Memo

Aan : MT SSC DeSom
Van : Ray Flinkerbusch
Datum : 22 februari 2019, goedgekeurd MT: 25 februari 2019
Betreft : **CISO bulletin #2, SSC DeSom Informatie Beveiligings Principes**

Beveiligings principes bepalen de koers in het opstellen en uitwerken van het informatiebeveiliging beleid. Ze fungeren als toetsingskader om dit beleid te beoordelen op alle aspecten van de levenscyclus van informatie en onderliggende systemen.

Reikwijdte

Het volgen van de principes is verplicht voor *data onder verantwoordelijkheid* van SSC DeSom in de breedste zin van het woord '*data*', te weten; creëren, bewaren, verwerken, verzenden, vernietigen. Dit heeft betrekking op de data zelf, de onderliggende en ondersteunende platformen, locaties, gegevensdragers en connectiviteit.

Toepasbaarheid

De principes zijn van toepassing op zowel nieuwe initiatieven alsmede de bestaande omgeving en huidige projecten. Hierin wordt het "pas toe of leg uit"-principe gehanteerd welke ter beoordeling aan de CISO van SSC DeSom wordt voorgelegd.

De principes

De volgende tabel geeft een kort overzicht:

Principe	Omschrijving	Kern
DSM-IBP-1	We beschermen primair onze data ongeacht het platform, de applicatie of de locatie	data security first
DSM-IBP-2	De sterkste –en, waar mogelijk, meest kosteneffectieve beveiligingstechnologieen zijn onderdeel van elk ontwerp	secure by design
DSM-IBP-3	Beveiligingsmaatregelen bevinden zich op meerdere lagen conform verschillende beschermingmethoden	defense in depth
DSM-IBP-4	Het uitgangspunt is beveiligingsmaatregelen nemen tenzij…	secure by default
DSM-IBP-5	De primaire instelling is volgens het 'standaard-weigeren-beleid'	default deny
DSM-IBP-6	In geval van storing en/of systeemdefecten blijven beveiligingsmaatregelen altijd van kracht	fail secure
DSM-IBP-7	Elke uitrol of implementatie wordt volgens beveiligingsindustrie aanbevolen werkwijze uitgevoerd waarbij de ondersteunende software en handreikingen beschikbaar zijn	secure in deployment
DSM-IBP-8	De maatregelen onder ons beveiligingsbeleid zijn consistent	no security gap approach

Memo

Vrijstelling

Het is mogelijk dat er aan één of meerdere principes niet voldaan kan worden bij uitvoering van een project of implementatie van een nieuw product. Bijvoorbeeld vanwege te hoge kosten of een beheerinspanning die niet in verhouding staat tot het resultaat.

Als de aanvragende partij het niet eens is met het initiële oordeel van de CISO kan men de argumentatie schriftelijk voorleggen aan het MT met het verzoek tot vrijstelling. De vrijstelling wordt geregistreerd en afgegeven voor maximaal één jaar waarna deze opnieuw beoordeeld dient te worden.

-o-o-o-