Bijlage 2.0 Procesbeschrijvingen

## Processen in het kader van informatiebeveiliging

|  |  |  |  |
| --- | --- | --- | --- |
| **Procescode** | **Doel** | **Wel/niet automatiseren** | **Toelichting** |
| A.Servers | Centraal bijhouden wat de belasting van de servers is. | Wel | Ik heb met dit onderwerp gewerkt op meerdere stages, hierbij kreeg ik vaak van dit soort vragen en moest ik rapporten maken.  Het automatiseren van procescodes van servers kan veel voordelen hebben denk aan:  Efficiency: Automatisering kan helpen bij het sneller uitvoeren van taken en het verminderen van fouten die kunnen optreden bij handmatige uitvoeringen van beheerders.  Scalability: Als een bedrijf groeit, kan automatisering helpen bij het efficiënt beheren van meer servers en hierdoor alles soepeler laten verlopen, dit kan enorm schelen in kosten.  Consistency: Automatisering kan helpen bij het garanderen van consistentie in hoe servers worden beheerd en geconfigureerd.  Monitoring: Automatisering helpt mogelijk bij het bewaken van de status van servers en het detecteren van problemen sneller hierdoor runt je bedrijf nog efficiënter en blijft je infrastructuur operationeel.  Conclusie het bijhouden van je belasting op je servers is essentieel hierdoor kan je anticiperen en je server draaiend houden, en indien nodig opschalen en vervolgens de klant tevreden houden of je bedrijf operationeel houden. |
| A.Users | Centraal bijhouden wie wanneer op de systemen werkt. | Wel | Het is erg slim om als bedrijf logs te maken van welke systeem beheerder of gebruiker, gebruikt maakt van systemen hierdoor kan je zien wie wat voor het laatst heeft gewijzigd en vervolgens als het fout is gegaan of je iemands werk wilt controleren er toch een log van is.  Der is een nadeel, dit kan best wat vragen aan dataopslag afhankelijk van jouw infrastructuur en dus een redelijke kostenplaat meebrengen, dit geldt voor automatisering in het algemeen. |
| A.Cleandesk | Centraal bijhouden wie aan het eind van de dag informatie op het bureau achterlaat. | Niet | Ik ben van mening dat dit niet essentieel is en dus niet geautomatiseerd hoeft te worden.  Indien data beveiligd moet opgeslagen worden in een ssd met vpn acces of op een beveiligde data server, dan zal de beheerder hier van dit weten en dit dus niet laten slingeren op zijn bureaublad.  Verder horen de werkstation op slot te zijn en beveiligd dus niet jan de alle man kan zomaar op zijn of haar bureaublad.  Het kan handig zijn om het te automatiseren van een security standpunt zodat gebruikers toch een reminder krijgen dat er data die belangrijk is op bureaublad los staat maar dit is toch wat mij betreft te ver. |
| A.Logout | Centraal bijhouden wie er vergeet uit te loggen aan het einde van de werkdag. | Wel | Dit is een essentieel deel en zeer verstandig om te automatiseren, hierdoor kan de beveiliging van gegevens beter worden beveiligd omdat de gebruiker wordt uitgelogd na een bepaalde tijd van inactiviteit. (Security)  Ook helpt dit met het voldoen aan de AVG als bedrijf uiteraard is dit essentieel als bedrijf om op order te hebben omdat dit wettelijk verplicht is. (Security)  In en uitloggen zal altijd op dezelfde manier gaan waardoor fouten worden verminderd (Consistency).  Ten slotte kan het helpen met de compliance van het bedrijf het op orde houden van de logs hierdoor blijft het overzichtelijk. |
| A.PaperPassword | Centraal bijhouden wie wachtwoorden op een toegankelijke plek opschrijft. | Wel | Dit vindt ik een van de iets minder essentiële automatiseringen die nodig zijn, echter zeg ik toch wel.  Wachtwoorden laten slingeren is never nooit verstandig, dus is het belangrijk om bij te houden wie hij/zij wachtwoord opslaat, waarbij het erg toegankelijk is of toegankelijk via andere manieren (Collega die hier zomaar bij kan). Hierdoor kan de gebruiker een reminder krijgen om deze data op een secure fault op te slaan dit brengt dus minders security risks mee door het te automatiseren.  Indien wachtwoorden worden gelekt kan er gekeken worden wie verantwoordelijk waren voor de opslag van deze wachtwoorden.  En als laatste zal dit helpen met het voldoen aan de norm wachtwoorden op een beveiligde plek opslaan. |
| A.Mailsize | Centraal bijhouden hoeveel ruimte elke medewerker gebruikt voor mailopslag. | Niet | Het is niet essentieel maar kan handig zijn om te zien wie te veel data gebruikt voor wat of wie juist meer nodig heeft.  Automatiseren hiervan net als andere kost best veel geld en vereist veel middelen, dit kan ook uitdagingen meebrengen zoals testen en implementeren van nieuwe systemen hiervoor, er moet een analyse komen die bepaal of het waard is om dit soort data bij te houden automatisch.  Het brengt wel de nodige voordelen denk aan minder tijd om email op slag te beheren.  Het kan fouten voorkomen denk aan dubbele opslag etc. |
| A.Desktop | Controle op toelaatbaarheid achtergrondafbeelding werkstation. | Niet | Achtergrond afbeeldingen op werkstation kunnen beter onder een normvallen van bepaalde regels, en gebruikers hier op attenderen, om dit te automatiseren is wat mij betreft veel geld en tijd ergens steken wat niet echt nodig is.  Het zal de beveiliging verbeteren dat niemand zomaar iets als achtergrond neerzet en elke file download echter raad ik hier een goeie anti virus voor aan. |
| A.UserSignal | Signaleren als er iemand op een account met administratorprivileges inlogt. | Wel | Dit is belangrijk voor het bedrijf, zo weet je altijd wanneer er op een admin account wordt ingelogd, als deze persoon niet er is of niet werkt maar toch inlogt  Is er dus een security breach hierdoor wordt de beveiliging van infrastructuur en bestanden gewaarborgd.  De compliance voorschriften worden voldaan bijhouden van activiteiten en inlog van Admins of gebruikers met admin privileges.  Problemen kunnen makkelijker opgespoord worden doormiddel van een Audith Trail. |
| A.Monitor | Controleer servers op ongebruikelijke processen. | Wel | Ongebruikte processen op servers worden sneller opgespoord en gezien security standpunt.    De controle kan sneller worden uitgevoerd dus er worden tijd en middelen bespaard.  Compliance voorschriften worden voldaan.  Problemen worden beter opgespoord door audith trail dit helpt de organisatie. |
| A.PrintSignal | Controle of iemand zijn printouts bij de printer laat liggen. | Niet | Als je iets uitprint haal je dit op dit lijkt me logisch, er wordt zelfs een reminder gegeven op het werkstation dat deze wordt uitgevoerd en klaar is, twee aparte meldingen.  Meestal wordt er volgens de avg wet], dit op een locatie gedaan in kantoor met biometrisch beveiliging of pas beveiliging. Ook staat hier een papier versnipperraar als dit toch wordt gevonden bij de printer het vernietigd wordt.  Overigens wordt deze ruimte bewaakt met camera’s.  Dus is het van mij niet nodig om meer tijd en moeite plus middelen en geld in deze automatisering te steken. |