NDËRGJEGJËSIMI PËR KRIJIMIN E SISTEMEVE LEHTËSISHT TË REKUPERUESHËM NDAJ SULMEVE KOMPJUTERIKE

BOJAXHIU A.[1], DHIMO G.[2], DHËMBI A.[3]

[1,3]Universiteti i Tiranës, Fakulteti i Shkencave të Natyrës, Departamenti i Informatikës

[2]Universiteti i Gjøvik, Departamenti i Sigurisë së Informacionit, Norvegji

e-mail: areti.bojaxhiu@fshn.edu.al

Përmbledhje

Siguria absolute nuk ekziston. Skandali i fundit i NSA (National Security Agency), sulmi në LinkedIn dhe shumë sulme të tjera e provojnë këtë. Organizata ka nevojë për përgjigje të shpejtë për situata që cënojnë sigurinë dhe mënyra e vetme për të bërë këtë është që të implementoj sisteme elastike. Nëse ndodh një incident duhet të merren masa për të zbutur rrezikun, minimizuar dëmin dhe pas ndryshimeve duhet të bëhen analiza mbrojtëse për të shmangur sulmin në të ardhmen. Azhornimi me të rejat e teknologjisë është një domosdoshmëri për një organizatë të suksesshme dhe implementimi i teknologjive të reja, që kanë mbrojtje ndaj rreziqeve të reja bëjnë, që kjo organizatë të jetë në dijeni për këto tipe sulmesh. Krijimi i sistemeve lehtësisht të rekuperueshëm është e vetmja mënyrë për t'u mbrojtur nga e panjohura.

Abstract

Absolute security does not exist. The recent NSA (National Security Agency) scandal, the recent attack on LinkedIn and many others prove this. The organization needs quick and fast responses to such situations and the only way to do this is to build resilient systems. When an incidents occurs measures must be taken to mitigate the threat, minimize the damage and after careful analysis change and update defenses to avoid it in the future. Keeping up with technology development is a must for a successful organization, and as new technology are implemented new risks come along of which the organization is unaware. Resilience is the only way to be protected from the unknown.

Fjalëkyçe: Sisteme të rekuperueshëm, elasticitet, siguria, sulme, incidente, rreziqe.

Hyrje

Elasticiteti është përcaktuar si:

-aftësia e një sistemi për të rimarrë formë pas deformimit të shkaktuar nga sulme të jashtme,

-aftësia për t'u përshtatur lehtësisht të ndaj ndryshimeve, (George *et.al.*,2014).

Në lidhje me elasticitetin e organizatës kuptojmë aftësinë për të përgatitur dhe për t'iu përgjigjur kërcënimeve të cilat rrezikojnë aftësinë e tij për të ofruar shërbim të besueshëm dhe më e rëndësishmja për t'iu përgjigjur kërcënimeve, të cilat pengojnë ofrimin e shërbimeve. Në këtë mënyrë, kur sulmi ndodh në sistemet organizative, operatorët e dinë se si dhe kur duhet të

reagojë në mënyrë që të minimizojnë rrezikun dhe të vazhdojnë të ofrojnë shërbime. Për të arritur qëndrueshmërinë duhet të bëhen analiza shumë të detajuara ndaj rreziqeve. Ka shumë rreziqe që nuk mund të shmangen, ose që kanë një mundësi shumë të lartë të ndodhin, si sulmet DDOS (distributed denial-of-service) mbi koorporatat, rrjedhjet e brendëshme të informacionit ose raste të ngjashme me këto. Për këto lloj rreziqesh, organizata duhet të zbatoj masat e duhura për të ulur ndikimin e tyre.

Kur një organizatë është shumë e varur nga sistemet e IT dhe teknologjisë për të ofruar sistemet e saj kryesore, atëherë konceptet e vazhdimësinë dhe rikthimit të sistemit duhet të përfshihen në planin e organizatës. Këto dy koncepte së bashku me trajtimin e incidentit dhe të mësuarit të incidentit janë aftësitë kryesore për të krijuar një organizatë elastike. Një organizatë që mund të rikthehet në gjendje pune nga sulmet, e cila mund të siguroj vazhdimësinë e shërbimeve bazë, pasi ka dëme të konsiderueshme dhe mund të shmang këto sulme në të ardhmen quhet organizatë elastike. Subjekti i tillë mund të ketë disa dëme, kur një kërcënim është materializuar, por dëmi do të zbutet, shërbimet bazë do të vazhdojë të punojnë dhe i njëjti gabim nuk do të përsëritet në të ardhmen, duke mbrojtur reputacionin e organizatës dhe të ndërtimit të besimit, i cili është një aset i paçmuar.

Metodologjia dhe rezultate

Studimi bazohet në disa prej eksperiencave më të mira botërore në lidhje me implementimin e metodave për të siguruar elasticitet në fushën e sigurisë së organizatave. Në vijim kemi paraqitur këto studime.

1. Analiza Kosto-Përfitim

Elasticiteti është i kushtueshëm. Ai përfshin vazhdimësinë e biznesit, e cila ndonjëherë është arritur me të dhënat e qëndrave paralele (zgjidhje e kushtueshme), të cilat janë klon i një sistemi primar dhe janë të vendosura larg fizikisht. Një sistem elastik ka nevojë për plane të rimëkëmbjes për burimet, të cilat mund të përfshijnë sisteme të kushtueshme rezervë të të dhënave kritike të biznesit, mjedis të mbrojtur për këto rezerva dhe më shumë. Gjithashtu, mirëmbajtje e një ekipi të reagimit të shpejt ndaj sulmeve (CERT) nuk është lirë. Ajo kërkon trajnimin dhe menaxhimin e stafit, së bashku me mjete të shtrenjta që ekipi ka nevojë të jetë operativ. Një tjetër teknikë e kushtueshme për të përmirësuar elasticitetin është teprica. Shërbime kritike të biznesit nuk duhet të ketë një pikë të vetme të dështimit dhe kanë nevojë për tepricë. Kjo është arsyeja pse ndërtimi i një organizate elastike duhet të jepet në analizën kosto-përfitim të këtyre faktorëve. Hapi i parë në këtë proces është një proces i kujdesshëm i analizës së riskut. Ka shumë metodologji për të identifikuar dhe kategorizuar rreziqet. Për shembull, një prej tyre është OCTAVE Allegro. Ajo merr parasysh çdo informacion të organizatës, përcaktojnë prioritetet e tyre dhe merr në konsideratë rreziqet e tyre dhe se si mund të zvogëlohen ato. Ky është një cikël që mund të imagjinohet si në skemën më poshtë:

Figurë 1. Cikët rreziqesh

2. Modelimi dhe analiza e elasticitetit (RMA)

Mikrosofti ka zhvilluar një metodologji për modelin e elasticitetit dhe analizave për shërbimin cloud, (Microsoft Corporation *et.al*.,2014). Sot pjesa më e madhe e organizatave kanë/ose janë në proces të emigrojnë në shërbimin cloud. Mirëpo shërbimet janë të ekspozuara ndaj rreziqeve dhe dështimet në këtë rast, janë mjaft të zakonshme (Microsoft Corporation *et.al*.,2014).

Kjo është arsyeja pse rikthimi i gjendjes fillestare është bërë një çështje shumë e rëndësishme. Burimi i dështimit mund të ndryshoj statusin nga status i zakonshëm në status i rrallë dhe dëmi nga i vogël në dëm i madhë. Më poshtë janë disa nga burimet e dështimeve, (Microsoft Corporation *et.al*.,2014).

Figurë 2. Dështimet

Dështimet janë të pashmangshme dhe do të ndodhë që organizata duhet të përqëndrohet në identifikimin e tyre sa më shpejtë të jetë e mundur dhe të zhvillojnë masa për të minimizuar shtrirjen në kohë dhe efektin mbi konsumatorët.

Përfitimet e metodologjisë RMA mund të kategorizohen si më poshtë:

Çështje sigurie në dizenjim, (Microsoft Corporation *et.al*.,2014).

Identifikimi i boshllëqeve në elasticitetin e sistemeve para zbatimit të tyre ose edhe para kodimit të tyre dhe hartimin e sistemit në mënyrë, që të jetë në gjendje për të zbuluar dhe për të zbutur dështimet. Kjo do të thjeshtojë punë më vonë, kur sistemi është në mjedisin e prodhimit, për t'u zbatuar masat kundër-dështimit.

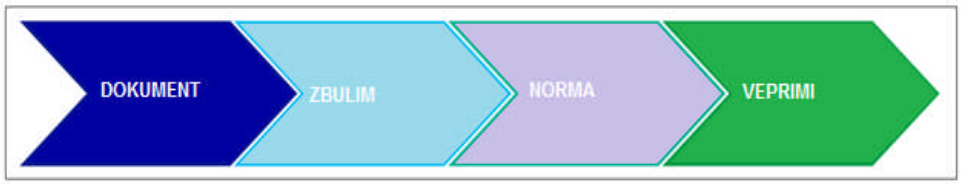
Prioriteti siguri-lidhje, (Microsoft Corporation *et.al*.,2014).

Qëllimi i RMA është që të përgatisë një listë të dështimeve për çdo shërbim, të cilat janë mjaft të zakonshme. Kjo do të thotë se duke u fokusuar në këto dështime, duhet të kemi prioritet mbi parandalimin. Ajo është shumë më e besueshme për t'u fokusuar në rikthimin duke qënë se shërbimet mund të jetë shumë komplekse që përfshijnë shumë faktorë dhe komponente të palës së tretë. Parandalimin e të gjitha shkaqeve të mundshme që mund të çojë në një dështim është e pamundur.

Sigurimi i rezultateve të prekshme në lidhje me besueshmërinë,(Microsoft Corporation *et.al*.,2014)

Duke përdorur mjetet dhe metodat e RMA ekipi merr një kuptim më të mirë për sistemin dhe si komponentet janë të lidhura me njëra-tjetrën. Duke patur varësitë ekipi mund të identifikojë pikat ku sistemit mund të jetë sulmuar.

Procesi RMA ka katër faza që mund të shihen në skemën e mëposhtme:



Figurë 3. Fazat e RMA

2.1. Dokumenti

Në fazën e parë të Dokumentit ekipi duhet të krijojë një diagram me të gjitha burimet, varësitë dhe ndërveprimit të komponentëve, (Microsoft Corporation *et.al.*,2014). Kjo është pjesa më e rëndësishme në identifikimin e çdo entiteti të këtyre subjekteve dhe krijimin e një diagrame të lehtë për të kuptuar, kjo është kritike në suksesin dhe përdorshmërinë e RMA. Kjo është detyra e parë e fazës së dokumentimit. E dyta është për transferimin e tyre në manual RMA.

Disa këshilla që janë të rëndësishme gjatë detyrës së parë janë:

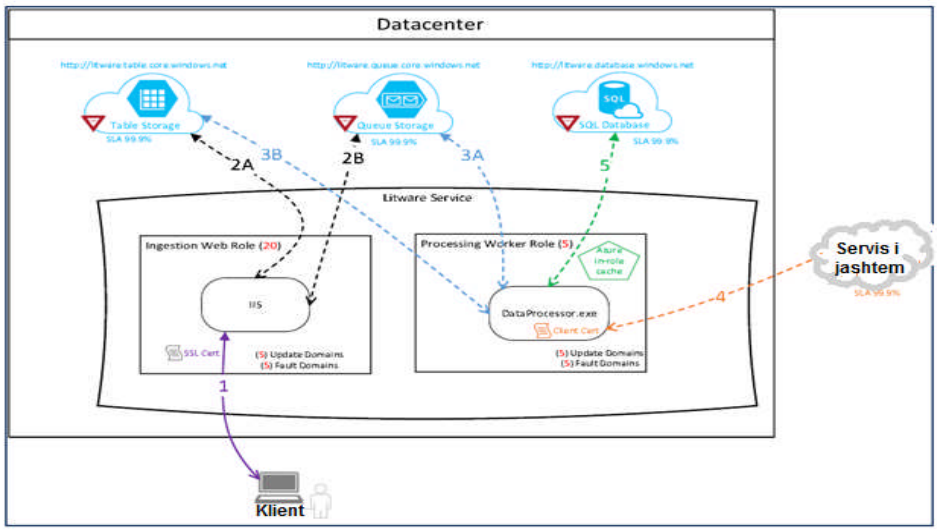
Mos përfshi hardware fizike, (Microsoft Corporation *et.al*.,2014).

Hardware është një burim i dështimeve në mjedisin cloud. Rolet në server dhe instancat e secilit server janë më të rëndësishme. Gabime fizike janë dhe do të jenë burimi i dështimeve; por nuk është produktive për të vendosur komponente hardware si rutera, kartat e rrjetit, përpunuesve dhe disqeve të ilustruara në figurën 4. Numërimi i rasteve është i rëndësishëm, (Microsoft Corporation *et.al*.,2014)

Çdo rast i një njësie funksionale duhet të vihet në diagram, çdo rol në server së bashku me vendndodhjen e tyre gjeografike duhet të shtohet. Në këtë mënyrë bëhet një analizë më e mirë se si dështimi i një komponenti mund të ndikojë te një klient. Gjithashtu ajo është e lehtë për të implementuar tepricë, e cila është një nga teknikat kryesore për të arritur elasticitetin. Përfshi të gjitha varësitë, (Microsoft Corporation *et.al*.,2014).

Sistemet cloud kanë shumë varësi dhe shumë prej tyre përfundojë jashtë. Ata nuk janë në pronësi të ekipit cloud dhe janë kritike për shërbimin. Secila prej këtyre varësive duhet të jetë në diagram.

Më poshtë është një diagram e thjeshtë varësie:



Figurë 4. Diagram kompotentesh (CID)

Në detyrën e dytë të fazës së dokumentit, diagrama duhet të përkthehet në një manual RMA, i cili është një listë ndërveprimi që do të përdoret gjatë fazës së ardhshme, që do të identifikojë llojet e mundshme të dështimit në çdo ndërveprim, (Microsoft Corporation *et.al.*,2014). Për më shumë rreth manualit mund të shikoni në figurën, (Microsoft Corporation *et.al.*,2014).

2.2. Zbulimi

Faza e zbulimit kryhet përmes idesë ku të gjitha disiplinat duhet të marrin pjesë dhe të jenë aktive. Qëllimi është të identifikohen dhe të regjistrohen dështimet e mundshme në çdo ndërveprim përmes sistemit. Një nga pjesëmarrësit kryesorë në fazën e zbulimit është ekipi i zhvillimit që ata e dinë shumë mirë se si sistemi sillet në çdo ndërveprim, (Microsoft Corporation *et.al.*,2014).

Disa nga fushat për çdo dështim përfshihen, (Microsoft Corporation *et.al.*,2014):

•Kategori dështimi. Një emër i shkurtër për llojin e dështimit.
•Përshkrim dështimi. Një përshkrim i dështimit.
•Pasojat. Informacion në lidhje me mënyrën se si ky dështim ndikon në shërbim ose te klienti, duke marrë parasysh trajtimin e gabimit.
•Zbulimi. Informacion se si ky dështim është zbuluar nga sistemi dhe çdo njoftim.
•Rimëkëmbja. Informacion rreth rimëkëmbjes së tanishme, përpjekjet e rikthimit të sistemit që lidhen me këtë dështim.

2.3. Norma

Duke përdorur dështimet e identifikuara në fazën e zbulimit ne mund të numërojmë dhe të regjistrojmë të gjitha efektet e dështimeve. Rezultati i fazës është një listë e rrezikut të llogaritur, ku ndikimi dhe mundësia e çdo

rreziku është marrë në konsideratë. Procedura është e njëjtë si në fazën e zbulimit, e cila nuk duhet të jetë më shumë se 90 minuta.

2.4. Veprime

Gjatë veprimeve merren hapa me qëllim të zbatimit të zgjidhjes në bazë të prodhimit të fazës normë. Bazuar në llogaritjen e rrezikut ekipi mund të vendosi prioritetet ku të përcaktoj se cilat hapa duhet të ndërmerren në fillim. Organizata duhet të investojë në fusha që janë identifikuar për rreziqe të larta në mënyrë për të ulur kohën e zbulimit. Kur është bërë mjaft investim për listën e rrezikut, disa nga rreziqet mund të shkojnë nga prioritet të lartë në prioritet të mesëm.

Përfundime

Elasticiteti është një domosdoshmëri. Çdo organizatë varet nga sistemet e IT dhe teknologjisë për të ofruar shërbimin e tyre. Dështimet e zgjatura dhe të përsëritura do të çojnë në humbje të reputacionit dhe dëmit financiar për organizatën. Këto kosto janë në përgjithësi shumë më të mëdha sesa hartimi dhe zbatimi i sistemeve elastike dhe zgjidhjet. Vazhdueshmëria e biznesit dhe rikthimi nga dështimet janë shumë të rëndësishme për mbrojtjen e organizatës. Teprica është një teknikë për rritjen e elasticitetit, e përdorur shpesh në ditët tona për të ndihmuar organizatën në ofrimin e shërbimeve të tyre kryesore. Mungesa e tolerancës, koha e ulët e rimëkëmbjes, periudhat e dështimeve janë të gjithë faktorë të rëndësishëm që një organizatë duhet të marrë në konsideratë kur planifikon dhe zgjedhjen e sistemeve të reja ose teknologji për biznesin e tyre.

Organizata ka nevojë që të kryejë kontrolle periodike dhe analiza të rrezikut, në mënyrë që të ketë një ide të qartë të situatës për elasticitetit në mjedisin e tyre. Implementimi i metodologjive si RMA apo të ngjashme do të shmangë shumë probleme dhe uljen e dëmeve nga rreziqet dhe sulmet, të cilat janë në rritje dhe zhvillohen me një normë të rrezikshme.

Literatura

Cybersecurity: Build Trust, Visibility, and Resilience;

http://www.cisco.com/web/strategy/docs/gov/cybersecurity_bvr_wp.pdf

Resilience by design for cloud services; Microsoft Corporation. (2014)

George A. Wright., Terrye N., Schaetzel. (2014): Cyber Security: Designing and Maintaining Resilience

Hugh Boyes. (2013): Resilience and Cyber Security of Technology in the Built Environment; Partnering for Cyber Resilience; World Economic Forum; (2012)