Security Patchbeleid

Kader Informatiebeveiliging

Versie 1.1 3 november 2022

Leeswijzer

Dit kaderdocument is een nadere uitwerking van het 'Amsterdam UMC Informatiebeveiligingsbeleid', welke is vastgesteld door de Raad van Bestuur.

De kaders zijn voor een belangrijk deel gebaseerd op de NEN7510-2. Daarnaast geldt bij het vaststellen van de uitvoeringsrichtlijnen de security architectuur principes, adviezen van de leverancier of gezaghebbende instituten over de inrichting (*best practices*) en het ontwerp en inrichting van de gehele ICT-infrastructuren van Amsterdam UMC.
Dat betekent ook meteen dat kaders en hun uitvoeringsrichtlijnen niet op zichzelf staan, maar als een geheel en als een set aan beveiligingsmaatregelen worden toegepast.

Met deze set aan beveiligingsmaatregelen, willen we verlies diefstal, manipulatie, of onbevoegde toegang tot gegevens voorkomen. Deze maatregelen kunnen vanuit verschillende perspectieven gemotiveerd worden, namelijk;

- De maatregel verkleint de kans van een aanval of misbruik
- De maatregel beperkt de schade geleden door misbruik

Documenthistorie en referenties

NEN7510-2 referenties

#	Paragraaf
12.6.1	Beheer van technische kwetsbaarheden

Overige Referenties

Auteur	Titel	Bron

Versiebeheer

Datum	Versie	Auteurs	Wijzigingen
25-01-2021	v0.1	P. Leeraert	Initiële opzet adhv NEN7510 Kaderdocument-patchbeleid VUmc (gemarkeerd met *PCH…*)
01-02-2021	v0.8	P. Leeraert	Review ASB
02-03-2021	v1.0	P. Leeraert	Definitieve versie vastgesteld door het MT van de Dienst ICT
11-04-2022	v1.1	P. Leeraert	Verduidelijkt dat patches effectief moeten zijn na installatie en dus mogelijk een reboot nodig hebben. Verder tekstuele aanpassingen.

Distributie

Datum	Versie	Aan	Functie of rol
25-01-2021	0.1	ASB overleg	Initiële opzet adhv NEN7510
01-02-2021	0.2	Ketenoverleg Dienst ICT	
	1.0	MT Dienst ICT	Goedkeuring
22-03-2022	1.05	ASB overleg	
24-11-2022	1.08	Ketenoverleg Dienst ICT	
	1.1	MT Dienst ICT	Goedkeuring

Wijzigingen

Artikel Nummer	Titel	Wijziging

Tags

Informatiebeveiliging; IT Security; NEN; NEN-7510; patches;

©2022 - Amsterdam UMC, Templateversie 1.4

Doel

Het doel van dit document is

Het geven van kaders en richtlijnen voor het tijdig patchen van software met security kwetsbaarheden. Hierdoor blijft gebruikte software beschermd tegen misbruik en uitbuiting van beveiligingslekken.

Doelgroepen zijn

- Management van het Amsterdam UMC, (eindverantwoordelijken en stellen van prioritering)
- Systeemeigenaren, (bijhouden van software binnen de gestelde tijdslijnen)
- Applicatiebeheerders (bijhouden van software binnen de gestelde tijdslijnen)
- Projectleiders (rekening houden met randvoorwaarden zodat tijdig patchen mogelijk wordt)

Scope

In scope
Dit security patchmanagementbeleid betreft alle systemen van het Amsterdam UMC, inclusief ICT systemen ten bate van medische systemen.

Begrippenlijst

De gebruikte kernbegrippen in dit beleidskader.

Begrip	Uitleg
Kwetsbaarheid	Eigenschap van een samenleving, organisatie of informatiesysteem (of een onderdeel daarvan) die een kwaadwillende partij de kans geeft om de legitieme toegang tot informatie of functionaliteit te verhinderen en te beïnvloeden dan wel ongeautoriseerd te benaderen.
Patch now	Security update die zo snel mogelijk geïnstalleerd moet worden doordat de impact van een geslaagde aanval groot kan zijn.
Security patch	Een patch (letterlijk: 'pleister') kan bestaan uit reparatiesoftware of kan wijzigingen bevatten, die direct in een programma worden doorgevoerd om het desbetreffende programma te repareren of te verbeteren.
Urgente patch	Zie patch now
Vulnerability	Engels - Zie kwetsbaarheid

Voor de volledige begrippenlijst, volg deze link.

Software security patches

Misbruik of uitbuiting van kwetsbaarheden in software voorkomen.

1. Op gevonden of potentiële technische kwetsbaarheden, wordt passende en tijdige actie ondernomen
2. Software kwetsbaarheden worden getoetst op risico's en geclassificeerd
3. Software op systemen met een verhoogd risico worden met voorrang gerepareerd
4. Elke software op elke laag kan kwetsbaarheden bevatten en moet beheerd worden
5. Amsterdam UMC volgt het changeproces bij de installatie van patches

Technische kwetsbaarheden
Een kwetsbaarheid (Engels: vulnerability), is een zwakke plek in de configuratie of in de software. Een programmeerfout in de software (of code) veroorzaakt vaak een kwetsbaarheid. Het gebruiken van verouderde protocollen is een andere reden.

Deze zwakke plekken kunnen door cybercriminelen misbruikt worden om systemen te laten crashen (*Denial of Service*) of toegang te krijgen tot het systeem. Als kwetsbaarheden in software bekend zijn, kan de leverancier updates uitbrengen om deze programmeerfouten te verhelpen, zo'n update heet een "security patch".

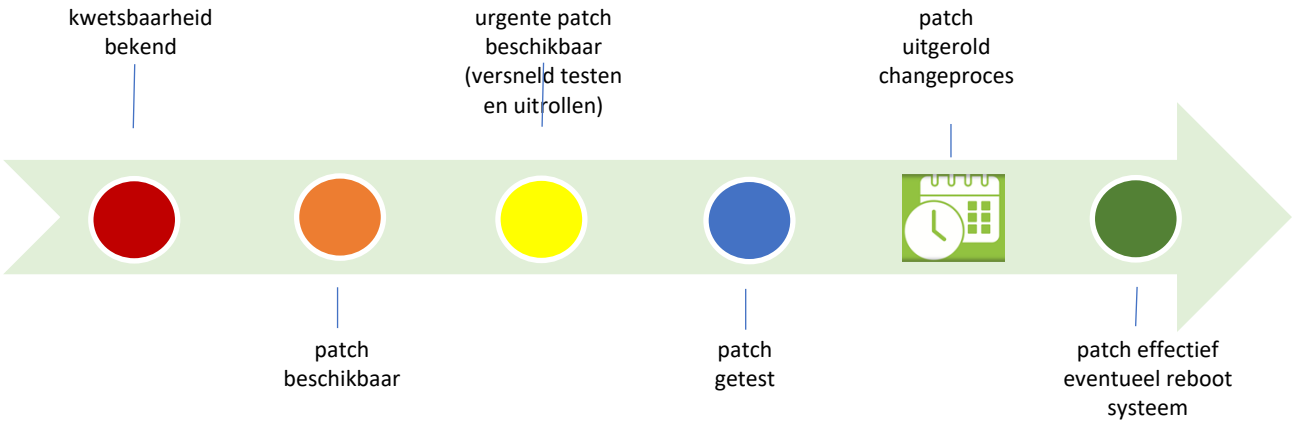
Security patches repareren dus kwetsbaarheden in software zodat de vertrouwelijkheid en integriteit van software wordt hersteld of in tact blijft.

Een security patch kan drie functies hebben:

- het verhelpen van (functionaliteit) fouten in de programmatuur
- het verhelpen van (security) kwetsbaarheden in de programmatuur
- het toevoegen (soms ook verwijderen of veranderen) van functionaliteit

Urgente patches (patch now)
Urgent geclassificeerde kwetsbaarheden (ook wel 'patch now' genoemd), worden met voorrang en mogelijk buiten de reguliere patchcycli om behandeld. Deze kwetsbaarheden vormen een hoog risico voor de beschikbaarheid en veiligheid van Amsterdam UMC. Denk bijvoorbeeld een kwetsbaarheid wat er toe leidt dat een aanvaller vanaf internet administrator rechten kan verkrijgen op een kritisch systeem.

Hieronder staat een grafische weergave van de security patch cyclus.



Dit patchmanagementbeleid behandelt een aantal uitgangspunten voor patchmanagement. Het implementeren van patchmanagement en de te hanteren procedures zijn een verantwoordelijkheid

van de betreffende teams en van changemanagement. In de richtlijnen ligt de nadruk op de prioriteitstelling en planning van patches.

In dit document zijn de volgende items beschreven

1. Kaders
   1.01 Alle toegepaste software wordt gerepareerd op kwetsbaarheden
   1.02 De “Defense in Depth”—strategie is uitgangspunt voor patchen
   1.03 Vaststellen prioriteit voor software kwetsbaarheden op basis van risicoafwegingen
   1.04 Patchbeleid volgt het Amsterdam UMC changeproces
   1.05 Bij een gevonden technische kwetsbaarheid wordt passend en tijdig actie genomen
2. Uitvoeringsrichtlijnen
   2.01 Er is een actuele en volledige inventaris in de CMDB
   2.02 De prioriteit van kwetsbaarheden wordt bepaald volgens een vastgestelde methodiek
   2.03 Gecentraliseerd updaten van systemen met security patches volgt een vast tijdspad
   2.04 Voor urgente kwetsbaarheden wordt een versnelde procedure ‘patch-now’ gevolgd
   2.05 Indien nodig wordt een reboot uitgevoerd om de patch effectief te maken
   2.06 De installatie van patches is geautomatiseerd waar mogelijk
   2.07 Updates van security patches zijn actief binnen de gestelde urgentietijden
   2.08 Iedere patch wordt standaard getest
   2.09 Patches worden gefaseerd over de ICT-omgevingen uitgerold
   2.10 Beheer volgt proactief informatie over uitgebrachte softwareversies en aanpassingen
3. Governance en excepties op dit kader
   3.01 Uitzonderingen op dit kader
   3.02 Een bestaande uitzondering wordt herzien bij wijzigingen op het systeem

Bijlage A – Security Patch Proces, Rollen en Verantwoordelijkheden

Bijlage B – NCSC Inschalingsmatrix

1. Kaders

1.01 Alle toegepaste software wordt gerepareerd op kwetsbaarheden

Beschrijving	Patchmanagement is van toepassing op alle lagen met software: op firmware van apparatuur, op besturingssystemen en applicatieonderdelen van server platforms en distributieplatforms (CDW, VIEW of OneView) en op applicatieonderdelen van bedrijfssystemen.	
Achtergrond	Alle software kan fouten bevatten of gebruik maken van inmiddels achterhaalde technieken waar beveiligingslekken in zitten en moeten dus gerepareerd worden om veilig te blijven.	
Implicaties	Er zijn verschillende typen software die op systemen actief kunnen zijn.	• Operating systems • Middleware, zoals databases • Applicaties, zoals office • BIOS en dergelijke • Firmware netwerk componenten of servers • Out-of-Band management controllers (bv. HP Insight manager) • Virtualisatie software • Appliances • IoT

1.02 De “Defense in Depth”—strategie is uitgangspunt voor patchen

Kern	Meerlaagse verdediging of *defense in depth* is een beveiligingsstrategie waarbij meerdere verdedigingslagen in en rond te beveiligen systemen en data zijn aangebracht. Het falen van één verdedigingslaag wordt daardoor opgevangen door de volgende laag. Deze strategie is uitgangspunt voor netwerkzonering bij Amsterdam UMC.	
Achtergrond	Beperkt de schade bij succesvol binnendringen op enige plaats in de infrastructuur en geeft beheer de mogelijkheid om patches volgens een tijdsplanning uit te rollen	
Implicaties		• Zie 2.01 en verder

1.03 Vaststellen prioriteit voor software kwetsbaarheden op basis van risicoafwegingen

Kern	Ken alle patches een prioriteitstelling toe op basis van een risicoafweging. Hanteer de klassen: Urgent, Hoog, Midden, Laag.	
Achtergrond	De technische maatregel voor patchen is herleidbaar naar geïdentificeerde risico’s van een fout of kwetsbaarheid in de software en de risico’s die vormt voor Amsterdam UMC.	
Implicaties	Stel methode vast voor het bepalen van de urgentie voor het verhelpen van security kwetsbaarheden	• Pas NCSC, Inschalingsmatrix toe • Zie 2.02

1.04 Patchbeleid volgt het Amsterdam UMC changeproces

Kern	Het patchbeleid sluit aan bij het bestaande changeproces van de Dienst ICT. Hierbij valt te denken aan afspraken omtrent impactanalyse, CAB, communicatie naar gebruikers, back-up en roll-back eisen, OTAP, service windows, enzovoorts.	
Achtergrond	Changeproces borgt een veilige en robuuste methode voor test en implementatie waardoor de risico’s op uitval beperkt worden, of bij uitval via een back-out procedure herstelt kan worden	
Implicaties	Volg het changeproces van het Amsterdam UMC	• Testen • Back-up en roll-back • Gefaseerd uitrollen met pliotgroepen • Reboot van het systeem

1.05 Bij een gevonden technische kwetsbaarheid wordt passend en tijdig actie genomen

Kern	Als reactie op de identificatie van potentiële technische kwetsbaarheden behoort passende en tijdige actie te worden ondernomen zodat de kwetsbaarheid kan worden gerepareerd	
Achtergrond	Om de kans op misbruik zo klein mogelijk te houden moet er snel gehandeld worden.	
Implicaties	Het Amsterdam UMC stelt de rollen en verantwoordelijkheden in samenhang met het beheer van technische kwetsbaarheden vast; 1. met inbegrip van het monitoren van de kwetsbaarheden, 2. een risicobeoordeling van de kwetsbaarheden, 3. het installeren van herstelprogramma's (patching), 4. het traceren van bedrijfsmiddelen en de vereiste coördinatieverantwoordelijkheden	1. Niet in dit kader 2. Zie 2.02 3. Zie 2.03 en verder 4. Zie bijlage A
	Een tijdpad behoort te worden gedefinieerd waarbinnen moet worden gereageerd op aankondigingen van potentieel relevante technische kwetsbaarheden;	• Zie 2.04
Noot	*NEN7510-2; 12.6.1*	

2. Uitvoeringsrichtlijnen

2.01 Er is een actuele en volledige inventaris in de CMDB

Kern	Configuratie Management Database heeft een inventarisatie van alle assets	
Achtergrond	Een actuele en volledige inventaris van bedrijfsmiddelen is een voorwaarde voor een doeltreffend beheer van technische kwetsbaarheden. Tot de specifieke informatie die nodig is om beheer van technische kwetsbaarheden te ondersteunen behoren informatie over de softwareleverancier, versienummers, huidige toepassingsstatus (bijv. welke software is geïnstalleerd op welke systemen) en de persoon of personen in de organisatie verantwoordelijk voor de software	
Implicaties	Assets zijn geregistreerd in de CMDB van het Amsterdam UMC	• CMDB registratie
	Afhankelijkheden tussen verschillende assets die een applicatie(keten) vormen, zijn vastgelegd	• Afhankelijkheden zijn inzichtelijk in de CMDB
Noot	*NEN7510-2; 12.6.1*	

2.02 De prioriteit van kwetsbaarheden wordt bepaald volgens een vastgestelde methodiek

Kern	Ken alle patches een prioriteitstelling toe op basis van een risicoafweging. Hanteer de klassen: Urgent, Hoog, Midden, Laag.	
Achtergrond	De technische maatregel om te patchen is herleidbaar naar geïdentificeerde risico's van een fout of kwetsbaarheid in de software. Aansluiting op standaarden en *best practices* van leveranciers.	
Implicaties	De uitrol van patches hangt af van de classificatie van de urgentie Start initieel met de door de leverancier opgegeven urgentie. Echter deze kan overruled worden door CERT-teams of overheidsinstanties zoals Nationaal Cyber Security Centrum (NCSC)	Volgorde voor uitgangspunt urgentie 1. Zorg specifiek CERT team 2. NCSC[1] 3. Beoordeling leverancier
	Neem bij de weging mee waarbij een Hoge kwetsbaarheid een impact op zeer vertrouwelijk systemen heeft, versneld worden uitgerold	Versnelde uitrol bij • Bij urgentie 'Hoog' • Bij impact[2] op zeer vertrouwelijke (zorg) systemen
Noot	[1] *Zie Bijlage C - Inschalingsmatrix* [2] *Potentieel kan dit ook een browser zijn op VDI wanneer dit toegang verschaft tot deze systemen*	

2.03 Gecentraliseerd updaten van systemen met security patches volgt een vast tijdspad

Kern	Hanteer een geplande cyclus voor patches, die gestandaardiseerd worden getest en uitgerold.	
Achtergrond	Creëer efficiëntie in het uitrol proces doordat implementatie voorspelbaar en volgens een standaard proces verlopen. Dit voorkomt ad-hoc maatregelen wat de kans op fouten vergroot.	
Implicaties	Maak werkzaamheden ten behoeve van software updates en testen een regulier onderdeel van de planning.	• Plan patch werkzaamheden in • Standaardchange voor regulier patchen

2.04 Voor urgente kwetsbaarheden wordt een versnelde procedure ‘patch-now’ gevolgd

Kern	Urgent geclassificeerde kwetsbaarheden (ook wel ‘patch now’ genoemd), worden met voorrang en mogelijk buiten de reguliere patchcycli om behandeld.	
Achtergrond	Om de kans op misbruik zo klein mogelijk te houden moet er snel gehandeld worden. Dit kan om een verkorte cycli vragen om het risico weg te nemen.	
Implicaties	De beheerder of het Security CERT teamlid nemen het initiatief om een kwetsbaarheid als urgent op te pakken. In samenspraak wordt bekeken wat het risico is en de te nemen acties.	Bepalen urgente risico • Beheerder en • Security CERT-teamlid
	De verantwoordelijkheden bij urgente kwetsbaarheden zijn belegd bij de beheerder en het Security CERT-team	• Beheerder zorgt voor de implementatie • CERT-team bewaakt status, voortgang
	Voer als Urgent geclassificeerde patches zo snel mogelijk uit zoals bepaald onder 2.04 Beperk het testen van de patches tot de strikt noodzakelijke tests.	Urgente patch (*patch now*) • Urgent voer spoedchange uit • Alleen strikt noodzakelijke testen

2.05 Indien nodig wordt een reboot uitgevoerd om de patch effectief te maken

Kern	De kwetsbaarheid in de software verhelpen door middel van een security patch en optioneel een systeem reboot.	
Achtergrond	Vaak hebben patches na installatie een reboot van het systeem nodig. Hierdoor is de kwetsbaarheid effectief gedicht en de patch operationeel.	
Implicaties	Na installatie van een patch wordt een reboot gepland	• Herstart vindt uiterlijk plaats binnen 1 week[1] na installatie van de patch
	Bij sommige systemen kan een reboot grote impact hebben op de beschikbaarheid van systemen of applicaties.	• Eigenaar vraagt exceptie aan bij IT-security van de Dienst-ICT • Uitstel van een herstart is maximaal 3 maanden
Noot	[1]*Voor urgente patch now wordt een reboot zo snel mogelijk doorgevoerd. Zie ook 2.04.*	

2.06 De installatie van patches is geautomatiseerd waar mogelijk

Kern	Het patchen gebeurt centraal en is geautomatiseerd waar dit mogelijk is.	
Achtergrond	Creëer efficiëntie in het uitrol proces zodat de implementatie voorspelbaar en volgens een standaard proces verloopt. Dit voorkomt ad-hoc maatregelen wat weer de kansen op fouten vergroot.	
Implicaties	Automatiseer waar mogelijk	Automatiseer de uitrol[1] • Besturingssystemen • Kantoorapplicaties
Noot	[1]*Een voorbeeld is Windows OS updates met SCCM*	

2.07 Updates van security patches zijn actief binnen de gestelde urgentietijden

Kern	Volg een tijdsplan waarbinnen de updates uitgevoerd moeten zijn om de kans op misbruik door cybercriminelen te verkleinen.	
Achtergrond	Handhaven van snelheid bij het oplossen van kwetsbaarheden is van belang. Software waarvan patches beschikbaar komen, hebben bekende kwetsbaarheden die misbruikt kunnen worden door cybercriminelen binnen een zeer kort tijdsbestek. Systemen die direct aan het Internet gekoppeld zijn, zoals DMZ-systemen, zijn hierbij een makkelijk doelwit.	
Implicaties	Voer als Urgent geclassificeerde patches zo snel mogelijk uit en niet later dan hieronder in de tabel weergegeven.	• Zie 2.04
	Systemen in een semi-vertrouwde zone, zoals DMZ, zijn het meest blootgesteld aan het Internet en lopen een hoog risico op misbruik van beveiligingslekken. Hierdoor moet de kans zo beperkt mogelijk worden gehouden door de patch zo snel mogelijk te installeren.	Systemen in een semi-vertrouwde zone • DMZ systemen hebben een versnelde implementatie
	Voor afwijkingen op deze tijdslijnen wordt het exceptieproces gevolgd en de risico's gemitigeerd.	• Mitigeer risico's, zie 2.05 en 2.11 • Voor uitzonderingen zie 3.01

Urgentietabel – Tijdslijnen waarbinnen security patches geïnstalleerd moeten worden

	Urgent	Hoog	Midden	Laag	Opmerking
	< 72 uur	30 dagen[1]	60 dagen	90 dagen	
Versnelde uitrol		14 dagen			Zie 2.04
Centrale uitrol		30 dagen	30 dagen	30 dagen	Zie 2.03
DMZ	< 24 uur	< 1 dag	7 dagen	30 dagen	

[1] *Kalenderdagen*

2.08 Iedere patch wordt standaard getest

Kern	Test alle patches voorafgaand aan de uitrol in een representatieve testomgeving.	
Achtergrond	Security patches behoren te worden getest en geëvalueerd voordat ze worden geïnstalleerd om te waarborgen dat ze doeltreffend zijn en niet resulteren in bijverschijnselen die niet kunnen worden getolereerd.	
Implicaties	Alle updates worden getest, beoordeeld en geïnstalleerd middels changeproces	• Volg het changeproces • Denk aan testen en back-out scenario zodat terug gegaan kan worden naar de oorspronkelijke situatie
	Zet een testomgeving op voor alle systemen waarvoor deze nog ontbreken. Automatiseer testprocessen en plan consequent tijd vrij om testen uit te voeren.	• Er is een adequate testomgeving • Of beperk test en rol gefaseerd uit, zie 2.04 en 2.09
Noot	*Zie ook 2.04 Voor urgente kwetsbaarheden wordt een versnelde procedure gevolgd* *En 2.09 Gefaseerde patch uitrol om de impact van eventuele bugs te spreiden*	

2.09 Patches worden gefaseerd over de ICT-omgevingen uitgerold

Kern	Rol een patch gefaseerd uit op de productieomgeving van een platform om de impact van een eventuele bug in de patch te spreiden.	
Achtergrond	Onvoorziene problemen met een patch blijven beperkt tot een kleine gebruikersgroep en er kan directe kennis worden opgebouwd hoe de patch zich gedraagt in onze omgeving.	
Implicaties	Definieer voor een distributieplatform de groep key-users die deel uit maakt van de eerste fase van de uitrol.	• Bepaal groep key-users • Rol deze groep als eerste uit
	Definieer voor een serverplatform de groep systemen die deel uitmaakt van de eerste fase van de uitrol.	• Bepaal eerste fase systemen uitrol
	Na evaluatie van de impact verder uitrollen of aanpassen	• Evalueer impact update

2.10 Beheer volgt proactief informatie over uitgebrachte softwareversies en aanpassingen

Kern	Richt voor ieder systeem een methode in om over uitgebrachte patches geïnformeerd te worden	
Achtergrond	Proactieve informatie over de beschikbaarheid van patches geeft tijd om bewust te zijn van risico's en afhankelijkheden met andere softwareproducten. (zoals operating system en bovenliggende middleware). Daar anticipatie wordt beheer efficiënter.	
Implicaties	Beheerder volgt nieuwsbrieven van leverancier (of derden) over de door hun beheerde producten	Abonneer op distributielijsten • leverancier • technische communities
	De beheerder (van de dag) controleert dagelijks of er nieuwe security patches van toepassing zijn, op de beheerde systemen.	Dagelijkse check door de beheerder (van de dag)
Noot	*Zie verder ook Bijlage A - Security Patch Proces, Rollen en Verantwoordelijkheden*	

3. Governance en excepties op dit kader

3.01 Uitzonderingen op dit kader

Kern	Geeft aan hoe een uitzondering of exceptie op dit kader aangevraagd moet worden en aan welke voorwaarden er voldaan moet worden.	
Achtergrond	Uitzonderingen worden gemanaged volgens de NEN7510 'Pas toe – Leg uit' principe waarbij het risico's van de voorgestelde alternatieve maatregelen worden getoetst of het restrisico acceptabel is.	
Implicaties	Uitzonderingen op dit beleid zijn alleen mogelijk wanneer is voldaan aan de onderstaande voorwaarden:	
	Vastgesteld is door de Dienst ICT beheer dat er geen alternatieven mogelijk zijn om de gewenste functionaliteit te bieden op een manier die binnen dit beleid valt	• Vaststelling Dienst ICT beheer
	En er is een Risico Analyse (RA) uitgevoerd op de uitzonderingssituatie.	• RA opgesteld
	De Directeur Dienst ICT van mening is dat de dienst of functionaliteit van dusdanig belang voor het Amsterdam UMC is dat dit in aanmerking kan komen voor een uitzondering omdat het bedrijfsbelang opweegt tegen het extra beveiligingsrisico (gespecificeerd in de RA) dat hierdoor ontstaat.	• Uitzondering bekrachtigt door Directeur Dienst ICT
	Uitzonderingen op dit beleid wordt schriftelijk aangevraagd bij en beoordeeld door de IT Security Officer via ITSM applicatie.	• Via ServiceNow • Expliciete toestemming IT Security Officer
	Dit schriftelijk verzoek motiveert het volgende:	• Reden van de uitzondering en waarom er niet aan de eis(en) van dit kader voldaan kan worden • Inschatting van het overblijvende restrisico door de technisch specialist • Toelichting van alternatieve maatregelen

3.02 Een bestaande uitzondering wordt herzien bij wijzigingen op het systeem

Kern	Wijzigingen (changes) op het systeem of op de infrastructuur, kunnen invloed hebben op de beperkte (exceptie) beveiliging.	
Achtergrond	Systemen met excepties zijn kwetsbaarder voor aanvallen door cybercriminelen. Omdat het restrisico op de beveiliging van eerder afgegeven excepties door systeemwijzigingen kunnen veranderen, moet het beveiligingsrisico heroverwogen worden of dit nog steeds binnen een aanvaardbaar niveau is.	
Implicaties	Als er veranderingen plaats vinden aan de opzet van het systeem in kwestie nadat de exceptie is toegestaan conform bovenstaande procedure, dan zal door de ITSO bepaald worden of de Risico Analyse (RA) opnieuw uitgevoerd moeten worden	• Bij wijzigingen wordt er naar gestreefd de exceptie weg te nemen en zo het beveiligingsrisico te minimaliseren • Eigenaar informeert de IT Security Officer over de (aanstaande) wijziging • IT Security Officer beoordeelt of de Risico Analyse (RA) opnieuw moet worden uitgevoerd
	Er wordt opnieuw een Risico Analyse (RA) uitgevoerd op de uitzonderingssituatie.	• Zie 3.01

Bijlage A – Security Patch Proces, Rollen en Verantwoordelijkheden

Inleiding

Het tijdig uitvoeren van software updates (patches) is van belang voor de continuïteit en veiligheid van ICT diensten. Omdat hier regelmatig meerdere partijen bij betrokken zijn is in dit document uitgewerkt welke rollen en daarmee ook verantwoordelijkheden er in het proces zijn.

Eigenaarschap

Binnen Amsterdam UMC is er een beheerteam hoofdaannemer van een software-component. Onder een software-component wordt het volgende verstaan:

Eén of meerdere software-onderdelen die een logisch geheel vormen en waarvan de verantwoordelijkheid voor het functioneren, updaten en lifecycle management bij één partij belegd zijn. Dit kan een compleet OS zijn (bv. Windows 10) maar, een enkel softwarepakket (bv. Adobe Acrobat) of zelfs een enkel programma (bv. putty.exe).

Binnen dienst ICT is het hoofdaannemerschap belegd bij een beheerteam en meestal is dit daarbinnen dan ondergebracht bij een specifiek aantal beheerders met kennis van het product.

CMDB

De hoofdaannemer van een software-component wordt vastgelegd in de CMDB. Zo is voor iedereen eenvoudig te zien wie verantwoordelijk is voor functioneren, updates en lifecycle management.

Taken

Zoals in de definitie van software-component te lezen valt is er altijd sprake van meerdere taken. Dit document gaat alleen in op het tijdig installeren van security patches.

Verantwoordelijkheden

Het beheerteam dat hoofdaannemer is, is ook verantwoordelijk voor het tijdig uitvoeren van security updates. De onderbouwing om dit hier te beleggen zijn:

- Kennis en kunde aanwezig over het software-component en alles daaromheen
- Voor zover er sprake is van een supportpartner (bv. reseller) zijn de contacten en contracten hier bekend
- Werkzaamheden zijn onderdeel van het standaard takenpakket
- Werkzaamheden zijn bij meer dan één persoon belegd waardoor er garantie is voor het tijdig uitvoeren van de security updates

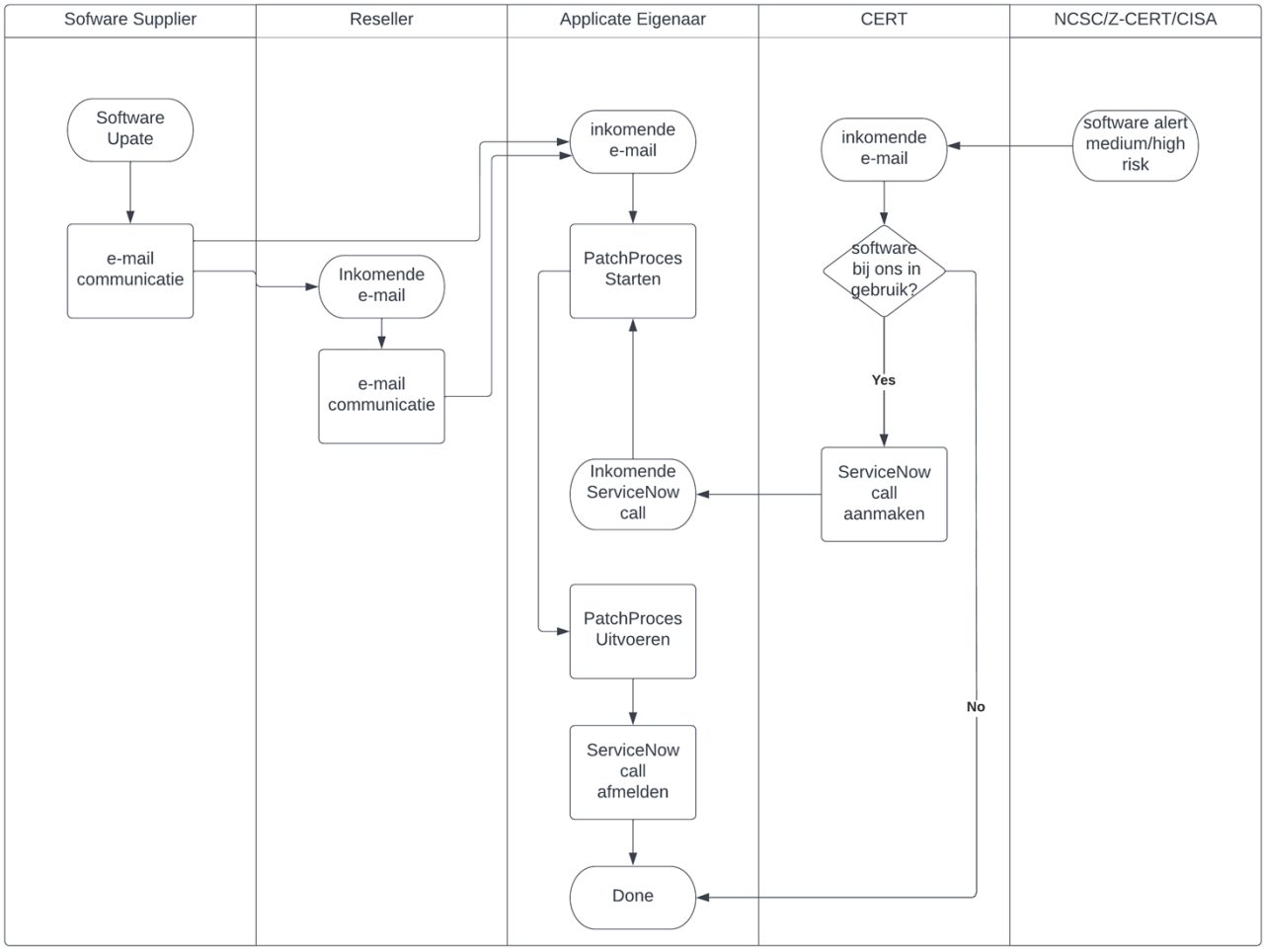
Het kader “Informatiebeveiliging – Patch beleid” geeft de kaders voor het proces rondom de security updates.

Rol CERT

Het CERT krijgt informatie van de eigen kanalen over medium en hoog risico kwetsbaarheden van software-componenten. Deze informatie wordt gedeeld met het cluster via ServiceNow. De security informatie is aanvullend op het patch proces en bedoeld als extra zekerheid zodat deze kwetsbaarheden de urgentie krijgen die bij het risico hoort.

Uitwerking proces in swimlanes

Hieronder is het proces grafisch uitgewerkt.



Bijlage B – NCSC Inschalingsmatrix

Noot:
Zie voor de laatste versie het NCSC.nl op trefwoord ‘Inschalingsmatrix’.

Inschalingsmatrix
De beveiligingsadviezen van NCSC-NL bevatten een inschaling van de beschreven kwetsbaarheid. Per advies wordt een Kans op uitbuiting en Schade bij uitbuiting gedefinieerd. De mogelijke waarden per onderdeel zijn Low, Medium of High. Voor zowel de Kans als Schade inschalingen wordt een set vragen beantwoord, die leiden tot een waarde. Wanneer er specifieke omstandigheden zijn, kan worden afgeweken van de matrix en kan de waarde voor Kans en/of Schade worden veranderd. Beveiligingsadviezen voor kwetsbaarheden met de waarde Low voor zowel de Kans als de Schade, worden niet uitgestuurd.

Kans
De kans wordt bepaald door onderstaande vragen te beantwoorden en de waarde toe te kennen die achter elke optie staat.

Vraag	Optie 1		Optie 2		Optie 3	
Is de kwetsbaarheid aanwezig in de standaard configuratie/installatie?	Nee	1	Onduidelijk/Ja	3		
Is er Exploitcode beschikbaar?	Geen	1	Proof of Concept (PoC)	4	Exploit	6
Zijn er technische details beschikbaar	Geen	1	Enigszins	2	Volledig	3
Vereiste toegang	Fysiek	1	LAN/directe omgeving	4	internet	6
Vereiste credentials?	Admin	1	User	2	Geen	4
Hoe complex is het technisch gezien om de kwetsbaarheid uit te buiten?	Complex	1	Gemiddeld	2	Eenvoudig	3
Is er gebruikersinteractie nodig?	Complex	1	Eenvoudig	3	Geen	4
Wordt de kwetsbaarheid in het wild uitgebuit?	Nee	1	Beperkt	2	Grootschalig	3
Wordt de kwetsbaarheid, naar verwachting, op korte termijn misbruikt of verschijnt er een exploit?	Nee	1	Ja	3		
Beschikbaarheid oplossing?	Ouder dan 2 maanden	1	Tot 2 maand oud	2	Geen	3

Verklaring van de kans vragen

Is de kwetsbaarheid aanwezig in de standaard configuratie/installatie?

Wanneer de kwetsbaarheid zich in een specifieke configuratie-instelling of installatie bevindt, is de kans dat een systeem kwetsbaar is minder groot dan wanneer de kwetsbaarheid standaard aanwezig is.

Is er Exploitcode beschikbaar?
Hoe minder een aanvaller hoeft te doen om systemen te kunnen compromitteren, hoe hoger de kans dat dit ook gebeurt.

Zijn er technische details beschikbaar
Hoe meer technische details beschikbaar zijn, hoe (relatief) eenvoudiger het wordt om een exploit te schrijven wat de kans dat deze verschijnt vergroot. Mogelijke waarden zijn:

- Geen: er zijn geen details over de kwetsbaarheid gepubliceerd.
- Enigszins: er is een aantal details gepubliceerd. Het is bekend welke component of functie een probleem bevat en onder welke omstandigheden de kwetsbaarheid aanwezig is.
- Volledig: het exacte commando binnen de kwetsbare functie bekend is gemaakt, of kwetsbaarheid is aangetoond in de broncode.

Vereiste toegang
De kans dat een kwetsbaar systeem wordt gecompromitteerd wanneer het toegankelijk is voor een beperkte groep mensen is kleiner dan wanneer het rechtstreeks vanaf het internet benaderbaar is. Mogelijke waarden zijn:

- Fysiek/Directe omgeving: de aanvaller moet fysiek in de buurt van het systeem zijn of met een gebruikersaccount kunnen inloggen.
- LAN: De aanvaller moet via het LAN netwerkverkeer kunnen sturen naar het kwetsbare systeem.
- Internet: Diensten zoals een webserver of een mailserver zullen worden aangemerkt als benaderbaar via het internet.

Vereiste credentials
Wat voor gebruikersrechten heeft de aanvaller nodig om de kwetsbaarheid te kunnen uitbuiten?

Hoe complex is het technisch gezien om de kwetsbaarheid uit te buiten
Een kwetsbaarheid die eenvoudig uit te buiten is zal mogelijk eerder tot een werkende exploit leiden dan een technisch zeer complex probleem.

Is er gebruikersinteractie nodig?
Moet de gebruiker worden overgehaald om een document te openen of een website te bezoeken?

Wordt de kwetsbaarheid in het wild uitgebuit?
Wordt actief misbruikt op het internet? Is er sprake van grootschalig misbruik? Of een gerichte aanval?

Wordt de kwetsbaarheid binnenkort misbruikt of verschijnt er een exploit?
Deze vraag kent een gevoelswaarde toe aan de inschaling.

Beschikbaarheid oplossing
Wanneer er geen oplossing bekend is, is het zeer interessant voor aanvallers om de kwetsbaarheid uit te buiten.

Door bovenstaande waarden toe te kennen aan de antwoorden ontstaat een kanswaarde per kwetsbaarheid. Op basis van discussiesessies en meerdere proefwegingen is bepaald dat de onderstaande verdeling wordt gehanteerd om een betrouwbare inschaling te doen.

- Low: 10 –18
- Medium: 19 –27
- High: 28 -38

Schade

De schade wordt bepaald door een van de onderstaande schadeomschrijvingen te kiezen.
Wanneer meer dan één type schade kan worden veroorzaakt, wordt de zwaarste inschaling gebruikt.

Schadeomschrijving

Denial of Service (DoS)
De kwetsbaarheid kan ertoe leiden dat een dienst niet meer bereikbaar/bruikbaar is

Uitvoeren van willekeurige code
Na uitbuiting kan code ofsysteemcommando's worden uitgevoerd.

Rechten op afstand (remote (root-) shell)
Na uitbuiten van de kwetsbaarheid krijgt de aanvaller toegang tot een interactieve(root-)shell op afstand.

Verwerven lokale admin/root-rechten (privilege escalation)
Een reguliere gebruiker kan zich verhoogde rechten toe-eigenen door het uitbuiten van de kwetsbaarheid op het lokale systeem.

Lekkage informatie
Door een kwetsbaarheid uit te buiten kan systeeminformatie of data buit worden gemaakt.

Vraag	Optie 1		Optie 2		Optie 3	
Denial of Service	Nee	Low	Ja, Client	Low	Ja, Infrastructuur dienst	High
Uitvoeren van willekeurige code	Nee	Low	Ja, Gebruikers rechten	Medium	Ja, Root / Administrator rechten	High
Rechten op afstand (remote (root-) shell)	Nee	Low	Ja, remote shell	Medium	Ja, remote root-shell	High
Verwerven lokale admin/root-rechten (privilege escallation)	Nee	Low	Ja	Medium		
Lekkage informatie	Nee	Low	Ja, systeem informatie	Medium	Ja, data	High

Inschalingsmatrix.pdf