MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Policejní akademie ČR

Bezpečnostní seminář

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Co je kybernetická bezpečnost

Úvodem bych chtěl podotknout, že v rámci právního pořádku České republiky není do současné doby platný žádný zákon, který by uceleně upravoval problematiku kybernetické bezpečnosti.

Předmětem kybernetické bezpečnosti je nutnost zabezpečit bezpečí v kyberprostoru, dále ochrana dat před zničením, krádeží a zneužitím zločinnými hackery (státními, ale i soukromými) a prioritou je rovněž ochrana osob, jichž se data týkají.

Většina rizik hrozící informačním systémům nepochází od hackerů, kteří se snaží škodlivými kódy proniknout k systému a k tam uloženým datům, aby provozovali své „zábavné hry“, ale od konkurence, vlastních zaměstnanců, zákazníků nebo obchodních partnerů či jiných států. Aktivní a moderní zabezpečovací softwarové bariéry a ochranné programy jistě ve většině případů pomohou, nezabrání však, aby například konkurence znemožnila za využití útoku na data společnosti provoz systému, třeba jen na omezenou dobu.

Většina států vidí v ochraně kybernetického prostoru jeden ze svých základních bezpečnostních úkolů. Velká Británie nově stanovila základní hrozby proti státu a kybernetický útok je v žebříčku hrozeb podřazen hned pod terorizmus a jadernou hrozbu. Ministerstvo obrany USA konstatuje, že kybernetický prostor se připojuje k tradičním válečným doménám a zahrnuje jej do své obranné doktríny.

Problém kybernetické bezpečnosti se netýká pouze státních institucí, firem, ale v souvislosti s prudkým rozvojem využívání elektronického bankovnictví, elektronické komunikace (např. datové schránky apod.) se dotýká i fyzických osob. Je čím dál větší nebezpečí související s omezením činností, které jsou důležité pro chod státní správy a samosprávy (eliminace komunikačního prostředí apod.), krádežemi jednak identity osoby, ale i padělaním platebních karet a tzv. „vybílením“ bankovních kont.

Pro informaci uvádím, že podle statistik EU bankomatové podvody vzrostly v roce 2010 v Evropě oproti roku 2009 o 24 procent.

Dalším, podle mého názoru opomíjeným problémem jsou tzv. sociální sítě, zejména sdílení osobních dat uživatelů v různých reklamních sítích a jejich případné zneužití a to jak ze strany reklamy, tak i z hlediska vydírání, krádeží údajů apod.

Velkým problémem je kybernetická špionáž, či diverzní akce, prováděná v rámci kyberprostoru.

V tomto směru je vhodné dodržovat deset zásad, které zveřejnila společnost SecureWorks:

- Využívat odborníky na informační bezpečnost
- Přehled o tom, která aktiva je třeba chránit a jaká jsou s nimi spojená rizika
- Vědomí, kde leží vaše zranitelnosti
- Dát do pořádku či zmírnit zranitelnosti vhodnou strategií

- Porozumět taktikám útočníků, jejich technikám a procedurám, které umožní přetvořit obranná opatření do vhodných podob
- Být připraven zabránit útoku či odpovědět tak rychle, jak je možné – v případě kompromitace
- Preferovaná je prevence, ale nutností je také detekce a vhodná odpověď
- Mít k dispozici nouzový plán k tomu, co dělat v případě, když se stanete obětí kybernetické války
- Přesvědčit se, že dodavatelé v rámci kritických infrastruktur nejsou kompromitováni a mějte k dispozici vhodná opatření v případě, že jejich systémy budou narušeny
- Národní kritická infrastruktura nesmí být plně závislá na internetu, ale musí být operabilní i v případech, kdy přijde krize kybernetické bezpečnosti.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ochrana utajovaných informací

Na rozdíl od kybernetické bezpečnosti má ochrana utajovaných informací v rámci České republiky dlouhou tradici. Od roku 1971 byla ochrana státního a hospodářského tajemství upravena zákonem č. 102/1971 Sb., o ochraně státního tajemství a předpisy Federálního ministerstva vnitra. Po roce 1990 byl zákon č. 102/1971 Sb. několikrát novelizován především s ohledem na společenské změny v České a Slovenské Federativní republice.

V roce 1998 byl Parlamentem ČR přijat zákon č. 148/1998 Sb., o ochraně utajovaných informací. Tímto zákonem byl zřízen Národní bezpečnostní úřad jako ústřední orgán státní správy na úseku ochrany utajovaných skutečností.Zákon byl dále předložen do legislativního procesu i z důvodu, že v zákoně č. 102/1971 Sb. nebyly odpovídajícím způsobem řešeny podmínky, které musí osoba splnit, aby jí byl umožněn přístup k utajované skutečnosti a v tomto zákoně nebyly nijak upraveny přístupy k utajované skutečnosti ze strany právnických osob. Posledním, v neposledním případě nejdůležitějším faktem byla skutečnost, že zákon neupravoval výměnu utajovaných skutečností s dalšími státy a toto byl, v souvislosti s připravovaným vstupem České republiky do Severoatlantické aliance největší problém.

V současné době je ochrana utajovaných informací upravena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Zákon upravuje jednotlivé druhy zajištění ochrany utajovaných informací:

a) personální bezpečnost, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,

b) průmyslovou bezpečnost, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem,

c) administrativní bezpečnost, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,

d) fyzickou bezpečnost, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,

e) **bezpečnost informačních nebo komunikačních systémů**, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému a

f) **kryptografickou ochranou**, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Kryptografická ochrana

Ross Anderson shrnul nedávné informace, které proběhly britským a americkým tiskem a uvádí, že kryptografická ochrana informací opět nabývá na významu a to nejen mezi orgány státu, ale i mezi soukromými subjekty. V době, kdy se ucelené soubory informací předávají za pomoci vysokorychlostního internetu a pokračuje stávající trend propojování státní sféry s internetem je stáhnutí národních databází pomocí kybernetického útoku záležitostí vteřin. Z tohoto důvodu opět nabývá na vážnosti kryptografická ochrana informací.

Utajovanou informaci můžeme zpracovávat a přepravovat pouze v certifikovaném utajovaném systému za splnění podmínek fyzické a personální bezpečnosti.

Problematika kryptografické bezpečnosti je mimo zákon č. 412/2005 Sb. upravena vyhláškou č. 524/2005 Sb., ze dne 14. prosince 2005 o zajištění kryptografické ochrany utajovaných informací a vyhláškou č.523/2005 Sb., ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. Citované vyhlášky stanoví podrobnosti o zkoušce zvláštní odborné způsobilosti pracovníka kryptografické ochrany, způsoby a prostředky manipulace s kryptografickým materiálem, podrobnosti způsobu vyznačování náležitostí na utajované informaci z oblasti kryptografické ochrany a administrativní pomůcky kryptografické ochrany a další podrobnosti k zajištění kryptografické ochrany utajovaných informací jakož i požadavky na informační systémy nakládající s utajovanými informacemi a provádění jejich certifikace, na komunikační systémy nakládající s utajovanými informacemi a ochranu utajovaných informací před jejich únikem kompromitujícím elektromagnetickým vyzařováním a provádění certifikace stínicích komor.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Vládní utajené spojení
IS Vega

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Vládní utajené spojení

Zákon České národní rady č. 2/1969 Sb., ze dne 8. ledna 1969 o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky (kompetenční zákon) stanoví v § 12, že „Ministerstvo vnitra je ústředním orgánem státní správy pro vnitřní věci, mimo jiné provozuje informační systém pro nakládání s utajovanými informacemi mezi orgány veřejné moci“. (Platí od roku 2008).

Vládní utajené spojení je od roku 1969 provozováno Ministerstvem vnitra. Na základě usnesení vlády ČR č. 966 ze dne 7.10.2002 je provozováno jako analogový komunikační systém s nepřetržitým provozem. Nynější vládní utajené spojení je určeno pro přenos utajovaných skutečností do stupně utajení „DŮVĚRNÉ“ mezi nejvyššími státními a vládními činiteli a určenými vedoucími pracovníky ústředních orgánů státní správy a jejich příslušných pracovišť krizového řízení. Důvěrnost a integrita utajovaných skutečností při jejich přenosu je zajištěna certifikovaným kryptografickým prostředkem SECTEL 9600 TORO, který je provozován v hlasovém a faximilním režimu.

Na základě usnesení vlády č. 112 ze 4. února 2004, je budován nový formační systém vládního utajeného spojení Vega-D (IS Vega-D), který nahradí současné vládní utajené spojení, komunikační systém Vektor. IS Vega-D po dokončení výstavby splní požadavky současnosti na kryptograficky zabezpečený přenos dat a hovoru do stupně utajovaných informací Důvěrné.

IS Vega-D zajistí v rámci státní správy kryptograficky zabezpečenou komunikaci na území ČR do úrovně krajských úřadů a do zahraničí na vybrané zastupitelské úřady ČR.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

IS Vega-D bude komunikačně propojen se současně budovaným IS Beta, což je rezortní utajené spojení Ministerstva vnitra, PČR a HZS ČR. Tím bude umožněna kryptograficky zabezpečená komunikace a přenos dat do úrovně krajských ředitelství PČR a krajských ředitelství HZS ČR.

Uživateli IS Vega-D jsou pracovníci úřadů (stanovené funkce), jejichž systemizace byla schválena vládou v rámci usnesení vlády č. 112/2004Sb.

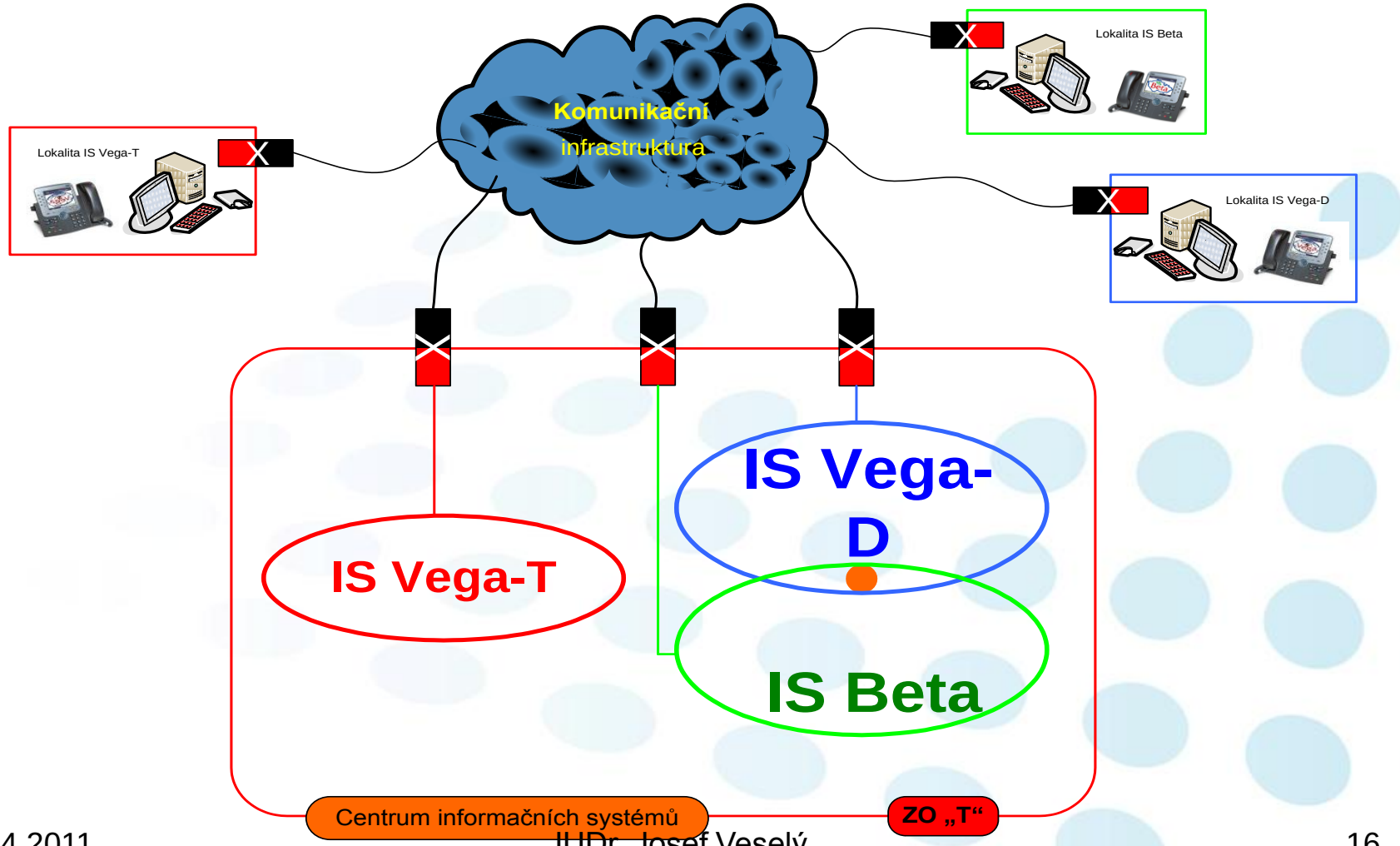
K zabezpečení kryptografické ochrany přenášených utajovaných informací budou použity, Národním bezpečnostním úřadem certifikované kryptografické prostředky, které jsou certifikovány i pro přenos UI z EU a NATO do stupně UI Důvěrné. Provozovatelem obou uvedených IS je Ministerstvo vnitra ČR.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

IP telefonní přístroj@logo IS Vega

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

IS Vega-T @ IS Beta @ IS Vega-D



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Systémové řešení bezpečnosti IS

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

IS Vega-D splňuje funkční požadavky:

- Kryptograficky zabezpečený přenos utajovaných informací ve formě dat a IP telefonie, přenosový protokol TCP/IP,
- IS Vega-D nesmí být komunikačně propojen s jinými datovými systémy (IS Vega-T, Internet, Intranet, atd.),
- IS je vybudován jako konstrukčně neuzavřené s možností dalšího rozvoje služeb a uživatelské kapacity,
- veškeré výstupy z IS Vega-D do „veřejného“ komunikačního (přenosového) prostředí je provedeno přes bránu, kterou tvoří IP kryptografický prostředek,
- stupeň utajovaných informací Důvěrný,
- přípojná kapacita IS 500 uživatelů na cca. 75 lokalitách,
- elektronický podpis,
- časové razítko,
- e-mail pošta,

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Lokalita @ Uživatel IS

Uživatel IS musí být prověřen „D“!

Koncová zařízení IS:

- Rack KP (umístěn bezvýhradně v ZO „D“)
- IP telefonní přístroj
- čtečka identifikačních karet
- stolní PC s vyjímatelným HDD (pro ZO „V“)

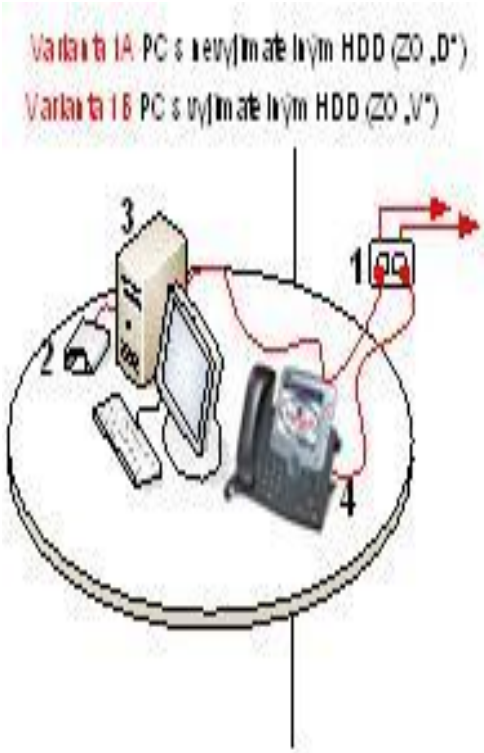
nebo

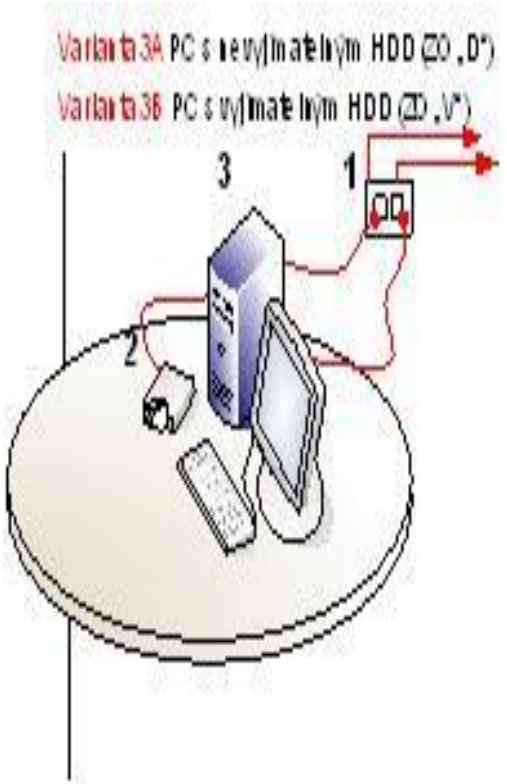
- stolní PC s nevyjímatelným HDD (pro ZO „D“)

- Lokalita, je množina uživatelů IS připojená na Rack KP

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Možné varianty koncových zařízení uživatele a požadované ZO:





MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

- zařízení, která nejsou součástí IS musí být umístěny ve vzdálenosti **500mm** od zařízení IS
- je-li PC s vyjímatelným HDD může být **minimálně** v ZO **„V“**
- je-li PC s nevyjímatelným HDD **musí** být umístěn v ZO **“D“**
- **PC lze využít ke zpracovávání UI obdobně jako v systémech „VYDRA“ a „DUDEK“**
- **uživatel IS musí být držitelem prověrky fyzické osoby stupně „D“**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Identifikační karty

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Čtečka identifikačních karet@CK

- zařízení, která nejsou součástí IS musí být umístěny ve vzdálenosti **500mm** od zařízení IS
- jedinečná identifikační karta uživatele bez režimu, **NEPŘENOSNÁ!!,**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dotazy, otázky ?

Děkuji za pozornost