Priloga 8: Računalniška varnost

1. Upravljavec mora v skladu z zahtevami iz te priloge zagotoviti, da so digitalni računalniški in komunikacijski sistemi ter mreže ustrezno zaščitene pred računalniškimi napadi, vključno s projektno oceno ogroženosti.
2. Upravljavec mora zaščititi digitalne računalniške in komunikacijske sisteme in omrežja, povezane z:
   a) varnostnimi funkcijami in funkcijami, pomembnimi za varnost,
   b) funkcijami v povezavi z varovanjem,
   c) nalogami v zvezi s pripravljenostjo na izredni dogodek, vključno z oddaljenimi komunikacijami, in
   č) podpornimi sistemi in opremo, ki bi lahko, če so ogroženi, negativno vplivali na varovanje, varnost ali pripravljenost na izredni dogodek.
3. Upravljavec mora zavarovati sisteme in omrežja, opredeljene v točki 2 te priloge, pred računalniškimi napadi, ki bi:
   a) negativno vplivali na celovitost ali zaupnost podatkov in/ali programske opreme,
   b) preprečili dostop do sistemov, storitev in/ali podatkov ter
   c) negativno vplivali na delovanje sistemov, omrežij in pripadajoče opreme.
4. Da bi izpolnili zahteve iz zgornjih točk te priloge, mora upravljavec:
   a) analizirati digitalne računalniške in komunikacijske sisteme in omrežja ter opredeliti sredstva, ki morajo biti zaščitena pred računalniškimi napadi, da zadosti zahtevam iz zgornjih točk tega poglavja;
   b) vzpostaviti, izvajati in vzdrževati program računalniške varnosti za zaščito sredstev, opredeljenih v točki 4.a te priloge, in
   c) vključiti program računalniške varnosti v načrt fizičnega varovanja kot njegov sestavni del.
5. Program računalniške varnosti mora biti zasnovan tako, da se:
   a) varnostne kontrole izvajajo tako, da se sredstva, opisana v točki 4.a te priloge, zavarujejo pred računalniškimi napadi,
   b) uporablja in vzdržuje strategije obrambe v globino za zagotavljanje odkrivanja, odzivanja in odgovarjanja na računalniške napade,
   c) ublaži škodljiv vpliv računalniških napadov in da se
   č) zagotovi, da zaradi računalniških napadov ni negativnih vplivov na funkcije pomembnih sredstev, opredeljenih v točki 4.a te priloge.
6. Kot del programa računalniške varnosti upravljavec:
   a) zagotovi seznanjenost osebja in zunanjih izvajalcev z računalniškimi varnostnimi zahtevami ter ustrezno usposabljanje, ki je potrebno za opravljanje dodeljenih nalog in odgovornosti;
   b) ovrednoti in upravlja računalniška tveganja;
   c) zagotovi, da so kakršnekoli spremembe sredstev, opisane v točki 4.a te priloge, predhodno ovrednotene tako, da se cilji uspešnosti za računalniško varnost, opisani v 2. točki te priloge, lahko dosežejo.
7. Program računalniške varnosti mora opisovati, kako se bodo zahteve iz te priloge izvajale, hkrati pa mora upoštevati posebnosti določenega objekta, ki vplivajo na izvajanje.
8. Program računalniške varnosti mora vsebovati ukrepe v primeru izrednega računalniškega dogodka in povrnitev v normalno stanje po računalniškem napadu. Program računalniške varnosti mora opisati, kako upravljavec:

a) ohrani sposobnost za pravočasno odkrivanje in odzivanje na računalniške napade,
b) ublaži posledice računalniškega napada,
c) odpravi izkoriščene ranljivosti in
č) obnovi prizadete sisteme, omrežja oziroma opremo, ki jih je prizadel računalniški napad.

9. Upravljavec mora vzpostaviti in vzdrževati pisne postopke za izvajanje programa računalniške varnosti.