NOTRANJI VARNOSTNI INCIDENTI IN TVEGANJA POVEZANA Z DELOM OD DOMA

OPIS

Zaščita programske opreme, dokumentov in podatkov ter postopkov pri delu na delovnem mestu in od doma

Tekom poslovanja organizacije nastane veliko pomembnih dokumentov in se zbira veliko podatkov, ki so vedno bolj v digitalni obliki. Za njih v primerjavi s fizičnim gradivom obstaja veliko večje tveganje za izgubo, uničenje ali preprosto krajo. Največkrat se bojimo, da bi brez teh elektronskih dokumentov in podatkov ostali zaradi namenskih varnostnih incidentov od zunaj, pozabljamo pa na tveganja znotraj organizacije. Vaši zaposleni do elektronskih dokumentov in podatkov, ki jih hranite v različnih registrih in aplikacijah, dostopajo v skladu s politiko dostopa, kljub temu pa se dogaja, da dokumenti oz. podatki preprosto izginejo – se jih po pomoti izbrišejo ali spremenijo. Še večje tveganje pa so tisti zaposleni, ki iz različnih razlogov to delajo namensko, naj bodo to nezadovoljni zaposleni ali pa celo taki, ki izvajajo krajo poslovnih informacij.

Ta tveganja so v trenutnih razmerah, ko veliko zaposlenih dela od doma, kjer ne poznamo tehničnega okolja, še toliko večja – vi pa jim morate posvetiti še toliko več pozornosti.

Udeležite se usposabljanja, ki ga pripravljamo v sodelovanju s strokovnjakoma na področju raziskovanja varnostnih incidentov.

Praktična online delavnica je namenjena vsem zaposlenim s področja upravljanja informacijske varnosti, ki morate zagotoviti ustrezne preventivne ukrepe za zaščito programske opreme, elektronskih dokumentov in shranjenih podatkov, v primeru suma neustreznega ravnanja zaposlenega pa ugotoviti, kaj se je z njimi zgodilo in čim hitreje omejiti ter odpraviti nastalo škodo. V primeru ugotovljenih napak in posledično škode pa tudi morate poiskati dokaze ter jih primerno zavarovati.

Pomembno je, da se udeležite praktične delavnice, ker boste:

- seznanjeni s **tveganji informacijske varnosti pri delu od doma oziroma na daljavo;**
- **vzpostavili sistem zaščite** dokumentov in podatkov v elektronski obliki;
- **poznali tveganja in predvideli možne scenarije** izgube, uničenja ali kraje;
- **analizirali** morebitno **nastalo škodo** in **izbrali** primerne ukrepe za opravo posledic.

Prav tako boste dobili **odgovore na vaša konkretna vprašanja,** ki izhajajo iz vaše vsakdanje prakse: v razgovoru s strokovnjaki pridobite nasvete za najustreznejše rešitve na področju prepoznavanja in preprečevanja varnostih incidentov na področju informacijske varnosti.

Online seminar spremljate preko lastnega računalnika, **ni vam treba zapuščati delovnega mesta ali doma.** Vprašanja postavljajte sproti, predavatelja bosta nanje odgovarjala sproti ali na koncu.

Vprašanja nam pošljite vnaprej – na naslov: petra.ertl@forum-media.si

- Upravljanje incidentov
- Varstvo osebnih podatkov in poslovnih skrivnosti
    - Osebni računalniki, delovno okolje
    - Mobilne naprave
    - Komunikacijska oprema

    - Fizični mediji, papirna dokumentacija
    - Okuženi in odtujeni mediji – USB ključi
- Delo od doma ali oddaljene lokacije
    - Tveganja
    - Zagotavljanje ustreznega delovnega okolja
    - Sledljivost vstopa v informacijski sistem delodajalca in omejitve (tehnične, časovne …)
- Ukrepanje v primeru incidentov
    - Preiskava incidenta (ugotavljanje trenutnega stanja in rekonstrukcija dogodkov)
    - Zavarovanje dokazov
    - Nadaljnji pravni ukrepi
    - Kraja elektronskih dokumentov in podatkov (sledljivost shranjevanja; kopiranja) zunaj in znotraj organizacije
    - Aplikacije za hrambo podatkov in dokumentov
    - Prenarejanje in ponarejanje informacij in dokumentov
    - Revizijske sledi (dokumenti, informacije, aplikacije)
    - Revidiranje procesov z namenom dokazovanja prevar (kraje, brisanje, manipulacija z dokumenti in podatki v aplikacijah, pregled revizijskih sledi …)
    - Podpora zunanjega izvajalca (detektiva, revizorja, javnih pooblaščenih organov …)
- Vaje na konkretnih primerih iz prakse

AVTORJI

mag. Filip Božič

Mag. Filip Božič je certificiran etični heker in vodilni presojevalec za področje upravljanja varovanja informacij ter neprekinjenega poslovanja. Predava na usposabljanju za DPOje ter številnih konferencah in izobraževalnih programih. Široko tehnično znanje na področju informatike že dve desetletji nadgrajuje z organizacijskimi pristopi k ščitenju informacijskega premoženja v Sloveniji in širše.

Žiga Primc

Žiga Primc je certificirani etični heker (CEH), detektiv z licenco št. 162 in varnostni strokovnjak za varnost informacij v organizaciji, ki že vrsto let preiskuje in rešuje vdore v organizacije, kraje poslovnih skrivnosti, izsiljevanja organizacij in izobražuje zaposlene v organizacijah na področju varovanja informacij vseh oblik.

SPLOŠNI POGOJI

Prejeti predračun je treba poravnati najmanj tri dni pred izvedbo spletnega seminarja. Za proračunske porabnike veljajo plačilni pogoji v skladu z zakonodajo o javnih plačilih. Pisna odpoved udeležbe je mogoča najkasneje tri delovne dni pred izvedbo spletnega seminarja. Udeleženci, ki po tem roku prekličejo udeležbo ali se spletnega seminarja ne udeležijo, niso upravičeni do povrnitve kotizacije oz. so dolžni poravnati celotno kotizacijo. Lahko pa se spletnega seminarja udeleži drugi udeleženec. Pridržujemo si pravico do odpovedi spletnega seminarja – v tem primeru kotizacijo povrnemo v celoti.