BYROJA KOSOVARE E SIGURIMIT - BKS
KOSOVSKI URED OSIGURANJA - KUO
KOSOVO INSURANCE BUREAU - KIB
Nr. 749/22 Dt. 02.08.22
PRISHTINË

BKS
Byroja Kosovare e Sigurimit
Kosovski Ured Osiguranja
Kosovo Insurance Bureau

POLITIKAT
E MBROJTJES SË SISTEMIT INFORMATIV

Prishtinë, 2022

Në bazë të nenit 12, shkronja a), pika 5 e statutit të Byrosë Kosovare të Sigurimit dhe nenit 53 të Ligjit Nr. 05/L-045 për Sigurimet, Asambleja e Përgjithshme e Anëtarëve, miraton këtë:

POLITIKAT
E MBROJTJES SË SISTEMIT INFORMATIV

1. Parimet e Përgjithshme

Sigurimi si veprimtari themelore e Byrosë Kosovare të Sigurimit kërkon mbështetje cilësore dhe të pandërprerë informative, nga e cila jetësisht është e varur organizata. Ligjet në Kosovë, para së gjithash, Ligji për Sigurimin, Ligji për Mbrojtjen e të dhënave personale, dhe tjera si dhe obligimet kontaktuese ndaj palëve të veta, Byrosë Kosovare të Sigurimit i përcaktojnë kërkesat konkrete për mbrojtjen e informatave dhe për zotërimin e rreziqeve informative. Të dhënat dhe informatat e mbledhura në sistemin informativ, paraqesin pasuri kyçe të BKS-së dhe mundësojnë perspektivën afariste afatgjate të saj. Njëkohësisht, teknologjia informative mundëson lehtësira te reja afariste dhe zvogëlim të shpenzimeve afariste.

Drejtori i BKS-së, në bazë të këtyre veprimeve, konstaton domosdoshmërinë e mbrojtjes adekuate dhe sigurimin e informatave dhe mjeteve të teknologjisë informative në shoqëri dhe jep mbështetje të plotë aktiviteteve të nevojshme në këtë lëmi.

Dokumenti "Politikat e mbrojtjes së sistemit informativ" (në vazhdim e njohur si: politika mbrojtëse) përcakakton orientimet themelore për mbrojtjen e sistemit informativ, gjegjësisht mbrojtjen e të dhënave informative dhe mjeteve të teknologjisë informative në mesin afarist të brendshëm të subjektit.

Qëllimi kryesor i mbrojtjes së sistemit informativ si infrastrukturë kyçe të BKS-së, është sigurimi i afarizmit të pandërprerë në përputhje me obligimet ligjore dhe kontraktuese si edhe me parimet e afarizmit të kujdesshëm dhe të mbrojtur, kurse në anën tjetër kufizimi i dëmtimeve potenciale afariste në masën më të vogël të mundshme duke parandaluar dhe zvogëluar efektet e incidenteve të sigurisë . Po ashtu, duhet siguruar qasje deri te informatat dhe shërbimet informative në subjekt në atë mënyrë që të mundësojë afarizëm optimal dhe efikasitet të investimeve në informatikë.

Sistemi informativ i Byrosë Kosovare të Sigurimit nënkupton rrethanat e tërësishme në të cilat paraqiten, përpunohen dhe shfrytëzohen informatat pa marrë parasysh format e paraqitjes dhe mënyrën e ruajtjes si dhe infrastrukturën teknologjike (në mediumet e ndryshme elektronike, si ato të shtypura, të shkruara, të folura, etj.). Mbrojtja dhe sigurimi janë të duhura për tërë sistemin informativ.

Komponentët e mbrojtjes së informatave janë:

1. **besueshmëria** - sigurimi se informatat u janë në dispozicion atyre që janë të autorizuar që t'i marrin;
2. **tërësia** - mbrojtja e saktësisë dhe tërësisë së informatave dhe i procedurave të procedimit;

3. **munndësia për t'i pasur** - sigurimi i informatave dhe i procedimit te tyre me shfrytëzim optimal të burimeve, para se gjithash, të atyre kadrovike dhe financiare;

Vetitë e rëndësishme të informatave, të cilat duhet siguruar janë edhe:

1. **suksesi** - përpuethshmëria e informatave dhe procedimit të tyre me nevojat dhe pritjet e shfrytëzuesve (përshtatshmëria, shfrytëzueshmëria, rregullësia, azhuriteti);
2. **efikasiteti** - sigurimi i informatave dhe i procedimit me shfrytëzim optimal të burimeve, para së gjithash kadrovike dhe financiare;

Rreziqet kyçe në lëmin e sigurisë së sistemit informativ janë:

1. veprimi jo i mjaftueshëm i sistemit informativ ose të komponentëve të tij për shkak të pajisjeve teknike ose programore jo adekuate, ose të pamjaftueshme, rënies së pajisjeve, humbjes së të dhënave ose mungesës së kuadrove të kualifikuara në lëmin e informatikës;
2. futjet jo të rregullta, ndryshimet ose humbjet e të dhënave për shkak të gabimeve ose të ndërhyrjeve të qëllimshme të të punësuarve ose të bashkëpunëtorëve të jashtëm;
3. zbulimi i qëllimshëm ose i paqëllimshëm i të dhënave sekrete, të cilat si të tilla janë përcaktuar me rregullativën ligjore ose me klasifikimin intern të Byrosë Kosovare të Sigurimit ose vjedhja e të njejtave;
4. afarizmi i joligjshëm.

Incidenti i sigurisë është çdo ngjarje që ka ose mund të ketë si pasojë humbjen ose zvogëlimin e pasurisë së kompanisë, ose dëm në mjetet afariste ose të veprimit, i cili shkelë procedurat e sigurisë në organizatë. Qëllimet e mbrojtjes së informatave dhe të sistemit informativ të Byrosë Kosovare të Sigurimit janë:

1. sigurimi i afarizmit të sigurtë,të kujdesshëm,të pandërprerë dhe të suksesshëm të kompanisë;
2. sigurimi i përputhshmërisë së afarizmit me dispozita ligjore dhe obligimet kontraktuese;
3. sigurimi i sistemit informativ nga rreziqet e ambientit,posaçërisht sigurimi nga viruset e kompjuterëve dhe nga programet tjera qëllimkëqija;
4. sigurimi i gatishmërisë maksimale të sistemit informativ;
5. sigurimi i dëmtimeve minimale afariste në rastet e ngjarjeve të jashtëzakonshme (incidente të sigurisë);
6. sigurimi i investimeve të suksesshme dhe efikase në teknologjinë informative;
7. shfrytëzimi i suksesshëm i përparësive afariste, të cilat i mundëson teknologjia informative.

Sistemi informativ i Byrosë Kosovare të Sigurimit mbrohet me sistemin e masave të sigurisë së brendshme (kontrollimeve)të cilat sigurojnë arritjen e qëllimeve të politikës së sigurisë. Në nivelin organizativ më të rëndësishem janë këto dokumente dhe masa:

1. politika e përgjithshme e sigurisë e dokumentuar dhe e shpallur;
2. rregulloret e hollësishme dhe procedurat e punës në lëmenj të caktuar të mbrojtjes së sistemit informativ;

3. përkufizimi i kompetencave dhe i ndarjes se detyrave;
4. klasifikimi i të dhënave në sistemin informativ të Byrosë Kosovare të Sigurimit, sipas shkallës së besueshmërisë;
5. planifikimi i kapaciteteve teknike dhe kadrovike në lëmin e informatikës, si dhe të mjeteve adekuate financiare;
6. sigurimi i arsimimit adekuat në lëmin e sigurisë të sistemit informativ;
7. procedurat e pranuara të raportimit për incidente të sigurisë;
8. planifikimi i afarizmit të pandërprerë të kompanisë dhe vendosja e veprimit normal të sistemit infornativ sipas incidenteve të sigurisë;
9. kontrollimet e rregullta të vlerësimeve të rreziqeve informative,dokumenteve të politikës mbrojtëse dhe të zbatimit të masave mbrojtëse në praktikë si edhe adoptimi i sistemit të mbrojtjes.

Ne nivel të veprimit dhe të shfrytëzimit të sistemit informativ të Byrosë Kosovare të Sigurimit janë me rëndësi të posaçme këto kontrollime:

1. kontrollimet fizike dhe logjike të qasjes në të dhëna, aplikacioneve programore dhe mjeteve të teknologjisë informative, si nga ambienti i brendshëm ashtu edhe nga i jashtëm;
2. mbikëqyrja mbi përdorimin e internetit, postës elektronike dhe shërbimeve tjera telekomunikative dhe sigurimi i mbrojtjes më këtë rast;
3. mbrojtja prej viruseve të kompjuterit dhe programeve qëllimkëqija;
4. procedura për përpilimin e rregullt të kopjeve të sigurisë të të dhënave dhe ruajtja e tyre;
5. sigurimi i mbrojtjes adekuate të të dhënave të cilat duhet ruajtur kohë më të gjatë dhe asgjësimi adekuat i këtyre të dhënave mbas skadimit të kohës obligative të ruajtjes;
6. sigurimi i gjurmeve të revizionit dhe të të dhënave për raportin mbikëqyrës;
7. sigurimi i dokumentarizimit të plotë dhe të tërësishëm të sistemit informativ;
8. procedurat gjatë zhvillimit ose blerjes,testimit dhe bartjes në shfrytëzim te rregullt për zgjidhje programore dhe për pajisjet teknike.

Politika e mbrojtjes së sistemit informativ është dokument bazë në lëminë e mbrojtjes së informatave në Byronë Kosovare të Sigurimit. Rregulloret e veçanta dhe procedurat e punës më hollësisht përcaktojnë kontrollimin e ambientit në rajone të veçanta të veprimit dhe të shfrytëzimit të sistemit informativ. Duhet respektuar qëllimet afariste dhe përfaqësitë e kompanisë si dhe rregullativën ligjore dhe nënligjore, të cilat i takojnë afarizmit të kompanisë dhe parimet e përgjithshme të praktikës së mirë te sigurisë.

3. Kompetencat dhe përgjegjësit lidhur me mbrojtjen e sistemit informativ

Për përgatitjen dhe publikimin e dokumenteve, të cilat rregullojnë mbrojtjen e sistemit informativ të Byrosë Kosovare të Sigurimit dhe aplikimin e suksesshëm në praktikë është përgjegjës Menaxhmenti i BKS-së. Gjatë përgatitjes së këtyre dokumenteve drejtorët e departamenteve bashkëpunojnë me Qendrën Informative.

Po ashtu, Drejtori i BKS-së është përgjegjëse për verifikimin dhe modernizimin e dokumenteve të mbrojtjes së sistemit të informimit në përputhje më ndryshimet në ambientin afarist, teknologjik dhe ligjor, për të cilat do të marrë azhurime periodike mbi domosdoshmërinë e këtij modernizimi.

Posaçërisht, gjatë futjes së teknologjive të reja, aktiviteteve të reja të tregut, ndryshimeve në rregullativën ligjore, është i nevojshëm vlerësimi i rreziqeve informative dhe përshtatëshmeria adekuate e ambientit kontrollues. Duhet verifikuar edhe veprimi i masave të futura mbrojtëse në praktikë me qëllimet e parashtruara, efikasitetin, shpenzimet dhe në ndikimin në afarizmin e organizatës. Drejtori i BKS-së, për aktivitete të veçanta në lëmin e mbrojtjes së sistemit informativ, mund të autorizojë individët në organizatë, përkatesisht të lidhë kontrata adekuate me zbatuesit e jashtëm.

Kujdestari i sistemit informativ të Byrosë Kosovare të Sigurimit është Departamenti i Qendrës Informative, të cilin e udhëheqë Drejtori i departamentit. Kompetencat themelore dhe përgjegjësitë e departamentit të Qendrës informative si kujdestar janë:

1. sigurimi i veprimit të rregullt të infrastrukturës informative (kompjuterëve, rrjetit, komunikimeve), instalimeve, mirëmbajtjes dhe mbikëqyrjes së veprimit;
2. mirëmbajtja e sistemeve operacionale dhe të pajisjeve aplikative programore në kuptim të sistemit të programeve dhe supërstrukturës së tyre, rregullimeve (posaçërisht të atyre të sigurisë) dhe kryerjes së instalimeve adekuate;
3. zhvillimi dhe mirëmbajtja e pajisjeve vetanake aplikative programore,
4. mirëmbajtja e bazave të të dhënave;
5. sigurimi i kopjeve të sigurisë të të dhënave dhe programeve si edhe ruajtja e tyre;
6. mbrojtja nga viruset e kompjuterit dhe programet tjera qëllimkëqija;
7. mbikëqyrja mbi qasjet në sistemin informativ;
8. administrimi i sistemit;
9. përcjellja e ngarkesës së sistemit dhe planifikimi i kapaciteteve informative;
10. përcjellja e zhvillimit të teknologjive informative dhe mirëmbajtja e njohurive profesionale;
11. shkollimi dhe ndihma e shfrytëzuesve të sistemit informativ;
12. motivimi për përmirësimet në lëmenjtë e afarizmit,teknikës dhe të sigurisë.

Me politiken e mbrojtjes dhe me dokumente dhe procedura tjera të nevojshme duhet të njoftohen të gjithë të punësuarit në Byronë Kosovare të Sigurimit, të cilët kanë qasje në sistemin informativ. Përshkrimi i vendit të caktuar të punës në Byronë Kosovare të Sigurimit duhet të përmbajë autorizime dhe përgjegjësi adekuate për mbrojtjen e sistemit të informimit. Gjatë sigurimit të mbrojtjes shfrytëzuesit janë përgjegjës për mbrojtjen e elementeve të caktuara të sistemit informativ, në të cilat kanë qasje dhe zbatim të procedurave të mbrojtjes në përputhje me autorizimet dhe përgjegjësitë që burojnë nga vendi i punës dhe nga autorizimet e veçanta të mundëshme.

Zbatuesit e jashtëm gjatë qasjes në sistemin informativ të Byrosë Kosovare të Sigurimit duhet të respektojnë kërkesat e njëjta të sigurisë sikur të punësuarit. Me këto kërkesa duhet të jenë të njoftuar në mënyrë adekuate dhe me kohë. Është e këshillueshme që në kontrata adekuate të

formalizohen kërkesat e mbrojtjes. Ndërhyrjet e zbatuesve të jashtëm në elementet e sisitemit informativ (p.sh. mirëmbajtja e pajisjeve, vendosja dhe mbindërtimi i pajisjeve programore) duhet të dokumentohen dhe të verifikohen nga ana e personit të autorizuar të Byrosë Kosovare të Sigurimit.

Shërbimi i auditimit të brendshëm i Byrosë Kosovare të Sigurimit në përputhje me planin e vet të punës vërteton veprimin e kontrollimeve të brendshme në lëmin e mbrojtjes së sistemit informativ të subjektit.

4. Elementet e sistemit të mbrojtjes së sistemit informativ

Në këtë kaptinë jnaë përshkruar orientimet themelore në lëmenjtë më kryesore të mbrojtjes, të cilët më hollësisht mund të rregullohen me rregullore të posaçme.

4.1. Përkufizimi i kompetencave dhe ndarja e detyrave

Përkufizimi i kompetencave dhe ndarja e detyrave zvogëlon rrezikun e keqpërdorimit për shkak të pakujdesisë ose të veprimeve qëllimkëqija. Parimi themelor është se individi nuk duhet të realizojë veprime, të cilat në lidhje reciproke do t'i mundësonin keqpërdorimin (p.sh. lejimi-regjistrimi i faturës-realizimi i pagesës). Posaçërisht duhet siguruar pavarësia e funksioneve mbikëqyrëse prej lëndes për mbikëqyrje. Përkufizimi i kompetencave dhe ndarja e detyrave vlen si për realizimin e funksioneve afariste ashtu edhe për veprime specifike në lëmin e informatikës, përkatësisht shfrytëzimin e sistemit informativ.

Drejtori i Byrosë Kosovare të Sigurimit kujdeset që në suaza të mundësive dhe në përputhje me planet afariste, të vendosë dhe mirëmbajë plotësimin e tillë të kuadrit të punës që të jetë i mundshëm respektimi optimal i parimit të ndarjes së detyrave. Kur për shkak të plotësimit të kufizuar kadrovik ose të mungesave të përkohshme të punëtorit të autorizuar nuk është e mundur ndryshe, duhet futur masa adekuate plotësuese të mbrojtjes si p.sh. realizimin e operacioneve më të ndjeshme në prani të më së paku dy personave të autorizuar (principi i katër syve) dhe të dokumentimit të ditarëve.

4.2. Kualifikimi i të dhënave sipas shkallës së besueshmërisë

Të dhënat, veprimet dhe rrethanat për të cilat ka mësuar gjatë afarizmit me sigurimet e veçanta, me të siguruarit dhe më përfituesit e së drejtës nga sigurimi, BKS është e obliguar ti mbrojë si të besueshëm. Njësoj, si të besueshem duhet mbrojtur informatat afariste të brenshme të Byrosë Kosovare të Sigurimit në çfarëdo forme qofshin.

Shkalla e tillë e mbrojtjes kërkon kontroll rigoroz në qasje në të dhënat e besueshme, evidencën e përmbledhjes së të dhënave me të dhëna të tilla (edhe të kopjeve), mbikëqyrja mbi shfrytëzimin e të dhënave duke përfshirë ato në ekstrakte dhe raporte si edhe në rastin e këmbimit të këtyre të dhënave përmes postës elektronike dhe komunikimeve tjera si dhe asgjësimit të sigurt të të dhënave, përkatësisht të bartësve të këtyre të dhënave pas skadimit të kohës së përcaktuar për ruajtje.

4.3. Mbrojtja fizike

Hapësirat afariste Byrosë Kosovare të Sigurimit janë të mbrojtura fizikisht me roje gjatë 24 orëve. Rekomandohet që hyrja në hapësira të veçanta afariste ose sektorë të veçantë të jetë e mundur vetëm me përdorimin e kartelës adekuate. Vizituesit mund të hyjnë në hapësirat e Byrosë Kosovare të Sigurimit, përveç në hapësirat posaçërisht të dedikuara për punë me palë vetëm pas paraqitjes në recepcion dhe sipas rregullit, në përcjellje të të punësuarit, të cilit i dedikohet vizita.

Posaçërisht duhet mbrojtur qasja në hapësira me pajisje të rëndësishme kompjuterike, p.sh. serverët dhe pajisjet komunikuese. Këto hapësira duhet të jenë të mbyllura, kurse çelësat duhet t'i kenë vetëm personat e autorizuar. Element i mbrojtjes fizike është edhe hapësira për furnizim me energji pandërprerje me autonomi mjaft të madhe në të cilat janë të kyçur shërbyesit dhe aparatet e rëndësishme komunikuese.

Pajisjet kompjuterike, të dhënat, programet dhe dokumentacionin tjetër, që janë pronë e Byrosë Kosovare të Sigurimit, nuk lejohet të bartën prej hapsirave të subjektit pa lejen e Drejtorit Ekzekutiv, ose personit të autorizuar prej tij. Masat e veçanta duhet të ndërmerren për mbrojtjen e të dhënave në kompjuteret transmetues (bartës). Shfrytëzuesit janë të obliguara të parapengojnë çfarëdo qasje të personave të paautorizuar tek kompjuterët e vetë. Ndarja e pajisjeve, mediumeve dhe dokumentacionit me memorie duhet zbatuar në atë mënyrë, që pamundëson keqpërdorimin e mëvonshëm të të dhënave.

4.4. Mbrojtja logjike

Qasja deri tek modulet e veçanta të pajisjeve programore dhe brenda tyre deri tek funksionet dhe të dhënat duhet të rregullohet me sistemin e emrave të shfrytëzuesve, fjalëkalimeve dhe të drejtave për qasje, të cilat shfrytëzuesve ua jep Drejtori, përkatësisht personi i autorizuar për këtë (pronari i procesit afarist ose aplikacionit, respektivisht Drejtori i Departamentit përkatës). Parimi themelor për dhënien e së drejtës në qasje është që shfrytëzuesi ka nevojë për të drejtë të caktuar më të madhe vetëm përkohësisht, për këto nevoja i duhet siguruar emër i veçantë shfrytëzimi me të drejta adekuate. Është e nevojshme edhe ajo, që të gjitha të drejtat e shfrytëzuesve, të cilat nuk i nevojiten më, pa vonesë t'i revokojnë këto të drejta (p.sh. me rastin e ndryshimit të vendit të punës ose të ndërprerjes së marrëdhënies së punës).

Këshillohet që pasjisja programore të mbështesin verifikimin e të drejtës në qasje për përdorimin e funksioneve të veçanta dhe të shënojn operacionet e rëndesishme në dritarët e sistemit. Kur verifikimi i të drejtave në qasje në pajisjet programore nuk është zgjidhur në mënyrë të mjaftueshme precise, shfrytëzuesi duhet t'i përmbahet autorizimit të vendit të vetë të punës, përkatësisht autorizimet tjera të veçanta.

Shfrytëzuesit,emrat e vet të shfrytëzuesve dhe fjalëkalimet e veta,duhet t'i mbrojnë si të dhëna të besueshme,sepse marrin mbi vete të gjithë përgjegjësinë për sjelljet të cilat janë bërë nën emrin e tyre. Kur të përfundojnë punën ose të lëshojnë vendin e punës,duhet obligativisht të ç'lajmërohen nga sistemi. Qasja në sistemin informativ duhet të jetë e mbikëqyrur.

4.5. Mbrojtja e të dhënave gjatë këmbimit elektronik

Gjatë këmbimit elektronik të të dhënave (p.sh. posta elektronike dhe internet) duhet siguruar nivel të njëjtë të mbrojtjes si tek afarizmi në sistemin e brendshëm informativ të Byrosë Kosovare të sigurimit.

Elementet më të rëndesishme të mbrojtjes në këtë lëmi janë:

1. mbrojtja e lidhjeve të jashtme me firewall dhe me zgjidhje tjera;
2. mbrojtja nga viruset kompjuterike dhe programet tjera qëllimkëqija;
3. përdorimi i shifrimeve dhe shkresave digjitale gjatë bartjes të të dhënave të besueshme;
4. sigurimi i autenticitetit dhe të autorizimit të shfrytëzuesve të jashtëm.

Shfrytëzuesit duhet të jenë të njoftuar me udhëzimet për punë të sigurt me postë elektronike dhe internet. Duhet siguruar renditja dhe përpunimi i drejtë i dokumentacioneve të arritura nëpërmes të kësaj rruge. Qasja deri te sistemet për këmbim elektronik të të dhënave duhet të jetë e mbikëqyrur.

4.6. Mbrojtja nga virusët kompjuterike dhe programet tjera qëllimkëqija

Mbrojtjen ndaj pajisjeve programore qëllimkëqija (virusët, etj.) e paraqesin këto komponente:

1. në të gjithë kompjuterët duhet vendosur programe antivirusore për kontrollimin e datotekave lokale,disketave dhe postës elektronike,të cilat duhet të zbatohen dhe modernizohen rregullisht;
2. lejohet vetëm përdorimi i pajisjeve programore origjinale (të licencuara);
3. është e ndaluar vendosja e pajisjeve programore pa lejen e drejtorisë ose të kujdestarit të sistemit informativ.

Përdoruesit nuk duhet hapur lajmërimet e postës elektronike të dërguesve të panjohur, posaçërisht jo për "atachment" të dyshimtë.

4.7. Kopjet e sigurisë dhe ruajtja e tyre

Kopjet e sigurisë janë elementi më i rëndësishëm, i cili mundëson vendosjen e sërishme të sistemit informativ pas incidentit të sigurisë, me ç'rast vjen deri te humbja e të dhënave të punës ose të prishja e pajisjeve programore. Për këtë është e domosdoshme që për çdo ditë të sajohen kopjet e sigurisë të të gjitha të dhënave afariste (baza e të dhënave, dokumentet e ndryshmë, kontrollueset, etj.). Kopjet e sigurisë të të dhënave në shërbyesit e të dhënave në departamentin e Qëndres Informative përpilohen nga vetë përdoruesit çdo ditë, gjegjësisht mbas çdo ndryshimi të të dhënave për të cilat janë të ngarkuara dhe kjo në CD. Sipas mundësisë, sistemi intern i kompjuterëve i kompanisë duhet të jetë i konfiguruar në atë mënyrë që të jetë e mundshme bërja e kopjeve të sigurisë nga vendi i centralizuar.

Duhet ruajtur, gjithashtu edhe kopjet e sigurisë të të gjitha programeve sistemore dhe aplikative dhe dokumentacioni i detajizuar të parametrave specifike të vendosur dhe të instalimit të pajisjeve të aparateve dhe programeve. Përdorimi i kopjeve të sigurisë duhet të jetë i mbikëqyrur dhe i shënuar.

4.8. Planifikimi i kapaciteteve në lëmin e informatikës

Drejtori i Byrosë Kosovare të Sigurimit dhe i Departamentit të Qendres Informative janë përgjegjës për planifikimin e kapaciteteve teknike dhe stafit në lëmin e informatikës dhe për sigurimin e mjeteve adekuate financiare. Me këtë rast duhet përcjellur ngarkesat vijuese të sistemit informativ dhe respektuar kërkesat e ardhshme,të cilat burojnë nga veprimtaritë ekzistuese dhe të reja afariste të kompanisë. Kujdes të posaçëm duhet kushtuar stafit për shkak të kohës së gjatë që nevojitet për të fituar njohuri specialistike.

Planifikimi i kujdesshëm duhet edhe me rastin e futjes së shërbimeve, zgjidhja programore dhe pajisjeve teknologjike të reja. Kërkesat operative të sigurisë duhet përcaktuar, dokumentuar dhe verifikuar para kalimit në përdorim praktik.

4.9. Zhvillimi dhe mirëmbajtja e sistemit informativ

Futjen e mjeteve të reja të teknologjisë informative (p.sh.,kompjuterët, pajisjet programore) ose të ndërhyrjeve mirëmbajtëse me të mëdha e lejon drejtori. Me këtë rast, përveç arsyeshmërisë ekonomike, duhet verifikuar se edhe pajisja e re e dedikuar për qëllim të caktuar afarist a do të garantoj nivel adekuat të mbrojtjes së sigurisë dhe se nuk do të jep efektin në kundërshtim me sistemin ekzistues mbrojtës të kompanisë.

Zhvillimi i pajisjeve programore duhet të rrjedhë në ambient zhvillimor të ndarë (veçuar). Në procedurën e zhvillimit është i rëndësishem bashkëpunimi i shfrytëzuesve për qëllim të konstatimit të funksionalitetit adekuat dhe instalim me kohë të funksioneve mbrojtëse (kontrollimi i futjeve, kontrollimi i të dhënave gjatë përpilimit, gjurmat e revizionit, etj.).

Para bartjes së kësaj pajisjeje në veprim operativ, duhet bërë testim i tërësishëm, të përpilohet dokumentacioni teknik dhe shfrytëzues si dhe të sigurohet aftësimi adekuat i shfrytëzuesve.

Rregulla të njëjta përdoren edhe me rastin e ndryshimeve dhe mirëmbajtjen e elementeve të sistemit informativ.

4.10. Mbrojtja e sistemit informativ gjatë marrjes me qira të shërbimeve informative

Përveç shfrytëzimit të kapacatiteve të brendshme, Byroja Kosovare të Sigurimit mund të marrë me kontraktojë edhe shërbime të tjera të caktuara informative nga zbatuesit e jashtëm. Kjo posaçërisht u përket këtyre lëmive:

1. zhvillimit dhe mirëmbajtjes së pajisjeve programore për mbështetje afarizmit të institucionit;
2. mirëmbajtja e sistemit informativ në segmentet ku janë të nevojshme njohuritë specifike;
3. këshillim në lëmin e mbrojtjes së sistemit informativ.

Për marrjen me qira të shërbimeve informative tek zbatuesit e jashtëm vendos drejtoria.me këtë rast duhet respektuar parimet e mbrojtjes së informatave në institucion, sidomos nga aspekti i zotërimit të rreziqeve të sigurisë. Marrëdhëniet me zbatuesin e jashtëm të shërbimeve informative rregullohen me kontratë, e cila për mbrojtjen e informatave përmban përcaktime që sigurojnë nivel të njëjt të mbrojtjes që vlejnë për të punësuarit në Byronë Kosovare të Sigurimit.

4.11. Arsimimi i shfrytëzuesve të sistemit informativ

Të punësuarve në Byronë Kosovare të Sigurimit dhe bashkëpunëtorve të jashtëm duhet t'u sigurohet arsimimi adekuat dhe aftësimi për perdorim të sigurt me informata dhe kjo para se t'ju lejohet qasja në sistemin informativ. Kjo posaçërisht ka të bëjë me njoftimin e hollësishëm me dokumentet interne në lëmin e mbrojtjes së informatave dhe të parimeve të përgjithshme të praktikës së mirë mbrojtëse.

Shfrytëzuesit e sistemit informativ në Byronë Kosovare të Sigurimit duhet të jenë aty për aty, të njoftuar me ndryshimet dhe plotësimet e sistemit të mbrojtjes, posaçërisht me përgjegjësitë konkrete personale. Shfrytëzuesve të autorizuar duhet t'u sigurohet arsimimi adekuat plotësues në institucionet e jashtme.

4.12. Procedurat lidhur me incidentet e sigurisë

Për incidentet e sigurisë shfrytëzuesit e sistemit informativ të Byrosë Kosovare të Sigurimit duhet, pa vonesë, t'i lajmërojnë eprorët - Departamentin e Qendrës Informative ose Drejtorin. Raporti mund të jetë me gojë ose me shkrim dhe duhet të përmbaj sa më shumë informata për rrethanat në të cilat ka ardhur gabimi ose parregullsia në mënyrë që të konstatohet dhe të evitohet më lehtë gabimi.

Shfrytëzuesit e sistemit informativ janë të obliguara që të shënojnë çdo mungesë të mbrojtjes ose cënimet të sistemit informativ ose shërbimeve që i kanë hetuar ose që në të dyshojnë. Po ashtu, janë të obliguar të shënojnë çdo pasjisje programore, për të cilën u duket ose janë të bindur se nuk veprojnë drejtë ose janë të natyrës qëllimkeqe.

4.13. Planifikimi i afarizmit të pandërprerë

Drejtori i Byrosë Kosovare të Sigurimit është përgjegjëse për përgaditjen e planeve të afarizmit të pandërprerë të kompanisë në rastet e ndryshme të aksidenteve. Nga Qendra Informative duhet përgaditur planet e rivendosjes së sistemit informativ në rastet e rënies së pajisjeve, të humbjes së të dhënave, rënies se komunikimeve, energjisë elektrike si edhe të fatkeqësive natyrore dhe të tjera. Më këtë rast duhet siguruar pajisje të mjaftueshme rezervë në suaza vetanake ose tek partnerët e huaj. Posaçërisht duhet verifikuar mundësin e futjes në veprim sërish të sistemit nga kopjet e sigurisë të të dhënave dhe të programeve.

Planet e afarizmit të pandërprerë duhet verifikuar në praktikë dhe plotësuar sipas ndryshimeve në ambientin ligjor, afarist dhe teknologjik.

4.14. Kontrollimet e mbrojtjes së sistemit informativ

Në kuadër të mbrojtjes së sistemit informativ të Byrosë Kosovare të Sigurimit duhet rregullisht, kurse më së paku një herë në vit, të kontrollohen dokumentet dhe masat valide në lëmi,e posaçërisht:

1. vlerësimet e rreziqeve informative,të cilat paraqiten në ambientin afarist gjithnjë të përcjellur;
2. dokumentet e politikës mbrojtëse (politikat, rregulloret, procedurat e punës);

3. zbatimi dhe veprimi i masave mbrojtëse në praktikë, sidomos nga aspekti i përputhshmërisë me qëllimet e parashtruara, efikasiteti, shpenzimeve dhe ndikimit në afarizmin e institucionit.

Në bazë të këtyre kontrollimeve duhet në mënyrë adekuate të përputhet sistemi i mbrojtjes. Kontrollimet i realizojnë Drejtori, Departamenti i Qendrës Informative dhe Auditori i brendshëm.

5. Përcaktimi përfundimtar

5.1. Deklarata për njohjen dhe aprovimin e politikës të mbrojtjes

Të punësuarit në Byronë Kosovare të Sigurimit dhe zbatuesit e jashtëm, të cilët kanë qasje në sistemin informativ të Byrosë Kosovare të Sigurimit, duhet të nënshkruajnë deklaratën me të cilin vërtetojnë se janë të njoftuar me dokumentet e politikës mbrojtëse në shoqëri, që këto i kuptojnë dhe se me këtë aprovojnë përgjegjësi adekuate për mbrojtjen e të dhënave.

Deklaratat duhet të përfshijnë përcaktimet kyçe të rregullativës së brendshme për mbrojtjen e të dhënave, posaçërisht të atyre për të cilat është paraparë përgjegjësia potenciale materiale dhe penale sipas ligjit dhe ato, të cilat i përkasin obligimit të përherëshem të mbrojtjes së të dhënave të besueshme edhe pas skadimit të marrëdhënies së punës në Byronë Kosovare të Sigurimit. Nënshkrimi i deklaratës është kusht për punësim në Byronë Kosovare të Sigurimit. Nënshkrimi i deklaratës është kusht për punësim në Byronë Kosovare të Sigurimit, përkatësisht për atë që bashkëpunëtori i jashtëm me nënshkrim të deklaratës mund të ketë qasje në sistemin informativ të kompanisë. Deklaratën e nënshkruar e ruan administrata në dosjen personale të të punësuarit, përkatësisht në dosjen e zbatuesit të jashtëm. Përcaktimet e kësaj deklarate qëllimisht futen edhe në kontratat me zbatuesit e jashtëm.

5.2. Shkeljet e politikës së mbrojtjes dhe sanksionet

Shkeljet e përcaktimeve të politikës së mbrojtjes të sistemit informativ dhe të dokumenteve tjera të politikës mbrojtëse dhe të procedurave në Byronë Kosovare të Sigurimit paraqet shkelje të rëndë të obligimeve të punës, për të cilat punëtori mund të jetë përgjegjës në procedurë disiplinore, përkatësisht kundërvajtje ose veprim penal, sipas ligjit. Drejtoria në rast të dyshimit për shkelje, ngritë procedurë formale disiplinore.

Agim Elshani
Kryesuesi i Asamblesë së Përgjithshme të Anëtarëve

Prishtinë,
Datë 27.06.2022