Procijenite zrelost i sposobnosti svojeg sigurnosno – operativnog centra

Kibernetička sigurnost jedna je od prioritetnih tema brojnih organizacija. Prema PwC-ovom globalnom istraživanju o povjerenju u digitalno okruženje za 2025. godinu, više od tri petine (66 %) direktora sektora informacijskih tehnologija smatra kibernetičke rizike najznačajnijim rizicima koje će njihova organizacija nastojati otkloniti u sljedećih 12 mjeseci. Zato je važno osigurati **učinkovitost i zrelost sigurnosnih operacija**, kako pojedinih organizacija, tako i rješenja koja nude pružatelji upravljanih sigurnosnih usluga (engl. Managed Security Service Providers, MSSP).

PwC-ovi stručnjaci u tu svrhu koriste **metodologiju SOC-CMM** (Security Operations Center – Capability Maturity Model) kojom možete steći strukturiran **pregled vašeg sigurnosno – operativnog centra** (engl. Security Operations Center, SOC). Naši stručnjaci vam mogu pomoći u utvrđivanju ključnih područja za poboljšanje i dati vam konkretne smjernice kako biste mogli postići više razine operativne zrelosti.

Procjena u skladu s metodologijom SOC-CMM može pomoći:

Organizacijama:

- povećati otpornosti na kibernetičke prijetnje
- osigurati usklađenost s regulativama (NIS2, Zakon o kibernetičkoj sigurnosti), najboljim praksama i međunarodnim standardima
- pomoći menadžmentu donositi informirane odluke o investicijama u kibernetičku sigurnost
- povećati povjerenje dionika, klijenata i regulatornih tijela u sposobnost organizacije da učinkovito upravlja sigurnosnim prijetnjama i incidentima
- provjeriti kvalitetu ugovorene usluge i procijeniti mogućnosti poboljšanja

Pružateljima upravljanih sigurnosnih usluga:

- provjeriti i osigurati visoku razinu kvalitete svojih usluga
- bolje pozicionirati svoju uslugu na tržištu
- planirati poboljšanja svojih usluga
- optimizirati resurse i poboljšati učinkovitost
- izgraditi povjerenje klijenata

Procjena sigurnosno – operativnog centra u skladu s metodologijom SOC-CMM

Model SOC-CMM sastoji se od 5 domena i 26 aspekata, od kojih se svaki procjenjuje pomoću posebnog alata.

U procjeni zrelosti uključene su sljedeće domene:

1. Poslovanje – kako su poslovni zahtjevi prevedeni u zahtjeve za sigurnošću i upravljanje incidentima
2. Ljudi – broj i vrsta ljudskih kompetencija na raspolaganju
3. Proces – jesu li uspostavljeni svi potrebni procesi i koja je njihova zrelost
4. Tehnologija – sposobnost korištene tehnologije
5. Usluge – sposobnost glavnih usluga koje davatelj pruža

Procjenu provode PwC-ovi stručnjaci s dugogodišnjim iskustvom na području operativne kibernetičke sigurnosti, certificirani za procjenu pomoću metodologije SOC-CMM. Naš tim podatke prikuplja u okviru radionica i intervjua s glavnim dionicima, pregledom krovne i procesne dokumentacije i uvidom u korištenu tehnologiju, nakon čega dokumentira dokaze kojima se potkrepljuju konačni nalazi te donosi stručno mišljenje i ocjena.

Ova metodologija omogućuje kvantitativno mjerenje zrelosti sigurnosno – operativnog centra, osiguravajući objektivno ocjenjivanje i donošenje odluka temeljenih na podacima.

PwC-ov tim

Igor Hitrec

Viši menadžer, tim za upravljanje informacijskim rizicima, PwC Hrvatska
SOC-CMM Certified Assessor (SOC-CA)
igor.hitrec@pwc.com

Arijan Šimek

Viši konzultant, tim za upravljanje informacijskim rizicima, PwC Hrvatska
SOC-CMM Certified Assessor (SOC-CA)
arijan.simek@pwc.com