PRIVACY COMPANY tv

Adfiz

Het treffen van adequate organisatorische en technische beveiligingsmaatregelen

Nieuwsjaarscongres Adfiz

Ing. Luuk Akkermans CISA CISM

11 januari 2018

I. Informatiebeveiliging

Waarom is informatiebeveiliging zo belangrijk?

I. Informatiebeveiliging
Waarom eigenlijk?

I. Informatiebeveiliging
Waarom eigenlijk?

II. De basis

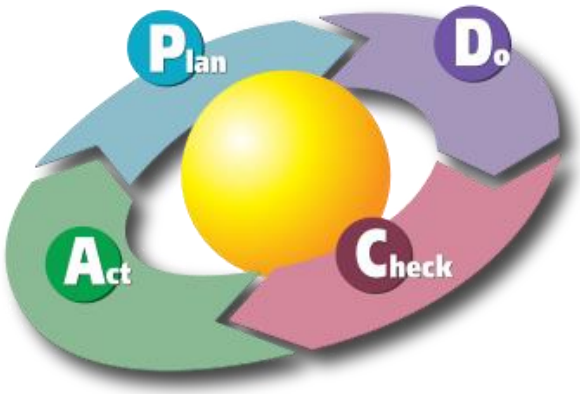
Informatiebeveiliging? Wat is dat nou eigenlijk? En hoe zorg je ervoor dat je de benodigde maatregelen goed borgt in de organisatie?

II. De basis
Informatiebeveiliging algemeen

- Informatiebeveiliging != IT security -> er is meer dan techniek alleen: *mens, proces en techniek*.
- Draait om informatie en het beveiligen ervan
- Risico gedreven ("passende maatregelen")
  - BIV classificatie
  - Risicoanalyse
  - "Risk appetite"
- Bewegend binnen kaders: <u>informatiebeveiligingsbeleid</u>
- Maar waar hebben we het nou eigenlijk over? Waar moeten maatregelen voor genomen worden? En hoe bewaak je die dan?

II. De basis
Plan, Do, Check en Act!

- De PDCA cyclus (jaarlijks) zorgt voor een "levend" proces:
  - **Plan** – Maak een plan. Welke maatregelen ga je wanneer nemen?
  - **Do** – Voer die maatregelen uit!
  - **Check** – Controleer of de maatregelen de gewenste effecten hebben bereikt.
  - **Act** – Stuur bij of introduceer een nieuwe maatregel waar nodig.
- Zonder cyclus kan het effect van de maatregel niet bepaald worden – dit zal niet resulteren in **passende technische** en **organisatorische** maatregelen!

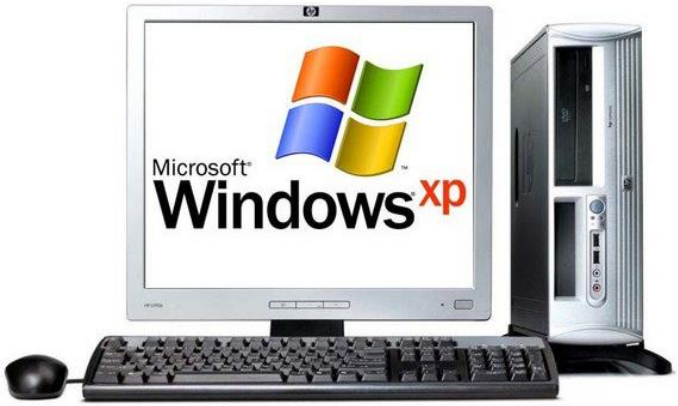


III. Technische en organisatorische maatregelen

*Passende **technische** en **organisatorische** maatregelen, rekening houdend met de stand der techniek.*

III. Maatregelen
Wat staat er in de AVG?

- Passende **technische** en **organisatorische** maatregelen, met nadruk op **aantoonbaarheid** (documentatieplicht, PIA) en **stand der techniek**.



- Expliciet genoemd: **pseudonimisering**, encryptie
- Privacy by Design (PbD), privacy by default

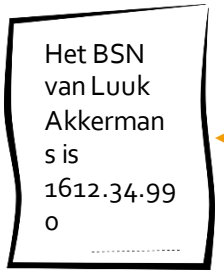
III. Maatregelen
Zomaar een lijst met maatregelen..

- ✓ fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole
- ✓ opslag van gegevens in een kluis
- ✓ project-, risico- en incidentenmanagement
- ✓ data opsplitsen
- ✓ dataminimalisatie
- ✓ back-ups
- ✓ integriteitscontroles
- ✓ meerfactor-authenticatie (2fa)
- ✓ monitoring en logging
- ✓ controle van toegekende bevoegdheden
- ✓ privacybewustzijn- en beveiligingstrainingen
- ✓ managementrapportages over risicobeheer
- ✓ beperken inzageniveau
- ✓ periodiek een audit of hack- of penetratietest uitvoeren
- ✓ richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken
- ✓ responsible-disclosure beleid
- ✓ geheimhoudingsverklaringen
- ✓ service level agreements (met boeteclausules)
- ✓ verwerkersovereenkomsten
- ✓ screening personeel en VOG-verklaring.

III. Maatregelen
Pseudonimiseren? Anonimiseren?

Pseudonimiseren? Anonimiseren? Wat is dat? En wat is eigenlijk het verschil?

III. Maatregelen
Anonimiseren



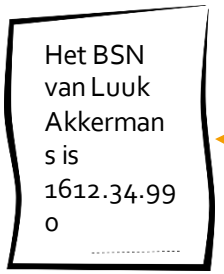
Goed leesbaar document met persoonsgegevens

Persoonsgegevens niet leesbaar

Eenmalige "willekeurige" sleutel

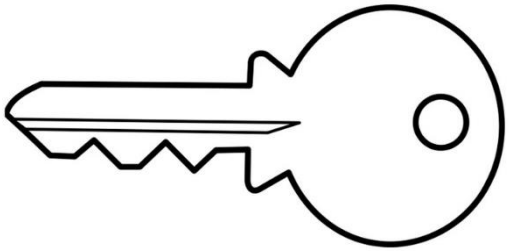
- **Niet meer herleidbaar** – in het geval van persoonsgegevens niet meer herleidbaar naar een uniek individu.
- **Onomkeerbaar**

III. Maatregelen
Pseudonimiseren



Goed leesbaar document met persoonsgegevens

Persoonsgegevens niet leesbaar



Vooraf vastgestelde sleutel (goed bewaren!)

- **Herleidbaar!**
- **Omkeerbaar!**
- *Ja maar..**hoe** dan?*

III. Maatregelen
Pseudonimiseren en encryptie

Pseudonimiseren, is dat dan hetzelfde als encryptie?

- Nee – bij pseudonimiseren wordt veelal gebruik gemaakt van encryptie als techniek (door gebruik te maken van een privé sleutel) om een deel van de gegevens onleesbaar te maken.
- Encryptie als techniek wordt o.a. ook gebruikt bij:
  - https – b.v. bij online banking
  - BitLocker – versleuteling van de gehele harde schijf van een pc

III. Maatregelen
Logische toegangsbeveiliging

- Ook wel bekend als autorisatiecontrole.
- Één van de basismaatregelen voor het beveiligen van informatie.
- Vaak gebruikte principes:
  - Need to know – heb je echt toegang tot die informatie nodig?
  - Least privilege – gebruik een minimale set aan rechten
- **Belangrijk:**
  - Voer periodieke autorisatiecontroles uit
  - Maak aantoonbaar dat het aanmaken, aanpassen en verwijderen van autorisaties conform een proces uitgevoerd wordt – inclusief goedkeuring!

III. Maatregelen
Organisatorische maatregelen

- Geheimhouding
- Gedragscodes
- Screening
- Bewustwording

- Maar **helaas** ook: een proces voor disciplinaire maatregelen moet ingericht zijn en medewerkers moeten hierop geattendeerd worden.

IV. ISO 27001

De kracht en de zwakte van het hebben van een ISO 27001 certificaat.

IV. ISO 27001

De kracht en de zwakte

- NEN-ISO/IEC 27001:2013
- Is één van de internationale standaarden op het gebied van IB
- Beschrijft een **Information Security Management System (ISMS)** dat dmv de jaarlijkse **Plan Do Check Act (PDCA) cyclus** IB borgt in de organisatie. Annex A bevat een set aan gestandaardiseerde normen.
- Certificering mogelijk, vaak gezien als een commercieel uithangbord
- Wat is dan NEN-ISO/IEC 27002? Geen ander normenkader, maar een best-practice voor de normen uit 27001
- Ben je veilig met een ISO 27001 certificaat? **Niet per se** (DigiNotar)

IV. ISO 27001
De kracht en de zwakte

Waarvoor is ISO een prima basis?

I. Als eis aan een leverancier:
   - ISO 27001 als basis voor het nemen van de juiste maatregelen
   - ISO 27001 certificering

II. Als basis voor het nemen van de juiste maatregelen voor het inrichten van de eigen organisatie.

V. De verwerkersovereenkomst

Wat staat er zoal in een verwerkersovereenkomst en wat moet ik weten over het beveiligingsplan van de verwerker?

V. Verwerkersovereenkomst
Inhoud verwerkersovereenkomst

- Wat staat er nou eigenlijk in een verwerkersovereenkomst?
  - Duidelijke afspraken voor de verwerker;
  - Die ook nog geldig zijn na het einde van het contract;
  - ..maar weinig concrete maatregelen –"passende" technische en organisatorische maatregelen.
- Right to audit ("recht op controle")
- Melden van een datalek
- Beveiligingsplan van de bewerker – inclusief "statement of compliance"

V. Verwerkersovereenkomst
Beveiligingsplan van de verwerker

Beveiligingsplan van de verwerker?

- Vaak een generiek plan – niet ingezoomd op de dienst die geleverd wordt.
- Vraag de leverancier dan ook de specifieke kenmerken van de dienst, met name gericht op de vertrouwelijkheid, te specificeren (*dit kan eventueel ook in een dienstbeschrijving*).

Goed verhaal Luuk, maar wat nu?

- Denk vanuit de positie van de klant – hoe zou jij willen dat jouw informatie wordt beschermd?
- Volg de “hoe word ik privacy proof” stappen (10) zoals door Adfiz beschreven.
- Download deze presentatie en gebruik de checklist in de bijlage ter ondersteuning bij het nemen van passende **technische** en **organisatorische** maatregelen.

Vragen?

Voor meer informatie of vragen:

www.privacycompany.eu

info@privacycompany.eu

PRIVACY COMPANY tv

Adfiz

Bijlage

Checklist technische- en organisatorische maatregelen

✓ Informatiebeveiliging checklist

Algemeen

Op de volgende slides is de informatiebeveiliging checklist onderverdeeld in een aantal categorieën welke overeen komen met de categorieën uit de ISO 27001 norm. De checklist kan gebruikt worden ter ondersteuning bij het implementeren van informatiebeveiligingsmaatregelen ter beveiliging van informatie en/of persoonsgegevens.

Disclaimer

Deze checklist heeft niet tot doel om volledig te zijn maar geeft een overzicht van een aantal basis maatregelen die getroffen dienen te worden ter beveiliging van informatie en/of persoonsgegevens.

✓ Informatiebeveiliging checklist (1 / 3)

Informatiebeveiligingsbeleid

- ☐ Formuleer het informatiebeveiligingsbeleid (b.v. op basis van ISO 27001).
- ☐ Bekrachtig het informatiebeveiligingsbeleid door het goed te laten keuren door de Directie en communiceer dit aan de medewerkers.

Organiseren van informatiebeveiliging

- ☐ Stel een informatiebeveiligingsfunctionaris aan (kan prima als "rol").
- ☐ Stel een informatiebeveiligingsplan op (meerjarenplan, wanneer ga je "wat" doen?).
- ☐ Voer het plan uit, gebruikmakend van een PDCA cyclus.

Personeel

- ☐ Voeg een geheimhoudingsverklaring toe aan de standaard set documenten behorend bij een arbeidsovereenkomst en zorg dat alle medewerkers deze getekend hebben.
- ☐ Leg generieke afspraken en verantwoordelijkheden m.b.t. informatiebeveiliging vast in bijvoorbeeld een gedragscode en laat deze door alle medewerkers tekenen.

Beheer van bedrijfsmiddelen

- ☐ Maak een overzicht van alle (ICT) bedrijfsmiddelen. Onder bedrijfsmiddelen vallen PC's, smartphones, tablets, printers, applicaties, informatiebronnen, etc.
- ☐ Borg dat het overzicht van (ICT) bedrijfsmiddelen wordt beheerd en bijgewerkt indien nodig.

✓ Informatiebeveiliging checklist (2 / 3)

Toegangsbeveiliging

- ☐ Implementeer een proces voor het aanmaken, aanpassen en verwijderen van autorisaties.
- ☐ Voer periodieke autorisatiecontroles uit en leg deze vast.

Fysieke beveiliging

- ☐ Stel regels op voor de fysieke beveiliging van het kantoorpand en voor het opruimen van vertrouwelijke informatie op werkplekken (clean desk).
- ☐ Voer periodieke "clean desk" controles uit.

IT beveiliging (IT security)

- ☐ Maak een overzicht van de netwerkstructuur van de organisatie, inclusief eventuele (private) cloud omgevingen en geef aan welke beveiligingsmaatregelen zijn genomen om het netwerk te beveiligen tegen misbruik van buitenaf.
- ☐ Stel een proces op om periodiek de IT infrastructuur te testen op kwetsbaarheden (vulnerabilities) en indien nodig maatregelen te treffen om de kwetsbaarheid te mitigeren.
- ☐ Stel een proces op om periodiek de IT infrastructuur te updaten / patchen aan de hand van beschikbare (beveiligings) updates van de leveranciers (denk bijvoorbeeld aan Microsoft patches).
- ☐ Stel een backup-proces op dat dagelijks alle vertrouwelijke informatie en/of persoonsgegevens op een veilige manier backupped en test periodiek (minimaal eens per half jaar) of het mogelijk is om een backup terug te zetten (restore test).

✓ Informatiebeveiliging checklist (3 / 3)

Communicatiebeveiliging

- ☐ Zorg voor maatregelen om veilige communicatie van informatie met externe partijen (b.v. klanten) mogelijk te maken en pas deze maatregelen structureel toe.
- ☐ Maak een overzicht van alle (interne) informatiestromen en verifieer of afdoende maatregelen getroffen zijn om de vertrouwelijkheid van de informatiestromen te garanderen.

Leveranciersrelaties

- ☐ Maak een overzicht van leverancierscontracten en bepaal in hoeverre de leverancier toegang heeft tot vertrouwelijke informatie of persoonsgegevens.
- ☐ Zorg dat verwerkersovereenkomsten zijn afgesloten met leveranciers (waar van toepassing).

Informatiebeveiligingsincidenten

- ☐ Stel een proces op voor het beheersen van een informatiebeveiligingsincident en/of datalek.
- ☐ Bepaal wie incidenten en/of datalekken rapporteert naar de benodigde instanties.

Bedrijfscontinuïteit

- ☐ Bepaal welke (bedrijfs)processen kritiek zijn voor de organisatie (indien het proces niet beschikbaar is, kan er geen werk uitgevoerd worden).
- ☐ Leg vast op welke wijze de kritieke processen gecontinueerd moeten worden tijdens een incident, en test deze "werkwijze" minimaal jaarlijks.