Siguria e informacionit, politikat e sigurisë dhe ndërgjegjësimi i përdoruesve në fushën e sigurisë

Burbuqe Beqiraj

Abstrakti

Siguria e informacionit po mbetet një shqetësim i madh për shumë institucione dhe organizata, pasi që, rreziqet në këtë rast mund të kenë pasoja negative tek bizneset dhe në marrëdhëniet me klientët. Dihet se vetëm teknologjia nuk mund të garanton një mjedis të sigurt të informacionit dhe se rol të rëndësishëm në këtë aspekt kanë edhe përdoruesit. Mungesa e vetëdijesimit dhe përgjegjësia morale janë arsyet kryesore të shkeljeve te sigurisë. Tanimë shumë kompani janë bërë viktima të sulmeve kibernetike, për shkak të menaxhimit të dobët dhe pamundësisë për të përcaktuar rreziqet në lidhje me mbrojtjen e të dhënave. Prandaj është e rëndësishme të kryhen analiza të vazhdueshme të menaxhimit të rrezikut si dhe trajnimi i përdoruesve në fushën e sigurisë së informacionit. Ky punim fokusohet në disa modele, të cilët adresojnë zhvillimin dhe rishikimin e politikave të sigurisë së informacionit si dhe vetëdijesimin e personelit për sigurinë e informacionit duke u bazuar në konfidencialitetin, integritetin dhe disponueshmërinë. Studimi ka për qëllim identifikimin e shkeljeve të sigurisë, vlerësimin e kërcënimeve, analizimin e masave të sigurisë dhe paraqitjen e përvojave të ndryshme nga fusha e sigurisë së informacionit.

1. Hyrje

Siguria e informacionit vazhdon të mbetet një nga shqetësimet me të mëdha për qeveritë dhe kompanitë e ndryshme, prandaj, është e domosdoshme që vazhdimisht të shqyrtohen praktikat dhe politikat e sigurisë për të shmangur rreziqet që kanë të bëjnë me keqpërdorimin e informacionit.[2] Gjithashtu ndërgjegjësimi i përdoruesve ka një rol të rëndësishëm në menaxhimin e rrezikut dhe incidenteve të sigurisë së informacionit.[6] Shumë kompani nuk janë në gjendje të arrijnë sigurinë e informacionit pasi që personeli i tyre nuk është i vetëdijshëm për përgjegjësitë dhe rolin që ka në lidhje me misionin e kompanisë, dhe nuk arrijnë të kuptojnë praktikat dhe politikat e sigurisë.[1]

Mirëpo ekzistojnë faktorë si shkëmbimi i njohurive rreth sigurisë së, bashkëpunimi dhe përvoja në sigurinë e informacionit për të cilët supozojmë që ndihmojnë në ndërgjegjësimin e përdoruesve dhe ndikojnë ne qëndrimin dhe sjelljen e tyre, për të ofruar sigurinë e informacionit.[7]

Përveç trajtimit të këtyre faktorëve, ky punim fokusohet në identifikimin e kërkesave të sigurisë, ku përfshihet vlerësimi rreziqeve, kërkesat ligjore dhe kërkesat e kompanive për sigurimin e informacioneve. Mirëpo qëllimi kryesor i punimit është identifikimi i shkaktareve të incidenteve të sigurisë në kompani të ndryshme, kompani të cilat në të kaluarën u përballën më incidente të sigurisë.

2. Shqyrtimi i literaturës

2.1 Siguria e informacionit dhe kërkesat e sigurisë

Siguria e informacionit është një element i rëndësishëm i çdo organizate që nënkupton mbrojtjen e informacioneve dhe elementet e tij kritike nga një gamë e gjerë kërcënimesh. Konfidencialiteti, integriteti dhe disponueshmëria e informacionit janë karakteristikat kryesore të sigurisë së informacionit.[8] Siguria e informacionit mund të arrihet duke zbatuar një sërë kontrollesh të përshtatshme përfshirë procedurat dhe strukturat organizative. Prandaj, është shumë e rëndësishme që një organizatë të bëjnë identifikimin e kërkesave të sigurisë, karakteristikat kryesore të kërkesave të sigurisë janë:

- Vlerësimi i rrezikut që merr parasysh strategjinë e përgjithshme dhe objektivat e organizatës
- Kërkesat ligjore, rregullative dhe kontraktuale që kontraktorët dhe ofruesit e shërbimeve duhet të përmbushin
- Caktimi i objektivave dhe kërkesave të organizatës për mbrojtjen e informacioneve

Gjatë identifikimit të kërkesave duhet të aplikohen dokumentet e politikave të sigurisë së informacionit, caktimi i përgjegjësive dhe menaxhimi i incidenteve që bazohen në legjislacionet në fuqi, siç janë: mbrojtja dhe privatësia e të dhënave personale, mbrojtja e të dhënave organizative, dhe të drejtat e pronësisë intelektuale.[8]

2.2 Modelet e sigurimit të informacionit

Konfidencialiteti, integriteti dhe disponueshmëria ka shërbyer për disa dekada si model konceptual i sigurisë së informacionit. Më vonë ky model u zgjerua me elemente tjera siç janë: Dobia, Autentifikimi, Mosnjohja, Shkaktaret e rrezikut, Llojet e kontrollit, Politikat për mbrojtjen e informacionit, dhe Objektivat e sigurisë së informacioni.

Me zhvillimin e modelit *Business Model for Information Security* (BMIS), u implementuan praktika për sistemet e informacionit, të cilat përfshinë dizajnin dhe strategjinë e organizatës, burimet njerëzore, proceset dhe teknologjinë.

Mirëpo, mangësi e këtyre modeleve ka qenë mungesa e trajtimit të qëllimeve të sigurisë, qeshje të cilat më vonë u shyrtuan në modelin *Reference Model of Information Assurance and Security* (RMIAS). Ky model përbëhet nga katër dimensione, të cilat janë:

• Cikli i jetës - përshkruan progresin e sigurisë së informacionit gjatë zhvillimit, dimension i cila përfshinte kërkesat e sigurisë, dizajnin e sigurisë, implementimin dhe monitorimin e sigurisë

• Klasifikimi i informacioneve - përshkruan natyrën e informacioneve që duhet të mbrohen

• Qëllimi i sigurisë - përshkruan aftësitë për t'i rezistuar kërcënimeve të ndryshme, dimension i cili përfshin integritetin, konfidencialitetin, disponueshmërinë, privatësinë e të dhënave

• Kundërmasat e sigurisë - kategorizon masat e disponueshme për mbrojtjen e informacioneve, duke përfshirë strategjinë organizative, burimet njerëzore, strukturat ligjore dhe teknike

Këto karakteristika konsiderohen të detyrueshme për fushën e sigurisë së informacionit.[5]

2.3 Organizimi i politikave të sigurisë dhe vlerësimi i kërcënimeve

Megjithëse shumica e kompanive përdorin teknologji të ndryshme për mbrojtjen e informacionit, një gjë e tillë nuk është e mjaftueshme. Organizimi i politikave të sigurisë ka rol të rëndësishëm në sigurinë e informacionit. Prandaj politikat e sigurisë së informacionit duhet të jenë të qarta dhe të kuptueshme për personelin, pasi që një planifikim i dobët i politikave të sigurisë mund të rezultojë në mungesë të mbrojtjes së të dhënave ose mos zbatimit nga përdoruesit. [3] Sjellja e përdoruesve në pajtueshmëri me politikat e sigurisë dhe përgjegjësia morale është sfidë mjaftë e madhe për kompanitë. Promovimi i sjelljes së mirë të përdoruesve dhe zbatimi i politikave të sigurisë mund të jenë një politikë efektive në kompani.[6]

Po ashtu vlerësimi i kërcënimeve konsiderohet të jetë një faktor i rëndësishëm që ndikon në organizimin e politikave të sigurisë së informacionit. Përmes vlerësimit të kërcënimeve mund identifikohen kërcënimet ndaj aseteve, të vlerësohet cenueshmëria, dhe të gjenden shkaqet e ndodhjes së incidenteve.[8] Rezultatet e vlerësimit të kërcënimeve ndihmojnë në përcaktimin e masave të përshtatshme për menaxhimin e kërcënimeve dhe zbatimin e kontrolleve për t'u mbrojtur nga kërcënimet e ndryshme.

2.4 Teknikat e sigurisë së informacionit

Për të arritur sigurinë e informacionit çdo kompani ka në përdorim teknika të ndryshme të mbrojtës, por që në përgjithësi fokusi kryesor është në menaxhimin e fjalëkalimeve, përdorimin e email-it, përdorimin e internetit, dhe përdorimin e programeve të ndryshme të cilat janë të parapara me politikat e sigurisë së informacionit.

Menaxhimi i fjalëkalimeve - koncepti i fjalëkalimit të përdoruesit është themelor në sigurimin e informacionit. Fjalëkalimi është një nga masat për të arritur sigurinë e informacionit. Politikat e sigurisë së informacionit trajtojnë menaxhimin e fjalëkalimit dhe shpjegojnë hapat e përdoruesit që duhet t'i ndjek për të ndryshuar fjalëkalimin, si dhe shpjegon praktikat më të mira që në lidhje me menaxhimin e fjalëkalimeve.

Përdorimi i e-mailit - përgjegjësitë e secilit departament të IT-së janë definuar në dokumente të veçanta të politikave të sigurisë së informacionit. Përgjegjësitë që kanë të bëjnë me përdorimin e e-mailit ndihmojnë përdoruesit të jenë më të kujdesshëm në çështje të tilla si *fishing*. Shpërndarja në mënyrë automatike e email-it zyrtar nga serverë të ndryshëm paraqet rrezik të lartë të sigurisë. Megjithëse është kritike, çështja e dërgimit të email-it deri më tani nuk është paraparë në asnjë dokument të politikave të sigurisë së informacionit.

Vërtetimi i të dhënave - dokumentet duhet të jenë gjithmonë të vërtetuara, ato para shkarkimit duhet të kontrollohen nëse kanë origjinë nga burime të dyshimta. Vërtetimi dokumenteve mund të bëhet nga programe të tilla si *antivirus*. Prandaj, një *antivirus* i përshtatshëm është thelbësor për mbrojtjen e informacionit. Shumica e programeve të tilla përmbajnë funksionin e përditësimit automatik për viruset e rijë.

Firewall - është një program kompjuterik i cili ndihmon në identifikimin e viruseve me qëllim për të dëmtuar informacionet. Firewall, analizon çdo të dhënë dhe bllokon ato që nuk i plotësojnë kriteret e parapara të sigurisë, prandaj është shumë e rëndësishme që të gjitha të dhënat që kalojnë përmes internetit të trajtohen nga ky program.

Përdorimi i internetit – përdoruesit vazhdimisht paralajmërohen të shmangin përdorimin e pavend të in-

ternetit, duke përfshirë këtu edhe përdorimin e infrastrukturës institucionale si dhe diskutimin e çështjeve të ndjeshme të cilat nuk kanë të bëjnë me detyrat e punës. Përveç kësaj, institucionet kanë të drejtë të monitorojë përdoruesit gjatë përdorimit të internetit për të siguruar respektimin e politikave të sigurisë.[3]

Mirëpo, përfshirja e vetëm këtyre elementeve në sigurimin e informacionit është e pamjaftueshme. Kompanitë dhe institucionet duhet të ofrojnë programe ndërgjegjësimi për sigurinë, veçanërisht kur dihet se incidentet e shumta të sigurisë shkaktohen nga mungesa e vetëdijes së përdoruesve.

2.5 Ndërgjegjësimi i përdoruesve për sigurinë së informacionit

Ndërgjegjësimi është çështje më rëndësi në çdo sistem të menaxhimit të sigurisë. Zëvendësimi i proceseve manuale me ato digjitale për të ofruar shërbime të shpejta dhe të lehta, dhe kërcënimet e ndryshme që paraqiten bën që ndërgjegjësimi për sigurinë e informacionit çdo vit të bëhet edhe më i rëndësishëm. Ndërgjegjësimi është një proces dinamik, që paraqet nevojën për trajnimin e përdoruesve dhe përditësim të vazhdueshëm të programeve dhe politikave të sigurisë.[6] Përpjekjet që kanë të bëjnë me ndërgjegjësimin përfshijnë ndryshimin e sjelljes së përdoruesve dhe përforcimin e praktikave të sigurisë në mbrojtjen e aseteve fizike dhe informacioneve te rëndësishme. Shumë faktorë ndikues janë identifikuar në ndërgjegjësimin e sigurisë së informacionit të tilla si konfidencialiteti, integriteti dhe disponueshmëria.[1] Po ashtu shkëmbimi i njohurive rreth sigurisë së informacionit, përvoja dhe bashkëpunimi ndikojnë në ndërgjegjësimin e përdoruesve.[7]

Shkëmbimi i njohurive është sfida më e rëndësishme e kësaj fushe. Ndarja e njohurive rreth sigurisë së informacionit më të tjerët është një qasje efektive për të rritur nivelin e ndërgjegjësimit të përdoruesve në sigurinë e informacionit dhe mund të rezulton në menaxhimin e kohës dhe të parave.[4] Po ashtu, shkëmbimi i njohurive rreth sigurisë së informacionit mund të ketë efekt në zgjidhjen e problemeve, duke krijuar ide të reja dhe duke zbatuar politikat ose procedurat e sigurisë.

Gjithashtu përvojat e mëparshme në fushën e sigurisë së informacionit janë një burim shumë i vlefshëm në ndërgjegjësimin e sigurisë së informacionit.[7] Përvoja i referohet njohurive dhe aftësive që kanë të bëjnë me trajtimin e incidenteve, për të parandaluar, menaxhuar dhe zbuluar rrezikun duke përfshire strategjinë, planifikimin, procedurat, politikat dhe standardet të ndryshme të menaxhimit të sigurisë së informacionit.[4] Mungesa e njohurive dhe përvojës në sigurinë e informacionit është problemi kryesor i përdoruesve në punën e sigurisë së informacionit. Kështu që përvoja mund të ndikon pozitivisht në reagimin e përdoruesve ndaj incidenteve dhe në zbatimin e politikave të sigurisë së informacionit.

Qendra e informacionit për sigurinë ndihmon ekspertët të mbledhin, integrojnë, klasifikojnë dhe shpërndajnë njohuritë që kanë të bëjnë më sigurinë e informacionit, me ekspertët dhe punonjësit e tjerë. Bashkëpunimi në mes ekspertëve, grupeve ose organizatave që punojnë së bashku për të arritur qëllime të përbashkëta në fushën e sigurisë së informacionit është një nga politikat më të suksesshme, dhe gjithashtu u mundëson përdoruesve lehtësisht të kuptojnë dhe të adresojnë problemet kritike të informacionit.

Hapësira kibernetike është një hapësirë dinamike dhe ndërgjegjësimi i përdoruesve duhet të trajtohet shpesh, kështu që ndërhyrja e nevojshme në fushën e sigurisë së informacionit rrit nivelin e ndërgjegjësimit në fushat e sigurisë dhe raportimin e incidenteve.[4]

3. Identifikimi i incidenteve të sigurisë – Raste studimi

Në vazhdim janë paraqitur disa raste të kompanive të ndryshme, të cilat në të kaluarën janë përballur me incidente të ndryshme të sigurisë dhe kanë analizuar shkaktaret e ndodhjes së incidenteve.

3.1 Rasti I - Banka Agro-Allied

Kjo banke ishte një nga bankat më shumë përgjegjësi publike, që jepte hua kryesisht për sektorin e bujqësisë. Kjo bankë u ballafaqua më vjedhjen e 'kasetave kompjuterike' gjatë transferimit te tyre për në Departamentin e Byrosë së Kreditit të Bankës Qendrore të Nigerisë. Kasetat të cilat ishin zhdukur përmbanin të dhënat personale dhe historitë e pagesave të miliona klientëve.

Arsyeja pse kjo bankë u gjend në një situatë të tillë, ishte për shkak të mos identifikimit me kohë të rrezikut, pasi që besonin se mënyra e shërbimit për transferimin e të dhënave ishte shumë e sigurt dhe se sipas tyre të dhënat nga kasetat ishin vështire për t'i lexuar, sepse për leximin e tyre nevojiteshin pajisje harduerike.

Pas këtij rasti, banka vendosi që të bënë transferimin e informacionit dhe të dhënave të vlefshme në mënyre elektronike duke përdorur metoda të kriptimit dhe metoda tjera si më të sigurta.[2]

3.2 Rasti II - Performance Evaluation Bureau

Byroja e Vlerësimit të Përformancës (*Performance Evaluation Bureau*) ka qenë e regjistruar si një organi-

zatë private në Afrikën Perëndimore. Filialet e kësaj byroje operonin me disa departamente të policisë, departamentin e shëndetësisë dhe institucione tjera si universitete, kolegje dhe banka, të cilat ndihmojnë në hetimin e krimeve, në kontrollin e kredive etj.

Byroja ishte sulmuar nga disa persona të cilët kishin arritur të kenë qasje në informacionet duke përfshirë të dhënat personale, informacionet e klientëve dhe raportet e kreditit. Edhe pse në atë kohë kishte supozime të shumta rreth shkakut të ndodhjes se incidentit nëse ky ishte një mashtrim i kryer nga persona të brendshëm, apo u shkaktua nga krimi i organizuar, e rëndësishme ishte që rasti kishte ndodhur pasi qe organizata nuk kishte arritur të identifikojë vrimat e hapura të sistemit për të mos mundësuar një ngjarje të tillë.[2]

3.3 Rasti III - Organizata YHLI

YHLI ishte një nga kompanitë kryesore prodhuese në Azi, e cila u përball me shkelje të sigurisë së informacionit. Kompania kishte shërbyer si rast specifik për të hetuar si faktori njeri mund të ndikojnë në menaxhimin e sigurisë dhe për të studiuar faktorët që duhet të merren parasysh gjatë planifikimit dhe zbatimit të sigurisë, dhe gjatë shkëmbimit të informacioneve.

Sipas kompanisë, sistemi i informacioneve ishte sulmuar nga persona të paautorizuar, të cilët kishin qasje të drejtpërdrejt ne bazën e të dhënave të klientëve, por që nuk mund të konfirmohej si kishte ndodhur sulmi pasi që nuk kishte prova te mjaftueshme se si ishin vjedhur të dhënat personale të klientëve dhe numrat e kredit kartave të tyre.

Paaftësia e kompanisë për të përcaktuar nëse sulmi në të dhënat e klientëve kishte ndodhur, tregoj se nuk kishte një sistem të menaxhimit në kohë reale. Po ashtu, në këtë rast u zbulua se siguria e informacioneve nuk ishte trajtuar ashtu siç duhet, dhe nuk kishte një plan për menaxhimin e vjedhjes së informacioneve.

Si pasoje e mungesës se planifikimit te duhur dhe mungesës se vlerësimit të rrezikut ndodhi qe organizata të falimentonte.[2]

4. Përfundimet

Zhvillimi i hapësirës kibernetike dhe kërcënimet e ndryshme, po sfidojnë sigurimin e infrastrukturës së informacionit. Kompanitë dhe institucionet e ndryshme duhet të kuptojmë rëndësinë e mbrojtjes së të dhënave dhe informacioneve të vlefshme nga teknologjitë dhe praktikat e dobëta.

Përdorimi i teknikave të ndryshme (menaxhimi i fjalëkalimeve, përdorimin i email-it, përdorimi i internetit, dhe përdorimi i programeve të ndryshme) për mbrojtjen e informacioneve janë një zgjidhje e duhur për shumë kompani dhe institucione, edhe pse rëndësia e tyre ndryshon varësisht nga njëra tjetra, si dhe përdorimi i tyre ndonjëherë nuk është në përputhje me politikat dhe udhëzimet e sigurisë.

Por që në përgjithësi incidentet e sigurisë së informacionit po ndodhin për shkak te mungesës së identifikimit të rrezikut në kohën e duhur, ose për shkak të mungesës së një sistemi të menaxhimit në kohë reale. Po ashtu incidentet mund te ndodhin për shkak se mbrojtja e të dhënave trajtohet vetëm si çështje teknike, duke mos arritur të kuptohet rëndësia e përdoruesve në mbrojtjen e informacionit dhe në krijimin e politikave të sigurisë dhe menaxhimin e rrezikut.

Ndërgjegjësimi i përdoruesve ka efekt pozitiv në sigurinë e informacioneve dhe mund të konsiderohet një nga politikat më të suksesshme në identifikimin e kërcënimeve, vlerësimin e kërcënimeve dhe trajtimin e tyre. Ndërsa ndërgjegjësimi i përdoruesve ndikohet nga bashkëpunim, përvoja dhe ndarja e njohurive më të tjerët, ku dhe vërtetohet supozimi i dhënë në fillim të punimit.

Ndonjëherë është e pamundur që të parandalohen të gjitha incidentet e sigurisë që mund të shkaktojnë humbjen e të dhënave dhe informacioneve, por kompanitë duhet të kenë politikat dhe praktika e duhura të sigurisë që të paktën të minimizojnë dëmet e incidentit. Gjithashtu duhet të zhvillojnë aftësinë për të ndryshuar dhe përshtatur me kërcënimet e reja që mund të shkaktojnë dëmtime në infrastrukturën e informacionit.

5. Referencat

[1] N. M. N. M. Z. R. I. Faizatul Akma Mohd Adnan, Rasimah Che Mohd Yusoff, "Information security awareness:case study in stock-broking company," *International Conference on Information Technology and Society*, pp. 93–98, 2015.

[2] J. O. Oyelami, "Managing the theft and sabotage of information: An organizational case study on information security breaches and rick analysis," *IRACST - International Journal of Computer Science and Information Technology and Security*, pp. 154–159, 2014.

[3] F. H. Alqahtani, "Developing an information security policy: A case study approach," *Procedia Computer Science*, pp. 691–697, 2017.

[4] N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Computers & Security*, pp. 70–82, 2016.

[5] J. H. Yulia Cherdantseva, "A reference model of information assurance & security," *8th International Conference on Availability, Relaibility and Secu-*

rity (ARES) 2013, SecOnt workshop, pp. 546–555, 2013.

[6] R. V. S. Nader Sohrabi Safa, "An information security knowledge sharing model in organizations," *Computers in Human Behavior*, pp. 442–451, 2016.

[7] R. V. S. S. F. N. A. G. T. H. Nader Sohrabi Safa, Mehdi Sookhak, "Information security conscious care behaviour formation in organizations," *Computers & Security*, pp. 65–78, 2015.

[8] S. C. M. I. Bexhet Kamo, Besmir Zanaj, "Information security policy, design and implementation in a telecommunication company," *International Journal of Science, Innovation & New Technology*, pp. 1–7, 2012.