REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Priporočene vsebine za osnovno usposabljanje s področja informacijske in kibernetske varnosti

KAZALO

I. UVOD

Informacijska in kibernetska varnost sta ključna temelja zanesljivega in zakonitega delovanja organizacij v javnem in zasebnem sektorju. Ker je posameznik, ki upravlja z informacijsko-komunikacijsko tehnologijo pogosto prva tarča zlonamerne aktivnosti, morajo imeti zaposleni osnovno znanje o prepoznavanju in preprečevanju varnostnih groženj.

V skladu z Zakonom o informacijski varnosti (Uradni list RS, št. 40/25) morajo zavezanci iz zakona izvajati redna usposabljanja za ozaveščanje zaposlenih. Z željo, da bi usposabljanja dosegla namen, da zaposleni pridobijo dovolj znanj in spretnosti, s katerimi se usposobijo za prepoznavanje tveganj za informacijsko in kibernetsko varnost ter njihovega vpliva na storitve, ki jih opravlja subjekt, Urad Vlade Republike Slovenije za informacijsko varnost priporoča naslednji pristop pri izvedbi osnovnega usposabljanja oziroma ozaveščanja zaposlenih:

- **Način izvedbe:** spletni tečaji, e-učenje ali delavnice v živo, v obsegu od 30 do 60 minut.
- **Prilagajanje glede na vloge:** vsebina se lahko dopolni z vidika delovnega mesta zaposlenega.
- **Redno obnavljanje znanja:** najmanj enkrat letno ali ob pomembnih spremembah delovanja subjekta oziroma incidentih.
- **Preverjanje znanja:** vključitev kvizov, izdaja in hramba potrdil o udeležbi.
- **Krepitev varnostne kulture:** z dodatnim ozaveščanjem (e-nasveti, kratki videi, simulacije *phishing* napadov, ipd.) skozi celo leto.

II. KLJUČNE PRIPOROČENE VSEBINE USPOSABLJANJA

1. Splošna znanja za vse zaposlene

- **Prepoznavanje spletnih prevar**
    - *Phishing*, poslovne goljufije, lažne spletne trgovine, sumljivi e-poštni naslovi, metode socialnega inženiringa.
    - Kaj storiti ob sumu zlorabe.
- **Zlonamerna programska oprema (*malware*)**
    - Nevarnosti zlonamernih priponk in okužene povezave.
    - Pomembnost posodabljanja programske opreme.
    - Kaj storiti ob sumu okužbe naprave z zlonamerno programsko opremo.
- **Gesla in dostopi**
    - Uporaba močnih gesel, redno menjavanje, geselski upravljalniki.
    - Večfaktorska avtentikacija kot obvezna zaščita ključnih sistemov.
    - Postopek o sumu zlorabe poverilnic.
- **Varnost naprav in omrežij**
    - Varna raba naprav, zaklepanje zaslona, zaščita mobilnih naprav, uporaba zaščitenih omrežij.
    - Previdnost pri delu od doma ali na službeni poti.
    - Prepoznava nenavadnega obnašanja naprav.

- **Varno ravnanje z informacijami**
    - Prepoznavanje zaupnih podatkov, zaščita osebnih podatkov in poslovnih informacij.
    - Varnost fizičnih dokumentov in nadzor nad prenosljivimi mediji (npr. USB ključki).
    - Postopek o zaznavi suma zlorabe informacij.

2. <u>Dopolnitve glede na delovno vlogo</u>

- **Administrativno in finančno osebje**
    - Goljufije z lažnimi zahtevki za nakazila, spremembe bančnih podatkov, t. i. direktorske prevare.
- **Zaposleni v nabavi, prodaji in marketingu**
    - Pasti pri spletni komunikaciji z dobavitelji, lažne ponudbe, zloraba družbenih omrežij.
- **IT osebje in skrbniki informacijskih sistemov**
    - Napredna tehnična znanja: posodobitve, zaščita omrežij, nadzor nad dostopi, varnostno kopiranje in restavriranje podatkov, zaznavanje incidentov in odziv na njih, dnevniški zapisi in revizijske sledi.
    - Znanja in spretnosti za oceno praks obvladovanja tveganj.
- **Vodstveni kader**
    - Odgovornost za upravljanje z viri in tveganji, dodeljevanje sredstev, strateško ukrepanje ob incidentih, varnostna kultura v kolektivu.

III. ZAKLJUČEK

Usposabljanje zaposlenih s področja informacijske varnosti je ključni gradnik celovite zaščite informacijsko-komunikacijskih sistemov organizacije. Z ustreznim usposabljanjem zaposlenih zmanjšamo tveganje za napake, ki lahko vodijo v resne varnostne incidente. Sistematičen pristop k ozaveščanju zaposlenih prispeva k večji stopnji varnostne kulture, dvigu odpornosti organizacije na grožnje in skladnosti z zakonodajo.

Napadalci se usmerjajo na tako imenovani človeški faktor, ker je pogosto lažje zavesti posameznika kot zaobiti ali prebiti napredne tehnične zaščite. Zaposleni tako pogosto nehote postanejo vektor napada (prevarani z lažno pošto, okuženimi priponkami, škodljivimi spletnimi povezavami, ipd.).

Odgovorne osebe se morajo zavedati, da se varnost organizacije začne pri posamezniku, saj vsaka odločitev, še tako majhen klik ali previdnost zaposlenega lahko pomembno vpliva na zaščito, nemoteno delovanje organizacije in zagotavljanje storitev celotne organizacije.