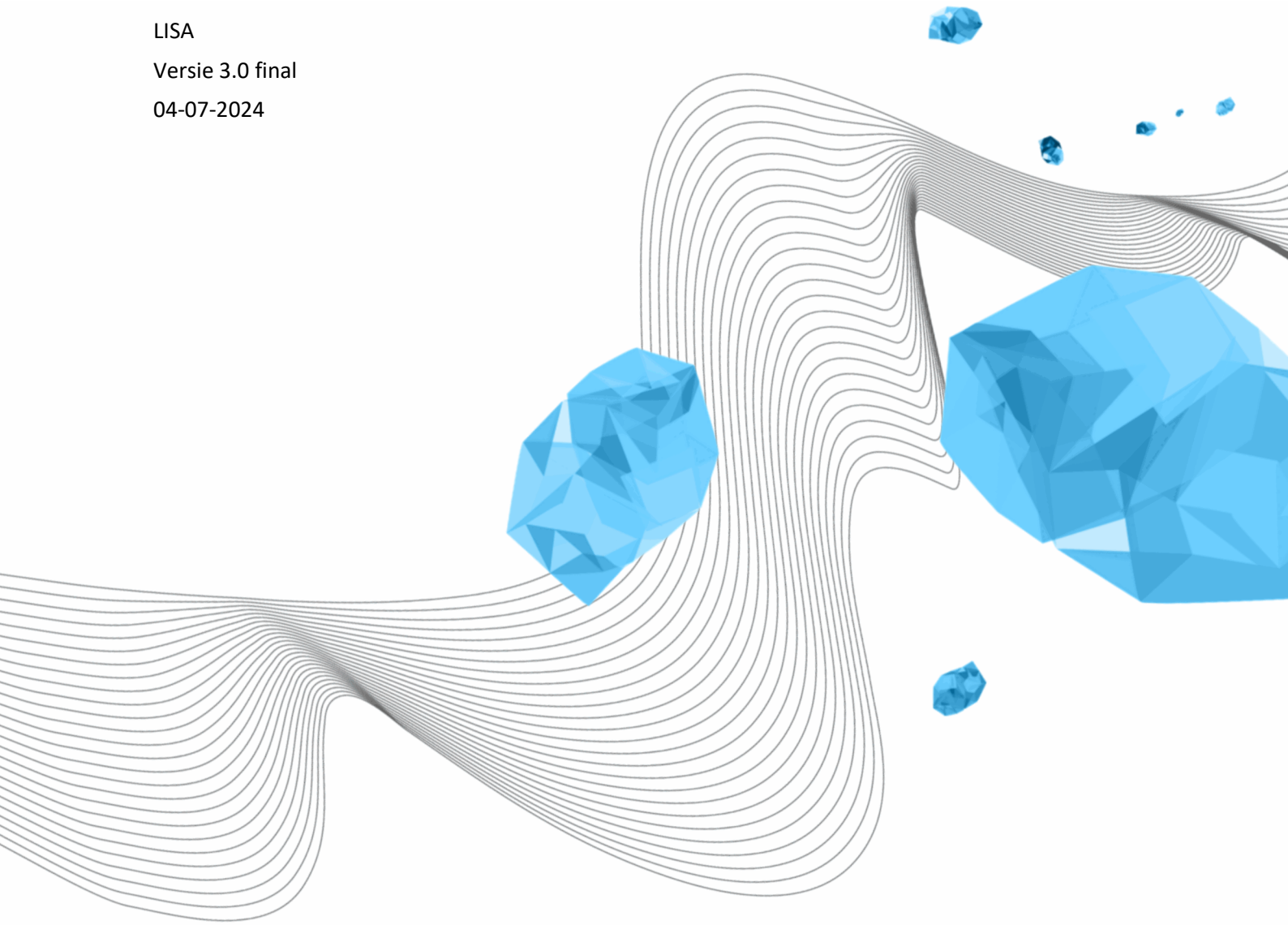
Status: Versie 3.0 final
Datum vastgesteld in MT-LISA: 08-07-2024
Datum vastgesteld in CvB: 03-09-2024
Herzien: 04-07-2024

PATCHMANAGEMENTRICHTLIJN UNIVERSITEIT TWENTE

LISA
Versie 3.0 final
04-07-2024



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Patchmanagementrichtlijn Universiteit Twente

KENMERK
LISA-394

VERSIE (STATUS)
3.0

DATUM
04-07-2024

AUTEUR(S)
Henk Swaters

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
0.5	25-22-2020	H.W.Swaters	Initiële versie besproken in MT-LISA
1.0	09-11-2022	H.W.Swaters	Herzien door CISO en security managers
1.1	25-11-2022	H.W.Swaters	Vastgesteld MT-LISA 21-11-2022
2.0	23-06-2023	H.W.Swaters	Evaluatie, geen wijzigingen, huisstijl aangepast
3.0	4 juli 2024	H.W.Swaters	Volledig herzien en herschreven

DISTRIBUTIELIJST

VERSIE	DATUM	GEDISTRIBUEERD AAN	OPMERKING
0.5	25-11-2020	MT-LISA, security management, teamleiders	
1.0	09-11-2022	MT-LISA, security managers, LISA Intranet	
1.1	25-11-2022	MT-LISA, security managers, LISA intranet	Vastgesteld MT-LISA 21-11-2022
2.0	23-06-2023	MT-LISA, security managers, LISA intranet	Vastgesteld MT-LISA 10-07-2023
3.0	08-07-2024	MT-LISA	Vastgesteld MT LISA 08-07-2024

INHOUDSOPGAVE

1 INLEIDING

De patchmanagementrichtlijn van de Universiteit Twente (UT) beschrijft de maatregelen en procedures voor een effectieve uitvoering van patchmanagement. Deze richtlijn is in overeenstemming met het informatiebeveiligingsbeleid van de Rijksoverheid, de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de Baseline Informatiebeveiliging Rijksdienst (BIR). Zie de bijlage voor details.

2 PATCH MANAGEMENT

Een patch (fix, hotfix) is een update die een deel van de software bijwerkt om een bug of fout te herstellen die na de release is ontdekt. Deze patchmanagementrichtlijn richt zich op patches die kwetsbaarheden met betrekking tot Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) oplossen. Updates of upgrades die alleen nieuwe functionaliteiten toevoegen, vallen niet onder deze patchmanagementrichtlijn, tenzij ze patches bevatten.

De UT benadrukt het belang van patchmanagement omdat het nalaten hiervan de kwetsbaarheid van systemen vergroot. Deze richtlijn is van toepassing op alle medewerkers die betrokken zijn bij het beheer van hardware en software binnen de UT-organisatie.

3 PATCH MANAGEMENT CYCLUS

3.1 ONTVANGST EN BEOORDELING

Zodra een nieuwe patch beschikbaar is, moet deze worden gedocumenteerd en beoordeeld door het IT-beheerteam.

3.2 IMPACT ANALYSE

Voer een impactanalyse uit om te bepalen hoe de patch bestaande functionaliteiten en systemen kan beïnvloeden.

3.3 TESTOMGEVING

Voer de patch indien mogelijk eerst uit in een gescheiden testomgeving.

3.4 TERUGVALOPTIES

Zorg voor een gedetailleerd rollback-plan voor het geval de patch problemen veroorzaakt in de productieomgeving.

4 MAATREGELEN

De volgende maatregelen zijn vastgesteld voor de UT:

4.1 TECHNISCHE INTEGRITEIT

De technische integriteit van programmapakketten en infrastructurele programmatuur wordt gecontroleerd door middel van een signature- of hashingmechanisme en een controlegetal van de leverancier, dat via een vertrouwd kanaal is verkregen. Dit kan ook geautomatiseerd door een betrouwbaar mechanisme uitgevoerd worden zoals Puppet of Windows Update.

4.2 RISICO-EVALUATIE

Indien een patch beschikbaar is, dienen de risico's verbonden aan de installatie van de patch te worden geëvalueerd. Indien de kans op misbruik en schade laag is, kan de patch worden ingepland bij de eerstvolgende onderhoudsronde van het systeem. Indien de kans op misbruik of schade hoog is wordt de patch met spoed uitgevoerd.

4.3 TESTING EN ROLLBACK

Alle patches dienen voor installatie te worden getest, maar voor systeemsoftware waarbij de leverancier betrouwbare en geteste patches levert kan de evaluatie en het testen overgeslagen worden, indien er een mechanisme bestaat om een foutieve patch terug te draaien.

4.4 SPOEDPATCHES

Spoed patches (er is een bekende exploit of een high security risk) worden zo snel mogelijk, maar uiterlijk binnen één dag opgepakt. Indien dit niet mogelijk is, bijvoorbeeld omdat de uitrol niet mogelijk is of te veel tijd in beslag neemt, dan worden er in overleg met de systeemeigenaar adequate mitigerende maatregelen getroffen.

4.5 GEAUTOMATISEERDE PATCHBEHEER TOOLS

Maak gebruik van geautomatiseerde patchbeheer tools zoals Microsoft MECM, WSUS, Jenkins, of andere CI/CD pipelines om het patchproces te stroomlijnen.

Zorg ervoor dat deze tools up-to-date zijn en correct geconfigureerd zijn om alle relevante systemen en applicaties te beheren.

4.6 COMMUNICATIE EN DOCUMENTATIE

Communiceer geplande patch-activiteiten duidelijk naar alle stakeholders, inclusief verwachte downtime en impact op de gebruikers.

Documenteer alle stappen van het patchproces, inclusief de resultaten van de impactanalyse, tests, en uiteindelijke implementatie.

Documenteer welke patches zijn toegepast op welke systemen en wanneer.

4.7 CHANGE MANAGEMENT

Stem de implementatie en de goedkeuring af volgens de bestaande changeprocessen.

5 VERANTWOORDELIJKHEDEN

5.1 IT-BEHEERDER (VERANTWOORDELIJK VOOR UITVOERING)

Voert patchmanagementrichtlijn tijdig en adequaat uit voor systemen onder zijn/haar beheer.

Lever periodiek een evaluatie aan over de uitvoering van de patchmanagementcyclus en geef verbeterpunten aan.

In het geval van spoedpatches, waar de uitrol niet mogelijk is of te veel tijd in beslag neemt, moeten er adequate mitigerende maatregelen worden getroffen in overleg met de systeemeigenaar.

5.2 LEIDINGGEVENDE VAN IT-BEHEERDER (PROCESVERANTWOORDELIJK)

Verantwoordelijk dat de patchmanagementrichtlijn tijdig en adequaat uitgevoerd wordt.

Zorgt ervoor dat alle IT-beheerders en ontwikkelaars op de hoogte zijn van de patchmanagementprocedures en tools.

Organiseert periodieke training om best practices in patchbeheer te delen en de bewustwording te verhogen.

5.3 SYSTEEMEIGENAAR (EINDVERANTWOORDELIJK OVER DE TOEPASSING VAN PATCHES)

Laat een impactanalyse uitvoeren om de mogelijke gevolgen van de patch op de bestaande functionaliteiten en de stabiliteit van het systeem te begrijpen.

Besluit, in overleg met het IT-beheerteam en securitymanagement, welke patches toegepast moeten worden en wanneer.

5.4 ROL SECURITY MANAGEMENT (MONITORING EN AUDITS)

Voert regelmatige monitoring, assessments of audits uit om te controleren of alle patches correct zijn toegepast en of het patchbeheerproces wordt gevolgd.

Documenteert eventuele afwijkingen en corrigerende maatregelen.

Stelt periodieke rapporten op over de status van het patchbeheer, inclusief statistieken over toegepaste patches, outstanding patches, en compliance-status.

Mag in urgente gevallen het besluit nemen om een patch als spoedpatch te bestempelen.

6 REVIEW VAN DEZE RICHTLIJN

Deze richtlijn wordt jaarlijks herzien om ervoor te zorgen dat deze up-to-date blijft met de nieuwste beveiligingsstandaarden en -praktijken. De volgende herziening vindt plaats medio 2025. Er kunnen reden zijn voor een tussentijdse evaluatie. Als die evaluatie er aanleiding toe geeft zal de richtlijn eerder worden aangepast.

De CISO van de Universiteit Twente is verantwoordelijk voor deze richtlijn.

Dit regelement wordt vastgesteld door MT-LISA.

BIJLAGE 1: STANDAARDEN

Deze richtlijn is in lijn met het informatiebeveiligingsbeleid van de Rijksoverheid, de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de Baseline Informatiebeveiliging Rijksdienst (BIR). Hieronder is beschreven hoe de voorgestelde maatregelen overeenkomen met deze standaarden:

NEN/ISO 27002:2007

De NEN/ISO 27002:2007 standaard biedt best practices voor informatiebeveiligingsbeheer. De voorgestelde maatregelen sluiten hierbij aan door een systematische benadering van patchmanagement, inclusief risicobeoordeling, testing, monitoring, en compliance-audits. Specifieke relevante secties zijn:

- Patchbeheer: Implementeren van een systematisch proces voor patchbeheer en risicobeoordeling.
- Controlemechanismen: Gebruik van signature- en hashingmechanismen om de integriteit van patches te waarborgen.
- Training en Bewustwording: Regelmatige trainingen om bewustwording en naleving van beveiligingsprocedures te verzekeren.
- Audits en Compliance: Periodieke audits om de effectiviteit van beveiligingsmaatregelen te controleren.

BASELINE INFORMATIEBEVEILIGING RIJKSDIENST (BIR)

De BIR biedt richtlijnen voor het beheren van informatiebeveiligingsrisico's binnen de Nederlandse Rijksdienst. De voorgestelde richtlijnen voldoen aan de BIR door het volgende te benadrukken:

- Risicobeoordeling: Evaluatie van risico's verbonden aan het toepassen van patches, inclusief het prioriteren van patches op basis van kritikaliteit.
- Incidentbeheer: Snel reageren op beveiligingsincidenten door spoedpatches toe te passen en mitigerende maatregelen te treffen.
- Integriteitscontroles: Controle van de integriteit van programmapakketten en patches om de beveiliging van systemen te waarborgen.

INFORMATIEBEVEILIGINGSBELEID VAN DE RIJKSOVERHEID

Het informatiebeveiligingsbeleid van de Rijksoverheid legt de nadruk op een gestructureerde aanpak voor het beheer van informatiebeveiliging. De voorgestelde maatregelen ondersteunen dit beleid door:

- Beheer van kwetsbaarheden: Invoering van processen voor het identificeren, evalueren, en mitigeren van kwetsbaarheden.
- Communicatie en documentatie: Heldere communicatie en documentatie van patchactiviteiten en beveiligingsmaatregelen.
- Periodieke controles: Uitvoeren van periodieke vulnerabilityscans, pentests, en risico-assessments.