

Your Logo Here

**Patch management**

beleid

|  |  |
| --- | --- |
|  | DisclaimerDit document kan gebruikt worden als template voor het opzetten van een patch managementbeleid binnen jouw organisatie. Dit document bevat een aantal uitgangspunten die je kan opnemen in je eigen patch managementbeleid. Niet alle uitgangspunten zullen van toepassing zijn, maak daarom een eigen afweging om bepaalde uitgangspunten wel of niet op te nemen. Naast de input uit dit document is het belangrijk input te verzamelen van de verschillende afdelingen binnen je organisatie. [organisatie] – Patch management beleid**Doel:**  Dit document beschrijft de beleidsuitgangspunten ten aanzien van informatiebeveiliging voor de invulling van het patch managementbeleid. Patch managementbeleid geeft richting aan de wijze waarop een organisatie maatregelen wenst te treffen voor een adequate inrichting en uitvoering van patch management. Het doel van patch management is tweeledig:1. Het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde informatievoorziening;
2. Het op een zo efficiënt mogelijke wijze en met zo min mogelijk verstoringen creëren van een stabiele (veilige) informatievoorziening.

Patch management is gericht op het verminderen van risico’s als gevolg van benutting van gepubliceerde technische kwetsbaarheden. **Scope:** De uitgangspunten opgesteld in dit document gelden voor alle werknemers en leveranciers van [organisatie] die toegang hebben tot de systemen en het netwerk van [organisatie], hierbij wordt geen onderscheid gemaakt tussen apparaten van [organisatie] en/of persoonlijke apparaten.**Patch definitie:** Nieuwe versie van software. In deze nieuwe versie heeft de leverancier kwetsbaarheden in het systeem hersteld. Hij heeft geen nieuwe functies toegevoegd (Cybersecurity Woordenboek, 2019). **Policy**Alle medewerkers van [organisatie] spelen een rol als het gaat om het patchen van apparaten/software met als doel het oplossen van kwetsbaarheden en daarmee mitigeren van risico’s als gevolg van misbruik van deze kwetsbaarheden. De mate van verantwoordelijkheid is afhankelijk van de functie van de desbetreffende medewerker. 1. Alle medewerkers:
2. Schakel de functie - automatisch updaten - in op al je apparaten die verbonden zijn aan het netwerk van [organisatie] , inclusief persoonlijke apparaten. Hetzelfde geldt voor de besturingssystemen waar je gebruik van maakt (bijvoorbeeld Windows, OS X, iOS, Android, etc.);
3. Negeer de automatische update notificaties van je apparaten/software niet. Zorg ervoor dat je de update zo snel mogelijk, maar tenminste binnen 24 uur installeert;
4. Geef de voorkeur, tijdens een selectieproces voor software of cloud diensten, aan leveranciers die een adequaat en effectief patching beleid en de daarbij behorende procedures hebben.
5. IT afdeling
6. Zorg ervoor dat patches worden geïnstalleerd, of worden geïnstalleerd om te testen, binnen 72 uur nadat de patch uitgebracht is door de leverancier van systemen in jouw infrastructuur;
7. Abonneer je op alle notificatie mogelijkheden van relevante leveranciers om zo tijdig notificaties van patches te ontvangen;
8. Patches voor kritieke systemen en of software dienen idealiter eerst te worden getest alvorens deze in de *productie* omgeving worden geïmplementeerd;
9. Afbeelding met tekening  Automatisch gegenereerde beschrijvingOngeacht of er wel of geen relevante kwetsbaarheidsberichten zijn dienen de beheerders toch minimaal 1x per maand te checken of er patches beschikbaar zijn op de website van de leverancier;
10. Van alle uitgevoerde en niet uitgevoerde patches wordt door de ICT beheerder een logboek bijgehouden.

Aldus vastgesteld door de directie van [organisatie] op [datum], [Naam. Functie] [Naam. Functie] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

