Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011- 2015

Slovník vybraných pojmů

Úvod:

Tento slovník není klasickým výkladovým slovníkem a nečiní si proto obvyklý nárok na výkladovou a termínovou korektnost. Slovník je přidruženým dokumentem materiálu Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011-2015 a stručně vysvětluje pojmy, které s kybernetickou bezpečností souvisí.

autentičnost (authenticity) - vlastnost (údajů) vyjadřující to, že údaje jsou pravé, což se dá i ověřit (autentifikace), a proto jim lze důvěřovat; důvěra v platnost přenosu informace, přenesené zprávy nebo v to, že zprávu poslal ten, kdo se za jejího odesílatele vydává.

autentifikace (authentication) - ověření identity uživatele, procesu nebo zařízení, nebo původu zprávy

bezpečnostní incident ((computer) security incident) - porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a Komunikační Technologie.

bezpečnostní politika (security policy) - (1) na úrovni organizace základní dokument, který vymezuje strukturu bezpečnostního rizika, odpovědnost za ochranu informací v organizaci, úroveň ochrany informací. (2) na úrovni systému soubor pravidel a praktik, které specifikují nebo regulují, jak systém (nebo organizace) poskytuje bezpečnostní služby, aby chránil citlivé nebo kritické zdroje systému.

bezpečnostní opatření (security safeguards) - ochranná opatření pro zajištění bezpečnostních požadavků kladených na systém. Mohou mít různý charakter (fyzická ochrana zařízení a informace, personální bezpečnost - kontrola pracovníků, organizační opatření – provozní předpisy atd.)

bezpečnostní požadavky (security requirements) - požadavky kladené na informační systém, které jsou odvozeny ze zákonů, instrukcí, právních úprav, závazných norem a standardů, vnitřních předpisů organizace; prostředí, ve kterém systém působí a poslání, které plní; nutné pro zajištění důvěrnosti, dostupnosti a integrity informací, která se v systému zpracovává.

CERT (computer emergency response team)-tým odborníků, jejichž úkolem je řešit bezpečnostní incidenty. První CERT založila americká agentura Defence Advanced Research Projects Agency (DARPA) pod názvem The CERT Coordination Center (CERT/CC3), na Carnegie Mellon University v Pittsburghu (Pennsylvania). Název CERT je registrován v USA, a proto se v Evropě používá pojem CSIRT. Existují i další podobná označení, která jsou synonymem pojmu CERT (CERT nebo CERT / CC (Computer Emergency Response Team / Coordination Center), CSIRT (Computer Security Incident Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team), SERT (Security Emergency Response Team))

CSIRT (computer security incident response team) - tým odborníků na informační bezpečnost, jejichž úkolem je řešit bezpečnostní incidenty. CSIRT poskytuje svým klientům potřebné služby při řešení bezpečnostních incidentů a pomáhá jim při obnově systému po bezpečnostním incidentu. Aby snížily rizika incidentů a minimalizovaly jejich počet, pracoviště CSIRT poskytují svým klientům také preventivní a vzdělávací služby. Pro své klienty poskytují informace o odhalených slabinách používaných hardwarových a softwarových prostředků a o možných útocích, které těchto slabin využívají, aby klienti mohli dostatečně rychle ošetřit odhalené slabiny.

červ (worm) – škodlivý, autonomně se kopírující, autonomně se šířící ucelený (self contained) program, který se šíří v počítačových sítích.

Data - jakékoli vyjádření (pro ICT se uvažují typicky data v digitální podobě) skutečnosti, schopné přenosu, interpretace či zpracování. Účelem dat je přenášet a dále zpracovávat odraz skutečnosti. Jsou to jakékoli zaznamenané poznatky či fakta.

elektronický podpis (electronic signature) - bezpečnostní funkce pro zajištění integrity a autentičnosti digitálních dokumentů. Má podobu čísla, vypočteného na základě podepisování dokumentů a jedinečného soukromého klíče podepisující osoby.

ENISA - (European Network and Information Security Agency) - agentura založená Evropskou unií jako Centrum excelence v oblasti síťové a informační bezpečnosti v roce 2004. Jejím úkolem je pomáhat EU, jejím členským státům, soukromému sektoru a veřejnosti při prevenci a řešení bezpečnostních problémů a při reakcích na bezpečnostní problémy.

FIRST - Celosvětově působící asociace , která spojuje cca 200 pracovišť typu CERT

HOAX - poplašná zpráva, která se svým obsahem snaží vyvolat dojem důvěryhodnosti. Informuje např. o šíření virů nebo útočí na sociální cítění adresáta. Často obsahuje škodlivý kód nebo odkaz na internetové stránky se škodlivým obsahem.

identifikace (identification) - akt nebo proces, během kterého entita předloží systému nějaký identifikátor, na jehož základě systém může rozeznat entitu a odlišit ji od jiných entit.

Identita - sada vlastností, které jednoznačně určují konkrétní objekt – věc, osobu, událost,

ICT (ICT-Information and Communication Technology) - informační a komunikační technologií se rozumí veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení.

Informace - data, která mají smysl (význam). Je to údaj, ke kterému si člověk přiřadí význam.

informační bezpečnost (information security)
(1) soustava vzájemně provázaných opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření bezpečnosti informačních a komunikačních technologií pro zajištění **dostupnosti, důvěrnosti a integrity informací**. Informační bezpečnost je dále zajištěna **spolehlivostí a zodpovědností**.

Dostupnost (availability) – zajištění toho, aby informace a s nimi spojená aktiva byly přístupné autorizovaným (oprávněným) uživatelům (entitám) podle jejich potřeb v požadovaném čase;
Důvěrnost (confidentiality) – zajištění toho, aby informace byly dostupné pouze osobám (entitám, procesům) oprávněným pro přístup k těmto informacím;
Integrita (integrity) – ochrana správnosti (před modifikací - neoprávněnou změnou) a zajištění kompletnosti (úplnosti);
Spolehlivost (reliability) – zajišťuje konzistenci chování a výsledků
Zodpovědnost (responsibility)– je určena individuální zodpovědnost;

(2) schopnost systému na dané úrovni spolehlivosti odolávat náhodným událostem i záměrným akcím, které kompromitují dostupnost, důvěrnost a integritu uložených nebo přenášených dat a služby poskytované nebo zpřístupňované daným systémem

informační systém (information system) - je funkční celek, nebo jeho část zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky.
informatizace společnosti - proces transformace společnosti, během něhož probíhá nasazování ICT spojené s přehodnocením tradičních procesů zpracování informace a jejich nahrazování novými, zohledňující možnosti a omezení IKT. Cílem informatizace společnosti je zefektivnění její fungování prostřednictvím ICT, výsledkem úspěšné informatizace by měla být postindustriální, **informační společnost**. Což je společnost založená na využívání informačních a komunikačních technologií. Základem je neustálá výměna znalostí a informací a práce s nimi za předpokladu schopnosti jim rozumět. Tato společnost pokládá vytváření, šíření a manipulaci s informacemi za nejvýznamnější ekonomické a kulturní aktivity.

Zajištění **integrity dat -** znamená přijetí opatření, která vylučují možnost nepozorované změny údajů a zajišťují správnost prezentace (čtení) těchto údajů. Zajištění integrity technického systému znamená vyloučení možnosti jeho neoprávněné modifikace.

informační a komunikační infrastruktura organizace - z hlediska organizace to je souhrn všech komponentů informační a komunikační technologie (dále ICT), které organizace používá k plnění svého poslání.

kritická komunikační a informační infrastruktura státu
Slouží k informačnímu zajištění řádné funkceschopnosti kritické infrastruktury státu a označuje komplex informačních a komunikačních systémů a jejich služeb. Obsahuje součásti jako jsou telekomunikace, počítačové systémy a jejich programové vybavení, internet, přenosové sítě, poskytované služby atd.

kyberprostor – (**cyberspace)** nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Umožňuje vytvářet, uchovávat, využívat a vzájemně vyměňovat informace. Zahrnuje počítače, aplikace, databáze, procesy, pravidla, komunikační prostředky.

kyberterorismus - je zneužitím kyberprostoru pro teroristické účely, tak jak jsou definovány vnitrostátním a mezinárodním právem.

kybernetická bezpečnost - vyjadřuje schopnost kyberprostoru odolávat úmyslně i neúmyslně vyvolaným hrozbám a v případě škodlivého zásahu dosáhnout opětné bezpečného stavu.

kybernetický útok - je využití kybernetické zbraně za účelem poškození určeného cíle.

kybernetický protiútok - je využití kybernetické zbraně za účelem poškození určeného cíle v odpověď na předchozí kybernetický útok.

kybernetická obrana - zahrnuje způsobilost subjektu efektivně se bránit kybernetickému útoku, zmírnit jeho následky a dosáhnout opětné rovnováhy.

Meziresortní koordinační rada pro oblast kybernetické bezpečnosti - MKRPKB

Zřízena na základě usnesení vlády České republiky ze dne 24. května 2010 č. 380.

Podporuje výkon gesční a koordinační role MV ČR v oblasti kybernetické bezpečnosti vyžadující součinnost státních institucí a v této oblasti plní mimo jiné tyto úkoly:

- Koordinuje činnost státních institucí v oblasti kybernetické bezpečnosti
- Koordinuje státní instituce při plnění úkolů vyplývajících z členství ČR v mezinárodních organizacích
- Vytváří podmínky pro hladké fungování spolupráce mezi členy rady
- Řeší aktuální otázky a předkládá odborné návrhy a doporučení ministru vnitra a jeho prostřednictvím vládě
- Sleduje plnění závěrů z jednání rady jejími členy

- shromažďuje, analyzuje a vyhodnocuje údaje o stavu zajištění kybernetické bezpečnosti poskytované členy koordinační rady,
- připravuje návrh zprávy o stavu zajištění kybernetické bezpečnosti České republiky, která je pravidelně předkládána ministrem vnitra vládě jako výchozí dokument, který stanovuje priority a z nich vyplývající úkoly v oblasti kybernetické bezpečnosti pro nadcházející období,
- spolupracuje s externími odbornými subjekty a využívá jejich výstupů v zájmu zajišťování kybernetické bezpečnosti České republiky.
-
- Spolupracuje s externími odbornými subjekty a využívá jejich výstupů v zájmu zajišťování kybernetické bezpečnosti ČR

Zřízení rady a výkon její činnosti nezbavuje státní instituce zodpovědnosti kybernetickou bezpečnost v rámci kompetencí

počítačová síť (computer network) - soubor počítačů spolu s komunikační infrastrukturou (Komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.

spam (spam) - masové šíření nevyžádané elektronické pošty nejčastěji kvůli komerčním důvodům (reklama, marketing). Spam zatěžuje počítačové sítě nechtěnou komunikací, způsobuje ztráty času a případně finančních prostředků (u uživatelů platících za objem přenesených dat). Nevyžádané e-mailové zprávy mohou být i nositelem škodlivého softwaru

špionážní program / software (spyware) - typ škodlivého programu, který je tajně nebo nenápadně instalován do cílového systému na to, aby získával informace o organizaci nebo jednotlivcích bez jejich vědomí

TERENA - Trans-European Research and Education Networking Association, evropská mezinárodní organizace podporující aktivity v oblasti internetu, infrastruktur a služeb v rámci akademické komunity.

TF-CSIRT - mezinárodní fórum umožňující spolupráci týmů CSIRT na evropské úrovni. Dělí se na dvě skupiny – uzavřenou, která je přístupná pouze akreditovaným týmům, a otevřenou, která je přístupná všem zájemcům o práci týmů CSIRT. TF-CSIRT je jednou z aktivit mezinárodní organizace TERENA. Pracovní skupina TF-CSIRT se schází obvykle několikrát ročně.

trojský kůň (Trojan horse) - program, který plní na první pohled nějakou užitečnou funkci, ale ve skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, které poskytuje.
údaje (data) - reprezentace informací formalizovaným způsobem vhodným pro komunikaci, výklad a zpracování.

virus, počítačový (computer virus) - počítačový program, který se replikuje připojováním své kopie k jiným programům. Může obsahovat část, která ho aktivizuje, pokud dojde ke splnění některých podmínek (např. čas) v hostitelském zařízení. Šíří prostřednictvím Internetu (elektronická pošta, stahování programů z nespolehlivých zdrojů), pomocí přenosných paměťových médií apod.

škodlivý software (malicious software - malware) - programy, jejichž cílem je poškodit programy a data na hostitelském zařízení (počítači, mobilním telefonu, PDA, průmyslové řídící systémy a další zařízení, která jsou řízena nebo obsahují software), získat údaje z hostitelského zařízení nebo ovládnout hostitelské zařízení Mezi škodlivý software patří počítačové viry, trojské koně, červy, špionážní software.

zranitelnost (vulnerability) - slabé místo v informačním systému, bezpečnostních procedurách systému, vnitřních kontrolách nebo implementaci, které může aktivovat nebo využít nositel hrozeb.