OPLEIDING #ICT EN INFORMATIEMANAGEMENT

gdpr awareness – in-house opleiding

informatieveiligheid binnen uw organisatie

omschrijving

INTRODUCTIE

Openbare besturen (steden, gemeenten, OCMW's, Politiezones, Brandweer, ...) en andere non en social profit organisaties hebben een DPO of Informatieveiligheidsconsulent in dienst. Deze persoon dient te waken over de informatieveiligheid binnen de organisatie. Eén van de taken van een DPO is o.a. het opmaken (en in uitvoering brengen) van een informatieveiligheidsplan.

Eén van de jaarlijks terugkerende actiepunten - in dit veiligheidsplan - is alle medewerkers van de organisatie (op terugkerende tijdstippen) te informeren betreffende de potentiële risico's die de informatieveiligheid in gevaar kunnen brengen. Onder het motto 'voorkomen is beter dan genezen (preventie)' is het organisatiebreed (laten) organiseren van een infosessie rond deze thema's een standaard" best practice" geworden die reeds zijn nut voldoende bewezen heeft.

We ontvangen heel wat vragen van organisaties die deze infosessie(s) willen laten organisen door Escala. Het is als DPO immers niet altijd evident om als rechtstreeks betrokkene bij het dagdagelijkse implementatie van het intern beleid en vaak ook als beslissingsnemer (of als adviseur), vanuit die dubbele positie ook de infosessies te verzorgen.

OMSCHRIJVING

Tijdens deze infosessie krijgen de deelnemers op een **zeer praktijkgerichte wijze** (o.a. via reële dagdagelijkse voorbeelden) inzicht in de (soms) grote gevolgen die kunnen voortvloeien uit onzorgvuldige (of ondoordachte) handelingen die de informatieveiligheid (of IP) van een organisatie (of van een individu) in het gedrang kunnen brengen.

Vanuit 12 verschillende invalshoeken (domeinen) wordt er aandacht besteed aan deze thema's, met als doel de deelnemers inzichten aan te reiken en bepaalde gevaren tijdig te doorzien om op deze wijze zoveel als mogelijk security breaches te voorkomen waardoor er mogelijks belangrijke hoeveelheden informatie kunnen gelekt of gestolen worden. Op basis van deze 12 thema's wordt - waar relevant - op (zeer) éénvoudige en begrijpbare wijze "in de huid gekropen" van hackers en komen zowel recente als hacking technieken/scenario's aan bod zodanig dat de deelnemers de aangereikte begrippen technieken ten volle kunnen begrijpen. Deze scenario's worden telkens geïllustreerd op basis van voorbeelden die de media hebben gehaald maar waarbij nu ook duiding wordt gegeven hoe de hackers tewerk zijn gegaan.

Via deze infosessie worden de deelnemers geïnformeerd over de (digitale) gevaren rond thema's informatieveiligheid, privacy en security. Deze verworven inzichten zijn zowel bruikbaar binnen de organisatie als binnen de privé levenssfeer van de medewerker. Want aandacht voor informatieveiligheid, privacy en security kent geen grenzen en heeft vooral te maken met een gedragswijziging van de medewerker. Deze gedragswijziging start en eindigt dus niet aan de ingang van de organisatie maar is een continu gegeven geworden binnen ons dagdagelijks leven.

Deze infosessie heeft dan ook als doel bij iedere medewerker een **gedragswijziging** teweeg te brengen door hem/haar veel bewuster dan voorheen te laten omgaan met informatie, privacy, IT technologie, sociale media ... en andere betrokken technologieën maar ook andere handelingen en gewoontes waarin mogelijke gevaren (kunnen) schuilen.

VOOR WIE IS DEZE OPLEIDING BESTEMD?

Elke medewerker binnen non en social profit (lokale besturen, OCMW's, VZW's, ...)

METHODOLOGIE

De docent zal aan de hand van een presentatie en een aantal zeer aanschouwelijke filmpjes een 12-tal security en privacy principes bijbrengen aan de deelnemers. De opgedane kennis is zeer laagdrempelig en deze kennis is naast de professionele werkomgeving eveneens zeer nuttig om in de gewone privé omgeving eveneens toe te passen. Op het einde van de sessie dienen de deelnemers veel bewuster om te gaan met aspecten die invloed hebben op security en privacy en dient - in bepaalde gevallen - aan te zetten tot een gedragswijziging van de

medeweker(s).

Vraag vrijblijvend een offerte en bied deze opleiding aan als een "in-house" maatopleiding binnen uw organisatie:
De opleiding wordt vooral als maatopleiding aangeboden voor grotere groepen. Op basis van een vrijblijvend gesprek kan de inhoud - indien wenselijk - verder afgestemd - op de concrete noden van uw organisatie.

programma

Korte intro over risico's (IT en andere): algemeen, als introductie tot de verschillende domeinen

- Domein 1: Surfing the web
  - Bedrijfspolicy en acceptabel gebruik
  - Downloaden en installeren van software
  - Copyright beschermd materiaal
- Domein 2: Data protection
  - Van het beschermen van je online identiteit tot GDPR compliance
  - Hoe ga je om met persoonsgegevens (verkiezingen, afgestudeerden, etc.)
  - Kan ik zomaar foto's posten na een event?
- Domein 3: Insider threats
  - De "ongelukkige medewerker"
  - There is no patch to human stupidity or ignorance
  - Het gebruik memorysticks en online tools zoals Dropbox, etc.
  - Bewust of onbewust een bestand doormailen
- Domein 4: Malicious links
  - Links met slechte reputatie, wat is dat?
- Domein 5: Malware
  - Verschillende vormen malware en hun potentiële effecten
- Domein 6: Mobile devices
  - Mobiele toestellen gebruiken en connecteren (smartphones en tablets)
- Domein 7: Security outside of the office
  - Wat is een sleutelplan?
- Domein 8: Passwords policy
  - Paswoorden zijn persoonlijk
- Domein 9: Physical security
  - Follow-me printing
  - Fysieke toegangscontrole tot archieven
- Domein 10: Social networking & social engineering
  - De hulpwaardige helpdesk medewerker of de ongeduldige VIP
- Domein 11: Phishing and spear phishing
  - Definities en hoe te herkennen?
  - SMSishing
- Domein 12: Ransomware
  - Wat is het en wat zijn de gevolgen
  - Waarom doen hackers het?