Patchmanagementbeleid Gemeente Tilburg

Het patchmanagementbeleid van de Gemeente Tilburg geeft richting aan de wijze waarop de gemeente maatregelen wenst te treffen voor een adequate inrichting en uitvoering van patchmanagement. De gemeente onderschrijft het belang van patchmanagement omdat het niet op een gestructureerde wijze bijhouden van patches voor gemeentelijke systemen er voor kan zorgen dat kwetsbaarheden van die systemen toenemen. Dit beleid is van toepassing op iedereen die binnen de gemeente een rol heeft in het uitvoeren van patchmanagement.

De volgende uitgangspunten zijn vastgesteld voor de gemeente Tilburg en deze zijn ontleend aan het gemeentelijk informatiebeveiligingsbeleid, ISO 27002 en de BIO:

1. Dit is het patchmanagementbeleid opgesteld en door het MT van de afdeling Informatietechnologie goedgekeurd.
2. Er is een proces ingericht voor het beheer van kwetsbaarheden en patching van (systeem) software binnen de gemeente. (Kwetsbaarheden kunnen zich onder andere voordoen binnen Applicaties, Systemen , Websites, Devices (Laptops, IOT) etc.
3. Het uitvoeren van patches volgt het changemanagement proces.
4. Onderdelen van onze informatievoorziening moeten (bij voorkeur geautomatiseerd) gecontroleerd kunnen worden of de laatste updates (patches) zijn doorgevoerd.
5. Het doorvoeren van een patch vindt niet geautomatiseerd plaats. Uitzonderingen worden afgestemd in de taakgroep informatiebeveiliging en gedocumenteerd.
6. Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden besproken (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch). Bij deze risicoafweging wordt minimaal de systeemeigenaar betrokken. Bij vermoeden van hoog risico wordt de taakgroep informatiebeveiliging geconsulteerd.
7. Alle updates en patches dienen voor installatie te worden getest op toepasbaarheid en betrouwbaarheid.
8. Behoudens de door de leverancier goedgekeurde updates worden er geen wijzigingen aangebracht in programmapakketten en infrastructurele programmatuur.
9. Alleen officieel door de leverancier geleverde patches en updates worden geïnstalleerd.
10. Voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden updates/patches zo spoedig mogelijk doorgevoerd, echter maximaal binnen één week. Minder kritische beveiligingsupdates/-patches moeten worden ingepland bij de eerst volgende onderhoudsronde van het systeem. Hierbij volgens we de lijnen en berichtgeving vanuit de Informatiebeveiligingsdienst (IBD) en Nationaal Cyber Security Centre (NCSC).
11. Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van het Nationaal Cyber Security Centre (NCSC) of voor gemeenten door een CERT zoals de Informatiebeveiligingsdienst (IBD).
12. Als een functionele patch is aangebracht dient conform het changeproces de documentatie te worden bijgewerkt met de nieuwe versienummers van componenten.
13. Als een systeem gepatched is wordt de systeemdocumentatie bijgewerkt naar de laatste stand van zaken, de configuratie management database wordt geüpdate met de nieuwe versienummers van componenten.

14. Van alle uitgevoerde en bewust niet uitgevoerde patches wordt door de ICT beheerders een logboek bijgehouden waarin de afweging is beschreven.
15. Maandelijks wordt de status van niet uitgevoerde patches gerapporteerd naar de betrokken teammanagers. Indien de patches structureel niet worden uitgevoerd escaleert de teammanager naar de CISO en proceseigenaar.