UNIVERSITETI I TIRANËS
FAKULTETI I EKONOMISË
DEPARTAMENTI STATISTIKË & INFORMATIKË E ZBATUAR

PUNIM DIPLOME PËR PROGRAMIN E STUDIMEVE TË CIKLIT TË PARË BACHELOR NË DEGËN INFORMATIKË EKONOMIKE

Dobësitë dhe siguria e sistemeve të infomacionit

PUNOI:
GLIQIRI RIZA

PEDAGOGU UDHËHEQËS:
MSc. ROMINA MUKA

Tiranë, Shtator 2018

Deklaratë

Unë, e nënshkruara Gliqiri Riza, deklaroj që: (1) Kjo mikrotezë përfaqëson punimin tim origjinal, për trajtimin e temës së diplomës, përveç rasteve të cituara përgjatë punimit dhe referencave të përmendura në përfundim. Gjithashtu dëshmoj se (2) ky dokument nuk është përdorur më herët, si mikrotezë ose projekt në asnjë universitet tjetër.

Gliqiri Riza

Shtator 2018

Abstrakt

Sistemet e informacionit kanë ndryshuar mënyrën se si njerëzit jetojnë, bëjnë biznes, madje edhe mënyrën e qeverisjes. Këto sistemet janë shndëruar në një pjesë thelbësore të përditshmërisë, pasi përdorimet e tyre e bëjnë shumë më të lehtë dhe më të shpejtë kryerjen e detyrave të caktuara, të thjeshta a të një shkalle shumë të lartë kompleksiteti me një shpejtësi relativisht të madhe. Megjithatë bashkë me zhvillimet teknologjike të tyre, sistemet e informacionit përballen edhe me kërcënimet serioze të sigurisë, që vendosin në dyshim besueshmërinë dhe i bëjnë ato më të hapur e të ekspozuar ndaj sulmeve.

Në këtë punim do të trajtohen pikërisht çështje të sistemeve të informacionit të para nga këndvështimi i sigurisë. Pas një përshkrimi konciz të sistemeve të informacionit, njohjes me karakteristikat kryesore dhe llojet e sistemeve, kalohet tek pjesa analitike, ku qëllimi i kapitujve është njohja me dobësitë që shfaqin sistemet, problematikat, masat, politikat dhe arkitektura e nevojshme për pasjen e sistemeve të sigurta.

Një pjesë e rëndësishme e punimit lihet në dispozicion të sugjerimeve dhe masave që nevojiten të ndërmerren në mënyrë që sistemet e informacionit të plotësojnë objektivat nga ana e çështjeve të sigurisë. Kjo pjesë trajton gjithashtu projeksione dhe sfida që parashtrohen për të ardhmen duke dhënë rekomandime rreth përmirësimeve të mundshme.

Fjalë kyç: sistem, informacion, siguri, dobësi, besueshmëri, konfidencialitet.

Qëllimi i temës

Qëllimi i këtij punimi diplome është të analizojë sistemet e informacionit nga ana e sigurisë dhe dobësitë që ata shfaqin, të cilat cënojnë besueshmërinë e të dhënave dhe origjinalitetin e inputeve mbi të cilat ngrihen këto sisteme. Përgjatë punimit bëhet një përshkrim njohës me sistemet e informacionit, llojet kryesore të tyre dhe rëndësinë në rritje që ata po fitojnë me kalimin e kohës. Megjithatë theksi kryesor i punimit vendoset tek analizat nga ana e sigurisë, problematikat e hasura dhe masat për zgjidhjen e problemeve e mbrojtjen e sigurisë, qofshin ato të aplikueshme për situata konkrete apo të implementuara së bashku me sistemin, si pjese e arkitekturës së tij.

FALENDERIME DHE MIRËNJOHJE

Në përfundim të këtij cikli studimesh, dua të shpreh falenderimin tim për personat që më ndihuman për të përmbushur me sukses këtë rrugëtim, të cilëve sot u jam shumë mirënjohëse.

Së pari falenderoj stafin e pedagogëve dhe profesorëve, për ndihmën dhe punën e palodhur gjatë këtyre viteve! Gjithashtu gjatë kësaj periudhe, pata fatin dhe kënaqësinë e madhe të bashkëpunoj me MSc. Romina Muka, në rolin e pedagoges sime udhëheqëse. Ndaj një falenderim i veçantë i shkon asaj për mbështetjen e ofruar gjatë realizimit dinjitoz të këtij punimi dhe kontibutin e çmuar në finalizimin me sukses të tij. Faleminderit të gjithëve nga zemra!

Së fundi, mirënjohja më e thellë i shkon familjes sime, së cilës i detyrohem për gjithçka të arritur, për çdo sukses dhe njeriun që jam sot!

Faleminderit!

TABELA E PËRMBAJTJES

LISTA E SHKURTIMEVE

1. ACL - The Access Control List
2. AI - Artificial Intelligence
3. ALG - Application Layer Gateaways
4. CNSS - The Committee on National Security Systems
5. DES - Data Encryption Standard
6. DMZ – Demilitarized Zone
7. DSS - Decision Support System
8. EMR - Electronic Medical Record
9. ES - Expert System
10. IDS - Intrusion Detection Systems
11. IT - Information Technology
12. MIS - Management Information Systems
13. PF- Packet Filtering
14. RBAC- Role-Based Access Control
15. SDLC- System Development Life Cycle
16. SI - Sisteme Informacioni
17. SOAP- Simple Object Access Protocol
18. TPS - Transaction Processing System
19. UPS - Uninterruptible Power Supply
20. VPN - Vitual Private Network
21. XML - eXtensible Markup Language

LISTA E FIGURAVE

KAPITULLI 1
Hyrje

Zhvillimi i shpejtë i teknologjisë së informacionit, ka krijuar bindjen dhe na ka bërë më të ndërgjegjshëm se sistemet e informacionit janë një instrument i fuqishëm në zgjidhjen e problemeve. Fakti që sot jetojmë në një shoqëri informacioni, bën që këto sisteme të përdoren gjerësisht thuajse në çdo fushë të jetës. Duke filluar që nga shkollat, menaxherët e bizneseve, kujdesi shëndetësor e deri tek shërbimet ushtarake, sistemet e informacionit përdoren jo vetëm për rujatjen e të dhënave, por edhe për kryerjen e llogaritjeve, ndihmën në marrjen e vendimeve dhe veprime të tjera për editimin e të dhënave.

Duke pasur parasysh që shpesh këto të dhëna janë kritike dhe konfidenciale, kërkohen masa konkrete në mbrojtjen dhe sigurinë e tyre. Të dhënat janë padyshim pasuria më e vyer e një organizate dhe humbja, manipulimi dhe fakti që nuk arrihet të merren masat e duhura për mbrojtjen e tyre rezulton në kosto më të larta, humbje besimi të klientëve dhe investitorëve, madje ndonjëherë edhe kërcënim të sigurisë kombëtare të një vendi.

1.1 Prezantim i përgjithshëm

Përdorimi i sistemeve të informacionit është i lidhur ngushtësisht me informacionin sensitiv, humbja dhe manipulimi i të cilit është një rrezik që i kanoset kompanive apo organizatave që i përdorin ato. Prandaj, menaxhimi dhe mbrojtja e informacioneve sensitive që shërbejnë si input për sistemet e informacionit është shndëruar në prioritet dhe një nevojë në rritje.

Nisur nga fakti se në ditët e sotme sisteme të tilla përdoren jo vetëm për detyra bazike, por edhe në veprimtari shumë komplekse, siç janë vendimet e menaxherëve të një biznesi apo përcaktimi i diagnozave të pacientëve, në rastin e sistemeve të implemntuara në mjekësi, bën që të lindë nevoja e pasjes së informacioneve të duhura dhe të sigurta. Të dhëna të korruptuara dhe ndryshuara janë një kërcënim serioz, ndaj sot theksi vendoset fuqishëm tek siguria e këtyre të dhënave dhe mbrojtja e tyre, në mënyrë që rezultatet e sistemeve të informacionit të jenë faktike dhe të pakompromentuara.

1.2 Objektiva

Përgjatë këtij punimi do të realizohet njohja me sistemet e informacionit, çfarë janë dhe si funksionojnë, llojet e ndryshme të tyre duke përfshirë veçoritë përkatëse të secilit. Megjithatë fokusi do të përqëndrohet në dobësitë me të cilat hasen këto sisteme, sa i sigurt është

informacioni që shërben si input për to dhe arkitektura e nevojshme në pasjen e sistemeve të sigurta. Punimi ka gjithashtu një karakter analizues që synon të informojë rreth mirëmbajtjes së sistemve të tilla dhe masat e nevojshme që duhen ndërmarrë, me qëllim që të mos cënohet siguria e tyre. Së fundi, pas analizës së detajuar arrihet në konkluzione, sugjerime dhe projeksione rreth së ardhmes së SI.

KAPITULLI 2
Sistemet e informacionit

Teknologjia e informacionit dhe zhvillimi me shpejtësi i saj dekadat e fundit, bën që kompjuteri dhe aplikime të tjera të automatizuara të luajnë një rol jetik në shoqërinë e sotme. Detyra të thjeshta apo më komplekse që më herët kryheshim në mënyrë manuale dhe linin hapësirë për gabim, sot kryhen në një fraksion sekonde dhe nuk ka vend për dyshime në vërtetësinë e rezultatit. Për më tepër, kompjuterat me fuqi përpunuese tepër të lartë dhe në një kohë të shkurtër janë sot një instrument kyç në përpunimin e informacionit, duke bërë të mundur kryerjen e aktivitetve që dikur nuk mendohej të zgjidheshin nga një makineri. Si rezultat i këtyre rrethanave, zgjidhja e problemeve gjendet pikërisht tek sistemet e informacionit dhe implementimi i tyre për qëllime të caktuara.

2.1 Prezantim me sistemet e informacionit

Sistemet e informacionit janë bërë aq të zhvilluara, të detajuara dhe teknologjikisht të besueshëm, sa së bashku me besueshmërinë në rritje të tyre, vihet re një rritje të rentabilitetit, konkurrencës dhe efikasitetit për çdo biznes që ka të implementuar dhe përdor një sistem të tillë. Sistemet e informacionit mund të përkufizohen si një tërësi e organizuar komponentësh për mbledhjen, transmetimin, përpunimin dhe ruajtjen e të dhënave, në mënyrë që informacioni i përftuar të jetë i përdorëshëm për qëllime të tjera të mëtejshme. (Zwass, 1997)

Sa më e sofistikuar bëhet teknologjia, aq më tepër rritet disponueshmëria e shërbimeve të tilla për organizatat. Kështu për shembull, sistemet e informacionit bëjnë të mundur bërjen e biznesit në mënyra elektronike dhe larg asaj tradicionale, që kemi pare deri më tani. Njerëzit janë të aftë të menaxhojnë llogaritë e tyre bankare nëpërmjet bankave online në çdo kohë dhe kudo, në vend që të paraqiten fizikisht pranë një filiali banke, duke shmangur vonesat, rradhët e gjata dhe pa iu nënshtruar proceseve të gjata të verifikimit. Përveç kësaj, transaksionet kryhen nëpërmjet fatura elektronike, në vend të faturave të letrës për të reduktuar shpenzimet e dorëzimit të fletëpagesave.

2.1.1 Çfarë është një SI?

Një sistem informacioni është një tërësi elementesh të ndërlidhur që mbledhin, manipulojnë dhe afishojnë të dhënat dhe informacionet si dhe parashikojnë edhe një mekanizëm

feedback-u, për të kontrolluar nëse objektivat janë përbushur ose jo. (Ruseti et al., 2005) Sistemet e informacionit dhe implementimi i tyre kanë si funksion kryesor të ofrojnë vlerë për përdoruesit nëpërmjet shërbimeve që priren të lehtësojnë veprimtaritë e tyre të përditshme.

2.1.2 Karakteristika të përgjithshme

Siç jepet edhe nga përkufizimi, një sistem informacioni nuk mund të kuptohet i veçuar nga mbledhja, përpunimi dhe afishimi i të dhënave, procese mbi të cilat ngrihet vetë ekzistenca e sistemit. Mbledhja e të dhënave ose grumbullimi i tyre është hapi i pare dhe duhet patur parasysh që të kryhet me rigorozitet pasi këto të dhënat do të shërbejnë si input për sistemin. Ndaj ato duhet të jenë të sakta, pa gabime dhe të pa kompromentuara. Pikërisht mbi këto të dhëna kryhen llogaritje, krahësime, veprime matematikore ose editime të tjera, me qëllim që ato të kthehen në output të përdorshëm dhe ky është pikërisht procesi i përpunimit të të dhënave. Kur rezultati i tyre shfaqet në formën e dokumentave e raporteve dhe është i gatshëm për të gjeneruar rezultat për qëllime të ndryshme, themi se kemi të bëjmë me output. Mënyra se si të dhënat mblidhen, përpunohen dhe afishohen bën që sistemet e informacionit të ndahen në dy grupe të mëdha, manule dhe të kompjuterizuar. Megjithatë, mund të ndodhë që gjatë këtyre hapave të ndodhin gabime dhe rezultati të mos jetë faktik. Për të kontrolluar dhe korrigjuar të tilla situata përdoret mekanizmi i feedback-ut.

2.2 Rëndësia e tyre në shoqërinë e sotme

Në ditët e sotme, sistemet e informacionit luajnë një rol jetik në mbarëvajtjes e punës dhe proceseve të ndjekura nga organizatat, firmat dhe kompanitë. Vlen të përmendet se, pavarësisht shtrirjes dhe implementimit të tyre të gjerë në shumë fusha, bizneset janë thuajse të varur nga këto sisteme për të pasur sukses. Ka shumë arsye pse sistemet e informacionit janë kaq të rëndësishme dhe të nevojshme.(Henderson et al., 1999)

Së pari, nëpërmjet tyre bizneset mund të përmirërojnë vazhdimisht efikasitetin e veprimtarive të tyre për të arritur përfitueshmëri më të lartë dhe përsosmëri operacionale. Kjo për shembull bëhet e mundur gjatë kontrolleve të inventarit, në mënyrë që konsumatorët të gjejnë gjithmonë atë që kanë dëshirë.

Së dyti, sistemet e informacionit luajnë një rol të madh për bizneset në krijimin e produkteve dhe shërbimeve të reja. Modele të reja biznesi mund të krijohen dhe ato përshkruajnë se si një kompani prodhon, krijon dhe shet produktet e shërbimet e saj.

Për më tepër, këto sisteme ndihmojnë shumë edhe në krijimin e një marrëdhënieje besueshmërie me konsumatorët dhe furnitorët. Kur një komani i ofron shërbime cilësore konsumatorëve të saj, më shumë gjasa që ata të kthehen përsëri dhe si rezultat do të bëhen më shumë porosi për furnitorët, duke krijuar kështu afrimitet me të dyja palët.

Sistemet e informacionit gjithashtu bëjnë të mundur që menaxherët të përdorin të dhëna në kohë reale, për të marrë vendimet e duhura në lidhje me menaxhimin strategjik. Kështu, jo vetëm përmirësojnë vendimmarrjen, por kursejnë edhe kohën dhe koston, që në rrethana të tjera do u duhej të shpenzonin për të kërkuar paraprakisht informacionin e nevojshëm.

Nga ana tjetër duhet thënë se, bizneset investojnë në këto sisteme, jo vëtëm për konsumatorët, por edhe për të bërë punët e tyre sa më lehtë që munden. Për shembull, Citibank prezantoi makinën e parë të ATM-ve për të bërë më të lehtë për klientët pasjen e aksesit në paratë e tyre, por edhe për të ulur rradhët në banka.

Së fundi, kur një kompani implementon një sistem të tillë, ajo është e prirur të sigurojë avantazh kompletitiv mbi konkurrentët dhe rivalët e saj në treg. Kjo bën që të rritet besimi tek kompania, përfitueshmëria dhe të ardhurat e saj.

KAPITULLI 3
Kategorizimi në disa lloje dhe prezantimi i tyre

Sistemet e informacionit, ashtu siç u paraqit edhe më herët, nisur nga zhvillimet e shpejta teknologjike, janë shumë të përdorëshëm në fusha të ndryshme të veprimtarisë njerëzore, nga veprimet më të thjeshta, e deri tek zgjidhja e problemeve shumë serioze dhe komplekse, ku thujse po zëvendësojnë trurin njerëzor. Për këtë arsye, nevojitet që, bazuar në qëllimin e përdorimit të një sistemi informacioni, të projektohen dhe dizenjohen sisteme me karakteristika të veçanta dhe të ndryshëm nga njëri-tjetri, por me qëllimin e përbashkët, përmbushjen me sukses të objektivave dhe zgjidhjen e problemeve.

3.1 Llojet kryesore

Për zgjidhjen e problemeve të ndryshme që parashtrohen dhe arsyen pse po implementohet dhe përdoret një sistem informacioni, ekzistojnë lloje të ndryshme sistemesh të tilla. Sistemet e informacionit kategorizohen në disa lloje kryesore, ku përfshihen sistemet e përpunimit të transaksioneve, sistemet e informacionit të menaxhimit, mbështetjes së vendimeve, sistemet ekspert dhe inteligjenca artificiale. Secili prej tyre ka një tërësi veçorish dhe karakteristikash, të cilat jepen në vijim:

3.1.1 Sistemet e përpunimit të transaksioneve

TPS(Transaction Processing Systems), të njohura gjerësisht si sistemet e përpunimit të transaksioneve janë sisteme që merren me përpunimin e informacioneve për transaksionet rutinë të biznesit, duke përfshinë grumbullimin, modifikimin dhe ruajtjen e dhënave. Më pas, për këto të dhëna të procesuara, këto sisteme gjenerojnë në kohë reale raporte dhe dokumenta. (O'Brien, 2005)

Karakteristikat e një TPS përfshijnë performancën, besueshmërinë dhe qëndrueshmërinë. Për të përmbushur këto veçori, të dhënat duhet të jenë lehtësisht të disponueshme në një depo të dhënash(data warehouse), duhet të ekzistojnë procedurat e ruajtjes dhe procesi i rikuperimit, në mënyrë që me anë të back-up-eve të herëpasherëshme të mbrohen të dhënat nga dështimet e sistemit, të njeriut, viruset kompjuterike, aplikacionet e dëmshme softuerike ose fatkeqësitë natyrore.

Shpesh, TPS krahësohen me sistemet e përpunimit batch, ku shumë kërkesa ekzekutohen në të njëjtën kohë, megjithatë ndërmjet tyre ka ndryshime thelbësore. Sistemet e përpunimit të transaksioneve kërkojnë ndërveprimin e përdoruesit, ndyshe nga përpunimi batch ku nuk kërkohet përfshirja e tij. Në përpunimin batch rezultatet e çdo transaksioni nuk janë të disponueshme menjëherë, por me një vonesë, sepse shumë kërkesa janë duke u ekzekutuar dhe ruajtur. Në përpunimin e transaksioneve nuk ka vonesë dhe rezultatet e çdo transaksioni janë të disponueshme në kohë reale, ndaj ato njihen shpesh edhe si sisteme real- time. Zakonisht, sistemet TPS kanë një shkallë të lartë integriteti të të dhënave, ku gabimet janë të rralla, të tolerueshme dhe mund të kontrollohen lehtësisht. Ndërsa tek përpunimi batch nuk mund të thuhet e njëjta gjë, pasi gjatë vonesës kohore, gabimet janë të shpeshta dhe të dhënat mund të kompromentohen.

3.1.2 Sistemet e informacionit të menaxhimit

MIS(Management Information Systems) është akronim që përdoret për t'iu referuar sistemeve të informacionit të menaxhimit. Një MIS është është një bashkësi e integruar sistemesh, pajisjesh, procedurash, baza të dhënash dhe njerëzish, që ndërveprojnë së bashku për të përpunuar, ruajtur dhe prodhuar informacione të dobishme për organizatën. (O'Brien et al., 2006)

Sistemet e informacionit të menaxhimit kanë si qëllim të ndihmojnë në përmbushjen me sukses të objetivave të një organizate. Ato janë një ndihmë e madhe për drejtuesit e menaxhimit strategjik të kompanive në organizimin, planifikimin dhe përmbushjen me sukses dhe efiçencë të detyrave, si dhe në marrjen e vendimeve të duhura në procesin e punës. Kjo realizohet nëpërmjet raporteve që gjenerohen nga sistemet e informacionit të menaxhimit. Këto raporte mund të jenë hard ose soft copy, në formate fikse ose standard dhe përdorin si input të dhënat e brendëshme të vendosura në sistem. Rëndësia e raporteve të MIS qëndron në faktin që ndihmojnë menaxherët jo vetëm në marrjen e vendimeve, por edhe për të hartuar plane të suksesshme biznesi dhe pasjen e kontrollit mbi veprimtarine operacionale të kompanisë.

3.1.3 Sistemet e mbështetjes së vendimeve

DSS(Decision Support Systems) ose sistemet e mbështetjes së vendimeve janë sisteme interaktive të bazuara në software, që synojnë të ndihmojnë menaxherët në vendimmarrje, në rastet kur kemi të bëjmë me problem të pasrtukturuara dhe vëllime të mëdha të informacioni, që mund të jetë gjeneruar nga sisteme të ndryshme informacioni, të përfshira në proceset organizative të biznesit. (McLeod et al., 2007) DSS përdor informacion përmbledhës, trendet, modelet përjashtimore dhe analitike, në mënyrë që vendimi të jetë i duhur dhe frytdhënës . Një sistem i mbështetjes së vendimeve vërtet ndihmon në vendimmarrje, por nuk jep domosdoshmërisht një vendim. Më pas me anë të raporteve që përpilohen nga DSS në përfundim të procesit, nga dokumentat dhe informacionet e përpunuara, janë vendimmarrësit ata që identifikojnë dhe zgjidhin problemet dhe marrin vendime.

Vendimet të cilat merren me ndihmën e një sistemi të tillë janë dy llojesh, vendime të programuara dhe jo të programuara.Vendimet e programuara janë në thelb procese të automatizuara ose për punë të përgjithshme rutinore, të cilat ndodhin më shumë se sa një here dhe ekzistojnë rregulla dhe udhëzime fikse për zgjidhjen e tyre.Vendimet e paprogramuara, nga ana tjetër ndodhin në situata të pazakonta dhe jo të adresuara, kur kemi të bëjme me vendime të reja që nuk kanë protokolle të fiksuara, por merren në bazë të informacionit në dispozicion. Sistemet e mbështetjes së vendimeve zakonisht përfshijnë vendime jo të programuara pasi ato bazohen në diskrecionin, perceptimin dhe gjykimin personal të personit drejtues.

Prandaj, në këto raste raportet gjenerohen në varësi të situatës dhe me një përmbajtje e format të caktuar.

3.1.4 Inteligjenca artificiale

Inteligjenca artificiale, e referuar shpesh edhe si AI(Artificial Intelligence) është fushë e shkencave kompjuterike që thekson krijimin e makinave inteligjente që punojnë dhe reagojnë si njerëzit, duke shfaqur karakteristika të inteligjencës. Së fundi AI po shndërohet me shpejtësi në një pjesë shumë thelbësore të industries teknologjike, duke qënë se hulumtimet dhe rezulatet e saj bëhen gjithnjë e më teknike e të specializuara. Sisteme ose pajisje të tilla kompjuterike, për përmbushjen e objektivave projektohem me tipare si aftësia për të arsyetuar, perceptimi dhe zgjidhja e problemeve, veprimi në situata të panjohura e komplekse duke zbatuar njohuritë e fituara nga eksperienca e mëparshme, aftësia për të manipuluar objekte, etj.

Me shpikjen e teknologjive të reja revolucionare, superinteligjenca ndihmon në zgjidhjen e problemeve madhore, si të kurimi i sëmundjet, simulimi i realitetit virtua për t'i bërë situatat sa më të prekshme dhe mund të jetë ngjarja më e madhe në historinë njerëzore. Prandaj gjatë dizenjimit të sistemeve të tilla, ekziston si qëllimi kryesor vlefshmëria, siguria dhe kontrolli. Megjithatë vëmendja kryesore përqëndrohet tek siguria, duke qënë se, hakimi apo dështimi i sistemit në një kompjuter të zakonshëm nuk është më shumë se një shqetësim i vogël, por në rast se kemi të bëjmë me një sistem inteligjent që kontrollon makinën, aeroplanin, stimuluesin, apo çdo sistem tjetër situata bëhet tepër serioze dhe çështja e sigurisë, gjithnjë e më e rëndësishme. (Bench-Capon et al., 2007)

3.1.5 Sistemet ekspert

Këto lloj sistemesh, të cilave shpesh u referohen edhe si ES(Expert Systems) janë programe kompjuterike që përdorin teknologjitë e inteligjencës artificiale për të simuluar gjykimin dhe sjelljen e një njeriu ose një organizate që ka njohuri dhe përvojë eksperte në një fushë të caktuar. Sistemet ekspert përdoren gjerësisht sot në shumë industri, shërbime financiare, telekomunikacionin, kujdesin shëndetësor, përcaktimin e diagnozave mjekësore, lojërat elektronike dhe aviacion.

Në mënyrë të përmbledhur, një sistem ekspert përfshin një bazë të njohurish që përmban përvojën e grumbulluar dhe konkluzione ekspertësh të fushës, të organizuara në protokolle ose grupe rregullash për zbatimin e bazës së njohurive për çdo situatë të veçantë që përshkruhet në program. Aftësitë e sistemit mund të përmirësohen duke e përditësuar bazën e njohurive me rregulla të reja, vërtetësia e të cilave është provuar shkencërisht. Sistemet aktuale përfshijnë aftësit zgjidhjeje të problemeve bazuar në përvojë, ashtu si bëjnë njerëzit ndaj besueshmëria dhe siguria e tyre është gjithnjë në rritje. (Jackson, 1998)

KAPITULLI 4
Siguria e sistemeve të informacionit

Sistemet e informacionit janë bërë pjesë integrale e jetës së përditshme në shtëpi, biznese, qeveri dhe organizata. Megjithatë bashkë me zhvillimin dhe përhapjen në masë të tyre, edhe siguria e sistemeve të informacionit është një nga sfidat më të mëdha me të cilat ballafaqohet epoka teknologjike e shoqërisë. Duke qënë se brezi i tanishëm teknologjik është bërë kaq i varur nga sistemet e informacionit, problemet që i kanosen sistemeve të informacionit kërcënojnë gjithashtu rendin e veprimtarive të përditshme. Megjithëse aktivitetet e përditshme të tyre janë është zhvilluar thuajse deri në përsosje, ka shumë probleme aktuale si hakimi, spamming, software me qëllim të keq, spoofing dhe vjedhjet e identitetit, që kërcënojnë besueshmërinë dhe sigurinë e sistemeve të informacionit.

4.1 Çfarë është siguria e sistemeve të informacionit?

Në thelb, siguria përkufizohet si gjendja e të qënit i lire nga rreziqet dhe i mbrojtur nga kundërshtarët apo kushdo tjetër që me ose pa qëllim synon të të dëmtojë. (Whitman et al., 2009) Megjithatë, në kontekstin e të dhënave dhe sistemeve të informacionit, siguria i referohet ruajtjes së të dhënave dhe sistemeve nga aksesi i paautorizuar, përdorimi, zbulimi, prishja, modifikimi ose shkatërrimi i çdo forme tjetër. CNSS e perkufizon sigurinë si mbrojtjen e informacionit dhe elementëve të tij kritikë, duke përfshirë sistemet dhe pajisjet hardware që përdorin, ruajnë dhe transmetojnë të dhënat. Masat e nevojshme për të pasur sisteme të sigurta informacioni janë: politikat, ndërgjegjësimi, trajnimi, edukimi dhe teknologjia.

4.1.1 Politikat e sigurisë

Për të mbrojtur sigurinë e sistemve të informacionit ekzistojnë një sërë kontrollesh e mjetesh të mundshme, por organizatat gjithashtu duhet të zbatojnë politikat e sigurisë si një formë e kontrollit administrativ. Një politikë të mire, SANS Institute e përkufizon si një deklaratë ose plan i formalizuar, i shkurtër dhe i nivelit të lartë që përfshin përqasjet e përgjithshme të një organizate, qëllimet, objektivat dhe procedurat e pranueshme për një fushë të caktuar lëndore. Politikat kërkojnë pajtueshmëri ndaj mosrespektimi i një politike rezultojë në veprime disiplinore.

Politikat e sigurisë janë një pikë fillimi në zhvillimin e një plani të përgjithshëm sigurie pasi një politikë e mirë informacioni siguron udhëzimet për punonjësit që përdorin informacionet e kompanisë dhe i ofron kompanisë mundësi për rekurs në rast se një punonjës bën një shkelje. Ato zakonisht nuk përcaktojnë detajet specifike teknike, por fokusohen në rezultatet e dëshiruara dhe bazohen në parimet udhëzuese të konfidencialitetit, integritetit dhe disponueshmërisë.

4.2 Mjetet e sigurisë së sistemeve

Për të mbrojtur sisgurinë e sistemeve të informacionit, organizatat kanë në dispozicion një shumëllojshmëri mjetesh. Secili prej këtyre mjeteve mund të përdoret si pjesë e një politike të përgjithshme të sigurisë së informacionit, me qëllim përmbushjen me sukses të objektivave.

1. Së pari, një nga mjetet kryesore është autentifikimi. Autentifikimi mund të arrihet duke identifikuar dikë përmes një ose më shumë prej tre faktorëve: diçka që ata e dinë, diçka që ata kanë, ose diçka që ata janë. Forma më e zakonshme është identifikimi i përdoruesit dhe fjalëkalimi por ajo është lehtësisht e kompromentueshme dhe nga ana tjetër edhe identifikimi me çelës ose kartë mund të jenë problematike, duke qënë se identiteti mund të vidhet lehtë. Së fundi po përhapet në masë përdorimi i pamjes në identifikim, por sa efektive mund të jetë kjo metodë para një ATM-je? Prandaj një mënyrë më e sigurt për të autentikuar një përdorues është të bëhet vërtetimi i shumë faktorëve, duke kombinuar dy ose më shumë faktorë të renditur më lart. Një shembull i kësaj do të ishte përdorimi i një RSA SecurID token. Pajisja RSA do të gjenerojë një kod të ri hyrjeje çdo gjashtëdhjetë sekonda. Për të hyrë në një burim informacioni duke përdorur pajisjen RSA, duhet bërë kombinimi i një PIN-i me katër shifra, me kodin e gjeneruar nga pajisja. E vetmja mënyrë për të vërtetuar siç duhet është duke i ditur të dyja dhe duke pasur pajisjen RSA.

2. Një tjetër mjet sigurie është kontrolli i aksesit në informacion. Pasi një përdorues vërtetohet, hapi pasardhës është sigurimi se ata që mund të aksesojnë burimet e informacionit janë personat e duhur. Kjo bëhet përmes përdorimit të kontrollit të aksesit, për të cilin ekzistojnë disa modele të ndryshme. Për çdo burim informacioni që një organizatë dëshiron të menaxhojë, mund të krijohet një listë e përdoruesve që kanë aftësinë për të ndërmarrë veprime specifike. Ajo quhet listë e kontrollit të aksesit(ACL)

dhe për secilin përdorues caktohen aftësi specifike si leximi, shkrimi, fshirja ose shtimi. Vetëm përdoruesit me ato aftësi lejohen të kryejnë këto funksione dhe nëse një përdorues nuk është në listë, ata nuk kanë aftësi për të ditur madje as ekzistencën e burimit të informacionit.

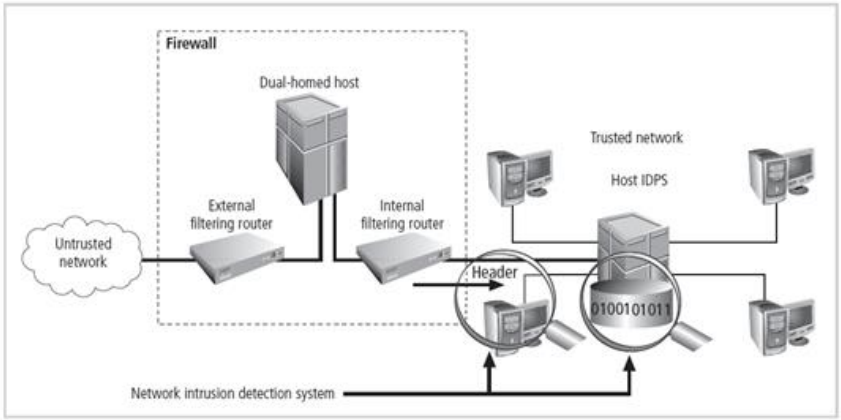
ACL-të janë të thjeshta për të kuptuar dhe ruajtur, megjithatë kanë disa mangësi, për shembull, çdo burim informacioni duhet të menaxhohet veçmas, kështu që nëse një administrator sigurie dëshiron të shtojë ose të largojë një përdorues në një sërë burimesh informacioni, procesi do të ishte mjaft i komplikuar dhe me rritjen e numrit të përdoruesve e burimeve, ACL-të bëhen të vështira për t'u mbajtur. Kjo ka çuar në një metodë të përmirësuar të kontrollit të aksesit, të quajtur kontroll i aksesit bazuar në rol, ose RBAC. Me RBAC, në vend që t'u japin përdoruesve të caktuar të drejtat e qasjes në një burim informacioni, atyre u caktohen role.Më pas, nëpërmjet këtyre roleve pëcaktohen rregullat e aksesimit. Kjo u lejon administratorëve një punë më të thjeshtuar për të menaxhuar përdoruesit me role të veçanta dhe përmirësimin e sigurisë.

3. Duke përdorur teknologjitë e tjera të sigurisë, organizatat mund të mbrojnë në mënyrë efektive burimet e tyre të informacionit duke i bërë ato të padukshme për botën e jashtme, por në rastet kur punonjësve apo konsulentëve u duhet të punojnë nga shtëpia dhe aksesojnë të dhënat rrjetit të brendshëm të biznesit nga një vendndodhje e largët, këto masa nuk janë frytdhënëse. Në këto raste, kërkohet një rrjet vitual privat(VPN). VPN lejon një përdorues që ndodhet jashtë rrjetit të korporatës të kalojë përmes firewall-it dhe të hyrë në rrjetin e brendshëm. Përmes një kombinimi të software-ve dhe masave të sigurisë, kjo i lejon një organizate të lejojë qasje të kufizuar në rrjetet e saj, duke mundësuar njëkohësisht një siguri të përgjithshme.

4. Një tjetër pajisje që mund të vendoset në rrjet për qëllime sigurie është sistemi për zbulimin e ndërhyrjeve ose IDS. Një IDS nuk aplikon ndonjë masë sigurie shtesë, por në vend të kësaj, ajo ofron funksionalitetin për të identifikuar nëse rrjeti po sulmohet dhe është një pjesë thelbësore e çdo konfigurimi të mirë të sigurisë. Ky lloj sistemi mund të konfigurohet për të parë për lloje të veçanta aktivitetesh dhe pastaj të lajmërojë personelin

e sigurisë nëse aktiviteti ndodh. IDS gjithashtu mund të identifikojë lloje të ndryshme të trafikut në rrjet, informacioni i të cilave mund të përdoret për analiza të mëvonshme.

Përdorimi i IDS për sigurinë e rrjetit



Burimi: Principles of information Security

Fig. 4.1

5. Gjithashtu një mjet thelbësor për sigurinë janë planet e back-up-it të informacionit për organizatën, pasi të dhënat duhet të mbahen jo vetëm në serverat e korporatës, por gjithashtu duhet të replikohen edhe në një server të largët(offsite storage). Kjo bëhet pasi, nëse të gjitha informacionet ruhen në të njëjtën strukturë si kopjet origjinale të të dhënave, në raste fatkeqësie natyrore ose dështimi, ato do të humbasin plotësisht. Një plan i mirë back-up përbëhet nga disa komponentë. Së pari nevojitet një analizë e plotë e burimeve të informacionit organizativ, që konsiston në një inventar të plotë të gjithë të dhënave, qofshin ato në server, Cloud apo kujtesa të jashtme dhe përcaktimin e mënyrës më të mirë për mbrojtjen e tyre. Një tjetër aspekt thelbësor është frekuenca e back-up-eve të informacionit, shpeshtësia e të cilave bazohet në atë se sa të rëndësishme janë të dhënat për kompaninë, e kombinuar me aftësinë e kompanisë për të zëvendësuar çdo të dhënë që është humbur. Të dhënat kritike duhet të bëhen back-up çdo ditë, ndërsa të dhënat më pak kritike mund të replikohen çdo javë. Së fundi, kryhet testimi i rivendosjes së të dhënave, ku rregullisht, kopjet rezervë duhet të vihen në provë duke u rikthyer në serverin aktual. Kjo do të sigurojë që procesi po funksionon në rregull dhe të dhënat ruajnë besueshmërinë e origjinalitetin.

(Bourgeois et al., 2015)

4.3 Trekëndëshi CIA i sigurisë së informacionit

Që prej fillimeve historike të modeleve të sigurisë së informacionit apo futjes në përdorim të kompjuterave, modeli tradicional CIA (Confidentiality, Integrity dhe Availability), është përdorur siparimi bazë i sigurisë së informacionit. Prej më shumë se njëzet vjetësh siguria e informacionit përdor konfidencialitetin, integritetin dhe disponueshmërinë si parimet kryesore të saj. (CNSS, 1992)

Konfidencialiteti i referohet aftësisë që informacioni dhe të dhënat të jenë të besueshme dhe të mos ekspozohen ndaj personave e sistemeve të tjera të paautorizuar për të pasuar akses tek to. Transaksionet me kartë krediti në internet dhe të dhënat personale mjekësore në kujdesin shëndetësor janë rastet tipike kur të dhënat duhet të mbahen konfidenciale. Integriteti, nga ana tjetër lidhet me aftësinë e informacionit për të qënë i plotë, i pakorruptuar apo ndryshuar në forma të tjera. Integriteti siguron që të dhënat janë të sakta dhe të kenë një përfaqësim origiinal e të pandryshuar. Së fundi, disponueshmëria i mundëson përdoruesve që të aksesojnë informacionin në kohën që duan dhe të dhënat të vihen në dispozicion të tyre pa pengesa. Për shembull parandalimi i sulmeve të mohimit të shërbimit në sistemet bankare online do të ishte një rast i suksesshëm i zbatimit të këtij parimi.

Megjithëse modeli CIA është i përshtatshëm në sistemet ku veprimet llogaritëse janë të thjeshta, ai nuk shihet si i përshtatshëm për sisteme më të mëdha dhe më komplekse siç janë ato që lidhen me biznesin elektronik(e-biznes), sistemet elektronike të regjistrave mjekësor(EMR) dhe sistemet qeverisëse elektronike (e-gov). Kjo ndodh për shkak se ky model shfaq mangësi thelbësore në ekzistencën e vet. Për shembull, karakteristikat e mos-refuzimit dhe autenticitetit të zhvillimit aktual të informacionit nuk përfshihen në modelin CIA. Gjithashtu, një fushë tjetër që ha debat rreth këtij modeli është posedimi i informacionit. Për shembull, bërja e kopjeve të paautorizuara të softuerit me të drejtë autori përbën vjedhje, por nuk shkel parimet e modelit CIA dhe rasti cilësohet më tepër posedim sesa cënim i konfidencialitetit, integritetit dhe disponueshmërisë. (Parker, 1998)

4.4 Metodologjia SDLC për zhvillimin e sistemeve të sigurta

Siguria e sistemeve të informacionit mund të kontrollohet nëpërmjet masave mbrojtëse që synojnë t'i bëjnë sistemet sa më të besueshëm. Megjithatë një hap i rëndësishëm për mbrojtjen e sigurisë së tyre fillon që me dizajnimin dhe zhvillimin. System Development Life Cycle ose SDLC, që i referohet pikërisht ciklit të jetës së zhvillimit të sistemeve është një metodologji për dizenjimin dhe implementimin e sistemeve të sigurta në kompani dhe organizata. Ajo i referohet një qasjeje formale, bazuar në në një sekuencë të strukturuar procedurash, që synojnë të zgjidhin problemet dhe përmbushin objektivat. Në këtë mënyrë procesi i ndodhur është rigoroz dhe probabiliteti i suksesit rritet ndjeshëm.

SDLC përbëhet nga gjashtë faza kryesore. Së pari, investigimi lidhet me vendosjen e objektivave dhe kufizimeve për të përcaktuar çfarë bën sistemi dhe problemet që ai zgjidh. Faza e dytë është Analiza, që konsiston në vlerësimin e organizatës, sistemeve aktuale dhe mangësive të tyre ekzistuese në lidhje me çështjet e sigurisë. Së treti qëndron dizenjimi logjik, pra zgjedhja e aplikimeve dhe programeve të afta për të ofruar zgjidhjet e nevojshme dhe pas tij dizenjimi fizik që lidhet me teknologjitë që mbështesin alternativat e përcaktuara nga dizenjimi logjik. Pasi të gjitha këto hapa kryhen me sukses, sistemi i ri që blihet ose krijohet, implementohet në organizatë dhe kryhen testet e pranimit dhe performancës së tij. Së fundi qëndron faza e mirëmbajtjes dhe ndryshimeve, që merret me rishikimin dhe modifikimet e mundshme të sistemit në mënyrë që të përmbushen me efektivitet objektivat. Kjo është faza më e gjatë dhe në shumicën e rasteve edhe më e shtrenjta. (Whitman, et al., 2009)

KAPITULLI 5
Dobësitë që hasen

Siguria e sistemeve të informacionit është e lidhur ngushtësisht me integritetin, privatësinë dhe konfidencialitetin e burimeve dhe aktiviteteve të saj. Nëse integriteti i tyre i referohet faktit se sa të besueshme janë të dhënat për t'u përdorur në vazhdim, konfidencialiteti është status i akorduar ndaj të dhënave, duke kufizuar përdorimin dhe shpërndarjen e tyre, në mënyrë që disa të dhëna të mbahen të pazbuluara.(Joshik, 2015) Mbajtja e të dhënave konfidenciale realizohet me anë të politikave të privatësisë.

Megjithatë thuajse shumicën e kohës, për shkak të faktorëve e shkaqeve të ndryshme, kompanive u kanoset një rrezik konstant, që i bën sistemet e informacionit më vulnerabël dhe të aftë për t'u sulmuar. Për pasojë, kompania mund të përballet me humbje apo vjedhje informacionit, korruptim e manipulim të të dhënave apo probleme të tjera teknike, që pengojnë mbarëvajtjen e proceseve të punës. Këto faktorë kërcënues quhen ndryshe edhe dobësi të sistemit dhe për t'i mënjanuar apo mbajtur ato në kontroll është e nevojshme që një organizatë të identifikojë natyrën e kërcënimeve të mundshme dhe të krijojë një sërë masash, për të siguruar privatësinë dhe konfidencialitetin e informacionit të ruajtur në sistem.

5.1 Çfarë janë dobësitë e sistemeve të informacionit?

Dobësitë e një sistemi informacioni, i referohet një termi sigurie kibernetike që përbbledhe çdo të metë në sistem duke e bërë atë më të rrezikuar për t'u sulmuar. Një dobësi gjithashtu i referohet çdo lloj mangësie në një sistem kompjuterik, që e ekspozon sigurinë e informacionit ndaj çdo kërcënimi të mundshëm.(Alghazzawi et al, 2014) Një nga objektivat primarë në dizenjimin dhe mirëmbajtjen e sistemeve të informacionit është zvogëlimi sa më shumë të jetë e mundur i dobësive, pasi kjo bën që hackerat dhe individët e rrezikshëm të kenë më pak shanse për të aksesuar informacionin e paautorizuar. Përdoruesit e një sistemi kompjuterik dhe personeli mirëmbajtës mund të mbrojnë sistemet e informacionit nga dobësitë duke përditësuar software-t në mënyrë të vazhdueshme. Kështu jo vetëm përmirësohen gabimet, por gjenden gjithashtu edhe dobësitë ekzistuese në software-t aktualë dhe kërkohen mënyra për të mbrojtur kundër tyre.

5.2 Kërcënimet kryesore të sigurisë

Siç u paraqit edhe më herët, dobësitë e sistemeve të informacionit, nëse nuk trajtohen me seriozitetin e duhur e bëjnë sistemin vulnerabël dhe shumë të ekspozuar ndaj risqeve që i kanosen. Kjo bën që siguria e sistemit të cënohet dhe për pasojë sistemi, besueshmëria e tij dhe të dhënave që ai proceson të vihen në rrezik. Gjatë gjithë kohës ndaj sistemit parashtrohen kërcënime të shumta, megjithatë kërcënimet e sigurisë kanë katër burime kryesore:

5.2.1 Abuzimi dhe krimi kompjuterik

Krimi kompjuterik përfshin çdo veprim të paligjshëm në të cilin përdoret si mjet primar një kompjuter, ndërsa abuzim është përdorimi joetik i një kompjuteri. Kërcënimet e sigurisë të lidhura me krimin kompjuterik ose abuzimin përfshijnë:

1. Viruset kompjuterike janë segmente kodit që janë në gjendje të kryejnë veprime me qëllim të keq si futja në sistem e kopjeve të programeve të tjera të replikueshme në mënyrë të pavarur. Viruset infektojë programet dhe sistemet në mënyrë progressive. Programi i sulmuar mund të funksionojë siç duhet, por në një moment të caktuar do të kryejë një veprim destruktiv të ideuar nga sulmuesi që shkruan virusin. Të ngjashëm me viruset janë edhe krimbat. Ato janë programe të pavarura që transmetojnë kopje të vetes përmes rrjeteve të telekomunikacionit dhe kanë nevojë për një veprim, për shembull klikim që të fillojnë replikimin.
2. Metoda e kalit të Trojës është maskimi i një sërë udhëzimesh të dëmshme brenda një programi të autorizuar që të shkaktojnë veprime të paautorizuara.
3. Bombat logjike janë udhëzime të paautorizuara, të bashkëngjitura shpesh me teknikën e kalit të Trojës, të cilat qëndrojnë pasive derisa të ndodhë një ngjarje specifike ose deri në një kohë specifike. Kjo ndodh pasi janë të programuar në mënyrë të tillë që të mbajnë kontrollin e orës së brendshme të kompjuterit.
4. Mohimi i Shërbimit(Denial of Service) ndodh kur sistemi bëhet i papërdorshëm nga përdoruesit legjitimë.
5. Rrjedhja e të dhënave ndodh si pasojë e një shumëllojshmërie metodash për marrjen e të dhënave të ruajtura në një sistem, prandaj për mbrojtjen e tyre mund të përdoret kodimi.

6. Përfytyrimi është të fituarit e aksesit në sistem duke identifikuar veten si një person tjetër. Në këtë mënyrë duke shmangur kontrollet e identifikimit apo përdorur të dhëna legale, të njohura nga sistemi, imituesi gëzon privilegjet e një përdoruesi legjitim.
7. Dial Diddling i referohet ndryshimi i të dhënave para ose gjatë hyrjes, me qëllim që të ndryshohet përmbajtja e bazës së të dhënave.
8. Spoofing është konfigurimi i një sistemi kompjuterik për t'u maskuar si një sistem tjetër në rrjet, në mënyrë që të fitojë akses të paautorizuar në burimet e sistemit që imiton.
9. Superzapping është përdorimi i një programi që mund të anashkalojë kontrollet e rregullta të sistemit për të kryer akte të paautorizuara.
10. Gërmimi është qasje e paautorizuar në informacion duke kërkuar nëpër "mbetjet" dhe informacionet në dukje të padëmshme, që lihen në kompjuter në përfundim të një dite pune. Teknikat variojnë nga kërkimi i koshave të mbeturinave ose depozituesve për printime për të skanuar përmbajtjen e kujtesës së një kompjuteri.
11. Wiretapping lidhet me përgjimin e linjave të telekomunikacionit për të marrë informacion.

(Jen Yeh et al., 2007)

5.2.2 Dështimet e hardware dhe software

Një tjetër kërcënim që i kanoset sistemeve të informacionit janë edhe dështimet e pajisjeve hardware apo programeve kompjuterike software që përfshin sistemi i informacionit. Dështimet e hardware i referohen çdo mosfunksionimi brenda qarqeve elektronike të pajisjeve apo komponentëve elektromekanikë të një sistemi kompjuterik. Prandaj rimëkëmbja nga një dështim i tillë hardware kërkon riparim ose zëvendësimin lokal të pjesës së dëmtuar. Nga ana tjetër, dështimet në software janë pamundësi e një programi për të vazhduar përpunimin e të dhënave, për shkak se dëmtimi i ndodhur sjell ndryshime në mënyrën e veprimit dhe logjikë të gabuar. Efekti i një procesi të tillë është i ngjashëm me bombat logjike të trajtuara më herët. Si dështimet në hardware, ashtu edhe ato software, bëjnë që pajisjet apo programet të mos funksionojnë në mënyrën e duhur, duke mos plotësuar objektivat e punës së tyre dhe për pasojë, për shkak të përpunimeve jo të sakta, as rezultatet të mos jenë ato faktike. (Schroeder et al., 2009)

5.2.3 Gabimet njerëzore

Pavarësisht gjithë kërcënimeve të trajtuara më herët, vlen të theksohet se për një organizatë punonjësit janë ndër kërcënuesit më të mëdhenj të të dhënave, duke qënë të parët që kanë kontakt të afërt me to, ndaj gabimet njerëzore ndeshen shpesh dhe kanë pasoja serioze. Gabimet njerëzore në një sistem informacioni i referohen të gjitha veprimeve dhe akteve që rrezikojnë sigurinë e kompanisë, megjithëse kryhen pa qëllime keqdashëse. Zakonisht gabimet vijnë si pasojë e mungesës së eksperiencës së punonjësve, supozimeve të gabuara dhe trajnimeve jot ë duhura ose të munguara në ambjentin e punës.(Whitman et al.,2009)

Si pasojë e gabimeve njerëzore në sistemin e informacionit, organizatat mund të ndeshen me pasoja serioze dhe probleme të mëdha. Kështu për shembull, pa qëllime tendencioze mund të zbulohen informacione të klasifikuara, të ruhen informacione të një rëndësie të veçantë në zona të pambrojtura, të futen në sistem të dhëna të gabuara apo ato të fshihen dhe ndryshohen aksidentalisht. Të gjitha këto veprime do të çonin jo vetëm në dështim të mbrojtjes së të dhënave, por edhe cënim mjaft serioz të sigurisë së përgjithshme të një firme. Të tilla kërcënime mund të shmangen me anë të procedurave kontrollore të thjeshta ose më komplekse, si një njoftim i dyfishtë për klikimet e komandave kritike, ose verifikimi i tyre nga një pale e dytë. (Safianu et al., 2016)

5.2.4 Fatkeqësitë natyrore

Në qoftë se, kategoritë e tjera të dobësive mund të parandalohen në rast se organizatat I trajtojnë me seriozitetin e duhur, ekzistojnë disa lloj kërcënimesh të cilat nuk mund të parandalohen dhe këto janë forcat e natyrës dhe fatkeqësitë natyrore. Në raste të tilla, kemi të bëjmë me kërcënime të rrezikshme që nuk mund të mënjanohen kur ndodhin, por e vetmja gjë që një firmë mund të bëjë është reagimi ndaj tyre. Tek fatkeqësitë natyrore përfshihen për shembull tërmetet, përmbytjet, zjarret dhe çdo aktivitet natyror i ngjashëm që ndërpret jo vetë jetën njerëzore, por edhe ruatjen, transmetimin dhe përdorimin e infomacioneve. Organizatat mund të përballen me to duke zbatuar kontrolle për kufizimin e dëmeve, duke përgatitur plane reserve për vazhdimin e veprimtarisë operacionale dhe duke hartuar plane të frytshme për rimëkëmbjen nga fatkeqësia. (Wu et al., 2007)

5.3 Metodat e vlerësimit të dobësive

Në mjedisin e sotëm të sistemeve të shpërndara, ku pothuajse çdo punonjës i një organizate ka akses në sistem, kërcënimet e sigurisë janë një shqetësim serioz. Shpesh dobësitë e sistemve vijnë pikërisht kur cënohet siguria ndaj për t'i mënjanuar ato nevojitet vlerësimi i këtyre dobësive. Vlerësimi i dobësive është procesi i identifikimit, klasifikimit dhe përcaktimit të prioriteteve që duhet të kenë dobësitë e sistemeve kompjuterike. Në këtë mënyrë bëhet e mundur që organizata të bëjë vlerësimin e kërcënimeve të mundshme për të reaguar në mënyrë të përshtatshme kundrejt tyre. Ky proces i ofron organizatës një njohje më të mirë të pasurive të saj, dhe rrezikut të përgjithshëm, duke zvogëluar gjasat që hakerat të shfrytëzojnë këto mangësi për të sulmuar sistemin.

Dy janë metodat kryesore të vlerësimit të dobësive. Së pari, procedura e vlerësimit të riskut është një vlerësim metodik i probabilitetit të humbjeve për shkak të ekspozimeve të sigurisë. Rreziku përcaktohet si produkt i shumës që mund të humbasë për shkak të ekspozimit të sigurisë dhe probabilitetit që një humbje e tillë do të ndodhë. Probabiliteti nga ana e vet vlerësohet nga frekuenca e ndodhive të tilla në të kaluarën. Metoda e dytë e vlerësimit të dobësive është analiza e skenarit. Ajo është metodë e kontrollit të sistemit që përfshin sulme të simuluara në sistem në mënyrë që të përcaktohet cënueshmëria e tij. (Alghazzawi et al., 2014)

KAPITULLI 6
Kontrollet e sistemeve të informacionit

Për të mbrojtur operacionet organizative të kompanive, mbarëvajtjen e procesve të punës, reputacionin e tyre, por edhe informacionet e të dhënat, pasuritë organizative e individët, nga një sërë kërcënimesh të ndryshme, nevojiten kontrolle të vazhdueshme. Sulmet kibernetike, fatkeqësitë natyrore, dështimet strukturore dhe gabimet njerëzore, me qëllim ose jo qofshin ato, janë disa dobësi që ndeshen më së shumti. Prandaj kontrollet e sigurisë dhe privatësisë rekomandohen të zbatohen, në mënyrë që, të mbrohet siguria e informacionit dhe të mbahet në nivele të pranueshme dhe moderuara rreziku i privatësisë.

6.1 Çfarë janë kontrollet e SI?

Kontrollet trajtojnë një sërë problematikash për sigurinë dhe privatësinë, mbështetur në infrastrukturën e përdorur dhe politikat ekzekutive, direktivat e rregulloret në përputhje me standardet, nevojat dhe misionin e një biznesi. Procesi i kontrollit përfshin aktivitetet që zhvillohen nga grupe të specializuara profesionistësh, në përputhje me proceset operative dhe teknologjitë me të cilat operohet, për të pare nëse gjithçka është në rregull dhe kur kjo nuk ndodh, të dedektohen problemet që e shkaktojnë këtë keqfunksionim në sistem.

Në lidhje me çështjet e sigurisë së sistemit, kontrollet kryhen në dy perspektiva kryesore. Perspektiva e funksionalitetit që lidhet me funksionet e sigurisë dhe mekanizmat e ofruar dhe perspektiva e sigurisë, e cila i referohet masave të besimit që zbatohen. Janë pikërisht këto dy linja kontrolli dhe zbatimi me rigorozitet i tyre, që ndihmojnë për të siguruar që sistemet e informacionit dhe parimet inxhinierike që përdoren në projektimin e tyre të jenë mjaftueshëm të besueshme.

(Ross, 2014)

6.2 Roli i kontrolleve

Në mënyrë që operacionet e sistemeve të informacionit të jenë të sigurta, objektivat e tyre të përmbushen në mënyrë efikase dhe të ruhen asetet e të dhënat e ruajtura nga këto sisteme, brenda një kompanie duhet të ndërmerren shpesh kontrolle që zbatojnë një sërë politikash dhe masash proceduriale. Kontrollet e sistemeve të informacionit ndodhin për tre arsye kryesore:

Parandalimi i ndodhjes së një gabimi ose sulmi, zbulimi i një shkeljeje dhe zbulimi e korrigjimi i një situate emergjente që nuk ndodh shpesh.

6.3 Llojet kryesore të kontrolleve

Siç u përmend edhe më herët, për të mbikqyrur mbarëvajtjen e veprimtarive operacionale firmave dhe bizneseve, rekomandohen të ndërmerren kontrolle të vazhdueshme. Ato mund të jenë për shkaqe dhe të natyrave të ndryshme. Megjithatë kontrollet që aplikohen mbi sistemet e informacionit klasifikohen në dy grupe të mëdha, kontrollet e përgjithshme dhe ata të aplikimit. Kontrollet e përgjithshme janë ata që zbatohen për gjithë aktivitetin e një organizate të marrë në tërësi. Nga ana tjetër, kontrollet e aplikimit, ndryshe nga të parat, janë specifike për një aplikim, çështje ose problem të veçantë në proceset e punës. (Joshik, 2015)

6.4 Kontrollet e përgjithshme

Këto lloj kontrollesh aplikohen mbi gjithë veprimtarinë e organizatave në përgjithësi dhe mbulojnë të gjitha sistemet e implementuara në një firme, ose në degët apo njësitë e saj më të vogla. Kontrollet e përgjithshme klasifikohen gjithashtu në shumë nëngrupe të tjera me karakteristika të veçanta, të cilat trajtohen në vijim:

6.4.1 Kontrollet administrative

Kontrollet administrative janë ato të cilat kanë si qëllim kryesor zbatimin me rigorozitet të kontrolleve të tjera në organizatë. Ato ndodhin zakonisht të bashkangjitura me proceduar të tjera, siç janë auditimet dhe mbikqyren nga menaxherët strategjikë. Kontrollet administrative kanë disa detyra, si publikimi i politikave dhe procedurave formale të ndjekura gjatë kontrolleve, shqyrtimi dhe mbikqyrja e vazhdueshme e personelit, si dhe ndarja e detyrave përkatëse tek secili punonjës.

6.4.2 Kontrollet e zhvillimit dhe mirëmbajtjes së sistemve

Në mënyrë që sistemet e informacionit dhe të dhënat që shërbejnë si input-e për to, të jenë sa më të sigurta dhe të mbrojtura nga kërcënimet nevojitet zhvillimi i sistemeve me disa cilësi specifike. Për këtë arsye gjatë procesit të zhvillimit të sistemeve, duhet të përfshihen në një rol aktiv edhe auditorët e brendëshëm të tyre, të cilët kontrollojnë nëse sistemi është i sigurt, i

auditueshëm dhe gjeneron rezultatet e duhura. Ata gjithashtu kontrollojnë nëse dokumentacioni është i mirëmbajtur e i pakompromentua dhe nëse nevojiten ndryshime të mëtejshme.

6.4.3 Kontrollet operacionale

Kontrollet operacionale janë politika, procedura dhe masa që ndërmenrren në lidhje me sistemin e informacionit, në mënyrë që me të dhënat të operohet në mënyrë të besueshme e të sigurt. Tek kjo kategori përfshihen: kontrollet mbi personelin operacional, mirëmbajtja e pajisjeve kompjuterike në përdorim, arkivimi i sigurt i të dhënave të ruajtura më herët dhe aksesimin tek bazat e të dhënave në përputhje me lejet e përdoruesve përkatës.

6.4.4 Mbrojtja fizike e qëndrave të të dhënave

Siç u trajtua më herët, tek kontrollet operacionale bënin pjesë edhe kontrollet për mbrojtjen e bazave dhe qëndrave të të dhënave nga aksesi i pautorizuar. Megjithatë, bazat e të dhënave nuk rrezikohen vetëm nga faktori human, por siguria e tyre cënohet shpesh edhe për shkak të sulmeve natyrore dhe elementëve mjedisorë. Të dhënat janë aseti më i çmuar i një firme, ndaj sa më të sigurta të jenë ato, aq më mire përmbushen objektivat.

Ndaj duhet që shpesh të aplikohen masa që kontrollojnë nëse kushtet fizike të mjedisit, si për shembull, klima apo lagështia janë në përputhje me kushtet që kërkon një pajisje, për të vepruar me efektivitet. Ato gjithashtu mund të kontrollojnë burimet e energjisë dhe rastet emergjente ku patjetër energjia duhet të jetë e disponueshme. Rekomandohet që sistemet të kenë të instaluar një furnizim të pandërprerë me energji(UPS) për të siguruar funksionimin e vazhdueshëm, duke qënë se shpesh për shkak të ndërprerjes totale ose të pjesshme të rrymës, sistemi dështon.

6.4.5 Kontrollet e hardware-ëve

Ndodh shpesh që të dhënat të korruptohen për shkaqe të ndryshme, si ai ai kur gabimet ndodhin në pajisjet fizike të një sistemi dhe rezultati mos jetë ai i pritshëm ose faktik. Megjithatë për zbulimin dhe në disa raste edhe korrigjimin gabimeve që ndodhim me të dhënat gjatë përpunimit vepron procesori qendror kompjuteri nëpërmjet qarqeve që përmban.

Disa nga kontrollet për gabimet më të shpeshta që hasen janë kontrolli i paritetit, ai i gjendjes së pajisjeve përpunuese dhe toleranca e sistemit ndaj gabimeve. Kontrolli i paritetit

ndodh kur çdo byte i të dhënave të ruajtura përmban një bit shtesë, i quajtur një bit pariteti, i cili ndihmon në zbulimin gabimeve në vlerë gjatë përpunimit.

Kontrollet rreth gjendjes së pajisjeve përpunuese iu referohen operacioneve që pajisja mund të suportojë. Pajisjet përpunuese zakonisht kanë dy gjendje, gjendjen e privilegjuar dhe atë të përdoruesit.Gjendja e privilegjuar, është e rezervuar vetëm për software-in e sistemit dhe përdoruesit nuk mund ta aksesojnë atë. Gjatë kësaj gjëndjeje, sistemi mund të kryejë çdo veprim të mundshëm. Nga ana tjetër, gjendja e përdoruesit ndodh kur ky i fundit ka kontroll mbi pajisjen dhe zgjedh çfarë do të kryejë me të. Eventualisht është gjendje në të cilën mund të kryhen vetëm disa operacione specifike.

Ekzistojnë gjithashtu edhe kontrolle rreth tolerances së sistemit ndaj gabimeve dhe ato i referohen sistemeve që vazhdojnë të funksionojnë edhe pasi disa nga komponentët e tyre të përpunimit dështojnë. Sistemet të tilla kompjuterike projektohen dhe ndërtohen me komponentë shtesë, si për shembull disa procesorë në një konfigurim multiprocessing. Kështu nëse një nga përpunuesit dështon, të tjerët mund të ofrojnë shërbime me cilësi më të ulët, por efektiv.

6.4.6 Kontolli i aksesit në sistem: Identifikimi, Autentikimi dhe Firewall-et

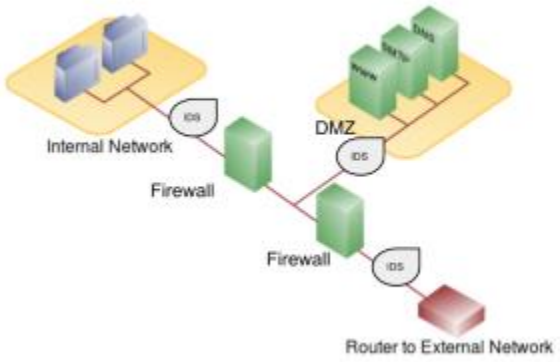
Së bashku me mjedisin e informatizuar ku implementohen, një nga kërcënimet më serioze që i kanoset sistemve të informacionit është aksesi i paautorizuar, pasi në sistem mund të hysh nga pothuajse kudo e në çdo kohë. Prandaj duke lejuar vetëm hyrjet e autorizuara me anë të masave të caktuara, ky kërcënim mbahet në nivele të moderuara. Në mënyrë që kjo të ndodhë, duhet fillimisht që personat e autorizuar të identifikohen dhe vërtetohen nga sistemi. Ky process përbëhet nga disa hapa. Së pari, një përdorues fillimisht duhet të identifikohet në sistem, zakonisht me një emër ose një numër llogarie. Më pas sistemi krahëson informacionin e ruajtur për përdoruesin e identifikuar duke bërë një kontroll të dyfishtë dhe së fundi i kërkohet përdoruesit të japë një fjalëkalim ose një mjet tjetër me anë të të cilit mund të vërtetohet.

Nga ana tjetër për identifikimin në një sistem informacioni mund të zbatohen edhe veçoritë biometrike të sigurisë. Kjo mënyrë mbështetet në përdorimin e karakteristikave personale dhe identifikimin e veçorive unike që zotëron çdo person, ku përfshihet zëri, shenjat e gishtave, gjeometria e dorës, nënshkrimi, skanimi i retinës, njohja e fytyrës apo analiza e modelit gjenetik.

Megjithatë, pavarësisht masave të trajtuara më sipër, sot një nga mënyrat më të përdorshme për shmangien e aksesit të sistemit nga persona të paautorizuar janë firewall-et. Një firewall është një pajisje hardware dhe software që pengon hyrjen në Intranet-in e një firme nga interneti publik, por lejon hyrjen në Internet. Përdorimi i një firewall është për të siguruar që në rrjet kalon vetëm trafiku i autorizuar. Firewall-i hardware është pajisje e lidhur me rrjetin dhe filtron pako bazuar në një sërë rregullash, ndërsa ai software shkon në sistemin operativ dhe përgjon paketat kur arrijnë në një kompjuter.

Disa organizata mund të zgjedhin të zbatojnë firewall-e të shumta si pjesë e konfigurimit të sigurisë së rrjetit të tyre, duke krijuar një ose më shumë pjesë të rrjeti, që janë pjesërisht të siguruara. Ky segment i rrjetit quhet DMZ, thuajsenë rolin e zonës së çmilitarizuar nga ushtria dhe është vendi ku një organizatë mund të vendosë burime që kanë nevojë për aksesim më të gjerë, por që ende duhet të sigurohen.

Konfigurimi i rrjetit me Firewall dhe DMZ



Burimi: Information Systems or business and beyond

Fig. 6.1

6.4.7 Kontrolli i aksesit në informacion:Enkriptimi

Një mënyrë tjetër për të ndaluar aksesin në informacioni është ta paturit e një forme komunikimi të pakuptueshme nga përdorues e paautorizuar dhe kjo mënyrë është pikërisht enkriptimi. Enkriptimi është transformimi i të dhënave në një formë të paqartë për këdo që nuk zotëron një çelës të duhur që të dekodojë informacionin nëpërmjet procesit të anasjelltë, dekriptimit duke kuptuar kështu përmbajtjen.(Laudon et al.,2004) Në ditët e sotme, kriptimi po fiton rëndësi të veçantë, pasi tregtia elektronike e përdorin në masë në rrjetet e

telekomunikacionit. Kriptimi gjithashtu, siguron mbrojtje të të dhënave të koduara edhe nga hakerat, apo hajdutët e informacionit, të cilët duke u maskuar si përdorues të ligjshëm, mund të kenë arritur të kenë akses në informacion, veçse fakti që informacioni është i koduar, e bën për ta të padobishëm. Pra, kjo teknikë është e rëndësishme jo vetëm në mbrojtjen e sistemit, por edhe të komunikimit dhe bazës së të dhënave.

Dy teknikat më të rëndësishme të enkriptimit janë enkriptimi standard i të dhënave me çelës privat, Data Encryption Standard (DES) dhe enkriptimi me çelës publik.

Kriptimi është kodimi i të dhënave, ose ndonjë teksti në përgjithësi, me një shifër që mund të dekodohet vetëm nëse dikush ka çelësin e duhur. Ajo i bën të dhënat e koduara të padobishme për dike që mund t'i aksesojë për qëllime të tjera. Disavantazhi kryesor i DES është se çelësat duhet të shpërndahen në mënyrë të sigurt. Meqenëse çelësat duhet të ndryshohen shpesh, ekspozimi i tepërt mund të bëhet kërcënim serioz. Gjithashtu ndërmjet dërguesit dhe marrësit është e nevojshme një lidhje paraprake në mënyrë që të ndajnë të njëjtin çelës privat.

Në sistemet me çelës publik, nevojiten dy çelësa për të siguruar transmetimin e sigurt, njëri është çelësi i kodimit dhe tjetri është çelësi i dekodimit. Meqenëse çelësi i dekodimit të fshehtë nuk mund të rrjedhë nga çelësi i kodimit, çelësi i kodimit mund të bëhet publik, prandaj nuk ka nevojë për shpërndarje të sigurt të çelësave midis palëve para komunikimit të tyre. Megjithatë kjo mënyrë kriptimi kërkon më shumë kohë se sa sistemet me çelësa privatë dhe mund të degradojë performancën e sistemeve të informacionit.

6.4.8 Planifikimi i rimëkëmbjes nga fatkeqësitë

Pasi ndodh një fatkeqësi ose dështim sistemi, parashtrohen dy detyra të rëndësishme, sigurimi për të mënjanuar rrezikun e mbetur dhe një plan për rimëkëmbjen nga fatkeqësia. Plani për rimëkëmbjen nga fatkeqësitë përcakton se si një kompania do të vazhdojë të mbajë në veprim shërbimet e nevojshme për operacionet e saj të biznesit përballë katastrofës që ka ndodhur. Në planifikimin e rimëkëmbjes së fatkeqësive, detyra e parë është të identifikohen funksionet biznesit që kanë nevojë për vëmendjen maksimale, në mënyrë që mos përqëndrohemi tek funksionet më pak jetësore, që jo vetëm nuk do të sillnin zgjidhjen e problemit, por llogariten edhe si kosto shtesë për organizatën.

Plani i rimëkëmbjes së katastrofave për këto funksione duhet të përmbajë katër komponentë kryesorë: planin e emergjencës, planin rezerve, planin e rimëkëmjes dhe atë të

testimit. Një plan emergjence zakonisht specifikon se kur situata cilësohet si fatkeqësi dhe veprimet që duhet të ndërmerren nga punonjës të ndryshëm në pozicione të caktuara. Nga ana tjetër, plani rezervë specifikon se si do të kryhet përpunimi i informacionit gjatë emergjencës. Ai detajon se si duhet të veprohet me pajisjet dhe objektet rezervë, për të patur një back-up të sigurt të dhënash dhe specifikon objektin e quajtur vend i rikuperimit, ku ato do të vendosen. Ka raste kur mbahet një lidhje ndërmjet bazave të të dhënave dhe planit të rimëkëmbjes, në mënyrë që të sigurohet një akses tettë dhënat më të fundit që ka prekur fatkeqësia.

Ekzistojnë disa alternative kryesore se si veprohet me të dhënat në rastet e rikuperimit të tyre nga një dështim i tillë. Së pari, ato mund të ruhen në një objekt të ndodhur gjeografikisht larg nga kompania qëndrore, por në pronësi të kësaj të fundit. Një mënyrë tjetër është marrëveshje reciproke me kompani që zotërojnë një sistem kompjuterik të ngjashëm. Së fundi, është përdorimi i një cold ose hot site, që ofrohen nëpërmjet nënkontraktimit nga kompani të cilat ofrojnë shërbime me kontratë për rimëkëmbjen e fatkeqësive nën kontratë. Një hot site është një faqe që vepron përputhje me kërkesat e kompjuterave klientët, të cilët mund ta përdorin site-in brenda 24 orëve nga fatkeqësia.Ndërsa cold sites, të quajtura ndryshe shells janë ndërtesa, të disponueshme për të pranuar pajisjet pas marrjes së një njoftimi të caktuar.

Janë gjithashtu edhe plani i rimëkëmbjes dhe ai i testimit. I pari specifikon se si do të rivendosen të dhënat dhe përpunimi në faqen origjinale, duke përfshirë përgjegjësitë e hollësishme të personelit ndërsa plani i testimit specifikon se si do të testohen komponentët e tjerë të planit, për të kontrolluar nëse çdo gjë ndodh në mënyrën e duhur pasi fatkeqësia ka kaluar.

6.5 Kontrollet e aplikimit

Kontrollet e aplikimit janë kontrolle që ndërmerren në mënyrë specifike për një sistem informacioni të veçantë për shembull, llogaritë e pagave, sistemi i përpunimit të porosive, faturave, etj. Këto lloj kontrollesh mund të zbatohen si në komponentët e automatizuar, ashtu dhe në ato manuale të sistemit. Fushat kryesore ku ndodhin kontrollet e aplikimit janë: input-i, prodhimi, telekomunikacionet dhe rrjetat, si dhe baza e të dhënave.

Qëllimi i kontrolleve të inputeve është të parandalohet futja në sistemin e informacionit e të dhënave të paplota, të gabuara ose të papërshtatshme. Ato zbatohen për të kontrolluar saktësinë dhe plotësinë e të dhënave si dhe validimin e inputeve, që këto të fundit të hyjnë në formatin e

duhur. Pasi të dhënat futen në sistem, hapi i rradhës është përpunimi i tyre dhe që ky process të mos përmbajë gabime, edhe këtu aplikohen të ashtuquajturat kontrolle përpunimi.

Nga ana tjetër, kontrollet e prodhimit ose output-it janë kryesisht procedurat manuale që synojnë të sigurojnë që informacioni i paraqitur në raportet dhe ekranet e sistemit është i një kualiteti të lartë, i plotë dhe i disponueshëm vetëm për individët e autorizuar.

Telekomunikacioni dhe rrjetat janë komponenti më pak i sigurt dhe më vulnerabël i sistemeve të informacionit. Prandaj për të mbrojtur informacionet që shëmbehen nëpërmjet tyre, teknika më e mire është kodimi i këtyre të dhënave në qarkullim.

Për sa i përket skedarëve të sistemeve të informacionit dhe bazave të të dhënave, ato janë komponenti më i vyer i firmave, pasi arkivojnë të dhënat që shërbejnë si input për çdo veprimtari të sistemit, ndaj janë gjithmonë në vëmendje për t'u mbrojtur nga modifikimi, shkatërrimi i çdo lloj forme apo qasja e padëshiruar. Masat kryesore për mbrojtjen e të dhënave të ruajtura në sisteme janë ruajtja dhe rikuperimi, autorizimi i lejeve dhe aksesi, si dhe kontrollet mbi ndërveprimin me skedarët.

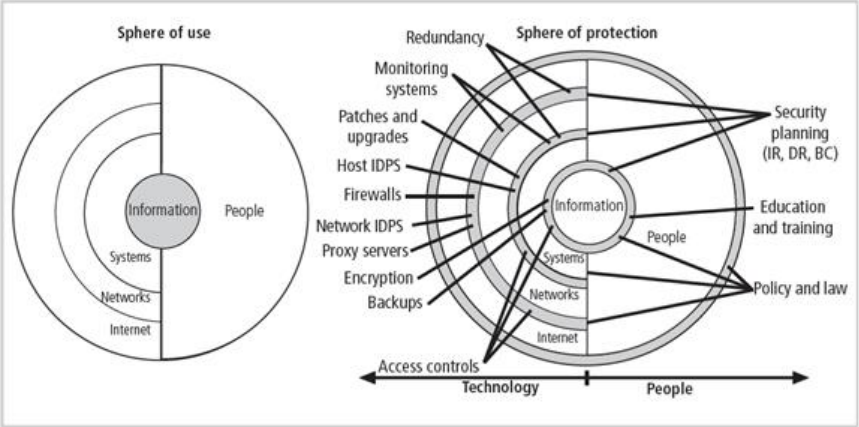
KAPITULLI 7
Arkitektura e nevojshme për sisteme të sigurta

Më tepër se sa marrja e masave mbrojtëse dhe aplikimi i kontrolleve të rregullta, mbrojtja e sigurisë së sistemve të informacionit nga sulmet që e cënojnë, mund të sigurohet nëpërmjet zhvillimit dhe dizenjimit të arkitekturave kompjuterike me karakteristika të caktuara. Në këtë mënyrë sistemi i implementuar, që në thelb të veprimtarisë së tij do kryejë operacionet e nevojshme dhe përmbushë objektivat e kërkuar. Me zhvillimin e proceseve teknologjike dhe operacionale kohët e fundit edhe arktiketuarat synojnë të përmirësohen dhe të sjellin vlerë të shtuar për sistemin në tërëri. Në këtë kapitull do të trajtohen pikërisht modele mbi të cilat kthehet vëmendja dhe përdoren në masë për të siguruar mbrojtje e besueshmëri për sistemet e informacionit.

7.1 Dizenjimi i arkitekturës së sigurisë

Sigurisht që për zhvillimin e sistemeve të sigurta, dizenjimi i arkitekturës së nevojshme është hap vendimtar. Themeli i kuadrit të sigurisë së sistemeve të informacionit është përdorimi i sferave të sigurisë, pra zbatimi i politikave të sigurisë në shtresa të ndryshme të organizimit të sistemit. Mbrojtja në thellësi kërkon që organizata të vendosë kontrolle dhe masa mbrojtëse të mjaftueshme, në mënyrë që një pale e tretë që kërkon të ndërhyjë, të përballet me shtresa të shumta kontrolli. Më pas është perimetri i sigurisë ai që cakton deri në çfarë pike aplikohen masat dhe kontollet. Perimetri i sigurisë është pika ku mbrojtja e sigurisë së organizatës mbaron dhe fillon bota e jashtme, por vlen të theksohet se ai nuk zbatohet për sulmet e brendëshme nga kërcënimet e punonjësve apo dështimet e mundshme.(Whitman, 2009)

Arkitektura me shtresa e sigurisë së sistemve



Burimi: Principles of Information Security

Fig. 7.1

7.2 Teoria e çelësave dinamikë

Në seksionin 6.4.7 u bë një trajtim i Enkriptimit, si një masë mrojtëse e rëndësishme për sigurinë e sistemeve dhe informacionit që kalon në rrjet. Megjithatë çelësat publikë rezultojnë në kërcënime dhe shqetësime serioze të sigurisë në lidhje me ndjeshmërinë e sistemeve të informacionit. Kjo ndodh për shkak se entropia pasiguria e çelësave zvogëlohet kur çelësat janë të përfshirë në komunikim të shpeshtë, ndaj ata përballen me një rrezik të madh të ekspozimit.
Duke qënë se çelësat dinamikë ofrojnë siguri më të madhe, arktitektura që përmban këta lloj çelësash shërben si mbrojtje më efektive për sistemet e informacionit duke eliminuar kërcënimet e shkaktuar nga përdorimi i çelësave publikë.

Një çelës dinamik është çelës simetrik i vetëm që përdoret për gjenerimin e argumenteve dhe mesazheve të enkriptuara në një rrjedhë komunikimi. Përdorimi i tyre paraqet komplikime në sinkronizim për sistemet kriptografike, megjithatë ata ndihmojnë me probleme të tilla si reduktimi i shpërndarjes kryesore dhe rritja e sigurisë. Ekzistojnë tre arsye kryesore për përdorimin e çelësave dinamikë në sigurimin e sistemve të informacionit.

Së pari, sigurimi i informacionit të ndjeshëm duke përdorur çelësat simetrikë për një kohë të gjatë e bën sistemin më të ekspozuar ndaj sulmeve ndërkohë që përdorimi i çelësave dinamik i bën sulmet më të vështira për të ndodhur dhe parandalon aksesin e paautorizuar. Përveç kësaj, çelësat dinamikë janë shumë më të vështirë për t'u gjetur dhe dekoduar kështu mesazhi i shifruar kërkon përpjekje massive për t'u thyer.

Gjithashtu, shumica e algoritmeve të kodimit kërkojnë që çelësat kriptografikë të shpërndahen në mënyrë të sigurt para se të kryhet titrimi, por pikërisht shpërndarja është një nga dobësitë e algoritmeve simetrike kyçe. Nga ana tjetrë, çelësat asimetrikë nuk kërkojnë shpërndarje sekrete, por janë përgjithësisht të ngadalta dhe të ndjeshme ndaj sulmeve. Kjo situatë mund të përmirësohet duke përdorur algoritmat e çelësave të vetëm asimetrikë për të shpërndarë të dhënat e koduara. Ky proces përmirëson sigurinë e përgjithshme në mënyrë të konsiderueshme.(Wu, 2009)

7.3 Modeli aktual i sigurisë

Siç u trajtua në seksionin 4.3, modeli aktual i përdorshëm në sigurinë e informacionit është modeli CIA dhe duke qënë se sistemet e informacionit trashëgojnë vetitë e informacionit të sigurt, parimet thelbësore të modelit CIA, pra kofidencialiteti, integriteti dhe disponueshmëria vlejnë edhe për sistemet e ndjeshme të informacionit. Megjithatë, në po të njëjtin seksion u trajtuan edhe disa mangësi të këtij modeli, që e bëjnë atë jo shumë efikas për përdorim në sistemet komplekse të zhvilluara së fundi. Për këtë arsye, me zhvillimin e shpejtë të IT ishte i nevojshëm një model i ri më gjithëpërfshirës. Kështu, nisur nga kufizimet e modelit CIA, ishte Departamenti Amerikan i Mbrojtjes që aprovoi shtimin e dy elementëve të tjerë, autenticiteti e mosnjohja dhe zhvilluesit e sistemeve u inkurajuan t'i përfshijnë ato në dizenjim. (Latham et al., 1985)

7.3.1 Gjashtëkëndëshi i Parkerit

Megjithatë edhe pas ndryshimeve të modelit CIA u pa se përsëri për sistemet moderne modeli nuk mbronte plotësisht sigurinë e të dhënave. Prandaj ishte Donn B. Parker që në 1998, duke argumentuar mangësitë e CIA-s, propozoi një model të ri, të quajtur Gjashtëkëndëshi i Parkerit(Parkerian Hexad), ku përveç kofidencialitetit, integritetit dhe disponueshmërisë u shtuan edhe tre elementë dobishmëria, autenticiteti dhe posedimi. Dobishmëria lidhet me aftësinë e informacionit për të qënë i dobishëm për një qëllim të caktuar, ndërsa autenticiteti i referohet vlefshmërisë, përputhshmërisë dhe vërtetësisë së të dhënave. Për sa i përket posedimit, është aftësia për të mbajtur, përdorur e kontrolluar informacionin.

Modeli Parkerian nuk është mbivendosës, që do të thotë se çdo parim është

absolutisht e nevojshme për të siguruar ruajtjen e sigurisë dhe gjithashtu mund të përdoret për të vlerësuar sigurinë e sistemeve të informacionit. (Parker, 1998) Megjithatë edhe ky model ka kufizime. Ashtu si trekëndëshit CIA, edhe këtu mungon atributi i mosnjohjes, shumë i aplikueshëm për shembull në rastin e transaksioneve bankare në internet.

Një e metë tjetër që modeli Parkerian nuk përfshin është edhe privatësia. Privatësia mund të nënkuptohet nga konfidencialiteti, por ajo shkon përtej kësaj, pasi informacioni i ndjeshëm i përdoruesve duhet të mbrohet, dhe mbrojtja është vetëm një pjesë e politikave të sigurisë. Mbrojtja gjithashtu kërkon që përdoruesit të menaxhojnë informacionin e tyre, siç është delegimi i lejeve. Për shembull, në një sistem të kujdesit shëndetësor, një pacient duhet të jetë në gjendje të kontrollojë të dhënat e tij të ndjeshme dhe të autorizojë personat që mund të kenë akses në këtë informacion, por modeli i Parkerit nuk bën asnjë nga këto specifikime mbi autoritetin e informacionit.

KAPITULLI 8
Mirmbajtja e sistemeve të informacionit

Pasi sistemet e informacionit dizenjohen dhe implementohen në një firmë, në mënyrë që veprimtaria dhe procest e kësaj të fundit të kryhen me përpikmëri, vjen një hap tjetër po aq thelbësor, mirëmbajtja. Mirëmbajtja e sistemeve të informacionit cilësohet si procesi i modifikimit të një sistemi informacioni për të përmbushur vazhdimisht kërkesat organizative dhe ato të përdoruesve të tij. Mirëmbajtja është një pjesë shumë e rëndësishme dhe e kushtueshme, pasi e bën sistemin të punojë në mënyrë më efektive dhe redukton kostot e firmës në afat të gjatë kohe. Ajo është gjithashtu një burim i vlefshëm për departamentin e planifikimit, pasi shpesh përdoret për përgatitjen dhe planifikimin e punëve të ardhshme.

8.1 Çfarë është mirëmbajtja e sistemeve të informacionit?

Mirëmbajtja e sistemeve të informacionit i referohet të gjitha procesve dhe veprimtarive që kanë si qëllim të mbajnë sistemin funksional dhe të sigurt. Kjo realizohet duke kryer ndryshimet e korrigjimet e nevojshme në sistem dhe duke i dokumentuar këto ndryshime, në mënyrë që të jenë të disponueshme për një përdorim të nevojshëm në raste problemesh të ngjashme. Veprimet kryesore që përfshin procesi i mirëmbajtjes janë administrimin e ID-ve dhe llogarive të përdoruesve, menaxhimi i lejeve e të drejtave të tyre për autorizimin ose ndalimin e aksesit në sistem, monitorimin e përdorimit të sistemeve dhe përpilimin e statistikave mbi to. (Joshik, 2015)

Mirëmbajtja e sistemeve të informacionit përfshin dy linja kryesore, të cilat ndryshojnë shumë nga njëra-tjetra, qoftë në kosto ashtu edhe në objektiva. Mirëmbajtja e pajisjeve, ka si qëllimi të mbajë pajisjet e sistemit kompjuterik në gjendje pune, pa ndryshuar funksionalitetin e tyre. Nga ana tjetër, mirëmbajtja e sistemeve , që iu referohet përgjithësisht aplikacioneve software-ike përfshin të gjitha modifikimet që kryhen mbi një software, pasi të jenë përfunduar përpunimet e të dhënave në veprim e sipër.

Mirëmbajtja e softuerit në fakt përbëhet nga tri lloje aktivitetesh. Mirëmbajtja perfekte i referohet përmirësimit dhe modifikimit të sistemve për t'iu përgjigjur ndryshimit të kërkesave të përdoruesve dhe nevojave organizative, përmirësimit të efikasitetit të sistemit dhe përmirësimit të dokumentacionit. Mirëmbajtja adaptive ka të bëjë me ndryshimin e aplikacionit për ta përshtatur atë në një mjedis të ri hardware ose software. Mirëmbajtja adaptive mund të përfshijë, për shembull, lëvizjen e një aplikacioni nga një kornizë kryesore në një mjedis klient / server ose

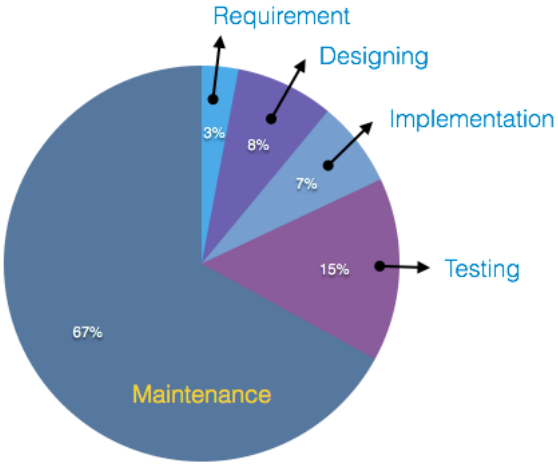
konvertimin e tij nga një skedar në një mjedis të bazës së të dhënave. Së fundi, mirëmbajtja korrektuese është korrigjimi i një gabimi të zbuluar gjatë veprimtarive operacionale.

8.1.1 Kostot e mirëmbajtjes

Dy linjat e mirëmbajtjes, ajo hardware dhe software, ashtu si në krijim e dizenjim, edhe në mirëmbajtje kanë kosto të ndryshme. Zhvillimet teknologjike me ritme të shpejta, të kohëve të fundit dhe përhapja në masë e pajisjeve elektronike, bëjnë që për pasojë pajisjet hardware të kushtojnë më pak se shumë vite më parë. Vetë ligji i Moor-it e provon këtë. Ai thotë se për çdo dy vjet, tek pajisjet elektronike dyfishohet numri i transistorëve ndërkohë që çmimi përgjysmohet. Pra për një pajisje më performante dhe me fuqi përpunuese më të madhe, paguhet më pak. Kjo ka bërë që edhe kostoja e tyre e mirëmbajtjes të mos jetë shumë e lartë. Zëvendësimi i një pjese të dëmtuar apo gjithë pajisjes, ka nevojë thjesht për blerjen e pjesës fizike dhe implementimin e saj, ndaj nuk janë të kushtueshme. Zakonisht, ky aspekt i mirëmbajtjes së sistemit mbulohet nga kontratat e mirëmbajtjes me prodhuesit e pajisjeve.

Nga ana tjetër, nuk mund të thuhet e njëjta gjë për mirëmbajtjen e software-ve. Sot gjithnjë e më tepër, programeve kompjuterike po iu shtohen funksionalitete të tjera dhe kompleksiteti i tyre është rritur ndjeshëm. Ata përdoren për zgjidhjen e problemeve shumë të vështira, me volum të madh të dhënash dhe shpejtësi tepër të lartë. Për pasojë, mirëmbajtja e sostware-ve të përdorur nga sistemet e informacionit kushton relativisht shumë dhe kostot rriten me kalimin e kohës, ndryshe nga hardware-ët. Kostoja e kësaj mirëmbajtjeje gjatë jetës së dobishme të një aplikacioni është zakonisht dyfishi i kostos së zhvillimit. Disa nga faktorët që ndikojnë në kostot e larta të mirëmbajtjes së software-ëve janë: madhësia e të dhënave, besueshmëria e software-it, karakteristikat e produktit e shkalla e kompleksitetit, aftësia analitike, gjuha e programimit e përdorur, kohëzgjatja e ekzekutimit, cilësia e dokumeteve të gjeneruar, zhvillimi teknik, aftësitë ruajtëse të të dhënave, etj. (Dehaghani et al., 2013)

Kostot e mirëmbajtjes së software-ëve



Burimi: "Software Evolution and Refacturing" (Bradley, 2010)

Fig. 8.1

8.2 Politikat e veprimit

Në mënyrë që mirëmbjatja e sistemeve të informacionit të kryhet në përputhje me objektivat dhe të përmbushet qëllimi i saj primar, pra që sistemi të ruajë funksionalitetin dhe sigurinë e vet duhet të ndiqen disa politika të caktuara veprimi. Së pari, nevojitet të përpilohet një regjistrim historik i pajisjeve, që përfshin informacionin origjinal të specifikimit, prodhuesin, historinë e kohës dhe kushteve të punës, si dhe një regjistër të rezultateve të inspektimit me të gjitha mirëmbajtjet e kryera. Gjithashtu dokumentacioni përkatës duhet të tregojë se cilat masa sigurie zbatohen dhe cilat leje janë të nevojshme gjatë çdo aktiviteti, në orarin e përcaktuar për fushën përkatëse të inspektimit. Së fundi, një tjetër hap i rëndësishëm do të ishte një mënyrë për caktimin e prioritetit të detyrës së riparimit dhe mirëmbajtjes së sistemit e pajisjeve në veprim. Kjo do të sillte automatikisht planifikim më të mire të veprimtarive të nevojshme dhe do të rriste prioritetin e punëve të shtyra.

KAPITULLI 9
Masat e nevojshme për sisteme të sigurta informacioni

Teknologjia gjithnjë e në rritje, sot vazhdon të jetë më tepër se më pare një ndihmë e madhe për sipërmarrjet dhe kompanitë. Kjo pasi teknologjia iu ofron këtyre të fundit lëvizshmëri dhe kushte optimale veprimi, produktivitet të lartë dhe tkurrje të kostove operacionale. Megjithatë përveç risive të shumta dhe inovacioneve të dobishme që sjell, ajo paraqet edhe shqetësime gjithnjë e në rritje në lidhje me çështjet e sigurisë. Nisur nga fakti që sistemet e informacionit janë një ndër implementimet më me vlerë të teknologjisë, ato kanë nevojë për masa, që duhen ndërmarrë në mënyrë që sistemet e informacionit dhe të dhënat që përpunohen nga to,të jenë të sigurta.

9.1 Çfarë mund të bëhet?

Shpesh mendohet se zgjidhja kryesore e problemeve të sigurisë së sistemeve të informacionit është dizenjimi i duhur i tyre. Megjithatë, në ditët e sotme, në vend që vëmendja të përqëndrohet tek kjo mënyrë, zgjidhjet e sigurisë fokusohen kyresisht në hapa më të vegjël në dukje, por që janë në të vërtetë shumë efektive. Kështu për të mundësuar mbrojtjen e sigurisë masat e nevojshme ndodhim tek firewalls, routers, konfigurimi i serverve, mbrojtja e fjalëkalimeve dhe enkriptimi. Kjo ka bërë që të zhvillohen metodologji të reja që përfshijnë sigurinë e faktorëve të lartpërmendur në proceset e tyre të zhvillimit. Ndaj masat kryesore që mund të aplikohen mbi sistemet e informacionit, që këto të fundit të jenë sa më të sigurta janë:
(Villarroel et al., 2005)

9.1.1 Mbrojtja me fjalëkalime

Mund të duket si një masë shumë e thjeshtë, por shumë sulme kibernetike ndodhin pikërisht për shkak të protokolleve të dobëta të fjalëkalimeve. Prandaj aksesi nëpër pajisje elektronike, rrjetet celulare dhe të dhënat e ndjeshme duhet të rruhet me emra unikë përdoruesish dhe fjalëkalime po kaq unike për secilin individ. Një fjalëkalim i forte dhe i sigurt duhet të përmbajnë numra, shkronja, simbole dhe nuk duhet të bazuohet në fjalë të zakonshme, terma standarde fjalie ose datat lehtësisht të gjetshme si ditëlindjet. Çdo përdorues duhet të ketë më tej një fjalëkalim unik kudo që shfaqet në një pajisje ose rrjet. Gjithashtu është mire që në llogari të ndryshme të të njëjtit përdorues, të përdoren fjalëkalime të ndryshme.

9.1.2 Përdorimi i skanimit për viruse dhe përditësimi i software-ve

Pak rëndësi ka nëse punoni nga shtëpi ose në një rrjet zyrësh ku keni të implementuar një sistem informacioni, gjithmonë duhet të instalohet një program skanimi virusesh, të cilat janë një masë e dobishme sigurie dhe madje kanë kosto relativisht të ulëta, duke qënë se shumë prej këtyre aplikacioneve tashmë ofrohen falas. Përditësimi i vazhdueshëm i programeve, duke përfshirë shkarkime të rregullta dhe azhornime të sigurisë është gjithashtu i domosdoshëm pasi ndihmon në mbrojtjen kundër viruseve të reja dhe varianteve të përmirësuara të kërcënimeve të vjetra që i kanosen sistemit.

9.1.3 Dizajnimi i sistemeve të sigurta

Një hap shumë i rëndësishëm është edhe dizajnimi i sistemeve në mënyrë të tillë, që siguria të jetë një ndër komponentët kryesorë. Kështu për shembull, duke kufizuar aksesin në infrastrukturën teknologjike të sistemit, bëhet i mundur reduktimi i ekspozimit ndaj hakerëve dhe hajdutëve të informacionit. Gjithashtu dështimet e sistemit mund të eleminohen duke kontrolluar aksesin e panevojshëm në hardware dhe software dhe duke kufizuar lejet e përdoruesve e sistemeve individuale vetëm për pajisjet dhe programet e nevojshme. Dëmeve e mundshme në rrjet mund të shmangen po ashtu tuaja nëpërmjet përdorimit të një grupi unik adresash, identifikuesish, servera dhe emra domainësh për secilin përdorues, grup pune ose departament.

9.1.4 Sigurimi i trajnimit bazë

Shumica e shkeljeve të sigurisë ndodhin si rezultat i gabimit njerëzor ose pakujdesive. Prandaj për të krijuar një kulture organizative që përqëndrohet mbi sigurinë kompjuterike, janë të nevojshme programet e trajnimit që paralajmërojnë punonjësit për rreziqet e mundshme dhe përdorimin e pakujdesshëm të rrjeteve, programeve dhe pajisjeve. Kështu të gjitha masat e tjera të sigurisë, që nga procedurat themelore e deri tek protokollet mbi të cilat organizata ushtron veprimtarinë e saj do të njihen nga çdo anëtar i stafit.

9.1.5 Shmangia e bashkëngjitjeve të panjohura në e-mail

Asnjëherë nuk duhet klikuar kurrë tek bashkëngjitjet e postës elektronike, pasi ato mund përmbajnë viruse, trojans ose krimba kompjuterikë. Para hapjes së tyre, është e

këshillueshme të kontaktohet dërguesi për të konfirmuar përmbajtjen e mesazhit. Megjithatë në rastet kur burimi është i rrezikshëm, duhet bërë kujdes për fshirjen e mesazhit, bllokimin e llogarisë së dërguesit dhe paralajmërimin e të tjerëve për të bërë të njëjtën gjë.

9.1.6 Mbajtja e të dhënave sensitive jashtë kujtesës Cloud

Cloud computing u ofron bizneseve shumë përfitime dhe reduktime të kostos. Megjithatë shërbimet e tilla gjithashtu mund të paraqesin kërcënime shtesë pasi të dhënat ndodhen në serverë të largët, që ndërveprojnë gjatë gjithë kohës me palë të treta dhe mund të sjellin probleme serioze në lidhje me çështjet e tyre të sigurisë. Ndaj këshillohet që për shumë shërbime, që lidhen me të dhëna konfidenciale dhe sensitive, të tregohet kujdes dhe informacionet të mbahen jashtë Cloud.

9.1.7 Kontrolli i vazhdueshëm i punonjësve

Ndërsa hakerat mashtrues bëjnë gjithnjë e më tepër përpjekje për marrjen dhe kompromentimin e të dhënave, shumica e ndërhyrjeve të paautorizuara ndodhin brenda firewall-eve të kompanive. Monitorimi i vazhdueshëm i punonjësve është gjithashtu i nevojshëm, pasi shpesh për t'u bindur rreth kredibilitetit të tyre nuk mjafton thjesht një CV. Ndaj rekomandohet që një periudhë fillestare prove, gjatë së cilës aksesi në të dhëna të ndjeshme është i ndaluar ose i kufizuar. Një prektikë e ngjashme monitorimi dhe kontrolli për aktivitete të dyshimta në rrjet mund të ndiqet edhe me punonjësit e rinj.

9.1.8 Mbyllni dhe provoni thirrjen përsëri

Të ashtuquajturit "social-engineers", shpesh i mashtrojnë viktimat duke pretenduar të jenë dikush që nuk janë. Nëse një përfaqësues i supozuar nga banka ose partner strategjik pretendon të dijë të dhëna sensitive, është e këshillueshme që thirrja të ndërpritet dhe të kontaktohet drejtpërdrejtë personi i pretenduar, me një numër publik për të konfirmuar nëse thirrja ishte thirrja ishte faktike. Në këtë mënyrë jo vetëm shmanget sulmi por ruhen edhe të dhënat e kompanisë.

9.1.9 Të qënurit vigjilent

Në përfundim të punës së përditshme, këshillohet që të fshihen gjithë informacionet e ndjeshme dhe konfidenciale, që përfshjnë dokumentet me emra të korporatave, adresat, numra llogarish apo të dhëna e transaksione të tjera. Gjithashtu, asnjëherë raportet dhe dokumentat sensitive nuk duhet të lihen në hapësira publike, ku mund të aksesohen nga persona të paautorizuar. Fjalëkalimet duhen ndryshuar rregullisht, veçanërisht pasi janë mësuar nga dikush tjetër me të cilin janë ndarë më herët. Të gjitha këto mund të duken si hapa cliché por duke u treguar vigjilentë mund të parandalohen shkelje të madhe të sigurisë së të dhënave.

9.1.10 Të qënurit i kujdesshëm me klikimet

Mashtrimet me anë të phishing veprojnë duke dërguar e-mail-e nga burime në dukje të besueshme dhe kërkojnë fjalëkalime ose informacione personale. Madje ka edhe mashtrime të tilla ku hakerat krijojnë faqe interneti të rreme që inkurajojnë viktimat e mundshme për të dhënë informacione konfidenciale. Prandaj gjithmonë duhen përdorur adresa të njohura internet dhe të shmanget klikimi në faqe dhe linke të dyshimta, të cilat mund të kërcënojnë sigurinë.

KAPITULLI 10
E ardhmja e sigurisë së sistemeve të informacionit

Duke qënë se numri i software-ve kompjuterikë dhe aplikacioneve vazhdojnë të rriten, nevoja për siguri luan një rol gjithnjë e më të rëndësishëm për sistemet e informacionit dhe zhvillimin e tyre. Shoqëria po bëhet gjithnjë e më e e varur nga aplikacionet kompjuterike, por edhe shërbimet Web gjithashtu. Prandaj sistemet e informacionit nuk mund të kuptohen të distancuara nga zhvillimet teknologjike. Megjithatë së bashku përparimet e vazhdueshme të teknologjisë dhe rritjen e varësisë, vijnë dhe çështje të reja të sigurisë. (Breu et al., 2004) Më herët u trajtuan gjerësisht çështjet aktuale të sigurisë, por çfarë rezervon e ardhmja e sistemeve të informacionit dhe masave, për t'i bërë ata sa më të besueshëm?

10.1 Ku po shkojmë?

Në të shkuarën dizenjimi i sistemeve të informacionit zhvillohej në kushtet e mungesës së informacionit dhe parashikimeve për të ardhmen, gjë që pa qëllim bëhej shkak që sistemi të ishte më vulnerable. Në ditët e sotme nuk mund të flitet për të njëjtën situatë, megjithatë zhvillimi i shërbimeve të internetit parashtron kërcënime të reja për sistemet e informacionit.Disa nga këto kërcënime të reja janë diversiteti dhe numri tepër i lartë i specifikimeve standarde që nuk ofrojnë një vizion të qartë të problemit dhe zgjidhjes; gjendja aktuale në të cilën gjendet shumica e specifikimeve të sigurisë; format e reja të standardeve XML të nevojshme për të strukturuar të dhënat e komunikimin e sigurt të tyre; auditimi; proceset automatike dhe inteligjente të kryera nga makinat dhe ndërveprueshmëria e kërkesave dhe elementeve të sigurisë. (Gutierrez et al., 2004).

Teknologjia XML, që së fundi po implemtohet në masë për dizenjimin e sistemeve të informacionit dhe shihet si e ardhmja e tyre, përbëhet nga disa standard: Enkriptimi XML, Nënshkrimi Dixhital XML dhe Sistemi kryesor i manaxhimit XML. Enckriptimi XML ofron një model për enkriptimin dhe dekriptimin e plotë të dokumentave dhe elementet XML. Ai zgjidh problemet me konfidencialitetin dhe shpërndarjen e mesazheve të shkëmbyera nëpërmjet internetit, duke përdorur protokollin SOAP (Simple Object Access Protocol). SOAP është protokoll për shkëmbimin e informacionit në një mjedis të decentralizuar dhe të shpërndarë, në mënyrë që të dhënat të mbahen sa më të sigurta gjatë kalimit nëpër rrjeta. Edhe pse XML zgjidh disa probleme, ka gjithashtu çështje sigurie që ende kanë nevojë për vëmendje. Specifikimet e

XML dhe SOAP nuk shpjegojnë se si ruhet konfidencialitetin dhe origjinalitetin i informacionit që transportohet

10.2 Projeksionet e së ardhmes

Duke pasur parasysh përhapjen e pandërprerë të rrjeteve të sistemit të informacionit dhe fakti burimet e një rrjeti janë të ndarë ndërmjet përdoruesive, siguria e rrjetit do të vazhdojë të luajë një rol mbizotërues. Natyrisht, e ardhmja rezervon rrjete që do të shtrihen dhe përhapen në distanca shumë të mëdha gjeografike. Gjithashtu këtyre rrjeteve do iu duhet të suportojnë rritjet e mëdha në numrin e përdoruesve, shtimin e nyjeve e lidhjeve dhe ofrimin e shërbime shumë të sofistikuara.(Ghosh, 2002) Të gjitha këto kërkesa sjellin edhe një rritje ndërgjegjësimi rreth çështjeve të sigurisë dhe masave që duhen ndërmarrë, që shkëmbimi i informacionit nëpër sisteme të bëhet në mënyrë të besueshme. Prandaj për të siguruar rrjete të tilla, zgjidhja shihet shpesh tek Sistemet e zbulimit të ndërhyrjeve (IDS), Filtrimi i paketave (PF) dhe Application Layer Gateways (ALG). Ato nuk përdoren vetëm për të kontrolluar trafikun nëpë rrjet si për shembull sa paketa hyjnë dhe dalin nga sistemi, por gjithashtu përdoren për filtrimin e trafikut të keq dhe të paautorizuar në bazë të rregullave që aplikohen. (Koch et al. 2012)

10.3 Sfidat që rezervon e ardhmja

Sigurisht që bashkë me zhvillimet me ritme të shpejta që janë duke u përhapur në masë dhe projeksionet që pritet të bëhen realitet në të ardhmen, duhet që të gjenden e projektohen zgjidhje më efikase për problemet e parashtruara në lidhje me çështjet e sigurisë të sistemeve të informmacionit. Prandaj për zhvilluesit e sistemeve lind nevoja që të ndiqen studime dhe metoda kërkimi në aspekte më pak të njohura, pasi e ardhmja parashtron sfida të shumta.

Një nga këto sfida është për shembull zhvillimi i algoritmave vetë- rimëkëmben nga dështimet e lidhjes ndërmjet nyjeve. Në rastet kur kemi të bëjmë me shkëmbime informacioni me shpejtësi dhe bandwidths shumë të lartë, një shkëputje e lidhjes ndërmjet nyjeve do të sillte eventualisht rënien e sistemit dhe probleme tepër serioze, sidomos për aplikimet në mjekësi dhe ushtri. Çdo teknikë restaurimi manual do të ishte e papërshtatshme pasi ato janë tepër të ngadalta dhe shpejtësia e sistemit do të binte ndjeshëm. Me përdorimin e algoritmave që bëjnë të mundur vetë-korrigjimin, në mënyrë automatike problemet do gjenin zgjidhje dhe integriteti original i informacionit nuk do të cënohej.

Nga ana tjetër, masat e sofistikuara të sigurisë dhe procedurat komplekse për të parandaluar sulmet, në përgjithësi kërkojnë llogaritje me precision të lartë. Duke pasur parasysh edhe faktin se e ardhmja rezervon rrjete, shpejtësia e të cilave me gjasë do të vazhdojë të rritet, është kritike që të zhvillohen pajisje dhe arkitektura të reja që të përmbushin këto objektiva. Zgjidhja do të gjendej në dizajnimi e arkitekturave inovative që suportojnë rritjen e kërkesave të sofistikuara kompjuterike dhe me aftësi llogaritëse të shtuara.

Përmirësime e kërkime të tjera mund të bëhen edhe në lidhje me stabilitetin e performacës së sistemeve apo lokalizimin e shpejtë të burimeve të disponueshme. Gjithnjë e më shumë, ekspertët në sistemet e informacionit vendosin theksin mbi rolin e stabilitetit dhe disponueshmërisë së sistemit duke aplikuar metoda kërkimore në inxhinierimin e sistemeve të kontrollit, të cilat mund të përdorin një qasje empirike për të lidhur qëndrueshmërinë e sistemit me performancën rritje të rrjetit.
(Ghosh, 2002)

10.4 Inteligjenca e sigurisë

Inteligjenca e sigurisë përgjithësisht mund të cilësohet si një mjet ruajtje, për të cilën aktualisht punohet shumë dhe mendohet se në të ardhmen do luajë një rol jetik në mbrojtjen e informacioneve dhe të dhënave të sistemeve kompjuterike. Në thelb, ajo përbëhet nga informacione, mjete dhe taktika të dobishme për mbrojtjen ndaj rreziqeve që kërcënojnë kompanitë, të brendshme ose të jashtme qofshin ato.

Veçantia qëndron në faktin se inteligjenca e sigurisë shfaq cilësi të intelektit njerëzor dhe mund të bëjë dallimin e menjëherëshëm të fakteve të vërteta dhe atyre të trilluara ose të korruptuara në mënyra të tjera. Duke u nisur nga fakti se të dhënat dhe input-et e firmave janë pjesa themelore mbi të cilat ngrihet gjithë sistemi, kjo do të ishte një ndihmë e madhe për mbarëvajtjen e punës së tyre. Prandaj informacionet duhet të mblidhen përmes praktikave të duhura, në mënyrë që të jenë të zbatueshme, faktike dhe të kenë përdorim praktik për organizatën. Sinkronizimi i këtyre mjeteve u mundëson bizneseve të fitojnë informata të përditësuara për nevojat e sigurisë, në mënyrë që të shmangin situatat e rrezikshme dhe të përmirësojnë incidentet. Pra në vetvete, inteligjenca e sigurisë është mjet dhe jo qëllim për të mbrojtur dhe fuqizuar një kompani.

Nga ana tjetër, me gjithë zhvillimet teknologjike dhe lirine e veprimit që makineritë po fitojnë, duke shfaqur tipare inteligjence dhe thujse duke zëvendësuar trurin njerëzor, ka pikëpyetjet të shumta. Sot, falë përparimeve të fundit, janë në veprim pasjisje dhe shpikje të tilla, thjesht ideja e të cilave para disa dekadash ndeshej në fanta-shkencë. Zhvillimite të këtij lloji, sot më shumë se më parë kanë potencial për t'u bërë më inteligjente se njeriu, sepse me apo pa dashje, atyre po iu jepet një aftësi e tillë intelekti, që mundet edhe të zëvendësojë pa problem trurin njerëzor. Prandaj sot nuk ka asnjë mënyrë të sigurt për të parashikuar se si sisteme të tilla superinteligjente do të sillen. A mund të mbahen ato nën kontroll? Vetë evolucioni ka treguar se njeriu zotëron planetin, vetëm sepse përdor inteligjencën dhe intelektin, ndryshe nga çdo qënie tjetër . Megjithatë nëse diçka më inteligjente do të arrijë të shpiket, a do të mbetet më njeriu në kontroll të gjithçkaje?

KAPITULLI 11
Konkluzione

Në përfundim të këtij punimi, pasi u trajtuan sistemet e informacionit dhe çështjet e sigurisë, vlen të vendoset theksi pikërisht tek mbrojtja e saj, si parimi themelor që i bën sistemet më të të besueshëm. Të dhënat dhe informacionet e një organizate janë padyshim pasuria më me vlerë e saj ndaj mbrojtja e tyre nga sulmet e kërcënimet që synojnë t'i manipulojnë e korruptojnë ato në forma të ndryshme qëndron në pararojë të objektivave themelore.

Sistemeve të informacionit sot, po iu besohen jo vetëm veprime transaksionesh të thjeshta, përkundrazi, ata janë sot të implementuar thuajse kudo. Shtetet qeverisen me ndihmën e tyre, ushtritë dhe stabiliteti i një vendi varet nga to, sisteme të zhvilluara komplekse janë implementuar në mjekësi, ku ruajnë, përpunojë dhe përcaktojë diagnoza sëmundjesh bazuar në input-in që iu jepet, për të mos folur pastaj për bizneset, kur sistemet e informacionit janë pjesa më vitale e menaxhimit strategjik.

Nisur nga gjithë kjo rëndësi e ditëve të sotme, sisteme që tolerojnë dobësitë dhe ku nuk mbrohet siguria e të dhënave përkthehen jo vetëm në kosto operacionale shtesë por edhe rrezikshëri për individët, shtetet dhe bizneset. Prandaj, për të pasur sisteme të sigurta informacioni që përmbushin me objektivitet dhe sukses qëllimet e tyre, duhet të aplikohen kontrolle të herëpasherëshme, të merren masat e nevojshme, të implementohen e zgjidhen arkitekturat e duhura, si dhe të bëhen kërkime të mëtejshme ku duhet të kthehet vëmendja në të ardhmen për përmirësime të mëtejshme.

KAPITULLI 12
Sugjerime

Pas trajtimit të kapitujve dhe njohjes me çështjet e parashtruara, sigurisht që arrihet në disa përfundime. Së pari vlen të përmendet se mbrojtja e sigurisë së përgjithshme të sistemit mund të realizohet edhe me hapa të vegjël, të ndëmarrë nga çdo punonjës. Veprime të tilla si mbrojtja me fjalëkalime, skanimi për viruse, trajnimi i stafit, back-up i të dhënave, përditësimi i software-ëve, shmangia e e-mail-eve të panjohur, apo madje edhe thjesht të qënit vigjilentë në punën e përditshme, rreth rrezikut që i kanoset informacioneve nga sulmet e paautorizuara, janë në dukje veprime të vogla, por që luajnë një rol të rëndësishëm.

Sigurisht që jo gjithçka duhet të lihet në dorë të punonjësve, sepse shpesh me qëllim të keq ose thjesht nga një gabim i rastit janë ata kërcënimi në fjalë. Ndaj do të rekomandohej që për mbrojtjen e sistemeve, të përdoreshin firewall-e, sisteme të zbulimit të sulmeve(IDS), kur po tentohet një i tillë, rujatja në server offsite i informacionit pas back-up, përdorimi i DMZ-ve, etj. Megjithatë një nga masat më të mira do të ishte enkriptimi i infomacionit dhe pëdorimi i çelësave, për kodimin e të dhënave konfidenciale e të ndjeshme. Madje pikërisht çelësat dinamikë do të ishin akoma më efektivë dhe të sigurt në përdorim.

Për sa i përket arkitekturës kompjuterike të sistemeve, sigurisht që luan një rol vendimtar në sigurinë e tyre, Përdorimi i një arkitekture me shtresa, ku mbrojtja në thellësi bën të mundur që personat e paautorizuar të ndeshen me shumë shtresa kontrolli është gjithashtu shumë efikas. Megjithatë, përdorimi i standardeve XML në dizenjimin e arkitekturës i jep zgjidhje edhe problemeve të mundshme të kriptimit që pëson informacioni nëpër shtersa.

Nga ana tjetër, e ardhmja parashton sfida të reja dhe sugjerohet që për sisteme më performantë, të punohet në lidhje me algoritma vetë-rimëkëmbës ndaj dështimeve, kështu restaurimi do të ndodhë më shpejt dhe nuk do të cënojë integritetin e të dhënave. Gjithashtu përmirësimet në lidhje me fuqinë përpunuese të sistemit, për volum më të lartë të dhënash janë të detyrueshme duke qënë se çdo ditë e më shumë teknologjia e infomacionit po fiton pushtet dhe po përdoret kudo.

KAPITULLI 13
Referenca

1. (Alghazzawi et al., 2014)- Daniyal Alghazzawi, Syed Hamid Hasan & Mohamed Salim Trigui, "Information Systems Threats and Vulnerabilities", vëll. 89, 2014
   International Journal of Computer Applications

2. (Bench-Capon et al., 2007) – T.J.M. Bench-Capon & Paul E.Dunne, "Argumentation in artificial intelligence", vëll. 171, fq. 619-641, 2007
   Për më tepër: https://dl.acm.org/citation.cfm?id=1285088

3. (Bourgeois et al., 2015) – Dave Bourgeois & David T. Bourgeois, "Information Systems for bussines and beyond", kap. 6, 2015

4. (Breu et al., 2004)- Ruth Breu, Klaus Burger, Michael Hafner, Gerhard Popp, "Towards a Systematic Development of Secure Systems", 2004

5. (CNSS, 1992) – CNSS, National Training Program for Information Systems Security (INFOSEC) Professionals, National Security Telecommunications and Information Systems Security Committee, 1992

6. (Dehaghani et al., 2013)- Sayed Mehdi Hejazi Dehaghani & Nafiseh Hajrahimi, "Which factors affect software projects cost more?", fq.63- 66, 2013

7. (Ghosh, 2002)- Sumit Ghosh, "Principles of Secure Network Systems Design", kap.8, f1. 187-192, 2002
   Springer Science+Business Media New York

8. (Gutierrez, 2004)- Carlos Gutierrez, Eduardo Fernndez-Medina & Mario Piattini. "Web Services Security: Is the Problem Solved", 2004

9. **(**Henderson et al., 1999) – J.C. Henderson & H. Venkatraman, "Strategic alignment: Leveraging information technology for transforming organizations", vëll. 38, 1999
   Për më tepër: https://ieeexplore.ieee.org/abstract/document/5387096/

10. (Jackson, 1998) – Peter Jackson, "Introduction to Expert Systems", vëll. 3, 1998
    Për më tepër: https://dl.acm.org/citation.cfm?id=521024

11. (Jen Yeh et al., 2007)- Quey Jen Yeh & Arthur Jung-Ting Chang, "Threats and countermeasures for information system security: A cross-industry study", vëll. 44, 2007

12. (Joshik, 2015)- P.Joshik, "Managing and contolling information systems", kap.14 &16, 2015
    University of Missouri-St. Louis
    Për më tepër: http://umsl.edu/

13. (Koch et al. 2012) - R.Koch, B. Stelte & M. Golling, "Attack trends in present computer networks", 4th International Conference on Cyber Conflict IEEE, 2002

14. (Latham et al., 1985) - D.C. Latham, S.L. Brand, G. Hammonds, P.S. Tasker, D.J. Edwards & R.R. Schell, "Department of Defense Trusted Computer System Evaluation Criteria", DoD 5200.28
US National Security Institute, 1985

15. (Laudon et al.,2004) – Keneth C.Laudon &Jane P. Laudon, "Management Information Systems: Managing the Digital Firm", New Jersey: Prentice Hall, 2004.

16. (McLeod et al., 2007) – Raymond McLeod, Jr. & George P. Schell, "Management Information Systems", vëll. 8, kap. 13, 2007

17. (O'Brien et al., 2006) – James A. O'Brien & George M. Marakas, "Management Information Systems", vëll. 7, 2006

18. (O'Brien, 2005) – James A.O'Brien, "Introduction to information systems", vëll.12, 2005

19. (Parker, 1998) – D.B. Parker, 'Fighting Computer Crime: A new Framework for Protecting Information", 1998
New York. Wiley Computer Publishing, John Wiley & Sons, Inc.

20. (Ross, 2014) – Ronald S.Ross, "Security and Privacy Controls for Federal Information Systems and Organizations [including updates as of 1/15/2014]", 2014
Për më tepër: https://www.nist.gov/publications/security-and-privacy-controls-federal-information-systems-and-organizations-including-0

21. (Ruseti et al., 2005) - Bashkim Ruseti & Kozeta Sevrani, "Sistemet e Informacionit të Menaxhimit", fq. 8, 2005

22. (Safianu et al., 2016) – Omar Safianu & Frimpong Twum, "Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection", 2016

23. (Schroeder et al., 2009) – Bianca Schroeder & Garth Gibsoon, " A large-scale study of failures in high-performance computing systems", vëll. 7, 2009

24. (Zwass, 1997) - Vladimir Zwass, "Bazat e sistemeve të informacionit", 1997
Foundations of Information Systems
Irwin/McGraw-Hill Companies, Inc. New York

25. (Villarroel et al., 2005) – Rodolfo Villarreal, Eduardo Fernandez-Medina, Mario Piattini, "Secure information systems development- a survey and comparison", vëll. 24, fq. 308-321, 2005

26. (Whitman et al.,2009) – Michael E.Whitman & Herbert J.Mattord, “Principles of information security”, vëll. 4, 2009

27. (Wu et al., 2007) - Junxiu Wu, Qiang Feng, Bijun Liang & Angsheng Wang, “ The integrated information system for natural disaster mitigation”, vëll. 6, 2007

28. (Wu, 2009) – Xianping Wu, “Security Architecture for sensitive information systems”, Faculty of Information Technology
Monash University, Australia, 2009