Moje otázky PV017

1. Příklad na určení velikosti úrovně rizik. (přesné zadání si nepamatuji)?

úroveň rizika= F(pravdepodobnosť útoku)\* F’(dopad útoku)

pravdepodobnostný charakter rizika:

1.(L, Low) zanedbateľný výskyt útoku

2.(M, Medium) bežný výskyt útoku

3.(H, High) výskyt útoku hraničiaci s istotou

Dopad útoku

1.(L) zanedbateľný/akceptovateľný

2.(M) bežný

3.(H) katastroficky

Riziko

(L) akceptovateľné - súčin = 1 alebo 2

(M) bežné – súčin = 3 alebo 4

(H) katastrofické – súčin = 6 alebo 9

2. Charakterizujte hlediska, ze kterých se posuzuje úroveň záruky za bezpečnost (Security assurance requirement) SAR?

SAR- je treťou častou ISO/IEC 15408

-popis ako spoľahlivo sa majú SFR implementovať, obsahuje časť III kriterií, výčtové zoznamy pre vývojárov/hodnotiteľov, popisy opatrení prijímaných behom vývoja/hodnotenia produktu s cieľom vyhovenia/dokázania deklarovanej bezpečnostnej funkčnosti, napr. požaduje sa prevedenie úplného otestovania funkčnosti

-úroveň splnenia požiadavkou na záruku determinuje zaradenie predmetu hodnotenia(TOE) na konkrétnu úroveň záruky- Evaluation Assurance Level (EAL) 0,1,...,7 -numerické škálovanie podľa dosiahnutého plnenia rôzne silných požiadavkou na bezpečnosť

-jedna sa o definíciu kriterií pre stanovenie/hodnotenie profilu ochrany(PP) a bezpečnostných cieľov (ST) z hľadiska: Správy konfigurácie, Sprievodnej dokumentácie, Posúdenia zraniteľnosti, Dodania a prevádzky, Podpory životného cyklu, Zaisťovania údržby, Vývoja a Testovania

3. Popište vztahy mezi aktivum, riziko, útočník, zranitelné místo, hrozba, útok?

aktivum- cokolvek co ma pre organizaci nejaku hodnotu

riziko- možnost vyskytu utoku

utočník- ten kto vyuzije nedokonalost v bezpecnostnej ochrane

zranitelne miesto- slabina v navrhu, implementaci, provozu... systemu ktory obhospodaruje

aktiva

hrozba- reprezentuje potencionalny motivaci k utoku

útok- realizacia hrozby

Utocnik ma zaujem o aktiva ktore maju pre neho nejaku hodnotu. Preto hlada zranitelne miesto v systeme aby ho mohol vyuzit pre ich ziskanie. Utocnik vytvara hrozbu pretoze chce ziskat aktiva ktore mu nepatria. Pokus o ziskanie tychto aktiv je utok, realizuje sa hrozba. Riziko hovori o tom aka je pravdepodobnost ze sa nejaky utocnik pokusi o utok.

4. Stručně popište po krocích proces řešící zvládání rizik?

1.krok- zoradenie plánovaných implementačných akcií podľa úrovne odpovedajúcich rizík

(od najvyšších po najnižšie), výstup: zoznam s poradím akcií

2.krok- zhodnotenie volieb doporučených opatrení, hodnotí sa realizovateľnosť volieb

(kompatibilita, prijateľnosť pre užívateľa...) a analyzuje sa efektívnosť volieb

opatrení, Výstupom je zoznam realizovaných opatrení

3.krok- analýza potrebných nákladov na implementáciu opatrení a potenciálneho zisku,

demonštrácia, že náklady sú ospravedlniteľné znížením rizika

4.krok- finálny výber najefektívnejších opatrení, môžu kombinovať technické, provozné,

riadiace rysy, výstupom: zoznam vybraných opatrení

5.krok- pridelenie zodpovednosti za implementáciu vybraných opatrení skúseným ľudom

(expertom), výstup: zoznam zodpovedných osôb za implementáciu

6.krok- vypracovanie podrobného plánu implementácií(riziko, úroveň rizika, doporučené

opatrenia, priorita implementácie, vybrané plánové opatrenia, potrebné zdroje,

zodpovedná osoba, data začiatku a ukončenia implementácie. požiadavky na

údržbu opatrení)

7.krok- implementácia opatrení

5. Popište metody hodnocení objektu při auditu?

-Vyšetrovanie: kontrola, skúmanie alebo analýza objektov s cieľom porozumieť alebo získať dôkazy; je možné čiastočne automatizovať

-Interview: rozhovor s jednotlivcami alebo skupinami v organizácii s cieľom zistiť, kde získať dôkazy; nie je možné automatizovať Hodnotí sa aj nápomocnosť zamestnancov auditorom

-Test: cvičná prevádzka objektu za definovaných podmienok s cieľom porovnať skutočné a očakávané chovanie objektu; je možné automatizovať Musí byť opakovateľný, reprodukovateľný a vykonávaný odborníkmi

-Vyšetrujú sa špecifikácie (politiky, plány, dokumentácia) mechanizmy (HW, SW, reakcie na incidenty) a procesy(prevádzka systému, administrácia, riadenie)

6. Popište minimální dokumentovou základnu ISMS?

ISMS(Information Security Management System) = komplexný systém riadenia informačnej bezpečnosti šitý na mieru konkrétnej organizácii

Dokumentácia ISMS musí odpovedať ISO 27001 a musí obsahovať:

• Definíciu oblasti, definíciu politiky inf. bezp., výsledky ohodnotenia rizík, SoA

•Popis riadiacej štruktúry projektu ISMS – odpovedá organizačnej schéme organizácie

•Zápisy z jednaní vedenia – dôkazy akcií

•Plán zvládania rizík + zodpovednosti a požadované akcie ISMS =

manuál ISMS prístupný všetkým zamestnancom

4 vrstvy dokumentovej základne ISMS (od najvyššej):

•Politiky(vrcholový management) – stratégie, princípy, plán zvládania rizík, SoA,napr. politika riadenia prístupu – stabilné dokumenty autorizované správnou radou

•Procedúry(výkonný management) – popisujú implementáciu politík, napr. „práva pre užívateľov sú r, w, x“; autorizuje ich Chief of Security Officer (CSO)

•Návody(prevádzka) – požiadavky na vykonávanie špecifických úloh,ktoré vyplývajú z procedúr, popis práce, „individual user agreement“; autorizuje ich CISO

•Správy(všetci) – zber dát, záznamy, dotazníky, formuláre, výsledky auditov

Štruktúra manuálu ISMS:

•Úvod - kto, kedy, prečo manuál vydal, popis obsahu, princípy, SoA...

•Vymedzenie oblasti

•4 vrstvy dokumentovej základne

•Popis postupu v rámci cyklu PDCA, výstupy jednotlivých etáp

•Politika informačnej bezpečnosti

•Popis organizačných štruktúr a rolí

•Zoznam, vlastníci, použitie a klasifikácia aktív

•Bezpečnosť ľudských zdrojov

•Fyzická a areálová bezpečnosť

•Riadenie komunikácie a prevádzky IS (napr. zálohovanie)

•Riadenie prístupu (cez sieť, k OS, k informáciám)

•Plán činnosti po útoku

•Plán zachovania kontinuity činnosti (Business Continuity Plan)

•Súlad s právom a štandardm

1. Popsat, jaký je vztah mezi: aktiva, hrozba, zranitelnost, útok, útočník, riziko, opatření  
vid vyššie

2. Co se rozumí celkovou politikou bezpečnosti informací v organizaci?  
súhrn bezpečnostných zásad pre ochranu informačných aktív, vyjadruje sa obvykle neformálne, v prirodzenom jazyku(použitím matematického jazyka je možné dosiahnuť najvyššiu dôveryhodnosť ale použiť sa dá len zriedka)  
ČO sa chráni(aké aktívum) a KTO to chráni- stanovenie bezp. cieľov  
PROTI KOMU/COMU sa to chráni, kto je potencionálny útočník, ako a prečo môže útočiť  
AKO sa chráni- spôsob uplatňovania opatrení potrebných pre dosiahnutie požadovanej úrovne  
KDE sa chráni- vymedzuje štruktúru organizácie, chránenú oblasť  
má vyhovovať bezpečnostnej politike organizácie, je nezávislá na konkrétnych IT,

4. Security vs safety  
SAFETY- stav bytia v chránenej oblasti, v ktorom je zaistená ochrana proti fyzickému, sociálnemu, duchovnému, finančnému, politickému, emocionálnemu, pracovnému, psychologickému, vzdelávaciemu alebo inému typu alebo dôsledku zlyhania, poškodenia, chyby, nehody alebo inej udalosti ktorá by mohla byť požadovaná za nežiadúcu, Bezpečie môže mať podobu chránenia osôb alebo hmotných či nehmotných hodnôt pred udalosťami alebo vystavením skutočnostiam spôsobujúcim zdravotné, ekonomické... straty, Stav keď platí že za definovaných podmienok niekto alebo niečo nespôsobí škodu  
SECURITY- chránenie proti úmyselným škodám, chránenie pred poškodením osôb alebo hmotných či nehmotných hodnôt(aktív) v dôsledku úmyselných činov ako sú prepadnutie, vlúpanie alebo vandalizmus, Informačná bezpečnosť- ochrana proti úmyselným škodám a nežiadúcim akciám na informačných aktívach

1) napište vhodný diagram reakce na bezp. událost

???

2) popište procesy v jednotlivých fázach PDCA

PDCA alebo Plan-Do-Check-Act

PLAN- definícia oblasti ISMS, Definícia politiky informačnej bezpečnosti, Definícia

systematického prístupu k ohodnocovaniu rizík, Vypracovanie procedúr riešiacich ohodnotenie rizík a prevedenie ohodnotenia rizík, Identifikácia a vyhodnotenie možnosti ako zvládať riziká, Výber cieľu ochrany a implementovatelné opatrenia pre každú možnosť, Vypracovanie Prehlásenia o aplikovateľnosti vybraných opatrení  
DO- formulácia plánov zvládania rizík- vytvorenie dokumentácie tohto plánu, Implementácia plánu zvládania rizík vrátane opatrení, Zaškolenie relevantných zamestnancov, definícia programu systematickej výchovy k bezpečnostnému uvedomeniu, Zaistenie zdrojov a operácii pre výkon činnosti ISMS, Implementácia procedúr umožňujúcich promtnú detekciu bezpečnostných incidentov a reakcie na ne  
CHECK- trvalý proces monitorovania, inšpekcie, testovania, auditu ISMS v jeho bežnom provoze, Trvalý proces skúmania dôkazových materiálov vedením organizácie,   
ACT- Identifikácia a dokumentovanie potrebných zdokonalení ISMS

3) popište metodologie ohodnocení rizik a vstupy a výstupy jednotlivých fázi ohodnocení

Metodológie:

-Elementárne ohodnotenie rizík- prevzatie opatrení na základe analógie podobných systémov

a zo všeobecných štandardov

-Neformálne ohodnotenie- ohodnotenie rizík na základe znalostí jednotlivcov- odborníkov na

bezpečnosť bez použitia štandardných štruktúrovaných metód a nástrojov

-Detailné ohodnotenie- ohodnotenie rizík štandardnými štruktúrovanými metódami

a nástrojmi vo všetkých fázach(Identifikácia aktív, zraniteľných miest...)

-Kombinované ohodnotenie- ako je to kde nutné sa použije elementárne, neformálne alebo

detailne ohodnotenie rizík

ohodnotenie rizík tvoria podprocesy: Identifikácia rizík, Analýza rizík a Vyhodnotenie

Identifikácia zraniteľností- účelom určiť, čo by mohlo spôsobiť škodu a pochopiť ako môže ku škode dôjsť

Vstup: správy z predchádzajúcich ohodnotení, výsledky auditov, požiadavky na bezpečnosť

výsledky testov bezpečnosti, publikované skúsenosti...

Výstup: správa obsahujúca zoznam potencionálnych zraniteľností v oblastiach riadenia,

provozu a technického zabezpečenia  
Identifikácia hrozieb- identifikácia potencionálnych hrozieb a vypracovanie správy obsahujúcej zoznam aplikovateľných hrozieb

Vstup: história útokov na systém, dáta od spravodajských služieb, odborné médiá

Výstup: správa o hrozbách obsahujúca zoznam hrozieb, kt. by mohli využiť zraniteľnosť

Analýza Odhad škôd spôsobených úspešným útokom

Vstup: analýza dopadov na podnikateľské procesy, dokumentácia organizácie- analýza

dopadov podnikateľskej činnosti a kritické ohodnotenie aktív

Výstup: škálovacia stupnica dopadov

Vyhodnotenie  
 Vstup: pravdepodobnosti uplatnenia hrozieb, hodnoty dopadov, adekvátnosť sučasných

a už plánovaných opatrení

Výstup: rizika a súvisiace úrovne rizík, zoznam rizík prioritne radený podľa kritérií

ohodnocovania rizík vo vzťahu k bezpečnosti incidentu

4) početný príklad s riziky

???

5) vlastnosti digitálnych dôkazov

Relevancia- musí byť možné dokázať, že získaný materiál sa vzťahuje k šetreniu, obsahuje

informácie napomáhajúce vyšetrovaniu konkrétnej udalosti a sú dobré dôvody pre to

aby bol získaný

Spoľahlivosť- všetky procesy použité pri manipulácii s potencionálnymi dôkazmi majú byť

auditovateľné a opakovateľné, výsledky musia byť reprodukovateľné

Dostatočnosť- detektív si musí byť vedomý, že zhromaždil dostatočné množstvo materiálu

umožňujúceho riadne vyšetrovanie, ktoré sa má previesť

Auditovateľnosť- DEFR/DES musí dokumentovať a zdôvodniť svoje akcie, aby nezávislý

pozorovateľ mohol zhodnotiť, či boli adekvátne

Opakovateľnosť- získavame rovnaké výsledky pri použití rovnakej metódy testovania,

rovnakých nástrojov a za rovnakých podmienok

Reprodukovateľnosť- získavame rovnaké výsledky pri použití rovnakej metódy testovania,

inými nástrojmi a za iných podmienok

Ospravedlniteľnosť- DEFR/DES musí zdôvodniť, že použité procesy boli správne a

nevyhnutné a iný DEFR/DES by to mal potvrdiť zopakovaním procesov

6) popište PP, strukturu a obsah

PP- Protection profile- Profil ochrán  
-dokument typicky vytváraný užívateľom alebo nejakou užívateľskou komunitou  
-identifikuje požiadavky na bezpečnosť pre isté prostredie  
-efektívne definuje triedu bezpečnostných zariadení, napr. použitie čipových kariet pre dosiahnutie nepopierateľnosti alebo sieťový firewall  
-PP ide použiť ako šablónu pre definíciu bezpečnostného cieľa  
-hodnotenie PP- prebieha pred formálnou deklaráciou PP relevantnou autoritou zodpovednou za bezpečnosť IT, cieľom hodnotenia je získanie istoty, že PP správne identifikuje požiadavky  
-Štruktúra:  
 -Úvod: orientačný popis riešeného problému v jazyku bežného užívateľa  
 -Popis zariadenia: účelu, chovania, štruktúry  
 -Bezp. problém: vlastnosti prostredia, hrozby  
 -Bezp. ciele  
 -Bezp. požiadavky: preklad bezp. cieľov do tech. požiadaviek, ktoré musia byť splnené  
 -Odôvodnenie bezp. cieľov

1.Popisat genericke kroky reakcie na vyskyt bezpecnostneho incidentu.

Plán a príprava- vypracovanie politiky správy bezp. incidentov, aktualizácia politik inf.

bezp., ustanovenie ISIRT, skolenie na správu incidentov, testovanie postupov

Detekcie bezp. udalosti a vypracovanie správy o nej- koncový užívateľ okamžite nahlasuje

incident na help desk

Posúdenie udalostí a vydanie rozhodnutí o incidente- posúdenie či bezpečnostná udalosť

reprezentuje bezpečnostný incident

Reakcia na incident- ak daná udalosť reprezentuje incident, reaguje ISIRT, prechod do

núdzového stavu, eliminácia šírenia útoku, odstavenie napadnutých častí od siete,

informovanie manažmentu, identifikácia zdroja útoku, vyšetrovanie, obnova stavu

Poučenie z incidentu- klasifikácia incidentu, vypracovanie záznamu, vedenie dôkazov, získanie skúseností ako vylepšiť inf. bezpečnosť, prehodnotenie rizík

2.Co sa rozumie celkovou politikou bezpecnosti informacii v organizacii?

Poziadavky na obsah tejto politiky.

vid vyššie

3.Charakterizujte kategorie poziadavkov na zaruku dosiahnutia bezpecnosti

informacii, ktorych splenenie sa dokazuje pri urcovani vysky zaruky za

specifikovanu funkcnu skladbu bezpecnostnych opatreni podla standardu ISO15408

(Common Crteria).

- **Security Functional Requirements** (SFRs, funkčne požiadavky)

o Čo TOE robí / má robiť? – ciele z hľadiska bezp. informácií

o Ktoré bezpečnostné funkcie je možne poskytovať?

o Poskytovane bezpečnostne funkcie vznikajú implementáciou SFRs

- **Security Assurance Requirements** (SARs, požiadavky zaručiteľnosti bezpečnosti)

o Je TOE urobený dobre a robí to čo ma?

o Ako spoľahlivo sa majú SFR implementovať, aké opatrenia sa prijímajú počas

vývoja? (napr. použitie verzovacieho systému zdrojových kódov)

o Definícia kritérií pre stanovenie/hodnotenie PP a ST z hľadisiek dokumentácie,

správy konfigurácie, dodania, prevádzky, podpory životného cyklu, údržby

o Úroveň splnenia požiadaviek určuje zaradenie TOE na konkrétnu úroveň

záruky, **Evaluation Assurance Level** (EAL) – od 0 po 7

**EAL1: funkčne testovaný TOE**

o Bezchybná prevádzka v súlade s dokumentáciou

o Hodnotenie bez účasti vývojára za minimálne náklady

- **EAL2: štrukturálne testovaný TOE (~ TCSEC C1)**

o Nízka až stredná záruka za bezpečnosť, nie je dostupná kompletná informácia o vývoji, ale vývojár poskytne špecifikácie o high-level návrhu bezp. funkcii

o EAL1 + overenie výsledkov testov od vývojára, analýza sily funkcii

o Napr. účtovný SW

- **EAL3: metodicky testovaný a kontrolovaný TOE (~ TCSEC C2)**

o EAL2 + Silnejšie testy bezp. funkcii, kontrola vývojového prostredia

o Napr. bankový SW pre styk so zákazníkmi

- **EAL4: metodicky navrhnutý, testovaný a preskúmaný TOE (~ TCSEC B1)**

o Najvyššia úroveň, ktorú je možné spätne dosiahnuť pre už existujúci produkt

o EAL3 + low-level návrh TOE, kontrola niektorých zdrojových kódov

o Windows 2000 SP3

- **EAL5: semi-formálne navrhnutý a testovaný TOE (~ TCSEC B2)**

o Prísne uplatnenie dobrej komerčnej vývojárskej praxe – napr. pre čipové karty

o EAL4 + úplná impl. TOE, analýza skrytých kanálov, semi-formálny návrh

- **EAL6: EAL5 so semi-formálne overeným návrhom (~ TCSEC B3)**

o EAL5 + modulárny a vrstvový návrh TOE, štruktúrovaná implementácia

o Pre ochranu aktív s vysokou hodnotou vo vysoko rizikových prostrediach

- **EAL7: EAL6, ale formálne navrhnutý a overený (~ TCSEC A)**

o Formálny model bezp. politiky, formálny detailný návrh, white-box testy

o Nezávisle potvrdenie výsledkov všetkých testov

4.Popisat elementarne kroky procesu ohodnotenia rizik.

-ohodnotenie rizík je získanie informácií pre účinné určenie/voľbu opatrení potrebných k zmene rizík na prijateľnú úroveň pomocou procesov, ohodnotenie rizík tvoria podprocesy: Identifikácia rizík, Analýza rizík a Vyhodnotenie

Identifikácia rizík:

-Identifikácia aktív- vypracovanie zoznamu aktív zahrnutých do oblasti a s nimi

súvisiacich relevantných podnikateľských procesov, identifikácia vzťahov, dopadov

a kritickosti

-Identifikácia zraniteľnosti- vypracovanie zoznamu zraniteľnosti aktív v oblasti na základe

info o aktívach, hrozbách a existujúcich opatreniach  
 -Identifikácia hrozieb- vypracovanie zoznamu hrozieb a ich zdrojov  
 -Identifikácia dopadu útokov/škôd – identifikácia možných škôd na základe znalosti aktív

a relevantných podnikateľských procesov, hrozieb a zraniteľnosti súvisiacich

s aktívami  
 -Identifikácia existujúcich a už plánovaných opatrení- vypracovanie zoznamu opatrení

a stavu ich používania/implementácie   
Analýza rizík:  
 -určenie veľkosti rizík  
 -Kvalitatívna- obvykle iniciálna analýza pre získanie prehľadu a indikácie hlavných rizík,

používa škály na odhad potencionálnych škôd a odhad frekvencií výskytu útoku  
 -Kvantitatívna- obvykle sa používa iba pre hlavné riziká, je založená na súčinoch

pravdepodobností útokov a numerickej výške škôd  
 -posúdenie dopadu škôd- zoznam škôd pre jednotlivé scenáre útokov na aktíva

rešpektujúce zvolené kritéria hodnotenia dopadov

-posúdenie pravdepodobnosti výskumu pre jednotlivé scenáre útokov- na kvalitatívnej

alebo kvantitatívnej bázy

Vyhodnotenie rizík:

-odvodenie úrovne rizík z odhadov pravdepodobnosti útokov a z odhadov očakávaných

strát porovnaním oproti stanoveným kritériam

5.Popisat fazy zivotneho cyklu ISMS a charakterizovat dielcie kroky plniace

jednotlive fazy. (ISMS project roadmap)  
PDCA

6.Aktiva: A, B, C, D. Potencialne skody pri utoku: 5000000, 50000, 1000,

10000. Intervaly vyskytu utookov: rok, tyzden, minuta, den. Navrhnut

klasifikaciu rizik. Popisat metodiku volby typu opatreni zaistujucich ochranu

pred relevantnymi rizikami.

zaradit a obkecat

1) Common criteria - popsat Protection Profile a Security Target

Protection Profile- určuje požiadavky na bezp. pre isté prostredie

-dokument vytváraný užívateľom(zákazníkom, zadávateľom)

-definuje triedu bezp. zariadení a generické požiadavky na ich bezpečnosť

-napr. sieťové firewally pre riadenie prístupu

- výrobok (TOE) ich môže certifikovať ako vyhovujúci PP

- môže byť použitý pre definíciu bezpečnostného cieľa

Security Target- definuje bezp. vlastnosti produktu

-dokument vytvorený výrobcom/vývojárom

-bezpečnostne vlastnosti poskytovane produktom, SFR

-súčasťou CC je štandardný katalóg týchto funkcií, ale žiadna nie je povinná

-výrobok (TOE) sa hodnotí podľa toho, ako splna SFR deklarované v ST

-je možné hodnotiť aj to, či ST vyhovuje zadanému PP

1, Zakladni a rozsirujici kriteria dle OWASP  
OWASP- The Open Web Application Security Project  
-štandard vývoja, testovania, hodnotenia a kritérií záruk bezpečnej webovej aplikácie