Security audits en end user security awareness in de praktijk

Waarom Security audits en Security Awareness sessies hand in hand gaan!

Opleiding IT PRO

OMSCHRIJVING

Introductie

GDPR-Club seminarie

Onder het motto verkomen is beter dan genezen, zou elke DPO (jaarlijks) een aantal terugkerende preventieve maatregelen moeten opnemen in zijn informatieveiligsplan. Met als jaarlijks terugkerend punt binnen dit plan: het uitvoeren van een (externe) security Audit en het organiseren van interne infosessies rond informatieveiligheid voor alle (nieuwe) medewerkers van het bedrijf.

Tijdens seminarie krijgt inzichten over hoe wanneer en wat van zowel Informatieveiligheidssessies als het (laten) uitvoeren van een security audit en hoe op basis van dit security Audit rapport een actieplan opstellen met een terugkoppeling naar het informatieveiligheidsplan dat dient geactualiseerd de worden.

Omschrijving

GDPR-Club for DPO, Legal, IT en Managers

De seminaries van de GDPR-Club hebben als doel - alle professionals die betrokken zijn met *'Informatieveiligheid'* - actuele diepgaandere kennis en *'best practices'* aan te reiken. Hierbij komt - een laatste stand zaken - betreffende belangrijkste (kern)taken/domeinen waarbinnen een informatieveiligheidscel dient te functioneren aan bod. De spreker(s) van elk seminarie is/(zijn) expert(en) binnen het specifieke vakdomein dat in het desbetreffende seminarie behandeld wordt.

Bedrijven die lid zijn van de *'IT-Club - Circle of excellence'* krijgen automatisch toegang tot alle seminaries van de *'GDRP-Club formule'*.

Webinar of op de campus? Aan u de keuze!

Vanaf dit clubjaar kan elke clublid - per seminar - zelf vrij kiezen als u deze wenst online mee te volgen (Webinar) dan wel op de campus. Om praktische redenen (ifv geldende COVID richtlijnen mbt maximale bezetting leslokaal) vragen wij wel uw keuze minstens één week voor startdatum kenbaar te maken. U kan gerust uw keuze tijdens de hernieuwing van het lidmaatschap kenbaar maken en eventueel (minstens één week voor start) bijsturen ifv uw wensen.

Exclusief voor clubleden: Webinars zullen vanaf heden ook opgenomen worden!

Alle(*) seminaries / webinars zullen vanaf september ook opgenomen en nadien beschikbaar gesteld worden. Vanaf eind september krijgt elk Clublid toegang toegang tot het digitaal platform waarop zowel de presentaties van de sprekers als de opnames beschikbaar zullen zijn.

(*) Rekening houdend met de GDPR-wetgeving.

Thema's en seminaries onder voorbehoud van mogelijke wijzigingen (praktisch en actualiteit).

Voor wie is deze opleiding bestemd?

- Functionaris gegevensbescherming
- Data Protection Officer
- Juridische medewerkers
- IT manager, diensthoofd IT
- Business Managers

Voorkennis

Basiskennis GDPR terminologie is aanbevolen.

PROGRAMMA

Deel 1 – Security Audits: Noodzaak, frequentie en actieplan [18u00 - 19u30]

De bedrijfscontinuïteit van zowel grote als kleine bedrijven, staat of valt met een correct werkende ICT omgeving. Het niet beschikbaar zijn van bepaalde ICT diensten (bvb mailserver, website, database, ...) voor enkele uren, kan reeds een grote impact hebben op de dienstverlening naar uw klanten toe of kunnen de interne productiviteit van uw medewerkers gevoelig laten dalen. Ondanks dit gegeven spenderen bedrijven nog steeds teveel tijd aan het reactief oplossen van curatieve problemen, i.p.v. periodiek inplannen en uitvoeren van preventief onderhoud zoals het laten uitvoeren van interne/externe Security Audits.

- De noodzaak van een periodieke Security Audit
  - Bespreking van de mogelijke gevaren
  - Concrete cases die noodzaak van security Audits aantonen
- Aanpak van een Security Audit
  - De scoop van de Security Audit: Asset list en security perimeter
  - Mogelijke audits
  - Type audits (White box - Black box)
  - Opmaken belangrijkste gevaren (threat list)
  - Huidige en toekomstig bedreigingen in kaart brengen
  - Vastleggen van prioriteiten ifv Assets en bedreigingen
- Het uitvoeren van een Security Audit in de praktijk
  - Opmaak van een security rapport en een actieplan
  - Implementeren van Network access controles
  - Implementeren van Intrusion prevention
  - Implementeren van Identity en access management
  - Maken van Backups
  - E-mail protection en filtering
  - Verhinderen van fysieke intrusions
- Security Audit: opmaak van een Informatieveiligsplan
- Concrete tips en best practice

Pauze: [19u30 - 19u50]

Deel 2 – Informatieveiligheid [19u50 - 21u00]

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 bijzonder mbt persoonsgegevens, maar ook IP) 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.

Noodzaak, aanpak en insteek van infosessie informatieveiligheid naar het brede publiek toe:

Overzicht van meest voorkomende bedreigingen.

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

- Surfing the web
- Data protection
- Insider threats
- Malicious links
- Malware
- Mobile devices
- Security outside of the office
- Passwords policy
- Physical security
- Social networking & social engineering
- Phishing and spear phishing
- Ransomware

DOCENT

Ivo Depoorter, Stafmedewerker ICT en gegevensbescherming bij GTB