VENDIM
Nr. 130, datë 17.2.2016

PËR DISA NDRYSHIME DHE SHTESA NË VENDIMIN NR. 289, DATË 17.5.2006, TË KËSHILLIT TË MINISTRAVE, "PËR ORGANIZIMIN DHE FUNKSIONIMIN E AGJENCISË SË LEGALIZIMIT, URBANIZIMIT DHE INTEGRIMIT TË ZONAVE/NDËRTIMEVE INFORMALE (ALUIZNI)", TË NDRYSHUAR

Në mbështetje të nenit 100 të Kushtetutës dhe të neneve 4 e 46, të ligjit nr. 9482, datë 16.2.2006, "Për legalizimin, urbanizimin dhe integrimin e ndërtimeve pa leje", të ndryshuar, me propozimin e ministrit të Zhvillimit Urban, Këshilli i Ministrave

VENDOSI:

Në vendimin nr. 289, datë 17.5.2006, të Këshillit të Ministrave, të ndryshuar, bëhen këto ndryshime dhe shtesa:

1. Pika 2 ndryshohet si më poshtë vijon:

"2. ALUIZNI ka Drejtorinë e Përgjithshme në Tiranë dhe drejtori varësie në çdo qendër qarku. Përjashtimisht, në qarqet Durrës, Fier dhe Vlorë, ALUIZNI ka përkatësisht dy drejtori, si dhe në Tiranë shtatë drejtori varësie.".

2. Pas pikës 4 shtohet pika 4/1 me këtë përmbajtje:

"4/1. Në përputhje me organikën dhe strukturën e miratuar sipas pikës 4 të këtij vendimi, drejtori i Përgjithshëm i ALUIZNI-t përcakton kompetencat territoriale dhe/ose lëndore të drejtorive të qarqeve Durrës, Vlorë, Fier dhe Tiranë.".

Kudo në vendim emërtimi "Ministria e Zhvillimit Urban dhe Turizmit", zëvendësohet me "Ministria e Zhvillimit Urban".

Ky vendim hyn në fuqi menjëherë dhe botohet në Fletoren Zyrtare.

KRYEMINISTRI
Edi Rama

ANEKSI I
I VENDIMIT TË KËSHILLIT TË MINISTRAVE NR. 69, DATË 27.1.2016, BOTUAR NË FLETOREN ZYRTARE NR. 13, DATË 5.2.2016

ANEKSI I

1. Siguria e operacioneve

Ofruesi i kualifikuar i shërbimit të besuar duhet të përdorë sisteme dhe produkte që janë të mbrojtura kundër modifikimeve dhe garantojnë sigurinë teknike dhe besueshmërinë e proceseve të mbështetura në to. Në veçanti:

a) Një analizë e kërkesave të sigurisë duhet të kryhet gjatë dizenjimit dhe fazës së specifikimeve të çdo projekti të zhvillimit të sistemeve nga ofruesi i kualifikuar i shërbimit të besuar për të garantuar sigurinë në sistemet e teknologjisë së informacionit.

b) Integriteti i sistemeve dhe informacionit duhet të mbrohet kundër viruseve, programeve keqdashëse dhe atyre të paautorizuara.

c) Mediumet e përdorura brenda sistemeve duhet të trajtohen në mënyrë të sigurt për t'i mbrojtur ato nga dëmtimi, vjedhja, dhe aksesi i paautorizuar.

ç) Procedurat e menaxhimit të mediumeve duhet t'i mbrojnë ato kundër vjetërimit dhe përkeqësimit të mediumeve brenda periudhës kohore që të dhënat janë të nevojshme për t'u ruajtur.

d) Procedurat duhet të përcaktohen dhe të zbatohen për të gjitha rolet e besuara dhe administrative që ndikojnë në sigurinë e sistemeve e të shërbimeve.

dh) Ofruesi i kualifikuar i shërbimit të besuar duhet të specifikojë dhe të zbatojë procedura të tilla që të garantojë se *security patches* aplikohen brenda një kohe të arsyeshme pasi ato janë bërë të disponueshme. Një *security patch* nuk duhet të aplikohet nëse do të paraqiste dobësi ose paqëndrueshmëri të mëtejshme që do të shmangnin përfitimet e aplikimit të tyre. Arsyeja për mosaplikimin e *security patches* duhet të dokumentohet.

2. Menaxhimi i incidenteve

Të përgjithshme

Aktivitetet e sistemit në lidhje me aksesin në sistemet IT, përdoruesi i sistemeve IT dhe kërkesat e shërbimit do të monitorohen. Në veçanti:

a) Aktivitetet e monitorimit duhet të marrin parasysh sensitivitetin e çdo informacioni të mbledhur ose të analizuar.

b) Aktivitetet anormale të sistemit që tregojnë një shkelje potenciale të sigurisë, duke përfshirë ndërhyrjen në rrjetin e ofruesit të kualifikuar të shërbimit të besuar, do të zbulohen dhe do të raportohen si emergjenca.

c) Sistemi IT i ofruesit të kualifikuar të shërbimit të besuar do të monitorojë ngjarjet e mëposhtme:

i) Ndezjen dhe fikjen e funksioneve të logimit;

ii) Vlefshmërinë dhe përdorueshmërinë e shërbimeve (services) thelbësore në rrjet dhe sistem.

ç) Ofruesi i kualifikuar i shërbimit të besuar do të veprojë menjëherë dhe në mënyrë të koordinuar që t'u përgjigjet incidenteve dhe do të kufizojë impaktin e shkeljes së sigurisë. Ofruesi i kualifikuar i shërbimit të besuar do të caktojë personelin me rol të besuar që të ndjekë të gjitha alarmet e ngjarjeve të një sigurie potencialisht kritike dhe të garantojë që incidentet përkatëse raportohen në përputhje me procedurat e tij të brendshme.

d) Ofruesi i kualifikuar i shërbimit të besuar do të përcaktojë procedura për të njoftuar palët e interesuara në përputhje me rregullat e çdo shkeljeje sigurie ose humbjeje të integritetit që ka një impakt të rëndësishëm në shërbimet e besuara të sigurta dhe mbi të dhënat personale të ruajtura në to.

dh) Në rastet kur shkelja e sigurisë ose humbja e integritetit ka efekte kundrejt personit fizik ose juridik të cilit i është ofruar shërbimi, ofruesi i kualifikuar i shërbimit të besuar do të njoftojë gjithashtu personin fizik ose juridik për shkeljen e sigurisë ose humbjen e integritetit pa vonesa.

e) Raportet e auditit do të analizohen dhe do të rishikohen rregullisht për të evidentuar prova të aktivitetit keqdashës dhe për të njoftuar personelin për ngjarje të mundshme kritike të sigurisë.

ë) Pas zbulimit të një cenueshmërie që nuk është adresuar më parë, ofruesi i kualifikuar i shërbimit të besuar do të marrë masat e duhura për ndreqjen e saj, brenda një periudhe të arsyeshme kohore. Nëse kjo nuk është e mundur, ofruesi i kualifikuar i shërbimit të besuar do të krijojë dhe do të zbatojë një plan për të ulur cenueshmërinë kritike ose do të dokumentojë bazën faktike për përcaktimin se cenueshmëria nuk kërkon ndreqje.

f) Raportime të incidentit dhe procedura përgjegjëse do të përdoren në mënyrë që dëmi nga incidentet e sigurisë dhe keqfunksionimi të minimizohet.

3. Kontrolli i aksesit

Aksesi në sistemin e ofruesit të kualifikuar të shërbimit të besuar do të jetë i mundur vetëm për personat e autorizuar. Në veçanti:

a) Kontrollet do të mbrojnë *domain*-et e rrjetit të brendshëm nga aksesi i paautorizuar duke përfshirë aksesin nga zotëruesit dhe palët e treta. *Firewall*-et duhet të konfigurohen në mënyrë të tillë për të parandaluar të gjitha protokollet dhe akseset që nuk nevojiten për funksionet e ofruesit të kualifikuar të shërbimit të besuar.

b) Ofruesi i kualifikuar i shërbimit të besuar do të administrojë aksesin e përdoruesve, operatorëve,

administratorëve dhe audituesve të sistemit. Administrimi do të përfshijë menaxhimin e llogarisë së përdoruesit, auditimin, modifikimin kohë pas kohe dhe heqjen e aksesit.

c) Aksesi tek informacioni dhe zbatimi i funksioneve të sistemit do të kufizohet në përputhje me politikat e kontrollit të aksesit. Sistemi do të sigurojë kontrolle të mjaftueshme të sigurisë kompjuterike, të roleve të besuara të identifikuara në praktikat e ofruesit të kualifikuar të shërbimit të besuar, duke përfshirë ndarjen e administrimit të sigurisë dhe funksionet e zbatimit. Veçanërisht, përdorimi i programeve mbështetëse do të kufizohet dhe do të kontrollohet.

ç) Personeli i ofruesit të kualifikuar të shërbimit të besuar do të identifikohet dhe do të autentifikohet përpara përdorimit të funksioneve kritike të lidhura me shërbimet. Personeli do të jetë përgjegjës për aktivitetet e kryera.

d) Të dhënat sensitive do të mbrohen kundër zbulimit nëpërmjet mjeteve të ripërdorshme të ruajtjes të të dhënave.