblížíme problematiku, aspekty a metody zabezpečení informačních systémů. Druhá kapitola této části se bliží zaměří na problematiku informační bezpečnosti, jejího zajištění i jejich základních hrozeb. Pro tyto oddíly jsme zvolili metody analýzy a syntézy, kdy vycházíme z právních základů, dalších teoretických rámců, přístupů a návodů i dokumentů předkládajících strategii informační bezpečnosti (např. Národní strategie informační bezpečnosti ČR).

Ve třetí kapitole druhé části sledujeme hlavní metody a podoby zneužití ICTs proti státu. Věnovat se budeme motivacím ke kybernetickým útokům. Přiblížíme tři nejčastější příklady kybernetických útoků proti státu - kybernetickou špionáž, kybernetický terorismus a tzv.
hacktivismus. Nejprve budeme vycházet z metody analýzy a syntézy, jelikož nám půjde o představení základních přístupů k těmto rizikům a útokům. Při rozboru konkrétních příkladů kybernetických útoků bude využito empiricko-analytického přístupu.

Poslední kapitola prezentuje přístupy EU k informační a kybernetické bezpečnosti. Zaměříme se na iniciativy eEurope a i2010 a možnosti jejich dalšího rozvoje resp. revize. Za užití analyticko-empirického přístupu zde prezentujeme konkrétní unijní dokumenty, iniciativy a postupy, které byly přijaty a aplikovány v oblasti informační a kybernetické bezpečnosti.

Hypotézou této diplomové práce je vnímání EU coby stěžejní entity stojící za zrychleným vývojem zavádění nástrojů e-governmentu v ČR v první dekádě 21. století, a to z důvodů finanční i morální podpory rozvoje elektronizace státní správy ve Společenství. Druhou výzkumnou tezi této studie je pojetí a pochopení kybernetické bezpečnosti a kybernetických hrozeb coby relevantních stratégických a bezpečnostních výzev současnosti, které je třeba zahrnout do bezpečnostních strategií států i mezinárodních organizací jako je EU či NATO.

Oblast e-governmentu představuje velice širokou oblast pro výzkum i praktické rozvíjení přístupů. Proto je cílem této práce předložit základní milníky vývoje e-governmentu v ČR, který ještě není ukončen. Nebylo tedy možné dostatečně zmapovat a zanalyzovat zejména poslední dosud navržené fáze elektronizace státní správy, plné spuštění projektu datových schránek či zřízení centrálních registrů veřejné správy, a to jednoduše z důvodu poměrně krátkého časového odstupu nebo vzhledem k tomu, že se nacházíme v období před začátkem daného projektu. Nicméně i přesto se zde o zhodnocení pokusíme a svá východiska a závěry v textu uvádíme. Je však třeba poukázat na to, že zde stále zůstává prostor pro další analýzy a bádání (např. problematica eHealth, eJustice, otázky ICTs a životního prostředí ad.). Podobně tak v případě EU můžeme očekávat rozvoj přístupů k informační a kybernetické bezpečnosti a případné, avšak z našeho pohledu nezbytné, přijetí jednotné politické a strategické koncepce věnující se kybernetické bezpečnosti, jak ji navrhuje komisařka Viviane Reding.
Téma kybernetické bezpečnosti představuje v zásadě rodící se a postupně se rozšiřující výzkumnou oblast. V této prácí si dáváme za cíl předložit a analyzovat základní východiska tohoto konceptu. Níže představený výklad by se mohl jevit v některých ohledech jako poněkud zkratkovitý. Nicméně záměrem je v tomto textu poukázat na existenci problematiky a reálné hrozby kybernetických útoků proti státu a s tím pak sledovat teoretické základy kybernetické bezpečnosti i soudobé praktické jevy a kroky učiněné v této oblasti. Můžeme předpokládat, že téma kybernetické bezpečnosti bude předmětem dalších studií a výzkumů.
1. E-GOVERNMENT

V současnosti můžeme sledovat poměrně významné kroky v rozvoji elektronizace státní správy nebo e-governmentu v ČR. V hojně míře je využíváno kontaktního místa CzechPOINT, kde občané získávají výpisy z různých rejstříků a databází veřejné správy. Letošní r. 2009 uvedl projekt datových schránek, jenž by měl znamenat určitou revoluci ve způsobu komunikace občanů s orgány veřejné moci. V roce následujícím je naplánované zřízení tzv. centrálních registrů veřejné správy, v nichž mají být efektivněji spravována data, která státní správa shromažďuje pro své náležité fungování. Nicméně úsilí o rozvoj nástrojů e-governmentu, s většími či menšími úspěchy i klopýtnutími, je možné v ČR sledovat již od počátku 90. let minulého století.

V první kapitole této práce se nejprve zaměříme na vymezení pojmu e-government. Zodpovíme otázku, co si konkrétně pod tímto pojmem představí. Prezentujeme základní vnitřní a přístupy k této problematice v rámci vědecko-výzkumné obce, ale také některých významných mezinárodních organizací a samozřejmě také české vlády, konkrétně Ministerstva vnitra, které je za realizaci e-governmentu u nás zodpovědné.

Následně přibližíme vývoj zavádění nástrojů e-governmentu i politických přístupů a postojů k němu v ČR. Sledovány budou také posuny v rámci právních norem a právního ukotvení e-governmentu, jež je stěžejní pro proces jeho úspěšné realizace. V této souvislosti navážeme uvedením základních praktických projevů českého e-governmentu, tedy elektronického podpisu, elektronického podání a doručení, projektu CzechPOINT a konečně datových schránek.

1. 1. Vymezení pojmů

Pro výraz e-government se v současnosti často nehledá odpovídající překlad do jiných jazyků. Stal se pojmem, který se v moderních společnostech používá v původním anglickém tvaru a vymezuje se spíše v rovině obsahové. V zásadě je vnímán jako soubor úkolů, „které se
zabývají elektronizací výkonu činnosti veřejné správy nebo v širším pojetí spíše orgánů veřejné moci vůbec.7

E-government představuje neologismus vzniklý ze zkrácení anglického výrazu „electronic government“ čili elektronická správa či vláda,8 jak lze také tento výraz přeložit do češtiny.9 E-government můžeme tedy definovat „jako využití informačních a komunikačních technologií (např. dálkové počítačové síť, internet, mobilní technologie apod.) veřejnou správou k poskytování informací a veřejných služeb nejširší veřejnosti.“11 Z podobného základu vychází také definice Evropské komise, která e-government vníma jako „užití informačních a komunikačních technologií ve veřejné správě, kdy jsou spojeny organizační změny a nové možnosti za účelem zlepšit veřejné služby a demokratické procesy.“12 Aspekt zlepšení veřejné služby občanům pak vede také k chápání výrazu e-government jako spojení dvou slov, a to „efektivní vládnutí či správa“.13

Přístupy k vysvětlení pojmu e-government a jeho vnímání obecně se liší. Představíme ovšem pouze některé z nich, jež považujeme za nejvýstížnější k pochopení tohoto výrazu i jeho fungování. Centrum pro technologie ve správě předkládá poměrně jednoduchou definici e-governmentu: E-government je užití informačních technologií k podpoře vládních kroků, k zapojení občanů a k poskytování vládních služeb.15 Důraz je kladen na čtyři základní dimenze, které odpovídají funkcím veřejné správy - e-services (elektronicky dostupné informace, programy a služby veřejné správy, často skrze internet), e-democracy (užití elektronických médií ke zvýšení účastní občanů na rozhodovacích

---

9 V tomto textu však budeme používat výraz e-government. Při citaci budeme uvádět výraz, jak je uveden v originále.
10 Information and communication technologies (ICTs).
11 TUŠEROVÁ, L.: c.d.
14 Centre for Technology in Government při New York State University.
procesech), *e-commerce* (elektronická výměna peněz za zboží a služby, elektronická platba daní či složenek apod.) a *e-management* (užití informačních technologií ke zlepšení fungování veřejné správy). Právě e-management je stěžejní pro dobré fungování e-governmentu, neboť se zaobírá jeho správným využíváním a spravováním.\textsuperscript{16}

Výkonem a implementací e-governmentu se zabývá také intenzivně EU. Ta jej také definuje jako zavádění ICTs k zajištění lepších služeb veřejné správy občanům i firmám. Komunikace s orgány veřejné správy má být snadnější a levnější. S pohledu EU efektivní e-government představuje zdokonalení správy obecně a umožnění většího zapojení občanů do politického procesu.\textsuperscript{17}

OECD se pak ve své definici e-governmentu zaměřuje na způsoby veřejné správy a opět její možné další zlepšení. E-government může rovněž zvyšovat důvěru občanů ve veřejnou správu. Občan má totiž možnost přímo a aktivněji se zapojit do politického procesu, a to snadnějším přístupem k informacím i státním službám či kontrolou práce svých zastupitelů. Je tak vytvářena otevřená a zodpovědnější správa, což napomáhá omezit korupci.\textsuperscript{18}

OECD také předkládá čtyři základní principy výkonu e-governmentu – vize a politická vůle, společná struktura a kooperace, zaměření na zákazníka (občana) a zodpovědnost. \textit{Vize a politická vůle} souvisí s vůdcovstvím a závazkem, které jsou podmínkou změny k lepší správě, a integraci e-governmentu do širší politické reality a praxe vedoucí k tomuto zlepšení. \textit{Společná struktura a spolupráce} znamená propojení práce různých státních úřadů, aby nedocházelo zejména k duplicitě, a zajištění dostatečného financování jejich fungování souvisejících projektů. \textit{Zaměření na uživatele–občana} představuje princip dostupnosti, možnosti výběru způsobu komunikace s úřady, aktivního zapojení občana a konečně důvěrnosti, tedy zajištění ochrany osobních údajů uživatelů. \textit{Zodpovědnost}

souvisí s transparentností a jasným stanovením kompetencí úřadů i jednotlivců, stejně jako sledování a vyhodnocení služeb.19

Na definici e-governmentu předloženou OECD navazuje vysvětlení pojmů ze strany Institutu pro rozvojovou politiku a management Manchesterské univerzity.20 Podle jeho definice e-government opět znamená zavedení ICTs prostředků ke zlepšení veřejné správy. Zahrnuje tři oblasti: zlepšení vládních procesů (eAdministration), napojení a spojení občanů (eCitizens a eServices) a budování vnějších kontaktů a interakcí (eSociety).21

Občan je v rámci těchto pojetí e-governmentu ve vztahu k veřejné správě vnímán jako zákazník. Vlády se snaží zlepšit vztah a kontakt mezi svými občany a orgány státní moci. E-government je také chápán jako forma veřejné správy orientovaná na zákazníka neboli občanu. Vláda, která aktivně využívá nástrojů e-governmentu, pak bývá označována jako „costumer-centric“. Jejím hlavním cílem je využívání daňových prostředků ke zvyšování spokojenosti zákazníků-občanů.22

Světová banka (WB) uvádí definici e-governmentu coby využití prostředků ICTs vládními úřady. Výsledkem je opět změna vztahu mezi občany a podnikatelskou sférou a státem. Ta může vést k „lepší dostupnosti vládních služeb občanům, ke zlepšení kontaktů a vztahů s podnikatelským sektorem a průmyslem, k posílení pozice občanů prostřednictvím přístupu k informacím a také k efektivnější správě. Výslednými výhodami pak může být nižší míra korupce, větší transparentnost a spokojenost, růst příjmů a snížení nákladů.“23

---

20 Institute for Development Policy and Management, University of Manchester.
Dosáhnout na požadované služby státu a jeho úřadů stejně jako komunikace s nimi má být pro občana jednodušší.\textsuperscript{24}

WB uvádí v popisu vztahu mezi občanem a veřejnou správou analogii e-governmentu a e-commerce (elektronického obchodu), kdy se obchodník snaží navázat bližší vztah se zákazníkem (B2C, business to customer) či kdy dochází ke zlepšování vztahů mezi jednotlivými firmami a podniky (B2B, business to business). V oblasti e-governmentu se státní správa snaží navázat bližší a lepší kontakty s občany (G2C, government to citizen), s obchodními společnostmi (G2B, government to business) a také mezi svými orgány navzájem (G2G, government to government).\textsuperscript{25}

L. Lowery ve své studii ještě přidává vztahy mezi státní správou a veřejností (G2P, government to public) a vládním aparátem a jeho zaměstnanci (G2E, government to employees). Důležitými pojmy jsou u Lowery veřejná dostupnost a poskytnutí (public provision), digitální demokracie (digital democracy) a hospodářský rozvoj (economical development).

**Veřejná dostupnost** znamená nepřetržitý přístup ke všem službám a informacím veřejné správy. **Digitální demokracie** souvisí s definicí e-governmentu coby procesu užití prostředků elektronické komunikace k dosažení kontaktu s voličem i občany, stejně jako využití elektronických médií k volbám či v rámci volební kampaně. To by mohlo zvýšit politickou účast, zájem i znalost občanů. **Rozvoj ekonomiky**, který je stěžejní pro úspěšnou vládu, vychází z předpokladu, že tento je do značné míry závislý na využití moderních komunikačních technologií a dostupnosti informací.\textsuperscript{26}

V. Lidínský a kol. ve své knize vychází z definice OSN, kdy e-government představuje „(T)rvalou povinnost veřejné správy zlepšovat vztah mezi občany a veřejným sektorem poskytováním levných a

\textsuperscript{24} Např. Czech POINT (viz níže kapitola 1.5.3. CzechPOINT) či osobní počítač.

\textsuperscript{25} \textit{Definition of E-Government}.

efektivních služeb, informací a znalostí.\textsuperscript{27} Dále je v jejich publikaci představena definice Ministerstva vnitra resp. bývalého Ministerstva informatiky, kdy „eGovernment představuje transformaci vnitřních a vnitřních vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy.\textsuperscript{28} A konečně autoři kolem Lidinského uvádějí také svoji vlastní definici: „eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb.\textsuperscript{29}"

Na závěr uvedeme pojetí e-governmentu ze strany české vlády a Ministerstva vnitra ČR. Tento přístup je pak stěžejní pro postupy a projekty zavádění jeho nástrojů u nás. E-government je symbolizován postavou eGona, který de facto představuje e-government.\textsuperscript{30} Základními součástmi e-governmentu, resp. základními životními funkcemi eGona jsou mozek (základní registry veřejné správy), srdce (eGovernment Act, čili zákon o e-governmentu\textsuperscript{31}), oběhový systém (komunikační infrastruktura veřejné správy, KIVS) a prsty (CzechPOINT coby univerzální kontaktní místo). Fungování e-governmentu je pak vysvětleno analogicky jako fungování živého organismu. Skrze prsty je přijat podnět. Skrze oběhový systém je vyslán signál do mozku, který informaci vyhodnotí a správný orgán rozhodne. Prstům je pak vyslána informace o tom, co mají dělat.\textsuperscript{32}

Pro potřeby této práce jsme výše uvedená pojetí a vysvětlení propojili a e-government vnímáme jako způsob veřejné správy, kdy státní moc i jiné veřejné instituce využívají prostředků moderní elektronické komunikace (zejména Internetu) za účelem zlepšení a zefektivnění

\textsuperscript{29} LIDÍNSKÝ, V. a kol.: c. d., s. 7.
\textsuperscript{30} Projekt eGon tedy projekt elektronizace veřejné správy byl zahájen v r. 2006.
\textsuperscript{31} Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. (Viz níže kapitoly 1.2. Rozvoj e-governmentu v ČR, 1.4. Právní ukotvení e-governmentu v ČR a 1.5.4. Datové schránky.)
fungování státní správy. Stěžejná je zkvalitnění vztahů s občany i firmami a usnadnění jejich přístupu k orgánům veřejné administrativy a získání informací o veřejné správě (zejména téměř nepřetržitým online přístupem k internetovým stránkám či aplikacím). Efektivita státní správy má být dosažena mimo jiné také odstraňováním duplicit skrze žádoucí fungování jejích centrálních registrů, což přispívá k omezení množství informací shromažďovaných o občanech často vícekrát v různých, navzájem nepropojených databázích. Cílem je zlepšení komunikace také mezi orgány a úřady státní správy.

1. 2. Rozvoj e-governmentu v České republice


---

34 Tamtéž, s. 25.
35 Blíže k projektu viz Tamtéž, s. 13-14.
Výstavba státního informačního systému ČR, který navrhoval zahrnutí registrů nemovitostí i obyvatel včetně registří sociálních dávek, zdravotního pojištění i ekonomických subjektů do jednoho informačního systému. Nicméně zejména kvůli postupným přesunům kompetencí mezi rezorty a jinými orgány státní správy došlo k podstatnému zpomalení této iniciativy. O rok později byl založen Úřad pro státní informační systém, který však zůstal v zásadě bez kompetencí, neboť v praxi si každý resort vytvářel vlastní informační systémy.37

Významným posunem byl strategický dokument Státní informační politika – cesta k informační společnosti schválený vládou v r. 1999.38 Dokument měl představovat národní koncepci budování tzv. informační společnosti.39 Podstatou státní informační politiky se stalo „vytvoření veřejně přístupné služby přes příslušné komunikační rozhraní za účelem rozvoje oboustranné komunikace mezi veřejnou správou a občany."40 Ve stejném roce byla přijata Koncepce budování informačních systémů.41

Základní zásadou budování informačních systémů v ČR se stal princip minimalizace. Jeho podstatou „byla snaha po minimalizaci informací, které jsou požadovány veřejnou správou po adresátech, zejména vyloučit situaci, kdy jsou data vyžadována vícekrát, a to i chybně... informaci, kterou již stát, resp. jeho orgán jednou má, nebude vyžadovat znovu. Princip minimalizace se měl prosadit, i pokud jde o počet registrů, případně jejich obsah."42 Tento princip je v koncepci elektronizace veřejné správy přítomen stále (např. v konceptu centrálních

---

40 MATES, P. – SMEJKAL, V.: c.d., s. 15.
43 Tamtéž, s. 27.
registrů, kdy se vedená data nemají duplikovat a každý registr je jejich jediným garantovaným zdrojem.

V r. 2000 byl Úřad pro státní informační systém nahrazen Úřadem pro veřejné informační systémy, který se měl věnovat rozvoji a vytváření informačních systémů veřejné správy. Došlo k posunu od ideje vytvoření jednotného státního informačního systému k reálnější soustavě informačních systémů veřejné správy (ISVS). Ty jsou „souborem informačních systémů, které slouží pro výkon veřejné správy.“

Úřad pro ISVS byl však také zrušen a v r. 2002 přešly jeho pravomoci i působnost na Ministerstvo informatiky. Jedním z nejvýznamnějších počinů ministerstva v této oblasti se stalo spuštění Portálu veřejné správy v říjnu 2003, který „představuje informační systém, poskytující systematické informace o jednotlivých subjektech, jejich činností a výsledcích těchto činností.“ Mimo celostátní informační systémy byly budovány také sítě na regionální či místní úrovni.

I přes některé vládní iniciativy v oblasti rozvoje e-governmentu její úsilí nepředstavovalo v této době přílišný úspěch a posun. Zájezdně nedostatek a komplikaci v rozvoji e-governmentu lze v této době považovat nedobudování základních registrů veřejné správy a

43 Viz níže kapitola 1.4. Vývoj právního ukotvení e-governmentu a vládních postojů k němu.
44 Na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. (MATES, P. – SMEJKAL, V.: c.d., s. 16)
45 Tamtěž, s. 27-28.
48 Internetová adresa portálu: http://portal.gov.cz
49 MATES, P. – SMEJKAL, V.: c.d., s. 16.
způsobů jejich spravování, které by také umožňovaly jejich sdílení.\textsuperscript{52} Toto se postupně daří naplňovat až spolu s aplikací a užíváním kontaktního místa CzechPOINT a plánovaným projektem vytvoření centrálních registrů, tedy mozku Egona.

V rámci rozvoje informačních systémů nicméně r. 2000 vznikl elektronický portál místních samospráv ePUSA.\textsuperscript{53} Informační systém ePusa\textsuperscript{54} je společný pro Ministerstvo vnitra ČR, kraje a ostatní samosprávy. Jeho základním cílem je „být jediným garantovaným zdrojem informací o subjektech samosprávy, a zamezit tak jejich duplicitnímu zjišťování orgány veřejné správy."\textsuperscript{55} ePusa má poskytovat informace jak zaměstnancům krajských úřadů, tak také veřejnosti. Kraje i ostatní orgány veřejné správy jsou odpovědné za správnost údajů o nich v ePuse vedených.\textsuperscript{56}

Na úroveň obcí, které by aktivním přístupem k obohacování obsahu portálu ePusa měly také zvýšit zájem svých občanů o zavádění a využívání Internetu a elektronické komunikace s úřady, je směřován také projekt EVA neboli Elektronicky všední administrativy či Elektronická a Vaše Asistentka.\textsuperscript{57} Jeho působnost je v kompetenci Ministerstva vnitra ČR. Cílem projektu je „umožnit zveřejňování kontaktních údajů o jednotlivých obcích pro potřeby podnikatelské, informování veřejnosti, ale také řešení krizových situací."\textsuperscript{58}

Dalšímu rozvoji využívání elektronických komunikačních prostředků a e-governmentu na místní úrovni však často brání nedostatek finančních prostředků.\textsuperscript{59} Důležité je také poskytnutí potřebného školení úředníků kompetentních k výkonu a užití nástrojů a úkolů spojených s e-governmentem.

\textsuperscript{52} MATES, P. – SMEJKAL, V.: c.d., s. 16-17.
\textsuperscript{53} Partnerem tohoto projektu je také portál Města a obce online, který funguje od r. 1996. Internetová adresa projektu – http://www.moof.cz.
\textsuperscript{54} Webová adresa portálu: http://www.epusa.cz
\textsuperscript{56} Na jejich základě jsou také krajím zasílány přístupové informace pro zřízení datových schránek (viz níže).
\textsuperscript{57} Internetová adresa projektu: http://www.naseeva.cz/
\textsuperscript{58} MATES, P. – SMEJKAL, V.: c.d., s. 17.
\textsuperscript{59} Tamtéž, s. 21.
Vláda Vladimíra Špidly ve svém programovém prohlášení z roku 2002 věnovala problematice budování informačního systému veřejné správy poměrně velkou pozornost. Vláda se zde přihlásila k myšlence podpory a rozvoje informační společnosti jako důležitého nástroje pro rozvoj vzdělanosti, ekonomiky a služeb veřejné správy. Patrný je tady odkaz na iniciativy eEurope a také Státní informační politiku. Elektronizace veřejné správy zde byla chápána jako nástroj úspory financí a také podpora zvýšení komfortu vztahu mezi státem a občanem. Tento úkol měl podle představy vlády průřezový, nadregionální charakter.

V roce 2002 tak bylo pro naplňování tohoto úkolu vytvořeno Ministerstvo informatiky coby ústřední orgán správy pro informační a komunikační technologie, pro telekomunikace a poštovní služby. Budování informační společnosti v ČR mělo vycházet z principů Státní informační politiky a dokumentů EU, zejména tzv. eEurope. Následné vlády Stanislava Grosse i Jiřího Paroubka ve svých programových prohlášeních sledovaly trend efektivizace veřejné správy skrze aplikace a rozšiřování využitelnosti jednotného informačního systému veřejné správy.

V dalších letech byly schvalovány další strategické dokumenty pro rozvoj e-governmentu v ČR, například Státní informační a komunikační politika – e-Česko 2006 s výhledem do r. 2006. Tato iniciativa navazuje

---

61 Tamtéž.
62 Viz níže kapitola 1.3. Působení EU na rozvoj e-governmentu v ČR.
63 Programového prohlášení vlády (2002).
65 Viz výše.
na Státní informační politiku z r. 1999 a je zaměřena na rozvoj tzv. informační společnosti v ČR, stejně jako náležité rozšíření tzv. vysokorychlostního Internetu.69

Kroky k rozvoji informačních systémů u nás rovněž vycházely z iniciativ EU (eEurope a i2010) a byly postaveny na čtyřech základních prioritách - zajištění bezpečné a dostupné komunikační služby, informační vzdělanost, moderní veřejné služby on-line a dynamické prostředí pro elektronické podnikání. Česká vláda se zaměřila na budování elektronických služeb veřejné správy, pokračování liberalizace sektoru elektronických komunikací, dále na rozvoj vysokorychlostního Internetu. Potřeba bylo také vytvořit odpovídající právní strukturu pro informační společnost. Dále byla podporována informační gramotnost a elektronické podnikání.70

Kolem r. 2005 však došlo opět ke zpomalení vývoje e-governmentu na celostátní úrovni. Ministerstvo informatiky se zaměřilo na elektronickou komunikaci a digitální vysílání. Budování informačního systému bylo upozaděno. V říjnu 2005 však přesto byla vládním usnesením č. 1340 přijata Národní strategie informační bezpečnosti ČR.71

Ministerstvo informatiky bylo zrušeno k 1. červnu 2007. Jeho kompetence v rámci informační politiky převzala tři ministerstva, Ministerstvo obchodu a průmyslu (problematika související s hospodářským rozvojem země a elektronického obchodování a podnikání).72 Ministerstvo pro místní rozvoj (problematika spojená

---

69 Státní informační a komunikační politika byla vládou schválena v březnu 2004 a usilovala o reakci na vývoj v oblasti informační společnosti tak také telekomunikace, kdy tyto dva pojmy se vzájemně prolínají. Je zde také reflektován vstup ČR do EU, a tedy také dokumenty Společenství týkající se informační společnosti (zejména eEurope 2005: Informační společnost pro všechny) stejně jako konkurenceschopnost ČR v této oblasti. Stěžejními jsou v dokumentu eCesko 2006 tyto body: 1) budování moderních a bezpečných služeb veřejné správy dostupných on-line; 2) pokračování liberalizace sektoru elektronických komunikací s cílem zajistit efektivní konkurenční prostředí; 3) podpora rozšíření vysokorychlostního přístupu k internetu a zajištění jeho dostupnosti pro všechny skupiny obyvatelstva; 4) pokračování legislativního zakotvení informační společnosti; 5) podpora zvyšování počítačové gramotnosti obyvatel; 6) podpora rozvoje elektronického podnikání vytvářením vhodných technologicky neutrálních podmínek. (Státní informační a komunikační politika. e-Cesko 2006.)

70 MATES, P. – SMEJKAL, V.: c.d., s. 29.

71 Problematika informační bezpečnosti viz níže kapitola 2.2. Informační bezpečnost.

72 Zvyšování konkurenceschopnosti (zavádění inovací technologií, výrobků a služeb; podpora vědy a výzkumu a jejich vazeb na průmysl a podnikání; snižování surovinové a energetické náročnosti průmyslové výroby; podpora informačních technologií), podpora podnikání a podpora
s informační metodickou pomocí vyšším územním samosprávným celkům, městům, obcím a jejich sdružením) a konečně Ministerstvo vnitra, které převzalo kompetence v oblasti e-governmentu.

Ministerstvo informatiky bylo zrušeno v souladu s programovým prohlášením Topolánkovy vlády. Jeho činnost měla v oblasti rozvoje e-governmentu převzít mimo jiné také Rada pro rozvoj informační společnosti. Jako důvody zrušení ministerstva se uvádí zejména jeho nedostatečná „síla“, kdy jeho kompetence byly tak specifické, že svou velikostí odpovídalo spíše odboru určitého ministerstva. Na druhou stranu projekt rozvoje e-governmentu, který se pro jeho činnost jevil jako stěžejní, potřeboval kooperaci a zapojení napříč ministerstvy.

Rada pro rozvoj informační společnosti je odborným poradním orgánem vlády, která je zřízena svým usnesením č. 293 z 28. března 2007. Má plnit koordinační roli místo zrušeného Ministerstva informatiky a poskytovat vládě vědomostní základnu pro její rozhodování v koncepčních otázkách rozvoje informační společnosti. Jejím účelem je dosažení co největší meziresortní koordinace v této oblasti. Radu vlády pro rozvoj informační společnosti, která má 28 členů, vede řídící výbor, v jehož čele stojí premiér a jehož dalšími členy jsou ministři vnitra, financí a průmyslu a obchodu. Další členové jsou jmenováni na základě svých expertních a odborných znalostí. V Radě jsou zastoupeni také nejdůležitější instituce, kterých se rozvoj informační společnosti a budování e-governmentu týká, tedy zástupci státní správy a samosprávy,

---

75 Členy byli nebo jsou např. Jan Fischer (premiér úřednické vlády květen 2009-jaro 2010 a předseda Českého statistického úřadu), Michal Mejstřík (ředitel Institute of Economic Studies, Univerzita Karlova), Jaroslav Mil (předseda Svazu obchodu a průmyslu ČR), Eduard Kožušník (vedoucí projektu e-Stat) či Evžen Tošenovský (bývalý předseda Asociace krajů a hejtman Moravskoslezského kraje).
Parlamentu ČR, odborných a podnikatelských asociací i akademické sféry.\textsuperscript{76}

V rámci Konference ISSS\textsuperscript{77} v dubnu 2008 schválila Rada pro rozvoj informační společnosti Strategii rozvoje služeb pro informační společnost. Vizí tohoto dokumentu je zařadit ČR mezi pět nejlepších zemí EU v úrovni rozvoje e-governmentu.\textsuperscript{78} Jeho hlavním cílem pak je „změnit českou veřejnou správu takovým způsobem, aby byla občanovi plnohodnotným partnerem v moderní demokratické společnosti, využívající informační a komunikační technologie pro svůj rozvoj a posílení konkurenceschopnosti.“\textsuperscript{79}

Implementace Strategie má vycházet z realizace několika vzájemně provázaných projektů rozdělených do pěti oblastí: základní registry státní správy, univerzální kontaktní místo, zaručená a bezpečná elektronická komunikace mezi úřady navzájem a úřady a občanem, dále digitalizace datových fondů a konečně služby pro informační společnost (zdravotnictví, sociální služby, veřejná správa jako soudnický apod., správa státního rozpočtu ad.).\textsuperscript{80}

Strategie také stanovuje milníky v rozvoji informační společnosti v časovém horizontu. V roce 2009 mají být spuštěny datové schránky spolu s existencí sítě univerzálních kontaktních míst veřejné správy.\textsuperscript{81} V roce 2010 mají být zprovozněny základní registra v rámci existujících kontaktních míst. Ve stejném roce má být také dokončen legislativní proces spojený s realizací cílů Strategie. V roce 2012 mají být funkční aplikace pro oblasti zdravotnictví, sociální péče, správního, soudního a


\textsuperscript{78} Internet ve státní správě a samosprávě.


\textsuperscript{80} Tamtéž; srov. Strategie rozvoje služeb pro informační společnost., s. 5.

\textsuperscript{81} V tomto bodě je možné zaznamenat úspěch strategie. Projekt datových schránek by byl spuštěn k 1. červenci 2009. Kontaktní místa CzechPOINT fungují a dále se úspěšně rozvíjejí.
daňového řízení a má být funkční infrastruktura pro dlouhodobé ukládání a archivaci elektronických dokumentů. V roce 2015 se plánuje dokončení procesu elektronizace datové základny, včetně elektronizace geografických informací.  

Programové prohlášení vlády Mirka Topolánka z ledna 2007 se také vyslovuje pro rozvoj sítě kontaktních míst CzechPOINT. A zavazuje se k předložení zákona o elektronické komunikaci (eGovernment Act). Programové prohlášení vlády také pojednává o zvýšení výkonnosti českého soudnictví skrze elektronizaci, tedy zavádění projektu tzv. eJustice. Konkrétně se zde hovoří o elektronickém platebním rozkazu pro zjednodušení platby jednoduchých a typizovaných peněžitých částek. Navrhované bylo také zavedení plně elektronizovaného insolvenčního rejstříku a tzv. elektronického spisu, který by měl zlepšit a zjednodušit komunikaci mezi jednotlivými justičními orgány. Má být také umožněna plně elektronická komunikace mezi účastníky soudního řízení.


Nicméně úspěchy v oblasti rozvoje e-governmentu Topolánkova vláda nebyla schopna dostatečně prezentovat a jejich vliv byl upozděn jinými politickými tématy. Následná úřednická Fischerova vláda se ve svém programovém prohlášení z června 2009 zavázala pokračovat v projektech rozvoje e-governmentu, jak je specifikovala vláda předchozí.

---

82 Strategie rozvoje služeb pro informační společnost., s. 4.
83 Viz níže kapitola 1.5.2. Elektronické doručování a podání.
85 Zavedení CzechPOINTu, datové schránky a schválení zákona o centrálních registrech státní správy.
Důraz je kladen zejména na úspěšné zavádění datových schránek a podporu projektu CzechPOINT. Fischerova vláda usiluje o zajištění financování současného rozvoje e-governementu přednostně ze zdrojů poskytnutých EU.88

Je však třeba také uvést, že zejména samosprávy resp. krajské úřady se při aplikaci principů e-governementu potýkaly a často potýkají s nejasným centrálním konceptem. Vládní iniciativy jako Státní informační politika – cesta k informační společnosti či Státní informační a komunikační politika měly spíše deklaratorní charakter. Byly koncipovány jako strategické plány. Chyběly však závažné právní normy, které by sjednocovaly postup zavádění nástrojů e-governementu v ČR. Krajské úřady si tak vytvářely metodiku užití e-governementu samy.89


---


89 Aktivní v tomto ohledu byl např. Plzeňský kraj, který vytvářel metodiku a analýzy, jež přejímaly i další kraje.


92 Koncepce informatizace Plzeňského kraje., s. 7.
o e-governmentu (eGovernment Act), se stalo stěžejní pro efektivnější zavádění prostředků e-governmentu na krajské úrovni. Také financování elektronizace veřejné správy je silně ovlivněno stále se vyvíjející legislativou i pravidly pro zavádění e-governmentu. Je totiž obtížné v prostředí významné finanční podpory elektronizace veřejné správy z evropských strukturálních i komunitárních fondů vytvořit patřičné projektové žádosti a reagovat na patřičné projektové výzvy.

Krajské úřady lze však považovat za určité příkopy v rozvoji využívání nástrojů e-governmentu. Staly se také jakýmsi lídry v tomto procesu. Všechny krajské úřady disponují možností elektronického podání, komunikace i prezentace na Internetu. Souvisí to s obdobím, kdy byla upravena struktura územní samosprávy a kraje byly r. 2000 zřízeny coby vyšší územně správní celky. Od počátku fungování krajských úřadů existovala jakási centrální vize na české i evropské úrovni o elektronizaci veřejné správy, byť konkrétní kroky k jejímu provedení v ČR nebyly ještě známé. Existovaly také potřebné technologické podmínky pro rozvoj elektronického spravování dat. Údaje krajských úřadů pak mohly být elektronicky vedeny od počátku, čímž se vyhnuly poměrně náročné konverzi dokumentů z fyzické do elektronické podoby.

Se zaváděním elektronických systémů souvisí také patřičný rozvoj elektronické komunikační technologie a schopnosti úředníků státní správy i občanů je využívat a používat. Existuje zde též riziko vytváření informačních propastí mezi občany způsobené rozdílnými možnostmi přístupu k těmto komunikačním prostředkům. Proto je věnován poměrně velký prostor iniciativám orientujícím se na zpřístupnění tzv. veřejného Internetu, často zdarma. S rozvojem elektronické komunikační technologie a podpory schopnosti úředníků i občanů užívat nástroje e-governmentu souvisí již výše zmíněna Státní informační a komunikační politika e-Česko 2006. S jejím cílem rozšíření vysokorychlostního

93 Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů viz níže kapitola 1.4. Vývoj právního ukotvení e-governmentu a vládních postojů k němu.
94 EU již měla podíl na vytváření této vize skrze své projekty eEurope, v případě ČR v této době eEurope+. (Viz níže kapitola 1.3. Působení EU na rozvoj e-governmentu v ČR.)
95 K rozvoji využívání a podpory hlubší implementace elektronických komunikačních prostředků (zejména internetu) viz MATES, P. – SMEJKAL, V.: c.d., s. 18-19.
96 Viz výše např. Národní plán počítačové gramotnosti.
Internetu souvisí také program rozvoje online služeb i jejich dostupnosti pro co nejširší okruh osob Národní politika pro vysokorychlostní internet – broadband strategie.\(^{97}\) Nelze také opominout vliv EU a jejich strategických dokumentů souvisejících s podporou informační společnosti.

1. Působení EU na rozvoj e-governmentu v ČR


Iniciativám eEurope se budeme věnovat také v závěru této práce v kapitole 2.4. EU a její pojetí informační a kybernetické bezpečnosti.
nové kandidátské státy byla vypracována ještě třetí strategie, eEurope+, zaměřená na co největší rozšíření alespoň nízkorychlostního Internetu.


V rámci EU je problematika informační společnosti (information society) a e-governmentu spravována v působnosti komisaře pro informační společnost a média. Tato společná oblast souvisí s vytvořením jednotného trhu i harmonizací pravidel v rámci Společenství. V prostředí, kdy je výrazný počet finančních transakcí i nákupů učiněn přes Internet, bylo třeba také vytvořit jednotné principy v rámci celé EU. Ta se tedy tradičně zaměřuje na tržní otázky spojené s elektronizací.

---

100 Tzv. východního rozšíření v letech 2004 a 2007.
101 Po vstupu těchto zemí do EU se jich však už týkal Akční plán eEurope 2005. Na ten ČR zareagovala svými strategiemi, zejména Státní informační a komunikační politikou a Národní politikou pro vysokorychlostní internet (viz výše).
107 E-commerce, e-banking, ale také působení na srovnání roamingových cen volání s těmi místními.
Nicméně problematika rozvoje elektronické veřejné správy je sledována rovněž, a to zejména z hlediska jejího zefektivnění a zlevnění. Důraz je kladen také na větší demokratizaci a personalizaci veřejné správy. Občané totiž budou moci pohodlněji z prostředí svých domovů i adresněji skrze obrácení se na konkrétní úřad komunikovat se státní správou.

V případě, že je přístup k vyspělým ICTs i informacím některým skupinám či obyvatelům nedostatečný, může také docházet k jakési manipulaci ze strany osob disponujícími těmito prostředky. EU se tedy zaměřuje na zvyšování počítačové gramotnosti. Orgány EU dále sledují rizika spojená s případným zneužitím informací o občanech, které jsou zprostředkovávány elektronicky. Komisařka V. Reding se zaměřila ve svém nedávném návrhu projektu Digital Europe (Digitální Evropa), který by měl navázat na končící i2010, mimo jiné na rozšíření vysokorychlostního Internetu pro všechny občany EU. V její vizí představuje Digitální Evropa též prostředí zvýšených možností investic a obchodování.

V listopadu 2009 se ve švédském Malmö konala již pátá konference ministrů zodpovědných za problematiku e-governmentu v členských i kandidátských státech EU a v zemích EFTA. Výsledkem

---

109 Putting Citizens First.
112 Viz níže kapitola 2.4. EU a její pojetí informační a kybernetické bezpečnosti.
115 První z konferencí věnovaných problematice e-governmentu se konala v listopadu 2001 v průběhu belgického předsednictví, kdy se jednalo mimo jiné o příležitost výměny zkušeností mezi členskými státy EU. Další ministerská konference zaměřená na rozvoj a posílení e-governmentu se konala v červenci 2003 v italském Como, kdy byl e-government označen jako

Dokument zdůrazňuje inkluzivitu a aktivnější zapojení co největšího počtu aktérů do úspěšného rozvoje e-governmentu. Ten má být zaměřený na občana a na usnadnění využívání jeho služeb (citizen-centric, resp. user-centric). Předpokládá se také zapojení tzv. třetí strany, tedy zintenzivnění vzájemné spolupráce mezi státní správou, soukromými firmami, občanskou společností i samotnými občany. Opět je akcentován význam jednotného evropského trhu, kdy využití a nástroje e-governmentu mají odpovídat jeho principům (zejména přeshraniční služby, mobilita občanů ad.).

EU z podstaty svého existence a základních idejí podporuje spolupráci svých členů a vzájemné sdílení jejich zkušeností nejen v oblasti zavádění a rozvoje e-governmentu. Patrný je tento trend v závěrech deklarace z Malmö, ale jak si ukážeme později, také v dokumentech a praxi vztahujících se k zajištění kybernetické bezpečnosti ve Společenství. Informační společnost a s ní spojené využití ICTs jako základ

---


115 Např. zapojení občanů států a usnadnění jejich komunikace s úřady, pokud studují či pracují v jiných členských státech Unie.

116 Ministerial Declaration on eGovernment., s. 2-3.
ekonomického i společenského rozvoje EU je z tohoto důvodu rovněž zařízeno ve stran centrálních orgánů Společenství, zejména Komise. V tomto spatoříme jakousi morální podporu EU pro rozvoj elektronizace a efektivizace veřejné správy, která je také spojená s demokratizací a možností většího zapojení občanů do veřejného života (viz princip inkluzivní společnosti z iniciativy i2010 či myšlenka customer-centric zaměřené veřejné správy apod.).

Nezanedbatelná či spíše zásadní je také finanční podpora Společenství pro rozvoj elektronizace veřejné správy ve svých členských zemích. Současné unijní rozpočtové období 2007-2013 dosud nápadně koreluje s největšími pokroky v zavádění nástrojů e-governmentu v ČR.

Společenství, v rámci 3. projektové výzvy označené CIP ICT PSP.\textsuperscript{119} Komunitární program na rozvoj ICTs je zaměřen na plnění cílů Lisabonské strategie resp. iniciativy i2010.\textsuperscript{120}

Zhodnocení čerpání evropských finančních zdrojů bude možné až po ukončení výzev i konkrétních projektů. Například v srpnu 2009 však byla většina schválených projektů alokovaných v 2. prioritní ose Integrovaného operačního programu orientované na zavádění a rozvoj sítě kontaktních míst Czech POINT.\textsuperscript{121} Nicméně již teď můžeme říci, že finance využité v projektech spojených s elektronizací veřejné správy posunuly celkový vývoj e-governmentu výrazně dopředu.

1. 4. Vývoj právního ukoření e-governmentu a vládních postojů k němu

Problematiku zavádění informačních systémů a s tím spojené zpracovávání osobních údajů určitým způsobem právě ukoření. Totalitní režim před rokem 1990 právní úpravy nakládání s osobními daty nepovažoval za důležité, zejména z důvodů udržování občanů v nevědomosti o svých praktikách.\textsuperscript{122} Nastolení demokratického režimu znamenalo změnu vnímání v nakládání s informačními systémy. Jejich vedení je třeba považovat za výkon státní či veřejné moci, kterou je nutno provádět jen v mezích a způsoby stanovenými zákonem.\textsuperscript{123} Každý informační systém státní správy tak musí být podložen nějakou zákonnou úpravou, která vymezuje jeho vznik, způsob zpracovávání dat v něm obsažených a dále


\textsuperscript{122} MATES, P. – SMEJKAL, V.: c. d., s. 24.

E-government je v ČR založen na několika zákonných a podzákonných úpravách. Nicméně jejich počet i proměnlivost často znesnadňuje orientaci v nich a schopnost veřejnosti správně přijmout technické i politické možnosti e-governmentu.

V r. 2000 byl vytvořen Úřad pro veřejné informační systémy, který měl zajišťovat realizaci Státní informační politiky. ISVS jsou spravovány na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Zákon stanovuje práva a povinnosti správek ISVS a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. V návaznosti na to upravuje působnost Ministerstva vnitra jako ústředního správního úřadu pro tvorbu a rozvoj informačních systémů veřejné správy. Ministerstvo vnitra na základě projektového přístupu omezuje vznik duplicit při provozování ISVS a zabezpečuje reálné požadavky na čerpání financí z veřejných rozpočtů v oblasti ICTs. Připravuje také technologické podmínky pro efektivnější výkon veřejné moci. Zákon o ISVS rovněž zřizuje již výše uvedený Úřad pro ISVS.


ISVS jsou tvořeny registry veřejné správy. V současnosti je třeba zaměřit se zejména na odstranění duplicit a neaktuálních informací v nich, které plynou z měnícího se a vyvíjejícího se životního stylu občanů.


Navrhovány jsou čtyři základní registry veškerých potřebných údajů o občanech. Nejprve to bude Registr obyvatel, který povede referenční údaje o občanech ČR a cizincích s dlouhodobým pobytem na území ČR a jeho správcem bude Ministerstvo vnitra. Druhým je Registr osob, jenž povede referenční údaje o právnických osobách, podnikajících fyzických osobách a orgánech veřejné moci a jehož správcem bude Český statistický úřad. Třetím bude Registr územní identifikace, adres a nemovitostí, kde budou vedeny referenční údaje o územních prvcích.

---

131 Prvními dvěma jsou CzechPOINT a datové schránky.
133 Zákon o základních registrech prošel třetím čtením.
134 Viz výše kapitola 1.1. Vymezení pojmů.
135 Jako první praktické využití e-governmentu chápeme elektronický podpis, dále zavedení CzechPOINTu, třetí pak datové schránky a konečně registry veřejné správy.
(například území státu, území samosprávného nebo správního kraje, území okresu, území obce, katastrální území, stavební objekt, adresní místo, pozemek v podobě parcely) a referenční údaje o územně evidenčních jednotkách (například části obce, ulice nebo jiná veřejná prostranství), a jehož správcem bude Český úřad zeměměřický a katastrální. A konečně čtvrtým bude Registr práv a povinností, který upravuje vedení referenčních údajů o agendách orgánů veřejné moci a dále reguluje vedení referenčních údajů o některých právech a povinnostech fyzických a právnických osob a vedení oprávnění přístupu k datům vedeným v základních registrech nebo v agendových informačních systémech. Správcem Registru práv a povinností bude Ministerstvo vnitra. Zákon o základních registrech také klasifikuje jimi vedené údaje na referenční, referované a ostatní.


---

Srov. také LIDÍNSKÝ, V. a kol.: c. d., s. 77-78; Zákon o základních registrech prošel třetím čtením.

137 Blíže k problematice typů údajů vedených v centrálních registrech viz LIDÍNSKÝ, V. a kol.: c. d., s. 77.


140 Zrovnaprávnění listinné a elektronické má však určité limity. Tento aspekt upravuje § 18, ods. 2 zákona č. 300/2008. (Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 18, ods. 2.)
Zákon o e-governmentu je také vnímán jako nepostradatelný pro rozvoj tzv. smart administration, která umožňuje zefektivnění, zprůhlednění, zrychlení, zkvalitnění a také zlevnění výkonu veřejné správy v ČR. Svým stanovením zákonných podmínek se stal klíčovým pro jednodušší a jasnější aplikace e-governmentu v ČR.

1. 5. Praktické projevy e-governmentu v ČR

Jak jsme si ukázali úsilí o zavedení a rozvinutí e-governmentu je možné v ČR sledovat v zásadě po celá 90. léta minulého století až do současnosti. Bylo třeba však překonat některé překážky a komplikace. Nejprve se jednalo zejména o problémy technického rázu (neexistence vyhovujícího připojení k Internetu a nedostatečná šířka pásma), ale také právního (absence pozitivní právní úpravy, nezbytná pro oblast orgánů veřejné moci). Významnou roli v tomto ohledu sehrála také určitá neschopnost jednotlivých resortů domluvit se na jednotné koncepci a postupu v rámci zavádění nástrojů e-governmentu, což nevyřešilo ani mocensky slabé Ministerstvo informatiky ČR. V této kapitole si přiblížíme konečně úspěšné a praktické projevy e-governmentu v ČR.

1. 5. 1. Elektronický podpis

Elektronický podpis byl prvním z významných a pro veřejnost nejviditelnějších kroků k praktickému využití e-governmentu v ČR. Právním základem pro elektronický podpis je zákon č. 227/2000 Sb., o elektronickém podpisu. Byl poměrně rychlou reakcí na směrnici EU č.

---

142 Egovernment Act – zákon o egovernmentu.
1999/93/EC145 o zásadách Společenství pro elektronické podpisy. 146 Důraz autoři zákona kladli na jeho obecnost a co nejméní technologickou závislost, aby nemusel být měněn s každým posunem v oblasti ICTs.47

V souvislosti s tím, že všechny dokumenty lze v současnosti převést do jejich elektronické podoby, lze podobně konvertovat také podpis jedince. Elektronický podpis pak umožňuje takto signovat dokumenty, u kterých by to v jejich fyzické podobě těžko šlo (např. fotografií, obsahy různých datových médií apod.).148 Zákon o elektronickém podpisu rozlišuje elektronický podpis obyčejný a elektronický podpis zaručený. Obyčejný elektronický podpis má podobu „údajů v elektronické podobě..., které umožňují ověření totožnosti podepsané osoby...“149 Může se tedy jednat o naskenovaný podpis sloužící např. jako podpisový vzor v bankách. Srovnání a posouzení pravosti podpisu je tedy založené na vizuálním zkoumání a je subjektivní.

Zaručený elektronický podpis150 je založen na principu tzv. podpisu digitálního.151 Ten je tvořen kombinací řady číslic.152 Ověření digitálního podpisu probíhá na základě tzv. veřejného klíče, neboli veřejným ověřovacím číslom. Ten musí být veřejně k dispozicí podobně jako podpisový vzor tradičního podpisu.153

---


146 Státy EU spěly k přijímání jednotných postupů v zavádění pravidel použití elektronického podpisu, a to zejména v návaznosti na elektronický obchod na společném trhu. V říjnu 1997 Evropský parlament obdržel studii O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování. Z ní pak vzešla Směrnice 1999/93/EC. (LIDÍNSKÝ, V. a kol.: c. d., s. 39.)


148 Vám tř. c. d. 126.

149 Zaručený elektronický podpis je elektronický podpis, který splňuje čtyři základní požadavky. Zaprůje je jednoznačně spojen s podepisující osobou. Zadruhé umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě. Zaťatři byl vytvořen a k datové zprávě připojen za pomoci prostředků, které má podepisující osoba pod svou výhradní kontrolou. A konečně je tento elektronický podpis k datové zprávě připojen tak, že je možno zjistit jakoukoliv následnou změnu dat. Zaručený elektronický podpis splňuje při správné implementaci nejvyšší bezpečnostní pravidla, což souvisí s jeho praktickým využitím, zejména při úřední komunikaci občanů a orgánů veřejné správy či v elektronickém bankovnictví. (LIDÍNSKÝ, V. a kol.: c. d., s. 40.)


150 Vám tř. c. d. 125.

151 Ten je tvořen kombinací řady číslic. Jedná se tedy o číslo, jehož výpočet je těžba provést pomocí počítače. Ověřit a vytvořit touto číslo dokáže počítač nebo čip.

152 Blíže k vytváření a šifrování algoritmus digitálního podpisu viz MATES, P. – SMEJKAL, V.: c. d., s. 128-129.

153 Vám tř. c. d. 134.
Podepisující pak vytváří svůj digitální podpis na základě vlastního a jedinečného šifrovacího *privátního klíče*. Výhodou elektronického, resp. digitálního podpisu je jeho jednoznačná příslušnost k digitálnímu dokumentu, který nelze změnit beze změny tohoto podpisu.\(^1^{154}\)

Elektronický podpis představuje jeden z nástrojů bezpečné elektronické komunikace. Základními bezpečnostními principy systému elektronického podpisu jsou důvěrnost informací (přístup k důvěrným informacím mají pouze určené subjekty), integrita (informace musí být zabezpečeny proti modifikaci) a neodmyslitelnost odpovědi (je třeba dokázat přesvědčit třetí stranu o přímé odpovědnosti subjektu za autorství, vlastnictví, odeslání i přijetí zprávy).\(^1^{155}\)

Elektronický podpis má dvě úrovně, které zajišťují a zvyšují bezpečnost podepisovacího procesu. Je to zaručený elektronický podpis a tzv. kvalifikovaný certifikát.\(^1^{156}\) Záruku o propojení konkrétní osoby, jejích osobních dat a jejího osobního digitálního podpisu poskytují tzv. certifikáty.\(^1^{157}\) Certifikát lze chápat jako obdobu identifikační karty či průkazu totožnosti v elektronickém světě.\(^1^{158}\)

Tyto certifikáty vydává a stvrzuje tzv. certifikační autorita.\(^1^{159}\) Jedná se o nezávislou třetí stranu, která zaručuje, že veřejný klíč skutečně náleží uvedené osobě.\(^1^{160}\) Certifikační autorita zajišťuje kvalitu a důvěryhodnost vydaných certifikátů, což je podpořeno i legislativními a technickými pravidly provozu instituce této certifikační autority.

Ta musí splňovat podmínky stanovené zákonem o elektronickém podpisu i upřesnění dle vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. Certifikační autorita

\(^{154}\) Blíže k problematice jedinečnosti digitálního podpisu a principu této jedinečnosti viz MATES, P. – SMEJKAL, V.: c. d., s. 132.

\(^{155}\) LIDINSKÝ, V. a kol.: c. d., s. 38.

\(^{156}\) Certifikát je definován jako datová zpráva, kterou vydal poskytovatel certifikačních služeb a která spojuje data pro ověřování podpisu s podepisující osobou a umožňuje ověřit její totožnost. Kvalifikovaný certifikát je pak certifikát, který má náležitosti stanové zákonem o elektronickém podpisu a byl vydán certifikační autoritou splňující předpisy tohoto zákona. (Zákon č. 227/2000 Sb., o elektronickém podpisu, §12; MATES, P. – SMEJKAL, V.: c. d., s. 145-146.)

\(^{157}\) Ty obsahují mimo svoji platnost, svého čísla ad., zejména také údaje identifikující danou osobu a její ověřovací veřejný klíč.

\(^{158}\) LIDINSKÝ, V. a kol.: c. d., s. 39.

\(^{159}\) Postup vytvoření certifikátu viz např. Tamtéž, s. 41-42.

\(^{160}\) Nebo také poskytovatel elektronického klíče.
pak získává od Ministerstva vnitra akreditaci k poskytování certifikačních služeb. Kvalifikované certifikáty, které tato akreditovaná certifikační autorita vydává, jsou pak považovány za nejkvalitnější a nejkvalifikovanější ve vztahu k elektronickému podpisu a standardem v komunikaci se státní správou. Certifikační autorita je tedy pověřena jakoukoli správou klíčů potřebných k bezpečnému elektronickému přenosu dat.

Důvěryhodnost poskytovatele certifikačních služeb je klíčová pro využití elektronické výměny dokumentů. Tato důvěra je v digitálním prostředí budována skrze infrastruktury veřejných klíčů (Public Key Infrastructure, PKI). Tuto infrastrukturu lze definovat několika způsoby. V zásadě se jedná o „souhrn hardwaru, softwaru, lidí, metod a procesů potřebných pro použití kryptografie veřejných klíčů pro určitou množinu osob.“ Je to soubor serverů, certifikačních autorit, registračních autorit, adresářů a aplikací, které umožňují elektronicky modelovat důvěru. PKI sama o sobě fyzicky neexistuje. Vždy se jedná o soubor provázaných řešení. Zpravidla se skládá z poskytovatele certifikačních služeb, centrální databáze PKI, kde jsou k dispozici seznamy vydaných certifikátů a certifikátů s ukončenou platností.

PKI tedy uživatelům umožňuje v prostředí v zásadě nebezpečného Internetu i jiných veřejných sítí si bezpečně vyměňovat data i finance prostřednictvím veřejného i tajného klíče. PKI je základním komponentem celkové bezpečnostní strategie a musí pracovat společně s ostatními bezpečnostními mechanismy. Představuje stále se vyvíjející

---


Blíže k otázce certifikačních autorit viz STĚDROŇ, Bohumír: Úvod do eGovernmentu. Praha 2007, s. 50-59.

162 LIDINSKÝ, V. a kol: c. d., s. 41.
163 ŠTĚDROŇ, B.: c. d., s. 50.
165 Tamtéž, s. 143.
koncept reagující na vývoj v elektronickém, ICT, ale také obchodním světě.  

Nejvýraznějšími bezpečnostními riziky elektronického podpisu jsou zpravidla odcizení privátního klíče, situace, kdy vydavatel si neoprávněně uchová soukromý klíč, resp. ho poskytne další osobě. Dále to může být padělání veřejného klíče odesílatele, tedy narušení autentičnosti veřejného klíče. Nicméně tento postup odporuje zákonu o elektronickém podpisu a je postižitelný dle tohoto zákona.

Bezpečnost elektronického podpisu je tedy založena na třech podmínkách. Nejprve se jedná o zajištění tajnosti privátního klíče uživatele. Dále se jedná o neprolomení kryptografického algoritmu. A konečně nesmí dojít k porušení autentičnosti veřejného klíče, tedy že tento náleží dané podepisující osobě.  

Zneužití veřejného i privátního klíče brání především matematické zákonitosti, tedy jeho složitý matematický výpočet.

---

1. 5. 1. 1. Novelizace zákona o elektronickém podpisu – kvalifikované časové razítko a elektronická značka


---

171 Osoba vydávající kvalifikované certifikáty, kvalifikované systémové certifikáty, kvalifikovaná časová razítko nebo prostředky pro bezpečné vytvoření elektronických podpisů.
172 Toto razítko musí obsahovat své číslo unikátní u daného poskytovatele certifikačních služeb, označení pravidel, podle kterých bylo razítko vydáno, a označení vydavatele razítku. Dále musí
Elektronická značka\textsuperscript{173} je de facto totéž jako elektronický podpis. Je však vytvořena technickým zařízením, nikoli osobou. Její tvoření je automatizované. Termín podepisující osoba je nahrazen termínem označující osoba,\textsuperscript{174} což může být fyzická osoba, právnická osoba nebo organizační složka státu. Vydání elektronické značky je jednodušší, časově i personálně méně náročné. Označující osoba nemusí nutně znát obsah označovaného dokumentu, resp. datové zprávy, která může být velmi rozsáhlá (např. při vydávání elektronických výpisů z úředních databází či při potvrzování přijetí elektronických zpráv apod.).\textsuperscript{175}

Elektronické značky mají také díky novému zákonu o elektronickém podpisu stejnou vlastnost a funkci jako úřední razítko a podpis úřední osoby na listině. Pokud jsou tyto dokumenty vydány orgány veřejné správy, jsou nazývány veřejnými listinami. Jejich obsah nemusí být dokazován na příklad při soudním jednání.\textsuperscript{176}

Zákon o elektronickém podpisu je dále doplněn nařízením vlády č. 495/2004 Sb., které stanovuje povinnost orgánů veřejné správy zřídit elektronické podatelny.\textsuperscript{177}

Toto nařízení vlády o e-podatelnách souvisí s kvalifikované časové razítko obsahovat hodnotu času odpovídající koordinovanému světovému času při vytváření kvalifikovaného časového razítka, data v elektronické podobě, pro která je toto razítko určeno, a konečně je třeba elektronická značka kvalifikovaného poskytovatele certifikačních služeb. (MATES, P. – SMEJKAL, V.: c. d., s. 153.; další vymezení časového razítka viz také Zákon č. 440/2004 Sb., § 2, ods. r)


Zákon č. 440/2004 Sb., čl. 1, § 2, ods. f a § 5a.


Tamtéž, s. 152.


Dle informací Ministerstva informatiky ke dni 1. ledna 2007 mělo e-podatelnu k dispozici 14 z 15 ministerstev, 10 z 11 dalších z ústředních orgánů státní moci (Český statistický úřad, Český úřad zeměměрický a katastrální, Český báňský úřad, Úřad průmyslového vlastnictví, Úřad pro ochranu hospodářské soutěže, Státní úřad pro jadernou bezpečnost, Národní bezpečnostní úřad, Energetický regulační úřad, Úřad vlády České republiky a Český telekomunikační úřad). Pouze Správa státních hmotných rezerv v té době svou e-podatelnu zřízenou neměla. V současnosti ji však disponují také většina krajských úřadů a 97 % obcí s rozšířenou působností Ze závěru zprávy Ministerstva informatiky pak vyplývá, že „(P)očet úřadů, které splňují požadavky nařízení vlády č. 495/2004 Sb. a provozují elektronickou podatelnu v souladu s vyhláškou 496/2004 Sb., o elektronických podatelnách, již dosahuje dostatečnou základnu pro elektronickou komunikaci občana s orgány veřejné moci. ” Komunikovat lze nejen s nejvyššími orgány státní správy, ale také s většinou obcí i krajských úřadů. V současnosti (4. srpna 2009) má zřízeno elektronickou podatelnu všech 16 ministerstev i Vláda ČR samotná. (Informace o zřízení elektronických podatel u orgánů veřejné moci. In: Ministerstvo vnitra ČR,
vyhláškou č. 496/2004 Sb. k elektronickým podatelnám. Ta „upravuje postup, jak mají orgány veřejné moci přijímat a odesílat datové zprávy prostřednictvím elektronické podatelné. „[178] Jsou zde také uvedeny postupy ověřování platnosti zaručeného elektronického podpisu a elektronické značky, stejně jako platnosti kvalifikovaného certifikátu a kvalifikovaného systémového certifikátu. [179] Vyhláška upravuje rovněž způsoby a okolnosti podání a doručení datové zprávy. [180]

Zavedení elektronického podpisu bylo dobře technicky připravené, nicméně hlavními překážkami pro jeho plošnéjší užití je zejména jeho omezená platnost a také zpoplatnění. Pro jedince či malé firmy se tak elektronická komunikace s úřady prostřednictvím elektronické podatelné a elektronického podpisu jeví jako nevýhodná a neefektivní. Institu tu elektronického podpisu však nelze upřít pozitivní vliv na vývoj e-governmentu v ČR, a to zejména v souvislosti se zrovnaprávněním elektronických a písemných forem dokumentů. Významný je také jeho rys nepopiratelnosti zprávy, kterou doprovází, a také možnosti jednoznačně ověřit identitu podpisujícího. [181] Omezené využívání elektronického podpisu lze také připsat nedostatečné propagaci mezi veřejností. [182]

### 1. 5. 2. Elektronické doručování a podání

V souvislosti s elektronickým podpisem je třeba také uvést problematiku elektronického doručování a podání na úřady. To umožňuje Správní řád ČR. Povinné pro úřady je také provozování elektronické úřední desky.

---


[179] Tamtéž.

[180] Za doručenou se považuje datová zpráva, která je k dispozici v elektronické podatelni. Zde se ukládá do úložiště spolu s uznávaným elektronickým podpisem či uznávanou elektronickou značkou. Elektronická podatelná obdrží jejich pravost a správnost dle zákona. (Blíže viz MATES, P. – SMEJKAL, V.: c. d., s. 190-192)


Zákon o elektronickém podpisu dává občanu možnost činit podání k orgánům státní moci elektronicky za použití zaručeného elektronického podpisu. Nicméně již dva roky po jeho vydání, tedy v roce 2002 např. občanský soudní řád tuto možnost nahradil podáním s běžným elektronickým podpisem. To je pak třeba do tří dnů doplnit fyzickým písemným dokumentem. Podle Matesa a Smejkala se jednalo o krok zpět a poukazuje to na nedostatečnou podporu elektronické komunikace v rámci státní správy.183

K menší podpoře e-governmentu se vyjadruje také A. Ptašnik v závěru své stati, kdy zdůrazňuje efektivitu a snižování nákladů při zavádění prvků e-governmentu do veřejné správy. Poukazuje na správně „namířené“ kroky z centrální úrovni, které však podrývá nejednotnost, nepochopení, ignoranci či pouze konzervatismus objevující se na různých úrovních veřejné správy.184

Státní orgány zatím elektronickou komunikaci v praxi příliš nepreferují, a to zejména kvůli nízkému zájmu občanů využívat tuto možnost, informační gramotnosti úředníků a technických možností na příklad u malých obcí a také kvůli obtížnému zpracovávání dokladů pro správní řízení do elektronické podoby (např. smluv s podpisem, notářsky ověřených zápisů apod.).185

Přesto se však situace pro elektronická podání a doručování za užití zaručeného elektronického podpisu postupně stává příznivější a většina orgánů státní správy jsou ji podstatně nakloněnější než dříve. Elektronická komunikace186 umožňuje omezit fyzickou přítomnost občana

---

O některých problémech zavádění elektronického podání a doručování viz Tamtéž, s. 162-163.
185 LIDÍNSKÝ, V. a kol.: c. d., s. 48.
186 V souvislosti s rozšiřováním možnosti užít elektronickou komunikaci a doručování je třeba se zabývat také problematikou konverze fyzických dokumentů v elektronické se zachováním jejich důkazní hodnoty. V tomto ohledu sehlavá základní roli legislativní úprava, která definuje pravidla elektronické komunikace i podmínky zrovnapravnění listinných a elektronických dokumentů. Stěžejně se v tomto ohledu jeví definice originálu resp. autentického dokumentu. Ten musí splňovat tato kritéria: je zachována integrita informací obsažených v dokumentu od okamžiku jeho dokončení v libovolné podobě, datová zpráva je v písemné podobě a konečně informace zůstanou nezměněné a kompletní ve srovnání s právě dokončeným dokumentem (s výjimkou připojení příslušných potvrzení nebo certifikátů zajišťujících integritu, eventuálně s výjimkou nezbytných změn vzniklých při komunikaci, úschově či převedení informací). (LIDÍNSKÝ, V. a kol.: c. d., s. 73.)
na úřadě, což vede k určitému usnadnění práce úředníka. Je také možno „odbavit“ více žádostí a dokumentů při stejném počtu zaměstnanců.\textsuperscript{187} Elektronická komunikace v rámci státní správy v ČR dostává nový impuls v podobě zavádění datových schránek či projektu eJustice.\textsuperscript{188} Je tak zde zřetelný posun ve prospěch četnějšího využití elektronické komunikace ve státní správě.

Zákon o ISVS\textsuperscript{189} zavedl možnost doručit datové zprávy orgánům státní moci prostřednictvím Portálu veřejné správy.\textsuperscript{190} Pro větší komfort a ochranu podavatele, tedy občana, je důležitý moment podání, tedy převzetí správce portálu, od kdy běží předepsané lhůty. Správce musí zprávu dodat do tří dnů od okamžiku podání. Prodleva tedy je „k tíži“ veřejné správy.\textsuperscript{191} S datovou zprávou má do jejího dodání oprávnění nakládat pouze odesílatel a správce.\textsuperscript{192}

Dle Matesa a Smejkala je způsob elektronického doručování a dodání nejasný, nesrozumitelný, a tedy nedostačující.\textsuperscript{193} Je to zapříčiněno hlavně nejednotností zákonných úprav o elektronickém podání a doručování pro různé orgány státní moci. Zavedení jednoho a efektivnějšího způsobu elektronického podání a doručení v rámci celé státní správy je „základním předpokladem pro plnohodnotné zavedení služeb e-governmentu a je plně v souladu s vládní politikou e-governmentu."\textsuperscript{194} Řešením se jeví zavedení tzv. datových schránek 1. července 2009, resp. 1. listopadu 2009, kdy byl zahájen jejich ostrý provoz.

\textsuperscript{187} Proto se také průkopníky ve využívání elektronické komunikace staly banky, které poskytováním svých elektronických bankovnictví umožnily vykonávání běžných úkonů spojených s ovládáním vlastního účtu prostřednictvím Internetu. Omezil se tak počet návštěv klienta v bance.


\textsuperscript{189} Viz výše.

\textsuperscript{190} Správcem Portálu veřejné správy, který nese zodpovědnost za podání i doručení této zprávy, je Ministerstvo vnitra ČR.

\textsuperscript{191} MATES, P. – SMEJKAL, V.: c.d., s. 185.

\textsuperscript{192} V případě správce portálu se jedná pouze o úkony nezbytné k dodání zprávy. Odesílatel má více možností. Může zprávu vzít zpět i změnit její obsah a podobně. Správce má však právo datovou zprávu zlikvidovat, pokud ji nelze dodat ani vrátit nebo pokud zpráva obsahuje nebezpečné složky, které by mohly přinést škodu (např. viry).

Tamtěž, s. 187.

\textsuperscript{193} Viz také SMEJKAL, V.: c.d.

\textsuperscript{194} MATES, P. – SMEJKAL, V.: c. d., s. 192.
1. 5. 3. Czech POINT


Záměrem koncepce CzechPOINT je koncentrace výkonu státní správy do jednoho kontaktního místa, ze kterého občan může komunikovat s různými orgány a úřady státní moci. Obíhat mají data, nikoli občan. Na jednom univerzálním místě lze „získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních organů.“ V konečné fázi projektu se předpokládá, že občan bude všechny tyto úkony vykonávat z domova přes internet a nebude muset navštěvovat ani kontaktní místo. Zde je používán pojem CzechPOINT@home, kdy se jedná o informační portál, jehož účelem je vytvořit jednoduchou a intuitivní platformu pro komunikaci občana s veřejnou správou a pomoci tak přesunout eGovernment z prostředí podatelen úřadů do domácího pohodlí občanů.

Dalším rozšířením možností a působení CzechPOINTu je uvedení tzv. CzechPOINT@office. Jedná se o vnitřní CzechPOINT v rámci úřadů a

195 Název lze vnímat také jako slovní hříčkou odkazující na „check point“, tedy místo kontroly.
196 Viz výše.
197 Spolu se zavedením elektronického podpisu a datových schránek (Viz níže kapitola 1.5.4. Datové schránky.).
200 Tamtéž.
orgánů veřejné moci. Jeho prostřednictvím lze provést autorizovanou konverzi elektronických dokumentů dle zákona č. 300/2008 Sb. a také výpis z rejstříku trestů z moci úřední. Služby CzechPOINT@ofice budou dále rozšiřovány.  

Původními výstupy CzechPOINTu byly výpisy z Katastru nemovitostí, Obchodního rejstříku a Živnostenského rejstříku. Postupně se možnosti přístupu k výpisům z veřejných i neveřejných registrů stejně jako možnosti podání ke správnímu řízení i autorizované konverze dokumentů rozšiřovaly. V roce 2008 přibyl přístup do Trestního rejstříku. Rok 2009 přinesl zatím nejrozsáhlejší posun ve službách poskytovaných CzechPOINTem. Bylo umožněno podávat podání k Živnostenskému úřadu, získávat výpisy z registru řidičů, Seznamu kvalifikovaných dodavatelů, Registru účastníků provozu modulu autovraky ISOH a Insolvenčního rejstříku. Zároveň je možné na CzechPOINTu vykonávat některé úkony spojené s používáním datové schránky (např. její zřízení, změna či zneplatnění přístupových údajů apod.).

Využívání kontaktního místa CzechPOINT z hlediska přístupu občanů lze hodnotit pozitivně. V jeho rámci již bylo vydáno více než dva miliony výpisů z různých rejstříků a rozšiřuje se také síť jeho provozoven.

1. 5. 4. Datové schránky

Datové schránky uvedl zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů platný od 1. července 2008

---

203 Veřejné registry: Obchodní rejstřík, Katastr nemovitostí, Živnostenský rejstřík, Seznam kvalifikovaných dodavatelů a Insolvenční rejstřík.
204 Z listinné do elektronické a naopak. CzechPOINT umožňuje také ověření provedení autorizované konverze.
206 Viz níže kapitola 1.5.4. Datové schránky.
208 Informačním i komunikačním portálem datových schránek je http://www.datoveschranky.info.
Jedná se o „elektronické úložiště, které je určeno k doručování dokumentů orgánů veřejné moci a k provádění podání vůči nim.“

Dochází také k částečnému, ale významnému nahrazení klasického doručování v listinné podobě. Dokumenty doručené prostřednictvím datové schránky budou mít stejnou váhu a platnost jako doručená zásilka s dodejkou i do vlastních rukou. Tyto úpravy „přinášejí zásadní změny v komunikaci mezi orgány veřejné moci a adresáty veřejné správy a v oblasti nakládání s dokumenty v rámci orgánů veřejné moci.“

Podobně jako elektronický podpis datová schránka zajišťuje nepopiratelnost odesílatele i příjemce. Rozdíly mezi datovou schránkou a současně běžně používaným e-mailem spočívají především v právní podstatě věci. Datová schránka také zatím neumožňuje komunikaci mezi právnickými a fyzickými osobami navzájem.

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů


Datová schránka je elektronickým úložištěm čili datovým prostorem, kam budou datové zprávy doručovány a uchovávány po určitou dobu. Datová zpráva, jejíž velikost může být maximálně 10 MB, je tvořena obálkou a obsahem zprávy. Může také obsahovat přílohy v libovolném formátu (s výjimkou přípon .exe a komprimovaných souborů). Jde hlavně o bezpečnostní riziko přenosu virové infekce v informačním systému. Provozovatel datové schránky má také možnost nepřijmout k odeslání zprávu obsahující škodlivý kód. Datovou zprávu definujeme dle zákona o elektronickém podpisu jako „elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou“.


Ministerstvo vnitra je také zodpovědné za zasílání přístupových údajů k datové schránce, která je pak zpřístupněna prvním přihlášením.
oprávněné či pověřené osoby, resp. do 15 dnů od doručení přístupových údajů.\textsuperscript{221}

Nakládat s datovou schránkou smí pouze tzv. oprávněná osoba.\textsuperscript{222} Jedná se v zásadě o osobu (fyzickou i právnickou), pro kterou byla datová schránka zřízena. U velkých organizací (právnické osoby, orgány veřejné moci apod.) pak jsou používáním datové schránky pověřeni tzv. administrátoři.\textsuperscript{223} Pro vstup do datové schránky je potřeba disponovat přihlašovacími údaji (jménem a heslem) a je možné použít také digitální nebo kvalifikovaný certifikát pro zvýšení bezpečnosti.\textsuperscript{224}

Orgány veřejné moci mají povinnost komunikovat prostřednictvím datové schránky, pokud ji má protistrana zřízenu.\textsuperscript{225} Povinné je zřízení datové schránky pro orgány veřejné správy a právnické osoby.\textsuperscript{226} Fyzické osoby, občané a živnostníci mají pouze možnost si datovou schránku zřídit.\textsuperscript{227}

Spolu s fungováním registrů veřejné správy budou datové schránky znamenat také umožnění kontroly občany, kdy a jak bylo nakládáno s jejich osobními údaji obsaženými v těchto registrech. Do datové schránky totiž přijde zpráva o průběhu použití příslušných osobních údajů.\textsuperscript{228}

Na rozdíl od elektronického podpisu je zřízení a využití datové schránky pro většinu subjektů zdarma.\textsuperscript{229} Zpoplatněna je jen autorizovaná

\textsuperscript{221} Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 10.
\textsuperscript{222} Ministr, hejtman, starosta, ředitel úřadu, jednatelé a vedoucí organizačních složek.
\textsuperscript{223} Dále může být využito také institutu pověřené osoby, kterou deleguje administrátor nebo oprávněná osoba. Blíže viz Zákon 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 8; srov. PROTIVOVÁ, I. a kol.: c. d., s. 31-32.
\textsuperscript{224} Datové schránky. Typový postup implementace. Občan., s. 5; Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 8.
\textsuperscript{225} Viz Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 17, ods. 1.
\textsuperscript{226} Ty je musejí mít zřízeny k 1. listopadu 2009, kdy byla ukončena tzv. přechodná fáze existence datových schránek (od 1. července 2009).
\textsuperscript{227} Výjimkou jsou advokáti, daňoví poradci, insolvenční správci, notáři a exekutoři, kterým bude datová schránka zřízena automaticky. Výjimku mají advokáti vedení v seznamu České advokátní komory a daňoví poradci, kteří si datovou schránku musí zřídit nejpozději do 1. července 2012.
konverze dokumentů z do elektronické podoby a zaslání přístupových údajů, pokud je o ně žádáno do tří let od předchozího předání. Zaslání datové zprávy orgánu veřejné moci budou hrazeny ze státního rozpočtu. V budoucnu se počítá se zpoplatněním komunikace mezi právnickými osobami. Platnost schránky je v podstatě neomezena. Z tohoto důvodu i skutečnosti, že datovou schránkou lze disponovat zdarma, lze očekávat větší zájem veřejnosti o tuto možnost elektronické komunikace se státní správou, než jak tomu bylo u elektronického podpisu či institutu elektronického doručování a podání.

Datová zpráva poslaná skrze datovou schránku nemusí mít sama o sobě elektronický podpis. Informační systém datové schránky automaticky připojuje k datové zprávě kvalifikované časové razítko, které připomíná Ministerstvo vnitra coby správce informačního systému datových schránek. Nicméně elektronický podpis je třeba v situaci, kdy je potřeba ověřený podpis, či pokud je nutné, aby dokument podepsalo více osob.

Problémem fungování datových schránk se v období po 1. červenci 2009 stal zejména nedostatek času pro testování provozu. Proces novelizace zákona o datových schránkách není ukončený. Kupříkladu větší organizace (např. krajské úřady) se potýkaly s touto komplikací kvůli velkému objemu jimi spravovaných dat. Krajský úřad je složitou organizační strukturou, která vykonává velký rozsah agend a má povinnost vést spisovou službu v plném rozsahu. Elektronizace spisové služby v období moderních ICT prostředků tak může podstatně zefektivnit práci


231 Blíže viz PROTVIPOVA, I. a kol.: c. d., s. 15-18.

232 Autorizovanou konverzi provádí kontaktní místo CzechPOINT.


234 Problémem fungování datových schránk se v období po 1. červenci 2009 stal zejména nedostatek času pro testování provozu. Proces novelizace zákona o datových schránkách není ukončený. Kupříkladu větší organizace (např. krajské úřady) se potýkaly s touto komplikací kvůli velkému objemu jimi spravovaných dat. Krajský úřad je složitou organizační strukturou, která vykonává velký rozsah agend a má povinnost vést spisovou službu v plném rozsahu. Elektronizace spisové služby v období moderních ICT prostředků tak může podstatně zefektivnit práci

235 V červnu 2009 byla přijata novela, která měnila zejména financování provozu systému datových schránek.
úřadu. Elektronickou spisovou službu využívá také např. projekt CzechPOINT při svých výstupech. Při vedení spisové služby elektronicky je pak pro orgán veřejné moci nezbytné umožnit její propojení se systémem datové schránky.

Provozovatel datových schránek, Česká pošta, k jejich užívání připravila také některé doplňkové služby. Jedná se na příklad o SMS upozornění o příchozí datové zprávě, datový trezor či bezpečný klíč k datové schránce. Lze očekávat další rozvoj i vývoj jak v těchto doplňkových službách, tak v celkovém konceptu datových schránek.

Ostrý provoz datových schránek zahájený 1. listopadu 2009 sice dosud neprovázely zásadnější technické problémy, ale systém se potýká spíše s nedůvěrou či nezájmem subjektů, které mají mít datovou schránku ze zákona zřízenou. Ministerstvo vnitra coby správce informačního systému datových schránek tak muselo zřídit 72 % z povinně aktivovaných datových schránek, a to jak právnickým osobám, tak některým orgánům veřejné moci. K 1. listopadu však tento způsob komunikace s veřejnou správou zvolilo přes 10 000 občanů, kteří povinnost zřídit si datovou schránku neměli.

První hodnocení fungování datových schránek představilo Ministerstvo vnitra spolu s Českou poštou na tiskové konferenci dne 18. listopadu 2009. Z jejich pohledu je systém stabilní a funkční. Aktivních je 98,5 % z 371 460 zřízených datových schránek. Úspěšnost doručení

---

238 Projekt datových schránek je s CzechPOINTem provázaný i v jiných oblastech. Je zde možné si datovou schránku zřídit. Na kontaktních místech Czech POINT lze také zažádat o nové přihlašovací údaje, znovuzapnutí přístupových údajů nebo zneplatnění datové schránky. (O datových schránkách)


241 Před stanoveným datem bylo aktivováno 110 284 datových schránků spadajících do této kategorie.

242 Konkrétně to bylo 10 186 aktivovaných datových schránek v této kategorii.

Datových zpráv prostřednictvím přihlášení uživatele (nikoli fikcí) je 88,7 %. Vyzvednutí datové zprávy přihlášením ve lhůtě do deseti dnů je téměř 95 %, což je ze strany České pošty hodnoceno jako poměrně úspěšnější způsob doručování než u listovních zásilek. Je také možné sledovat rostoucí počet aktivovaných datových schránek ze strany fyzických osob, ale také právnických osob. Skutečně aktivních datových schránek, tedy takových, ke kterým se jejich uživatelé skutečně přihlásili, je ale 53,6 %.

Tato čísla nás tedy vedou k optimistickému pohledu na využívání systému datových schránek. Pozitivní je z našeho pohledu rostoucí zájem o tento způsob komunikace se státní správou ze strany občanů, kteří nemají zákonnou povinnost mít datovou schránku zřízenou. Další hodnocení tohoto projektu je zejména z důvodu malého časového odstupu obtížné. Nicméně očekáváme zde další pokrok. Státní správa by se v této oblasti měla zaměřit právě na tzv. fyzické osoby a možnost komunikace skrze datové schránky jim co nejvíce zpřístupnit, a to prostřednictvím dostatečného internetového připojení, ale také náležitou propagací a osvětou. Je třeba zapracovat na uživatelském komfortu občanů-zákazníků.

Datové schránky představují pozitivní přínos pro rozvoj e-governmentu v ČR rozšiřováním jeho nástrojů a působnosti. Praktické využití prostředků e-governmentu ze strany občanů nicméně není ještě plně aplikované. V r. 2008 využívalo možnost komunikovat s veřejnou správou elektronicky 14 % Čechů. V tomto čísle zaostáváme za průměrem EU, který činí 28 %.


59
2. RIZIKA E-GOVERNMENTU A ZNEUŽITÍ ICTs PROTI STÁTU

Současná post-moderní společnost se stala do určité, i když významné míry závislá na vyspělých komunikačních prostředcích. Zejména se jedná o Internet, ale také mobilní telefony apod. Internet přestal být pouze místem pro akademickou činnost, ale stal se „globálním mainstreamovým obchodním a komunikačním médiem.\textsuperscript{246} V první části této práce jsme se zabývali rozvojem a zaváděním prvků e-governmentu, tedy prostředků moderních ICTs, do státní správy s hlavním cílem tuto zefektivnit, lépe zpřístupnit občanům a také zlevnit. Druhou část textu pak věnujeme skutečnosti, že informační systémy, na jejichž bázi e-government funguje, jsou ohrožitelné.

Z pohledu bezpečnosti státu se pak může jednat hlavně o narušení tzv. klíčových infrastruktur, resp. klíčových informačních infrastruktur. V současnosti podstatná část finančních transakcí probíhá prostřednictvím různých sítí (opět hlavně Internetu). K řízení dopravy, transportu či energetické sítě jsou využívány vyspělé ICTs. Správa informací o obranných složkách či komunikace mezi nimi probíhá pomocí těchto prostředků, stejně jako komunikace mezi složkami státní správy i občany. V tomto prostředí existuje reálné riziko zneužití tohoto využívání ICTs ze strany jak počítačových hackerů, tak také státních a nestátních aktérů cílících na omezení schopnosti jiného státu správně fungovat a zajišťovat základní funkce a služby svým občanům.

V této kapitole se však nejdříve budeme věnovat bezpečnosti informačních systémů, zejména ISVS, a také informační bezpečnosti coby teoretickému i praktickému přístupu k řešení problematiky ohrožení bezpečnosti informačních systémů, které jsou základem fungování e-governmentu. Prostor bude věnován také některým konkrétním příkladům zajištění této bezpečnosti. Následovat bude pojetí tzv. kybernetické bezpečnosti a rozpracování možností zneužití ICTs proti státu. V závěru této kapitoly představíme přístupy EU k zajišťování informační či kybernetické bezpečnosti.

\textsuperscript{246} BONI, William – KOWACICH, Gerald L.: Netespionage: The Global Threat to Information. Woburn 2000, s. 3. (http://books.google.com)
2. 1. Bezpečnost a zabezpečení ISVS

Bezpečnost informačních systémů patří k nejčastěji užívaným pojmům v teorii i praxi e-governmentu. Propojování počítačů veřejné správy do velkých sítí, kdy se orgány veřejné správy v důsledku obrovského objemu spravovaných a zpracovávaných dat musejí de facto spoléhat na moderní prostředky komunikace (zejména Internet a také Intranet), je otázka zajištění bezpečnosti těchto sítí jednou z nejpalčivějších.

I přes poměrně frekventované užívání pojmu bezpečnost informačního systému se jeví, že ne všichni tvůrci, provozovatelé i uživatelé informačních systémů ho chápou stejně. Bezpečnost ISVS lze vnímat jako cíl neboli ideální stav nebo jako prostředek k dosažení tohoto cíle. H. Křepelková ve svém článku popisuje bezpečnost informačního systému jako „stav informačního systému, kdy rizika, jímž je vystaven, jsou snížena na přijatelnou úroveň na základě vhodných bezpečnostních opatření.“

R. Jašek bezpečným informačním systémem rozumí „systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a při jejich likvidaci proti ztrátě důvěrnosti.“

Server Informační systémy veřejné správy nicméně dále nepředkládá jednoznačné vymezení pojmu bezpečnost informačních systémů, nýbrž prezentuje způsoby, jak tohoto stavu dosáhnout.

Pro stanovení bezpečnosti informačního systému se také uvádí spíše pojem zabezpečený, který také lépe odpovídá realitě. Je totiž třeba určit za jakých podmínek je daný ISVS bezpečný, resp. zabezpečený a míru zabezpečení daného ISVS. Někteří autoři také hovoří spíše o důvěryhodném informačním systému. Není možné zajistit absolutní

---

251 POŽÁR, J.: c. d., s. 50.
bezpečnost a je tedy třeba si uvědomit a přijmout určitou míru akceptovatelného rizika.\textsuperscript{252}

Bezpečností informačního systému však v zásadě rozumíme zachování důvěrnosti (zájistění, že daná informace je dostupná pouze oprávněným osobám; k tomu je zapotřebí identifikace uživatelů prostřednictvím ověřeného mechanismu pro zjišťování totožnosti), integrity (zájistění kompletnosti a správnosti informací a metod zpracování) a dostupnosti (přístupnost informace autorizovaným uživatelům dle jejich potřeby).\textsuperscript{253}

OECD v červenci 1992 přijala seznam devíti doporučených principů bezpečnosti informačních systémů s názvem Guidelines for the Security of Information Systems\textsuperscript{254}. Jejich obecnost umožňuje jejich aplikaci na různé organizace, firmy i úřady a jejich platnost je aktuální i v současnosti. Principy dle OECD tvoří vzájemně provázanou skupinu, kdy odpovědnost účastníků bezpečnostních přístupů se liší dle jejich rolí. Je však zdůrazněn aspekt demokratické společnosti a sdílení informací.\textsuperscript{255}

Prvním z principů je uvědomění si potřeby bezpečných informačních systémů, dále je to zodpovědnost všech účastníků v rámci informačních systémů. Účastníci v rámci informačních systémů mají adekvátně a včas ve vzájemné spolupráci předcházet, odhalovat a reagovat na případné bezpečnostní hrozby. Dalšími důležitými aspekty jsou etika, kdy jsou respektovány zájmy ostatních účastníků systému, demokracie dle principů otevřené, demokratické společnosti charakterizované svobodným tokem informací, a reálné zhodnocení rizik. Organizace mají aplikovat bezpečnost jako základní prvek svých informačních systémů a sítí v rámci své bezpečnostní struktury. Mají také přijmout jednoznačný přístup k bezpečnostní správě informačních systémů. A konečně je zdůrazňováno

\begin{footnotes}
\footnotetext[252]{JAŠEK, R.: c.d., 10.}
\footnotetext[253]{MATES, P. – SMEJKAL, V.: c. d., s. 65.}
\footnotetext[255]{Tamtéž, s. 9.}
\end{footnotes}
přehodnocování bezpečnostních rizik a politik dle aktuálního vývoje.\textsuperscript{256} Tyto principy definované OECD lze považovat za inspiraci pro přístup také českých veřejných orgánů k bezpečnosti ISVS.

Zákon č. 365/2000 Sb., o ISVS uvádí, že o bezpečnost provozu ISVS je zodpovědný jeho provozovatel, tedy orgány veřejně správy.\textsuperscript{257} Vyhláška č. 529/2006 Sb., o dlouhodobém řízení ISVS stanovuje,\textsuperscript{258} že orgán veřejné správy ve své informační koncepci určí dlouhodobé cíle pro řízení bezpečnosti ISVS. Těmito cíli jsou bezpečnost dat zpracovávaných v daném systému (nelze je neoprávněně číst, mazat či jinak měnit), bezpečnost programových a technických prostředků (tedy není možné měnit zdrojový kód programu bez oprávnění, ve vytvářených programech je nutné ověřovat všechna vstupní data) a také bezpečnost služeb, které ISVS poskytuje (poskytované služby musí být přístupné jen oprávněným uživatelům, o přístupu ke službám musí být pořizovány záznamy).

Orgán veřejné správy také stanovuje požadavky na bezpečnost ISVS a „stanoví plán řízení bezpečnosti, který obsahuje popis činností, které orgán veřejné správy vykonává pro dosažení stanovených požadavků na bezpečnost ISVS, včetně časového harmonogramu jejich plnění.“\textsuperscript{259} Bezpečnostní dokumentace ISVS je také součástí provozní dokumentace ISVS. Bezpečnostní dokumentace obsahuje bezpečnostní směrnic pro činnost bezpečnostního správce systému. Pokud daný orgán veřejné moci není provozovatelem tohoto ISVS či pokud má vazby s ISVS jiného správce, musí bezpečnostní dokumentace obsahovat také bezpečnostní politiku.\textsuperscript{260}

Bezpečnostní politika obsahuje popis opatření, která orgán veřejné správy uplatňuje při zajištění bezpečnosti ISVS. Je to klíčový dokument pro řešení bezpečnosti informačních systémů jakékoliv instituce a je schválený nejvyšším vedením této organizace. Vychází ze studie

\textsuperscript{257} Zákon č. 365/2000 Sb., o ISVS.
\textsuperscript{258} Správcem je OVM, který může pověřit provozovatele.
\textsuperscript{260} Tamtéž, § 4.

63
bezpečnosti či ze zadání instituce ve formě definovaných cílů, požadavků a analýzy rizik. Definuje tedy, co má být chráněno a také stanovuje rámec, jak této ochrany dosáhnout. Ukládá příslušné zodpovědnosti a pravomoci.\textsuperscript{261} Musí také existovat bezpečnostní směrnice pro činnost bezpečnostního správce systému.\textsuperscript{262} Ten je pak osoba pověřená orgánem veřejné správy pro výkon kontroly bezpečnosti ISVS.\textsuperscript{263}

Další aspekty bezpečnosti ISVS v ČR vycházejí také ze souvisejících zvláštních předpisů, zejména pak ochrany osobních údajů. Zabezpečením osobních údajů se zabývají paragrafy 13 až 15 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.\textsuperscript{264} Zákon také uvádí bezpečnost v souvislosti s elektronickým podpisem, kdy systém certifikační služby je bezpečný, pokud jím zpracovávaná data jsou důvěryhodná, je u nich zajištěna integrita, dostupnost a je prokazatelný jejich původ.\textsuperscript{265}

Bezpečnost ISVS je spojená rovněž s dodržováním určitých technických předpisů. Ty jsou uvedeny v zákoně č. 22/1997 Sb., o technických požadavcích na výrobky.\textsuperscript{266} Ten v § 4 zavádí „českou technickou normu“ v podobě dokumentu schváleného právnickou osobou pro opakované nebo stálé použití. Označována je jako ČSN. Není však obecně závazná.\textsuperscript{267}

Zaveden byl také pojem harmonizované ČSN. Jeho definice vychází z evropských právních úprav a dokumentů, zejména z rezoluce Evropské rady ze 7. května 1985 Nový přístup k technické harmonizaci a normám (New Approach to technical harmonization and

\begin{footnotesize}
\footnotesize
\begin{enumerate}
\item Více k problematice bezpečnosti a jejích kritérií viz MATES, P. – SMEJKAL, V.: c. d., s. 66-67. K otázce ověřování bezpečnosti viz Tamtéž, s. 68.
\item Přehled právních předpisů týkající se bezpečnosti ISVS předkládají rovněž Mates a Smejkal v kap. 2. 4. (Tamtéž, s. 79-80). Bezpečnost související s užitím elektronického podpisu již byla přibílena v kapitole 1. 5. 1. Elektronický podpis.
\item Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy, § 11, ods. 3 a 4.
\item Organizace či úřad může také dispozovat tzv. manažerem bezpečnosti informačního systému, který svou funkcí spadá do oblasti správy organizace, zabývá se poradenstvím pro oblast informační bezpečnosti, reprezentuje organizaci z hlediska bezpečnosti apod. (POŽÁR, J.: c. d., s. 80-81)
\item Blíže k funkci správce bezpečnosti informačního systému viz také POŽÁR, J.: c. d., s. 78-79.
\end{enumerate}
\end{footnotesize}


---


269 Kritéria ITSEC specifikují sedm tříd zaručitelnosti bezpečnosti IT pod označením E0-E6. ITSEC jsou formulována obecněji než původně pro vojenské účely vytvoření TCSEC (Trusted Computer System Evaluation Criteria), která jsou zaměřená na ochranu důvěrnosti informací. (Viz POŽÁR, J.: c. d., s. 50-52.)


272 Malwarem rozumíme tzv. škodlivý software (malicious software). Viz níže kapitola 2.2.1. Hrozby informační bezpečnosti.

273 Rozdělení norem na: 1. základní bezpečnostní normy pro obecné použití (bezpečnostní architektury); 2. funkční normy (popisují realizaci požadavků vyplývajících z obecných norem); 3. hodnotící normy (pro hodnocení bezpečnosti např. IS, produktů, postupů aj. Jsou to např. ITSEC, TCSEC); 4. speciální normy (pro určitou činnost, např. telekomunikace, či určité odvětví, obor nebo uživatele, např. armádu, finanční instituce, zpracování osobních údajů.) (MATES, P. – SMEJKAL, V.: c. d., s. 83.)

274 Blíže viz Tamtéž, s. 84.

Přehled nejvýznamnějších norem souvisejících s bezpečností informačních systémů uvádí také H. Křepelková. (Viz KŘEPELKOVÁ, H.: c.d.)

---

65
Za bezpečnost informačního systému v oblasti veřejné správy je zodpovědné Ministerstvo vnitra, konkrétně oddělení jeho Odboru služeb a projektu e-governmentu. Ten v této oblasti hlavně koordinuje bezpečnost informačních systémů orgánů veřejné správy skrze přípravu strategických a metodických dokumentů pro tuto oblast, zajišťuje spolupráce v oblasti informační a síťové bezpečnosti na evropské a mezinárodní úrovni.\(^{275}\)

2.2. Informační bezpečnost

V souvislosti s riziky e-governmentu a s ním spojeným vytvářením různých registrů státní správy a ISVS je třeba uvést také pojem informační bezpečnosti (information security). Požár jej definuje jako „obor zabývající se zabezpečením informací v informačních a komunikačních technologiích.“ Informační bezpečnost lze popsat také jako „vzájemně provázaná opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření informačních a komunikačních technologií pro zajištění dostupnosti,\(^{276}\) důvěryhodnosti\(^{277}\) a integrity\(^{278}\) informací.“\(^{279}\)

Informační bezpečnost může být vnímána také jako „odvětví zabývající se snižováním rizik vztahujících se k fenoménu informací.“\(^{280}\) Může také navrhovat řešení řídících, metodických, technických, právních i

\(^{275}\) Na evropské úrovni se jedná zejména o spolupráci s Evropskou agenturou pro síťovou a informační bezpečnost (ENISA), o které bude více uvedeno níže v kapitole 2.4. EU a její pojetí kybernetické a informační bezpečnosti. Dále se jedná o Pracovní skupinu pro informační bezpečnost a soukromí při OECD (viz Information Security and Privacy. In: OECD, http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html (19. září 2009).


\(^{277}\) Informace a s nimi spojené aktivity jsou dostupné autorizovaným uživatelům dle jejich potřeby.

\(^{278}\) Informace je dostupná pouze osobám s autorizovaným přístupem, tedy že se k nim nedostane nepovolzaná osoba.

\(^{279}\) Zabezpečení přesnosti a kompletnosti informací a metod zpracování.

\(^{280}\) POŽÁR, Josef a kol.: Základy teorie informační bezpečnosti. Praha 2007, s. 16.

jiných otázek v rámci příslušných organizací. Užší chápání pojmu se může týkat výhradně bezpečnosti informačních a komunikačních technologií.

Pokud informační bezpečnost chápejeme jako bezpečnost informací, pak ji lze definovat jako „ochranu dat organizace před neautORIZovaným přístupem nebo změnou a zajištění dostupnosti, důvěrnosti a integrity.“\textsuperscript{281} Jašek uvádí definici informační bezpečnosti coby „zodpovědnost za ochranu informací během jejích vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.\textsuperscript{282}

Informační bezpečnost je poměrně mladým oborem. Jeho počátky jsou kladeny do první poloviny 80. let, kdy se poměrně masově začaly přesouvat agendy a data všeho druhu do privátních výpočetních systémů. Ty se stávají centrem soustředění vysokých hodnot, neboť např. banky v nich vedou evidence účtů svých klientů, podniky či organizace je používají pro řízení výroby, bezpečnostní složky státu do nich ukládají data různých stupňů utajení.\textsuperscript{283} Je tedy nezbytné jak ze strany státních orgánů, tak firem formulovat strategické přístupy k informační bezpečnosti.

Vláda ČR přijala na základě svého usnesení č. 1340 v říjnu 2005 Národní strategii informační bezpečnosti ČR (NSIB). Jejím cílem bylo především „zvýšit důvěru občanů a subjektů komerční i nekomerční sféry v informační společnost, zlepšit celkové řízení informační bezpečnosti, rozvíjet znalosti o informační bezpečnosti, zlepšit mezinárodní spolupráci, shromáždit a doporučit nejlepší praxi pro oblast řízení informační bezpečnosti, zajistit základní lidská práva při používání informačních a komunikačních technologií a podporovat konkurenceschopnost české ekonomiky.\textsuperscript{284} Patrné je navazání na koncepty informační společnosti a bezpečnosti EU.\textsuperscript{285} Strategie formuluje snahy vlády ČR zavést cíle a směr informační bezpečnosti do praxe.

\textsuperscript{282} JAŠEK, Roman: c.d., s. 10.
\textsuperscript{283} Tamtéž, 9.
\textsuperscript{285} Viz níže kapitola 2.4. EU a její pojetí informační a kybernetické bezpečnosti.
Strategie vytváří společnou platformu pro zabezpečení informací veřejné správy, subjektů komerční i nekomerční sféry a jednotlivých občanů.


NSIB doplňují dvě přílohy. První se věnuje řízení informační bezpečnosti v rámci orgánů státu a veřejné správy a přiřazuje jim patřičné kompetence. K hlavním cílům rozvíjení informační bezpečnosti má být osvojení dobré praxe při zpracování informací a nastavení přiměřené základní úrovně bezpečnosti, dále pak zabezpečení vysoké úrovně informační bezpečnosti u kritických činností zaručující zpracování informací za mimořádných podmínek. Důležité je také angažování pracovníků orgánů veřejné moci k uvědomělé podpoře budování důvěryhodných informačních systémů, prosazování etického chování při užití, provozování a správě informačních a komunikačních systémů a konečně je třeba podpora aplikací nových zabezpečovacích prostředků.

Druhá příloha pak předkládá přehled právních předpisů a norem týkajících se informační bezpečnosti. Dává také doporučení pro její řízení a

---


---

286 Viz výše Kapitola 1. 2. Rozvoj e-governmentu v ČR.
289 Jsou to 1. zlepšení řízení informační bezpečnosti a řízení rizik, 2. rozvoj znalostí o informační bezpečnosti, 3. podpora národní a mezinárodní spolupráce v oblasti informační bezpečnosti, 4. podpora používání nejlepší praxe v oblasti informační bezpečnosti, 5. podpora ochrany lidských práv a svobod a 6. podpora konkurenceschopnosti české ekonomiky.
stanovuje její obecné zásady, postupy spravování a typy bezpečnostní dokumentace.\textsuperscript{292}

NSIB předpokládala také založení Výboru pro informační bezpečnost ČR, jehož účelem má být koordinace, vývoj, realizace vyhodnocování cílů NSIB. Vymezen byl také jako poradní orgán ministra informatiky. Zastoupení v něm měly mít všechno orgány státní správy nějakým způsobem zodpovědně za naplňování NSIB.\textsuperscript{293}

2.2. 1. Hrozby informační bezpečnosti

Bezpečnost informací uložených a spravovaných v daném informačním systému může být ohrožená nejen neadekvátním nakládáním s informacemi, ale také zvenčí, resp. proniknutím do informačního systému skrze škodlivý software (tzv. malware) nebo nabouráním se tedy hackingem. V této kapitole se budeme věnovat pojetí nástrojů a aspektů těchto hrozeb.

Hrozbu lze vnímat jako jakoukoli okolnost či událost působící na zranitelnou část informačního systému, která na něm může způsobit potenciální škodu. Hrozba může mít za následek poškození informačního systému nebo i organizace spravující tento systém. Hrozby mohou být náhodné nebo úmyslné, vycházet z vnějšího i vnitřního zdroje organizace a mohou mít dočasný i trvalý charakter. Hrozby lze rozdělit na objektivní\textsuperscript{294} a subjektivní.\textsuperscript{295} Dále můžeme hrozby kategorizovat dle jejich příčin.


\textsuperscript{293} Ministerstva informatiky, vnitra, obrany, školství a zdravotnictví, Národní bezpečnostní úřad, Bezpečnostní informační služba, Úřad pro zahraniční styky a informace, Policie ČR, Úřad vlády ČR, Úřad na ochranu osobních údajů, Asociace krajů ČR a Svaz měst a obcí.

\textsuperscript{294} Nezávislé na lidském faktoru. Jsou to např. přírodní katastrofy, výpadek elektrické energie, kdy je obtížné je předvídat a je tedy třeba se zaměřit na minimalizaci dopadů vhodným plánem obnovy. Dále jsou to např. elektromagnetické záření či poruchy technické a logické (porucha paměti, softwarová porucha apod.).

\textsuperscript{295} Hrozby plynoucí z lidského faktoru. Jsou to hrozby neúmyslné, způsobené prostřednictvím např. působení neškoleného uživatele systému, nebo úmyslné, subjektivní hrozby, které jsou představovány potenciální existenci vnějších útočníků (cízí zpravodajské služby, kybernetičtí
Jedná se o přerušení, kdy je některá část systému ztracena nebo nedosažitelná, či zachycení, kdy neautorizovaný subjekt získá přístup k některým datům obsaženým v informačním systému (příkladem může být odposlech telefonické konverzace či špionážní akce skrze tzv. spyware). Dalším příkladem je modifikace, tedy úmyslné změnění některých dat neautorizovanou osobou. A konečně se jedná o fabrikaci, kdy je neautorizovaně vytvořen nový, klamný objekt, o kterém uživatel nemusí vědět (např. trojský klůň). Útočník pak může provádět nekontrolované akce, které narušují informační bezpečnost počítačového systému.

Jašek uvádí kategorizaci hrozeb pro informační bezpečnost na kompromitaci, nedovolenou modifikaci hodnot, destrukci části nebo celého informačního systému zneužitím citlivých informací, použití klamných dat, špatnou interpretaci, neoprávněný přístup k hmotným (hardware) i nehmotným (data, informace) hodnotám a únik informací (kopie, krádež, odvodení apod.). V oblasti bezpečnosti státu se může jednat o narušení či ohrožení základních infrastruktur a komunikačních kanálů.

Útočníky na informační systém lze klasifikovat podobně jako typy hrozeb, tedy na vnitřní (osoba připojená do vnitřní komunikační sítě organizace, tedy současný nebo bývalý zaměstnanec), vnější (osoba, která nemá přístup k vnitřní komunikační sítě a musí překonávat její bezpečnostní aspekty). Výhodou vnějšího útočníka je jeho obtížná vystopovatelnost, neboť se díky technologii world wide web může vyskytovat kdekoli na svět. Nejnebezpečnějším útočníkem pak je „celý svět“ neboli Internet, kdy útok je veden z několika počítačů najednou (příkladem je tzv. denial-of-services, DoS). Útočníci mohou být také dle účinku svého útoku rozděleni na amatéry či náhodné útočníky, hackery, kteří usilují o proložení teroristé, hackeři, konkurenti apod.). Nicméně existují, a jsou také častější, vnitřní útisky z řad zaměstnanců organizace. Nejefektivnější je pak útok propojující vnitřní a vnitřní typy útočníků.


296 Software implementovaný do systému, aby získával a shromažďoval data za účelem průmyslové, komerční, ale také vojenské špionáže, resp. kybernetické špionáže (viz níže kapitola 2.3.3.1. Kybernetická špionáž.).

297 Hrozba plynoucí z fabrikace se vztahuje také k využití tzv. zombie počítačů. Modifikace pak je charakteristická pro tzv. defacement. (Viz níže kapitola 2.3.2. Metody kybernetických útoků)

298 JAŠEK, R.: c. d., s. 18.
bezpečnostních opatření a dostání se k neautorizovaným datům a informacím. A konečně se jedná o profesionální kybernetické zločince, kteří mají neomezený dostatek prostředků i času k provedení útoku. Často se jedná o počítačové profesionály, což odpovídá jejich znalostní kapacitě. 

2.2.2. **Metody zajištění informační bezpečnosti**

Cílem ochrany dat a informací je, jak jsme už uvedli dříve, zajistit jejich utajení, integritu a dostupnost. Některé metody počítačové bezpečnosti se zaměřují na předcházení útoku, jiné na jejich detekování.

Bezpečnosti lze obecně dosáhnout implementací určitých pravidel, postupů, procedur, organizační struktury i programových funkcí. Bezpečnostní opatření mohou být organizační i personální (např. povinnost pověřeného zaměstnance pravidelně zálohovat data, odkládat do trezoru prostředky umožňující přístup do systému apod.). Aplikovat lze také ochranu logickou, a to aplikací kryptografie nebo šifrování, či fyzickou, kdy je počítač oddělený od dostupných komunikačních prostředků a sítí. Je tak tedy zabráněno napadení celého systému virem či jiným malwarem, eventuálně hackerskému útoku, tedy nabourání se do daného systému.

Pro zajištění bezpečnosti informačních systémů je pak důležité zajistit komplexnost a provázanost jednotlivých opatření. Je nutná spolupráce informační bezpečnosti s personální, majetkovou, fyzickou i administrativní bezpečností. Zajištění bezpečnosti pak probíhá zejména prostřednictvím autorizovaného přístupu do systému, vytvářením záloh, instalací antivirových programů apod. Informační bezpečnost je tedy odpovědnost za ochranu informací při jejich vzniku, zpracování, ukládání, 

---

299 POŽÁR, J. a kol.: c. d., s. 39-41.

Motivaci útoků skrze Internet a proti informačním systémům se budeme věnovat v kapitole 2.3.1. Motivace k útokům v kybernetickém prostoru.

300 Např. v případě elektronické spisové služby je užito autorizovaného přístupu k datovým souborům a dokumentům pouze určité skupině osob s přístupovým právem. (ŠTĚDROŇ, B.: c.d., s. 90.)

301 ŠTĚDROŇ, B.: c.d., s. 43.
přenosu i likvidaci.\textsuperscript{302} Při přenosu dat se jako jediná možná a efektivní možnost ochrany dat jeví logická ochrana, tedy šifrování.\textsuperscript{303} Za použití této metody nejsou data pomocí běžných prostředků čitelná. Pro zajištění integrity je zde třeba vytvořit speciální protokol pro výměnu informací.\textsuperscript{304} Ochrana informací je možná také skrze softwarové a hardwarové kontroly.\textsuperscript{305} Hardwarová bezpečnost informačních systémů je založená na omezení, resp. umožnění přístupu do systému konkrétním osobám na základě užití identifikačních karet či biometrických systémů.\textsuperscript{306} Stěžejním aspektem ochrany informačních systémů je také již výše zmínovaná, efektivní a pochopitelná bezpečnostní politika.\textsuperscript{307} Dále lze bezpečnost informačního systému chránit také za pomocí počítačových programů, které jsou zaměřeny proti jiným aplikačním programům schopným poškodit či zcela zničit obsažená data, omezit, až vyloučit funkčnost systému či kompromitovat utajované informace.\textsuperscript{308} Jako jednoduchý příklad zde poslouží tzv. počítačové viry a antivirové programy.\textsuperscript{309} V oblasti softwarové ochrany bychom ještě rádi uvedli příklad tzv. spolehlivého softwaru. Je to takový software, kterému jeho uživatel věří a o němž je přesvědčen, že je funkčně korektní, což „vynucuje“ také u aplikací, které sám spouští. Příkladem spolehlivého softwaru je operační systém. Takový software disponuje také omezenými právy. Kontroluje a minimalizuje tak přístup k datovým fondům jiných, nespolehlivých programů. Omezuje také přístupy jednotlivých uživatelů k systému. Děje se tak hlavně skrze užití hesla.\textsuperscript{310} V souvislosti s riziky e-governmentu je třeba také uvést otázku ochrany osobních údajů. Díky modernějším a sofistikovanějším

\textsuperscript{302} POŽÁR, J. a kol.: c.d., s. 20-21.
\textsuperscript{303} Blíže k metodám šifrování viz Tamtéž, s. 43-46.; srov. POŽÁR, J.: c.d., kap. 14.
\textsuperscript{304} Příkladem může být elektronický podpis. (Viz výše kapitola 1.5.1. Elektronický podpis)
\textsuperscript{305} POŽÁR, J.: c.d., s. 119.
\textsuperscript{307} POŽÁR, J.: c.d., s. 119-120.
\textsuperscript{308} Blíže k problematice hardwarové ochrany viz Tamtéž, s. 121-129.
\textsuperscript{309} Tamtéž, s. 120.
\textsuperscript{310} Blíže viz Tamtéž, s. 136-138.

Správce osobního údajů (v tomto případě orgán státní správy) musí s těmito údaji nakládat v souladu s tímto zákonem. Ke správě mu musejí být poskytnuty pouze se souhlasem osoby, které se týkají. Bez tohoto souhlasu lze s osobními údaji pracovat jen v případě povinnostiplyňoucí ze zákona, ze smlouvy či jedná-li se o údaje zveřejněné dle zvláštních právních předpisů (např. obchodní nebo živnostenský rejstřík). Zamezit možnému zneužití osobních údajů má jejich zpracovatel.

V problematice zajištění žádoucí míry informační bezpečnosti je také využíváno praxe tzv. auditů. Auditem informačního systému rozumíme analýzu informačního systému, „jejímž cílem je posoudit, zda je systém ve shodě se stanovenými požadavky (uživatelskými, legislativními, kvalitativními, bezpečnostními, normalizačními apod.).

Audit provádí nezávislá autorizovaná osoba nebo instituce, která nemá přímou odpovědnost za funkce prověřovaného systému... (Dále se může jednat o...) záznam událostí a činností vykonaných uživatelem nebo jeho jménem, důležitých z hlediska bezpečnosti informačního systému (tzv. bezpečnostní audit). Spolu s identifikací a autentizací slouží k určení

---

311 Osobní údaje jsou informace o osobě, na jejíchž základě tuto osobu můžeme jednoznačně identifikovat. Může se jednat o rodné číslo či adresu, nepředpokládáme-li, že v daném domě nebydlí dva lidé stejného jména. (LIDÍNSKÝ, V. a kol.: c. d., s. 32)


313 LIDÍNSKÝ, V. a kol.: c. d., s. 33-34.
zodpovědnosti při vyšetřování bezpečnostních incidentů.” 314 Audit informačních systémů často provádí nezávislá instituce. Je tak využíváno služeb soukromých auditorských firem.

Podobná situace je také v oblasti zajišťování bezpečnosti ISVS. Orgány veřejné správy jsou v důsledku expertní náročnosti a kapacity nuceny najímat soukromé subjekty k zajištění informační bezpečnosti svých systémů. 315 Důvodem tzv. outsourcingu, tedy najímání externí organizace pro zajištění určité části činnosti firmy či instituce za účelem snížení nákladů, 316 jsou zejména mzdové otázky. 317 Je však třeba dbát na náležitou důvěryhodnost poskytovatele služeb informační bezpečnosti. V ČR vznikl také Český institut manažerů informační bezpečnosti, jehož cílem je zejména propagace a rozvoj odborné praxe manažerů informační bezpečnosti skrze výměnu zkušeností, pravidelná školení a publikační činnost. 318

2.3. Zneužití ICT prostředků k útokům proti státu

Útoky proti státu skrze zneužití vyspělých prostředků ICT, které postmoderní společnost současnou téměř neustále využívá, jsou vedeny v rámci tzv. kybernetického prostoru (cyberspace). Tento výraz poprvé uvedl spisovatel W. Gibson ve své knize Neuromancer v roce 1984. 319 Jeho popis kybernetického prostoru pojmenovává novou úroveň vývoje lidské

---

kultury, obchodování i technologie. Všechny tyto tři aspekty jsou zároveň spojeny v jeden. 320

Dále se nabízejí také další vysvětlení pojmu kybernetický prostor. J. Whittaker uvádí, že se jedná spíše o sérii symbolických definicí. 321 Kybernetický prostor může být vnímán jako „nefyzické prostředí tvořené propojenými počítači pracujícími v síti. V kybernetickém prostoru počítačovi uživatelé vzájemně komunikují podobnými způsoby jako v reálném světě, s jedinou výjimkou, kybernetické interakce nevyžadují fyzický pohyb, až na psaní.“ 322 Kybernetický prostor popisuje svět počítačů. 323 Základním předpokladem je telekomunikace čili komunikace na vzdálenost. 324 Gattiker pak kybernetickým prostorem rozumí „paralelní vesmír vytvořený a udržovaný počítači celého světa a komunikačními technologiemi, a který je jednoduše dosažitelný skrze počítač, kabel nebo telefonní modem připojený k systému.“ 325

Kybernetický prostor také představuje místo, kde se odehrává podstatná část lidské aktivity. 326 Lze také očekávat vzrůstající rozsah a objem lidských vztahů, ale také práce i toku peněz v rámci kybernetického prostoru. A to činí tento fenomén důležitým. Jak už jsme uvedli, v rámci kybernetického prostoru jsou aplikované prostředky ICT. Ty do určité míry přinesly společnosti novou zkušenost, virtuální svět, který je celosvětový a nezná hranic. Propojují se soukromé počítače a sítě s těmi veřejnými, vojenskými i civilními. 327

ICTs jsou v současnosti využívány v ekonomickém sektoru (např. elektronický obchod či elektronické bankovnictví), ale také ve stále větší míře ve státní správě (e-government) či vojenství. Zde elektronizace správy a komunikace nemusí znamenat jen zefektivnění a zlevnění veřejného sektoru, resp. obrany, ale také získání technologické výhody při podpoře

320 GATTIKER, Urs E.: The Internet as a Diverse Community: cultural, organizational, and political issues. Mahwah (NJ) 2001, s. 12. (http://books.google.com) (Přeloženo autorkou)
324 WHITTAKER, J.: c. d., s. 5.
326 Lidé se zde potkávají, pracují nebo si i hrají, učí se a objevují věci.
vojenských operací, sofistikovanou výzvědnou službou či skrze rychlé a spolehlivé komunikační kanály. Z vojenského hlediska znamená využití či zneužití kybernetického prostoru pro vojenský záměr či operaci možnost získání asymetrické převahy slabšího útočníka nad podstatně silnějším protihráčem. Využití kybernetického prostoru v tak širokém spektru fungování společnosti rozšířuje také možnosti, jak na i stát zaútočit a omezit je.

Důležitým aspektem použití metody kybernetického útoku je anonymita, a to díky anonymnímu charakteru moderních technologií. Je velmi komplikované až nemožné přesně určit původce konkrétního útoku v kybernetickém prostoru. Hackeri zneužívají počítače po celém světě skrze aplikaci škodlivých kódů (virů apod.). Vyšetřování kybernetického útoku pak vede většinou k těmto zneužitým počítačům (tzv. zombie počítačům). Hackeri také často využívají počítačů v zemích, které nemají příliš dobré diplomatické vztahy či možnost právního vynucení a mezinárodní spolupráce s atakovaným státem.

Využívání ICTs pro vojenské či útočné akce tak nabývá na realnosti. P. D. Allen a Ch. C. Demchak ve svém článku o izraelsko-palestinském konfliktu rozebírají čtyři fáze možné kybernetické války. Za prvé bude využito momentu překvapení a přizpůsobení. Stát bude atakovaný kvůli zranitelnosti svých webových stránek či informačních systémů, vlastněných soukromými subjekty i veřejným sektorem. Za druhé dojde k rychlé horizontální eskalaci, kdy se konflikt rozšíří do další země, tak nabývá na realistiku. P. D. Allen a Ch. C. Demchak ve svém článku o izraelsko-palestinském konfliktu rozebírají čtyři fáze možné kybernetické války. Za prvé bude využito momentu překvapení a přizpůsobení. Stát bude atakovaný kvůli zranitelnosti svých webových stránek či informačních systémů, vlastněných soukromými subjekty i veřejným sektorem. Za druhé dojde k rychlé horizontální eskalaci, kdy se konflikt rozšíří do další země,
či dokonce zemí.\textsuperscript{332} Za třetí autoři uvádějí rychlou \textit{nestátní internacionalizaci}, kdy útoky jsou často vedeny ze zahraničí individuálními kybernetickými útočníky. A za čtvrté bude docházet ke \textit{globálnímu poučení} a \textit{zintenzivnění rozvoje kybernetických zbraní}, což souvisí s velice rychlým pokrokom a rozvojem v oblasti ICTs.\textsuperscript{333}

Společnost zabývající se bezpečností sítí, Cyberoam, představuje tři kroky případné úspěšné kybernetické války. Nejprve dojde k získání \textit{kontroly nad protivníkovou sítí} s cílem zastavit, přesměrovat či znemožnit systému správně pracovat. Atakovaný pak nebude moci správně identifikovat útočníka. Za druhé bude \textit{útok veden na finanční systém} za účelem jeho zhroucení. A konečně kybernetický útočník převezme \textit{kontrolu nad národními službami} jako je energetická distribuce či telekomunikační systém. „\textit{V okamžiku, kdy je nepřítel schopen kontrolovat národní veřejné služby, finanční a komunikační systém, stát je přemožen.}“\textsuperscript{334}

Společnost Cyberoam prezentuje také podmínky úspěšného vedení kybernetického útoku. Dochází k zacílení těchto útoků na specifické „oběti“, ale také na jejich konkrétní slabá místa. Informace o zaměstnancích atakovaných entit jsou veřejně dostupné. Kybernetický útočník tak ví, komu má adresovat případný e-mail se škodlivým obsahem. Kybernetické útoky jsou také charakteristické svou krátkou životností a bleskovým vývojem v čase, což způsobuje obtíže v jejich vystopování i odhadu dalších útočníkových kroků. Zvýhodňují také spíše tyto útočníky, a to díky rychlému vývoji v technologiích. Kybernetická obrana stále ještě není dostatečně připravena k adekvátním reakcím na konkrétní kybernetické útoky.\textsuperscript{335}

V souvislosti s ohrožením státu skrze zneužití kybernetického prostoru uvádíme pojem kybernetická bezpečnost. Výše uvedená

\textsuperscript{332} V případě izraelsko-palestinského konfliktu jsou do určité míry zapojené také USA, jejichž stránky jsou napadány palestinskými hacktivisty. Izraelská strana se pak obrací na webové stránky v Libanonu či Íránu.

\textsuperscript{333} ALLEN, Patrick D. – DEMCHAK, Chris C.: \textit{The Palestinian – Israeli Cyberwar.} Military Review, březen-duben 2003, s. 54-57. (http://web.ebscohost.com)


\textsuperscript{335} Tamtéž.
informační bezpečnost je spojená s ochranou dat, informací v informačních systémech. Nicméně kybernetický útok nemusí být veden jen proti těmto systémům. Tento útok je veden za využití, resp. zneužití prostředků ICTs, tedy v kybernetickém prostoru. Může být veden proti informačním systémům, ale také proti komunikačním systémům a jiným kritickým infrastrukturám státu (např. energetická soustava, dopravní služby apod.). Kybernetickou bezpečností tedy rozumíme zajištění dostatečné bezpečnosti kybernetického prostoru a proti hrozbám v jeho rámci. Kybernetická bezpečnost může být vnímána jako rezistence vůči kybernetickým útokům.

V. Jirovský, V. Hník a O. Krulík uvádějí definici kybernetické bezpečnosti coby bezpečnostní disciplínu vztahující se na jakákoli technická zařízení pracující s daty (počítače, mobilní telefony, síťová zařízení a další hardware). EU v dokumentu eEurope 2005 kybernetickou bezpečnost vymezuje jako komunikační síť očištěné od hackerů, virů a bezpečné tak, že bude možné vybudovat důvěru zákazníků k elektronickým platbám.

2.3.1. **Motivace k útokům v kybernetickém prostoru**


V motivaci hackerů vykonávat svou činnost můžeme v průběhu času sledovat určitý vývoj. Nejprve tzv. nabourání se do systému či komunikační sítě představovalo jakýsi internetový exhibicionismus na

---

veřejnosti či alespoň v rámci hackerské komunity.339 Tato původní hackerská motivace je stále přítomná i u současných kybernetických útoků. Jde o jakousi výzvu a dokázání, že je možné to udělat. Proto je hacking spojen zejména se skupinou mladých, talentovaných uživatelů počítačů. E. Maiwald hovoří o tzv. nezacílených hackerech (untargeted hackers).340 Ti mohou být vedeni také záměrem vyjádřit svůj názor či ospravedlnit své počínání.341

Další motivací kybernetického útoku může být závist či umysl získat něčí bohatství. To se děje zejména skrze narušení důvěrnosti a neoprávněné získání přístupu do obchodních, finančních či komunikačních sítí.342 Rozvoj této motivace je možné sledovat s rozvojem využívání moderních ICTs pro komerční účely, zejména elektronické bankovnictví.

A konečně může mít hackerský útok původ v poškozujícím záměru (malicious intent) či vandalismu. Cílem je způsobit škody a ztráty. Jedná se často o tzv. zacílené hackery (targeted hackers). Jejich nebezpečí spočívá hlavně ve vyspělé technice, kterou užívají a disponují, a také v jednoznačně stanoveném cíli útoku.343 V této skupině kybernetických útočníků můžeme vidět největší riziko pro bezpečnost státu.

Kybernetické útoky proti státu mohou být také zaměřeny proti jeho ekonomickým entitám a strukturám. Jejich cílem je ale omezit či zlikvidovat infrastrukturu oběti kybernetického útoku. Motivace těchto kybernetických útoků může vycházet ze všech úrovní vývoje hackerských zájmů. Jejich míra nebezpečnosti se pohybuje od nízké úrovni tzv. defacementu přes středně ohrožující bezpečnost státu charakterizované užitím metody DoS344 dočasně paralyzující některou společnost či společnosti, část infrastruktury nebo úřad veřejné správy až

---

341 Blíže k vyjadřování názorů skrze hacking viz kapitola 2.3.3.3. Kybernetická propaganda a hacktivismus.
343 Tamtéž, s. 38.
k nejzávažnějším kybernetickým útokům proti státní ekonomice, kritické infrastruktúře či vojenským zařízením. Zde je nejčastěji užito metody distributivního DoS či škodlivého softwaru aplikovaného do napadeného informačního systému, který je schopen zničit data či systém jako celek. Útočníky mohou být nadaní individuálové, vysoce profesionalizovaní nestátní aktéři, ale také státem podporované skupiny.\[345\]

2.3.2. **Metody kybernetických útoků**

Metody pro vedení kybernetických útoků se také vyvíjejí a zlepšují. Je to spojené zejména s technologickým vývojem v kybernetickém prostoru i komunikačních aplikacích.\[346\]

Programové nástroje kybernetických útoků vycházejí v zásadě z využití tzv. škodlivého softwaru (malwaru). Jeho hlavní podoby jsou adware,\[347\] spyware,\[348\] trojské koně\[349\] a viry.\[350\] Zmínit je třeba také využití tzv. vnitřního nepřítele (insider threat). Kybernetické útoky vedené z vnitřku napadené entity, tedy například současnými nebo bývalými zaměstnanci, tvoří přibližně 55 % současných útoků proti kybernetickým sítím.\[351\]

---

348 Spyware je speciální softwarevý doplněk sloužící k tajnému zasílání uživatelových osobních dat. Původně se jednalo o nástroj využívaný v cíleném marketingu.
349 Trojští koně jsou speciální druhy počítačových virů, které jsou schopné skryt svou pravou identitu. Obvykle jsou to tzv. programy zadních vrátek, které jsou schopné spustit určitou činnost v konkrétním čase a bez vědomí regulárního uživatele.
Nejčastější technikou hacktivistů, hackerů se zájmem vyjádřit svůj postoj,352 se stal defacement, tedy změnění, odstranění nebo doplnění obsahu nebo přesměrování původní webové stránky. Význam pro určité ohrožení kybernetické bezpečnosti je u této metody v možné úpravě oficiálních informací (např. úřední deska orgánu veřejné správy), které pak mohou vést k nesprávnému postupu. V případě změnění obsahu vládních či armádních komunikačních kanálů může být následkem také nesprávně vedená obranná akce.353 Nicméně tzv. Intranet vládních i vojenských struktur je poměrně dobře chráněnou entitou a nesrovnalosti v něm je možné relativně rychle odhalit.354

Další častou metodou současných kybernetických útoků je tzv. odepření služeb (DoS) nebo také distribuovaný DoS. Server je zahlčen příliš velkým počtem žádostí o připojení, což vede k jeho kolapsu a nemožnosti správně fungovat. Útoky metodou DoS jsou vedeny pomocí tzv. botnetů neboli tisíců počítačů propojených pomocí škodlivého programu (trojský kůň apod.), které jsou na dálku kontrolovány a ovládány kybernetickým útočníkem. Jejich úkolem je opakovaně zasílat e-maily či žádat o přístup na konkrétní webovou stránku. Infikovaným počítačům se někdy také říká „zombie“ počítače, jelikož jejich běžní uživatelé nemusí o jejich účasti v kybernetickém útoku ani vědět.355

2.3.3. Příklady kybernetických útoků proti státu

Kybernetický prostor představuje širokou škálu možností a prostředků, jak ohrozit bezpečnost státu jako celku či alespoň jeho části. Metody a motivaci útoků jsme si představili v předchozích kapitolách. V této se bude věnovat třem konkrétním příkladům, jak lze skrze kybernetický prostor ohrozit integritu státu.

352 Blíže viz níže kapitola 2.3.3.3. Kybernetická propaganda a hacktivismus.
353 GEERS, K.: c. d.
2.3.3.1. Kybernetická špionáž

Kybernetická špionáž představuje rozšíření tradičního pojetí špionáže, tedy nekooperativní aktivity mezi stát, do oblasti kybernetického prostoru za využití post-moderních nástrojů ICTs. Použití Internetu „může snížit náklady a zkrátit čas sběru informací a může také zlepšit kvalitu získávaných informací.“ Dochází tak k zefektivnění práce rozvědky i kontrarozvědky.

Tak jak je výzvědná služba integrální částí bezpečnostních politik všech států, stala se i kybernetická špionáž součástí bezpečnostních přístupů post-moderních států. Zpráva o virtuální kriminologii společnosti McAfee vydaná r. 2008 odhaduje, že v kybernetické špionáži je aktivních přibližně 120 států a Čína je na vedoucí pozici. Americká CIA pak odhaduje, že státem sponzorovanou kybernetickou špionáží se zabývá 23 zemí s vedoucí pozicí Íránu, Sýrie a Indie. Information Warfare Monitor pak za lídry v oblasti kybernetické špionáže považuje USA, Velkou Británií a Izrael. Tyto země vnímají kybernetický prostor jako strategickou oblast podobně jako zemi, vzduch, moře a vesmír.

Čína coby jeden z předních představitelů v této oblasti využívá tzv. strategické kybernetické špionáže pro získávání informací o

---

357 BONI, W. – KOWACICH, G. L.: c.d., s. X.
364 Posledním velkým projevem čínské schopnosti využívat možnosti kybernetického prostoru byl špionážní atak na tibetskou komunitu odhalený na jaře 2009. (Blíže viz např. ŠTOLFOVÁ, Renata: Contemporary Security Threats within Cyberspace. NATO and EU Approaches to Cybersecurity. Maria Enzersdorf, AIES 2009. (Dosud nepublikovaný manusšript)


Malware, který se pro účely kybernetické špionáže nejčastěji používá, je spyware nebo trojíký kůň (zejména tzv. zadní vrátka, ještě jsou

---

368 Tracking GhostNet: Investigating a Cyber Espionage Network., s. 7
vytvářena spolu s oficiálním programem, aby byla později zneužita k jeho napadení).

Kybernetickou špionáž můžeme zaznamenat také v soukromém sektoru, kde se jedná zejména o tzv. průmyslovou špionáž.\textsuperscript{372} V oblasti kybernetické špionáže na osobní úrovni se jedná o tzv. phishing, kdy jsou sofistikovanou a psychologickou metodou získávána citlivá data uživatele.

\subsection*{2.3.3.2. Kybernetický terorismus}

Kybernetické útoky lze vnímat jako příklad nekonvenční a asymetricky vedené války či konfliktu. Toto uchopení kybernetických hrozb může vést k paralele s terorismem. Ucelená a obecně přijímaná definice tohoto jevu v současnosti neexistuje.\textsuperscript{373} EU nicméně usiluje o sjednocení pojetí terorismu napříč svými členskými státy. Jednotná definice by pak měla obsahovat objektivní (seznam vážných ohrožení) a subjektivní (akty považované za teroristické, úmyslně páchané s teroristickým záměrem) složky.\textsuperscript{374} OSN dosud nevyvinula žádnou definici terorismu,\textsuperscript{375} podobně jako NATO.

Někteří autoři či jiné instituce však vymezení pojmu terorismus nabízejí.\textsuperscript{376} Americké ministerstvo obrany například terorismus definuje jako „záměrné užití bezprávného násilí či hrozby s cílem vyvolat strach.“\textsuperscript{377} Jeho cílem je přesvědčit vládu či společnost následovat určité myšlenky či zájmy, které mohou být politické, náboženské i ideologické.

Pro účely této práce bychom zdůraznili vyvolání strachu a vliv na morálku obyvatelstva, který teroristický čin způsobuje. Kybernetický prostor totiž poskytuje ideální možnosti pro zneužití vysoké závislosti

\begin{itemize}
\item\textsuperscript{373} BASTL, Martin: c.d.
\item\textsuperscript{374} \textit{European Union plugging the gaps in the fight against terrorism}. In: European Commission, Justice and Home Affairs, http://ec.europa.eu/justice_home/fsj/criminal/terrorism/fsj_criminal_terrorism_en.htm (22. září 2009)
\item\textsuperscript{375} Viz \textit{There Is No UN Definition on Terrorism}. In: Eye on the UN, http://www.eyeontheun.org/facts.asp?i=1&p=61 (22. září 2009)
\item\textsuperscript{376} Viz např. BASTL, M.: c.d. Autor v tomto článku nabízí poměrně širokou škálu uchopení pojmu terorismu.
\item\textsuperscript{377} \textit{Department of Defence Dictionary of Military Terms}. Washington D.C. 2001, s. 452-453.
\end{itemize}
společnosti na ICTs a Internetu s cílem psychologicky působit na občany. Kybernetické útoky na strategické infrastruktury mohou způsobit dalekosáhlé škody srovnatelné s tradičním teroristickým útokem. Užití virtuálního světa kybernetického prostoru eliminuje riziko teroristů odhalení, ale také jejich fyzických ztrát.378

Vymezení pojmu kybernetický terorismus již tolik komplikací nezpůsobuje a jeho uchopení je předkládáno více zdroji. NATO definuje kybernetický terorismus jako „kybernetický útok užívající či zneužívající počítač nebo komunikační sítě za účelem způsobení dostatečné škody s cílem zastrašit společnost a mající ideologický podtext.“379 Americké ministerstvo vnitra uvádí vysvětlení kybernetického terorismu coby kriminálního aktu vedeného za pomocí počítače nebo telekomunikačních prostředků. Cílem je pak způsobit zmatek a nejistotu za účelem ovlivnit vládu či populace k přijetí určitých politických, ideologických či sociálních témát.380 Americká FBI pak tento jev vnímá jako „politicky motivovaný útok na informační a počítačové systémy, počítačové programy a data.“381 Centrum pro strategickú a bezpečnostnú studiu podáva vysvětlení kybernetického terorismu coby „užití nástrojů počítačové sítě s cílem vyřadit národní infrastrukturu či zastrašit vládu i civilní obyvatelstvo.“382 V případě napadení kritických infrastruktur, jako např. bank, energetické sítě apod. může způsobit ohromné ekonomické škody. Útok na obranné struktury a sítě spojený s následným fyzickým útokem pak může způsobit škody srovnatelné s válečným stavem. Kybernetický terorismus je považován za tzv. neletální typ teroristické akce.384

M. Janoušek ve svém textu rozlišuje dvě základní formy kybernetického terorismu. První je čistě propagační či informační související s vyjádřením negativního postoje či odmítavou reakcí na konkrétní mezinárodní či národní dění skrze využití možností, jež skýtá

---

379 EVERARD, P.: c.d., s. 119. (Přeloženo autorkou.)
380 Tamtéž, s. 119.
381 Tamtéž, s. 119. (Přeloženo autorkou.)
382 Webová stránka: http://www.cbss.cz/
383 EVERARD, P.: c.d., s. 119. (Přeloženo autorkou.)
384 JANOUŠEK, M.: c.d., s. 60.
kybernetický prostor.\textsuperscript{385} Daleko závažnější a nebezpečnější je pak vedení kybernetického teroristického útoku proti informačním sítím s cílem jejich likvidace. Zde se však kybernetický terorista vystavuje dalšímu riziku, kdy si de facto zničí vlastní operační prostor. Na druhou stranu však získá informační převahu a maximální informační vítězství, kdy je atakovaný dezorientovaný a nemůže reagovat na případné další útoky na jiných místech. Teroristické skupiny také mohou využívat kybernetického prostoru pro kontakt se svými členy, často lokalizovanými po celém světě.\textsuperscript{386}

2.3.3.3. Kybernetická propaganda a hacktivismus

Většina politicky motivovaných kybernetických útoků je vedena za účelem vyjádření deziluze či nesouhlasu se současným národním nebo mezinárodním děním. V tomto případě hovoříme spíše o politicky motivovaném hackování neboli hacktivismu.\textsuperscript{387} V jeho pojetí je Internet nejen prostor pro komunikaci, ale také nástroj pro akci (např. politickou).

Jeho rozmach přišel v druhé polovině 90. let minulého století, kdy za první rok skutečného hacktivismu je označován r. 1998. Od té doby začal počet kybernetických útoků významně růst.\textsuperscript{388} Je to dané mimo jiné také technologickým rozvojem i rozšířováním dostupnosti Internetu.

\textsuperscript{385} Nicméně tento jev spíše odpovídá charakteristice tzv. hacktivismu.
\textsuperscript{386} JANOUŠEK, M.: c.d., s. 61-62.

Od r. 1998 se hacktivismus rozšířil jak geograficky, tak i tematicky. Příklad vedení části konfliktu v kybernetickém prostoru je možné vidět v rámci izraelsko-palestinského konfliktu. Také během války na Balkáně v druhé polovině 90. let bylo možné sledovat aktivitu srbských hackaktivistů, kteří provedli tzv. defacement a na asi 50 různých webových stránkách se objevil vzkaz „Kosovo je Srbsko.“ V nedávné době jsme byli svědky dosud asi nejvážnějšího kybernetického útoku s prvky hacktivismu, a to v srdci evropské integrace i NATO, v Estonsku na jaře 2007.\(^{389}\)

Během bleskové války mezi Ruskem a Gruzií v srpnu 2008 bylo z ruské strany také použito nástrojů vedení kybernetického boje. Hackaktivisté morálně podporovaní ruskými oficiálními kruhy pronikli na gruzínské vládní stránky i servery některých částí důležité infrastruktury. Bylo použito zejména nástrojů defacementu, kybernetické propagandy a DoS.\(^{390}\) Je zde také možné sledovat nový trend ve vedení války, kdy jsou využívány možnosti kybernetického prostoru k podpoře klasických vojenských operací. Další novou charakteristikou vedení boje také může být zapojení civilistů, patrioticky laděných občanů vykonávajících tyto kybernetické útoky.\(^{391}\)


---


\(^{391}\) Podobnou situaci je možné sledovat v rámci palestinsko-izraelského konfliktu. Hacktivisté na obou stranách jsou podporováni k vedení kybernetických útoků (hlavně defacementu či DoS) proti druhé straně. (Viz ŠTOLFOVÁ, R.: c.d.)
Hacktivismus můžeme vztáhnout k fenoménu tzv. kybernetické propagandy, tedy rozšíření tradičního jevu propagandy do kybernetického prostoru. Kybernetická propaganda se stala součástí současných konfliktů podobně, jako se její klasická předchůdkyně zapojila do konfliktů a válek v průběhu historie. Jako nástroj ovlivňování protivníkovy morálky je užíváno post-moderních nástrojů komunikace široce rozšířených v populaci. Internet nabízí poměrně rychlou a levnou možnost jak šířit názory a působit na širokou skupinu lidí. Dopad propagandy může být různý, od jednoduchého vyjádření postoje bez zásadnější reakce veřejnosti k významným socio-politickým posunům.392

2.4. EU a její pojetí kybernetické a informační bezpečnosti

Zájem EU v rámci informační, resp. kybernetické bezpečnosti byl vždy spojený s obchodními a finančními aspecty. Společenství se zaměřilo na fenomén tzv. informační společnosti393 a její podporu a ochranu. Informační společnost je v EU vnímána jako důsledek jednotného trhu, harmonizace standardů a liberalizace telekomunikací.394 EU se tak zaměřuje na zabezpečení komunikačních sítí spojených s nejčastějšími elektronickými styky současnosti v běžné populaci, tedy elektronické bankovnictví, elektronické obchodování, ale také e-government apod. Cílem je pak zejména předcházet velkým finančním ztrátám spojených s případnými kybernetickými útoky na tyto komunikační kanály.395

EU je na mezinárodním poli považována za klíčovou entitu v oblasti kybernetické bezpečnosti. Souvisí to s její přední pozici světového ekonomického hráče a v současnosti se rozvíjejících elektronických transakcí, jež se stávají významnou charakteristikou ekonomického rozvoje post-moderní společnosti. Ve své pravomoci podporuje výzkum hodnotící

392 Např. situace na americké politické scéně po zveřejnění obrázků z věznice Abu Ghrajb).
393 Informační společnost je charakterizovaná vytvářením, využitím, distribucí a manipulací s informacemi coby nejvýznamnější ekonomickou, politickou a kulturní aktivitou. Základními nástroji informační společnosti jsou počítače a telekomunikační prostředky, tedy ICTs.
různé aspekty jakési informační revoluce posledních let a její dopad na současnou společnost, vzdělanost, obchodování i komunikaci.396

Výzkum v oblasti ICTs je také vnímán jako jeden z hlavních faktorů pro zajištění dostatečné míry kybernetické bezpečnosti. Výzkumem pro Komisi EU se zabývá jedno z jejích DG s názvem Joint Research Centre. To se v současnosti zaměřuje na poskytování vědecké i technické podpory pro vytváření koncepcí, zavádění a sledování konkrétních politik EU.397 Spolu s přijetím konceptu informační či znalostní společnosti se tento fenomén stal také jednou z pracovních oblastí tohoto výzkumného centra, konkrétně jeho Institutu pro ochranu a bezpečnost občanů.398

Po teroristických útocích z 11. září 2001 si nejen EU intenzivněji uvědomila potřebu dostatečného zabezpečení tzv. kritických infrastruktur (energetické sítě, telekomunikace, finanční sektor apod.). Direktiva Evropské rady o určení a tvorbě evropské kritické infrastruktury z r. 2006 identifikuje oblast ICT jako jednu z částí těoho infrastruktur.399 V březnu 2009 Komise navrhla přijetí politiky týkající se ochrany kritických informačních infrastruktur. Návrh zdůrazňuje principy prevence, připravenosti a uvědomění si rizik. Stanovuje také plán okamžitých akcí k posílení bezpečnosti a odolnosti kritických informačních infrastruktur.400

Dokument Komise předkládá pět pilířů řešení bezpečnosti kritických informačních infrastruktur. Nejprve se jedná o připravenost a prevenci, tedy určení míry schopnosti národních týmů reakce na počítačovou pohotovost (Computer Emergency Response Teams, CERTs) a vytvoření jakéhosi evropského partnerství mezi veřejným a soukromým sektorem a fóra pro členské státy ke sdílení informací a tzv. dobrých praktik. Druhým pilířem je náležitá detekce a reakce, tedy vytvoření přiměřeného mechanismu včasného varování. Třetím základem kybernetické bezpečnosti má být zmírňování a obnova skrze posilování obranných mechanismů EU v oblasti kritických informačních infrastruktur. Předposledním krokem je podpora mezinárodní spolupráce mezi členy EU i vně. A konečně mají být stanovena kritéria pro odvětví kritických informačních infrastruktur.401

Na přelomu milénia jsme mohli být svědky několika iniciativ EU zaměřených na využití ICTs pro rozvoj evropské společnosti i ekonomické síly. Jednalo se o iniciativy nesoucí název eEurope.402 Otázkám kybernetické bezpečnosti se věnovala eEurope 2005 z června 2002. Tato iniciativa mimo jiné také navrhovala zřízení jednotek pro kybernetickou bezpečnost (Cyber Security Task Force), které by byly podporovány jak veřejným, tak také soukromým sektorem, tedy firmami.

Je zde také uvedena myšlenka „kultury kybernetické bezpečnosti“.403 Všichni, kteří využívají možnosti kybernetického prostoru, si mají uvědomit rizika plynoucí z užívání tohoto média. Je třeba přijmout jakýsi závazek zodpovědnosti. Iniciativa se obrací na soukromé firmy a společnosti s významným ekonomickým vlivem ve státech, aby se podílely na vytvoření pravidel dobré praxe v užívání ICTs. Nicméně pozornost je věnována také jednotlivcům, občanům, kdy jejich uvědomění si hrozí nejenom z různých dalších projektů EU.

---

401 Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o ochraně kritické informační infrastruktury. Ochrana Evropy před rozsáhlými počítačovými útoky a narušení: zvýšujeme připravenost, bezpečnost a odolnost., s. 7-11.
Současným podkladem přístupu Společenství k informační společnosti i kybernetické bezpečnosti je iniciativa i2010. Ta se coby součást Lisabonské strategie zaměřuje zejména na ekonomický růst plynoucí z rozmanitějšího využívání ICTs. Otázky kybernetické bezpečnosti jsou v dokumentu zmíněny spíše okrajově. Samozřejmě povědomí o rizicích plynoucích z možného zneužití post-moderních ICTs bylo přítomno. Nicméně pozitivní aspekty jejich zapojování převázaly. EU v dokumentu spíše přistupuje k doporučení členským státům přijímat ochranné prostředky a podmínky zabezpečení svých komunikačních sítí. Je zde opět zdůrazněna spolupráce a sdílení zkušeností v oblasti kybernetické bezpečnosti.

i2010 zmiňuje bezpečnost konkrétněji v pasáži o jednotném evropském informačním prostoru. Cílem je posílit a podpořit bezpečnou a spolehlivou internetovou komunikaci, a zvýšit tak důvěru mezi investory, společnostmi a zákazníky. i2010 také navrhla, aby Komise vypracovala Strategii pro bezpečnou informační společnost s důrazem na růst obeznámenosti veřejnosti o možných kybernetických hrozbách a přístupu k nim.


Je to vzrůstající finanční motivace kybernetických útočníků, tedy zcízení citlivý dat pro neoprávněné finanční obohacení (např. phishing, spyware apod.). Rozšířenější používání mobilních komunikačních prostředků (zejména mobilních telefonů využívajících technologii 3G) bude znamenat rozšíření možností kybernetických útoků i proti nim. Nástroje ICT se staly nedělitelnou součástí evropského ekonomického rozvoje, stejně jako podmínkou správného fungování klíčových

---


Do posilování bezpečnosti informační společnosti se pak musí zapojit tyto skupiny – veřejná správa, společnosti i soukromé osoby. Veřejné orgány se mají zaměřit zejména na své informační systémy a jejich zabezpečení. Nejen pro zajištění celkové bezpečnosti, ale sloužit tak také jako příklad dobré praxe. Soukromé firmy mají přijmout bezpečnost svých sítí a komunikačních sítí jako pozitivní jev a kompetitivní výhodu. A konečně individuální uživatelé mají pochopit, že jejich soukromá komunikační síť je součástí jakéhosi globálního řetězce, nebo spíše sítě, kde jsou rizika sdílena. Opět je zdůrazněna myšlenka vytvoření obecné kultury kybernetické bezpečnosti. Úspěch strategie pak má být zaručen dialogem, partnerstvím a posílením patřičných nástrojů mezi všemi zúčastněnými stranami.\footnote{Tamtéž, s. 4-6.}


V r. 2004 EU zřídila Evropskou agenturu pro síťovou a informační bezpečnost (European Network and Information Security Agency, ENISA). Skrze toto těleso chce EU prosazovat celoevropskou spolupráci v oblasti informační bezpečnosti mezi státy i soukromým sektorem. Slouží jako
nezávislé expertní středisko pro ostatní orgány EU. Asistenci však poskytuje také členským státům, občanům, zákazníkům, soukromým firmám i veřejné správě.

ENISA je pověřena čtyřmi hlavními úkoly. Zaprvé je to poradní a asistenční služba Komisi a členským státům v oblasti zabezpečení sítí a informačních systémů a také v jejich dialogu se soukromým sektorem. Zadruhé ENISA sbírá a analyzuje data o bezpečnostních incidentech v Evropě. Dále poskytuje zhodnocení bezpečnostního rizika a možnosti jeho zvládnutí za účelem zajistit schopnost EU čelit kybernetickým hrozbám. A konečně přispívá k rozšiřování povědomí a prohlubování spolupráce mezi všemi hráči zainteresovanými v informační a kybernetické bezpečnosti. ENISA plní roli jakéhosi poradního vyjednávace (Advice Broker).

Dalšími úkoly ENISA je např. koordinace a zlepšení spolupráce mezi jednotlivými národními CERTs, stejně jako podpora jejich fungování.


410 Např. Komisi poskytuje technický základ pro vyvíjení či revizi komunitní legislativy v oblasti informační bezpečnosti.
413 Během gruzínsko-ruské války v srpnu 2008 byla využita také metoda tzv. hacktivismu, kdy pro-ruští hacktivisté využili defacement a DoS při kybernetických útocích na některé gruzínské webové stránky a servery (zejména oficiální vládní stránky, mediální servery apod.). (Viz kapitola 2.3.3.3 Kybernetická propaganda a hacktivismus)
komplexního přístupu EU k těmto výzvám. Opět je zdůrazněno rozšiřování povědomí o kybernetických rizicích a mezinárodní spolupráce.415

EU jako celek si uvědomuje potřebu dále prohlušovat koordinaci národních přístupů ke kybernetické bezpečnosti. Členské státy jsou zodpovědné za vytváření vlastních politik pro zabezpečení kritických informačních infrastruktur.416

V souvislosti s postupným vypršením platnosti iniciativy i2010 současné švédské předsednictví EU417 vydalo v září 2009 dokument s názvem Zelená vzdělanostní společnost (A Green Knowledge Society). Stěžejní myšlenkou je zde podpora vytvoření tzv. vědomostní společnosti418 skrze využívání soudobých ICTs. Dokument reviduje předešlou iniciativu a poukazuje na nové výzvy a rizika bezpečného digitálního světa současnosti. Důraz je pak kladen opět na ochranu kritických infrastruktur, růst povědomí veřejnosti o rizicích a spolupráci v rámci EU.419

V dubnu 2009 komisařka V. Reding navrhla vytvoření orgánu EU pro kybernetickou bezpečnost a obranu. V jejím pojetí je ENISA spíše „agenturou pro výměnu informací“, ale ve světle nedávných i možných budoucích kybernetických útoců je potřeba nové evropské entity, která by koordinovala postupy různých skupin a vyvinula konkrétní strategii pro boj s kybernetickými hrozbami současnosti.420 Reding také zdůrazňuje význam preventivních úkonů v rámci zajištění dostatečné bezpečnosti kybernetických sítí činěných v jednotlivých členských státech na určité jednotné rovině.

418 Vědomostní společnost můžeme popsát jako společnost, kde vzdělanost je základním zdrojem rozvoje.
ZÁVĚR

V uplynulých letech jsme zaznamenali ohromné změny a pokrok ve vývoji informačních a komunikačních prostředků. Tyto ICTs se staly našimi každodenními společníky a také nepostradatelnými doplňky pro mnoho našich aktivit. Rozšířily způsoby, jak můžeme obchodovat, podnikat, být v kontaktu se svými blízkými či ovládat své finance. Moderní ICTs také otevírají nové možnosti kontaktu státní správy s občany. V demokratických společnostech můžeme pozorovat úsilí o vstřícnost a otevřenost vůči občanovi. Veřejná správa se tak snaží do určité míry usnadnit nezbytný kontakt občanů s úřady. E-government coby elektronizovaná státní správa pak může znamenat významný příspěvek k tomuto úsilí.

E-government lze vnímat nejen jako elektronickou správu, kdy dochází k zavádění post-moderních ICTs do fungování veřejné správy, ale také jako správu efektivní. Sofistikované ICTs totiž mohou ulehčit přístup občana k úřadu, ale také zpřehlednit a zjednodušit komunikaci mezi jednotlivými složkami státní moci. Vytváření centrálních registrů má vést k odstranění duplicit i omezení schraňování příliš velkého objemu dat o jednotlivých občanech, často vícekrát v databázích různých úřadů.

Internet coby v rámci praktického e-governmentu nejvyužívanější podoba současných ICTs umožňuje téměř nepřetržitý přístup občanů k informacím. Ti pak nejsou nuceni docházet na úřady příliš často, mohou svůj volný čas rozvrhnout jinak, což nemalou měrou může přispět k zlepšení jejich postoje vůči státní moci. E-government může z podobného důvodu přispět také ke zvýšení vztahů s firmami nezbytnými pro ekonomický rozvoj země.

V ČR je možné sledovat snahu o zavedení nástrojů e-governmentu od počátku 90. let minulého století, kdy konec totalitního režimu znamenalo také určité volání po otevřenosti státní správy a větší vstřícnosti vůči občanovi. Nicméně poslední dekáda 20. století větší pokrok v oblasti elektronizace veřejné správy nepřinesla, a to zejména z důvodu nejednotnosti postoje jednotlivých orgánů státní moci k aplikaci e-governmentu. Bylo také třeba přijmout příslušnou právní úpravu, která by umožňovala jeho rozvoj skrze vytváření a správy patřičných registrů.
Pomalý rozvoj e-governmentu je třeba také přičíst nedostatečné počítačové gramotnosti i určité nedůvěře úředníků i občanů k využívání postmoderních ICTs. Tyto problémy jsou provázané a orgány centrální správy se snaží překonávat různými projekty a programy (např. Národní projekt počítačové gramotnosti apod.). Změna a výraznější posuny nastaly až na přelomu století, resp. v prvních letech 21. století.

Přesto byly od poloviny 90. let spouštěny projekty zlepšující přístup občanů k informacím skrze využití ICTs, zejména tedy Internetu. Jednalo se o portály ePusa, Elektronická a vlídná administrativa (EVA) či Portál veřejné správy ČR. V r. 1999 byl přijat strategický dokument s názvem Státní informační politika – cesta k informační společnosti, jehož hlavním cílem bylo zkvalitnění a lepší zpřístupnění vzájemné komunikace mezi státní správou a občany. O rok později pak byl zřízen Úřad pro informační systémy veřejné správy ČR. V r. 1999 byl přijat strategický dokument s názvem Státní informační politika – cesta k informační společnosti, jehož hlavním cílem bylo zkvalitnění a lepší zpřístupnění vzájemné komunikace mezi státní správou a občany. O rok později pak byl zřízen Úřad pro informační systémy veřejné správy, jež měl zajišťovat naplňování Státní informační politiky a měl koordinovat vytváření a působení soustavy informačních systémů státní správy. Jeho fungování pak bylo nahrazeno v rámci působnosti Ministerstva informatiky, které však bylo později také zrušeno a jeho kompetence v oblasti e-governmentu přešly r. 2007 do rukou Ministerstva vnitra. Otázky rozvíjení a podpory informační společnosti byly převedeny na Radu pro rozvoj informační společnosti se statutem poradního orgánu vlády.


Byl spuštěn projekt CzechPOINT, kdy občan získal možnost přístupu k různým registrům jako je obchodní rejstřík, trestní rejstřík a podobně, možnost ověřit dokumenty a listiny či sledovat průběh správního řízení, stejně jako dát podnět k jeho zahájení z jednoho kontaktního místa. V nedávné době byl do plného provozu uveden systém tzv. datových
schránek, jež lze s určitou mírou nadsázky označit za revoluci v komunikaci mezi občany a veřejnou správou. Usnadňuje se tím elektronické podávání a doručování, které sice bylo umožněno již dříve prostřednictvím tzv. elektronických podatelen. Nicméně využití této možnosti doručování a podání nebylo plně využíváno v souladu s jeho záměrem, a to zejména kvůli určité nejasnosti, často až nesrozumitelnosti a také nejednotnosti v přístupu napříč veřejnou správou.

První týdny po spuštění ostrého provozu datových schránek nás vedou k v zásadě optimistickému pohledu na tento projekt. Roste počet aktivovaných datových schránek i odeslaných datových zpráv. Úspěšnost jejich doručování se pohybuje kolem 90 %. Jako jednoznačně pozitivní jev vnímáme narůstající zájem o zřízení datové schránky ze strany občanů, jež k tomuto nemají zákonnou povinnost. Právě na ně by se v souvislosti s úspěšným rozvíjením e-governmentu v ČR orgány státní správy měly zaměřit a tuto možnost komunikace s veřejnou mocí jim co nejvíce zpřístupnit, např. dostatečným internetovým připojením či náležitou propagační a informační kampaní.

V souvislosti s elektronickým podáním a komunikací je třeba také zmínit institut elektronického podpisu. Ten představoval jeden z prvních praktických nástrojů, jak elektronicky komunikovat nejen se státní správou. Nicméně jeho využití v ČR neodpovídá jeho potenciálu, což pramení z jeho charakteristiky omezené platnosti i ze skutečnosti, že vytvoření podkladů jeho náležitého užívání (zejména vytvoření potřebných certifikátů) je zpoplatněno. Z hlediska občana jako jedince se tak disponování elektronickým podpisem jeví jako neefektivní. Omezené využívání elektronického podpisu pak také souvisí s limitovaným využíváním elektronických podatelen.

Následující r. 2010 má být ve znamení realizace výstavby základních registrů státní správy. Jejich záměrem je vytvoření jednotného systému spravování dat veřejné správy ve čtyřech registrech, kdy se má zabránit zejména jejich duplikování. Tyto databáze budou zároveň spolupracovat, takže nebude třeba ze strany občana uvádět stejně informace na různých úřadech. Provázanost těchto registrů se systémem
datových schránek pak také umožní kontrolu občana, kdy a za jakým účelem bylo nakládáno s jeho údaji, které jsou v nich vedeny.

Při sledování zrychleného vývoje a přístupů k zavádění nástrojů e-governmentu v českém prostředí nemůžeme přehlédnout určitou korelací s vývojem postojů k informační společnosti v rámci EU. Ta uznala ICTs jako hnací sílu svého ekonomického rozvoje na přelomu tisíciletí. Evropská informační společnost je vnímána jako důsledek jednotného trhu, harmonizace pravidel a liberalizace komunikačního trhu. V jejím rámci jsou zdůrazněny informace a potřeba jejich získávání i sdílení, stejně jako jejich ochrany pro rozvoj společnosti.

V rámci víry v ICTs coby základu rozvoje přijalo Společenství několik strategií a iniciativ podporující rozšiření využívání těchto prostředků veřejnosti. Byly vydány dokumenty eEurope zaměřené na dostatečné rozšíření Internetu a jeho využívání v EU, ale také v kandidátských zemích. V r. 2005 pak byla přijata iniciativa i2010, která je součástí tzv. Lisabonské strategie a která se zaměřila na zapojení co největšího počtu obyvatelstva do využívání post-moderních ICTs, zejména Internetu v ekonomické oblasti, ale také v komunikaci s veřejnou správou. Součástí též iniciativ byla podpora politik a postupů rozšiřování možností e-governmentu v členských, resp. kandidátských zemích EU.

Působení Společenství na své členy skrze výše uvedené strategické dokumenty je motivováno ideou, že evropský prostor a trh je společný pro všechny členské státy a rozvoj služeb v rámci tohoto prostoru nemá znát hranice. V tomto smyslu je zdůrazňován zejména ekonomický aspekt, tedy využívání možností elektronického nakupování či bankovnictví. Nezanedbatelný je také záměr EU zkvalitňovat životy svých „občanů“, a to v tomto ohledu skrze zlepšení fungování státní správy i komunikace s ní. Elektronizace státní správy tak má v rámci EU velkou podporu.

ČR tak svým vstupem do EU dostala jedinečnou možnost jak realizovat své plány v oblasti rozvoje e-governmentu za finanční pomoci strukturálních i komunitárních fondů Společenství. Řada projektů týkajících se efektivizace a elektronizace veřejné správy a jejího přiblížení se občanům je prováděna za výrazné podpory finančních zdrojů EU.

Zavádění prostředků e-governmentu je integrálně spjato s vytvářením informačních systémů obsahujících ohromná kvanta dat s různým stupněm citlivosti a utajení. Tato data je třeba chránit před jejich zneužitím, tedy je třeba zajistit dostatečnou informační bezpečnost těchto systémů. E-government tedy v zásadě představuje pozitivní využití ICTs, resp. kybernetického prostoru. Nicméně je třeba si uvědomit také rizika, jež jsou s aplikací těchto prostředků spojena.

Možnosti jak ohrozit informační bezpečnost, tedy snížit důvěryhodnost, integritu a dostupnost informací spravovaných v daném systému jsou různé. Mohou být fyzického charakteru, kdy médium nesoucí na sobě uložené informace může být fyzicky zničeno, ale také technického, kdy je kupříkladu systém infiltrován tzv. hackingem.

Tento text předložil některé přístupy k zajištění informační bezpečnosti v praxi i z teoretického hlediska. ČR od r. 2005 disponuje svou Národní strategií informační bezpečnosti, jež vytváří společnou platformu pro zabezpečení informací a dat veřejné správy, ale také subjektů komerční i nekomerční sféry a jednotlivých občanů. Zákon o informačních systémech veřejné správy uvádí, že za bezpečnost těchto systémů je zodpovědný jejich provozovatel, který také přijímá patřičnou bezpečnostní politiku.

Záměrem naší práce bylo, mimo jiné, poukázat na možnost zneužití ICTs proti státu a jeho integritě. Nejde tedy jen o ohrožení dat a informací vedených v informačních systémech veřejné správy, ale také o možnost zneužití určitou závislost současné společnosti na ICTs. Ty, jak už jsme uvedli, jsou nedělitelnou součástí mnoha aktivit soukromého, veřejného i obchodního života post-moderní společnosti. V rámci efektivizace státní správy jednotlivé její složky, a to včetně těch vojenských a obranných, mezi sebou komunikují skrze sofistikované komunikační


Nejčastěji dochází k jakémus politickému aktivismu skrze využití možností kybernetického prostoru, tedy k tzv. hacktivismu. V jeho rámci se útočník snaží vyjádřit svůj názor a postoj. Využívá různé prostředky a metody (hlavně Internetu), jak svoje vnímání situace rozšířit v co největším prostoru. Nejčastější technikou hackivistů je pak defacement, kdy jsou oficiální stránky státní správy, ale také politických stran či firem a médií obsahově změněny či přesměrovány na jiný server.

Tato podoba kybernetických útoků v zásadě nepatří k nejzávažnějším. Nicméně může souviset s kybernetickou propagandou, a tím nežádoucně působit na morálku obyvatel. Internet také umožňuje přístup do širokého okruhu domácností, a tím pádem možnost ovlivnit vnímání či postoje velkého počtu lidí.

Kybernetický terorismus je vnímán jako extenze klasického terorismu do prostředí kybernetického prostoru, resp. s využitím postmoderních ICTs. Cílem těchto kybernetických útoků se tak stávají kritické infrastruktury států, což může mít zásadní vliv na morální vystačení obyvatelstva, ale také na zajištění jeho správného fungování. V současnosti, kdy teroristické skupiny spíše představují globální sítě, pak kybernetický prostor dává možnost snadnější komunikace mezi jednotlivými členy i koordinace případných teroristických útoků. Nebezpečnost metody kybernetického terorismu je pak závislá na technologické vybavenosti a zručnosti dané teroristické skupiny.


Estonský případ představuje první příklad dočasné paralyzy země, kdy série koordinovaných kybernetických útoků proti kritickým infrastrukturám znamenala významné omezení náležitýho fungování země. Tato zkušenost otevřela debatu o možné kybernetické válce, nicméně incident samotný představuje spíše příklad tzv. hacktivismu, kdy se jednalo spíše o vyjádření nesouhlasu ruské populace žijící v Estonsku a pro-ruských aktivistů (hacktivistů) v zahraničí s přemístěním pomníku Rudé armády z centra Tallinnu. Kybernetické útoky byly ukončeny po několika dnech, resp. týdnech. Nebyly také spojeny s dalším vojenským či bezpečnost ohrožujícím aktem.

Závažnost estonského kybernetického zásahu však spočívá v tom, že stát jako entita přestal načas správně fungovat a nemohl zajistit svým občanům služby, které jim z jeho strany náleží. Možnost kybernetické války a otázky kybernetické bezpečnosti se tak staly součástí debat o současných bezpečnostních hrozbách v rámci vojensko- obranného, politického, ale i vědeckého obce. Přijímání strategií ohledně zajištění dostatečné kybernetické bezpečnosti, tedy zajištění vlastního kybernetického prostoru proti jeho zneužití či napadení, tak získalo na důležitosti. Nejde již jen o
zajištění bezpečnosti informací, ale o zamezení zneužití ICTs proti bezpečnosti státu a jeho občanů.

Příklad gruzínsko-ruské války a zapojení pro-rusky orientovaných hackaktivistů pak představuje možnou novou strategii ve vedení války. U konfliktů současnosti můžeme očekávat, že alespoň některá z jejich částí bude vedena v kybernetickém prostoru, který pak mimo jiné umožňuje zapojení individuálních aktivistů vedených patriotismickým postojem k podpoře vojenské operace své země.

EU se v otázce kybernetické bezpečnosti tradičně zaměřuje na její finanční aspekty a dopady. Vnímání ICTs a jejich využívání k obchodování coby pozitivní příspěvek do evropského ekonomického rozvoje vede k podpoře posilování kybernetických prostorů proti zneužití zejména v oblasti tzv. kybernetické kriminality. Ve svém působení se zaměřuje na vytvoření jakési obecné kultury kybernetické bezpečnosti, kdy si jak státy, tak soukromé subjekty, firmy i individuální uživatele ICTs uvědomí vzájemnou propojenost v rámci kybernetického prostoru napříč těmito sektory a že tento prostor není omezen hranicemi států.


Kybernetické útoky na Estonsko, pak byly jedním ze stěžejních důvodů vedoucích k přehodnocení globálních bezpečnostních hrozb ze strany EU a kybernetická bezpečnost se stala součástí seznamu současných bezpečnostních výzev, kterým Evropa čelí. To potvrdila Zpráva o implementaci Evropské bezpečnostní strategie vydaná v prosinci 2008, která také poukazuje na to, že tato oblast a přístup k ní potřebuje další rozvoj a práci. Komisařka pro média a informační společnost V. Reding pak na jaře 2009 uvedla, že současná bezpečnostní situace v rámci
kybernetického prostoru potřebuje přijetí jednotného postupu a založení jakéhosi exekutivního orgánu v rámci EU, který by se věnoval zajišťování kybernetické bezpečnosti ve Společenství.


S určitou zvědavostí pak můžeme pozorovat další vývoj přístupu EU ke kybernetické bezpečnosti své i svých členských států v souvislosti s prohlášením komisařky V. Reding z jara 2009. Postoj NATO coby vojensko-obranné entity k otázkám kybernetické bezpečnosti jsme do této práce již nezahrnuli. Nicméně věnovali jsme se již dříve ve studii o kybernetické bezpečnosti a přístupech NATO a EU.421 V této diplomové práci jsme chtěli zmapovat zejména pozici EU a její působení na rozvoj politik a strategií týkajících se rozvoje ICTs i jejich neúžitelnosti v jejích členských státech, ale také v rámci mezinárodní spolupráce. Postoj EU jako mezinárodního tělesa k otázkám informační a kybernetické bezpečnosti nás zajímal také z důvodu její do jisté míry v současnosti teprve se rodící obranně-bezpečnostní identity. Dalšímu bádání tak tedy přenecháváme budoucí strategické přístupy EU k problematice kybernetické bezpečnosti.


421 ŠTOLFOVÁ, R.: c.d.
ANOTACE

Autor: Bc. Renata Štolfová
Název katedry a fakulty: Katedra politologie a evropských studií
Filozofická fakulta Univerzity Palackého v Olomouci
Název práce: E-government a rizika plynoucí z využívání současných ICTs ve státní správě. Rozvoj e-governmentu v ČR. Informační a kybernetická bezpečnost aneb Je třeba se obávat kybernetické války?
Vedoucí práce: Mgr. Eva Lebedová
Počet znaků: 139 283
Počet titulů použitých pramenů a literatury: 252
Klíčová slova: e-government, elektronický podpis, elektronické doručování a podání, CzechPOINT, datové schránky, informační bezpečnost, kybernetická bezpečnost, kybernetické útoky, Česká republika, Evropská unie.
ANNOTATION

Author: Bc. Renata Štolfová

Submitted at: Department of Politics and European Studies
Philosophical Faculty, Palacky University Olomouc

Entitled: E-government and Its Risks Concerning Contemporary ICTs Use within the Public Administration. Development of E-government in the Czech Republic. Information and Cyber Security – Shall We Be Afraid of Cyberwar?

Supervised by: Mgr. Eva Lebedová

Word count: 139 283

Number of references: 252

Key words: e-government, electronic signature, electronic delivering and administrative action, CzechPOINT, data mail boxes, information security, cyber security, cyber attacks, Czech Republic, European Union.

Short description: The work is focused on e-government development in the Czech Republic from the beginning of 1990s. It follows the influence of EU on an intensification of e-government development within the Czech public administration in mid-2000s due to Community´ s financial and moral support. The second part of the study is dedicated to information and cyber security. A wide range of ICTs use opens other opportunities how to attack society and state. Examples of ICTs misuse lead to accepting the cyber threats as real contemporary strategic and security challenges.
Prameny a literatura

Prameny


Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. In:


Literatura


BARBER, Richard: *Hacking Techniques. The tools that hackers use, and how they are evolving to become more sophisticated*. Computer. Fraud and Security. 1. března 2003, č. 3, s. 9-12. (http://web.ebscohost.com)


GATTIKER, Urs E.: The Internet as a Diverse Community: cultural, organizational, and political issues. Mahwah (NJ), Lawrence Erlbaum 2001. (http://books.google.com)


Information Security and Privacy. In: Organisation for Economic Cooperation and Development (OECD), http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1_1_00.html (19. září 2009).


JIROVSKÝ, Václav – HNÍK, Václav – KRULÍK, Oldřich: Základní definice, vztahující se k tématu kybernetických hrozeb. In: Ministerstvo vnitra ČR,


POŽÁR, Josef a kol.: Základy teorie informační bezpečnosti. Praha, Vydavatelství Policejní akademie ČR 2007


**Social inclusion, better public services and quality of life.** In: European Commission, Europe’s Information Society,
Strategie rozvoje služeb pro informační společnost. In: businessinfo.cz,

Světové počítače v září nejvíce trápil červ Conficker, ty naše reklamní software.


ŠTOLFOVÁ, Renata: Contemporary Security Threats within Cyberspace. NATO and EU Approaches to Cybersecurity. Maria Enzersdorf, AIES 2009.

The e-government imperative: main findings. In: Organisation for Economic Cooperation and Development (OECD), Policy Brief, březen 2003,

The „Lisbon Strategy“ in Short. In: Výbor regionů,

There Is No UN Definition on Terrorism. In: Eye on the UN,

Tracking GhostNet: Investigating a Cyber Espionage Network. In: F-Secure,

TUŠEROVÁ, Lenka: E-government a jeho projevy v českém právu. Právnická fakulta Masarykovy univerzity,


Internetové odkazy

Administrativní registr ekonomických subjektů:
http://wwwinfo.mfcr.cz/ares/ares.html

Critical Information Infrastructure Research Co-ordination Project:
http://www.ci2rco.org

Český institut Manaţerů informační bezpečnosti: http://www.cimib.cz

CzechPOINT: www.czechpoint.cz

Datové schránky: http://www.datoveschranky.info

Egoncentrum: http://egoncentrum.cz/

eIdentity, a. s.: http://www.eidentity.cz/

Elektronická vlídná administrativa: http://www.naseeva.cz/

Evropská informační společnost: http://ec.europa.eu/information_society/


ePusa: http://www.epusa.cz/

Federace amerických vědců (FAS): http://www.fas.org/


Informační systémy veřejné správy: http://www.isvs.cz/

Information Warfare Monitor: http://www.infowar-monitor.net/

Integrovaný operační program: http://www.strukturalni-fondy.cz/getdoc/ae5865d4-be4a-403d-9461-7ee797397a20/Integrovany-operačni-program


Komisařka Reding:
http://ec.europa.eu/commission_barroso/reding/index_en.htm

Land Parcel Information System: http://www.lpis.cz/

Ministerstvo vnitra ČR: http://www.mvcr.cz
Operační program lidské zdroje a zaměstnanost: http://www.strukturalni-fondy.cz/getdoc/d26c8d6a-821b-45df-9c9c-29a8a55f7e1e/OP-Lidske-zdroje-a-zamestnanost

Portál Evropské unie: http://europa.eu
PostSignum OCA (Česká pošta, s. p.): https://qca.postsignum.cz/
PrimeLife: http://www.primelife.eu
První certifikační autorita, a.s.: http://www.ica.cz/
Sagit: http://www.sagit.cz
Senát Parlamentu České republiky: http://www.senat.cz/
Veřejná správa online: http://www.mool.cz
Vláda České republiky: http://www.vlada.cz/
ABSTRAKT

Inspirací pro napsání této diplomové práce byly kybernetické útoky na Estonsko na jaře 2007, jež způsobily dočasnou paralýzu země, a stát nemohl poskytovat náležité služby svým občanům. Tato pobaltíská republika je známá svou vyspělou aplikací post-moderních ICTs do různých odvětví života své populace. Relevantní bylo pro autorku zejména využívání nástrojů e-governmentu.


Zranitelnost současné společnosti pramenící ze závislosti na postmoderních ICTs, jež jsou využívány v široké škále našich činností, může být zneužita ke kybernetickým útokům proti státu. Druhým předpokladem této diplomové práce je tak vnímání kybernetické bezpečnosti a kybernetických útoků coby relevantních strategických a bezpečnostních výzev současnosti. Zkušenost Estonska i jiných zemí vskutku vedla k přehodnocení pojetí kybernetických hrozeb a jejich přítomnost je zahrnována do strategicko-bezpečnostních koncepcí jednotlivých států, ale i mezinárodních organizací, např. EU.

Text sleduje též motivace, prostředky i nejčastější typy kybernetických útoků. Pozornost je věnována rovněž teorii a praxi informační bezpečnosti tedy zajištění ochrany informačních systémů, neboť praxe e-governmentu je s nimi úzce spojena a současně fungování státu je charakteristické spravováním ohromných objemů dat o svých občanech právě v těchto informačních systémech a zaručení jejich náležitého zabezpečení před zneužitím či narušením jejich integrity a důvěryhodnosti se tak stává zásadní.

Klíčová slova: e-government, elektronický podpis, elektronické doručování a podání, CzechPOINT, datové schránky, informační bezpečnost, kybernetická bezpečnost, kybernetické útoky, Česká republika, Evropská unie.
ABSTRACT

The topic of this thesis was inspired by cyber attacks against Estonia in spring 2007. They paralyzed the country temporarily to provide appropriate services to its citizens. This Baltic state is known for its sophisticated use of post-modern ICTs within a wide range of its population's life. Especially the use of e-government tools was relevant for the author of the thesis.

The objective of this study is to present and analyse a development of e-government methods application in the Czech Republic with regard to the EU influence on this process. Our first hypothesis is therefore an acknowledgement of the Community as a driving force of more intensive development within the e-government tools application in the Czech Republic visible from mid-2000s. There can be seen certain correlation with the EU accession in 2004. It has been shown that structural and communitarian funds are an important financial source for electronic and effective public administration implementation. Indispensable is also an opportunity to share experience within this field among the Member states.

Contemporary society has become dependent on post-modern ICTs that are used in a wide range of our activities (e.g. e-banking, e-commerce, e-government etc.). This dependency causes its vulnerability that can be misused for cyber attacks against the state. Next presumption of this thesis is thus acknowledgement of cyber security and cyber attacks as relevant strategic and security challenges of today. The experience of Estonia but also other countries has led to revaluation of an approach to cyber threats and they have become present in strategic and security concepts of particular states as well as international organizations such as the EU.

The text also presents motivations, tools and the most common types of cyber attacks. The theory and practise of information security is also taken into consideration. Contemporary state functioning is characterized by huge amount of personal data storing. Their secure administration is therefore crucial.

Key words: e-government, electronic signature, electronic delivering and administrative action, CzechPOINT, data mail boxes, information security, cyber security, cyber attacks, Czech Republic, European Union.