ICT Academy

18 PE-uren

3-DAAGSE PRAKTIJKOPLEIDING

CYBER SECURITY AWARENESS & MANAGEMENT

ZORG VOOR EEN CONTINU ALERTE ORGANISATIE

HIGHLIGHTS

- Realiseer security bewust gedrag van boardroom- tot werkvloerniveau (en alles daartussen)
- Doorgrond de cyber risico's en bouwstenen van security awareness
- Interactief en praktisch: met cases van o.a. Rijkswaterstaat, NS, ING, Tele2
- Maak uw eigen security awareness programma plan

INCLUSIEF

- De visie van het NCSC
- Uw eigen security benchmark
- iPad Air met digitaal lesmateriaal

30 november,
1 en 7 december 2015

Coengebouw
Amsterdam

iir.nl/securityawareness

an informa business

GRIP OP DE MENSELIJKE FACTOR BINNEN UW CYBER SECURITY STRATEGIE

De menselijke factor is cruciaal voor de informatiebeveiliging van uw organisatie. Hoe gaan medewerkers in de organisatie met informatie om? Zijn medewerkers en toeleveranciers zich voldoende bewust van de alledaagse cyber risico's? En hoe houdt u ze bewust?

Tijdens deze praktische opleiding krijgt u inzicht in de bouwstenen van security awareness voor uw organisatie. Daarvoor zet u een doeltreffend security awareness plan op en verandert u het gedrag van uw medewerkers.

HOOFDDOCENT

Steven Debets is managing partner van de Cybersecurity & Continuïteit praktijk van Verdonck, Klooster & Associates. Hij is gespecialiseerd in de strategische toepassing van risicomanagement, cyber security en ICT compliance. Steven ondersteunt organisaties bij het opzetten van de besturing van risicomanagement, het inrichten van risicomanagement processen en het invoeren van technologieën om risico's te beheersen. Steven houdt zich bezig met de inrichting van managementsystemen voor cyber security en advisering op het gebied van identiteit en toegangsbeheer. Steven heeft veel ervaring met het uitvoeren van risicoanalyses op bedrijfsprocessen en beveiligings- en kwaliteitsaudits bij verschillende grote organisaties.

UW SPECIALISTEN EN GASTDOCENTEN

Brenno de Winter
IT beveiligings- en privacy-expert

Mark Braam
Aon

Joseph Mager
NS

Rogier van Wanroij
NCSC

Nico Verbeij
VKA

Kees den Breejen
Tele2 Nederland

Dirk-Jan Joor
RWS

Mark Cramer
ING

UW RESULTAAT

- U bent op de hoogte van actuele cyber terreur, het dreigingsbeeld voor 2016 en de consequenties daarvan voor uw organisatie.
- U heeft in kaart welke impact security risico's voor uw organisatie hebben. Tijdens de opleiding maakt u een concreet en doeltreffend security awareness programma plan. Zo kunt u het gedrag van medewerkers écht veranderen.
- U weet security awareness in uw organisatie optimaal te stimuleren en borging daarvan te toetsen.
- Inspiratie: u ontmoet experts en collega's met veel ervaring. Met hun kennis maakt u de cruciale stap om uw organisatie security bewust te maken!

WERKWIJZE

- Online intake: Voorafgaand heeft u een digitale intake waarin naar uw ervaring en leerdoelen wordt gevraagd
- Voorbereiding: U ontvangt twee weken voor de eerste opleidingsdag opgaven ter voorbereiding op de cursus. Tijdens de cursus vindt er feedback en terugkoppeling plaats.
- U werkt met digitaal lesmateriaal wat u één week voor de eerste opleidingsdag ontvangt.
- Voorbeelden uit de praktijk lopen als een rode draad door de cursus

DAG 1 – 30 NOVEMBER 2015

INZICHT IN CYBER DREIGINGEN, APT'S, CRYPTOWARE & PHISHING, RISK MANAGEMENT

Waar moeten medewerkers bewust van worden gemaakt, welke dreigingen zijn relevant?

09:00 **Ontvangst door uw hoofddocent**
- » Voorstellen en introductie
- » Uw persoonlijke doelstelling tijdens deze 3 dagen

Steven Debets, partner risk management, VKA

09:30 **Actueel: Advanced Persistent Threats (APT's) / cryptoware / phishing**
- » Hoe herkent u APT's, cryptoware, phishingmails?
- » Wat kunt u doen?
- » Welke stappen moet u nemen?
- » Hoe snel moet u handelen?
- » Praktijkvoorbeelden

Brenno de Winter, IT-expert op gebied van beveiliging en privacy

11:00 **Lessons learned uit grote cyber incidenten**
- » Wie zijn cyber criminelen, wat is hun doel en wie zijn de slachtoffers?
- » Wat is de (financiële) impact van deze cyber incidenten?
- » Hoe zijn getroffen organisaties omgegaan met het incident?
- » In hoeverre speelt de human factor een rol bij cyber incidenten?
- » Welke oplossingen zijn gekozen, zijn deze nog steeds effectief?

Brenno de Winter, IT-expert op gebied van beveiliging en privacy

12:30 **Gezamenlijke lunch**

13:30 **Praktijkcase NCSC en Rijkswaterstaat (RWS)**
- » Dreigingsbeeld 2015
- » Toelichting op dreigingsbeeld 2016
- » Hoe heeft RWS invulling gegeven aan het beveiligd werken?
- » Gekozen strategie en waarom?
- » Risicomanagement bij RWS

Rogier van Wanroij, manager expertise en advies cyber security, NCSC
Dirk-Jan Joor, programmamanager implementatie BIR, Rijkswaterstaat

15:00 **Risicomanagement m.b.t. cyber security**
- » Analyseren en beheersen van cyberrisico's
- » Benodigd beveiligingsniveau vaststellen & bepalen passende maatregelen
- » Hoe houdt u cyberrisico's onder controle?
- » Cyberrisico's en reputatieschade
- » Communicatie & rol van de risicoadviseur bij digitale incidenten

Mark Braam, senior consultant enterprise risk management, Aon

16:30 **Samenvatting van eerste opleidingsdag: lessons learned**

17:00 **Afsluiting**

PRAKTIJKOPDRACHT I
- » Formuleer de doelstelling + doelgroep(en) voor uw security awareness programma. Deze opdracht wordt besproken tijdens de 2e trainingsdag en is de eerste stap in uw awareness programma plan.
- » Invullen van security benchmarkvragenlijst (anoniem en vertrouwelijk)

DAG 2 – 1 DECEMBER 2015

SECURITY AWARENESS, INTERVENTIES, CULTUURVERANDERING

Inzicht in cyber risico's en bouwstenen van security awareness voor uw organisatie

09:00 **Cyber security awareness**

- Wat is de menselijke factor?
- Wat levert cyber security awareness de organisatie op?
- Hoe krijg ik mijn organisatie mee?
- Hoe creëer ik de gewenste cultuurverandering?
- Cyber security awareness bij het management
- Cyber security awareness op de werkvloer
- Voorbeelden van effectieve interventies

Nico Verbeij, senior adviseur verandermanagement, VKA

12:30 **Gezamenlijke lunch**

13:30 **Security awareness bij ING**

- Gekozen strategie en waarom?
- Wat heeft ING geleerd na ruim 10 jaar awareness?
- Belangrijkste factoren in security beleid
- Actuele ontwikkelingen en aandachtspunten

Marc Cramer, principal consultant cybercrime, ING

14:30 **Security awareness plan bij de NS**

- Gekozen interventies en waarom?
- Welke interventies zijn het meest effectief bij welke doelgroep?
- Voorbeeldaanpak (best practice)
- Inzetten van tools (e-learning, game): do's and don'ts

Joseph Mager, information security officer, Nederlandse Spoorwegen

15:30 **PRAKTIJKOPDRACHT II**

Behandeling van praktijkopdracht I

- Bepaal de key assets van uw organisatie
- Bepaal de belangrijkste cyber risico's voor uw organisatie
- Voer een risico analyse uit en leer voor welk soort cybercrime uw organisatie het meest kwetsbaar is

Steven Debets, partner risk management, VKA

16:30 **Samenvatting van tweede opleidingsdag: lessons learned**

17:00 **Afsluiting**

IIR ICT ACADEMY

De IIR ICT Academy leidt jaarlijks ruim 300 professionals op. Onze trainingen variëren van 1-daagse workshops tot uitgebreide opleidingen. Wat ze gemeen hebben: alle docenten komen direct uit de praktijk. Door zelf marktonderzoek te doen, blijven we ons trainingsaanbod steeds vernieuwen!

CEDEO GECERTIFICEERD

CEDEO is een onafhankelijke keuringsinstantie die de kwaliteit van human resources dienstverleners meet en waarborgt. Recentelijk heeft CEDEO een marktonderzoek uitgevoerd onder de klanten van IIR. Ruim 90% van de respondenten van het onderzoek was (zeer) tevreden over de trainingen van IIR!

DAG 3 – 7 DECEMBER 2015

OPZETTEN AWARENESS PROGRAMMA, BORGING & CONTINU VERBETEREN SECURITY AWARENESS

Inzicht in vereisen voor doeltreffend security awareness programma & structureel en continu beheersen van security bewuste organisatie

09:00 **Aanpak security awareness programma**

- Stakeholderanalyse: wie zijn belanghebbenden bij cyber dreigingen?
- Kernboodschap en awareness strategie
- Doelgroepen en (sub)doelstellingen
- Leermodellen van mensen en organisaties
- Draagvlakladder
- Effectiviteit van verschillende soorten interventies ahv praktijkvoorbeelden
- Valkuilen, tips & tricks

Steven Debets, partner risk management, VKA

10:00 **Borging & continu verbeteren security awareness**

- Governance, risk & compliance
- Opzetten van awareness campagne
- Metingen en onderzoek (0/1-meting, mystery onderzoek)
- Hoe effectief is mijn awareness campagne?
- Hoe weet ik dat deze campagne bijdraagt aan meer secure aware gedrag?
- Monitoring

Steven Debets, partner risk management, VKA

11:00 **Governance, risk & compliance bij Tele2**

- Hoe ver staat Tele2 als het gaat om security awareness?
- Gekozen strategie en waarom?
- Belangrijkste bottlenecks
- Hoe is Tele2 tot haar nieuwe awareness campagne gekomen en waarom?

Kees den Breejen, corporate security officer, Tele2 Nederland

12:30 **Gezamenlijke lunch**

13:30 **PRAKTIJKOPDRACHT III**

- Bespreek uw security benchmarkresultaten
- Bepaal de kernboodschap voor uw security bewuste organisatie
- Scherp uw security awareness plan aan voor uw doelgroep(en)
- Leer van de aanpak van medecursisten
- Bespreek verbeterpunten met cursisten en docent(en)
- Kom tot een afgerond security awareness plan zodat u deze direct kunt toepassen in uw organisatie

Steven Debets, partner risk management, VKA

16:30 **Samenvatting van derde opleidingsdag: lessons learned**

17:00 **Afsluiting**

INCLUSIEF INTERACTIEVE LEEROMGEVING

Alle presentaties, video's, artikelen en huiswerk staan op onze online leeromgeving. Zo heeft u alle cursusinformatie op één plek! Ook kunt u hier makkelijk contact houden met andere deelnemers, of vragen stellen aan uw docent!

IIR B.V., Kabelweg 37, 1014 BA Amsterdam:

Port betaald
Port Payé
Pays Bas

an informa business

Meld u aan met uw KLANTCODE:

3-DAAGSE PRAKTIJKOPLEIDING

CYBER SECURITY AWARENESS & MANAGEMENT

ZORG VOOR EEN CONTINU ALERTE ORGANISATIE

30 november, 1 en 7 december 2015, Coengebouw Amsterdam

UW INVESTERING

3-daagse praktijkopleiding	€ 2.699,-

Dit bedrag is per persoon, inclusief iPad Air, digitale documentatie, lunches, koffie/thee en exclusief BTW. Wilt u geen iPad Air en neemt u uw eigen tablet of laptop mee? Dan ontvangt u € 300,- korting. U kunt dit bij uw boeking aangeven.

AANMELDEN? 3 MAKKELIJKE MANIEREN:

1. Via internet: www.iir.nl/securityawareness
2. Via e-mail: aanmelding@iir.nl
3. Per telefoon: +31 (0)20 580 54 00

INHOUDELIJK CONTACT MET UW OPLEIDINGSADVISEUR?
Wilt u meer informatie over deze opleiding? Neem dat contact op met onze opleidingsadviseur Stephan Rienstra via 020 – 580 54 95 of per e-mail via s.rienstra@iir.nl.

MAATWERK VOOR UW TEAM?
IIR biedt naast de mogelijkheid van een individuele training of opleiding ook trajecten die op maat worden gesneden voor uw organisatie. Neem daarvoor contact op met onze InCompany adviseurs via 020 - 580 5414 of per e-mail via incompany@iir.nl

VOOR WIE BEDOELD?

Iedereen werkzaam in het bedrijfsleven of in de (semi) publieke sector die zich bezighoudt met cyber security, informatiebeveiliging en security awareness.

- Security managers
- Risk managers
- Compliance managers
- Business architecten
- IT Auditors
- Security Officers, CISO's
- Compliance Officers
- Privacy Officers,
- Privacy Functionarissen
- Beveiligingsfunctionarissen
- Communicatie medewerkers

IIR ICT | @ICT_cursus | www.iir.nl/securityawareness

Gegevensregistratie
Uw gegevens worden door IIR geregistreerd en gebruikt om u op de hoogte te houden van onze producten en die van zorgvuldig geselecteerde bedrijven. Mochten uw gegevens niet correct zijn of wenst u dat uw gegevens niet gebruikt wordt voor deze doeleinden, neem dan contact op met onze database afdeling via 020 - 580 5470 of e-mail database@iir.nl

Algemene voorwaarden
Op alle aanbiedingen zijn onze algemene voorwaarden van toepassing. Deze zijn gedeponeerd bij de K.v.K te Amsterdam, onder nummer 33200358. De algemene voorwaarden zijn te downloaden op onze website www.iir.nl/algemene-voorwaarden en worden op verzoek kosteloos toegezonden.