VERSLAG

Commissie 2: lokale economie en interne organisatie

Verslag van: 26-06-2023 van 19 u-15 - 20u15

Agenda: agendapunten mbt GR van schepen Poffé en schepen Huts

Verslaggever: Lucia Dewolfs

Voorzitter: Lucia Dewolfs

Aanwezig: Eddy Poffé, Rudi Hendrickx, Lucia Dewolfs, Daniel Vanluyten, John Vankeijenberg,, Joël Dereze, Gijsbrecht Huts, Jean Defau, Christophe Hendrickx, Nicky Martens;

Verontschuldigd: Bart Maes, Nele Daenen; Peter Loosen, Fabio Vanderlinden, Werner Thomas, Kris Franssens

---

1 Goedkeuring verslag mei 2023

Verslag van de commissievergadering van mei wordt goedgekeurd

Aanwezigheidslijst wordt door de aanwezigen ondertekend.

2. Agendapunten GR

Voorstelling door Patricia Willems (AD)

en Kenny Denruyter (ICT)

Organisatiebeheersingsrapport 2023

Decretale opdracht

Gestart in 2020

Voorstelling door MAT gebeurd en ook voorstelling voor de GRaad

Cfr ppt van de AD als bijlage

vraag raadslid : J.Vankeijenberg mbt veiligheid/preventie

> de stad is wat betreft preventie /veiligheid aangesloten bij Interleuven, waar ze via haar lidmaatschap kan beroep doen op een vaste deskundige; die via de diverse aangesloten stadsdiensten de veiligheid/preventie op punt stelt/houdt.

Een pluim voor de stad Tienen dienst ICT : case stad Tienen wordt door Cronos voorgesteld in najaar op roadshow Oost-Vlaanderen

3. Variapunten

Rondvraag over mogelijke variapunten bij de commissieleden : geen

De vergadering wordt beëindigd om 20u, gezien ook andere gelijklopende activiteiten in de stad voor schepenen en raadsleden.

Volgende commissie op maandag 25 september 2023.

Voorzitter en Verslaggever

Lucia Dewolfs

Organisatiebeheersings-rapport 2023

tienen

Organisatiebeheersing & -ontwikkeling: kader

- managementteam 14 mei 2024
- gemeenteraad 28 mei 2024
- raad voor maatschappelijk welzijn 25 juni 2024

→ rapportering gebeurt jaarlijks uiterlijk voor 30 juni

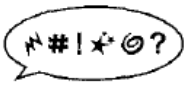
tienen

Inhoud

1. DEEL I - Jaarlijkse rapportering klachtenbehandeling
2. DEEL II - ICT Security
3. DEEL III - Informatieveiligheid
4. DEEL IV - Zelfevaluatie managementteam
5. DEEL V - Inspectie *POD Maatschappelijke Integratie*
6. DEEL VI - Veiligheid en preventie

tienen

1



Organisatiebeheersing & -ontwikkeling deel 1: klachtenbehandeling

reglement op het registreren en behandelen van klachten voor de stad en het *OCMW*
24 februari 2022 gemeenteraad
31 maart 2022 raad voor maatschappelijk welzijn

→ jaarlijks verslag over de opvolging van de klachten

→ hier
verslag jaarlijkse rapportering klachtenbehandeling 2022

tienen

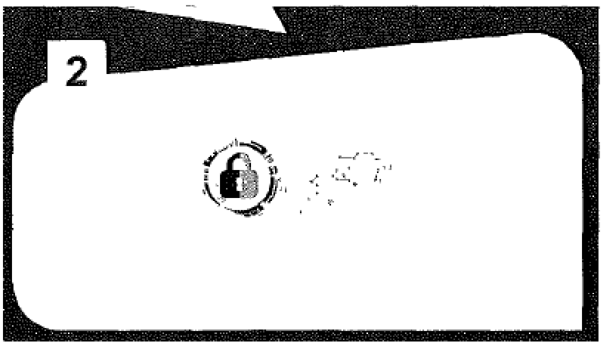
Organisatiebeheersing & -ontwikkeling: deel 1: klachtenbehandeling

ook in het OBR: het klachtenreglement

Art 1 ... doelstelling ... kunnen leiden tot verbeteracties teneinde een structurele oplossing te bieden voor vaak voorkomende problemen

→ Klachtenbeheer als bron voor verbetering werking

tienen



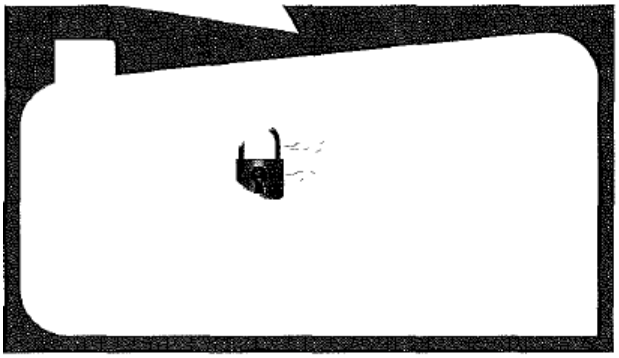
Organisatiebeheersing & -ontwikkeling deel 2: ICT Security

1 M365 security
- ✓ beveiligingstraject
- ✓ [illegible]
- ✓ digitaal paspoort
- ✓ datatraject

2 Hacking
- ✓ *acties geïmplementeerd*

3 Security audit Deloitte
- ✓ pijnpunten en de te ondernemen acties

tienen



Organisatiebeheersing & -ontwikkeling deel 3: informatieveiligheid

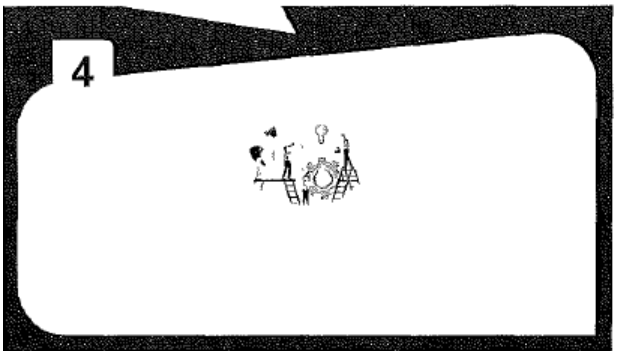
Meerjarenplan 2020-2025

BO14 = het maximaal digitaliseren van de organisatie

AP23 = een strategie uitwerken voor ICT, data en informatieveiligheid

ACTUS = beheren en bewaren van onze papieren en digitale informatie op een doordachte, volgens en volledige manier & verder werken aan de uitvoering van ons informatieveiligheidsbeleid

tienen



Organisatiebeheersing & -ontwikkeling deel 4: zelfevaluatie MAT

Basis = uitgebreide zelfevaluatie MAT (voorjaar 2023)
→ verbeterpunten

Prioriteiten voor het MAT
1 = Procesmanagement
2 = Rapporteren
3 = Continuïteitsplanning
4 = Ondersteuning in doordachtig gevolgde stukken
5 = Informatiebeheer

tienen

5

Organisatiebeheersing & -ontwikkeling deel 5: inspectie POD MI

POD MI
=Programmatische (federale) Overheidsdienst
Maatschappelijke Integratie

1. Jaarlijkse inspecties van de OCMW's
   → zie gebiedsgericht inspectietoezicht
2. Procesanalyse
   → zie SWZ dossiering: actieplan

Diensten

6

Organisatiebeheersing & -ontwikkeling deel 6: veiligheid en preventie

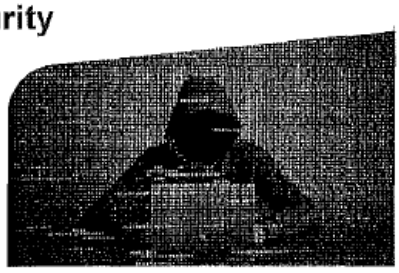
Globaal preventieplan (GPP) 2022-2025
- ✓ Werkgroep voorjaar 2022: update GPP
- ✓ GPP op 18 mei '22 Bestuurlijk Comité (BOC)
- ✓ GPP op 7 november '22 management team (MAT)
- ✓ GPP najaar 2023 opnieuw naar BOC en MAT
- ✓ GPP wordt minstens maandelijks geactualiseerd

In het OBR is een actuele stand van zaken bijgevoegd

Diensten

ICT security
Cyber security

Strategie & acties



tienen

Constante dreiging

"Het nieuwe normaal"

De M365 omgeving van een groot aantal medewerkers staat onder constante dreiging van hackers

Deze aanvallen kan je niet stoppen en zullen ook niet verminderen

Je moet de nodige acties ondernemen om de toegang te blokkeren aan de poort en het de hacker zo moeilijk mogelijk maken

Dat geldt ook voor je persoonlijke digitale omgeving bij je thuis (b.v. facebook e-mail ...)

tienen

Belang van alerte medewerkers

User awareness training

Social engineering – op afstand
- Doordrikken op phishing mails
  OPO training

Social engineering – persoonlijk
- Fys ele toegang verlenen aan onbevoegden
- USB sticks van derden
- Opsturen van gedownloade datenare bestanden

tienen

Iedereen is feilbaar

Iedereen kan gehacked worden

ICT infrastructuur is vergelijkbaar met een huis

Je kan het maximaal beschermen, mede binnen geraken lukt altijd, al dan niet mits het afgaan van diverse alarmbellen

Het is een kwestie van
- maximaal preventief te beschermen
  De kwetsbaarheden te beperken
  je (offline) back ups te waarmen

tienen

Inhoud

1. Aanzet tot aandacht voor veiligheid
2. *M365 evolutie & beveiliging*
3. Acties hacking Antwerpen & Diest
4. Acties security audit Deloitte

tienen

1. Aanzet tot aandacht voor ICT Security

Security Audit Deloitte via kabinet Somers

Maart 2020 > Rapport Deloitte
- Een nulmeting voor het bestuur
- Een oplijsting van aandachtspunten

Dienst ICT Stad Tienen
- Koppelen van actiepunten aan de aandachtspunten
- Stellen van prioriteiten in verdere uitrol digitalisering
- Vrijmaken van budgetten voor digitale veiligheid

- Opstart en opvolging van een beveiligingstraject

tienen

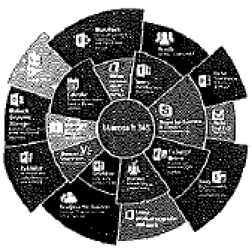
2. M365 Evolutie & Beveiliging

Wat is M365?

M365 is de afkorting voor Microsoft365

Dit is de verzamelnaam voor alle applicaties die worden aangeboden aan de medewerkers van de stad via het cloud platform van Microsoft. Deze is ook een beleving binnen de organisatie

- Office = Word, Excel, Powerpoint, Outlook
- Extra online tooling
  - SharePoint & OneDrive
  - Teams
  - Planner
  - OneNote



tienen

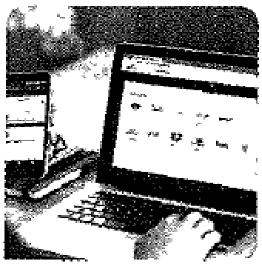
2. M365 Evolutie & beveiliging

Beveiligingstraject via Cronos (Secwise)

Beschermen van digitale identiteit & toegang
- Standaardiseren van de licenties op M365 E3 (budgettaire impact)
- Meerfactorauthenticatie implementeren
- *Voorwaardelijke toegang implementeren*

Veilig installeren en beheren van toestellen via M365 cloud
- Toestellen installeren met de juiste applicaties op basis van het e-mail adres (auto-pilot)
- Smartphones of tablets voorzien van een werkprofiel met *applicaties van de stad*
- Mogelijkheid om toestellen van op afstand te blokkeren of bedrijfskritische informatie te wissen
- Opvolgen van updates voor Windows of Microsoft Office om kwetsbaarheden te ondervangen
- Uitrollen applicaties en versiebeheer via centraal platform
- Versleutelen van de data op alle laptops & desktops van de stad (onbruikbaar bij diefstal)

tienen



2. M365 Evolutie & beveiliging

Meerfactorauthenticatie

Meerfactorauthenticatie is het bewijzen van je digitale identiteit (wachtwoord) aan de hand van een extra factor die bij die identiteit

Typisch via smartphone-app, sms of oproep

Andere voorbeelden zijn gezichtsherkenning, vingerafdruk of applicaties zoals de itsme app

tienen

2. M365 Evolutie & beveiliging

Voorwaardelijke toegang

Voorwaardelijke toegang is veelzijdig. Het bepaalt wanneer en hoe vaak meerfactorauthenticatie wordt gevraagd, maar het is ook een extra beveiligingslaag op je digitale M365 identiteit. Enkele voorbeelden:

- Enkel toestellen die veilig zijn krijgen toegang tot de M365 omgeving (bv. een laptop met antivirus moet actief zijn...)
- Enkel toestellen binnen de BENELUX krijgen toegang
- Toestellen die gekend zijn op onze lokale systemen worden als veilig beschouwd en vragen minder frequent naar meerfactorverificatie

tienen

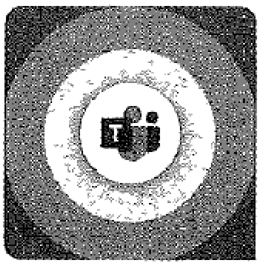
2. M365 Evolutie & Beveiliging

Data architectuur van de toekomst

Medewerkers van de stad Tienen gebruiken Teams vandaag als werkomgeving

- Communicatieplatform: telefonie, beeldbellen, chat
- Samenwerkingsplatform
  - Dienstenteams
  - Projectteams
  - Overlegteams
- Data wordt langzaam maar zeker meegenomen

Een degelijke beveiliging van het dataplatform van de toekomst is essentieel!



tienen

2. M365 Evolutie & beveiliging Vandaag is niet morgen

Een verzekering voor de toekomst

Wat vandaag werd opgezet, is morgen al verouderd. Een degelijke opvolging en regelmatige bijsturing is essentieel om digitaal veilig te blijven.

CARE contract

- Mogelijkheid tot escaleren van meldingen
- Directe lijn met beveiligingsexperts

CONNECT contract

- Om de vier maanden een audit van een specifiek deel van onze M365 beveiliging
- Rapport met te ondernemen acties
  - Intern op te nemen
  - Te escaleren via CARE tickets

tienen

"Meerstapsverificatie & voorwaardelijke toegang zijn vandaag essentiele bouwstenen voor een veilige omgeving."

"Door applicaties te koppelen aan de M365 omgeving (moderne authenticatie) verhogen we verder de veiligheid van onze applicaties."

3. Hacking besturen Acties

Hacking *Antwerpen en Diest* December 2022

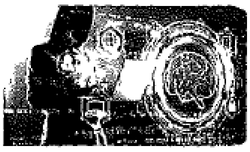
Oorzaken waren divers

- Geen bescherming van de digitale identiteit via meerfactorauthenticatie of voorwaardelijke toegang
- Eenvoudig doelwit voor ethische hackers door bv. het gebruik van post-its met gebruikersinformatie op publieke toestellen.
- Lekken in software van de toepassingen & hardware van grote leveranciers
- Gebrek aan opvolging/beheer van updates
- Offline backup werd niet gevoerd
- Omgeving thuiswerkers vertoonde kwetsbaarheden

Context ICT Stad Tienen

- Zette als één van de eerste lokale besturen bij de stap naar een hogere beveiliging (punt 2)
- Voerde 6x bij software en hardware interventies op om de systemen veilig te maken
- Vraagt steeds met de veiligheidsdienst de aandacht op bij gebruikers om het bewustzijn van digitale dreiging te verhogen.
- Ondernam enkele specifieke bijkomende acties

tienen



3. Hacking besturen Acties

Aanpassen back-up strategie

Hoe ging men te werk bij de getroffen besturen?

- De back-up software zat niet op de laatste versie. Een digitale achterpoort werd uitgebuit door hackers om toegang te verkrijgen
- Via deze toegang ging men bekijken waar de key's van back ups werden geplaatst
- Men vond toegang tot deze locaties en infecteerde de offline backup
- Vervolgens infecteerden ze alle lokale back ups
- Tenslotte infecteerden ze de live data
- 14 dagen na de hacking werd alles pas zichtbaar in de live omgeving en waren de backups voor de besturen reeds onbruikbaar gemaakt

tienen

3. Hacking besturen Acties

Aanpassen back-up strategie

Hoe beschermt de stad Tienen zijn omgeving hier tegen?

- Update backup software wordt opgevolgd door de leverancier
- De offline backup wordt in tegengestelde richting gemaakt
- De offline backup wordt wekelijks geplaatst op twee wisselende offline opslagmedia (8 versies)
- De hop wordt volledig & afgeschermd via hardware- en softwarematige firewalls (start copy: poorten open / end copy: poorten dicht)
- We gebruiken hiervoor minder kostelijke Linux systemen
- Traceerbaarheid & infectie worden onoverzichtelijk voor een hacker

tienen

3. Hacking besturen Acties

Een veiligere omgeving voor thuiswerk

Thuiswerken via laptop
- Enkel via opzetten van beveiligde (VPN) verbinding
- Enkel specifieke gebruikers die tot een bepaalde groep behoren kunnen deze verbinding starten
- *Moderne authenticatie* wat wil zeggen dat wachtwoord en meerstapsauthenticatie nodig zijn om toegang te verkrijgen

Thuiswerken voor medewerkers zonder laptops
- De onveilige omgeving (zie kwetsbaarheid hacking rapporten & de audit) werd uit dienst gesteld
- Een veilige omgeving werd aangeschaft ter vervanging met toegang via wachtwoord en meerfactorauthenticatie

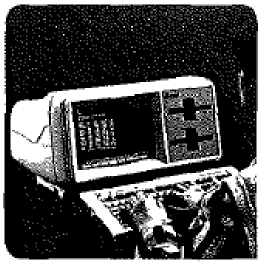
"Het vrijwaren van de offline backup is het meest kritische aandachtspunt binnen ICT security en Disaster Recovery, een verzekering om terug te keren naar een bepaald punt in de tijd."

4. Security Audit Andere acties

Gedateerde systemen van leveranciers

Een aantal kwetsbaarheden zijn de verantwoordelijkheid van de softwareleveranciers

- Verouderde servers, kwetsbare systemen & applicaties
  - De desbetreffende servers werden
    - Gemigreerd naar nieuwe recente servers
    - *Onder SLA contract geplaatst inzake proactieve updates & beschikbaarheid van de toepassingen.*



4. Security Audit Andere acties

Diverse kwetsbaarheden in opzet serveromgeving

Deze kwetsbaarheden waren de verantwoordelijkheid van de leverancier die de omgeving had opgezet

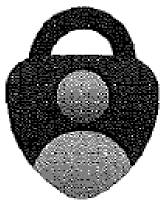
- Leverancier werd diverse keren aangeschreven
- Leverancier werd in gebreke gesteld
- Contract werd beëindigd
- *Schadevergoeding ontvangen*
- Een andere oplossing werd geïmplementeerd met de actiepunten uit de audit als concrete aandachtspunten

4. Security Audit Andere acties

Ontbreken van moderne authenticatie

Moderne authenticatie (meerstapsverificatie of toegang via ...) ontbreekt vaak op applicaties van externe leveranciers. Twee- of meerstapsverificatie is een vorm van moderne authenticatie

- Leveranciers die het kunnen implementeren hebben de aanpassing doorgevoerd
- Sommige leveranciers kunnen dit (niet) implementeren
  - Druk wordt opgevoerd
  - Andere applicaties dienen te worden overwogen in de toekomst



tienen

tienen

4. Security Audit Andere acties

Wachtwoordbeleid

Het wachtwoordbeleid werd op bepaalde vlakken aangepast door de dienst ICT

- Lokale beheerderswachtwoorden
  - Zijn niet meer op elke computer dezelfde
  - Veranderen elke dag automatisch
- Gebruikerswachtwoorden
  - Zijn minstens 12 karakters lang
  - Verstrijken jaarlijks
  - Worden gecombineerd met meerstapsverificatie en voorwaardelijke toegang

Wachtwoorden vervallen altijd, de optie "wachtwoord vervalt nooit" wordt niet meer toegelaten

4. Security Audit Andere acties

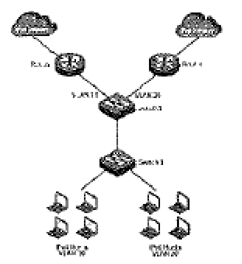
Beperken van <u>externe</u> beheerderstoegangen

Externe beheerderstoegang door leveranciers voor het onderhoud van hun systemen wordt beperkt in tijd door

- Standaard uitschakelen van de beheerders
- Activeren van deze beheerders op afroep

Voor systemen waar dit niet mogelijk is dienen we in de toekomst te kijken naar mogelijke cloud migraties

tienen



tienen

4. Security Audit Andere acties

Netwerksegmentatie & beveiliging

De bezorgdheden rond netwerksegmentatie werden ter harte genomen en ondertussen zijn servers in een gescheiden netwerk geplaatst

Netwerktoegangsbeveiliging (NAC) zal volledig in dienst worden genomen tegen oktober 2023. Dit *belet hackers om toegang tot ons netwerk te verkrijgen* via eigen (onveilige) toestellen.