Amsterdam UMC
Universitair Medische Centra

Locatie AMC

Titel	**Informatiebeveiliging - Patchbeleid - kader Amsterdam UMC**
Versie	2
Publicatiedatum	16-03-2021
Controledatum	15-03-2022
Status	Gepubliceerd

Auteur(s)

Leeraert, P.P.J. (Paul)

Autorisator(en)

Lauteslager, A.R. (Arnaud)

DocumentID

Kader Informatiebeveiliging – Patchbeleid

Versie 1.0 2 maart 2021

Leeswijzer

Dit kaderdocument is een nadere uitwerking van het 'Amsterdam UMC Informatie Beveiligingsbeleid' in vastgestelde beheersmaatregelen. In artikelen worden de maatregelen uitgewerkt die gelden voor dit domein.

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

Om verlies, diefstal, manipulatie, of onbevoegde toegang tot gegevens te voorkomen worden maatregelen ingezet. Maatregelen kunnen vanuit verschillende perspectieven gemotiveerd worden.

- De maatregel verkleint de kans van een aanval of misbruik
- De maatregel beperkt de schade geleden door misbruik.
- Maatregelen die ingezet worden om de schade te herstellen

Doel

Het doel van dit document is:

Het geven van kaders en richtlijnen voor toepassing van het patchen van software tegen security kwetsbaarheden als instrument voor het managen van risico's in de informatievoorziening.

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)

Doelstelling patchbeleid

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. Het Amsterdam UMC changeproces wordt gevolgd bij installatie van patches

Technische kwetsbaarheden (of *vulnerabilities*)
Een kwetsbaarheid 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".

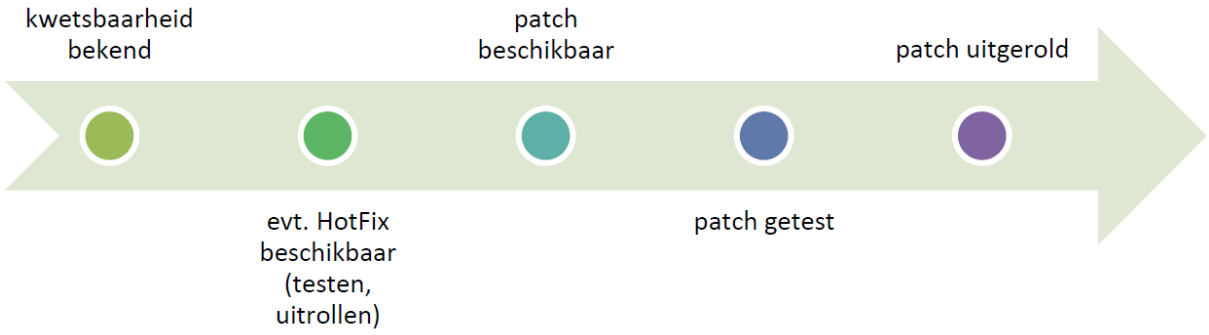
Security patches repareren dus kwetsbaarheden in software zodat de vertrouwelijkheid en integriteit van software wordt hersteld of in tact blijft.

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

Naast security patches wordt er ook wel gesproken over hotfix en service-packs. Een hotfix is een snelle nood-patch die het risico op misbruik van een ontdekte kwetsbaarheden kan reduceren. Een hotfix brengt wel risico's voor beschikbaarheid met zich mee omdat het over het algemeen niet via het intensieve Q&A (Quality and Assurance) traject is gevalideerd.

Hieronder staat een grafische weergave van de security patch life-cycle.



Vaak valt het bekend worden van de kwetsbaarheid gelijk met het beschikbaar komen van de patch, maar het kan goed zijn dat bij andere partijen (hackers, bepaalde overheidsdiensten, …) de kwetsbaarheid al langer bekend waren en mogelijk ook actief misbruikt zijn. Dit is een van de redenen om altijd het principe van "*Defense in Depth*" (meerlaagse beveiliging) te hanteren en zo het risico van de kwetsbaarheden in één laag te reduceren.

Het patchbeleid 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

Scope

Dit security patchmanagementbeleid betreft alle systemen van het Amsterdam UMC, inclusief ICT systemen ten bate van medische systemen. Echter medische apparatuur zelf is niet in scope.

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 Classificatie van software kwetsbaarheden
   - 1.04 Patchbeleid volgt het Amsterdam UMC changeproces
   - 1.05 Gevonden potentiële technische kwetsbaarheden behoort een passende en tijdige actie te worden ondernomen
2. Uitvoeringsrichtlijnen
   - 2.01 Actuele en volledige inventaris in CMDB
   - 2.02 Classificatie van software kwetsbaarheden volgens vastgestelde methodiek
   - 2.03 Gecentraliseerd updaten van systemen met security patches volgt een vast tijdspad
   - 2.04 Tijdsplan voor het updaten van systemen met security patches
   - 2.05 Voor urgente kwetsbaarheden wordt een versnelde procedure gevolgd
   - 2.06 Iedere patch worden standaard getest
   - 2.07 Gefaseerde uitrol over een platform
   - 2.08 Volg aanpassingen en nieuws over uitgebrachte softwareversies
   - 2.09 Mitigeer risico’s als updaten van de software niet mogelijk, of beschikbaar is
3. Governance en excepties op dit kader
   - 3.01 Excepties op dit kader
   - 3.02 Wijzigingen op het systeem met een bestaande exceptie

Bijlage A – NEN7510-2:2017

Bijlage B – NCSC Inschalingsmatrix

Documenthistorie

Begrippenlijst

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 of VIEW) en op applicatieonderdelen van bedrijfssystemen.	
Motivatie	Alle software kan fouten bevatten of gebruik maken van inmiddels achterhaalde technieken waar beveiligingslekken in zitten en moeten dus gerepareerd worden	
Maatregel	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 • ICT systemen ten bate van medische systemen

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

Beschrijving	Diepteverdediging 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.	
Motivatie	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	
Maatregel		• Zie 2.01 en verder

1.03 Classificatie van software kwetsbaarheden

Beschrijving	Ken alle patches een prioriteitstelling toe op basis van een risicoafweging. Hanteer de klassen: Urgent, Hoog, Midden, Laag.	
Motivatie	De technische maatregel om te patchen is herleidbaar naar geïdentificeerde risico’s van een fout of kwetsbaarheid. Aansluiting op standaarden en best-practices.	
Maatregel	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

Beschrijving	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.	
Motivatie	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	
Maatregel	Volg het changeproces van het Amsterdam UMC	• Testen • Back-up en roll-back • Gefaseerd uitrollen met pliotgroepen

1.05 Gevonden potentiële technische kwetsbaarheden behoort een passende en tijdige actie te worden ondernomen

Beschrijving	Als reactie op de identificatie van potentiële technische kwetsbaarheden behoort passende en tijdige actie te worden ondernomen	
Motivatie	Om de kans op misbruik zo klein mogelijk te houden moet er snel gehandeld worden. Echter zonder de bedrijfsvoering te verstoren.	
Maatregel	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. Niet in dit kader
	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 Actuele en volledige inventaris in CMDB

Beschrijving	Configuratie Management Database heeft een inventarisatie van alle assets	
Motivatie	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	
Maatregel	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, Voorheen PCH010*	

2.02 Classificatie van software kwetsbaarheden volgens vastgestelde methodiek

Beschrijving	Ken alle patches een prioriteitstelling toe op basis van een risicoafweging. Hanteer de klassen: Urgent, Hoog, Midden, Laag.	
Motivatie	De technische maatregel om te patchen is herleidbaar naar geïdentificeerde risico's van een fout of kwetsbaarheid. Aansluiting op standaarden en best-practices.	
Maatregel	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 B - 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

Beschrijving	Hanteer een geplande cyclus voor patches, die gestandaardiseerd worden getest en uitgerold.	
Motivatie	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.	
Maatregel	Maak werkzaamheden ten behoeve van software updates en testen een regulier onderdeel van de planning.	• Plan patch werkzaamheden in • Standaardchange voor regulier patchen
	Automatiseer waar mogelijk	Automatiseer uitrol[1] • Besturingssystemen • Kantoorapplicaties
Noot	[1]*Een voorbeeld is Windows OS updates met SCCM*	

2.04 Tijdsplan voor het updaten van systemen met security patches

Beschrijving	Volg een tijdsplan waarbinnen de updates uitgevoerd moeten zijn om de kans op misbruik door cybercriminelen te verkleinen.	
Motivatie	Handhaven van snelheid bij het oplossen van kwetsbaarheden, omdat bekende kwetsbaarheden op zeer korte termijn worden misbruikt.	
Maatregel	Voer als Urgent geclassificeerde patches zo snel mogelijk uit en niet later dan hieronder in de tabel weergegeven.	• Zie 2.05
	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 2.09 • Voor uitzonderingen zie 3.01

Urgentietabel – Tijdslijnen waarbinnen security patches geïnstalleerd moeten worden

	Urgent	Hoog	Midden	Laag	
	< 72 uur	30 dagen[1]	60 dagen	90 dagen	
Versnelde uitrol		14 dagen			Zie 2.05
Centrale uitrol		30 dagen	30 dagen	30 dagen	Zie 2.03
DMZ	< 24 uur	< 1 dag	7 dagen	30 dagen	

Noot [1] Kalenderdagen

2.05 Voor urgente kwetsbaarheden wordt een versnelde procedure gevolgd

Beschrijving	Urgent geclassificeerde kwetsbaarheden (ook wel 'patch now' genoemd), worden met voorrang en mogelijk buiten de reguliere patchcycli om behandeld.	
Motivatie	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.	
Maatregel	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

2.06 Iedere patch worden standaard getest

Beschrijving	Test alle patches voorafgaand aan de uitrol in een representatieve testomgeving.	
Motivatie	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.	
Maatregel	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 2.05 en 2.07
Noot	*Zie ook 2.05 Voor urgente kwetsbaarheden wordt een versnelde procedure gevolgd* *En 2.07 Gefaseerde uitrol over een platform*	

2.07 Gefaseerde uitrol over een platform

Beschrijving	Rol een patch gefaseerd uit op de productieomgeving van een platform.	
Motivatie	Onvoorziene problemen met een patch blijven beperkt tot een kleine gebruikersgroep.	
Maatregel	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

2.08 Volg aanpassingen en nieuws over uitgebrachte softwareversies

Beschrijving	Richt voor ieder systeem een methode in om over uitgebrachte patches geïnformeerd te worden	
Motivatie	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.	
Maatregel	Beheerder volgt nieuwsbrieven van leverancier (of derden) over de door hun beheerde producten	Abonneer op distributielijst • 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)

2.09 Mitigeer risico's als updaten van de software niet mogelijk, of beschikbaar is

Beschrijving	Scherm systemen waarvan de patch niet geïnstalleerd kan worden zodanig af dat de daardoor blootgestelde kwetsbaarheden niet benaderbaar zijn.
Motivatie	Wanneer een kwetsbaarheid niet kan worden opgelost dient een systeem zodanig te worden afgeschermd dat de kans zo klein mogelijk is dat van de kwetsbaarheid misbruik kan worden gemaakt. Het risico neemt toe als er exploit (hacker) software beschikbaar is voor deze kwetsbaarheid.

Maatregel	Indien geen patch beschikbaar is, behoren andere beheersmaatregelen te worden overwogen.	• Blokkeer de aanvalsroutes waarlangs de kwetsbaarheid misbruikt kan worden. • Toegangsbeveiligingsmaatregelen aanpassen of toevoegen, bijv. firewalls, rond de grenzen van netwerken • vaker monitoren om werkelijke aanvallen op te sporen • Stimuleer awareness omtrent de kwetsbaarheid en wees terughoudend in het gebruik ervan
	Beperking van functionaliteit	• Accepteer een beperkt verlies aan functionaliteit. • Doe dit aan de hand van een risico analyse
	Kan het risico niet weggenomen worden volg het exceptieproces	• Zie 3.01

3. Governance en excepties op dit kader

3.01 Excepties op dit kader

Beschrijving	Geeft aan hoe een uitzondering of exceptie op dit kader aangevraagd moet worden en aan welke voorwaarden er voldaan moet worden.	
Motivatie	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.	
Maatregel	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 Wijzigingen op het systeem met een bestaande exceptie

Beschrijving	Wijzigingen (changes) op het systeem of op de infrastructuur, kunnen invloed hebben op de beperkte (exceptie) beveiliging.	
Motivatie	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.	
Maatregel	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 – NEN7510-2:2017

12.6.1 Beheer van technische kwetsbaarheden

Beheersmaatregel
Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt, behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt, aan te pakken.

Implementatierichtlijn
Een actuele en volledige inventaris van bedrijfsmiddelen (zie hoofdstuk 8) 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.

Als reactie op de identificatie van potentiële technische kwetsbaarheden behoort passende en tijdige actie te worden ondernomen. Om een doeltreffend beheerproces voor technische kwetsbaarheden vast te stellen behoren de volgende richtlijnen te worden gevolgd:

a) de organisatie behoort de rollen en verantwoordelijkheden in samenhang met het beheer van technische kwetsbaarheden te definiëren en vast te stellen, met inbegrip van het monitoren van de kwetsbaarheden, een risicobeoordeling van de kwetsbaarheden, het installeren van herstelprogramma's (patching), het traceren van bedrijfsmiddelen en de vereiste coördinatieverantwoordelijkheden;
b) informatiemiddelen die worden gebruikt om relevante technische kwetsbaarheden te bepalen en om het bewustzijn hierover levend te houden, behoren te worden vastgesteld voor software en andere technologie (op basis van de inventarislijst van bedrijfsmiddelen, zie 8.1.1); deze informatiemiddelen behoren te worden geactualiseerd op basis van veranderingen in de inventarislijst of als andere nieuwe of nuttige middelen zijn gevonden;
c) een tijdpad behoort te worden gedefinieerd waarbinnen moet worden gereageerd op aankondigingen van potentieel relevante technische kwetsbaarheden;
d) als een potentieel technische kwetsbaarheid is geïdentificeerd, behoort de organisatie de samenhangende risico's en de te ondernemen acties vast te stellen; een dergelijke actie kan patching van kwetsbare systemen inhouden, of het toepassen van andere beheersmaatregelen.
e) afhankelijk van hoe urgent een technische kwetsbaarheid moet worden aangepakt behoort de te ondernemen actie te worden uitgevoerd in overeenstemming met de beheersmaatregelen in verband met wijzigingsbeheer (zie 12.1.2) of door responsprocedures voor informatiebeveiligingsincidenten te volgen (zie 16.1.5);
f) indien een patch uit een legitieme bron beschikbaar is, behoren de risico's die verbonden zijn aan het installeren van de patch te worden beoordeeld (de risico's die worden gevormd door de kwetsbaarheid behoren te worden vergeleken met het risico van het installeren van de patch);
g) 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; indien geen patch beschikbaar is, behoren andere beheersmaatregelen te worden overwogen, zoals:
    a. diensten of capaciteiten in verband met de kwetsbaarheid uitschakelen;

   b. toegangsbeveiligingsmaatregelen aanpassen of toevoegen, bijv. firewalls, rond de grenzen van netwerken (zie 13.1);
   c. vaker monitoren om werkelijke aanvallen op te sporen;
   d. bewustzijn omtrent de kwetsbaarheid kweken;

h) over alle procedures behoort een auditlogbestand te worden bijgehouden;
i) het beheerproces met betrekking tot de technische kwetsbaarheid behoort regelmatig te worden gemonitord en geëvalueerd om de doeltreffendheid en doelmatigheid ervan te waarborgen;
j) systemen met een hoog risico behoren eerst te worden aangepakt;
k) om gegevens over kwetsbaarheden te communiceren aan de functie die moet reageren op het incident en om te voorzien in uit te voeren technische procedures in geval van een incident, behoort een doeltreffend beheerproces met betrekking tot de technische kwetsbaarheid te worden afgestemd op incidentbeheeractiviteiten;
l) een procedure definiëren om de situatie aan te pakken waar een kwetsbaarheid is geïdentificeerd maar waar geen passende tegenmaatregel voorhanden is. In deze situatie behoort de organisatie risico's in verband met de bekende kwetsbaarheid te evalueren en passende opsporings- en corrigerende maatregelen te definiëren.

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

Documenthistorie

NEN7510-2 referenties

#	Paragraaf
12.6.1	Beheer van technische kwetsbaarheden

Overige Referenties

Auteur	Titel	Bron
L. Groenewegen	Kaderdocument-patchbeleid	VUmc

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

Distributie

Datum	Versie	Aan	Functie of rol
25-01-2021	v0.1	ASB overleg	Initiële opzet adhv NEN7510
01-02-2021	V0.2	Ketenoverleg Dienst ICT	

Wijzigingen

Artikel Nummer	Titel	Wijziging

Begrippenlijst

Zie https://edu.nl/ay6b4