Verhogen digitale weerbaarheid, deel1: Processen

Change management

- ☐ Alle wijzigingen hebben een eigenaar
- ☐ Relevante testen worden met succes uitgevoerd
- ☐ Wijzigingen hebben goedkeuring nodig van de CAB
- ☐ Wijzigingen volgen de OTAP straat
- ☐ Wijzigingen worden alleen uitgevoerd in het onderhoudsvenster

Alle IT systemen en applicaties zijn de gehele levensduur aan wijzigingen onderhevig. Om de ICT omgeving te vernieuwen zonder disrupties is een goed changemanagement proces van belang. Zijn de voorgestelde changes wel getest en werkt alles naar verwachting?

Om wijzigingen op een gestuctureerde wijze te plannen, uitvoeren en documenteren is het changemanagement proces nodig. Hierdoor zijn de wijzigingen vastgelegd en moeten o.a. worden getest, gedocumenteerd, geautoriseerd en geimplementeerd. De BIO benoemt een aantal controls die hier van toepassing zijn. Dit zijn onder andere de normen: 9.4.4.2, 12.1.2, 12.1.4, 14.1.1, 14.2.2, 14.2.3, 15.1.2, 15.2.2, 18.1.4.

Volgt een wijziging dit proces niet dan kunnen ernstige gevolgen optreden zoals funtionaliteiten die niet meer goed of zelfs helemaal niet meer werken. Om dit verder vorm te geven heeft de IBD de producten “Handreiking proces changemanagement” en “Samenhang beheerprocessen en informatiebeveiliging“ontwikkeld. Deze producten zijn beschikbaar op de website van de IBD.

Is dit door mijn gemeente geregeld?

De onderstaande punten helpen u om te toetsen of deze maatregel binnen uw gemeente is getroffen

- ☐ Er is een formeel, beschreven, geaccepteerd en werkend changemanagement proces
- ☐ Er is een Change Advisory Board (CAB) die de impact van de changes onderzoekt en goedkeurt (met alle betrokken disciplines)
- ☐ Alle wijzigingen volgen voor in gebruik name een vastgestelde test en acceptatie route volgens het OTAP principe (Ontwikkel, Test, Acceptatie en Productie)
- ☐ Alle wijzigingen worden doorgegeven aan het configuratiemanagement proces zodat de configuratie database kan worden bijgewerkt
- ☐ Er wordt gerapporteerd over de geconstateerde afwijkingen in het changemanagement proces
- ☐ Een wijziging dient altijd een roll-back scenario te hebben
- ☐ Wijzigingen worden uitgevoerd op basis van SLA afspraken, bijvoorbeeld in een onderhouds-venster. Afwijkingen hierop worden zorgvuldig afgestemd en gecommuniceerd. (Bijvoorbeeld spoed wijzigingen)

Incident management

- ☐ Er wordt gekeken naar trends om verbeteringen te initiëren
- ☐ Medewerkers weten waar ze informatie-beveiligingsincidenten kunnen melden
- ☐ Er is een escalatie pad
- ☐ Elk incident heeft een eigenaar
- ☐ Incidenten worden naar prioriteit ingedeeld

Helaas zullen incidenten altijd plaatsvinden binnen een organisatie. Hoe er vervolgens mee wordt omgegaan is van groot belang. Zijn we in staat om snel te reageren op een incident om de schade zoveel mogelijk te beperken?

Prioritering voor het behandelen van incidenten is noodzakelijk, incidenten op belangrijke systemen of applicaties dienen met spoed opgepakt te worden. De prioriteiten zijn bepaald in de SLA. Door incidenten te registreren en de eventuele oplossing op te nemen kan in de toekomst een zelfde soort incident sneller verholpen worden en kan er een trendanalyse uitgevoerd worden. De volgende BIO controls zijn hierbij van toepassing: 5.1.1, 5.1.2, 9.4.4.2, 12.3.1, 12.4.2, 12.6.1, 13.2.2, 15.1.1, 15.1.2, 15.2.1, 18.1.4.

Betrek de CISO bij de afhandeling van informatiebeveiligingsincidenten. De IBD wil graag dat grote incidenten bij hen worden gemeld.

Om dit verder vorm te geven heeft de IBD de producten “Voorbeeld incident management en response beleid” en “Samenhang beheer-processen en informatiebeveiliging“ ontwikkeld. Deze producten zijn beschikbaar op de website van de IBD.

Is dit door mijn gemeente geregeld?

De onderstaande punten helpen u om te toetsen of deze maatregel binnen uw gemeente is getroffen

- ☐ Er is een formeel, beschreven, geaccepteerd incidentmanagement proces
- ☐ Incidenten (en eventuele oplossingen) worden centraal geregistreerd
- ☐ Incidenten worden naar prioriteit ingedeeld en behandeld
- ☐ Incidenten worden afgehandeld volgens de oplostijden, zoals gedefinieerd in de SLA
- ☐ Er wordt een eigenaar aan elk incident toegewezen
- ☐ Informatiebeveiligingsincidenten zijn makkelijk te onderscheiden van overige incidenten
- ☐ Er wordt periodiek gekeken naar trends om verbeteringen te initiëren
- ☐ Ten minste grote incidenten worden geëvalueerd
- ☐ De servicedesk is opgeleid om correct met informatiebeveiligingsincidenten om te gaan
- ☐ Incidenten kunnen ook buiten de kantooruren worden opgelost
- ☐ Medewerkers weten wat informatiebeveiligingsincidenten zijn en waar ze deze kunnen melden
- ☐ Er wordt gerapporteerd over de geconstateerde afwijkingen in het incidentmanagement proces
- ☐ Er is een duidelijk escalatie pad, voor het geval incidenten niet volgens de SLA opgelost kunnen worden

Configuratie-management

- ☐ Er is een actueel, volledig overzicht van alle configuratieitems (CI)
- ☐ Er wordt in het netwerk gescanned naar nieuwe hardware en software
- ☐ Elk Configuratie Item (CI) heeft een eigenaar
- ☐ De classificatie van de CI wordt vastgesteld door de eigenaar en wordt eenduidig vastgelegd.

Om een ICT omgeving veilig te houden, is het van belang om te weten wat er zich allemaal binnen die omgeving bevindt. Zijn alle apparaten in beheer bij de IT-afdelingen of zitten er nog onbekende apparaten in het netwerk? En zo ja, wat doen die dan precies?

Om zicht te houden op de samenstelling van de ICT infrastructuur van je gemeente is het van belang dat er een goede inventarisatie en registratie gemaakt wordt van alle apparaten (en hun functie/configuratie/software) die zich in het netwerk bevinden. Dit conform BIO controls 8.1.1, 8.1.3, 12.5.1.

Helaas kunnen zich in de ICT omgeving ook ongeautoriseerde apparaten huisvesten. Ongeautoriseerde apparatuur, ook wel shadow-IT genoemd, vormen direct een gevaar binnen de ICT infrastructuur van je gemeente. Ongeautoriseerde apparatuur doet vaak ongeautoriseerde dingen. Het is van belang om deze apparatuur zo snel mogelijk uit het netwerk te verwijderen. In sommige gevallen zijn ongeautoriseerde apparaten toch noodzakelijk voor het vervullen van een taak binnen de gemeente. In dat geval zal het betreffende apparaat in beheer genomen moeten worden door de IT afdeling, zodat alle noodzakelijke beheerprocessen van toepassing zijn op het betreffende apparaat. Om dit verder vorm te geven heeft de IBD de producten “Handreiking proces configuratie-management“ en “Samenhang beheer-processen en informatiebeveiliging“ontwikkeld. Deze producten zijn beschikbaar op de website van de IBD.

Is dit door mijn gemeente geregeld?

De onderstaande punten helpen u om te toetsen of deze maatregel binnen uw gemeente is getroffen

- ☐ Er is een formeel, beschreven en geaccepteerd configuratiemanagement proces
- ☐ Er is een actueel, volledig overzicht van alle Configuratie Items (CI)
- ☐ Er wordt periodiek gerapporteerd, passend bij de P&C cyclus, over de aanwezige hardware & software en geconstateerde afwijkingen in
- ☐ het configuratiemanagement proces
- ☐ Alle configuratie wijzigingen worden gelogd
- ☐ Alle CI’s hebben een eigenaar
- ☐ Er wordt in het netwerk gescand naar nieuwe hardware en software
- ☐ De classificatie van de CI wordt duidelijk opgeschreven
- ☐ Eens per jaar wordt de classificatie van bedrijfskritische systemen opnieuw getoetst door de eigenaar en indien nodig bijgesteld
- ☐ Indien er wijzigingen in de ICT infrastructuur plaatsvinden (via change management) dienen de gegevens in de Configuratie Management database (CMDB) geüpdatet te worden

Patch management

- ☐ Afspraken voor patches zijn vastgelegd in SLA’s
- ☐ Er is een proces voor spoedpatches
- ☐ Volg het change management proces voor de uitrol van patches
- ☐ Er wordt regelmatig gecontroleerd op relevante patches

Om kwetsbaarheden te verhelpen is het belangrijk om alle systemen regelmatig te patchen. Dit is te realiseren middels patch management. Patch management is het proces waarmee patches op gecontroleerde, beheerste (risico beperkende) wijze uitgerold kunnen worden. Patches zijn doorgaans kleine programma’s die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en / of hardware. Het uitrollen van patches dient volgens het change management proces te gaan. BIO control 12.6.1 beschrijft wat men moet doen om het risico van misbruik te minimaliseren.

Om dit verder vorm te geven heeft de IBD de producten “Patch management voor gemeenten” en “Samenhang beheer-processen en informatiebeveiliging“ ontwikkeld. Deze producten zijn beschikbaar op de website van de IBD.

Is dit door mijn gemeente geregeld?

De onderstaande punten helpen u om te toetsen of deze maatregel binnen uw gemeente is getroffen

- ☐ Er is een formeel, beschreven en geaccepteerd patchmanagement proces
- ☐ De uitrol van patches volgen het changemanagement proces
- ☐ De toegepaste patches dienen in de Configuratie Management Database toegevoegd te worden
- ☐ Er is een specifiek proces voor kritische/beveiligings patches (spoedpatches)
- ☐ Er wordt gerapporteerd over de geconstateerde afwijkingen in het patchmanagement proces
- ☐ Onderhoudsvensters voor de installatie van patches zijn gedefinieerd in de SLA
- ☐ Patches worden beoordeeld op relevantie. De meest recente, relevante patches dienen binnen de gestelde termijn te zijn geïnstalleerd
- ☐ Er wordt regelmatig gecontroleerd of nieuwe relevante patches zijn uitgebracht

VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

v. 1.1 dd. 9 december 2019