c) niečím, čo ste (biometria, napr. odtlačok prsta).

Používateľovi, ktorý využíva vzdialený prístup do interného prostredia spoločnosti smú byť pridelené len schválené profily.

V prípade, keď sú vzdialené prístupy používané len príležitostne, prípadne v dopredu definovaných časových rozmedziach, je vhodné takýto prístup otvoriť len na požiadanie, t.j. prístupy, ktoré sú za bežných okolností uzatvorené, budú otvorené iba na základe predchádzajúcej žiadosti. Všetky činnosti realizované v rámci sieťového prostredia spoločnosti a v jednotlivých systémoch musia byť monitorované podľa požiadaviek bezpečnostných štandardov.

6.2 Používanie mobilných zariadení

Mobilné zariadenia (notebook, mobilný telefón, tablet), ktoré sa môžu používať v sieťovom prostredí BVS (lokálne alebo pomocou bezpečného vzdialeného prístupu) a bežne sa pripájajú aj priamo do verejnej nezabezpečenej siete (internetu).

Pre bezpečnosť mobilných zariadení platia vzhľadom na používanie v nechránenom prostredí vyššie požiadavky na bezpečnosť citlivých údajov pri ich uložení a pri prenose v externom sieťovom prostredí ako na zariadenia neprenosné.

Medzi základné bezpečnostné opatrenia patria najmä:

a) šifrovanie komunikácie,
b) šifrovane disku,
c) aktuálna ochrana endpointov,
d) aktuálna inštalácia bezpečnostných záplat OS a kritických aplikácií.

6.3 Riadenie personálnej bezpečnosti

Počas prijímacieho procesu musia byť primerane preverované schopnosti uchádzača plniť požadované pracovné činnosti a splnenie požiadaviek stanovených legislatívou. Zamestnanci musia byť informovaní o svojich zodpovednostiach a právomociach týkajúcich sa bezpečnosti informácií bezprostredne po nástupe do zamestnania.

Každý zamestnanec musí prejsť primeraným zácvikom, ktorý sa týka pracovných postupov súvisiacich s informačnou bezpečnosťou a správneho používania informačných systémov, do ktorých bude mať povolený prístup. V prípade významných zmien v bezpečnostnej dokumentácii musia byť zamestnanci opätovne preškoľovaní.

Každý zamestnanec, ktorý poruší povinnosť dodržiavania bezpečnostných opatrení a postupov, bude postihovaný sankciami definovanými v Pracovnom poriadku.

Pri vzdelávaní a motivovaní zamestnancov v oblasti kybernetickej bezpečnosti má dôležitú úlohu vzdelávací program kybernetickej bezpečnosti, ktorého cieľom je zvyšovať zodpovednosť zamestnancov za aktíva BVS. Predmetom vzdelávania v oblasti kybernetickej bezpečnosti je informovanie zamestnancov o prijatých opatreniach a súvisiacich postupoch.

7. RIADENIE DODÁVATEĽSKÝCH VZŤAHOV

Pri výbere dodávateľov sa musia popri iných kritériách brať do úvahy aj záruky v oblasti kybernetickej bezpečnosti. Zmluvné vzťahy musia zohľadňovať platné všeobecne záväzné právne predpisy Slovenskej republiky a bezpečnostné požiadavky BVS v oblasti kybernetickej bezpečnosti.

Podmienky výkonu prác tretími stranami, ako aj príslušné bezpečnostné požiadavky musia byť uvedené v zmluve s treťou stranou. Pri návrhu a implementácii bezpečnostných opatrení v oblasti kybernetickej bezpečnosti musí byť kladený veľký dôraz nielen na ochranu BVS pred

tretími stranami, ale aj na ochranu oprávnených záujmov tretích strán, ktoré vstupujú s BVS do obchodných vzťahov.

Všetky časti prevádzkovaných IS musia byť vyvíjané v súlade s legislatívnymi požiadavkami, formálnymi metodickými postupmi a bezpečnostnými požiadavkami politiky kybernetickej bezpečnosti. Všetky bezpečnostné požiadavky a opatrenia týkajúce sa vyvíjaného systému musia byť schválené Vedúcim OIT a Manažérom kybernetickej bezpečnosti. Počas celého procesu vývoja musia byť do vývoja zapojení okrem špecialistov z oblasti informačných technológií aj špecialisti zodpovední za informačnú bezpečnosť a koncoví používatelia. Prostredia na vývoj a testovanie systémov a produkčné prostredie musia byť fyzicky aj logicky oddelené. Systémy alebo ich časti sa môžu nasadiť do ostrej prevádzky až po ich otestovaní a akceptácii špecialistami z oblasti informačných technológií, kybernetickej bezpečnosti a koncovými používateľmi. Na testovanie môžu byť použité len databázy, ktoré neobsahujú osobné alebo inak citlivé údaje. Pri zabezpečovaní vývoja tretími stranami musia byť podmienky výkonu prác tretími stranami, ako aj bezpečnostné požiadavky uvedené v zmluve s treťou stranou.

Zamestnanci ani externí dodávatelia nesmú svojvoľne zasahovať do konfigurácie prevádzkovaných systémov, všetky realizované zmeny musia byť autorizované vlastníkom systému. Všetky požiadavky a rozhodnutia o zmene musia byť realizované dokumentovaným spôsobom, všetky významné realizované zmeny musia byť evidované podľa platných interných smerníc. Zmeny prostriedkov IS musia byť predmetom formálneho zmenového konania. Výber nových prostriedkov IS musí byť vykonaný na základe stanovených akceptačných kritérií, ktorých súčasťou musia byť aj bezpečnostné požiadavky. Účel a použitie nových prostriedkov IS musia byť schválené Vedúcim OIT a Manažérom kybernetickej bezpečnosti. Implementácii nových prostriedkov IS alebo akejkoľvek aktivite ovplyvňujúcej existujúce prostriedky IS musí predchádzať analýza rizík za účelom zistenia dopadu prípadných zmien na úroveň prevádzkovaných služieb a na bezpečnosť ostatných prostriedkov IS. V prípade identifikácie rizík musia byť navrhnuté a implementované primerané bezpečnostné opatrenia.

7.1 Riadenie dodávateľských služieb

Dodávateľské a zmluvné vzťahy (zmluvy uzatvárané s dodávateľmi, prípadne odberateľmi a inými externými subjektami) a predovšetkým vlastný prístup (fyzický či logický) tretích strán k IT/IS musí byť riadený.

Tam, kde vznikne potreba prístupu tretej strany, musí byť vykonané zhodnotenie rizík vyplývajúce z tohto prístupu tak, aby sa zistili dôsledky z hľadiska bezpečnosti a aby sa definovali požiadavky na bezpečnostné opatrenia. Opatrenia musia byť schválené a definované v zmluve s treťou stranou.

7.2 Akvizícia informačných systémov

Manažér kybernetickej bezpečnosti zodpovedá za to, že všetky bezpečnostné požiadavky na ochranu IKT sú zakotvené v zmluvných vzťahoch s tretími stranami ešte predtým, než je povolený adekvátny prístup k IS, prípadne ku technickej dokumentácii IS, a iba v rozsahu nevyhnutne nutnom pre výkon zmluvných záväzkov.

Dodávateľ sa musí zaviazať, že bude (a všetci jeho pracovníci) dodržiavať interné predpisy BVS, najmä Bezpečnostnú politiku.

V zmluvách s týmito subjektami musí byť definovaná povinnosť mlčanlivosti a ochrany dát vrátane informácií, na ktoré sa vzťahuje platná legislatíva (osobné údaje apod.), rozsah zodpovednosti za škody spôsobené činnosťou v IS a v odôvodnených prípadoch tiež napr. autorské práva (majetkové autorské práva), prípadne licenčné dohody ku oprávneniu výkonu majetkových práv.

V zmluvách musí byť definovaný rozsah zodpovednosti za škody spôsobené činnosťou v IS a povinnosti, ktoré sú pre tieto subjekty záväzné.

Bezpečnostné požiadavky uvedené v zmluvných podmienkach musia vychádzať z nižšie uvedených doporučení. Konkrétny výber bezpečnostných požiadaviek závisí na type služby alebo činnosti poskytovanej dodávateľom.

Minimálny rozsah opatrení uvedený v zmluvných podmienkach je definovaný §8 bod 2 Vyhlášky 362/2018 Z.z. v znení neskorších predpisov nasledovne:

1. Zmluva s treťou stranou obsahuje najmenej:
   a) obdobie trvania zmluvy,
   b) ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi,
   c) ustanovenie o povinnosti chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby tretej strane,
   d) ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia treťou stranou,
   e) konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana a vyjadrenie súhlasu s nimi,
   f) konkrétny rozsah činnosti tretej strany,
   g) zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby, s povinnosťou oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 zákona,
   h) ustanovenie o rozsahu, spôsobu a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby v tretej strane,
   i) vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa,
   j) ustanovenia o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
   k) ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona a ich vymedzenie,
   l) ustanovenie o spôsobe a forme hlásenia všetkých informácií majúcich vplyv na zmluvu,
   m) ustanovenie o sankčných mechanizmoch pri porušení zmluvy,
   n) ustanovenia o podmienkach a spôsobe ukončenia zmluvy,
   o) záväzok tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup prevádzkovateľovi základnej služby,
   p) záväzok tretej strany po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok tretej strany ostáva v platnosti aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu.

2. Zmluva s treťou stranou obsahuje bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) zákona.
3. Vývoj a akvizícia siete a informačného systému základnej služby sa uskutočňuje s ohľadom na zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii.
4. Evidencia všetkých uzatvorených zmlúv s treťou stranou je súčasťou bezpečnostnej dokumentácie podľa § 2 ods. 1 písm. c).

V prípade potreby zabezpečenia jednoznačnosti a úplnosti pri IS väčšieho rozsahu resp. významu je vhodné minimálny rozsah stanovený legislatívou rozšíriť o bezpečnostné požiadavky:

a) všeobecné pravidlá bezpečnosti informácií;
b) ochrana aktív IS zahrňujúca:
   - postupy slúžiace na ochranu aktív IS, vrátane informácií a programového vybavenia;
   - postup slúžiaci ku zisteniu, či nedošlo ku kompromitácii aktív IS, napríklad strate alebo modifikácii dát;
   - opatrenie zaisťujúce vrátenie či zničenie informácií/aktív IS po ukončení zmluvného vzťahu alebo v jeho priebehu;
   - integritu a dostupnosť aktív IS;
   - obmedzenie kopírovania a šírenia informácií.
c) popis každej služby, ktorá je tretej strane sprístupnená;
d) cieľová úroveň služby a neakceptovateľné úrovne služby;
e) konkrétne zmluvné záväzky tretích strán;
f) zodpovednosti vyplývajúce z právnych noriem, napr. z legislatívy (napr. Kybernetický zákon, zákon na ochranu osobných údajov);
g) ochrana duševného vlastníctva a autorské právo;
h) dohoda o riadení prístupu zahrňujúca:
   - povolené metódy prístupu a jeho kontrola, použitie jedinečných identifikátorov, ako sú používateľské identifikátory a heslá;
   - autorizačný proces pre prístup používateľa a jeho oprávnenia;
   - požiadavky na vedenie a dostupnosť zoznamu jednotlivcov, ktorí sú vzhľadom ku svojim preddefinovaným právam a privilégiám oprávnení využívať ponúkané služby.
i) popis overiteľných kritérií výkonnosti, spôsob ich sledovania a vyhodnocovania;
j) právo monitorovať a zakázať neoprávnené aktivity používateľa;
k) právo auditovať zmluvné povinnosti alebo právo nechať vykonať tieto audity treťou stranou;
l) popis eskalácie problému v prípadoch riešenia havárie; pokiaľ je to potrebné, musia byť zvážené pravidlá pre riešene havarijných situácií;
m) zodpovednosť za inštaláciu a údržbu technického a programového vybavenia;
n) jasné pravidlá hlásení a schválený formát týchto hlásení;
o) jasný a špecifikovaný proces riadenia zmien;
p) akékoľvek opatrenia fyzickej ochrany a mechanizmy, ktoré zaisťujú ich plnenie;
q) opatrenia ku zaisteniu ochrany pred škodlivým programovým vybavením;
r) systém hlásení, upozornení a vyšetrovania bezpečnostných incidentov a prípadov prelomenia bezpečnosti;

s) podmienky spolupráce tretích strán so subdodávateľmi.

8. RIADENIE VÝVOJA A ÚDRŽBY V OBLASTI INFORMAČNO-KOMUNIKAČNÝCH TECHNOLÓGIÍ

Z dôvodu zabezpečenia integrácie bezpečnosti do informačných systémov už v štádiu návrhu a vývoja, pred samotným nasadením do produkcie, ako aj zachovanie bezpečnosti počas údržby IS musíbyť zabezpečené riadenie procesov za splnenia bezpečnostných požiadaviek v minimálne nasledovnom rozsahu.

8.1 Bezpečnostné požiadavky na obstarávaný IS

Obstaranie (nákup alebo vývoj) nových IS a aplikácií prebieha v súlade s pravidlami a základnými požiadavky na kvalitu a bezpečnosť IS za predpokladu splnenia definovaných akceptačných kritérií, ktorá sa týkajú:

a) požiadaviek na bezporuchový chod;
b) splnenie bezpečnostných požiadaviek;
c) zaistenie dôvernosti, integrity a dostupnosti informácií spracovávaných v tomto systéme;
d) zachovanie kontinuity prevádzky;
e) kompatibility so stávajúcim SW a HW vybavením;
f) legislatívnej zhody vyvíjaných systémov;
g) a pokiaľ je to potrebné pre zaistenie prevádzky, alebo to vyžadujú iné predpisy (legislatívne požiadavky na archiváciu a pod.), musí po požadovanú dobu umožňovať spoluprácu, čitateľnosť a použiteľnosť dát spracovávaných v iných systémoch.

Projekt vývoja SW/IS musí obsahovať dokumentáciu venovanú bezpečnosti v každej fáze projektu (analytickej, testovacej a prevádzkovej).

Bezpečnostné požiadavky musia byť zakotvené aj v zmluve (vrátane napr. riešenia povinností nástupnickej organizácie či v prípade zániku dodávateľa) už vo fáze návrhu projektu ešte pred zahájením vlastného vývoja. To sa v plnej miere vzťahuje aj na zmenové konanie v priebehu vývoja.

Pri vývoji IS externým dodávateľom musia byť zvážené a zmluvne ošetrené najmä nasledujúce otázky:

i. dohoda vlastníctve kódu a práv duševného vlastníctva;
ii. certifikácia kvality a správnosti vyžiadaných prác;
iii. právo prístupu ku vývoju pre audit kvality a správnosti prevedenej práce;
iv. zmluvné podmienky pre kvalitu kódu;
v. testovanie kvôli odhaleniu chýb pred spustením do prevádzky.

8.2 Postupy nasadenia, testovania a údržby

8.2.1 Oddelenie testovacích dát

Proces testovania programového vybavenia, aplikácií a nástrojov nesmie zasahovať do produkčnej prevádzky v prípade, ak by mohol negatívne ovplyvniť prevádzkyschopnosť IT prostredia alebo bezpečnosť produkčných dát.

Ak sú pre testovanie používané testovacie dáta vytvárané z produkčných prevádzkových dát, je nutné zabezpečiť, aby tieto dáta neobsahovali citlivé (chránené či osobné) údaje alebo ich zabezpečiť tak, aby nedošlo k úniku týchto dát mimo chránené prostredie IS.

Rovnako je potrebné zabezpečiť, aby nemohlo dôjsť k prieniku testovacích dát do produkčnej prevádzky oddelením testovacích prostredí od produkčného prostredia a bezpečnú likvidáciu testovacích dát pred uvedením systému do prevádzky, čo sa vzťahuje ako na dodávateľské riešenia, tak na vývoj systémov, programového vybavenia a utilít vlastnými silami.

8.2.2 Postupy údržby informačných systémov a manažment záplat

Rozvoj IT je sledovaný a aktuálnosť zabezpečenia IT je riešená implementáciou najnovších bezpečnostných prvkov a opravných balíčkov (po nevyhnutnom preverení správnosti a funkčnosti neodkladne po ich uvoľnení výrobcom a overením ich správnej funkcionality v testovacom prostredí). Za túto činnosť zodpovedá vedúci oddelenia OSIKTI pre systémovú a infraštruktúrnu časť a vedúci oddelenia OSPA za aplikačnú časť..

V prípade nutnosti a podľa potreby sú vykonávané ďalšie preventívne bezpečnostné opatrenia podľa aktuálnej situácie v tejto oblasti.

Pravidelná aktualizácia OS (operačných systémov) a aplikácií na pracovných staniciach, serveroch a aktívnych prvkoch siete pri zachovaní funkčnosti a stability OS a štandardných aplikácií je základným prvkom bezpečnosti každého IT prostredia.

Za sledovanie nových aktualizácií, ich stiahnutie, postup testovania a nasadenia zodpovedá vedúci oddelenia OSIKTI resp. OSPA. Zodpovedná osoba pravidelne kontroluje (minimálne 1x týždenne) pomocou nástrojov WSUS a SCCM ako aj na stránkach výrobcu, či sú k dispozícii nové aktualizácie. Následne zabezpečí stiahnutie, testovanie a nasadenie aktuálnych záplat na pracovné stanice a servre.

Zodpovedná osoba 1x mesačne podáva súhrnnú správu o aktuálnom stave zraniteľností a stave inštalácie bezpečnostných záplat Vedúcemu OIT a Manažérovi kybernetickej bezpečnosti.

9. RIADENIE A PREVÁDZKA INFORMAČNO-KOMUNIKAČNÝCH TECHNOLÓGIÍ

Riadenie procesov prevádzky IKT a IS systémov je nevyhnutnou súčasťou prevádzky, cieľom ktorého je dosiahnutie bezpečnosti IS, detekcia škodlivého kódu a prevencia pred vznikom bezpečnostných incidentov.

9.1 Pravidlá prepájania systémov a prenosu elektronických informácií

Prestup medzi internou počítačovou sieťou spoločnosti a externými počítačovými sieťami musí byť riadený jedným, alebo oboma uvedenými spôsobmi:

a) úplné oddelenie pomocou samostatného terminálu, alebo úplne oddelená interná počítačová sieť vytvorená len pre tento účel (DMZ),
b) firewall (bezpečnostná brána) nakonfigurovaný internými špecialistami, alebo špecializovanou spoločnosťou a nezávisle auditovaný (ideálne treťou stranou).

Zamestnanci spoločnosti nesmú používať iný ako autorizovaný schválený spôsob konektivity do externých počítačových sietí z interného prostredia spoločnosti, resp. zo zariadení spoločnosti. Je prísne zakázané používať pre zriadenie konektivity vlastné prostriedky (napr. modemové karty a počítače) pripojené do internej počítačovej siete spoločnosti a zároveň pripojené do externých počítačových sietí obchádzaním zavedených pravidiel.

Porušenie pravidiel prístupu z a do externých počítačových sietí sa považuje za významné narušenie bezpečnostného systému a musí byť riešené v zmysle pravidiel upravujúcich riadenie bezpečnostných incidentov.

Centralizovanie prestupov medzi internou počítačovou sieťou spoločnosti a externými počítačovými sieťami cez jeden vstupno-výstupný bod musí zabezpečovať:

i. potreby používateľov vychádzajúce ich pracovných povinností,

ii. jednotné riadenie prestupu medzi sieťami,
iii. dodržiavanie bezpečnostných požiadaviek na všetkých prístupoch,
iv. riadenie prístup k určitým službám, alebo serverom v závislosti na používateľovi, resp. pridelených prístupových právach,
v. požadovanú mieru dostupnosti (redundancia).

Na prístupové miesto do externých počítačových sietí si spoločnosť vyhradzuje právo na nainštalovanie softvéru na filtráciu vstupných a výstupných tokov, ktorý filtruje vstupné toky na základe zoznamu zakázaných serverov, prípadne kľúčových slov. Pokiaľ sa filtrácia tokov vykonáva na úrovni klientskych staníc, musia byť tieto nástroje spravované centrálne a zabezpečené pred neautorizovaným prístupom a modifikáciou zo strany bežných používateľov.

Zároveň by mali byť v rámci internej počítačovej siete spoločnosti zavedené opatrenia pre riadenie smerovania tokov v sieti založené na mechanizmoch pozitívnej kontroly zdrojovej a cieľovej adresy. Pravidlá určené na overovanie zdrojovej a cieľovej adresy musia byť implementované na interných, ako aj externých sieťových prístupových bodoch.

Tieto pravidlá prepájania systémov a prenosu elektronických sú záväzné aj pre interné oddelenie operačnej technologickej prevádzkovej siete (OT network) a informačnej technologickej office siete (IT network) spoločnosti BVS.

V tomto prípade sa interná IT sieť voči OT sieti považuje za externú sieť.

9.2 Riadenie bezpečnosti sietí

Na zabezpečenie efektívneho oddelenia IKT zdrojov spoločnosti alebo zdrojov vyžadujúcich vyhradené prostredie, musia byť lokálne siete rozdelené do niekoľkých net-skupín (segmentov). Kritériá pre rozdelenie sietí musia byť založené na schválenej politike riadenia prístupu a preskúmaní dopadov filtrovania na výkonnosť siete. Ďalšie kritériá, ktoré musia byť pri segmentovaní siete zohľadnené sú:

a) hodnota a klasifikácia informácií uchovávaných a spracúvaných na sieti,
b) úrovne dôvery medzi jednotlivými sieťami,
c) jednotlivé body prepojenia sieťových segmentov.

9.2.1 Filtrácia a pravidlá

Filtrácia a pravidlá pre oddeľovanie jednotlivých sieťových segmentov musia byť nastavené tak, aby na úrovni lokálnej siete umožňovali:

a) filtrovať vstupné toky,
b) filtrovať výstupné toky,
c) definovať uzatvorené skupiny používateľov, ktorí môžu navzájom komunikovať.

9.2.2 Aplikácia filtrov

Aby bolo zaručené, že aplikovanie filtrov a prístupových pravidiel bolo realizované primerane s ohľadom na prevádzkové a bezpečnostné parametre sieťového prostredia musí byť vykonaná štúdia zameraná na:

a) identifikáciu vstupných a výstupných tokov,
b) definovanie funkčných potrieb filtrácie výberom autorizovaných a zakázaných tokov,
c) určenie syntaxe filtrov.

9.3 Riadenie kapacity systémov a služieb

Kapacita zdrojov systémov musí byť plánovaná vopred, aby bola zaistená dostupnosť jednotlivých zdrojov pri prevádzke systémov spoločnosti. Požiadavky na kapacitu a výkonnosť zdrojov systému musia byť monitorované administrátorom. Administrátor je povinný informovať o stave kapacít vedúceho príslušného útvaru a vlastníka systému a to vždy pri výraznej zmene minimálne však 1 krát mesačne.
Základnými informáciami, ktoré sú nevyhnutné pre efektívne plánovanie kapacít systému sú hlavne nasledovné informácie o:

a) súčasnom stave disponibility systému – diagnostika,
b) predpokladaných zmenách disponibility systému – predikcia.

V rámci spoločnosti je potrebné zvážiť použitie automatizovaného systému merania a predikcie disponibility zdrojov jednotlivých systémov. Zavedenie takéhoto prostriedku umožní administrátorovi predpovedať, kedy sa disponibilita systému môže znížiť natoľko, že ohrozí funkčnosť niektorého zo svojich subsystémov. Takýmto spôsobom je možné v predstihu riešiť rôzne problémy.

9.4 Riadenie kryptografických opatrení

Na ochranu dôvernosti najcitlivejších údajov musia byť použité kryptografické mechanizmy.

V prípade zabezpečenia Core bussines spoločnosti a prevádzky technológií v OT sieťach je potrebné nad rámec štandartného šifrovania MPLS siete a privátnych APNCS sieťí GSM použiť šifrovanie komunikácie ďalšou certifikačnou autoritou.

Za technickú koordináciu implementácie, správy a používania kryptografických mechanizmov interného prostredia zodpovedá odborný útvar spoločnosti, ktorý má na starostí informačnú bezpečnosť.

V prostredí spoločnosti smú byť použité len také technológie šifrovania, ktoré vyhovujú požiadavkám definovaným Bezpečnostnou politikou a boli schválené Manažérom kybernetickej bezpečnosti. Používanie neschválených technológií a prostriedkov je zakázané a je považované za bezpečnostný incident.

Šifrovacie technológie používané v rámci spoločnosti musia podporovať funkcie tzv. „key recovery“ tak, aby bola zabezpečená dostupnosť chránených údajov v prípade straty kľúča, úmyselného zneprístupnenia kľúča (sabotáž), alebo potreby kontroly obsahu. Použitie „key recovery“ musí byť odsúhlasené Manažérom kybernetickej bezpečnosti a autorizované Vedúcim OIT. Použitie „key recovery“ je podmienené prítomnosťou dvoch osôb vlastniacich časti kľúča.

10. RIADENIE SÚLADU

Cieľom riadenia súladu je zaistenie splnenia a dodržiavania všetkých legislatívnych požiadaviek, noriem a predpisov vyžadovaných pre prevádzku informačných systémov spoločnosti.

10.1 Audit kybernetickej bezpečnosti

Interný audit kybernetickej bezpečnosti sa vykonáva pravidelne 1krát za rok, v prípade potreby aj častejšie. Jeho cieľom je preveriť a posúdiť riziká spojené s bezpečnosťou prevádzkovaných IKT, IS, operačných systémov, SW nástrojov a spracúvaných dát v spoločnosti.

Súčasťou auditu kybernetickej bezpečnosti je aj kontrola technickej zhody, ktorá overuje súlad IS s implementáciou štandardov bezpečnosti (správna implementácia HW a SW opatrení). Kontrola sa môže vykonávať manuálne alebo pomocou automatizovaných SW prostriedkov.

Kontrola technickej zhody môže obsahovať napr. penetračné alebo technické testy, ktoré môžu byť vykonávané nezávislými expertami objednanými špeciálne na tento účel.

Nástroje a zdroje pre audit kybernetickej bezpečnosti podliehajú kontrole, musia byť chránené a prístupné iba povereným zamestnancom, pričom tento prístup musí byť zaznamenávaný (tj. monitorovaný a logovaný).

Auditné správy sú vzhľadom k obsahu a informáciám týkajúcim sa bezpečnosti, určené a dostupné iba povereným zamestnancom, zástupcom vedenia BVS a Manažérovi kybernetickej bezpečnosti.

Audit kybernetickej bezpečnosti vykonávaný orgánom posudzovania zhody v zmysle § 5 a §29 Zákona 69/2018 Z.z. sa vykonáva v peridicite a rozsahu stanoveným platnou legislatívou.

10.2 Spracúvanie osobných údajov a klasifikovaných informácií

Osobné údaje a klasifikované informácie podľa zákona o ochrane osobných údajov (Zákon č. 18/2018 Zb.) a zákona o kybernetickej bezpečnosti (Zákon č. 69/2018 Zb.) musia byť v spoločnosti zabezpečené zodpovedajúcim spôsobom proti zneužitiu a neoprávnenému prístupu.

Používatelia IS musia byť oboznámení s legislatívnymi požiadavkami kladenými na ochranu osobných údajov.

Spracúvanie a nakladanie s osobnými údajmi je riadené procesnou smernicou: „04_P2_Bezpečnostná smernica Ochrana osobných údajov“.

Postup a klasifikovanie informácií je riadený procesnou smernicou: „05_P2_ Klasifikačná smernica - Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa zákona 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov“.

10.3 Poskytovanie súčinnosti tretím stranám

Prevádzkované IS spolu so spracúvanými informáciami a používanými technológiami vyžadujú v niektorých prípadoch prístup tzv. tretích strán, jedná sa napr. o servisné zásahy pracovníkov dodávajúcich SW či HW alebo poskytujúcich podporu IT.

Pokiaľ prevádzkovaný IS vyžaduje prístup tretích strán, fyzický, či logický prístup alebo o časovo obmedzenú činnosť externých pracovníkov, musí byť prístup tretích strán riešený v súlade s Bezpečnostnou politikou tak, aby bola zaistená adekvátna úroveň bezpečnosti informácií.

Akákoľvek spolupráca s externou organizáciou musí byť ošetrená zmluvne, najmä z pohľadu bezpečnosti a zodpovednosti za možné riziká plynúce z tejto spolupráce.

Požiadavky tretích strán na zriadenie prístupu do prostredia IT BVS prostredníctvom používateľských účtov musia byť vždy najskôr dohodnuté a schválené Manažérom kybernetickej bezpečnosti a Vedúcim odboru IT.

11. RIADENIE KONTINUITY PROCESOV A ČINNOSTÍ

Cieľom riadenia kontinuity procesov a činností je zabezpečenie a zachovanie potrebnej dostupnosti informácií a služieb, zaistenie kontinuity činností a procesov vrátane havarijného plánovania.

11.1 Plány kontinuity prevádzkových činností

V rámci IS BVS je potrebné identifikovať rizikové procesy, ktoré je nutné zabezpečiť proti prípadnému prerušeniu alebo výpadku. Pre tieto procesy musí byť stanovený časový úsek akceptovateľného prerušenia (maximálna doba nedostupnosti), v jej priebehu je nutné zaistiť

znovuuvedenie do stavu pred výpadkom či haváriou a zaistiť tak kontinuitu kritických činností spoločnosti.

Za identifikáciu rizikových procesov zodpovedá Manažér kybernetickej bezpečnosti, ktorý v týchto otázkach spolupracuje s poverenými zamestnancami jednotlivých oddelení, vlastníkmi aktív IS.

11.2 Plány havarijnej obnovy prevádzky

Zachovanie kontinuity prevádzky IS BVS je prvoradým cieľom havarijného plánovania, tj. plánu pre riešenie havarijných situácií a plánu obnovy, ktorý je podrobne rozpracovaný v príslušnom Havarijnom pláne IKT. Potreba zaistenia prevádzky je závislá na správnom stanovení kritickosti procesov, na hodnote aktív a dopadu havárií na konkrétne aktíva informačného systému.

Havarijný plán IKT tvorí samostatný dokument, ktorý slúži ako detailný popis postupov a krokov pri výskyte všetkých uvažovaných prípadov možných havárií. Tento plán definuje tiež rozsah zodpovedností a povinností osôb zastávajúcich určené funkcie pre riešenie havárií.

Každý používateľ podľa svojej funkcie musí byť oboznámený s aktuálnymi havarijnými plánmi pre oblasť svojho pôsobenia a poznať svoju rolu a zodpovednosť v procese obnovy. Vedúci OSIKTI a OSPA sú povinný udržiavať havrijné plány v aktuálnom stave a zaistiť dostupnosť aktuálneho Havarijného plánu IKT i pre prípad havárie (napr. v tlačenej podobe).

11.3 Metodika zálohovania a obnovy informácií

Za účelom zabezpečenia kontinuity resp. havarijnej obnovy uvedenej vyššie je nevyhnutné periodické zálohovanie všetkých dôležitých dát a prevádzkovaných systémov.

Zálohovanie je v BVS realizované na jednotnej platforme a to na systémovej, blokovej, databázovej alebo súborovej úrovni, prípadne ich kombináciou. Úroveň, periodicitu, retenciu zálohovania definuje ako požiadavku vlastník aktíva a systému.

Po schválení Manažérom KB a Vedúcim OIT zálohovanie zabezpečuje odd. OSIKTI. Nastavenie a postup zálohovania tvorí samostatný dokument.

IV. Systém riadenia kybernetickej bezpečnosti

Účelom zavedenia systému riadenia kybernetickej bezpečnosti je stanovenie pravidelne sa opakujúcich procesov a postupov, ktoré zabezpečia, že úroveň kybernetickej bezpečnosti v BVS bude adekvátnym spôsobom pokrývať externé a interné riziká, bude odzrkadľovať kritickosť biznis procesov a bude v súlade so všetkými legislatívnymi požiadavkami a normami.

Informačná bezpečnosť musí byť organizačne riadená v súlade s pravidlami stanovenými touto politikou. Zodpovednosti za ochranu aktív a za vykonávanie špecifických procesov kybernetickej bezpečnosti musia byť jasne definované a zdokumentované. Pri ohodnocovaní a riadení rizík a návrhu bezpečnostných opatrení musí byť využívaná koordinovaná podpora všetkých zainteresovaných strán.

Proces riadenia kybernetickej bezpečnosti je realizovaný samostatne definovanými procesmi a usmerneniami a to v nasledujúcich krokoch:

Krok 1 - Analýza a prehodnotenie hrozieb a zraniteľností
Cieľom je aktualizácia databázy hrozieb a zraniteľností, identifikácia nových skutočností s ohľadom na realizovane opatrenia.

Zodpovedný: Manažér KB

Účastníci: Vlastníci aktív IS, Správcovia aktív IS, Ved. OIT, resp. nimi poverené osoby.

Pravidelnosť: 1x ročne