Verhogen digitale weerbaarheid, deel1: Maatregelen

1 Inventarisatie & beheer hardware/devices

- ☐ Inventariseer alle geautoriseerde apparatuur
- ☐ Verzamel de toegestane configuraties en sla deze centraal op
- ☐ Breng ongeautoriseerde hardware (shadow-IT) in kaart
- ☐ Bepaal de noodzakelijke acties voor zowel legitieme IT als shadow-IT

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 gemeenten 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, 8.3.1, 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 het product “Handreiking proces configuratiemanagement” ontwikkeld. Dit product is beschikbaar op de website van de IBD.

Is dit binnen mijn gemeente geregeld?

De onderstaande vragen helpen u om te toetsen of deze maatregel binnen uw gemeente is geïmplementeerd.
- ☐ Hardware/devices en device type zijn geïdentificeerd
- ☐ Mogelijkheid om een lijst met geïndentificeerde devices te maken en atributen te wijzigen indien nodig
- ☐ Alle hardware/devices hebben een eigenaar
- ☐ Er is een proces om hardware/devices te decommissioneren
- ☐ Alle hardware/devices zijn geregisteerd in een centraal overzicht
- ☐ Het overzicht is up to date & volledig
- ☐ Er is een gedocumenteerde definitie wat geautoriseerde apparatuur is
- ☐ Het doel van configuratiebeheer voor hardware/devices is eenduidig vastgelegd
- ☐ Er is een proces afgesproken dat het centrale overzicht periodiek evalueert
- ☐ Er wordt gerapporteerd over de aanwezige hardware/devices, geconstateerde afwijkingen en evaluatie van het proces

2 Inventarisatie & beheer software

- ☐ Inventariseer alle geautoriseerde software
- ☐ Verzamel de specifieke instellingen en sla deze centraal op
- ☐ Breng ongeautoriseerde software (shadow-IT) in kaart
- ☐ Bepaal de noodzakelijke acties voor zowel legitieme software als shadow-IT

Voor applicaties en software geldt hetzelfde als voor apparatuur. Het is noodzakelijk om goed inzicht te hebben in de geïnstalleerde software en om ongeautoriseerde software in kaart te brengen.

De te nemen maatregelen en acties zijn analoog aan die van ICT hardware. De “Handreiking proces configuratiemanagement” helpt hierbij. Dit product is beschikbaar op de website van de IBD.

Is dit binnen mijn gemeente geregeld?

De onderstaande vragen helpen u om te toetsen of deze maatregel binnen uw gemeente is geïmplementeerd.
- ☐ Software en software versie zijn geïndentificeerd
- ☐ Mogelijkheid om een lijst met geïndentificeerde software te maken en atributen te wijzigen indien nodig
- ☐ Alle software heeft een eigenaar
- ☐ Er is een proces om software te decommissioneren
- ☐ Alle software is geregisteerd in een centraal overzicht
- ☐ Het overzicht is up to date & volledig
- ☐ Er is een gedocumenteerde definitie wat geautoriseerde software is
- ☐ Het doel van configuratiebeheer voor software is eenduidig vastgelegd
- ☐ Er is een proces afgesproken dat het centrale overzicht periodiek evalueert
- ☐ Er wordt gerapporteerd over de aanwezige software, geconstateerde afwijkingen en evaluatie van het proces

3 Beheer kwetsbaarheden

- ☐ Onderzoek welke kwetsbaarheden in je ICT infra aanwezig zijn
- ☐ Bepaal de aanpak per gevonden kwetsbaarheid
- ☐ Registreer de gevonden kwetsbaarheden en hun oplossing

Kwetsbaarheden kunnen direct gevaar opleveren voor de ICT omgeving van de gemeente. Het is van belang om deze kwetsbaarheden te zoeken en te verhelpen. Een groot gedeelte van verstoringen binnen een ICT infrastructuur, veroorzaakt door indringers vindt een oorsprong in kwetsbaarheden binnen de ICT infrastructuur.

Om kwetsbaarheden te verhelpen is het belangrijk om alle systemen regulier te patchen. Dit is te realiseren middels patchmanagement.

Patchmanagement 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.

BIO control 12.6.1 beschrijft wat hiervoor ingericht zou moeten worden. De IBD heeft dit verder concreet uitgewerkt in het operationele product “Patchmanagement voor gemeenten”. Dit product is beschikbaar op de website van de IBD.

Is dit binnen mijn gemeente geregeld?

De onderstaande vragen helpen u om te toetsen of deze maatregel binnen uw gemeente is geïmplementeerd.
- ☐ Er is een anti malware beleid
- ☐ Kwetsbaarheden worden volgens het incident en change management proces verholpen
- ☐ Er is een proces om informatie over kwetsbaarheden en/of security incidenten te ontvangen (bijv. door IBD alerts)
- ☐ Er is een proces om kwetsbaarheden binnen de organisatie te onderzoeken
- ☐ Het is duidelijk wie er in de lead is om kwetsbaarheden te onderzoeken
- ☐ Alle systeemklokken zijn gesynchroniseerd met een nauwkeurige tijdbron (op het Internet)
- ☐ Kwetsbaarheden (en de eventuele oplossing) worden geregistreerd

4 Toegangsrechten

Medewerkers

- ☐ Gebruik enkel persoonlijke accounts, geen groepsaccounts
- ☐ Ken enkel de noodzakelijke rechten per rol toe
- ☐ Zorg dat wachtwoorden regelmatig gewijzigd worden
- ☐ Controleer de accounts en bijbehorende toegangsrechten frequent

Medewerkers:
Volgens het dreigingsbeeld voor gemeenten van de IBD vormt de eindgebruiker (bewust of onbewust) een van grootste dreigingen binnen het ICT-landschap. Om deze dreiging te verkleinen kunnen er een aantal maatregelen worden genomen op het gebied van logische gebruikers toegang. De BIO beschrijft deze maatregelen o.a. in controls 9.2.3, 9.2.4 en 11.2.1.

De minimale maatregelen die men met betrekking tot logische toegang voor gebruikers moet inregelen zijn:
– Gebruik unieke, naar personen herleidbare accounts.
– Ken alleen de noodzakelijke rechten toe per rol/account.
– Zorg dat het wachtwoord regelmatig moet worden gewijzigd.
– Dat het wachtwoord pas na 6 andere wachtwoorden weer mag worden gebruikt.
– Dat op reguliere basis de accounts en bijbehorende rechten worden gecontroleerd.

Beheerders:
Beheerders hebben vaak speciale accounts met meer rechten. Met deze rechten kunnen zij bijvoorbeeld nieuwe gebruikers aanmaken, wijzigingen doorvoeren en rechten van gebruikers uitbreiden of beperken. Als er misbruik gemaakt kan worden van deze beheeraccounts zou men schade kunnen aanrichten of zichzelf toegang kunnen verschaffen tot (bijzondere) persoonsgegevens.

BIO control 9.2.3 en 9.2.4 beschrijven hoe deze beheeraccounts moeten worden beschermd. In ieder geval moet de toegang tot beheeraccounts worden beschermd met behulp van twee factor authenticatie en mogen deze niet meer rechten hebben dan strikt noodzakelijk. Beheeraccounts worden enkel voor specifieke beheertaken gebruikt.

Met name voor de authenticatie van gebruikers en beheerders heeft de IBD het product “Wachtwoordbeleid” ontwikkeld. Dit product is beschikbaar op de website van de IBD.

Additioneel voor beheerders (privileged)

- ☐ Geef enkel toegang tot de noodzakelijke set van applicaties en commando’s
- ☐ Maak gebruik van two-factor authentication

Machine accounts

- ☐ Geef deze accounts minimale rechten, enkel voldoende voor de uit te voeren taak
- ☐ Gebruik een uniek account per service

Machine accounts:
Voor het uitvoeren van bepaalde geautomatiseerde taken, maakt men vaak gebruik van hiervoor bedoelde services op een computer/server. Een service is een computerprogramma dat op de achtergrond de betreffende taken uitvoert in het ICT-landschap.

Een dergelijke service maakt gebruik van een account met speciale rechten, om deze taken te kunnen uitvoeren. Dit noemt men een “Machine account”.

Een service is ook vatbaar voor misbruik en moet dus passend beschermd worden. In controls 9.2.3, 9.2.4 en 11.2.1 van de BIO wordt beschreven beschreven welke maatregelen van toepassing zijn voor zo’n service. Minimaal moet men hier het volgende voor inregelen:
– Iedere service gebruikt een eigen, uniek account.
– Het account beschikt over minimale rechten voor het uitvoeren van de taak.
– De accounts en bijbehorende rechten worden regelmatig geëvalueerd.

Is dit binnen mijn gemeente geregeld?

De onderstaande vragen helpen u om te toetsen of deze maatregel binnen uw gemeente is geïmplementeerd.
Algemeen:
- ☐ De organisatie heeft een centrale identity repository (bijv. AD)
- ☐ Alleen geautoriseerde gebruikers kunnen veranderingen aanbrengen binnen de indentiteit repositories
- ☐ Identiteiten kunnen gegroepeerd worden (categorieën afgestemd op organisatie)
- ☐ Om diensten en informatie te gebruiken is het nodig om gebruikers te authenticeren en te autoriseren
- ☐ Er is een wachtwoordbeleid dat de eisen beschrijft van een sterk wachtwoord die voldoet aan best practices
- ☐ Wachtwoorden mogen pas na 6x hergebruikt worden
- ☐ Het wachtwoordbeleid wordt met techniek geforceerd
- ☐ Alle accounts krijgen enkel de rechten die ze nodig hebben voor hun werk
- ☐ Er is een werkproces om wachtwoorden te verstrekken en te wijzigen op een veilige manier

Medewerkers:
- ☐ Er is een proces voor nieuwe medewerkers, medewerkers die van functie wijzigen en medewerkers die de organisatie verlaten
- ☐ Minimaal eens per 60 dagen wordt gecontroleerd of gebruikers nog toegang nodig hebben tot bepaalde informatiesystemen
- ☐ Accounts zijn uniek en naar een persoon te herleiden

Admin:
- ☐ Het gebruik van generieke admin accounts is minimaal
- ☐ Administrators gebruiken persoonlijke admin accounts en gebruiken deze enkel om activiteiten uit te voeren waar deze rechten voor nodig zijn
- ☐ Het aantal gebuikers met administator rechten is geminimaliseerd
- ☐ Er wordt geen gebruik gemaakt van groepsaccounts
- ☐ Admins maken ALTIJD gebruik van multifactor authenticatie

Machine Accounts:
- ☐ Per service wordt een uniek (machine) account gebruikt

5 Veilige configuraties

Software / applicaties

- ☐ Verander standaard wachtwoorden
- ☐ Pas standaard instellingen aan die tot misbruik kunnen leiden
- ☐ Installeer alleen de componenten die men nodig heeft
- ☐ Gebruik standaarden van de PTLU lijst

Bij het volgen van een default installatie van software pakketten en applicaties wordt er vaak gebruik gemaakt standaard instellingen en standaard wachtwoorden. Dit zijn ingangen voor misbruik van de betreffende software.

Het is zaak om deze standaard instellingen direct aan te passen, nog voordat de applicatie in productie gezet wordt. Het is daarbij verstandig om bij de configuratie van software en applicaties een bewezen baseline te volgen.

BIO controls 12.5.1 en 12.6.1 zijn hierop van toepassing.

De IBD heeft een baseline opgesteld met daarin de meest basale aandachtspunten bij het installeren van nieuwe software. Deze baseline is beschikbaar op de site van de Informatiebeveiligingsdienst.

Meer informatie over de PTLU lijst is te vinden op de website van het Forum Standaardisatie.

Is dit binnen mijn gemeente geregeld?

De onderstaande vragen helpen u om te toetsen of deze maatregel binnen uw gemeente is geïmplementeerd.
Software / applicaties:
- ☐ Software voldoet aan standaarden van de PTLU lijst
- ☐ Standaard instellingen zijn aangepast
- ☐ Standaard wachtwoorden zijn gewijzigd
- ☐ Software / applicaties zijn voorzien van de juiste patches

Netwerk app. & Firewalls

- ☐ Ongebruikte poorten dichtzetten
- ☐ Meest recente software geïnstalleerd
- ☐ Toegang beperkt tot enkel geautoriseerde beheerders

Om de ICT infrastructuur te beschermen voor gevaren/indringers van binnenuit ven buitenaf hebben veel gemeenten een firewall. Deze firewall blokkeert en filtert o.a. schadelijk internetverkeer. Een dergelijke firewall dient tevens zelf goed beschermd worden tegen indringers. Dit geldt ook voor de onderliggende netwerkapparatuur van de ICT Infrastructuur.

De BIO benoemt een aantal controls die hier van toepassing zijn. Dit zijn onder andere de controls: 9.2.4, 9.4.2, 12.5.1, 12.6.1, 13.1.1, 13.1.3.

Voorbeeld van concrete invulling: Laat systeembeheerders ongebruikte poorten dichtzetten en regelmatig de meeste recente software installeren. En verder beperk het aantal beheerders van de firewall en netwerkapparatuur tot een minimum.

Samengevat kan men stellen dat deze normen (en de activiteiten die daar uit voortvloeien) vallen onder de noemers “Hardening” en “Patchmanagement”.

De IBD heeft dit verder uitgewerkt in de producten “Hardeningbeleid voor gemeenten” en “Patchmanagement voor gemeenten”.
Deze producten zijn beschikbaar op de website van de IBD.

Servers

- ☐ Schakel ongebruikte services uit
- ☐ Zet ongebruikte poorten dicht (Host-FW)
- ☐ Webservers: Gebruik HTTPS en HSTS (PTLU-lijst)
- ☐ Zorg dat alle patches geïnstalleerd zijn
- ☐ Anti-Malware

Een server is een computer waarop websites of andere services draaien die door meerdere computers via een lokaal netwerk of het internet gebruikt kunnen worden. Bij een standaard inrichting van een server worden er vaak (ondersteunende) services geïnstalleerd die niet worden gebruikt en worden onnodige netwerkpoorten open gelaten.

Om een server tegen misbruik te beschermen moet deze worden ‘gehardend’. BIO control 12.5.1 en 12.6.1 beschrijven wat men moet doen om het risico van misbruik te minimaliseren.

Men moet hier minimaal het volgende voor doen:
– Het uitzetten/verwijderen van ongebruikte services.
– Het sluiten van ongebruikte netwerkpoorten.
– Het regelmatig patchen van de geïnstalleerde (systeem) software.

Samengevat kan men stellen dat deze controls (en de activiteiten die daar uit voortvloeien) vallen onder de noemers “Hardening” en “Patchmanagement”.

De IBD heeft dit verder uitgewerkt in de producten “Hardeningbeleid voor gemeenten” en “Patchmanagement voor gemeenten”. Deze producten zijn beschikbaar op de website van de IBD.

Werkstations (End-points)

- ☐ Zorg dat alle patches geïnstalleerd zijn
- ☐ Anti-Malware

Is dit binnen mijn gemeente geregeld?

De onderstaande vragen helpen u om te toetsen of deze maatregel binnen uw gemeente is geïmplementeerd.
Servers:
- ☐ Anti malware software is op alle servers geïnstalleerd
- ☐ (Web) servers gebruiken HTTPS / HSTS
- ☐ Servers zijn voorzien van de juiste patches
- ☐ Het aantal accounts & beheerders is geminimaliseerd op de servers
- ☐ Er vindt logging plaats op alle servers
- ☐ Ongebruikte poorten zijn gedeactiveerd
- ☐ Er is een proces voor wijzigingen/updates op de server

Endpoints:
- ☐ Anti malware software is op alle eindpoints geïnstalleerd
- ☐ Endpoints zijn voorzien van de juiste patches

Verhogen digitale weerbaarheid deel 1: is grotendeels gebaseerd op de eerste 5 CIS Basic Critical Security Controls V7 in relatie met de BIO. De 6de control wordt geadresseerd in de volgende stap: Monitoring & Response.

Basic CIS Controls
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, monitoring and Analysis of Audit Logs (Volgt in een toekomstige module)

VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

v. 1.1 dd. 9 december 2019