INTERNET CZ, a.s.

Forpsi Cloud

Riadenie rizík informačnej bezpečnostiy



OBSAH

1 Pojmy a definície 2
2 Hlavné referenčné normy 5
2.1 Norma ISO/IEC 27001 5
2.2 Norma ISO/IEC 27002 5
2.3 Norma ISO/IEC 27005 5
3 Metodika riadenia rizík informačnej bezpečnosti 6
4 Proces riadenia rizík 8
4.1 1. FÁZA – Stanovenie kontextu 8
4.1.1 Identifikácia služieb, procesov a makroprocesov 8
4.1.2 Identifikácia aktív 8
4.1.3 Vzťahy medzi makroprocesmi a aktívami 8
4.2 2. FÁZA – Analýza rizík 9
4.2.1 Posúdzenie vplyvov 9
4.2.2 Identifikácia a hodnotenie aktív 9
4.2.3 Analýza hrozieb a hodnotenie ich pravdepodobnosti 9
4.2.4 Analýza protiopatrení 10
4.3 3. FÁZA – Hodnotenie rizík 10
4.3.1 Model rizika a metodika 10
4.3.2 Platné bezpečnostné požiadavky a úroveň súladu 10
4.3.3 Výpočet inherentných a zvyškových základných rizík 11
4.4 4. FÁZA – Spracovanie rizika 11
4.4.1 Analýza prijatých rizík 11
4.4.2 Výsledky analýzy: zvyškové existujúce riziko 11
4.4.3 Analýza nedostatkov a výber protiopatrení 11
4.4.4 Plán spracovania rizika – racionalizácia intervencie 12
5 Frekvencia vykonávania analýz 12

INTERNET CZ, a. s.
Ktiš 2, 384 03 Ktiš IČO: 26043319 DIČ: CZ26043319
https://www.forpsicloud.cz - https://www.forpsicloud.sk

1 POJMY A DEFINÍCIE

Táto kapitola obsahuje niektoré definície, ktoré sa považujú za dôležité pre predstavenie modelu výpočtu a riadenia rizík informačnej bezpečnosti.

***BIA (analýza funkčných vplyvov)*:**

Analýza ekonomických, regulačných a reputačných vplyvov na podnikanie v súvislosti so stratou dôvernosti, integrity a dostupnosti informácií súvisiacich s daným procesom/službou a jej prerušením.

Dostupnosť:

Zabezpečiť, aby potrebné informačné systémy a údaje boli v prípade potreby k dispozícii na použitie.

Riadenie rizík informačnej bezpečnosti

Súbor činností a obchodných procesov určených na identifikáciu, meranie, zmierňovanie a monitorovanie rizík spojených so stratou dôvernosti, integrity a dostupnosti údajov a služieb.

Vplyv:

Negatívny dôsledok výskytu jednej alebo viacerých hrozieb.

Incident:

Udalosť súvisiaca s kybernetickou bezpečnosťou, ktorá má značnú pravdepodobnosť ohrozenia obchodných činností a ohrozenia informačnej bezpečnosti.

Integrita:

Ochrana údajov a informácií pred zmenami v ich obsahu, či už náhodnými alebo úmyselnými.

Hrozba:

Potenciálna príčina (úmyselná alebo náhodná) incidentu, ktorý by mohol poškodiť systém alebo organizáciu, čo by malo vplyv na **d**ôvernosť, **i**ntegritu a **d**ostupnosť informácií.

Typy hrozieb:

- Kybernetické hrozby – tieto hrozby majú negatívny vplyv na spoločnosť v dôsledku:
  - používania informačného systému alebo jeho komponentov (napr. útok hackerov),
  - vykonávania činností riadenia informačného systému (napr.: poškodenie internými pracovníkmi);
- Hrozby, ktoré nemajú kybernetický charakter – tieto hrozby majú negatívny vplyv na informačný systém spoločnosti v dôsledku toho, že:
  - majú priamy vplyv na poskytovanie služieb informačných systémov (napr. prírodné katastrofy, prerušenie služieb podpory);
  - ovplyvňujú spôsob riadenia informačného systému (napr. spôsob implementácie informačných procesov).

Ak chceme charakterizovať riziká spojené s každou hrozbou, musíme pochopiť:

- zraniteľnosťami komponentov informačného systému, alebo kde sa môžu naplniť hrozby;
- vystavenie komponentov hrozbe, inými slovami, ako ľahko sa hrozba naplní (napríklad server, ktorý vystavuje webovú službu zákazníkom, je viac vystavený útokom z internetu);
- typy následkov vzhľadom na to, že niektoré hrozby môžu byť „prostriedkom“ pre iné hrozby (napríklad neoprávnený prístup k webovému serveru môže útočníkovi umožniť krádež údajov, ale môže tiež umožniť vymazanie týchto údajov, ich zmenu, spáchanie podvodu atď.).

Možnosť alebo pravdepodobnosť výskytu:

Pravdepodobnosť, že sa môže vyskytnúť hrozba ovplyvňujúca jeden alebo viac informačných komponentov, ktorá môže mať počas určitého obdobia negatívny vplyv na podnikanie.

Riziko informačnej bezpečnosti (ďalej len „riziko“)

Kombinácia pravdepodobnosti výskytu hrozby a vplyvu na spoločnosť vo vzťahu k aktívam zahrnutým do analýzy. V závislosti od toho, kedy sú merané, môžno riziká definovať ako:

- Potenciálne alebo inherentné riziko (**rRp**):

  Maximálne riziko, ktorému je dané aktívum vystavené z hľadiska možnosti vytvorenia hrozby, ktorá môže mať vplyv na stratu dôvernosti, integrity a dostupnosti informácií. Všetky komponenty zapojené do analýzy služby prispievajú k určeniu inherentného rizika: procesy, aplikácie, údaje, infraštruktúry a v neposlednom rade ľudský faktor.

  V zásade ho predstavuje hodnota, ktorá sa vypočítava rôzne podľa použitej metodiky na základe súčtu všetkých možných hrozieb, ktorým je aktívum vystavené, s ohľadom na príslušné pravdepodobnosti výskytu a ich vplyv.

  Inými slovami, je to riziko, ktorému môže byť aktívum vystavené jednoducho kvôli svojej povahe a hrozbám s ňou spojeným. Napríklad počítač vystavený na verejnej sieti bez akýchkoľvek ochranných opatrení.

- Zvyškové riziko (**rRf**):

  Predstavuje riziko, ktorému môže byť služba vystavená po uplatnení protiopatrení na zníženie inherentného rizika.

- Konečné prijateľné riziko (**rRfa**):

  Predstavuje maximálny prah rizika prijateľný pre organizáciu.

Všetky uvedené hodnoty rizika treba považovať za dynamické, pretože sa v čase menia, keďže ich ovplyvňujú napríklad tieto prvky:

- vývoj hrozieb;
- zmena požadovaných úrovní služieb;
- zmeny v právnych ustanoveniach referenčných predpisov;

- organizačné zmeny, ktoré môžu mať vplyv na slabé stránky alebo pravdepodobnosť hrozieb, alebo zmeniť výsledný vplyv;
- posilnenie alebo oslabenie bezpečnostných protiopatrení.

Základné riziká:

Kybernetické riziká informačnej bezpečnosti spojených s každým aktívom a každým scenárom rizika.

Dôvernosť:

Ochrana údajov a informácií s cieľom zmierniť riziká spojené s neoprávneným prístupom k informáciám alebo ich používaním.

Cieľ bodu obnovy (RPO):

Týka sa prijateľnej straty údajov a predstavuje maximálne obdobie, ktoré uplynie od posledného uloženia dát z procesu a udalosťou, ktorá spôsobila zastavenia procesu.

Doba zotavenia (RTO):

Doba po incidente:

- za ktorú musí byť produkt alebo služba zotavená alebo
- za ktorú sa musí činnosť obnoviť alebo
- za ktorú sa musia zdroje obnoviť.

Scenár rizika:

Kombinácia dvoch alebo viacerých hrozieb, ktoré umožňujú ich klasifikáciu.

Zraniteľnosť:

Vlastný nedostatok procesu, služby alebo majetku, ktorý pri zneužití jednou alebo viacerými hrozbami umožňuje porušenie cieľov informačnej bezpečnosti (dôvernosť, integrita a dostupnosť). Patrí sem:

- neoddelené siete;
- používanie protokolov, ktoré nie sú chránené šifrovaním;
- operačné systémy, ktoré nie sú pravidelne aktualizované;
- databázy s nešifrovanými „citlivými“ údajmi;
- definície vírusov nie sú aktualizované;
- nemonitorovaný fyzický prístup;
- nedostatok automatických protipožiarnych systémov;
- nedostatočné záložné energetické systémy;
- atď.

2 HLAVNÉ REFERENČNÉ NORMY

V nasledujúcich odsekoch sú uvedené hlavné normy prijaté s cieľom zabezpečiť, aby vykonávané činnosti boli v súlade s medzinárodnými osvedčenými postupmi v oblasti bezpečnosti.

2.1 Norma ISO/IEC 27001

Norma ISO/IEC 27001:2013 predstavuje medzinárodnú bezpečnostnú normu a skutočný štandard na hodnotenie úrovne informačnej bezpečnosti, ktorý dokáže analyzovať technologické aj organizačné zložky, ktoré prispievajú k definovaniu systému riadenia informačnej bezpečnosti (ISMS).
Norma definuje požiadavky na ISMS a pomáha identifikovať, riadiť a minimalizovať rôzne hrozby, ktorým sú informácie pravidelne vystavované. Táto norma tiež stanovuje bezpečnostné kontroly, ktoré sa majú prijať na ochranu informácií tým, že sa zabezpečia pre zainteresované strany vrátane zákazníkov organizácie.

2.2 Norma ISO/IEC 27002

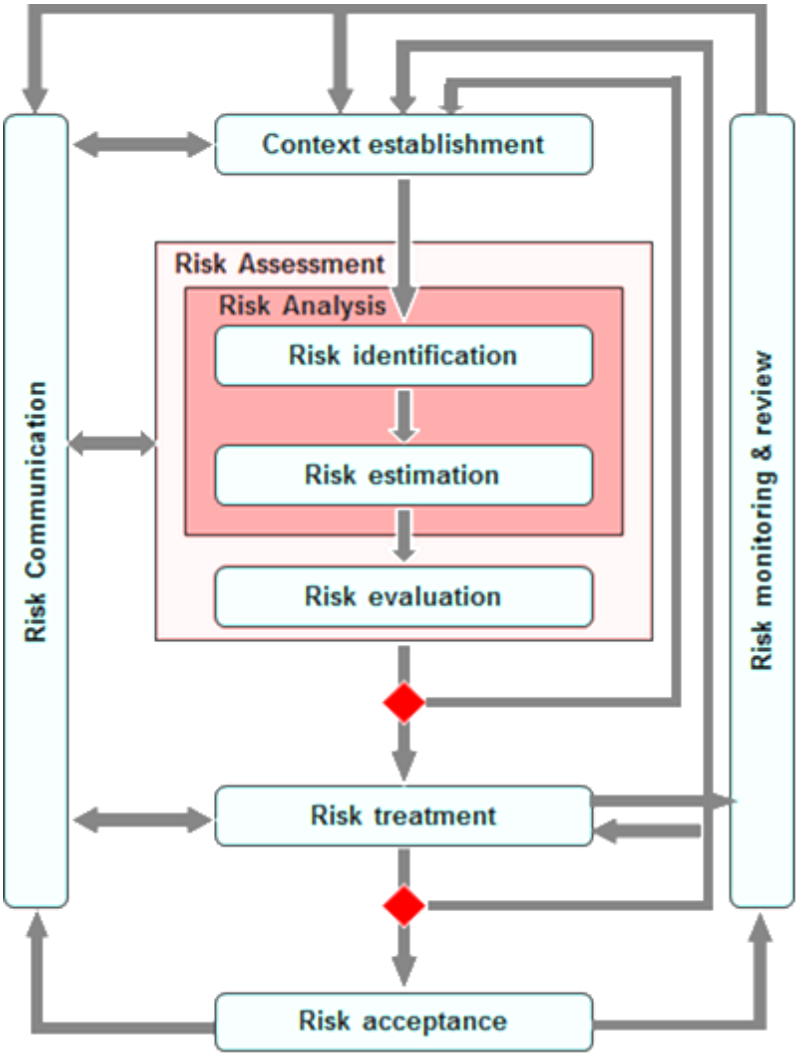
Norma ISO/IEC 27002:2013 definuje usmernenia a všeobecné zásady na zavedenie primeraného systému riadenia informačnej bezpečnosti v organizácii.
Norma ISO/IEC 27002:2013 predstavuje najmä medzinárodnú bezpečnostnú normu a skutočný štandard na posudzovanie organizačných, procedurálnych, technologických a regulačných aspektov bezpečnosti informačného systému s cieľom:

- kriticky vyhodnocovať služby a funkcie, ktoré príslušný systém už má alebo by mal mať;
- poukázať na slabé miesta systému;
- uviesť vhodné opatrenia na dosiahnutie úrovne bezpečnosti definovanej v cieľoch.

Je potrebné poznamenať, že norma ISO/IEC 27002 identifikuje bezpečnostné kontroly, ktoré by mala organizácia zvážiť, ale nenahrádza samotnú analýzu rizík.

2.3 Norma ISO/IEC 27005

Norma ISO/IEC 27005 opisuje proces riadenia rizík informačnej bezpečnosti a súvisiace činnosti, ktoré podporujú všeobecné zásady obsiahnuté v norme ISO/IEC 27001.
Norma má v súlade s normou ISO 31000 pomôcť spoločnostiam riadiť riziká informačnej bezpečnosti podobným spôsobom, akým riadia iné typy rizík.
Na obrázku 1 je znázornený proces riadenia rizík navrhnutý v norme ISO/IEC 27005:11, ktorý inšpiroval model prijatý a vyvinutý skupinou Aruba.



Obrázok 1 – ISO/IEC 27005: Proces riadenia rizík

3 METODIKA RIADENIA RIZÍK INFORMAČNEJ BEZPEČNOSTI

Pre skupinu Aruba S.p.A. predstavujú informácie aktívum, ktoré si vyžaduje starostlivé riadenie a ktoré je strategické pre ochranu a rozvoj podnikania spoločnosti.

V tejto súvislosti možno kybernetické riziko definovať ako akúkoľvek neistú udalosť, ktorá by mohla ohroziť jednu alebo viacero z nasledujúcich troch hlavných vlastností informačných aktív spoločnosti:

- **d**ôvernosť (údaje sú prístupné neoprávneným osobám),

- **i**ntegrita (údaje môžu podliehať neoprávneným zmenám a môžu sa meniť),
- **d**ostupnosť (počítačový systém sa nedá používať).

v závislosti od úrovne závažnosti, ktorá je prísne závislá od typu ovplyvnených informácií.

Hodnotenie rizík zohľadňuje nasledujúce možné typy vplyvu:

- ekonomický,
- regulačný,
- reputačný.

Riadenie rizík informačnej bezpečnosti je proces posudzovania vzájomných vzťahov medzi aktívami, hrozbami a zraniteľnosťami v organizácii. Cieľom tohto analytického procesu je identifikovať riziká spojené so zraniteľnosťami a hrozbami, ktoré sa nachádzajú v aktívach, a poskytnúť základ pre definovanie účinného bezpečnostného programu.

Posudzované kategórie rizík musia byť v súlade s typmi uplatniteľnými v danom kontexte. Posudzované riziká preto môžu pochádzať buď z vnútorných, vonkajších alebo environmentálnych hrozieb, ako aj z úmyselných činov alebo nedostatočného organizačného riadenia alebo nedbanlivosti jednotlivcov.

Hodnota rizika sa chápe ako funkcia hodnoty príslušných aktív, hodnoty hrozieb a zraniteľností.

Výsledky analýzy rizík sú zdokumentované a zahŕňajú:

- Jasná identifikácia kľúčových rizík;
- hodnotenie potenciálnych vplyvov, ktoré by každé z identifikovaných rizík mohlo mať na podnikanie;
- Plán odporúčaných opatrení na zníženie rizík a ich vrátenie na prijateľnú úroveň.

Skupina Aruba vytvára model kvalitatívnej analýzy, pretože dokáže okamžite poskytnúť vysoký stupeň povedomia o hlavných rizikách informačných a komunikačných technológií, ktoré ovplyvňujú dané technologické prostredie.

Prijatá metodika je nasledovná:

- Skupina Aruba ich používa na odhad hodnoty informácií v príslušných procesoch a úrovne rizika, ktorému sú vystavené, aby bolo možné prijať vhodné ochranné opatrenia.
- Uplatňuje sa aj pri vývoji nových infraštruktúrnych alebo aplikačných riešení, ktoré majú vplyv na bezpečnosť spravovaných údajov. V tomto prípade metodika umožňuje posúdiť, nakoľko kritické sú údaje a hrozby, ktorým sú vystavené, aby osoby zodpovedné za analýzu rizík mohli pri vývoji a obstarávaní počítačových systémov zaviesť vhodné ochranné opatrenia na minimalizáciu zraniteľnosti.

Hodnotenie rizika a analýza korelácií medzi aktívami, hrozbami a protiopatreniami sa vykonáva s podporou interne vyvinutého nástroja s využitím informácií zhromaždených počas špecifických stretnutí s rôznymi jednotlivcami zapojenými do analyzovaných procesov.

Metodika znamená, že je možné vytvoriť obchodný model, v ktorom sú popísané všetky základné prvky potrebné pre následné analýzy spolu s ich charakteristikami, hierarchickou štruktúrou a súvisiacimi spojeniami.

4 PROCES RIADENIA RIZÍK

Nižšie sú opísané hlavné fázy analytického modelu pre riadenie rizík spojených s informačnou bezpečnosťou, ktoré prijala a uplatňuje skupina Aruba S.p.A.

4.1 1. FÁZA – Stanovenie kontextu

Definovanie kontextu analýzy zahŕňa modelovanie situácie spoločnosti a identifikáciu hlavných podnikových služieb, procesov, makroprocesov a aktív.

Pokiaľ ide o identifikáciu zdrojov, ako navrhuje norma ISO/IEC 27005 „Informačné technológie – bezpečnostné techniky – riadenie rizík informačnej bezpečnosti“, zvažujú sa dva odlišné typy:

- **Primárne zdroje** – informácie, procesy, makroprocesy a obchodné služby;
- **Sekundárne zdroje alebo aktíva** – hardvér, softvér, personál, sieť, umiestnenie a organizácia.

4.1.1 Identifikácia služieb, procesov a makroprocesov

Pokiaľ ide o identifikáciu služieb a procesov organizácie, ako prvotné referencie sa používajú organizačné štruktúry zverejnené a sprístupnené prostredníctvom nástroja internej podnikovej komunikácie.
Následne sú jednotlivé procesy, ktoré prispievajú k poskytovaniu služieb, zoskupené do makroprocesov špecifických pre analyzovaný kontext.

4.1.2 Identifikácia aktív

V záujme presnej identifikácie aktív postupujeme takto:

1. **Identifikácia kategórií** informačných aktív (napr. hardvér, softvér, umiestnenie atď.) podľa klasifikačného systému vymedzeného v norme ISO/IEC 27005.
2. **Vyhodnotenie kategórií** informačných aktív podľa bezpečnostnej stratégie spoločnosti a obchodných, právnych a zmluvných požiadaviek.
3. **Identifikácia závislostí** medzi kategóriami aktív, ktoré boli kategorizované.

4.1.3 Vzťahy medzi makroprocesmi a aktívami

Po identifikácii aktív sa definujú závislosti medzi nimi a makroprocesmi.

Tieto závislosti znamenajú, že hodnoty vplyvu na dôvernosť, integritu a dostupnosť môžu byť priradené ku každej kategórii aktív (určené prostredníctvom rozhovorov BIA), aby bolo možné vypočítať základné kybernetické riziká spojené s každým aktívom.

4.2 2. FÁZA – Analýza rizík

4.2.1 Posúdzenie vplyvov

Posúdenie vplyvu (angl. Business Impact Analysis) sa vykonáva v súlade s metódou prijatou okrem hlavných medzinárodných noriem (ISO 27005, ISO 22301) zástupcami podniku.
Počas fázy rozhovoru BIA a s použitím interne vyvinutého nástroja na zber informácií manažéri rôznych oddelení spoločnosti hodnotia stratu dôvernosti, integrity a dostupnosti informácií spravovaných v rámci ich pôsobnosti z hľadiska ekonomického, regulačného a reputačného vplyvu podľa presne definovaných hodnotiacich stupníc.

Ako je uvedené v 1. FÁZE, jednotlivé procesy sú zoskupené do makroprocesov špecifických pre analyzovaný kontext. Vplyvy spojené s týmito makroprocesmi sa vypočítajú ako *„najhorší prípad“* jednotlivých vplyvov rôznych procesov, ktoré ich tvoria.

4.2.2 Identifikácia a hodnotenie aktív

Identifikácia aktív je východiskovým bodom, bez ktorého nie je možné správne a efektívne riadiť bezpečnosť spoločnosti. Inventár je v skutočnosti východiskovým bodom pre klasifikáciu aktív spoločnosti a pre analýzu úrovne rizika, ktorému sú vystavené.

Účelom tejto prevádzkovej fázy je zostaviť súpis informačných aktív alebo formalizovať existujúce metodiky, ktoré spoločnosť považuje za „kritické“ na dosiahnutie svojich obchodných cieľov, na splnenie svojich zmluvných záväzkov a nakoniec na splnenie pravidiel a právnych predpisov, ktorým podlieha jej činnosť.
Hlavnú hodnotu aktíva zvyčajne predstavujú informácie (alebo údaje), ktoré systém spracováva, pričom úlohu ich spracovania alebo ochrany prenecháva iným aktívam.
V tomto kontexte sa počas rozhovorov BIA priradí hodnota pre každé aktívum a pre každý z rozmerov bezpečnosti (dôvernosť, integrita a dostupnosť), ktoré sa vzťahujú na daný kontext.

Na základe informácií získaných počas rozhovorov je preto možné priradiť ku každému aktívu vplyvy vyplývajúce z makroprocesov, v ktorých sa používajú.

4.2.3 Analýza hrozieb a hodnotenie ich pravdepodobnosti

Metodika používaná v procese riadenia rizík informačnej bezpečnosti definuje včasný krok pri určovaní hrozieb, ktoré ovplyvňujú príslušné aktíva. Hrozby predstavujú všetky prvky alebo udalosti, ktoré môžu poškodiť aktívum.
Cieľom tejto činnosti je identifikovať hrozby a zraniteľnosti ovplyvňujúce aktíva identifikované a zahrnuté do procesu analýzy a riadenia rizík a posúdiť pravdepodobnosť ich výskytu.
Aby bol zoznam hrozieb úplný, odkazuje sa na zoznam hrozieb v norme ISO/IEC 27005, okrem úvah vypracovaných a uverejnených agentúrou ENISA po jej štúdiách na túto tému.
Jednotlivé hrozby sú následne zoskupené do realistických scenárov rizika pre analyzovaný kontext.

4.2.4 Analýza protiopatrení

Cieľom tejto činnosti je identifikovať protiopatrenia, ktoré sa považujú za potrebné na pokrytie scenárov rizika pre aktíva identifikované v predchádzajúcom kroku.

Aby sa zabezpečilo, že zoznam je úplný, Aruba Group S.p.A používa zoznam protiopatrení založený na osvedčených postupoch z prílohy A normy ISO/IEC 27001:2013. V závislosti od typu analyzovanej služby je možné posúdenia pre konkrétne subjekty obohatiť analýzou ďalších kontrol navrhnutých autoritatívnymi zdrojmi, ako sú ENISA, AgID, NIST atď.

Po definovaní zoznamu bezpečnostných kontrol sa tieto kontroly zmapujú vzhľadom na scenáre rizika, na základe ktorých sa môžu vykonať s cieľom znížiť pravdepodobnosť výskytu príslušných hrozieb alebo ich vplyv.

Protiopatrenia sa rozdeľujú na:

- **reaktívne** (r): na zníženie vplyvu,
- **preventívne** (p): na zníženie pravdepodobnosti výskytu hrozby.

4.3 3. FÁZA – Hodnotenie rizík

4.3.1 Model rizika a metodika

Hodnota rizika sa chápe ako funkcia $R = f(A, M, V)$hodnoty A príslušných aktív, M hodnoty hrozieb V a zraniteľností.

Prostredníctvom 2. FÁZY procesu riadenia rizík informačnej bezpečnosti je možné definovať model rizika (*Modelovanie hrozieb*). Ide o proces, ktorý sa používa na identifikáciu potenciálnych hrozieb a zraniteľností, hodnotenie pravdepodobnosti ich výskytu za konkrétnych okolností, ich zoradenie podľa priority a zníženie rizika ich výskytu zavedením vhodných protiopatrení.

Po definovaní základného kontextu proces *modelovania hrozieb* zahŕňa:

- vytvorenie zoznamu potenciálnych útokov/zraniteľností, ktorý obsahuje spôsoby, akými by mohla byť ohrozená dôvernosť, integrita a dostupnosť údajov;
- posúdenie najpravdepodobnejších útokov/zraniteľností, vylúčenie tých, ktoré sú nepravdepodobné alebo v každom prípade takmer nemožné na nápravu, a pre všetky ostatné uplatnenie kontrol, alebo protiopatrení, ktoré môžu byť technické alebo procedurálne.

4.3.2 Platné bezpečnostné požiadavky a úroveň súladu

Keď sa určia bezpečnostné požiadavky, ktoré sa považujú za uplatniteľné v kontexte analýzy (pozri časť s názvom „Analýza protiopatrení“), posúdi sa rozsah, v akom sa posudzujú požiadavky týkajúce sa 14 oblastí identifikovaných v prílohe A normy ISO/IEC 27001:2013.

Rozsah, v akom je každé protiopatrenie v súlade, sa vyjadruje podľa presne definovanej stupnice s hodnotami od 0, čo znamená, že neexistuje žiadne protiopatrenie, po 4, keď je protiopatrenie plne implementované.

Na analýzu úrovne súladu kontrolných mechanizmov požadovaných v prílohe A normy ISO/IEC 27001:2013 sa používajú informácie a dôkazy zhromaždené prostredníctvom špecifických hodnotiacich činností vykonávaných interne.

4.3.3 Výpočet inherentných a zvyškových základných rizík

Počas tejto fázy sa vypočíta hodnota vlastných a zvyškových základných bezpečnostných rizík v oblasti dôvernosti, integrity a dostupnosti (existujúcich, plánovaných a budúcich) spojených s analyzovanou službou.
Inherentné základné riziká pre každé aktívum a pre každý scenár, spojené podľa vyššie opísanej logiky, sa vypočítajú zohľadnením pravdepodobnosti výskytu jednotlivých rizikových scenárov a potenciálneho vplyvu, ktorý by mohli mať.
Po určení inherentných rizík sa na získanie zvyškových rizík (existujúcich, plánovaných a budúcich) zohľadnia hodnoty spojené s bezpečnostnými protiopatreniami potrebnými na zvládnutie identifikovaných scenárov rizika počas fázy vnútorného auditu, a to z hľadiska zníženia pravdepodobnosti hrozieb, ako aj z hľadiska zníženia ich vplyvu.

4.4 4. FÁZA – Spracovanie rizika

4.4.1 Analýza prijatých rizík

Jedným z pojmov, ktorým sa treba zaoberať pri riadení rizík, je pojem prijatých rizík. Tento pojem sa vo všeobecnosti vzťahuje na tie riziká, ktoré sa z nejakého dôvodu nedajú riešiť pohodlne alebo vôbec a ktoré sa jednoducho akceptujú.

Cieľom tejto činnosti je preto definovať kritérium, podľa ktorého možno jednoducho akceptovať dvojice hrozba-aktívum, ktoré zahŕňajú nízke riziko. Nad rámec jednotlivých prípadov je preto definovaná hranica, pod ktorou sa určité riziko jednoducho považuje za náklad, a preto sa nerieši.

4.4.2 Výsledky analýzy: zvyškové existujúce riziko

Práca spojená s analýzou a hodnotením rizík s prihliadnutím na uplatnené protiopatrenia (zvyškové riziko) sa vykonáva prostredníctvom:

- posúdenia bezpečnostných kontrol s ohľadom na osvedčené postupy uvedené v prílohe A normy ISO/IEC 27001:2013;
- analýzy vplyvu straty dostupnosti, dôvernosti a integrity informácií pre príslušné služby;
- analýzy zraniteľností a hrozieb pre aktíva;
- posúdenia súčasného stavu rizika informačnej bezpečnosti a určenia poradia priorít.

4.4.3 Analýza nedostatkov a výber protiopatrení

Na základe vykonanej analýzy a s cieľom riešiť všetky relevantné riziká/problémy v rámci služieb poskytovaných spoločnosťou Aruba Group S.p.A. a s cieľom neustáleho zlepšovania systému ISMS sa údaje získané z analýz vykonaných v nástroji na analýzu rizík spracúvajú s cieľom identifikovať rizikové oblasti, pre ktoré je potrebné definovať vhodné bezpečnostné opatrenia.

Na identifikáciu opatrení, ktoré sa považujú za potrebné na zlepšenie a zníženie rizík, sa preto z času na čas definuje analýza nedostatkov, ktorej cieľom je posúdiť rozdiel medzi súčasnou úrovňou uplatňovania bezpečnostných protiopatrení a maximálnou uplatniteľnou úrovňou.

4.4.4 Plán spracovania rizika – racionalizácia intervencie

Opatrenia identifikované v analýze nedostatkov sa potom zoskupia do konkrétnych projektových iniciatív a zdokumentujú v rámci plánu spracovania rizík.

5 FREKVENCIA VYKONÁVANIA ANALÝZ

Proces riadenia rizík informačnej bezpečnosti sa dokončí každých 12 mesiacov alebo skôr, ak dôjde k významnej udalosti. Medzi takéto udalosti patria:

- nové aktíva, ktoré spadajú do rozsahu riadenia rizík;
- nové hrozby v rámci organizácie aj mimo nej, ktoré neboli vyhodnotené;
- možnosť, že hrozby zneužijú nové alebo zvýšené zraniteľnosti;
- preskúmanie už identifikovaných zraniteľných miest s cieľom určiť tie, ktoré môžu byť viac vystavené novým alebo opätovne sa objavujúcim hrozbám;
- zvýšené vplyvy alebo dôsledky hrozieb na aktíva, zraniteľnosti a riziká, ktoré spolu vedú k neprijateľnej celkovej úrovni rizika;
- obzvlášť závažné bezpečnostné incidenty.

Okrem toho sa analýzy môžu vykonávať s rôznou frekvenciou, napríklad v súvislosti s dodržiavaním konkrétnych noriem alebo požiadaviek na certifikáciu.