KYBERNETICKÁ BEZPEČNOST

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OPVK Vzdělávací modul Kybernetická bezpečnost

KYBERNETICKÁ BEZPEČNOST

Základní kurz kybernetické bezpečnosti

NETWORK SECURITY MONITORING CLUSTER 2015

Tento modul je financován jako projekt v rámci 5. výzvy z prostředků ESF a státního rozpočtu ČR pod registračním číslem CZ.1.07/3.2.04/05.0014.

Seznam spolupracovníků:

Pavel Minařík

minarik@invea.cz

Lukáš Vondráček

vondracek@elat.cz

Petr Mikšovič

petr.miksovic@sovanet.cz

Petr Lacina

placina@uniscomp.cz

Petr Linke

petr.linke@novicom.cz

Projekt OPVK “Vzdělávací modul Kybernetická bezpečnost”

Reg.č. CZ.1.07/3.2.04/05.0014

1. ÚVOD DO PROBLEMATIKY KYBERNETICKÉ BEZPEČNOSTI

Kybernetická bezpečnost – kolikrát a jak často v poslední době slýcháme a vídáme tento pojem? Noviny, televize, diskuzní servery, ale mnohokrát i zapálené debaty u piva v hospůdce, o školních přestávkách, v práci nebo jen doma u večeře, skýtají nejednu příležitost dotknout se alespoň okrajově tohoto tématu. Diskuze na toto téma se bezděčně i plánovitě účastní téměř všichni – od dětí absorbujících mentorování snad poučených rodičů, přes kamarády nebo i jen známé, kolegy v práci, až po seniory naslouchající starostlivým radám a návodům vnoučat stran přežití ve světě jedniček a nul.

Navzdory skutečnosti, že zasvěcenost do této problematiky je u zmíněných skupin různá, snížení obtížnosti problému kybernetické bezpečnosti samozřejmě nenahrává ani vysoká dynamika rozvoje digitálního světa a jeho přesahu do světa reálného. Průkopnické doby, kdy se digitální technika teprve vyvíjela a náš každodenní život ovlivňovala jen minimálně, jsou dávno ty tam a náš současný reálný svět je na fungování toho paralelního - digitálního kriticky závislý. Chod bank, průmyslových podniků, nemocnic, dopravy, výroba potravin, resp. vlastně téměř čehokoliv, energetika i správa přírodních zdrojů, předpověď počasí, vzdělávání i zábava, veřejná správa a mnoho dalšího, to vše je dnes závislé na digitálním světě kolem nás. Naše existence a náš způsob života jsou přímo závislé na získávání, uchovávání a sdílení informací. Ano, jsme prostě závislí. Můžeme si sice namlouvat, že tomu tak není, ale je to jen milosrdná lež.

1.1. POČÍTAČOVÁ BEZPEČNOST, POČÍTAČOVÁ KRIMINALITA, NEEXISTENCE HRANIC, NEURČITOST ÚTOČNÍKA A OCHRANA NÁRODNÍHO KYBERNETICKÉHO PROSTORU

1.1.1. POČÍTAČOVÁ BEZPEČNOST

Něco o pojmosloví[1]

Klíčové pojmy řady disciplín jsou často chápány a používány intuitivně. Intuitivní chápání pojmů je sice do jisté míry účelné, ale má svá úskalí dokonce i uvnitř jedné disciplíny a vede často k nedorozuměním. Intuitivní chápání důležitých obecných pojmů (a nepřesné používání termínů ony pojmy označujících) méně vadí tehdy, pokud se významy těchto pojmů v různých disciplínách liší jen málo; když jsou sice „rozmazané“, ale přece jen dostatečně “sladěny” pro společně platný výklad. Pokud ale “jeden mluví o voze a druhý o koze”, pak nedosáhnou výsledku, i když používají stejná slova.

Předpokladem pro takové vnímání je obvyklost, zažitost v obecném jazyce. Tyto termíny jsou často českého nebo slovanského původu. Mezi ně patří například „bezpečnost“ nebo „zájem“. To samozřejmě neznamená, že není důležité i tyto pojmy náležitě přesně definovat.

Méně jednoty panuje u termínů pocházejících z cizích jazyků; například „strategie“, pojem používaný v celé škále vědních oborů i praktických disciplín – od vojenství, mezinárodní politiky až po ekologii. V těchto případech zodpovědní autoři vymezují, zda daný pojem chápou v širším nebo užším významu, nebo předkládají (nabízejí ke konsenzu) formulovanou definici pojmu. Slovníkové definice v takových případech nabízejí vedle sebe několik významů podle jednotlivých disciplín. Nejméně uspokojivé je do nedávné doby krajně rozkolísané používání klíčových termínů „hrozba“ a „riziko“ (viz příslušné heslo této publikace). Termín „krize“ se

[1] Převzato z PERSPEKTIVY VÝVOJE BEZPEČNOSTNÍ SITUACE, VOJENSTVÍ A OBRANNÝCH SYSTÉMŮ DO ROKU 2015, S VÝHLEDEM DO ROKU 2025, Česká bezpečnostní terminologie, Výklad základních pojmů, P. Zeman a kol., Brno 2002. Dostupné na: *www.defenceandstrategy.eu/filemanager/files/file.php?file=16048.*

zase používá natolik široce a metaforicky, že někdy téměř ztrácí vypovídací schopnost.

Pojem „bezpečnost“

Pojem „bezpečnost“ je, zcela logicky, základním pilířem a rozpoznávacím znakem bezpečnostní terminologie. V českém jazyce se bohužel poněkud stírá několik zásadních a v cizích jazycích zřetelnějších odlišností, které jinak máme při práci s tímto termínem k dispozici. Pracují s ním různé obory lidské činnosti (počínaje politikou a mezinárodními vztahy, přes ekonomii, stavebnictví, strojírenství, chemii, medicínu, až po vzdělávání a sociologii) a v daných kontextech jej tak často používáme s chápáním různého nebo mírně odlišného významu, aniž bychom si tuto skutečnost plně uvědomovali. S použitím výkladového slovníku pak můžeme zjistit, že pojem v zásadě významově reprezentuje neměnnost stavu věcí směrem negativním resp. ochranu před vlivy nebo jevy k tomu směřujícími.

Jiné jazyky, zejména například angličtina nebo francouzština v tomto ohledu poskytují jemnější rozlišení takového stavu. Pojem není ošetřen pouze slovem bezpečnost, ale rozdílnost výrazů „safety“ a „security“ příměji odlišuje strany zachování stavu, přičemž své vymezení opírají o sebe navzájem. Tyto výrazy v našem jazyce bohužel přímý protějšek nemají. Hovoříme tak například o car safety, ale také o homeland security. Zkratkovitě lze shrnout, že pojem safety je zde významově blíže například bezpečnosti jednotlivce (bezpečí), ovlivňovaného zejména faktory nedbalosti, kdežto pojem security je spíše bližší pojmu skupinové bezpečnosti. V různých oborech se pak tyto pojmy setkávají nejčastěji u významového ekvivalentu absence nějakých hrozeb, kdy takového stavu lze dosáhnout jejich eliminací nebo minimalizací či užitím ochrany před nimi.

Český slovník pojmů kybernetické bezpečnosti

Počítačová bezpečnost, resp. snahy o její řešení nás provázejí již nějakou dobu. Vývoj stíhá vývoj, a to nejen technický, ale i související společenský, kulturní, osobní. Ještě nedávno bylo slovo Facebook nesmyslem a nikdo ani nepomyslel, v kolika národních slovnících se zabydlí sloveso odvozené od názvu společnosti Google. Ruku v ruce s tímto vývojem a snahou věci řádně pojmenovávat logicky

dospěla problematika informačních a komunikačních technologií, telekomunikací, řízení bezpečnosti a všeho dalšího do bodu, kdy bylo třeba udělat jasno v pojmech, kdy často některé ani neměly řádný ekvivalent v Českém jazyce.

V České republice se k tomuto tématu aktivně postavila pracovní skupina AFCEA - Kybernetická bezpečnost. Ve spolupráci s českými odborníky na tuto oblast zveřejnila oficiální český slovník pojmů kybernetické bezpečnosti. Jeho první verze byla vydána v roce 2012. Záštitu převzal Národní bezpečnostní úřad ČR a nově vznikající Národní centrum kybernetické bezpečnosti. Slovník vydala Česká pobočka AFCEA a Policejní akademie ČR pod ISBN: 978-80-7251-378-9 (ve formátu PDF pod ISBN 978-80-7251-377-2.). Pro velký zájem se však nejednalo o poslední verzi. Dotisk druhého vydání z roku 2014 byl vydán pod ISBN 978-80-7251-397-0. Byl rozšířen a aktualizován obsah předchozího Výkladového slovníku kybernetické bezpečnosti za použití překladu české terminologie a pojmosloví z kybernetické bezpečnosti do anglického jazyka. Je tedy odlišného pojetí od předcházejících verzí.

Tento přístup pak lépe koreluje se shora naznačenou růzností chápání vysvětlovaných pojmů bezpečnosti, jakož i dalších uvedených pojmů a pomáhá lépe chápat naznačené pojmy, v kontextu překladu i tam, kde to bylo dříve obtížné. Pomáhá tak odborníkům pracovat lépe v situacích, kdy je důležitá nejen významová, ale i pojmová integrita se zahraničními a mezinárodními materiály.

Český slovník kybernetické bezpečnosti je užitečným vodítkem pro formulaci a interpretaci pojmů v rámci tohoto vzdělávacího programu, který uvedené pojmosloví a terminologický konstrukt zahrnuje a používá.

1.1.2. NEEXISTENCE HRANIC

Prostor je spojité prostředí rozkládající se bez hranic všemi směry, to je první podmínka pro konstatování jeho existence. Kyberprostor nemá vzdálenosti, jak je chápeme v rámci reálného světa. Nemá dokonce ani žádný rozměr. Kyberprostor nezná žádné nahoru, dolů, doleva nebo doprava. Jediný rozměr, který v něm lze

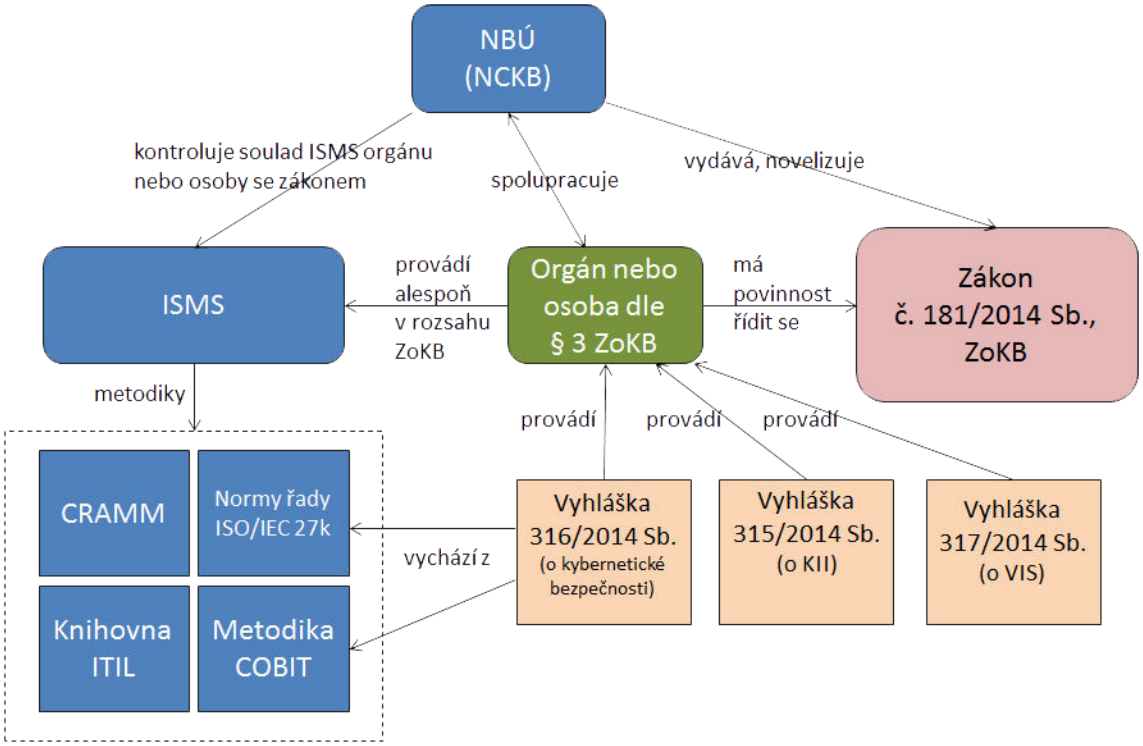
najít, je čas. Pro vnitřního pozorovatele však má podobu nekonečně velké koule. Jak je to možné bez rozměrů? Je totiž tvořen pouze informacemi, které nemusejí při své cestě od uživatele A k uživateli B překonat vzdálenost vyjádřenou v metrech nebo kilometrech. Rychlost přenosu informací z bodu A do bodu B je limitována pouze propustností infrastruktury. V tomto kontextu se nelze tedy spoléhat na to, že se někde u Starého Hrozenkova, u Aše nebo jinde "na čáře" obsah zastaví k proclení nebo k hraniční kontrole. Kyberprostor z tohoto pohledu nemá hranice srovnatelné s těmi, které jsme si zvykli vnímat v našem "fyzickém světě".

1.1.3. NEURČITOST ÚTOČNÍKA

Výhodou různých forem distančních útoků z hlediska útočníka nebo útočníků je možnost ukrýt se za přezdívku, tzv. „nick", nebo za jiný neurčitý identifikátor, či dokonce za celou kaskádu anonymizačních nástrojů, postupů a falešných identit (včetně například multiplikace nebo naopak agregace identit a atributů, které by mohly vést k jejich odhalení). Útoky prováděné pod rouškou anonymity jsou agresivnější, zákeřnější a využívají metody, které by útočník při přímém kontaktu, kdy je jeho totožnost zpravidla známa, ve většině případů nepoužil. Anonymita mu totiž dodává dojem nepolapitelnosti. Úspěšná společnost si v reálné komunikaci zpravidla dokáže s nepravostmi poradit celkem obstojně, ale podlé a zákeřné postupy, které se vymykají z rámce tradičního chápání světa, mohou i jí nadělat nemalé vrásky.

1.1.4. OCHRANA NÁRODNÍHO KYBERNETICKÉHO PROSTORU

Pro účinný postup bezpečnostních institucí proti bezpečnostním hrozbám v kyberprostoru je nezbytná široká mezinárodní spolupráce těchto institucí i s dalšími subjekty, které se zabývají vývojem nových technologií. Vedle sledování aktuálních směrů směřuje spolupráce proti cílenému napadání nebo poškozování informačních a komunikačních systémů. Ochrana národního kybernetického prostoru je problematika, která je ošetřena jednak legislativně a dále pak na úrovni organizace aplikací příslušných opatření v praxi. Legislativní rámec je dán zákonem č. 181/2014 Sb, o kybernetické bezpečnosti, který je závazný pro organizace – viz vyhláška č. 315/2014 Sb. a vyhláška č. 317/2014 Sb.



Obrázek 1 - Zákon o kybernetické bezpečnosti

Zdroj: upraveno NSMC podle NBÚ[2]

Opatření, mimo těch, která jsou nezbytnou součástí řádného budování bezpečnosti vlastních informačních systémů povinných subjektů i soukromoprávních entit, stojí především na ustavení a organizaci rámce spolupráce, komunikace a výměny informací mezi těmito subjekty navzájem a mezi státem pověřenými nebo zřízenými pracovišti pro koordinaci kybernetické bezpečnosti. Rovněž také uložením povinnosti účastníkům kybernetického života spolupracovat a aplikovat vhodná nebo doporučená opatření.

1.1.5. CERT/CSIRT[3]

[2] Převzato z: CERT/CSIRT Týmy a jejich role, A. Kropáčová, 2013. Dostupné na: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/.
[3] Převzato z: CERT/CSIRT Týmy a jejich role, A. Kropáčová, 2013. Dostupné na: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/.

Posun ve vnímání problému kyberkriminality je také možné spatřit ve zřizování nových organizací, které se aktivně zabývají ochranou kyberprostoru. Jako příklad je možné uvést budování CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team) týmů a Národních center kybernetické bezpečnosti (NCSC) po celém světě a snahu tyto útvary definovat po stránce obecného fungování (pole působnosti, poskytované služby, komunikační pravidla apod.) a vazeb, po stránce legislativní a zaintegrovat je do struktur pro krizové řízení v případě ohrožení státu.

1.1.6. CSIRT TÝMY

Osvědčeným nástrojem v boji proti kybernetickým hrozbám je sdružování odborníků v týmech nebo komunitách. S ohledem na potřebu koordinovaného postupu a akceschopnost v situacích, kdy je třeba aplikovat nějaká opatření nebo jen jednoduše procesně opakovatelným způsobem sdílet určité informace v nějakém ohraničeném rozsahu a cílové skupině, je takový přístup jednoduše jedním z vyzkoušených. V rámci boje proti kyberkriminalitě jsou takovým nástrojem týmy typu CERT (Computer Emergency Response Team) nebo CSIRT (Computer Security Incident Response Team). Vývojově i významově se sice vzájemně poněkud odlišují, ale ve skutečnosti lze dnes chápat obojí v podstatě jako ekvivalent, tedy tým, který je v rámci své působnosti odpovědný za řešení bezpečnostních incidentů dané komunity (ať už se jedná o komunitu uživatelů nebo dalších týmů). Jedná se tedy o místo, kam lze poskytovat a současně také kde lze hledat spolupráci při zjištění nebo podezření na bezpečnostní incident v rámci dané komunity.

CSIRT týmy jsou ustavovány zejména na úrovni jednotlivých organizací. Může se jednat například o poskytovatele internetových služeb (zpravidla ISP, poskytovatelé obsahu a další), nebo také o organizace, které těchto služeb využívají (podniky, banky, apod.) Základní úlohou CSIRT týmu je pak zejména spolupráce při řešení vzniklých incidentů. Tým zpravidla řeší to, co se vyskytne v rámci jeho pole působnosti a také to, co dokáže sám reálně ovlivnit.

Fakticky se ale jedná o postup, který fungoval již odedávna, jen méně formálně. Například administrátoři dvou systému si mezi sebou vyměňovali poznatky o vadách a problémech. Tento typ komunikace se tedy jen více zformalizoval. Rozdíl je především v tom, že týmy CSIRT se propojují do světové bezpečnostní infrastruktury, kde sdílejí informace a dodržují společné postupy ve společné věci poněkud formálněji. Základním a pochopitelným požadavkem komunity je, aby CSIRT tým zveřejnil své kontaktní informace a pravidla činnosti. Tedy to, kdo jsou členové, jaké mají kompetence, jak a kdy je možné tým zastihnout, rozsah, ve kterém je tým způsobilý konat a jakým způsobem, tzn. definování jeho pravomocí a odpovědnosti. Na základě pole své působnosti je potom tým kontaktován (např. napadenými) a řeší jemu příslušející problémy (incidenty).

Odvisle od kompetencí a možností řešení problémů (eliminace útoku, dohledání pachatele, obnovení provozu služby) můžeme identifikovat v zásadě dva typy týmů - interní (institucionální) nebo koordinační. Tým interního typu má obvykle možnost přímého zásahu (odpojit zdroj problému, zavést filtraci síťového provozu apod.), tým koordinačního typu možnost přímého zásahu nemá, jeho činnost se soustřeďuje na komunikaci, spolupráci a zprostředkování informací.[4]

Při řešení konkrétního incidentu, se ho účastníci zpravidla snaží řešit přímo u zdroje, tedy tam, kde je to ke zdroji nebo cíli incidentu nejblíže a lze co nejefektivněji zasáhnout. To je poměrně jednoduchá situace tehdy, když zdroj i cíl jsou v poli působnosti nějakého CSIRT týmu, protože je velmi jednoduché a rychlé najít konkrétního odborníka v místě problému. Ten potom také dokáže problém řešit a jeho reakce jsou předvídatelné, neboť pravidla pro to sám dobrovolně zveřejnil. Tento postup de facto horizontálního sdílení informací je velmi efektivní v tom, že komunikace nemusí nutně procházet různými úrovněmi komunikační hierarchie a je rychlá a přesná. Problém zpravidla nastává tehdy, kdy napadený nemůže nalézt odpovídající protějšek (ať už proto, že neexistuje, nedává o sobě žádné použitelné informace, odmítá problém řešit nebo prostě nereaguje). V takovém případě se pak ukazuje jako výhoda, pokud existuje někdo, kdo dokáže „zapůsobit.“ V minulosti tlak

[4] Převzato z: CERT/CSIRT Týmy a jejich role, A. Kropáčová, 2013. Dostupné na: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/.

komunity a okolí zpravidla pomohl celkem účinně zapůsobit na řešení problému, ale bylo to často pomalé a postupy pro řešení situací nebyly moc univerzálně opakovatelné a někde prostě nezabralo ani to. V tomto kontextu bylo třeba zajistit odstranění tak slabého místa komunikace a zde mají svou důležitou roli týmy národní a vládní.

1.1.7. HIERARCHIE?[5]

CERT/CSIRT týmy žádnou oficiální hierarchii, která by jeden tým činila nadřazeným jinému týmu, nemají. Všechny týmy jsou z hlediska komunikace, spolupráce a výměny informací rovnocenné a nejsou v těchto oblastech nijak limitovány. Je pravda, že existence národních a vládních týmů trochu evokuje, že nadřazenost mezi týmy existuje, ale není tomu tak. Jedinou „nadřazenost", ale spíše by bylo na místě říci „větší akceschopnost", může vrcholovému týmu dát legislativa, která upraví jeho pravomoci třeba v oblasti požadované reakce ze strany provozovatelů sítí, služeb apod.

Ve světě CSIRT/CERT týmů je klíčová ochota sdílet důležité informace o incidentu a hrozbách. K tomu je nezbytné, aby si týmy navzájem důvěřovaly a také aby svým týmům věřili uživatelé. Získat důvěru uživatelů a komunity je běh na dlouhou trať. Týmy musí své kvality dokazovat při všech aspektech své činnosti a důvěryhodnost si musí budovat postupně. A to nejen schopností pomoci, ale také schopností zajistit důvěrnost sdílených dat a korektní zacházení s nimi, transparentností chování apod. Při misi budování důvěryhodnosti je nesmírně důležitý osobní kontakt a výměna zkušeností.

1.1.8. …A TI OSTATNÍ

Nařízením Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, byla zřízena

[5] Převzato z: CERT/CSIRT Týmy a jejich role, A. Kropáčová, 2013. Dostupné na: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/.

evropská agentura pro elektronickou a informační bezpečnost ENISA. Funguje od 1. září 2005 a sídlí v Řecku ve městě Hérakleion na ostrově Kréta.

Posláním této agentury je zvyšování schopnosti EU, zemí EU a průmyslu předcházet obtížím v oblasti bezpečnosti sítí a informací, zvládat je a reagovat na ně.

Kromě toho ENISA poskytuje podporu a poradenství Komisi a zemím EU. Může být také požádána, aby podpořila Komisi v technické přípravné práci pro aktualizaci a rozvíjení právních předpisů EU.

ENISA dále podporuje a prohlubuje spolupráci různých subjektů činných ve veřejném i soukromém sektoru pro dosažení dostatečně vysoké úrovně bezpečnosti v zemích EU.

Pro dosažení svých cílů ENISA[6]:

- shromažďuje potřebné informace pro analýzu stávajících a vznikajících nebezpečí a poskytuje výsledky zemím EU a Komisi;
- poskytuje Evropskému parlamentu, Komisi, příslušným evropským nebo vnitrostátním subjektům poradenství a na žádost i podporu;
- podporuje spolupráci různých subjektů činných v oblasti (mimo jiné pořádáním konzultací a vytvářením sítí);
- usnadňuje spolupráci mezi Komisí a zeměmi EU při rozvoji společných metod předcházení obtížím v oblasti bezpečnosti;
- přispívá k budování povědomí o dostupnosti včasných, objektivních a úplných informací o otázkách bezpečnosti sítí a informací pro všechny uživatele (mimo jiné podporou výměny osvědčených postupů, včetně metod varování uživatelů, a slaďováním iniciativ veřejného a soukromého sektoru);
- je nápomocna Komisi a zemím EU v dialogu s průmyslem, aby se věnovaly bezpečnostním otázkám technického a programového počítačového vybavení;

[6] Převzato z: http://europa.eu/legislation_summaries/information_society/internet/l24153_cs.htm.

- sleduje vývoj norem pro produkty a služby v oblasti bezpečnosti sítí a informací a podporuje opatření pro posuzování a řízení rizik;
- přispívá k úsilí EU spolupracovat se zeměmi mimo EU a s mezinárodními organizacemi, aby byl prosazován globální přístup k otázkám bezpečnosti;
- formuluje své závěry, doporučení a poskytuje poradenství.

Agentura je aktivním participantem přípravy právních předpisů EU a orientuje se průřezově na všechny aspekty kybernetické bezpečnosti.

Kontrolní otázky

Kontrolní otázky slouží k ověření nastudovaných znalostí. Jsou součástí testu po prostudování každé kapitoly, kde jsou uvedeny i správné odpovědi.

Co je to CERT?

a) Zkratka pro elektronický zabezpečovací systém.
b) Tým, který je v rámci své působnosti zodpovědný za řešení bezpečnostních incidntů dané komunity.
c) Sdružení výrobců antivirových programů.

Co je to ENISA?

a) Evropská agentura pro bezpečnost sítí a informací.
b) Evropská agentura pro vzdělávání v oblasti kybernetické bezpečnosti.
c) Evropská agentura pro elektronické bankovnictví.

Co je to ČSN ISO/IEC 27001:2014 ?

a) Jedná se o sytém řízení bezpečnosti informací.
b) Jedná se o systém řízení kontinuity činností organizace.
c) Jedná se o systém řízení kvality.

Co je to bezpečnostní politika?

a) Dokument, ve kterém jsou uvedena opatření implementovaná v rámci ISMS v organizaci.
b) Dokument, ve kterém jsou identifikována aktiva organizace.
c) Jedná se o jeden ze stěžejních dokumentů organizace při zavádění ISMS. Jsou v něm uvedeny hlavní zásady a cíle, bezpečnostní potřeby, práva a povinnosti.

Co je to SOA - Prohlášení o aplikovatelnosti?

a) Dokument, ve kterém je zpracována bezpečnostní politika organizace.
b) V tomto dokumentu jsou uvedena opatření, která organizace aplikuje při zavádění ISMS.
c) Dokument, ve kterém jsou identifikována aktiva organizace.

Co je to riziko?

a) Jedná se o pravděpodobnost, že hrozba zneužije zranitelnosti.
b) Jedná se o pravděpodobnost, že zranitelnost zneužije hrozby.
c) Jedná se o pravděpodobnost, že aktivum zneužije zranitelnosti.

Co je aktivum?

a) Je to něco, co má pro organizaci hodnotu (např. dokumenty, SW, HW).
b) Je to něco, co nemá pro organizaci hodnotu.
c) Je to něco, u čeho si nejsme jisti hodnotou pro organizaci.

Co je hrozba?

a) Je to pravděpodobnost, že riziko zneužije aktivum.
b) Je to pravděpodobnost, že aktivum zneužije hrozbu.
c) Potenciální příčina incidentu, která může mít za následek poškození systému nebo organizace.

Co je zranitelnost?

a) Je to pravděpodobnost, že aktivum zneužije hrozbu.
b) Slabá stránka aktiva, která může být zneužita jednou nebo více hrozbami.
c) Je to pravděpodobnost, že riziko zneužije aktivum.