KRYEMINISTRIA

AGJENCIA KOMBËTARE PËR SIGURINË KOMPJUTERIKE (ALCIRT)

PROCEDURA E PËRSHKALLËZIMIT NË RAST TË NJË INCIDENTI KOMPJUTERIK

Miratuar me Urdhrin nr.131, datë 14.07.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT).

PROCEDURA E PËRSHKALLËZIMIT NË RAST TË NJË INCIDENTI KOMPJUTERIK

Përmbajtje

1. Hyrje

Menaxhimi efektiv i sigurisë kompjuterike përfshin një kombinim të parandalimit, zbulimit dhe reagimit. Përveç aplikimit të një sigurie të fortë, një sistem duhet të jetë në gjendje për t'iu përgjigjur incidenteve dhe të ketë të miratuara procedurat e duhura në rastin kur ndodh një incident që cënon sigurinë e informacionit. Trajtimi i incidenteve kompjuterike përbën një hap të madh në procesin e menaxhimit të sigurisë kompjuterike. Kjo procedurë është pjesë e një grupi procedurash dhe udhëzimesh që synojnë të ofrojnë një referencë si për menaxhimin ashtu edhe për stafin teknik dhe operacional, për të lehtësuar zhvillimin e një plani për trajtimin e incidenteve kompjuterike. Këto procedura dhe udhëzime do të përdoren gjithashtu për përgatitjen, zbulimin dhe përgjigjen që do të jepet gjatë këtyre incidenteve. Duke qenë se incidentet në sisteme të ndryshme kompjuterike kanë efekte të ndryshme dhe çojnë në pasoja të ndryshme, Institucionet (oficerët e sigurisë/CIRT) duhet të hartojnë një plan për menaxhimin e incidenteve kompjuterike, të përshtatur sipas nevojave të tyre operacionale dhe specifikave të sistemit që ata menaxhojnë.

2. Procedura e përshkallëzimit

Kjo procedurë përcakton mënyrën e përshkallëzimit të incidentit drejt menaxhimit të lartë dhe palëve të tjera të lidhura direkt me incidentin, për të siguruar marrjen e vendimeve në mënyrë të menjëhershme.

Në ecurinë e një incidenti, ku mund të shfaqen shumë çështje urgjente që duhet të adresohen, mund të jetë e vështirë gjetja e personit të duhur për të trajtuar një shumëllojshmëri çështjesh. Listat e kontaktit për adresimin e çështjeve ligjore, teknike, dhe menaxheriale duhet të jenë të përgatitura paraprakisht për të lehtësuar fazat e ndryshme të trajtimit të incidenteve kompjuterike.

Një procedurë e përshkallëzuar do të përcaktojë pikat e kontaktit (brenda dhe jashtë institucionit) me informacionin korespondues bashkangjitur, në nivele të ndryshme të njoftimit, bazuar në llojin dhe dëmin e shkaktuar nga incidenti.

Procedura e përshkallëzimit mund të jetë e ndryshme në varësi të llojit të incidentit, lidhur me pikat e kontaktit dhe veprimet që duhen ndjekur. Çdo institucion duhet të mbajë lista specifike

kontaktesh për të trajtuar lloje të ndryshme incidentesh që përfshijnë ekspertizë apo vendime të niveleve të ndryshme menaxheriale.

Në vazhdim jepen rekomandime në lidhje me procedurën e përshkallëzimit së bashku me procedurën e përshkallëzimit që duhet ndjekur në marrdhënie me palët e tjera jashtë Institucionit.

3. Palët që duhen njoftuar

Palët e përfshira në procedurën e përshkallëzuar duhet të evidentohen në varësi të llojit dhe të rëndësisë së incidentit, duke pasur parasysh kërkesat e sistemit.

Një incident si fillim mund të përfshijë vetëm stafin e brendshëm për të trajtuar problemin. Titullari mund të njoftohet në një fazë tjetër të trajtimit të incidentit. Nëse problemi nuk arrihet të zgjidhet, duhet të kërkohet mbështetja e palëve të tjera, të tilla si: kompania që ka mirëmbajtjen e sistemit, Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT) dhe nëse vlerësohet se incidenti përbën vepër penale të njoftohet Sektori Kundër Krimit Kompjuterik në Policinë e Shtetit.

Në çdo rast, pavarësisht sesi zgjidhet incidenti, Institucioni duhet ta raportojë atë tek ALCIRT duke plotësuar formën bashkëlidhur kësaj procedure. Të dhënat mbi incidentet e raportuara do të mblidhen nga ALCIRT në një bazë të dhënash:

a) Për t'u analizuar, me qëllim marrjen e masave për parandalimin e incidenteve të ngjashme në të ardhmen.
b) Për efekt evidentimi të incidenteve të ndodhura me qëllim mbajtjen e statistikave, të cilat japin një panoramë të përgjithshme të llojit, madhësise dhe frekuencës së incidenteve kompjuterike.

Çdo sistem duhet të ketë procedurën e vet të përshkallëzimit dhe pikat e kontaktit të cilat plotësojnë nevojat e tyre specifike operacionale.

Mund të njoftohen persona të ndryshëm në faza të ndryshme, në varësi të dëmtimit ose ndjeshmërisë së sistemit. Pikat e kontaktit që duhen përfshirë, por duke mos u kufizuar vetëm në to, janë:

4. Të brendshëm

a) Stafi mbështetës teknik dhe operacional;
b) Përgjegjësi i sistemit dhe/ose eprori;
c) Oficeri i sigurisë/CIRT i institucionit (nëse ka)
d) Stafi operacional i funksioneve apo sistemeve të përfshira në incident;
e) Koordinatori për informimin, përgatitjen dhe shpërndarjen nëpër media të informacionit.

5. Të jashtëm

a) Kompania që mirëmban sistemin, zhvilluesit e programeve, këshilluesit e sigurisë etj;
b) Ofruesit e Shërbimit (psh. ofruesit e shërbimit të internetit (ISP) etj.);
c) Përfaqësues nga ALCIRT;
d) Përfaqësues nga Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (IDP);
e) Përfaqësues nga Sektori kundër Krimit Kompjuterik pranë Policisë së Shtetit;
f) Subjektet dhe individët e prekur.

6. Lista e Kontakteve

Lista e kontakteve të palëve të përfshira duhet të përmbajë informacionin e mëposhtëm:

a) Emrin e personit përgjegjës;
b) Titullin e pozicionit të tij/saj;
c) Adresën e postës elektronike;
d) Numrin e tel (24 orë kontakt nëse është e nevojshme);
e) Numrin e faksit.

7. Procedura e përshkallëzimit

Forma e mëposhtme është procedura e përshkallëzimit për një incident kompjuterik.

Koha e raportimit	**Lista e kontakteve**	**Mënyra e kontaktit**
Brenda 15 minutave të para të incidentit	1. Përgjegjësi i sistemit TIK, 2. Stafi mbështetës, 3. Kompania e mirëmbajtjes së sistemit dhe ofruesit e shërbimit.	Linjat e tel në 24 orë të kompanisë/ofruesit të shërbimit [Tel/cel.]
Brenda 30 minutave të incidentit	Oficeri i sigurise/CIRT i institucionit (nëse ka)	Tel/cel.
Brenda 60 minutave të incidentit	Oficeri i Sigurisë duhet të njoftojë ALCIRT dhe të ofrojë një formë raportimi paraprake (bashkëngjitur) sa më shpejt të jetë e mundur	Tel/cel. ose postë elektronike
Çdo 60 minuta në vazhdim	Të gjithë të sipërpërmendurve për përditësimin e statusit	Cel. ose postë elektronike
Periodikisht	Oficeri i Sigurisë përditëson ALCIRT	Postë Elektronike
Pas rikthimit të sistemit (brenda një jave)	Oficeri i Sigurisë duhet të ketë formuluar një raport pas-incidenti (bashkëngjitur) për regjistrim në bazën e të dhënave të ALCIRT	Postë Elektronike
Nëse incidenti, sipas oficerit të sigurisë/CIRT, përbën vepër penale	Denoncohet në Polici për t'u hetuar më tej	Me linja të paracaktuara
Nëse janë përfshirë në incident të dhënat personale	Njoftohet Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (IDP) (kur është e mundshme njoftohen individët e prekur)	Me linja të paracaktuara

Raporti duhet të përfshijë informacionin e mëposhtëm:

- Informacion të detajuar të problemit çfarë, kur, si ndodhi dhe kohëzgjatja.
- Tregon nëse sistemi është nën sulm;
- Tregon nëse sulmuesi, nëse ka, është ende aktiv në sistem;
- Tregon nëse sulmi është nga burime lokale;
- Gjendja e përditësuar lidhur me rikthimin e sistemit.

- **ANEKSI 1**

Forma e Raportimit Paraprak të Incidentit Kompjuterik

Informacioni Shoqërues	
Emri i Institucionit:	
Përshkrim i shkurtër në lidhje me sistemin e prekur: (funksione, URL etj):	
Vendndodhja fizike e sistemit të prekur: ☐ Brenda Institucionit ☐ Jashtë Institucionit (ambienti i ofruesit të shërbimit) **Sistemi administrohet / përdoret nga:** ☐ stafi i brendshëm ☐ përdorues fundor ☐ ofrues i jashëm i shërbimit	
Informacion për raportimin e brendshëm	
Emri:	**Titulli:**

Kontakti i Zyrës:	**Kontakti në 24 orë:**
Adresa Elektronike:	**Numri i Faksit:**
Detaje rreth Incidentit	
Ora/Data (Zbulimit):	**Ora/Data (Raportuar në ALCIRT):**
Shenjat e Incidentit:	
Pasoja: ☐ Dëmtimi i Website-it ☐ Shërbimi i Ndërprerë (sulm i mohimit të shërbimit (DOS), mail bomb, dështim i sistemit)	

☐ Infektim masiv i kompjuterit nga viruset, hoaxes, sulme nga kode me qëllim të keq

☐ Humbje/dëmtim/ndryshim i paautorizuar i informacionit

☐ Kompromentim/rrjedhje e informacionit sensitiv

☐ Ndërhyrje/qasje e paautorizuar

☐ Të tjera, ju lutemi specifikojeni: _____

Ju lutemi jepni detaje mbi periudhën e ndikimit dhe ndërprerjes së shërbimit, nëse ka:

_____

Janë përfshirë në incident të dhënat personale?

☐ Po

☐ Jo

Nëse Po, kur është njoftuar zyra e Komisionerit për Mbrojtjen e të Dhënave Personale:

_____(data/ora)

Palë të tjera të njoftuara:

1. **_____ _____(data/ora)**
2. **_____ _____(data/ora)**
3. **_____ _____(data/ora)**

4. _____ _____(data/ora) **5. _____ _____(data/ora)**
Veprimet e Ndërmarra:
Gjendja Aktuale e Sistemit:
Informacione të Tjera:

Forma e mëposhtme është krijuar për të lehtësuar marrjen e informacionit të incidenteve kompjuterike. Në qoftë se ju besoni që jeni i përfshirë në një incident kompjuterik, lutem plotësoni – sa më shumë të jetë e mundur – formën e mëposhtme, dhe dërgojeni tek adresa contact@cirt.gov.al.

Ky informacion do të trajtohet në mënyrë konfidenciale.

Seksioni:Të dhënat e kontaktit të raportuesit	
Emri (i kërkuar):	
Mbiemri(i kërkuar):	
Adresa e email (i kërkuar):	
Numri i telefonit (i kërkuar):	
tjetër (numër Fax, …):	
Cfarë lloj institucioni/organizate po raporton këtë incident? Lutemi, citoni emrin e lloj institucioni/organizate (i kërkuar):	Zgjidhni o Qeverisje Qëndror o Qeverisje Lokale o Sektori privat o Sektori i huaj o Personal
Cili është efekti tek organizmi raportuesion? (i kërkuar):	Zgjidhni o Nuk e di o Asnje o Minimal o I ulët o I mesëm o I lartë

Cfarë lloj asistence po kërkoni në këtë moment (i kërkuar):	Zgjidhni o Asnjë o Kontaktim o Ndjekje
Përshkruani statusin aktual apo zgjidhjen e këtij incidenti. (i kërkuar):	Zgjidhni o Po ndodh o Nën kontroll o Ka ndodhur o Rrezik i ardhshëm o Nuk e di
Cila është ora e përafërt kur ka ndodhur incidenti? (Koha lokale):	
Kur u zbulua incidenti? (Koha lokale):	
Seksioni : Detaje të Incidentit	
Lutemi bëni një përshkrim të shkurtër të incidentit dhe pasojave(i kërkuar)	
Makina e prekur (i kërkuar)	
• Adresa IP ose emri i makinës (hostnames) _____ • Qëllimi i makinës _____ • Zona e Kohës _____	
Burimi i sulmit (lëreni bosh nqs nuk e dini):	
• Adresa IP ose emri i makinës (hostnames) _____	

• Qëllimi i makinës _____ • Jeni në kontakt? _____	
Versioni i programit (lëreni bosh nqs nuk e dini):	
Të dhënat dhe mënyrat e ndërhyrjes (lëreni bosh nqs nuk e dini):	
Dobësia e shfrytëzuar (lëreni bosh nqs nuk e dini):	
Sa sisteme janë prekur nga ky incident(lëreni bosh nqs nuk e dini):	
Si "site" janë prekur nga ky incident(lëreni bosh nqs nuk e dini):	
Të dhënat e përfshira në incident a ishin të enkriptuara	○ Jo ○ Nuk e di ○ Po ○ Jo
A ka pasur pasoja për infrastrukturën kritike nga ky incident?	○ Jo ○ Nuk e di ○ Po ○ Jo
Kush ishte metoda kryesore e përdorur për të identifikuar incidentin?	○ Nuk e di ○ Platë të treta

	○ Administratori ○ Programe AntiSpyëare ○ Programe AntiVirus ○ IDS ○ Log Revieë ○ Përdorues ○ tjetër
Nqs është e mundur , ju lutem përfshini 5-10 rreshta të "time-stamped logs" në "plain ASCII text".(psh.,CSV).	
Tjetër|	

Fluksi i punës për përshkallëzimin e një incidenti komjuterik