Republika e Maqedonisë së Veriut

Agjencia për mbikëqyrje të financimit kapital të sigurimit pensional
Nr. 08-939/7
30.9.2021-viti
SHKUP

Republika e Maqedonisë së Veriut
Agjencia për mbikëqyrje të financimit kapital të sigurimit pensional

Rregullat për sigurinë e informacionit të Agjencisë për mbikëqyrje të financimit kapital të sigurimit pensional

Koha e sistemit dhe sinkronizimi i orës

Të gjitha shënimet për log regjistrim duhet të përmbajnë kohën e sistemit. Ora e sistemit në sistemet e TI duhet të sinkronizohet me kohën e saktë të dakorduar të referencës (koha standarde zyrtare) në intervale të rregullta.

Proceset afariste

Pronari i procesit afarist është përgjegjës për mbrojtjen e informacioneve dhe të dhënave në kuadër të procesit afarist, si p.sh për mënyrën dhe vëllimin e zbulimit të informacioneve nga procesi afarist.
Nëse informacioni që ka nevojë për mbrojtje shkëmbehet gjatë proceseve afariste, atëherë pronarët e proceseve afariste duhet së bashku të përcaktojnë se si të sigurohet mbrojtja e përhershme e informacionit.

Përdorimi i mediave për të dhëna

Nëse mediat për të dhëna të sistemeve të TI, veçanërisht mediat për transferimin e të dhënave, përdoren në mënyrë të pakujdesshme ose të papërshtatshme, kjo mund të rezultojë në zbulimin e paqëllimshëm të informacionit për persona të paautorizuar ose humbjen e të dhënave.
Duhet të vendosen procedura përkatëse operative për t'u ofruar të gjithë të punësuarve udhëzime specifike për të vepruar me mediat për të dhëna, dhe sidomos për mediat për transferimin e të dhënave.
Mediat për të dhënat duhet të përdoren dhe ruhen në përputhje me kërkesat për mbrojtjen e prodhuesit.

Lidhjet VPN (qasje në distancë)

Që të qasemi në lokacionin dytësor nëpërmjet një lidhjeje VPN (Virtual Private Network - Rrjeti privat virtual) në rrjetin e brendshëm, duhet të përdoret një teknikë që urdhëron njohje të fshehtë dhe pronësi (vërtetim të autenticitetit me dy faktorë) si një kërkesë minimale.

Shkatërrimi i të dhënave

Kur sistemet e TI, për shembull pajisjet siç janë kompjuterët e lëvizshëm, kompjuterat laptop dhe telefonat celularë si dhe serverët, sistemet për ruajtje dhe bibliotekat për bekap janë hequr nga përdorimi, duhet të pamundësohet që informacionet e ndjeshme të bien në duar të gabuara (sipas Rregullores për masat teknike dhe organizative për të siguruar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale). Duhet të respektohen rregullat e mëposhtme të përgjithshme:

- Fshirje e sigurtë duke shkruar plotësisht mbi të dhënat paraprake të mediave për të

dhëna me të dhëna të padëmshme siç janë sekuencat e biteve në mënyrë të rastësishme, ose shkatërrim fizik i medias për të dhëna me prerjen, copëtimin ose me përdorimin e pajisjeve për demagnetizimin e tyre. Kjo e fundit do të zbatohet veçanërisht për mediat defekte për të dhëna, ku të dhënat nuk do të jenë në gjendje të shkatërrohen me përdorimin e "fshirjes së sigurtë".

- Shkatërrimi i të dhënave dhe fshirja e të dhënave duhet të realizohet ekskluzivisht me përdorimin e teknikave dhe mjeteve që do të sigurojnë që informacioni origjinal nuk mund të rikthehet.

Sigurimi i shërbimeve nga palët e treta

Në rastet kur shërbimet sigurohen nga palë të treta, kërkesat për mbrojtjen dhe sigurinë e të dhënave të cilat duhet të precizohen për sistemet e TI përkufizohen dhe kontrollohen përmes Kontratave me ofruesin e shërbimeve (kontraktuesin), për të cilët do të zbatohen kërkesat e mëposhtme:

- Kontratat për shërbimet e TI me palët e treta duhet të përmbajnë përshkrime të sakta të të gjitha aspekteve të mbrojtjes së të dhënave dhe që janë relevante për sigurinë, si dhe kërkesat për sigurimin e shërbimeve, veçanërisht mbrojtjen teknike dhe organizative të të dhënave dhe kontrollet e sigurisë të cilat duhet të realizojë kontraktuesi.
- Kur ofruesve të shërbimeve u është dhënë detyra për përpunimin e të dhënave personale, kërkesat përkatëse për mbrojtjen dhe sigurinë e të dhënave duhet të të specifikohen hollësisht në një kontratë të veçantë për përpunimin e të dhënave për të cilën është anagazhuar kontraktuesi.
- Kontratat me ofruesit e shërbimeve duhet të përmbajnë dispozitat e mëposhtme për aspektet e mbrojtjes dhe sigurisë së të dhënave, veçanërisht për sistemet kritike të TI;
  - E drejta e përdoruesit për të inspektuar dokumentacionin operacional dhe rrjedhat e punës;
  - Sigurimi i raporteve dhe evidenca nga ana e kontraktuesit;
  - Autorizimi i përdoruesit t'i jap udhëzime kontraktuesit;
  - Integrimi i nënkontraktuesve;
  - E drejta e përdoruesit ose e ndonjë pale të tretë të angazhuar nga përdoruesi për t'i kontrolluar sistemet e TI në lokacionin e kontraktuesit, duke përfshirë të drejtën e qasjes në ndërtesa dhe objekte dhe për të kontrolluar sistemet përkatëse të TI;
  - Metoda e përcjelljes së informacionit në lidhje me incidentet e lidhura me mbrojtjen dhe sigurinë e të dhënave, si dhe për bashkëpunim në rast të problemeve ose incidenteve serioze;
  - Paraprakisht do të vendosen në dispozicion rregullat e përcaktuara të cilat i referohen mbrojtjes dhe sigurisë së të dhënave.

Politika e ekranit të pastër dhe tavolinës së pastër

Informacionet rreptësisht konfidenciale dhe konfidenciale duhet të mbyllen kur nuk nevojiten dhe kur zyra është e zbrazët.

Kompjuterët dhe terminalet duhet të jenë në gjendje "log off" ose të mbrojtur me mekanizmin "screen lock" (ctrl, alt, del dhe enter/lock computer) kur nuk punon në to. Të gjitha screen-saver duhet të jenë të mbrojtura me fjalëkalim. Një përjashtim nga kjo rregull mund të bëhet vetëm me miratim nga ana e Kryetarit të këshillit të ekspertëve të Agjencisë.

Përgatiti: Emilija Ramova
16.8.2021 E. Ramova

Kryetar i Këshillit të ekspertëve
Maksud Ali