REPUBLIKA E SHQIPËRISË
KONTROLLI I LARTË I SHTETIT
DEPARTAMENTI I AUDITIMIT TË TEKNOLOGJISË SË INFORMACIONIT
KRYETARI

Adresa: *Rruga "Abdi Toptani" nr.1, Tiranë; Tel: 04251-267,* ***e-mail:*** *klsh@klsh.org.al,* ***web-site*** *www.klsh.org.al*

Nr. 357/11 Prot. Tiranë, më 14.09.2019

V E N D I M

Nr. 70, Datë 14.09.2019

PËR AUDITIMIN E USHTRUAR NË MINISTRINË E FINANCAVE DHE EKONOMISË, (MFE), NJËSIA E TEKNOLOGJISË SË INFORMACIONIT E AKSHI-T ATASHUAR PËR MFE "MBI AUDITIMIN E SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT" PËR PERIUDHËN NGA DATA 01.01.2018 DERI MË DATËN 30.06.2019.

Nga auditimi i Ministrisë së Financave dhe Ekonomisë, (MFE), Njësia e Teknologjisë së Informacionit e AKSHI-t atashuar për MFE, mbi sistemet e teknologjisë së informacionit, për periudhën nga 01.01.2018-30.06.2019, u konstatuan mangësi në: zbatimin e Marrëveshjeve të Nivelit të Shërbimit, identifikimin dhe administrimin e elementëve kritikë në ofrimin shërbimeve, mbivendosje të akteve ligjore dhe nënligjore, si dhe në saktësinë e veprimeve operacionale të input-it të të dhënave.
Pasi u njoha me Raportin Përfundimtar të Auditimit dhe Projektvendimin e paraqitur nga Grupi i Auditimit të Departamentit të Auditimit të Teknologjisë së Informacionit, shpjegimet e dhëna nga subjekti i audituar, si dhe vlerësimet mbi objektivitetin dhe cilësinë e auditimit nga Drejtori i Departamentit të mësipërm, Drejtori i Drejtorisë së Kontrollit të Zbatimit të Standardeve dhe Sigurimit të Cilësisë dhe Drejtori i Përgjithshëm, në mbështetje të neneve 10, 15, 25 dhe 30, të ligjit nr. 154/2014 miratuar në datën 27.11.2014 "*Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit*".

VENDOSA:

I. Të miratoj Raportin Përfundimtar të Auditimit "Për vlerësimin e sistemeve të teknologjisë së informacionit", të ushtruar në Ministrinë e Financave dhe Ekonomisë, (MFE), Njësia e Teknologjisë së Informacionit e AKSHI-t atashuar për MFE, sipas Programit të Auditimit nr. 357/1, datë 18.06.2019, miratuar nga Kryetari i Kontrollit të Lartë të Shtetit, për periudhën e aktivitetit nga data 01.01.2018 deri më datën 30.06.2019, me afat auditimi nga 06.06.2019-22.07.2019.

II. Të miratoj opinionin e auditimit, rekomandimet për përmirësimin e gjendjes dhe të kërkoj marrjen e masave sa vijon:

A. OPINIONI I AUDITIMIT

Grupi i auditimit mbështetur në Standardet ndërkombëtare të Auditimit përkatësisht në ISSAI 100, ISSAI 5300, ISSAI 5310 si dhe nenet 3 dhe 14 të ligjit 154 "*Për Organizimin dhe Funksionimin e KLSH*" datë 27.11.2014 konstaton se, mungesa e Strategjisë në drejtim të teknologjisë informacionit, mbart riskun e keq adresimit të burimeve të nevojshme për mbështetjen e veprimtarisë së MFE.
Në gjykimin tonë, identifikimi dhe administrimi i elementëve kritikë në ofrimin shërbimeve dhe garantimin e sigurisë së të dhënave si dhe vazhdimësisë në ofrimin e shërbimit nëpërmjet teknologjisë së informacionit është i pa pamjaftueshëm. Në këtë drejtim, përdorimi i sistemeve në MFE mbart një risk të lartë në mbarëvajtjen e funksionaliteteve të ndërtuara në shërbim të qëllimit dhe objektivave institucionale.
Ndërveprimi dhe bashkëpunimi i sistemeve të informacionit në lidhje me automatizimin e të dhënave me rëndësi të veçantë nuk është i konsoliduar.

B. PROPOZIME PËR NDRYSHIME APO PËRMIRËSIME NË LEGJISLACIONIN NË FUQI

1. Gjetje nga auditimi: Nga auditimi i ushtruar mbi sistemet e teknologjisë së informacionit në Ministrinë e Financave dhe Ekonomisë, u konstatua se baza ligjore, më konkretisht VKM nr. 352, datë 11.05.2016 "*Për krijimin e bazës së të dhënave shtetërore të Sistemit Informatik Financiar të Qeverisë (SIFQ)*" dhe VKM nr. 673, datë 22.11.2017 "*Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit*", i ndryshuar, janë në kundërshtim për sa i përket përcaktimit të institucionit administrues të SIFQ. Saktësisht, në VKM nr. 352, pika 5/a, citohet: "*Institucioni administrues i SIFQ është Ministria e Financave*", ndërkohë në VKM nr. 673, pika 9 citohet: "*AKSHI është administrator i çdo sistemi TIK që ka si përdorues institucionet apo organet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave*".
Në VKM nr. 673 *(si akt më i vonshëm kronologjikisht*), nuk përcaktohet asnjë dispozitë apo nen i cili shfuqizon apo ndryshon nenet e VKM nr. 352.
Aktualisht, të dyja VKM-të janë në fuqi, edhe pse kundërshtojnë njëri tjetrin për sa i përket administrimit të Sistemit Informatik Financiar të Qeverisë (SIFQ).
1.1 Rekomandimi: MFE dhe AKSHI të marrin masa për ngritjen e një grupi të përbashkët me qëllim hartimin, përcaktimin dhe propozimin në Këshillin e Ministrave të ndryshimeve të nevojshme në bazën rregullatore për të drejtat Administruese të Sistemit Informatik Financiar Qeveritar.

Menjëherë

C. MASA ORGANIZATIVE:

1. Gjetje nga auditimi: Nga auditimi i "*Process Order*" për vitin 2018, u konstatuan 33903 raste ku fusha "*Bill Amount*" është e barabartë me fushën "Shuma" (pra kontrata është mbyllur), por nuk ka marrë statusin "*Closed*", me qëllim mbylljen e procesit.
Gjithashtu u konstatuan 2 raste ku fusha "*Bill Amount*" është më e madhe se fusha "*Shuma*". Ky veprim do të thotë se furnitori është paguar më shumë se vlera e kontratës. Për pasojë, rezulton se sistemi i thesarit në këto raste nuk ka mekanizmat e duhur parandalues për mos lejim të tejkalimit të vlerës së kontratës.
1.1 Rekomandimi: MFE dhe AKSHI të analizojnë rastet e konstatuara të tejkalimit të vlerave të kontratave dhe më gjerë. Administruesit e sistemit të marrin masat e nevojshme për parandalimin automatik nga vetë sistemi të kësaj problematike.

Menjëherë

2. Gjetje nga auditimi: Nga verifikimi analitik i 374 userave aktiv të sistemit të SIFQ, u konstatua:
a) usera të cilët edhe pse e kanë përfunduar objektin për të cilin janë çelur, janë ende aktiv. Ky fakt mbart një risk të lartë për ndërhyrje të paautorizuara në sistem duke mos lënë gjurmë mbi aktivitetin që kanë kryer. Saktësisht: Oracle, Oracle3, Oracle5, Oracle7, Oracle9. Gjithashtu user-at nuk kanë një "End Date", pra edhe pas shkëputjes së marrëdhënieve të punës, punonjësve nuk u është mbyllur ende account-i.
b) useri FADMIN përdoret nga disa punonjës të cilat gjithashtu kanë userin e tyre, duke mos lënë gjurmë se cili punonjës ka kryer një veprim të caktuar me këtë user. Ky user ka 127 lloje të drejtash (atribute) në sistem, duke bërë që risku i përdorimit të tij nga shumë punonjës të jetë i lartë.
c) Nuk ka një rregullore/ manual ku të përcaktohen atributet që secili user duhet të gëzojë në varësi të pozicionit të punës që ka.
2.1 Rekomandimi: MFE në bashkëpunim me AKSHI-n të analizojë problematikat e konstatuar nga grupi i auditimit në lidhje me user-at e sistemit të SIFQ, duke marrë masat e nevojshme për çaktivizimin e user-ave të cilëve u ka përfunduar objekti i krijimit të tyre, fshirjen e useri-it FADMIN, i cili nuk i përket asnjë punonjësi në veçanti.
MFE në bashkëpunim me AKSHI-n të marrin masat e nevojshme për hartimin e një rregulloreje ku të përcaktohet qartë lidhja ndërmjet atributeteve të user-t me pozicionin e punës.

Menjëherë

3. Gjetje nga auditimi: Nga auditimi i Marrëveshjeve të Nivelit të Shërbimit në Ministrinë e Financave dhe Ekonomisë, si dhe duke patur në konsideratë ndryshimet e fundit të akteve ligjore dhe nënligjore, mënyrën e organizimit të funksionimit të strukturave dhe sistemeve të teknologjisë së informacionit në MFE, u konstatua se sipas VKM Nr. 673, datë 22.11.2017 "*Për riorganizimin e agjencisë kombëtare të shoqërisë së informacionit*", i ndryshuar, procesin e ofrimit të shërbimit duhet ta mbulojë vetë AKSHI, pasi ka aftësitë e nevojshme profesionale për ofrimin e këtyre shërbimeve.
Në marrëveshjen e nivelit të shërbimit datë 24.01.2018, ndërmjet Agjencisë Kombëtare të Shoqërisë së Informacionit dhe Ministrisë së Financave dhe Ekonomisë, protokolluar me nr. 420 (AKSHI) dhe nr. 653/1 (MFE), përcaktohen elementët që do të mbulohen nga AKSHI.
Gjithashtu mbështetur edhe në përshkrimet e punës të stafit të drejtorisë TIK të AKSHI-t atashuar pranë MFE, përkatësisht "*Sektori i Zhvillimit dhe Mirëmbajtjes dhe Sigurisë së Infrastrukturës*" ka detyra kryesore të përcaktuara për mirëmbajtjen dhe suportin në kategori të ndryshme.

Nga sa më sipër konstatohet se zërat e përfshira në këto marrëveshje në nivel shërbimi, gjenden të pasqyruara në kompetencat e përcaktuara nga VKM nr. 673 datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*", i ndryshuar dhe në marrëveshjen e nivelit të shërbimit datë 24.01.2018, ndërmjet Agjencisë Kombëtare të Shoqërisë së Informacionit dhe Ministrisë së Financave dhe Ekonomisë.

3.1 Rekomandimi: MFE dhe AKSHI të analizojnë nevojën e adresimit të shërbimeve të cilat janë pjesë e MNSH-ve aktuale dhe de-jure i janë ngarkuar në mënyrë të drejtpërdrejtë AKSHI-t. Në përputhje me aktet ligjore dhe nënligjore në fuqi, të identifikohen problematikat dhe të merren masat për zgjidhjen e tyre.

Në vijimësi

4. Gjetje nga auditimi: Nga auditimi u konstatua se Marrëveshjet në Nivel Shërbimi në MFE, nuk janë hartuar në përputhje të plotë me aneksin 2, të Udhëzimit nr. 2, datë 02.09.2013 "*Për standardizimin e hartimit të termave të referencës për projektet TIK në Administratën Publike*" pjesa III pika 10 Aneksi 2. Sipas VKM nr. 710, datë 21.08.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdimësisë së punës dhe marrëveshjeve të nivelit të shërbimit*", i ndryshuar, pika 2, germa c, dhe Udhëzimit të Ministrit të Shtetit për Inovacionin dhe Administratën Publike, nr. 1159, datë 17.03.2014 "*Për Hartimin e Marrëveshjeve të Nivelit të Shërbimit*", i ndryshuar, MNSH-ja duhet të ishte si aneks më vete bashkëlidhur kontratës administrative. Sipas Aneksit 1 të këtij Udhëzimi, ndër të tjera duhet të përcaktohen elementë të rëndësishëm për realizimin e procesit të mirëmbajtjes, si drejtuesi i projektit, personin e kontaktit, përkufizimet e termave teknikë, përshkrimi i shërbimeve, të drejtat dhe detyrimet e institucionit dhe të ofruesit të shërbimit, menaxhimi i shërbimeve, disponueshmëria e shërbimit, kufizimet e mundshme, mirëmbajtja e sistemit, matja e cilësisë së shërbimit, kërkesat e shërbimit, raporti i shërbimit dhe vlerësimet periodike, menaxhimi i vazhdueshmërisë së shërbimit, trajtimi i informacionit konfidencial, njoftimi i palëve, penalitetet e mundshme, dokumentacioni mbështetës, ndërprerja e MNSH-së, dhe të tjerë elementë të rëndësishëm që përcaktohen në aneksin 1.

4.1 Rekomandimi: MFE dhe AKSHI në vijimësi të marrin masa për përfshirjen e plotë të elementëve të Marrëveshjeve në Nivel Shërbimi sipas përcaktimeve ligjore dhe nënligjore në fuqi, me qëllim kontrollin e plotë të shërbimit të ofruar nga ana e operatorëve ekonomik.

Në vijimësi

5. Gjetje nga auditimi: Nga auditimi u konstatua se:

- Nga Sekretari i Përgjithshëm i MFE janë nxjerrë urdhra për ngritjen e grupeve të punës, ku pjesë përbërëse e grupit janë punonjës të AKSHI-t. Një veprim i tillë nuk citohet në asnjë pikë të marrëveshjes në nivel shërbimi ndërmjet dy institucioneve protokolluar me nr. 420 (AKSHI) dhe nr. 653/1 (MFE), ku t'i jepet e drejtë titullarit të një institucioni të ngrejë urdhra me punonjës/specialist të një institucioni tjetër. Gjithashtu këto institucione nuk janë në varësi të njëra tjetrës, për pasojë grupi i auditimit i vlerëson këto urdhra të pabazuara juridikisht.
- Në disa nga urdhrat e marrjes në dorëzim të aktiveve apo shërbimeve në fushën e teknologjisë së informacionit, pjesë e grupit të marrjes në dorëzim janë punonjës jo specialistë të fushës, veprim në kundërshtim me pikën 43 të Udhëzimit Nr. 30 Datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik", i ndryshuar, ku citohet "*Komisioni përbëhet nga specialistë të fushës sipas llojit të aktiveve dhe, në rast nevoje, edhe nga ekspertë të jashtëm.*

Në komision bëjnë pjesë jo më pak se tre veta, duke përfshirë edhe punonjësin me përgjegjësi materiale".

5.1 Rekomandimi: Organet drejtuese të MFE dhe AKSHI-t në të ardhmen të marrin masat e nevojshme për ngritjen e grupeve të punës me punonjës brenda institucioneve përkatëse, përcaktimin e përgjegjësive individuale si dhe në përputhje me kërkesat e Udhëzimit nr. 30, për vendosjen e specialistëve të fushës sipas llojit të aktiveve.

Në vijimësi

6. Gjetje nga auditimi: Teknologjia e informacionit zhvillohet pa Plan Strategjik, duke sjellë mos pasqyrim të qartë të objektivave të MFE lidhur me sigurinë institucionale dhe infrastrukturën TI, objektivat strategjikë për burimet njerëzore të strukturës së TI pranë MFE, në kundërshtim me strategjinë kombëtare të zhvillimit të dixhitalizimit.

6.1 Rekomandimi: Strukturat drejtuese në MFE dhe AKSHI, duke marrë në konsideratë kohën, burimet e nevojshme si dhe rëndësinë e të dhënave që institucioni zotëron dhe përpunon, të marrin masa për hartimin e Planit Strategjik të Teknologjisë së Informacionit, ku të adresohen qartë objektivat e institucionit duke patur parasysh ndryshimet e ndodhura me aktet ligjore dhe nënligjore.

Në vijimësi

7. Gjetje nga auditimi: Nga auditimi u konstatua se Drejtoria TIK në Ministrinë e Financave dhe Ekonomisë (MFE) aktualisht zbaton Manualin IT ku përcaktohen procedurat që do të ndiqen për krijimin, mirëmbajtjen dhe administrimin e infrastrukturës dhe sistemeve të informacionit, por ky manual është ende i pa miratuar nga nëpunësi autorizues.

7.1 Rekomandimi MFE në bashkëpunim me Drejtorinë TIK atashuar pranë MFE të marrin masa për përditësimin dhe miratimin e Manualin IT të Teknologjisë së Informacionit me ndryshimet e ndodhura me bazën ligjore dhe nënligjore.

Menjëherë

8. Gjetje nga auditimi: Nga auditimit u konstatua se Drejtoria TIK aktualisht e ushtron aktivitetin e saj me 9 punonjës, edhe pse struktura e miratuar është e përbërë nga 13 punonjës. Duke u nisur nga rëndësia specifike e Drejtorisë TIK në MFE konstatohen mungesa në staf në disa pozicione të rëndësishme të sektorëve të drejtorisë TIK, duke rritur riskun e mos përmbushjes së detyrave.
Drejtoria TIK pranë MFE nuk kryen trajnime në fusha specifike dhe nuk ka vendosur standarde të cilat do të çonin në rritjen profesionale dhe kualifikimin e stafit të TI.

8.1 Rekomandimi: Strukturat drejtuese të AKSHI-t në bashkëpunim me MFE të marrin masa për mirë menaxhimin e burimeve njerëzore duke plotësuar vendet vakante dhe të hartojnë politika për zhvillimin e tyre nëpërmjet trajnimeve në lidhje me sistemet, sigurinë dhe teknologjinë e informacionit, me qëllim përmbushjen e nevojave në fushën TIK në MFE.

Në vijimësi

9. Gjetje nga auditimi: Nga auditimi u konstatua se, MFE nuk ka regjistër të menaxhimit të incidenteve. Risqet menaxhohen mbi bazë ngjarjesh. Jepet suport, mbështetje teknike dhe logjike për operacionet IT që ndihmojnë mbarëvajtjen e strukturave të institucionit. Procedurat kryhen nëpërmjet shkëmbimeve verbale dhe nëpërmjet e-mail-eve, duke mos realizuar identifikimin e risqeve, mbart riskun e përsëritjes së incidenteve. Ekzistenca e një regjistri të menaxhimit të

incidenteve bazohet në Objektivat e Kontrollit të Teknologjisë së Informacionit COBIT, Manualin e Auditmit IT si dhe praktikave më të mira.
9.1 Rekomandimi: Strukturat Drejtuese në MFE në bashkëpunim me Drejtorinë e sistemeve dhe Teknologjinë e Informacionit atashuar pranë MFE-s të marrin masa për:
-identifikimin e risqeve IT dhe hartimin e regjistrit të risqeve mbi infrastrukturën TIK;
-dokumentimin dhe monitorimin e incidenteve;
-menaxhimin e ndryshimeve dhe dokumentimin e tyre.

Në vijimësi

10. Gjetje nga auditimi: Nga auditimi u konstatua se, Drejtoria e TIK e atashuar pranë MFE nuk ka hartuar raporte monitorimi dhe shërbimi në kundërshtim me pikën 4 të marrëveshjes në nivel shërbimit ndërmjet dy institucioneve protokolluar me nr. 420 prot., (AKSHI) dhe nr. 653/1 prot., (MFE), datë 24.01.2018.
10.1 Rekomandimi: Drejtoria e TIK pranë MFE në vijimësi të kryejë analizimin, prioritarizimin dhe ofrimin e shërbimeve të përcaktuara në MNSH-në ndërmjet institucioneve (MFE dhe AKSHI), hartimin e raporteve javore dhe mujore të shërbimeve të ofruara, me qëllim dhënien e sigurisë së arsyeshme për kryerjen me rigorozitet të suportit.

Në vijimësi

11. Gjetje nga auditimi: Për periudhën e audituar, procedurat e prokurimit si dhe lidhja e kontratave për mallrat apo shërbimet në fushën e teknologjisë së informacionit, janë zhvilluar dhe nënshkruar nga AKSHI, ndërsa vetë investimi si dhe detyrimi financiare kalojnë për MFE. VKM Nr. 673, datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*", i ndryshuar, saktësisht në pika 18, citon: "*Institucionet e administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave duhet të dorëzojnë pranë AKSHI-t 1 (një) kopje të dokumentacionit të plotë të çdo sistemi dhe infrastrukture TIK ekzistuese dhe kodin e burimit. Sistemet dhe infrastruktura TIK ekzistuese kalojnë nën administrimin dhe inventarin e AKSHI-t, së bashku me të drejtat dhe detyrimet juridiko-civile përkatëse brenda datës 30 shtator 2018*".
Me Urdhër të përbashkët të Sekretarit të Përgjithshëm të MFE dhe Drejtorit të Përgjithshëm të AKSHI-t, me nr. 5762 prot, datë 21.03.2018 (MFE) dhe nr. 1311 prot, datë 16.03.2018 (AKSHI), janë ngritur grupet e punës për evidentimin e sistemeve IT dhe infrastrukturave hardware të MFE, si dhe përcaktimin e listës së aktiveve të qëndrueshme të trupëzuara dhe të patrupëzuara objekt kalimi kapital.
Edhe pse ka kaluar rreth 1 vit e 4 muaj nga nxjerrja e urdhrit të përbashkët për kalimin e kapitalit, si dhe rreth 10 muaj nga afati i vendosur në VKM Nr. 673, ky proces ende nuk ka përfunduar. Aktualisht sistemet e IT dhe infrastruktura hardware e MFE, janë ende pjesë e inventarit të MFE, e për pasojë edhe detyrimet juridike dhe financiare mbi këto sisteme, në kundërshtim me pikën 18 të VKM nr. 673, datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit*", i ndryshuar.
11.1 Rekomandimi: Organet drejtuese të MFE dhe AKSHI-t të marrin masat e nevojshme për përfundimin e procesit të kalimit të aktiveve të sistemeve të informacionit nga MFE tek AKSHI, si dhe të përcaktojnë përgjegjësitë për vonesat e shkaktuara të zbatimit të kërkesave ligjore lidhur me këtë çështje.

Brenda vitit 2019

12. Gjetje nga auditimi: Nga auditimi mbi sigurinë e aksesit të network-ut u konstatua se:
-Nga konfigurimet nuk shikohen bllokime të *subneteve* të këtyre bankave drejt *subneteve* të MFE çka përbën risk për hyrje dhe skanime të rrjetit të MFE nga këto lidhje;
-Pajisja *firewall* ka të aktivizuar log çka bën të mundur për të verifikuar një sërë procesesh që routeri kryen si edhe ruajtjen e tyre. Routeri ka një memorie të vogël dhe këto log-e nuk mund të ruhen ose të analizohen live duke bërë të mundur detektimin në kohë reale të një sulmi ose të një hyrje të paautorizuara;
-Nuk ka të krijuar group users me nivele të ndara menaxhim/monitorim. Çdo veprim bëhet nga useri admin;
-Nuk janë marrë masa për të bërë *disable* userin admin dhe për të krijuar një user tjetër me të drejta admini. Kjo gjë do të parandalonte sulme nga scripte/viruse që mund të merren brenda serverave ose pc-ve në MFE. Shumica e viruseve që bëjnë DDoS, përdorin si username "admin";
-Në routerin me IP private [redacted] dhe IP publike [redacted] vërehet se ka usera të krijuar për shoqërinë [redacted] dhe usera oracle të cilët mund të aksesojnë edhe nga jashtë rrjetin e brendshëm si edhe shërbimet e MFE. Këta usera mund të logohen nëpërmjet VPN edhe nga jashtë MFE.
-Për routerin me ID [redacted] shikohet që faza IKE për *ipsec* ka një *pre shared key* me 3 karaktere "abc" për të gjitha lidhjet VPN të MFE me zyrat e rretheve si dhe me site të tjera. Passwordi që është përdorur nuk përmbush parametrat e sigurisë dhe përbën rrezik për akses nga palë të treta dhe të pa autorizuara.
12.1 Rekomandim: Drejtoria TIK e AKSHI-t pranë MFE të marrë masa për:
-Krijimin e konfigurimeve përkatëse bllokuese për të gjitha lidhjet VPN nga Bankat e nivelit të dytë drejt rrjetit privat të MFE;
-Krijimin e grupeve dhe usera-ve admin/monitorim;
-Useri admin të bëhet *disable* dhe të krijohet një user me emërtim ndryshe me të drejta administratori për të gjitha routerat/switchet e menaxhueshëm;
-Konfigurimin e një *script-i* në firewall i cili bllokon për 24 orë IP-në nëse nga kjo IP provohet me shumë se 3 here logimi të gabuar;
-Marrjen e masave për krijimin e një platforme të centralizuar për gjenerimin e alerteve sipas riskut për mbajtjen e log-eve për të gjitha pajisjet. Pasja e një platforme të centralizuar, parandalon në kohë reale sulme, dëmtime të pajisjeve si dhe ndihmon në ecurinë e shërbimeve TIK që MFE disponon.

Në vijimësi

13. Gjetje nga auditimi: Nga auditimi u konstatua se nga DPTH nuk është mbajtur një regjistër gabimesh (*hedhje gabim, korrigjime nëpër TDO apo edhe në MFE*) funksionale që bëhen nga userat e SIFQ, me qëllim trajtimin dhe hartimin e masave parandaluese e tyre në të ardhmen. Ekzistenca e një regjistri gabimesh bazohet në Objektivat e Kontrollit të Teknologjisë së Informacionit COBIT, Manualin e Auditmit IT si dhe praktikave më të mira.
13.1 Rekomandimi: DPTH të marrë masa për krijimin e një regjistri gabimesh me qëllim trajtimin dhe hartimin e masave parandaluese në të ardhmen.

Në vijimësi

14. Gjetje nga auditimi: Nga DPT merren të dhëna vetëm për të ardhurat. DPT dërgon ne MFE informacionin elektronik nëpërmjet file.txt i cili i korrespondon kontabilizimit të transaksioneve mbi të ardhurat tatimore të file-it txt dërguar paraprakisht nga MFE ne DPT mbi arkëtimin e këtyre të ardhurave. Çdo file ka një emër unik dhe një file nuk mund të ngarkohet më shumë se një here në SIFQ, në të kundërt SIFQ refuzon automatikisht ngarkimin e të njëjtit file më shumë se një herë. Në rastin e korrigjimeve kontabile që DPT dërgon në MFE lidhur me kontabilizime të të ardhurave dërguar me file-t e mëparshme, DPT dërgon një file të ri i cili përmban korrigjimet kontabile, ku çdo transaksion korrigjimi kontabil përmban numrin e referencës së pagës në SIFQ të cilës i referohet ky korrigjim. DPT file txt e upload-on në serverin FTP të mundësuar nga MFE. në momentin që në serverin FTP dërgohet një file txt, nga drejtoria IT në MFE dërgohet me email tek Drejtoria e Operacioneve të Thesarit vetëm emri i filet.txt dërguar nga DPT dhe punonjësi ne Drejtorinë Operacionale kryen ekzekutimin e programit të ngarkimit të këtij file në SIFQ. Pra shkëmbimi i drejtpërdrejtë i të dhënave ndërmjet sistemit të DPT dhe sistemit të thesarit (SIFQ) nuk kryhet në mënyrë automatike.

14.1 Rekomandimi: MFE, AKSHI në bashkëpunimin me DPT të marrin masat për krijimin e mekanizmave të nevojshëm për automatizimin dhe ndërveprimin e hedhjes së të dhënave ndërmjet sistemeve DPT dhe SFIQ.

Në vijimësi

15. Gjetje nga auditimi: Nga auditimi u konstatua se në sistemin e thesarit ndodhin në mënyrë të përsëritur bug-e (error-e) të natyrave të ndryshme, si në vijim:

- Bankës së Shqipërisë, pas rakordimit me bankat e nivelit të dytë, e dërgon atë ditën e nesërme në sistemin e thesarit me anë *Swift Server* (*me data encryption*). Gjatë shpërndarjes së postës, ndodh që posta e një dege të caktuar i kalon një dege tjetër që nuk i përket asaj. Pasi sinjalizohet nga punonjësit e degës së thesarit, kryhet riparimi i kësaj anomalie (bug-u) me anë të një skripti i cili e dërgon postën në degën përkatëse në mënyrë që të kryhet rakordimi i degës së thesarit. Ky bug është akoma prezent në sistemin e thesarit duke krijuar një anomali të tilla.
- U konstatua 1 rast ku sistemi i thesarit nuk i ka dhënë vlerë fushës së numrit rendor të veprimit të kryer, "*DOC SEQUENCE VALUE*", fushë e cila duhet të plotësohet automatikisht nga sistemi (*vlerë default*).

Bug-e të tilla me natyrë të ngjashme janë krijuar edhe në periudha të mëparshme, edhe pse janë raste të izoluara.

- Bugs të natyrave të ndryshme ndodhin në procese të tjera të sistemit të thesarit gjatë plotësimit të transaksioneve PO nga një përdorues të cilit i ndërpritet procesi i punës duke i nxjerrë error.

15.1 Rekomandimi: Nga MFE dhe AKSHI të analizohen të gjitha rastet e bug-eve të ndryshme të sistemit, si dhe të merren masat e nevojshme për trajtimin dhe eliminimin e tyre në të ardhmen.

Menjëherë

16. Gjetje nga auditimi: Në sistemin SIFQ janë të implementuara metodat e sigurimit të kontrollit të inputit me qëllim sigurimin e një produkti cilësor final, por nuk ka raporte mbi saktësinë e outputit. Nga auditimi u konstatua se mungojnë kontrollet periodike të outputit. Kontrollet kryhen vetëm në rastet kur ka sinjalizime për ndonjë parregullsi. Në rastin e fushës *PERIOD_NAME* nuk ka funksion të kontrollit të inputit. Grupi i auditimit testoi inputin në këtë fushë duke vendosur vitin 2022, e cila nuk përbën vlerë logjike për këtë fushë. Kjo vlerë u pranua nga sistemi.

16.1 Rekomandimi: MFE dhe AKSHI të analizojë rastin e konstatuar nga grupi i auditimit duke e shtrirë verifikimin edhe në fushat e tjera, duke dhënë zgjidhje të cilat të shërbejnë jo vetëm për rregullimet momentale të problematikës, por gjithashtu për krijimin e një kontrolli paraprak të këtyre inputeve edhe në vazhdimësi.

Në vijimësi

17. Gjetje nga auditimi: MFE nuk ka zhvilluar burimet njerëzore të Auditit të brendshëm me njohuri të mjaftueshme mbi ***teknologjinë e informacionit*** dhe nuk ka planifikuar, kryer misione auditimi në sistemet e TI-së, në auditimet e kryera gjatë vitit 2018 në kundërshtim me nenet 14 dhe 8 të Ligjit nr. 114/2015 "*Për Auditimin e Brendshëm në sektorin publik*". "*Të kryejë auditime IT sipas përcaktimeve të nenit 4, pika 6 dhe nenit 9 dhe në përputhje me Standardet ndërkombëtare për praktikën profesionale të auditimit të brendshëm".*

17.1 Rekomandim: MFE të marri masa për zhvillimin e burimeve njerëzore të Auditit të brendshëm me njohuri të mjaftueshme mbi teknologjinë e informacionit dhe mbulimin me auditim të brendshëm IT të sistemeve IT, drejtorisë IT pranë MFE si dhe përdoruesit e sistemeve informatike në përputhje me përcaktimet ligjore

Në vijimësi

18. Gjetje nga auditimi: Auditimi i brendshëm në MFE:

- nuk ka akses dhe nuk shfrytëzon për auditim informacion nga sistemet informatike të MFE-së.
- nuk përdor teknika të auditimit të bazuara në teknologji informacioni, edhe pse në dispozicion të njësisë është edhe programi IDEA, i cili shërben për auditim të bazave të të dhënave.
- nuk vlerëson nëse qeverisja e teknologjisë së informacionit në MFE mbështet strategjitë dhe objektivat institucionale.

18.1 Rekomandim: Drejtoria TIK e AKSHI-t atashuar pranë MFE, në funksion te kryerjes se detyrimeve ligjore t'i sigurojë Auditit të Brendshëm akses në sistemet informatike të MFE.

Në vijimësi

19. Gjetje nga auditimi: Nga auditimi me zgjedhje të rastësishme të ambienteve të serverave të 4 degëve të thesarit, saktësisht Vlora, Fieri, Lezha dhe Shkodra, u konstatuan problematika të tilla si:

-mungesë e UPS për rastet e luhatjes apo ndërprerjes së energjisë elektrike;
-gjeneratorë jashtë funksionit;
-pajisjet IT (pc, printera all in one, etj) ishin të amortizuara
-kondicioneri për dhomën e serverave ishte jashtë funksionit duke rritur riskun e mbinxehjes së pajisjeve dhe serverit;

19.1 Rekomandimi: MFE dhe AKSHI të marrin masa për pajisjen dhe standardizimin e infrastrukturës IT të degëve të thesarit, me qëllim sigurimin e kushteve optimale për ofrimin e shërbimit dhe mbarëvajtjen e punës pa ndërprerje.

Në vijimësi

D. TË TJERA

Raporti i Përfundimtar i Auditimit dhe Vendimi i Kryetarit të KLSH-së, do të përcillen krahas subjektit të audituar (MFE dhe AKSHI-t) edhe tek Kuvendi i Shqipërisë (Kryetarit të Kuvendit, Komisionit të Ekonomisë dhe Financave) dhe Kryeministrit të Shqipërisë.

Me ndjekjen e zbatimit të detyrave dhe masave të përcaktuara në këtë vendim ngarkohet Departamenti i Auditimit të Teknologjisë së Informacionit.

Bujar LESKAJ

K R Y E T A R