REPUBLIKA E SHQIPËRISË

AUTORITETI I MBIKËQYRJES FINANCIARE

Nr. 56 Prot.

Tiranë,
më 09.01.2024

AUTORITETIT KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Nr. 17 Prot.

Tiranë,
më 09.01.2024

MARRËVESHJE BASHKËPUNIMI DHE KONFIDENCIALITETI

Kjo marrëveshje bashkëpunimi dhe konfidencialiteti është dakordësuar ndërmjet palëve të mëposhtme:

a) Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (në vijim "AKCESK"), me adresë: Rr. "Papa Gjon Pali i II", nr.3, Tiranë, përfaqësuar nga Drejtori i Përgjithshëm Z. Igli Tafa,
dhe
b) Autoritetit të Mbikëqyrjes Financiare me adresë: Rruga "Dora D'Istria", Nr.10, Tiranë, përfaqësuar nga Nëndrejtori Ekzekutiv Mimoza Kaçi;

Duke pranuar se Teknologjitë e Informacionit dhe të Komunikimit (TIK) kanë hapur dritare të reja mundësish dhe janë mjete thelbësore për zhvillimin socio-ekonomik të shteteve;

Duke pranuar se TIK kanë sjellë gjithashtu lloje të reja kërcënimesh si: krimi kibernetik, spiunazhi kibernetik, aktivizimi, terrorizmi kibernetik, lufta kibernetike, sulmet ndaj infrastrukturës kritike, fushat e dezinformimit; dhe se këto kërcënime janë në rritje globalisht, ndërkombëtarisht, në mënyrë dinamike dhe po shfaqen gjithnjë e më të sofistikuara;

Palët kanë interesa strategjike të përbashkëta dhe bien dakord të bashkëpunojnë në fushën e informacionit bazuar në përfitime të njëjta dhe reciproke, për të përmirësuar bashkëpunimin në përgjigje të incidenteve të sigurisë së informacionit.

Duke pranuar rolin e Palëve në fushën e sigurisë kibernetike, në zbatimin e politikave dhe reagimeve operacionale, zhvillimin e mjeteve dhe në kuadrin rregullator.

Palët synojnë të përcaktojnë qëllimet kryesore, objektivat, fushat dhe format e bashkëpunimit, të përfshira në këtë marrëveshje për sa vijon.

Neni 1
QËLLIMI

Kjo marrëveshje bashkëpunimi dhe konfidencialiteti ka për qëllim të promovojë bashkëpunimin në fushën e sigurisë kibernetike, të përmirësojë shkëmbimin e informacionit ndërmjet palëve, si dhe të sigurojë konfidencialitetin e këtij informacioni në lidhje me sigurinë kibernetike, sipas përcaktimeve në nenin 5 të kësaj marrëveshje.

Neni 2
BAZA LIGJORE

Kjo marrëveshje hartohet në zbatim të ligjit nr. 2/2017 "Për sigurinë kibernetike", pikës 1, të nenit 18/1, të ligjit nr. 9572, datë 03.07.2006 "Për Autoritetin e Mbikëqyrjes Financiare", i ndryshuar, vendimit të Këshillit të Ministrave nr. 553, datë 15.7.2020, "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit" i ndryshuar.

Neni 3
STATUSI DHE FUSHA E MARRËVESHJES

1. Kjo marrëveshje bashkëpunimi përcakton kornizën brenda të cilës palët synojnë të bashkëpunojnë dhe shkëmbejnë informacionin konfidencial për të arritur qëllimet e përcaktuara në nenin 1.
2. Kjo marrëveshje nuk ka për qëllim të krijojë, mbajë ose imponojë të drejta dhe detyrime ligjore ndaj palëve ose ndërmjet palëve të treta. Zbatimi i kësaj marrëveshje nga palët e përcaktuara në të, i nënshtrohet përcaktimeve ligjore në fuqi.

Neni 4
FUSHAT E BASHKËPUNIMIT

1. Për të arritur qëllimin e mësipërm të kësaj marrëveshje, palët synojnë të bashkëpunojnë në fushat e mëposhtme:
   a) Ofrimin sipas kërkesës së palës skanime proaktive të rrjeteve dhe sistemeve të informacionit me qëllim identifikimin e vulnerabiliteteve me impakt të lartë të mundshëm;
   b) Vendosjen në dispozicion të kopjes së logeve;
   c) Raportimin e të gjitha llojeve të incidenteve të sigurisë kibernetike në përputhje me parashikimet ligjore në fuqi për sigurinë kibernetike;
   d) Ndarjen e informacionit në lidhje me përhapjen e programeve keqdashëse;
   e) Shkëmbimin e indikatorëve të rrezikut të sigurisë kibernetike;
   f) Ofrimin e informacionit për zgjidhjet e mundshme në fushën e sigurisë së informacionit;
   g) Shkëmbimin e materialeve edukative dhe trajnuese lidhur me sigurinë kibernetike;

h) Bashkëpunimin dhe koordinimin e ndërsjelltë në lidhje me zhvillimin e seminareve teknike, edukative dhe trajnimeve;
i) Ofrimin e asistencës informative këshilluese në hetimin dhe eliminimin e incidenteve të sigurisë së informacionit;
j) Shkëmbimin e informacionit mbi rreziqet e sigurisë së informacionit;

2. Mënyra e shkëmbimit të informacionit sipas këtij neni përcaktohen në Ankesin bashkëlidhur marrëveshjes.

Neni 5
SHKËMBIMI DHE PËRDORIMI INFORMACIONIT

1. Palët marrin përsipër të shkëmbejnë informacionin për qëllimet e kësaj marrëveshje duke ruajtur konfidencialitetin. Shkëmbimi i informacionit sipas kushteve të kësaj marrëveshje, do të kryhet në përputhje me legjislacionin në fuqi, politikat dhe mekanizmat në fuqi të palëve.
2. Në funksion të qëllimit të kësaj marrëveshje, Palët janë të detyruar që çdo shkëmbim informacioni ta trajtojnë si konfidencial në përputhje me përcaktimet e nenit 18/1, të ligjit nr. 9572, datë 03.07.2006 "Për Autoritetin e Mbikëqyrjes Financiare", i ndryshuar.
3. Asnjëra palë nuk do të shpërndajë informacionet e marra nga pala tjetër sipas përcaktimeve të kësaj marrëveshje, asnjë pale të tretë pa pëlqimin paraprak të Palës tjetër.
4. Palët do të zbatojnë mbrojtjen e të dhënave personale, sipas kuadrit ligjor në fuqi.
5. Palët do të caktojnë një person kontakti përgjegjës për komunikimet ndërmjet palëve në kuadrin e kësaj marrëveshjeje.
6. Çdo aktivitet i përbashkët që përfshin pronësinë intelektuale do të dakordësohet me shkrim nga palët për të mbrojtur interesat përkatëse.

Neni 6
ZGJIDHJA E MOSMARRËVESHJEVE

Çdo mosmarrëveshje ndërmjet palëve në lidhje me interpretimin dhe/ose zbatimin e kësaj marrëveshje do të zgjidhet në mënyrë miqësore nëpërmjet konsultimeve dhe/ose negociatave ndërmjet tyre.

Neni 7
FILLIMI, KOHËZGJATJA DHE PËRFUNDIMI I MARRËVESHJES

1. Kjo marrëveshje hyn në fuqi në datën e nënshkrimit të saj nga të dyja palët.
2. Kjo marrëveshje nënshkruhet për një afat të pacaktuar dhe palët mund ta ndërpresin atë në çdo kohë duke njoftuar palën tjetër me shkrim.
3. Aktivitetet që janë në proces në momentin e përfundimit të marrëveshjes, do të përfundojnë në përputhje me dispozitat e kësaj marrëveshjeje.
4. Kjo marrëveshje mund të ndryshohet me shkrim duke nënshkruar të dyja palët.
5. Një ndryshim i kësaj marrëveshjeje do të hyjë në fuqi në datën e percaktuar reciprokisht nga palët.

Neni 8
KOSTOT, SHPENZIMET DHE BURIME

Çdo palë merr persipër shpenzimet e veta dhe i siguron vetes burime për ekzekutimin e kësaj marrëveshje dhe shpenzimeve të tjera të lidhura me të. Të gjitha aktivitetet sipas kësaj marrëveshje do t'i nënshtrohen disponueshmërisë së burimeve financiare dhe njerëzore në përputhje me legjislacionin në fuqi.

Neni 9
TË NDRYSHME

1. Kjo marrëveshje hartohet dhe zbatohet në përputhje me legjislacionin shqiptar.
2. Kjo marrëveshje nëshkruhet në 4 (katër) kopje, 2 për secilën palë.

Neni 10
INFORMACIONET E KONTAKTIT

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE I SHQIPËRISË	**AUTORITETI I MBIKËQYRJES FINANCIARE**
Emër: Eriola Sadiku	Emër: Klodi Plloça
Institucioni: AKCESK	Institucioni: AUTORITETI I MBIKËQYRJES FINANCIARE
Telefon:	Telefon:
Adresë e-mail: eriola.sadiku@cesk.gov.al	Adresë e-mail: klodi.plloca@amf.gov.al
Telefon24/7: +355 4 22 210 39	Telefon24/7:
Telefon emergjencash: +355 69 20 88 722	Telefon emergjencash: +355 69 36 57 229
Adresa: Rr. "Papa Gjon Pali i II", nr.3, Tiranë	Adresa: Rruga "Dora D'istria", Nr.10 Tiranë

PËR
AUTORITETIN E MBIKËQYRJES FINANCIARE

NËNDREJTOR EKZEKUTIV
Mimoza KAÇE

PËR
AUTORITETIN KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

DREJTOR I PËRGJITHSHËM
Igli TAFA

ANEKS NR. 1

Në kuadër të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit, AKCESK me cilësinë e CSIRT Kombëtar, do të kryej monitorimin (24/7) dhe analizimin e logeve të sistemeve dhe rrjeteve të rëndësishme të infrastrukturës Agjencia e Mbikëqyrjes Financiare (AMF).

Monitorimi i infrastrukturës do të kryhet nëpërmjet analizimit të logeve me qëllim identifikimin e eventeve që cenojnë sigurinë e sistemeve dhe rrjeteve nën administrim të AMF.

Analizimi i logeve të sistemeve të AMF do të kryhet nga AKCESK nëpërmjet platformës ***Manage Engine Log 360.***

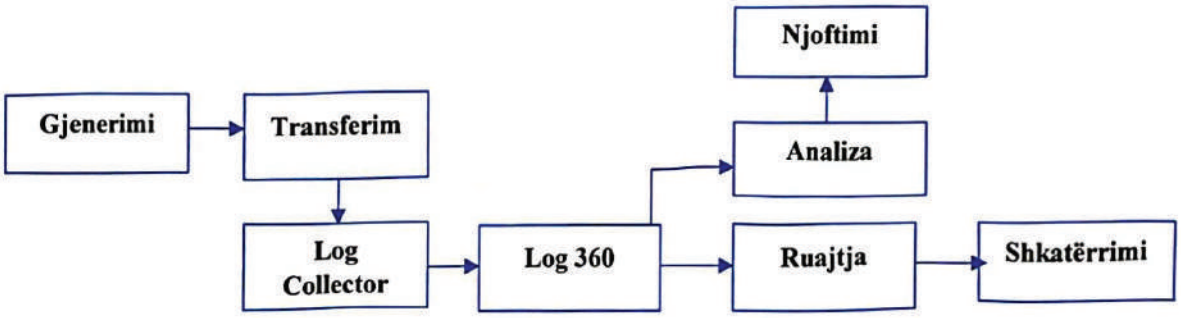
Për realizimin e këtij shërbimi, AMF duhet të vendosi në dispozicion burimet e nevojshme (PC brenda infrastrukturës së institucionit) për instalimin e (*log collector*) të cilët do të bëjnë mbledhjen e logeve dhe dërgimin e tyre në platformën Log 360 për tu analizuar.

Agjencia e Mbikëqyrjes Financiare (AMF) do të përcaktojë loget e sistemeve dhe rrjeteve që do të dërgohen në (*log collector)* për tu analizuar.

Për përcaktimin e loge-ve që do të analizohen sugjerohet të mbahen në konsideratë:

- Niveli i kritikalitetit të sistemit;
- Klasifikimi i aseteve të informacionit;
- Frekuenca me të cilën sistemet janë sulmuar ose kompromet uar më parë;
- Niveli i ekspozimit ndaj rrjeteve të jashtme.

Procesi i menaxhimit të log-eve paraqitet si në figurën e mëposhtme:



Gjenerimi – Konfigurimi i aseteve dhe sistemeve për të krijuar log-e

Asetet dhe sistemet e AMF do të konfigurohen për të krijuar log-e.

Transferimi – Transferimi i log-eve nga "storage" lokal i pajisjeve, në "Log collector të Manage Engine Log 360" të centralizuar për analiza të mëtejshme.

Pranë infrastrukturës AMF, në një PC do të instalohet një *log collector,* i cili do të mbledhë loget e rrjetit/sistemeve të AMF dhe do ti përcjell në platformën Manage Engine Log 360 për analiza të mëtejshme.

Ruajtja – Ruajtja dhe mbajtja e log-eve në mënyrë të sigurtë me qëllim kryerjen e analizave sa herë që është e nevojshme.

Log-et do të arkivohen për një periudhë të **1 mujore** (search retention) dhe **3 mujore** (storage retention) në përputhje me kërkesat ligjore në fuqi, politikat dhe procedurat e sigurisë së informacionit dhe kapaciteteve storage të platformës përkatëse.

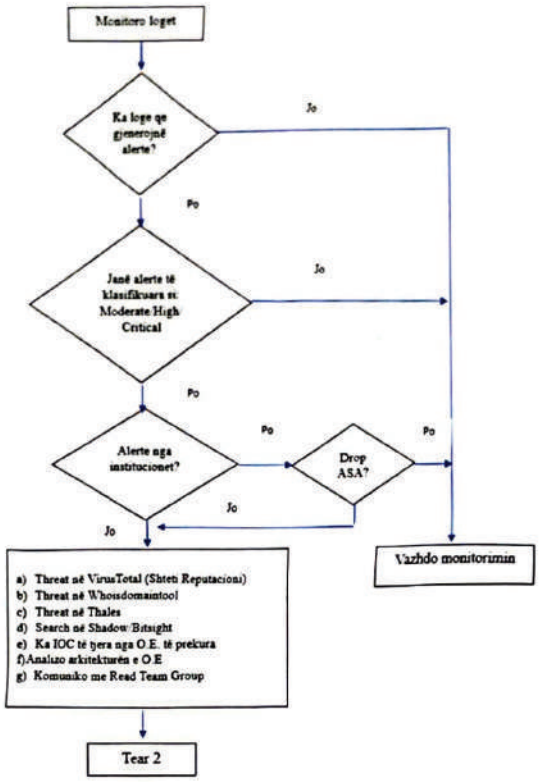
Analiza – Analizimi i log-eve për të identifikuar eventet e padëshiruara dhe error-et e sistemeve të informacionit.

Përpunimi i logeve të Log360 nga Qendra Operacionale CSIRT.

SOC Tier 1: Ka si qëllim të monitorojë log-et e klasifikuara të platformës Log360 dhe të njoftojë në rast alerti.

SOC Tier 2: Kryen inspektim të thelluar të problemit dhe koordinon aktivitetin me AMF për zgjidhjen e problemit.

Hapat e procesit të monitorimit të logeve detajohen në skemën e mëposhtme:



SOC Tier 1: Do të monitoroj loget që gjenerojnë alerte të klasifikuara si Moderate (Notice), High (Error, Warning) dhe Kritike (Emergency, Alert, Critical).
Monitorimi i logeve bëhet për IP që nuk janë bërë drop, deny, ose block nga Firewall-et.

Njoftimi: Agjencia e Mbikëqyrjes Financiare (AMF) do të njoftohet nëpërmjet ekipit të SOC për eventet/ngjarjet e sigurisë të identifikuara nga analiza dhe monitorimi i kryer nëpërmjet Log360.

Gjithashtu, do të njoftohet AMF për loget që janë lejuar (allow) nga Firewall ose që janë bërë drop, deny, ose block për herë të parë, por konsiderohen mjaft kritike.

Ekipi i SOC do të asistoje AMF deri në zgjidhjen përfundimtare të problematikave të evidentuara.

Shkatërrimi/ Asgjësimi – Fshirja e log-eve: Pas përfundimit të periudhës së arkivimit, loget fshihen/shkatërrohen në mënyrë automatike dhe të sigurtë nga platforma, duke siguruar mos përdorimin më të tyre.