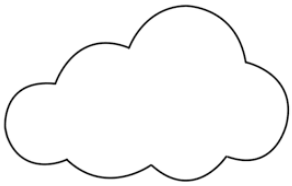
Versie 1.1
20171115

"Uitdagende ontwikkelingen vragen om actie"

Sfeerverslag van de 8e BIR Practitioner Community bijeenkomst.
Plaats: Hoofdkantoor UWV te Amsterdam
Datum: 15 november 2017

De bijeenkomst
Ad Kint opent het programma en heet allen van harte welkom. Hij benadrukt direct het belang van actuele ontwikkelingen op het terrein van Informatiebeveiliging en Privacybescherming. In het regeerakkoord is een duidelijke trend te zien. Gewezen wordt op het initiatief een ambitieuze cybersecurity-agenda op te stellen, waarin onder meer bedrijven gestimuleerd worden veiliger software te maken. Tevens komt de BIR2017 er aan, waarin uitgegaan wordt van compliance naar in control. Organisaties worden verwacht goed na te denken over de eisen die gesteld worden en hoe je daar op wilt sturen.
De deelnemers zijn vanmiddag benieuwd naar de betekenis van deze nieuwe ontwikkelingen.

Clouddienstverlening en de verantwoordelijkheid van de Overheid



Martin Vliem (Microsoft) gaat energiek van start en weet de aandacht van de deelnemers tot het eind toe vast te houden. Hij toont een filmpje over een orkest, waarin samenspel het toverwoord is. Om tot een mooi resultaat te komen moet iedereen weten, wat en wanneer hij iets te doen heeft, en ook hoe natuurlijk. Voor het publiek een onvergetelijke belevenis, een herinnering om nooit te vergeten.
Martin is lid van de CIP Werkgroep XaaS en vertelt over de zoektocht die de werkgroep heeft doorlopen. Uiteindelijk is de keuze gevallen op het opstellen van een whitepaper over 'Governance en clouddienstverlening'. Hierin wordt duidelijk gemaakt 'Waarom' de rol van de overheid belangrijk is en Cloud Governance ingeregeld dient te zijn.
Martin gaat in op de inhoud van de whitepaper: Cloud Governance, de rol en verantwoordelijkheden van de Overheid voor Succesvol en Veilig Cloud.
De totstandkoming van het 'Service ontwerp' speelt een zeer belangrijke rol als het om Security en Privacy gaat.
Waarom?

- Cloud security is een partnerschap onderhavig aan eigen verantwoordelijkheden die duidelijk belegd dienen te worden, zowel voor de Cloud Aanbieder als de ***Cloud Afnemer***.
- ***Cloud Afnemer*** heeft de verantwoordelijkheid om volgende te regelen:
  - *Cloud Strategie*
  - *Cloud Ontwerp*
  - *Cloud Uitrolprocessen*
- Een structureel risico evaluatieproces behoort bij een verantwoordelijk besluitvormingstraject
- Vraag om waarborgen en zekerheden van de Cloud Aanbieder
- Vul deze aan met additionele beheersmaatregelen in lijn met eigen risico-profile en vereisten

De deelnemers wijzen ook op de belangen van eenvoudig kunnen wisselen van cloud-provider en benadrukken ook aandacht te richten op het procurement perspectief.

Compliance management

Marinus Postma (DUO) is lid van de CIP werkgroep GRC tooling. De werkgroep presenteert vandaag het document 'Referentiemodel Compliance management'. Het dient als voorbeeld hoe het compliance management proces in een organisatie kan worden ingericht, zowel in de lijnorganisatie als de ondersteunende staforganisatie. Na een korte inleiding over onderwerpen als 'Besturing geprojecteerd op ISMS', 'Beheersmaatregel op Productniveau' en een overzicht over de rollen nodig voor Compliance management, worden vragen van de community leden besproken. Daarbij gaat het ook over het verschil in organisaties. Inderdaad, dien je rekening te houden met je eigen specifieke kenmerken van je organisatie. Het document helpt je om daarover na te denken bij de inrichting van Compliance management.
Aan de deelnemers wordt gevraagd inhoudelijke reacties op het document binnen 2 weken te sturen aan Ad Kint (ad.kint@uwv.nl). Elke bijdrage is van harte welkom.

Na de introductie worden de deelnemers uitgedaagd in kleine groepjes een aantal prikkelende stellingen over GRC nader te beschouwen. Bij de plenaire bespreking blijken de meningen behoorlijk op één lijn te liggen. Er worden ook belangrijke aanvullingen benoemd. De opbrengst van alle verzamelde reacties zou een prototype businesscase Compliance management kunnen zijn. Op de verzamelde reacties kunnen deelnemers ook na afloop van deze bijeenkomst nog aanvullingen doen, middels een email aan ad.kint@uwv.nl.

BIR2017

Na de pauze staat de komst van de BIR2017 centraal.

Kees van der Maarel (Ministerie van BZK), nauw betrokken bij de totstandkoming van BIR2017, stelt dat de nieuwe BIR gaat zorgen voor dialoog. Op 28 november wordt de BIR2017 formeel bekrachtigd door de ICBR.

Kees legt uit welke producten beschikbaar zijn ten behoeve van de invoering en uitvoering van de BIR2017.

De BIR2017 is geen statische baseline. Halfjaarlijks is er een onderhoudsslag. Die zorgt er voor dat rijksmaatregelen, handreikingen en FAQ's, o.a. op basis van feedback uit de praktijk, onderhouden kunnen worden. De CIP BIR Practitioners Community kan daar een bijdrage aan leveren. De PraCo BIR pakt deze uitnodiging graag aan.

Na een toelichting over achtergronden van de BIR2017 en nieuwe begrippen als basisbeveiligingsniveaus (BBN's), wordt de opzet van de BIR2017 (3 BBN's, controls, rijksmaatregelen en handreikingen) gepresenteerd.

Tijdens de presentatie komen vragen aan de orde over hogere beveiligingseisen op grond van bijv. EU-wetgeving. Deze hogere eisen worden opgenomen in BBN3 en worden gebaseerd op de NATO-richtlijnen. BBN3 is nog in ontwikkeling.
De BIR2017 is handzamer dan de oude BIR, mede door de toepassing van risicomanagement. Met behulp van de Quickscan Information Security (QIS) kan bepaald worden welk BBN van toepassing is. De BBN bepaalt welke controls c.q. rijksmaatregelen geïmplementeerd moeten worden. Met risicomanagement moet vervolgens bepaald worden welke maatregelen er naast de voorgeschreven rijksmaatregelen moeten worden getroffen om de controls adequaat in te vullen. Daarbij kunnen als inspiratie bijv. de implementatierichtlijnen uit de ISO27002 worden gebruikt.

Kees licht verder het waarom en de uitgangspunten van de BIR2017 toe.
Met name worden de verschillen duidelijk tussen de BIR2012 en de BIR2017:

- Van compliance naar in control
- Van maatregeloriëntatie naar risicoafweging
- 3 basisbeveiligingsniveaus & -toets
- Rijksmaatregelen als harde ondergrens
- Verantwoordingsregime
- Minder rijksmaatregelen
- Handreikingen
- Onderhoudscyclus

Het aantal BIR maatregelen is van 270 (rijks)maatregelen teruggebracht naar 71 rijksmaatregelen voor BBN1 en 136 rijksmaatregelen voor BBN2 .
De ADR vindt de rijksmaatregelen in de BIR2017 voldoende SMART en beschouwt het als een tactische kader waarmee de toetsbaarheid duidelijk verbetert.

Met hulp van de Mentimeter app is plenair de vraag 'Welke uitdaging geeft de BIR2017?' beantwoord. In de onderstaande woordwolk staan de antwoorden samengevat. Hoe groter het woord hoe vaker het antwoord is gegeven.

Tot slot
Ter afsluiting is nog gezellig nagepraat onder het genot van een hapje en een drankje.
Op 5 april 2018 staat de volgende bijeenkomst van de BIR Practitioners Community gepland. Altijd de moeite waard om alvast te noteren in je agenda.

Gemaakte afspraak:

- De getoonde presentaties worden ter beschikking gesteld aan BIR Praco-leden.
- Reacties op het document Referentiemodel Compliance management en aanvullingen op het prototype businesscase Compliance management, graag sturen aan ad.kint@uwv.nl.

Verslag: Tady Slebioda