Beleid Patchmanagement 2024-2026

Informatiebeveiliging & Privacy

SWO

Auteurs : Wilbert Hepping, Jan Lemstra

Versie : 2.0
Status : Definitief
Datum : 10 november 2023

INHOUDSOPGAVE

1. Inleiding 3
2. Beleidsuitgangspunten patchmanagement 5
3. Kwetsbaarheden beoordelen 6
4. Gehanteerde definities 7

Documenthistorie

Versie	Datum	Auteur(s)	Status / omschrijving wijziging
0.1	10-06-2021	Wilbert Hepping	Concept patchmanagement beleid
0.2	17-09-2021	Wilbert Hepping, Jan Lemstra	Aanpassingen na bespreking
0.3	15-02-2022	Wilbert Hepping	Aangepast na review automatisering
1.0	11-07-2022	Wilbert Hepping	Definitieve versie
2.0def	10-11-2023	Jan Lemstra	Update mbt automatische updates BIOS

Review

Naam	Functie	Datum	Onderwerpen
Ruben Bruinenberg	Systeembeheerder security	11-11-2021	Geheel document
Marlies Caneel	IT Processpecialist	11-11-2021	Geheel document
Eveliene Salomons-Storm	ISO	04-10-2023	Gehele document
Daisy Djodikromo	CPO	04-10-2023	Gehele document
Jasmijn de Pruis	PO	04-10-2023	Gehele document

Classificatie

Classificatie	Niveau
	Openbaar
X	**Intern (bedrijfsvertrouwelijk)**
	Vertrouwelijk
	Geheim

1. Inleiding

Patchmanagement is het proces waarmee patches op gecontroleerde beheerste (risicobeperkende) 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. Ieder systeem of apparaat dat software bevat en aan een netwerk gekoppeld is, is in principe onderhevig aan patchmanagent. De meest voor de hand liggende voorbeelden hiervan zijn: besturingssoftware, applicaties, switches, firewalls, servers (ook virtueel), camerasystemen etc. Patchmanagement wordt meestal uitgevoerd door de ICT-afdeling binnen een organisatie. Patchmanagement kan worden uitgevoerd met speciale tooling die de gehele infrastructuur inventariseert en het patchproces ondersteunt (vulnerability scanning tools en patch tooling). Voor patches op applicaties is men voornamelijk afhankelijk van berichtgeving vanuit leveranciers.

Doelstelling Patchmanagement
Het doel van patchmanagement is tweeledig:

1. Het is gericht op het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur;
2. Op een zo efficiënt mogelijk wijze met zo min mogelijk verstoringen stabiele (veilige) systemen te creëren.

Patchmanagement is gericht op het verminderen van risico's als gevolg van benutting van gepubliceerde technische kwetsbaarheden. Leveranciers van software en hardware geven regelmatig informatie over gevonden kwetsbaarheden in hun systemen, met daarbij een aanwijzing hoe deze kwetsbaarheden te bestrijden. Door de steeds complexere samenhang van de infrastructuur is het niet altijd de beste oplossing om iedere patch door te voeren. Met een 'defense in depth' strategie[1] kan beter bepaald worden waar en wanneer patches doorgevoerd worden of alternatieve oplossingen ingezet kunnen worden.

Goed uitgevoerd patchmanagement is essentieel om de bovenstaande doelstellingen te kunnen realiseren.

Het patchmanagementbeleid van de Samenwerkingsorganisatie de Wolden Hoogeveen (hierna: SWO) geeft richting aan de wijze waarop de organisatie maatregelen wenst te treffen voor een adequate inrichting en uitvoering van patchmanagement.
De organisatie onderschrijft het belang van patchmanagement omdat het niet op een gestructureerde wijze bijhouden van patches voor gemeentelijke systemen ervoor kan zorgen dat kwetsbaarheden van die systemen toenemen. Dit beleid is van toepassing op iedereen die binnen de organisatie een rol heeft in het uitvoeren van patchmanagement.

De beleidsuitgangspunten die de SWO hanteert zijn ontleend aan de Baseline Informatiebeveiliging Overheid v1.04 (BIO) en de wereldwijd gehanteerde CIS Security baselines (Center of Internet Security).

[1] Zie Hardening beleid SWO v1.0def

Vanuit de BIO gaat dit over onderstaande controls en de daaraan gekoppelde maatregelen:

H12. Beveiliging bedrijfsvoering
12.6.1: Beheer van technische kwetsbaarheden

Mochten de uitgangspunten tegenstrijdig zijn tussen de verschillende richtlijnen dan prevaleren de BIO controls en maatregelen.

2. Beleidsuitgangspunten patchmanagement

1. Er is een proces ingericht voor het beheer van kwetsbaarheden en patching van (systeem) software binnen de organisatie. Patches worden uitgevoerd volgen het proces wijzigingenbeheer.
2. Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste patches en updates[2] zijn doorgevoerd.
3. Het doorvoeren van een patch of update door een leverancier vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn gemaakt met de leverancier.
4. Security patches (bijvoorbeeld voor een BIOS-update of Windows OS) worden op servers en laptops geautomatiseerd doorgevoerd. Overige patches en updates op laptops en desktops worden handmatig doorgevoerd.
   Op servers wordt de Long-Term Servicing Channel (LTSC[3]) gebruikt.
5. Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden beoordeeld (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch) door de beheerder. Indien het risico hoog[4] is dat een verstoring van de productieomgeving optreedt, wordt de installatie van de patch ter beoordeling voorgelegd aan de ISO en de systeemeigenaar.
6. De technische integriteit van patches wordt gecontroleerd door middel van een checksum (controlegetal) en hashingmechanisme van de leverancier, dat via een vertrouwd kanaal is verkregen.
7. Alle patches, met uitzondering van de patches voor een BIOS of Windows-update, dienen voor installatie te worden getest.
8. Behoudens de door de leverancier goedgekeurde updates worden er geen wijzigingen aangebracht in programmapakketten en infrastructurele programmatuur.
9. Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is (categorie Hoog/Hoog (HH)) worden zo spoedig mogelijk doorgevoerd, echter maximaal binnen 1 kalenderdag. Minder kritische beveiligings-updates/patches moeten worden ingepland conform tabel 3.1.
10. Indien een kwetsbaarheid is geconstateerd, maar er nog geen patch beschikbaar is, dient gehandeld te worden volgens het advies van de Informatiebeveiligingsdienst voor gemeenten of een CERT zoals het NCSC.
11. Als een systeem gepatched is wordt de systeem documentatie bijgewerkt naar de laatste stand van zaken, de configuratie management database wordt geüpdatet met de nieuwe versienummers van componenten.
12. Van alle uitgevoerde en niet uitgevoerde patches wordt door de beheerder een logboek bijgehouden.
13. Indien niet duidelijk is of een update/patch verplicht en/of automatisch doorgevoerd moet worden, overlegt Automatisering hierover met de ISO of CISO.

[2] Zie H5. Gehanteerde definities voor uitleg van de termen
[3] https://docs.microsoft.com/en-us/windows-server/get-started/servicing-channels-comparison
[4] Risico bepaalt op basis van kennis en ervaring van de FAB-er en/of de systeembeheerder

3. Kwetsbaarheden beoordelen

Om de prioriteit voor afhandeling van patches te bepalen maken we gebruik van de twee methodieken.

Kwetsbaarheden via de VCIB-mailinglijst van de IBD

Via de IBD ontvangen wij kwetsbaarheidsmeldingen via de VCIB-mailinglijst (Vertrouwelijke Contactpersoon Informatiebeveiliging). In deze meldingen wordt de CVE-score opgenomen en wordt ook de kans op misbruik en de schade bepaald. Onderstaande tabel wordt gebruikt om de ernst van de bedreigingen vast te stellen. Deze wordt ingevuld in de kolom 'Risico'. Wanneer een bedreiging bijvoorbeeld een kans 'midden' heeft en de potentiële schade 'hoog' is, dan wordt uit de tabel afgeleid dat de totale uitkomst op 'hoog' uitkomt voor die specifieke dreiging.

		Kans		
		H	**M**	**L**
Schade	**H**	HH	H	M
	M	H	M	L
	L	M	L	LL

Tabel 3.1: Kwetsbaarheid score IBD

Op basis van de 'totale uitkomst' kan de prioriteit voor de afhandeling van patches bepaald worden.

Algemene score van kwetsbaarheden

Common Vulnerabilities and Exposures, meestal afgekort als CVE, is een databank met informatie over kwetsbaarheden in computersystemen en netwerken. Veelal wordt in rapporten van penetratietests verwezen naar gegevens in deze databank. Een voorbeeld van een verwijzing hiernaar is: CVE-2012-1650. De CVE gebruikt vervolgens het Common Vulnerability Scoring System (CVSS) om het dreigingsniveau (impact) van een kwetsbaarheid te bepalen. De score wordt gebruikt om prioriteit te geven aan de beveiliging van kwetsbaarheden. De score van een kwetsbaarheid wordt bepaald op een schaal van 0-10.

In onderstaande tabel wordt de CVSS score vertaald naar de categorie-indeling die de SWO gebruikt.

Severity	Base Score Range	Categorie SWO	Afhandeling (kalenderdagen)
None	0.0	n.v.t.	n.v.t.
Low	0.1-1.9	LL	eerst volgende onderhoudsronde
Low	2.0-3.9	L	eerst volgende onderhoudsronde
Medium	4.0-6.9	M	14
High	7.0-8.9	H	7
Critical	9.0-10.0	HH	1

Tabel 3.2: Kwetsbaarheid score CVE en afhandeling SWO

Op basis van deze categorie SWO kan de prioriteit voor de afhandeling van patches bepaald worden.

4. Gehanteerde definities

Systemen
Met systemen wordt in dit verband bedoeld: Servers, actieve netwerkcomponenten zoals firewalls en switches, desktops, laptops, smartphones en tablets. Kortom, alles met een besturingssysteem.

Patch
Een patch is over het algemeen iets dat wordt gepusht om een kritieke fout, bug of beveiligingsprobleem (kwetsbaarheid) op te lossen. Een patch verandert niets aan functionaliteit van de applicatie.

Hotfix
Oorspronkelijk werd de term hotfix gebruikt om een soort patch te beschrijven die kon worden toegepast zonder een service of systeem te stoppen of opnieuw te starten.

Update
Een update omvat het aanbrengen van wijzigingen in een applicatie, waaronder bugfixes, beveiligingspatches, ondersteuning voor nieuwe hardware, extra functionaliteit en andere verbeteringen. Een update verandert alleen het secundaire versienummer (van x.1 naar x.2).

Upgrade
Een upgrade is een grote herziening van de software (op een hoger niveau brengen). Hierbij gaat het om een nieuwere versie van de applicatie (met nieuwe functionaliteiten. Het gaat dan om een nieuwe versie (van 1.x naar 2.x).