Viti i XV-të i Botimit, Nr.2
Dhjetor 2023

EDUKIMI NË SIGURINË KIBERNETIKE

Fatmir Basholli *, Joana Minga *

** Departamenti i Inxhinierive, Fakulteti i Shkencave të Aplikuara dhe Ekonomike,*

Albania University, Tiranë.

Përmbledhje

Në vitet e fundit, interneti është bërë një element integral i stilit të jetës së përditshme të njerëzve në mbarë botën. Kriminaliteti online, nga ana tjetër, është rritur së bashku me rritjen e aktivitetit në internet. Siguria kibernetike ka përparuar shumë vitet e fundit për të vazhduar me ndryshimet e shpejta që ndodhin në hapësirën kibernetike. Siguria kibernetike i referohet metodave që një vend ose organizatë mund ta përdorë atë për të mbrojtur produktet dhe informacionet në hapësirën kibernetike. Një dekadë më parë, termi "siguri kibernetike" nuk ishte i njohur nga publiku i gjerë ne Shqipëri. Tani siguria kibernetike nuk është vetëm një problem që prek individët, por gjithashtu vlen për një organizatë, biznes ose edhe një istitucion publik, arsimor, ku sulmet kibernetike po ngrenë shqetësime për privatësinë, sigurinë dhe financat. Gjithçka po dixhitalizohet së fundmi, duke përdorur një sërë teknologjish të tilla si cloud kompjuter, telefonat inteligjentë dhe Internetin e Gjërave. Siguria kibernetike është një grup teknologjish, procesesh dhe praktikash që synojnë parandalimin e sulmeve që synojnë, dëmtimin dhe aksesin e paligjshëm në rrjete, kompjuterë, programe dhe të dhëna. Qëllimi kryesor i këtij artikulli është edukimi në kryerjen e një ekzaminimi të plotë të llojeve të sigurisë kibernetike, në kornizën e sigurisë, mjetet e sigurisë dhe vështirësitë në sigurinë kibernetike duke ditur që siguria kibernetike mbron të dhënat dhe integritetin e aseteve informatike që janë pjesë ose të lidhura me rrjetin e një organizate, me qëllim në mbrojtjen e këtyre aseteve nga të gjithë aktorët kërcënues gjatë gjithë ciklit jetësor të një sulmi kibernetik.

Fjalët çelës: *Siguria Kibernetike, Sulmet Kibernetike, Krimi Kibernetik, Siguria e Rrjetit, Interneti i Gjërave Siguria (IoT), Kornizat e Sigurisë*

EDUCATION AND CYBER SECURITY

Abstract

In recent years, the Internet has become an integral element of the daily lifestyle of people around the world. Online crime, on the other hand, has increased along with the increase in Internet activity. Cyber security has advanced greatly in recent years to keep up with the rapid changes taking place in cyberspace. Cybersecurity refers to the methods a country or organization can use to protect products and information in cyberspace. A decade ago, the term "cyber security" was not known by the general public in Albania. Now cyber security is not only a problem that affects individuals, but also applies to an organization, business or even a public, educational institution, where cyber attacks are raising concerns about privacy, security and finances. Everything is being digitized recently, using a variety of technologies such as cloud

computing, smartphones and the Internet of Things. Cybersecurity is a set of technologies, processes and practices aimed at preventing attacks that target, damage and illegal access to networks, computers, programs and data. The main purpose of this article is to educate in conducting a thorough examination of the types of cyber security, the security framework, security tools and difficulties in cyber security knowing that cyber security protects data and the integrity of IT assets that are part or connected to an organization's network, with the aim of protecting these assets from all threat actors throughout the life cycle of a cyber attack.

Keywords: *Cyber Security, Cyber Attacks, Cyber Crime, Network Security, Internet of Things (IoT) Security, Security Frameworks*

Hyrje

Interneti është një nga shpikjet më të rëndësishme të shekullit që ka pasur një ndikim të rëndësishme në jetën tonë. Sot, interneti ka thyer të gjitha barrierat dhe ka transformuar mënyrën se si ne komunikojmë, luajmë, punojmë, bëjmë pazar, paguajmë faturat dhe përshëndesim miqtë në ditëlindjet dhe përvjetorët e tyre. Bota jonë po bëhet gjithnjë e më shumë e lidhur në rrjet me informacion të dixhitalizuar që mbështet shërbimet perfshi kujdesin shëndetësor dhe infrastrukturat kryesore. Istitucionet publike, private dhe gjithë përdoruesit janë të shqetësuar për kërcënimet ndaj konfidencialitetit, integritetit dhe disponueshmërisë së informacionit të dixhitalizuar. Në një botë dixhitale që po përshkon në mënyrë progresive çdo fushë të jetës sonë të përditshme, siguria është një domosdoshmëri. Në sferën e teknologjisë së informacionit, siguria kibernetike luan një rol kritik. Kur hasim në një mashtrim, siguria kibernetike është gjëja e parë që të vjen në mendje. Mbrojtja e të dhënave tona personale në internet është bërë një shqetësim i madh. Numri i pajisjeve të lidhura në rrjet është zgjeruar me një ritëm të shpejtë në vitet e fundit, duke tejkaluar në rreth 60 miliardë pajisje deri në fund vitin 2023, çka rezulton në një rritje të numrit të pajisjeve të cenueshme, ku "siguria ka të bëjë me të dhënat" dhe është jetike për të ardhmen e sistemeve dhe shërbimeve inteligjente të sigurisë kibernetike. Specialistet e kësaj teknologjie, analizojnë të dhënat e sigurisë në formën e skedarit, regjistrit, paketat e rrjetit dhe burime të tjera përkatëse dhe përpiqen të zbulojnë kërcënimet kibernetike nga sulmuesit.

Sot sulmuesit ose siç eshte bere zakon te quhen "Hakerat", mund të kenë akses të lehtë të paautorizuar në informacionin e përpunuar duke përdorur teknologjitë e të dhënave të mëdha nëse theksi përqëndrohet në arritjen e sigurisë efektive kibernetike në të dhëna. Hakerët po bëhen më të zgjuar dhe po vijnë me mënyra të reja duke krijuar softuer të dëmshëm për të abuzuar me të dhënat e individëve, bizneseve dhe ato shtetërore. Softuerët me qëllim të keq, phishing, sulme në fjalëkalim, shkarkime përmes hiperlidhjeve, sulme me viruse, etj. janë të gjithë shembuj që ofrohen në debatet publike për sigurine kibernetike [1,2,3]. Kur ndeshemi me krimin kibernetik, ne duhet të marrim parasysh edhe sigurinë kibernetike dhe duhet të synojmë që çdo profesionist të bashkëpunojë me të tjerët për të mbrojtur konfidencialitetin, integritetin dhe disponueshmërinë e informacionit ose të dhënave, të cilat të gjitha janë komponentë kritikë të sigurisë kibernetike, ku duhet pranuar se asnjë sistem ose mjedis nuk është plotësisht i sigurtë, pavarësisht nga procedurat e sigurisë, standardet, apo teknologjitë.

Përdorimi i inteligjencës artificiale si një zgjidhje alternative e sigurisë ka zbuluar se shfrytëzimi i aftësive parashikuese dhe mbrojtëse të inteligjencës artificiale dhe mësimit të makinerive do të minimizojnë ndërhyrjet në sisteme dhe do të rrisë ritmin me të cilin zbulohen dhe shmangen sulmet [4,5].

Siguria e TI përfshin sigurinë kibernetike si një nëngrup. Siguria kibernetike mbron të dhënat dixhitale në rrjetet tuaja, kompjuterë dhe pajisje nga aksesi, sulmi dhe shkatërrimi i paautorizuar, ndërsa siguria e TI-së i mbron të dyja, të dhënat fizike dhe dixhitale.

Ndërsa sulmet e sotme janë më të sofistikuara dhe synojnë për viktima specifike bazuar në qëllimin e sulmuesit, të tilla si përfitimi financiar, spiunazhi, detyrimi ose ndëshkimi ku sulmet oportuniste të pacaktuara janë ende të zakonshme, pasi hajdutët kibernetikë mund të kryejnë sulme nga kudo që ndodhen në planet.

Krimi kibernetik mund të shfaqet në formën e ngacmimit kibernetik dhe ngacmimit në internet, të cilat

quhen krime të aktivizuara kibernetike, ose nëpërmjet rreziqeve të sigurisë që prekin vetë kompjuterin, të tilla si infeksionet malware, infeksionet e ransomware dhe vjedhja e keqpërdorimi i të dhënave personale, të cilat quhen krime të varura kibernetike [6,7,8].

Materialet dhe metodat rreth sigurisë kibernetike

Kërkesa në rritje për sigurinë kompjuterike, si dhe tendencat e kibernetizimit (përdorimi i qëndrueshëm i internetit në hapësirën kibernetike në mbrojtje nga grupe terroriste, milici ose grupe të tjera të ngjashme të përfshira në konflikte që promovojnë dhe shpërndajnë kauzat e tyre), janë objektiva kryesore të shekullit të njëzet e një. Rritja e krimit kibernetik, prodhimi i monedhave dixhitale dhe qeverisja elektronike janë shoqëruar së fundi nga një rritje e investimeve në teknologjinë e re për siguri kompjuterike në mbarë botën. Termi "siguri kibernetike" i referohet qasjeve dhe procedurave për ruajtjen e informacionit dixhital, ku një sistem informacioni ruan, transmeton ose përdor të dhënat. Në fund të fundit, të dhënat janë çfarë kërkon një kriminel, rrjeti i telekomunikacionit, serverët dhe kompjuterët janë thjesht kanale për të dhëna. Kur siguria kibernetike është efektive ul rrezikun e sulmeve e ndërhyrjeve dhe mbron kompanitë dhe individët kundër përdorimit të paligjshëm të sistemit, rrjetit dhe teknologjisë.
Siguria kibernetike është një grup strategjish dhe procesesh për mbrojtjen e kompjuterëve, rrjeteve, bazave të të dhënave dhe aplikime kundër sulmeve, aksesit të paligjshëm, modifikimit ose shkatërrimit. Ajo gjithashtu mund të luajë një rol jetësor në zhvillimin e teknologjisë së informacionit dhe shërbimeve të internetit. Ekzistojnë tendenca të ndryshme në sigurinë kibernetike, ku më e spikatura prej të cilave është aplikacioni në internet. Aplikacionet në ueb tani janë një nga platformat më të përdorurat për ofrimin e informacionit dhe shërbimeve nëpërmjet internetit. Siguria kibernetike i referohet teknologjive, teknikat dhe procedurave që përdoren për të parandaluar që kompjuterët, programet, rrjetet dhe të dhënat të ekzistojnë të hakuar, dëmtuar ose aksesuar pa autorizim. Specialistët në sigurinë kibernetike janë duke u marrë gjithnjë e më shumë me një gamë të gjerë kërcënimesh kibernetike në kohë pothuajse reale. Aftësia për të zbuluar, analizuar dhe u mbrojtur kundër kërcënimeve të tilla në kushte afërsisht në kohë reale nuk është e mundur pa përdorimin e kërcënimit inteligjent, në të dhënat e mëdha dhe teknikat e mësimit të makinerive. Siguria kibernetike është praktikë e mbrojtjes së kompjuterave, serverave, pajisjeve celulare, sistemeve elektronike, rrjeteve dhe të dhënave nga sulmet me qëllim të keq e njohur gjithashtu edhe si siguria e teknologjisë së informacionit ose siguria elektronike e informacionit [9,10].

Rezultate nga historia në sigurinë kibernetike

Krimbat, viruset, kuajt e Trojës, spyware dhe malware përmenden në informacionin e zakonshëm të teknologjisë së informacionit që në gjuhën popullore shpesh njihet si (IT) që shumë vjet më parë, ku zhvillimi i viruseve ishte katalizatori për krijimin të sigurisë kibernetike. Kriminelët kibernetikë përdorin këtë nocion për të krijuar softuer vetëpërsëritje, të tillë si viruset. Në vitin 1969, profesori Leonard Kleinrock dhe studenti Charley Kline dërgoi komunikimin e parë elektronik nga kompjuteri dhe ky është një rrëfim i njohur dhe një moment historik kryesor në historinë e botës dixhitale.
Krimbi i parë kompjuterik u ndërtua në vitet 1970 nga Robert Thomas, një studiues për BBN Technologies në Kembrixh, Masaçusen. Kacavjerrës ishte emri i krijesës, "UNË JAM KATARI: MË KAPNI NËSE MUNDET", i cili sulmoi kompjuterët duke kërcyer nga sistemi në sistem. I pari Softuer antivirus u ndërtua nga Ray Tomlinson, shpikësi i postës elektronike, i cili krijoi një program përsëritës të quajtur "The Reaper", i cili do të gjurmonte viruset dhe do ti fshinte ato, por krimi kibernetik u rrit dhe u bë më i fuqishëm dhe jo vetem "Kacavjerrës" por më pas edhe korrës. Me përmirësimin e softuerit dhe harduerit kompjuterik, u përmirësuan edhe shkeljet e sigurisë, por hakerët vazhdimisht synojnë të zbulojnë një dobësi të re ose një mjet për të anashkaluar masat e sigurisë.
Rusët ishin të parët që përdorën fuqinë kibernetike si armë, në vitin 1986. Marcus Hess, një shtetas gjerman, fitoi akses në 400 sisteme ushtarake, duke përfshirë CPU-të e Pentagonit. Ai synonte t'i shiste sekrete KGB-së, por një Astronom amerikan, Clifford Stoll, e kapi atë përpara se kjo të ndodhte. Në vitin

1988, një burrë i quajtur Robert Morris kishte një ide që synonte të testonte madhësinë e internetit. Për ta bërë këtë, ai shkroi një program që shkoi përmes rrjeteve dhe pushtoi terminalet UNIX dhe kopjoi veten. Krimbi Morris ishte jashtëzakonisht agresiv, ngadalësoj sistemet deri në pikën ku ato ishin të papërdorshme. Ai më pas u bë personi i parë që u dënua sipas ligjit për mashtrim dhe abuzim kompjuterik.
Virusi Melissa u lëshua në fund të vitit 1999. Ky ishte një makro-virus që ishte krijuar posaçërisht për të infektuar llogaritë e postës elektronike. Virusi do të kishte akses në këto emaile me qëllimin e dërgimit të emaileve masive. Ky autor ishte një nga të parët që u shpall fajtor për krijimin e malware, ndaj tij iu dha një ndeshkim me mandat pesëvjeçar pasi u akuzua se ka shkaktuar nje dëm prej 80 milionë dollarësh.
Në 2013 dhe 2014, Yahoo ishte objektivi i një prej sulmeve të rënda kibernetike, ku llogaritë e Yahoo që i përkisnin gati 3 miliardë njerëzve u rrezikuan si rezultat i sulmeve. Sulmuesit gjithmonë kanë përfituar nga dobësitë që ende nuk ishin parashikuar e adresuar deri në atë kohë dhe për këtë hakerët instaluan malware në sistemet e Yahoo duke përdorur teknika spear phishing, duke u dhënë atyre akses të pakufizuar në prapavijë. Ata fituan akses në bazat e të dhënave rezervë të Yahoo dhe vodhën të dhëna të ndjeshme si emra, email, fjalëkalime dhe pyetje e përgjigje për rikuperimin e fjalëkalimit.
Viruset me kalimin e kohës u bënë më vdekjeprurëse, pushtuese, të vështira për t'u shmangur duke nxjerrë jashtë funksionit sisteme të konsiderushme telekomunikacioni. Ne jemi njohur tashmë me sulme të mëdha kibernetike që kanë prekur edhe vëndin tonë gjate vitit 2022 e në vazhdim. Këto janë vetëm disa shembuj, që tregojnë se siguria kibernetike është një domosdoshmëri si për institucionet publike, ndërmarrjet e mëdha, ashtu edhe për bizneset e vogla. Siç tregohet në afatin kohor të mësipërm, siguria kibernetike është një lojë e pafund si macja me miun. Sulmuesit po fitojnë talente të reja e po aplikojne metoda e teknika inovative me zhvillimin e internetit e nga ana tjetër mbrojtësit e sistemeve po reagojnë duke qëndruar një hap më pas.
Sipas projeksionit të Gartner Inc. [11], shpenzimet globale të sigurisë kibernetike do të arrinin në 133.7 miliardë dollarë në vitin 2022. Ndërsa sulmet kibernetike po bëhen më të sofistikuara, institucionet publike, private planifikojnë të investojnë më shumë në gjetjen e zgjidhjeve në parandalimin e shkeljes së të dhënave.

Diskutime

Pse siguria kibernetike është thelbësore.

Ne jetojmë në një epokë dixhitale, e cila pranon se të dhënat tona personale janë më të ndjeshme se kurrë. Nga infrastruktura e internetit, ne të gjithë jetojmë në një botë të lidhur (bashkuar) ku të dhënat ruhen në kompjuterë dhe pajisje të tjera. Një komponent i ketyre të dhënave mund të përmbajë informacione të ndjeshme, të tilla si pronësia intelektuale, të dhënat financiare, informacion personal ose lloje të tjera të dhënash, në të cilat aksesi i paligjshëm ose ekspozimi mund të rezultojë në efekte negative. Një nga vështirësitë më të rëndësishme me të cilën do të përballet njerëzimi ne dekadat e ardhshme janë aktivitetet kibernetike. Sulmet kibernetike janë krimi me rritje më të shpejtë në botë dhe ato po bëhen më të mëdha, më të sofistikuara dhe më të shtrenjta. Sipas Cyber Security Ventures, Humbjet nga krimi kibernetik do t'i kushtojnë globit 6 trilionë dollarë në vit, pra shumë më tepër se dëmi i shkaktuar nga katastrofa natyrore në një vit dhe shumë më fitimprurëse se tregtia globale e të gjitha narkotikëve të mëdhenj të paligjshëm.
Sipas Cisco-s, bizneset e Azi-Paqësorit përballen me gjashtë sulme kibernetike në minutë, ku jo vetëm qeveritë dhe korporatat janë në rrezik nga veprimet dhe synimet e hakerëve, por edhe individët janë më shumë të rrezikuar. Hakerat po vjedhin informacionin personal të një individi dhe e shesin atë për përfitim, i cili njihet edhe si vjedhja e identitetit.
Duke pranuar se askush nuk është i imunizuar ndaj kërcënimit që vjen nga krimi kibernetik, që nga individët e deri te ata më të mëdhenj si korporatat shumëkombëshe etj., mbrojtja është një hap kritik për të fituar luftën kundër këtij krimi të koheve që po jetojmë.
Edukimi nëpërmjet arsimimit është një komponent kritik ndaj çdo plani të krimit kibernetik dhe është thelbësore që të gjithë në organizata, nga drejtuesit (CEO) e deri tek stafi nëpunës, të jetë i vetëdijshëm për rreziqet që lidhen me përdorimin e rrjeteve të telekomunikacionit dhe aplikacioneve të ndryshme. Rinia jonë është një nga popullatat më të rëndësishme për tu edukuar për sigurinë kibernetike, se ndërsa mund të mos jenë në bankë ose të bëjnë blerje në internet me karta krediti, ata mund të bien shumë të lehtë preh për

kriminelët kibernetikë dhe tu lejojnë keqbëresve që të fitojnë akses në të dhënat e tyre nëpërmjet llogarive personale të pasigurta. Fjalëkalimet e dobëta dhe email të pahijshëm ose praktikat sociale të medias online e bëjnë shumë më të lehtë që të tjerët të hyjnë në llogarinë tuaj dhe të kenë akses në informacionin personal, ku askush nuk e dëshiron që të jetë përgjegjës për një krimin kibernetik. Për sa më sipër, siguria kibernetike është bërë një pjesë e rëndësishme e biznesit dhe fokusi tani është përqëndruar te zhvillimi i planeve të duhura të reagimit që minimizojnë dëmin në rast të një sulmi kibernetik [12].

Llojet e sigurisë kibernetike

Është thelbësore të kuptosh shumë lloje të sigurisë kibernetike në mënyrë që të mbrohemi më mirë. Procedurat të përdorura për të mbrojtur të dhënat nga vjedhja ose sulmi njihen si lloje të sigurisë kibernetike. Kompjuterat, pajisjet celular, rrjetet e telekomunikacionit, serverat dhe të dhënat mbrohen të gjitha nga kërcënimet e jashtme nga siguria kibernetike, shpesh e njohur si siguria elektronike e informacionit. Ajo vepron si një pengesë sigurie, duke siguruar që të dhënat tuaja dhe çfarë ju ruani në pajisjet tuaja te mos janë të cenueshme ndaj sulmeve të jashtme. Siguria e infrastrukturës kritike, siguria e rrjetit, siguria e aplikacioneve, siguria e informacionit, siguria në renë kompjuterike, parandalimi i humbjes së të dhënave deri tek përdoruesi përfundimtar fundor duhet te jene problem i edukimit dhe higjenes kibernetike. Sulmet kibernetike sipas vlerësimeve te eksperteve te fushes, pritet t'i kene kushtuar ekonomisë globale mbi 6-7 trilion dollarë deri në fund te vitit 2022 [13].

Siguria në renë kompjuterike

Për shkak të rritjes së anonimitetit, ruajtja e të dhënave me bazë cloud është bërë një alternativë e njohur gjatë dekadës se mëparshme. Edhe pse ruajtja në renë kompjuterike është më e sigurt, duhet ta mbroni atë me softuer që monitoron aktivitetin dhe mund t'ju njoftojë nëse ndodh ndonjë gjë e pazakontë me llogaritë tuaja cloud. Cloud ndihmon në reduktimin e rreziqeve që lidhen me sulmet në ambiente, eshte një teknologji e bazuar në softuer që mbron dhe monitoron të dhënat tuaja në re. Prandaj, edhe shërbimet e Uebit të Amazonit, Microsoft Azure dhe Google Cloud u paraqesin klientëve te tyre një platformë kompjuterike cloud, ku përdoruesit mund të ruajnë dhe monitorojnë të dhënat, duke zbatuar një mjet sigurie. Siguria e kompjuterit në renë kompjuterike është e ngjashme me qendrat tradicionale të të dhënave ku kostot e mbajtjes së objekteve të të dhënave të mëdha dhe rreziku i shkeljeve të sigurisë është minimal [14].

Siguria e Infrastrukturës Kritike

Infrastruktura është jetike. Për të siguruar sisteme me infrastrukturë jetike, përdoren teknika të sigurisë kibernetike. Sistemet në të cilat shoqëritë mbështeten shumë jane rrjetet e energjisë elektrike, pastrimi i ujit, semaforët, sistemi bankar, qendrat tregtare dhe spitalet. Ato nuk janë të lidhura drejtpërdrejt me një shkelje të mundshme kibernetike, por mund të shërbejnë si një platformë për malware kibernetikë për të infektuar pikat fundore me të cilat janë lidhur këto sisteme. Këto organizata duhet të kenë një plan emergjence që do t'i ndihmonte klientet dhe bizneset e tyre që të mos përballen të vetëm me sulmet kibernetike. Siguria dhe qëndrueshmëria e kësaj infrastrukture kritike është jetike për sigurinë dhe mirëqenien e shoqërisë sonë ku Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) ka përgjegjësinë "Për Sigurinë Kibernetike" në Shqipëri [15,22].

Parandalimi i humbjes së të dhënave

Parandalimi i humbjes së të dhënave, siguron që të dhënat e ndjeshme ose jetike të mos dërgohen përtej rrjetit të biznesit. Fjala i referohet softuerit që lejon një administrator rrjeti të menaxhojë të dhënat që përdoruesit mund të dërgojnë dhe marrin. Zhvillon politika dhe praktika për trajtimin dhe parandalimin e humbjes së të dhënave, si dhe plane rikuperimi në rastin e një shkeljeje të sigurisë kibernetike. Vendosja e lejeve dhe politikave të rrjetit për ruajtjen e të dhënave është pjesë nga kjo. Parandalimi i humbjes së të dhënave zgjidh tre objektiva kryesore që janë pika të zakonshme të "dhimbjes" për shumë organizatat: mbrojtja / pajtueshmëria e informacionit personal, mbrojtja e pronësisë intelektuale (IP) dhe dukshmëria e të dhënave.

Siguria e aplikacionit

Përdor softuerin dhe harduerin për tu mbrojtur kundër rreziqeve të jashtme që mund të lindin gjatë zhvillimit të një aplikacioni. Për shkak se aplikacionet janë gjithnjë e më të aksesueshme nëpër rrjete të shumta, ato janë më të prekshme ndaj sulmevet kibernetike. Aplikacionet mund të mbrohen me softuer antivirus kibernetik, mure zjarri dhe shërbimet e enkriptimit. Kompanitë dhe organizatat mund të zbulojnë grupe të ndjeshme të të dhënave dhe t'i sigurojnë ato me aplikacione të specializuara në lidhje me grupet e të dhënave duke përdorur një rrjet sigurie për aplikacionin. Siguria e aplikacionit mund të përfshijë harduer, softuer dhe procedura që identifikojnë ose minimizojnë dobësitë e sigurisë. Një ruter që parandalon çdokënd nga shikimi i adresës IP të një kompjuteri nga Interneti është një formë e sigurisë së aplikacioneve harduerike [16].

Siguria e informacionit

Kriptimi i të dhënave, i njohur shpesh si siguria e të dhënave, mbron të dhënat nga aksesi ose ndryshimi i padëshiruar gjatë kohës që janë duke u ruajtur ose dërguar nga një makinë në tjetrën. Të dhënat në çfarëdo forme janë të mbrojtura nga përdorimi i paautorizuar, zbulimi, fshirja ose lloje të tjera keqdashjesh nga siguria e informacionit, të njohura edhe si InfoSec. Mantaps, menaxhimi i çelësave të enkriptimit, sistemet e zbulimit të ndërhyrjeve në rrjet, rregullat e fjalëkalimit dhe pajtueshmëria rregullatore janë shembuj të këtyre procedurave. Informacioni mund të jetë çdo gjë nga të dhënat tuaja personale në profilin tuaj të mediave sociale, të dhënat e telefonit celular, biometrikën, etj. Kështu, Siguria e Informacionit përfshin shumë fusha kërkimore si kriptografia, kompjuteri, celulari, analiza ligjore kibernetike, media sociale në internet etj.

Gjatë Luftës së Parë Botërore, sistemi i klasifikimit me shumë nivele u krijua duke pasur parasysh ndjeshmërinë e informacionit. Me shpërthimin e Luftës së Dytë Botërore, sistemi i klasifikimit u harmonizua zyrtarisht. Alan Turing ishte ai që deshifroi me sukses Machine Enigma e cila u përdor nga gjermanët për të koduar të dhëna per luftën. Programet e Sigurisë së Informacionit ndërtohen rreth tre objektivave, të njohur zakonisht si CIA Konfidencialiteti, Integriteti dhe Disponueshmëria.

Siguria e rrjetit

Ndërsa siguria kibernetike ka të bëjë me rreziqet nga jashtë, siguria e rrjetit mbron rrjetin tuaj të brendshmen nga ndërhyrja keqdashëse. Siguria e rrjetit të brendshëm ruan sigurinë e rrjeteve të brëndshme që nga ruajtja fizike e infrastrukturës dhe kufizimin e aksesit në të. Aktivitetet e përdoruesve gjithashtu regjistrohen sepse shumë nga faqet e internetit përdorin cookie të palëve të treta. Kjo mund të jetë e dobishme për bizneset në drejtim të zgjerimit të tyre operacional, por gjithashtu i ekspozon klientët ndaj mashtrimit dhe shfrytëzimit. Si rezultat, ndërmarrjet duhet të zbatojë një program sigurie për të monitoruar rrjetin e brendshëm dhe infrastrukturën për të parandaluar sulmet kibernetike dhe viruse të lidhura me rrjetin. Teknologjia e mësimit të makinerisë, sipas ekspertëve, mund përdoret për të informuar autoritetet në rast trafiku të pazakontë. Organizatat duhet të vazhdojnë të përmirësojnë punën e tyre sigurinë e rrjetit duke miratuar politika që mund t'i mbrojnë ata nga sulmet kibernetike. Ekipet e sigurisë janë tani duke përdorur mësimin e makinerive për të nxjerrë në pah trafikun e gabuar dhe për tu alarmuar nga rreziqet në kohë reale, gjë që i ndihmon ata te menaxhojne më mirë monitorimin e sigurisë së rrjetit. Administratorët e rrjetit po vazhdojnë të zbatojnë politika dhe procedurat për të mbrojtur rrjetin nga aksesi, modifikimi dhe shfrytëzimi i padëshiruar. Zbatimi i vërtetimit me dy faktorë (2FA) dhe krijimi i fjalëkalimeve të freskëta dhe të forta janë dy shembuj të sigurisë së rrjetit. Një shëmbull i mirë në ketë drejtim (2FA) janë bankat e nivelit të dytë që operojnë në vëndin tonë.

Edukimi i përdoruesit fundor

Duhet te pranojme se zgjidhjet e sigurisë kibernetike janë po aq të forta sa lidhjet e tyre më të dobëta, në të cilat janë njerëzit që i përdorin ato. Edukimi i përdoruesit fundor përfshin udhëzimin e përdoruesve për praktikat më të mira të tilla si mos klikimi në lidhje të papritura ose hapja e bashkëngjitjeve të çuditshme në email, ku të dyja menyrat mund të çojnë në përhapjen e malwareve dhe programeve të tjera

të rrezikshme. Mësimi i përdoruesve që të mos lidhin disqet USB të paidentifikuar dhe të tjera mënyra të ndryshme janë mësimet jetike e të rëndësishme për sigurinë e çdo organizate.

Siguria e Internetit të Gjërave (IoT).

Interneti i Gjërave mendohet të jetë mjeti i ardhshëm i revolucionit teknologjik. Sipas një parashikimi të eksperteve financiare, tregu IoT parashikohet të rritet me rreth 520 miliardë dollarë deri në vitin 2022. IoT i ofron përdoruesit një shumëllojshmëri të pajisjeve të rëndësishme dhe jo kritike, të tilla si pajisjet, sensorët, printerët, ruterat Wi-Fi, e ndër ruterë të tjerë përmes rrjetit të tij të sigurt [17,18]. Sipas Cytelligence, hakerat sulmuan shtëpitë inteligjente dhe pajisjet e internetit të gjërave (IoT) si televizorët inteligjentë, asistentët e zërit, monitorët per shikimin e bebeve dhe telefonat celular më shpesh në vitin 2019 dhe periudhës së pandemisë globale. Hakerët që marrin akses në kredencialet Wi-Fi të një shtëpie mundet gjithashtu të fitojne akses në informacionin personal të përdoruesve, të tilla si të dhënat mjekësore, deklaratat bankare dhe informacion mbi hyrjen në uebfaqe. Sipas sondazhit, një nga barrierat më të rëndësishme për vendosjen e IoT në çdo firmë paraqet rrezik sigurie, aktualisht organizatat po marrin analitikë të hollësishme për sisteme të ngulitura për një rrjet të sigurtë duke integruar sistemin me sigurinë IoT [19].

Siguria e pikës fundore

Shumica e shkeljeve të sigurisë në të kaluarën dhe sot po ndodhin përmes rrjetit. Nga ana tjetër, rreziqet e sotme, po drejtohen gjithnjë e më shumë nëpër pikat fundore, duke nënkuptuar se mbrojtja e rrjetit të centralizuar është të pamjaftueshme. Zhvendosja e perimetrave të sigurisë që nuk janë të përcaktuara qartë kërkojnë shtimin e niveleve të reja të sigurinë nëpërmjet mbrojtjes së pikës fundore. Për të shmangur rreziqet që mund të vijnë nga përdorimi i pajisjeve në distancë, siguria duhet të mbajë kontroll më të mirë mbi pikat e hyrjes [20,21]. Kjo u mundëson bizneseve të mbrojnë serverët e tyre, stacionet e punës dhe pajisjet celulare nga sulmet kibernetike si në nivel lokal ashtu edhe në distancë. Ndërlidhja e pajisjeve në një rrjet krijojnë pika aksesi për kërcënimet dhe dobësitë. Duke ndaluar përpjekjet për të hyrë ne këto pika hyrëse, siguria e pikës fundore mbron në mënyrë efektive rrjetin. Monitorimi i integritetit të skedarit, antivirusi dhe programet kundër malware etj., janë teknikat kryesore të përdorura.

Siguria e faqes në internet

Kjo përdoret për të parandaluar dhe mbrojtur faqet e internetit nga kërcënimet e sigurisë kibernetike në internet. Siguria e faqes në internet nënkupton që të mbulojë bazën e të dhënave, aplikacionet, kodet burimore dhe skedarët e faqes në internet. Në vitet e fundit, incidenca e shkeljeve të të dhënave në faqet e internetit është rritur në mënyrë të vazhdueshme, duke rezultuar në vjedhje identiteti, kohë joproduktive, humbjet financiare, reputacionin dhe dëmtimin e imazhit të Istitucionit (biznesit), e kështu me radhë. Arsyeja kryesore për këtë është se shumë pronarë të faqeve të internetit besojnë se faqja e tyre mbrohet nga ofruesi i tyre që mirëmban faqen në internet, rrjedhimisht duke i lënë ata të prekshëm nga sulmeve kibernetike.

Disa nga teknikat dhe mjetet e rëndësishme të përdorura për sigurinë e faqes në internet janë skanimi i vazhdueshëm i faqes në internet dhe heqja e malware, vendosja e mureve të zjarrit në aplikacione dhe testimi i sigurisë së aplikacionit, etj.

Siguria e të dhënave të mëdha

Sulme malware dhe ransomware, pajisje të korruptuara dhe të cenueshme dhe programe të brendshme të rrezikshme janë të gjithë shembuj të rreziqeve në sigurisë kibernetike që mund të zbulohen duke përdorur teknologjitë e analitikës së të dhënave të mëdha [22,23].

Analitika e të dhënave të mëdha duket se ka premtimin më të madh në drejtim të rritjes së sigurisë kibernetike në këtë fushë. Softueri i madh i analitikës së të dhënave mund t'ju ndihmojë në parashikimin e llojit dhe ashpërsisë së rreziqeve të sigurisë kibernetike. Duke aksesuar burimet dhe tendencat e të dhënave, ne mund të vlerësojmë kompleksitetin e një sulmi të mundshëm [24,25]. Këto mjete gjithashtu

ju mundësojnë të analizoni të dhënat aktuale dhe historike për të përcaktuar se cilat tendenca janë të pranueshme dhe cilat jo.
Ekspertët mund të përdorin analitikë inteligjente të të dhënave të mëdha [26,27] për të krijuar një model parashikues që mund të dërgojë një alarm sapo të zbulojë një pikë hyrëse që sulmon sistemin.

Siguria në Blockchain

Blockchain prezantohet si një libër i shpërndarë, duke iu referuar mënyrës se si një bazë të dhënash ndahet midis shumë pjesëmarrësve në një rrjet peer-to-peer pa përfshirjen e një autoriteti qëndror. Përdorimi i teknikave të Blockchain në rrjetet e shpërndarjes së përmbajtjes na mundëson të besojmë se këto rrjete janë fantastike dhe një shëmbull ilustrues se si ne mund të përdorim Blockchain për t'i shtuar vlerë proceseve ose teknologjisë ekzistuese të sigurisë së informacionit [28,29,30,31].
Rrjeti i shpërndarjes së përmbajtjes është një rrjet kompjuterash që janë të lidhura dhe përmbajnë versione të ndryshme të të njëjtit material. Qëllimi i dizajnit të tij është të optimizojë gjerësinë e një brezi të disponueshëm në një shërbim për të rritur disponueshmërinë dhe aksesin në të dhëna aq sa të mundshme. Së fundmi janë kryer disa sulme kundër platformave të mediave sociale si Twitter dhe Facebook, ku miliona llogari u cënuan si rezultat i këtyre sulmeve dhe informacioni i përdoruesit ra në duar të gabuara. Nëse teknologjitë Blockchain vendosen siç duhet në këto sisteme mesazhesh mund të shmangen sulmet kibernetike. Të dhënat e ndjeshme mund të mbrohen duke përdorur Blockchain duke siguruar një lloj të decentralizuar të ruajtjes së të dhënave. Hakerët do ta kishin më të vështirë, pse jo të pamundur, të shfrytëzonin të dhënat në sistemet e ruajtjes duke përdorur këtë strategji mbrojtese. Shumë kompani të shërbimit të ruajtjes po vlerësojnë mënyrat Blockchain që mundësojnë mbrojtjen e të dhënave nga hakerat [32,33,34,35,36].

Konkluzione

Me përparimin e shpejtë të teknologjisë, jeta jonë po dixhitalizohet gjithnjë e më shumë. Njerëzit tani jetojnë në një botë kibernetike ku të gjitha të dhënat dhe informacionet ruhen në mënyrë dixhitale dhe online. Qoftë biznesi në teresi, ofrimi i sherbimeve nëpërmjet platformës e-albania, blerejet elektronike, shërbimi në banka dhe gjithçka tani praktikisht mundësohet online. Fokusi në sigurinë kibernetike është më i shtuar në përpjekje për të karakterizuar problemin dhe për të përcaktuar nivelin e vërtetë të kërcënimit. Të gjithë individët, profesionistët, janë të shqetësuar për sigurinë kibernetike, njëkohësisht ligjvënësit aktualisht janë në diskutimin për përmirësimin e ligjit egzistues dhe përafrimin e tij me atë europian që pritet ta kemi së shpejti.
Siguria kibernetike është kritike për avancimin e teknologjisë së informacionit dhe shërbimeve të internetit në kushtet kur sulmet kibernetike do të jetë në rritje nga viti ne vit e ku janë aktivizuar jo vetëm hakerët e vetmuar por edhe aktorë të organizuar shtetërore përafërsisht si reparte ushtarake që kërkojnë të vjedhin të dhëna dhe të paralizojnë shërbimet për qytetarët dhe istitucionet publike.
Hapësira kibernetike nuk ka kufij, hapësira kibernetike e një kombi është një komponent i hapësirës kibernetike globale dhe nuk mund të izolohet dhe të përcaktojmë kufijtë e saj. Nuk ka qenë kurrë e lehtë të ruash sigurinë kibernetike, sepse edhe sulmet po bëhen më inovative çdo ditë. Siguria kibernetike është një teknologji që është krijuar dhe po modernizohet për të mbrojtur sistemet e informacionit.

Referenca

1. Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, "A Perusal of Big Data Classification and Hadoop Technology", International Transaction of Electrical and Computer Engineers System (ITECES), USA, Volume 4, No. 1, Pages 26-38, 2017 , DOI: 10.12691/iteces-4-1-4

2. Basholli, F.,Mema, B.,& Basholli, A. (2024). Training of information technology personnel through simulations for protection against cyber-attacks. Engineering Applications, 3(1), 45-58

3. Basholli, F.,Hyka,D., Basholli, A.,Daberdini,A.,& Mema,B.(2023). Analysis of cyber-attacks through simulation. Advanced Engineering Days, 7, 120-122

4. B. M. Thuraisingham, "Can AI be for Good in the Midst of Security Attacks and Privacy Violations?", Proceedings ACM CODASPY, 2020

5. Basholli, F.,Daberdini, A.,& Basholli, A. (2023). Possibility of protection against unauthorized interference in telecommunication systems. Engineering Applications, 2(3), 265-278

6. Hernandez-Suarez, At al.., Social sentiment sensor in Twitter for predicting cyber-attacks using ℓ1regularization. Sensors, 18(5), 1380, 2018

7. Basholli, F.,Daberdini, A.,& Basholli, A. (2023).Detection and prevention of intrusions into computer systems. Advanced Engineering Days, 6, 138-141

8. Basholli, F.,Mezini, R.,& Basholli, A. (2023). Security in the components of information systems. Advanced Engineering Days, 7, 185-187

9. Daberdini, A.,Basholli, F., Metaj, N.& Skenderaj, E. (2022). Cyber security in mail with Forti web and Fortinet for companies and institutions.5thAdvanced Engineering Days, 81-83

10. Basholli, A., Mema, B., Basholli, F., Hyka, D., & Salillari, D. (2023). The role of education in cyber hygiene. Advanced engineering Days, 7, 178-181

11. Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "A Close-Up View About Spark in Big Data Jurisdiction", International Journal of Engineering Research and Application (IJERA), Volume 8, Issue 1, (Part -I1), Pages 26-41, January 2018, DOI: 10.9790/9622-0801022641

12. C.M. Williams, R. Chaturvedi and K. Chakravarthy, "Cybersecurity Risks in a Pandemic", Journal of Medical Internet Res., vol. 22, no. 9, pp. 23692, 2020

13. M. Schwenk Jensen, J. Gruschka and N. Iacono, "On technical security issues in Cloud", IEEE International Conference on Cloud Computing, pp. 109-16, 2009

14. Yuya Jeremy Ong, Mu Qiao, Ramani Routray and Roger Raphael, "Context-Aware Data Loss Prevention for Cloud Storage Services", 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), 2017

15. X. Jin, W. Sun, Y. Liang, J. Guo and Z. Xie, "Design and implementation of intranet safety monitoring platform for Power secondary system", Automation of Electric Power System, pp. 99-104, Aug. 2011

16. Yusuf Perwej, Kashiful Haq, Firoj Parwej, M. M. Mohamed Hassan ," The Internet of Things (IoT) and its Application Domains", International Journal of Computer Applications (IJCA) ,USA , ISSN 0975 – 8887, Volume 182, No.49, Pages 36- 49, April 2019,DOI: 10.5120/ijca2019918763

17. Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "An Empirical Analysis of Web of Things (WoT)",

International Journal of Advanced Research in Computer Science (IJARCS), Volume 10, No. 3, Pages 32-40, 2019, DOI: 10.26483/ijarcs.v10i3.6434

18. Basholli, F., & Daberdini, A. (2023). Monitoring and assessment of the quality of electricity in a building. Engineering Applications, 2(1), 32-48

19. S. Kowtha, L. A. Nolan and R. A. Daley, "Cyber security operations center characterization model and analysis", Proc. IEEE Conf. Technol. Homeland Secur. (HST), pp. 470-475, Nov. 2012

20. Pajaziti, A.,Basholli, F.,& Zhaveli, Y. (2023). Identification and classification of fruits through robotic systemby using artificial intelligence. Engineering Applications, 2(2), 154-163

21. Yusuf Perwej, "The Ambient Scrutinize of Scheduling Algorithms in Big Data Territory",International Journal of Advanced Research (IJAR), ISSN 2320-5407, Volume 6,Issue 3, Pages 241-258, March 2018, DOI: 10.21474/IJAR01/6672

22. Basholli, F., (2022). Cyber warfare, a new aspect of modern warfare. VI International Scientific Conference on Security „CONFSEC 2022", 52-54, www.researchgate.net

23. F. Pasqualetti, F. Dorfler and F. Bullo, "Attack detection and identification in cyber-physical systems", IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013

24. Yusuf Perwej, Bedine Kerim, Mohmed Sirelkhtem Adrees, Osama E. Sheta, "An Empirical Exploration of the Yarn in Big Data", International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868, Foundation of Computer Science FCS, New York, USA, Volume 12, No.9,Pages 19-29, December 2017, DOI: 10.5120/ijais2017451730

25. Yusuf Perwej, Nikhat Akhtar, Firoj Parwej, "A Technological Perspective of Blockchain Security",International Journal of Recent Scientific Research (IJRSR), ISSN: 0976-3031, Volume 9, Issue 11,(A), Pages 29472 – 29493, November 2018, DOI: 10.24327/ijrsr.2018.0911.2869

26. Asif Perwej, Dr. Kashiful Haq, Dr. Yusuf Perwej, "Blockchain and its Influence on Market",International Journal of Computer Science Trends and Technology (IJCST), ISSN 2347 – 8578,Volume 7, Issue 5, Pages 82- 91, Sep – Oct 2019, DOI: 10.33144/23478578/IJCST-V7I5P10

27. Mema, B., & Basholli, F. (2023). Internet of Things in the development of future businesses in Albania. Advanced Engineering Science, 3, 196-205

28. Basholli, F., & Daberdini, A. (2022). Monitoring and evaluation of the quality of electricity in a building.5thAdvanced Engineering Days, 77-80

29. Hyka,D., Hyra,A.,Basholli,F.,Mema,B.,& Basholli,A.(2023). Data Security in Public and Private Administration: Challenges, Trends, and Effective Protection in the Era of Digitalization. Advanced Engineering Days, 7, 125-127

30. Mema, B.,Basholli, F.,& Hyka, D. (2023). ChatGPT in Albanian higher education: Transformation of learning and virtual interaction. Advanced Engineering Days, 8, 23-27

31. Harizaj, M.,Bisha, I., & Basholli, F. (2023). IoT integration in electric car chargers' Infrastructure. Advanced Engineering Days, 6, 152-155

32. Basholli, F.,Minga, J.,& Grepcka, A. (2024). Protection of buildings on a university campus from lightning strikes. Advanced Engineering Days, 8, 35-38

33. Yusuf Perwej, "A Pervasive Review of Blockchain Technology and Its Potential Applications", Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA, Volume 5, No. 4, Pages 30 - 43, October, 2018

34. Basholli, F.,Mema, B.,Hyka, D., Basholli, A.,& Daberdini, A. (2023). Analysis of security challenges in SCADA systems, a technical review on automated real-time systems. Advanced Engineering Days, 8, 18-22

35. Basholli, F.(2022). Electronic interference and protection from it.5thAdvanced Engineering Days, 74-76

36. Hyka, D., & Basholli, F. (2023). How secure is our medical data? Is Albania ready for the digitalization of the health care system?. Engineering Applications, 2(3), 235-242