Webapplicaties

Leids Universitair Medisch Centrum (LUMC)

Versiebeheer

Versie	Auteur	Datum	Opmerking
1.0	Michel Dieben	12-02-2024	Eerste actieve versie
1.1	Michel Dieben	11-03-2024	Concept voor versie 2
1.9	Michel Dieben	30-05-2024	Splitsing ontwikkelingsdeel naar ISMS 121 – Veilig Ontwikkelen
2.0	Michel Dieben	28-06-2024	Input van medelezers verwerkt. Definitieve versie 2
2.1	Joop Azier, Corné Baaij, Leontine Fillet	28-07-2025	Review uitgevoerd, table cryptografie TLS bijgewerkt o.b.v. huidige standaarden NCSC, toevoeging verplichting ACME.

INHOUDSOPGAVE

1. ACHTERGROND

1.1 INLEIDING

Om de veiligheid van het LUMC netwerk te garanderen behoren op alle aangesloten systemen passende maatregelen te zijn getroffen om te voorkomen dat het systeem door ongeautoriseerde derden benaderd of gebruikt kan worden. Dit beleid is een verbijzondering van het Informatiebeveiligingsbeleid LUMC (ISMS 003) ingericht op webapplicaties.

1.2 ROLLEN, TAKEN EN VERANTWOORDELIJKHEDEN

- De eigenaar is verantwoordelijk dat dit beleid gevolgd wordt. De uitvoer kan belegd zijn bij interne of externe beheerders.
- IT&DI Security is verantwoordelijk voor monitoring en handhaving.

1.3 REIKWIJDTE

Dit beleid is van toepassing op alle applicaties die via het internet te benaderen zijn en waarvan de server verbinding maakt met het LUMC netwerk. Dit geldt expliciet ook voor webapplicaties die deels extern gehost worden, maar communiceren met servers binnen het LUMC netwerk. Een voorbeeld hiervan is een webapplicatie waarvan de frontend in de cloud wordt gehost en de database on-premise staat.

Er wordt geen onderscheid gemaakt tussen applicaties die worden ontwikkeld door een interne of een externe ontwikkelaar.

Dit beleid geldt voor maar is niet beperkt tot servers die inkomende verbindingen accepteren voor de volgende diensten:

1.3.1 WEB SERVERS

Diensten zoals bijvoorbeeld websites of API’s over HTTPS.

1.3.2 FILE SERVERS

Diensten zoals bijvoorbeeld SFTP.

1.3.3 REMOTE ACCESS

Diensten zoals bijvoorbeeld SSH.

1.4 BEGRIPPEN

Begrip	Uitleg
Applicatie	Synoniem voor: programma, (web)applicatie, mobiele app, software.
Systeem	Verzameling van onderdelen dat bij elkaar als één geheel wordt gebruikt of beschouwd.
Onderdelen	Fysieke en virtuele systemen die gezamenlijk deel uitmaken van het systeem als geheel.
Interne ontwikkelaar	Een LUMC medewerker met aanstelling
Externe ontwikkelaar	Een partij dat niet als LUMC medewerker is aangesteld. Bijvoorbeeld: (commerciële) leverancier, onderzoeker, academische instelling, student, stagiair, ZZP'er, (consortium) partner.
SBOM	Software bill of materials
Externe bibliotheken	Bijvoorbeeld: dependencies, repositories
Externe software	Bijvoorbeeld: containers, images
Service	Softwareproces dat op de achtergrond draait en bepaalde functionaliteiten aanbiedt. Bijvoorbeeld: httpd, sshd

2. BELEID

Tenzij anders aangegeven moet aan onderstaande beleidsregels aantoonbaar worden voldaan.

2.1 ONTWIKKELING

Beleidsregels voor de ontwikkeling zijn beschreven in ISMS121 – Veilig Ontwikkelen. Aanvullend geldt:

a. De applicatie wordt minimaal gecontroleerd op de aanwezigheid van kwetsbaarheden in de OWASP Top Ten na elke wijziging in de broncode of configuratie;

2.1.1 LINKS

OWASP Top Ten | OWASP Foundation

2.2 OPERATIONALISERING

a. De server met het onderdeel dat vanaf het internet te benaderen is, is in een netwerkdeel geplaatst dat afgeschermd is van de rest van het LUMC netwerk;
b. Het systeem voldoet aan de ISMS115 - Standaard voor Systeemhardening;
c. De applicatie wordt gepubliceerd via F5 BIG-IP;
d. De gebruikte domeinnaam wordt aangevraagd door IT&DI en blijft ook nadat het niet meer gebruikt wordt in bezit van het LUMC;
e. De interne hostname van servers wordt niet gebruikt in openbaar beschikbare informatie zoals in een URI, een URL, certificaten, etc.;
f. Verkeer tussen het internet en de server wordt gecontroleerd middels de LUMC firewall én de LUMC Web Application Firewall;
g. Er wordt uitsluitend gebruik gemaakt van protocollen die encryptie ondersteunen (bijvoorbeeld: HTTPS in plaats van HTTP);
h. Indien een onversleuteld protocol wordt gebruikt moet verkeer worden omgeleid naar de versleutelde variant (bijvoorbeeld: HTTP to HTTPS redirect);
i. De applicatie maakt gebruik van een geldig certificaat;
    1. In het geval van systemen met meerdere onderdelen (zoals proxy's) moet het onderdeel dat openbaar toegankelijk is een public signed certificaat hebben;
    2. Systemen die intern met elkaar communiceren mogen ook een self-signed certificaat of LUMC PKI certificaat gebruiken;
    3. Systemen die extern gepubliceerd worden moeten gebruik maken van het ACME protocol op de F5 om certificaten automatisch te vernieuwen.
j. Verzoeken naar en antwoorden van de applicatie worden gelogd en minstens 6 maanden bewaard. De logging bevat minimaal informatie over:
    1. De herkomst en bestemming van verzoeken en antwoorden (hostname, IP);
    2. Tijd en datum;
    3. Gebruikersnaam;
    4. De gebruikte service (naam, instance nummer);
    5. Methode (GET, POST, etc.);
    6. De locatie waar het verzoek op betrekking had (bijvoorbeeld default.htm);
    7. Query informatie (bijvoorbeeld URI)
    8. Status informatie (bijvoorbeeld HTTP, Win32 status codes, substatus codes)

9. De grootte van het verzoek en antwoord (bijvoorbeeld bytes sent / received);
10. Het gebruikte protocol;
11. De User Agent;
12. Cookie informatie;
13. Referrer;

k. Ongebruikte applicaties zijn verwijderd om “Living of the Land” moeilijker te maken;
l. Processen hebben zo min mogelijk systeemrechten en nooit hoge rechten (system, root, admin, e.d.).

2.2.1 LINKS

Living off the Land: How hackers blend into your environment | Darktrace Blog

Living off the Land Binaries and Scripts Project (LOLBAS)

2.3 CONTAINERS

Indien gebruik wordt gemaakt van containers gelden de volgende beleidsregels:

a. Container images worden uitsluitend afgenomen van een leverancier die ervoor garant kan staan dat aan de voorwaarden binnen dit beleid wordt voldaan;
b. Indien gebruik wordt gemaakt van een container register is deze afdoende beveiligd;
c. Zelf gebouwde containers dienen te voldoen aan de beleidsregels zoals beschreven in ISMS121 - Veilig Ontwikkelen.

2.4 LOGISCHE TOEGANGSBEVEILIGING

a. Wachtwoorden binnen het systeem voldoen aan het LUMC wachtwoordbeleid (ISMS 118);
b. Multi-factor authenticatie (MFA) is te allen tijde verplicht op alle accountniveaus conform beleid Logische toegangsbeveiliging (ISMS110);
c. AD-tiering is toegepast indien beschikbaar, conform Beleid Accounts speciale toegangsrechten (ISNS119);
d. Autorisatie o.b.v. ‘Least privilege’ is toegepast op de applicatie en op de database, conform Logische toegangsbeveiliging (ISMS110).

2.5 BESCHERMING

a. Het systeem is opgenomen in het SOC/SIEM;
b. Het systeem is voorzien van de centraal beheerde endpoint protection oplossing;
c. Het systeem voldoet aan de LUMC Standaard voor Systeemhardening (ISMS 115);
d. Aanvullend zijn de servers geconfigureerd volgens de CIS richtlijnen op het hoogst beschreven niveau.

2.6 KWETSBAARHEDEN

a. Er wordt proactief gecontroleerd op kwetsbare componenten (zoals dependencies);
b. De detectie van kwetsbare componenten vindt continu plaats;

c. De servers zijn opgenomen in de vulnerability scan software van IT&DI;

d. Geen van de onderdelen mogen “End of Life” status hebben.

2.6.1 OPLOSSEN VAN KWETSBAARHEDEN

a. Kwetsbaarheden worden uiterlijk volgens onderstaande tabel verholpen. De maximum tijd begint vanaf het beschikbaar komen van de patch.

CVSS Score	CVSS Severity	Maximum tijd tot patchen
0	None	
0.1 – 3.9	Low	60 dagen
4.0 – 6.9	Medium	30 dagen
7.0 – 8.9	High	14 dagen
9.0 – 10	Critical	48 uur

Tabel – Maximum tijd tot patchen

2.7 VERWERKINGEN

2.7.1 VERWERKING VAN PERSOONSGEGEVENS

a. Indien persoonsgegevens worden verwerkt, dient het systeem te voldoen aan de ISO27001.

b. Gegevens worden versleuteld opgeslagen conform de Standaard voor cryptografie binnen het LUMC (ISMS109);

c. Gegevens worden versleuteld getransporteerd conform de Standaard voor cryptografie binnen het LUMC (ISMS109).

2.7.2 VERWERKING VAN PATIËNTGEGEVENS

a. Indien patiëntgegevens worden verwerkt, dient het systeem te voldoen aan NEN7510 (en alle aanverwante normen, zoals NEN7512 en NEN7513).

2.8 BEHEER

a. Er zijn voldoende geschoolde en ervaren beheerders met kennis van de applicatie voor de ontwikkeling, ondersteuning en het beheer van de applicatie (minimaal 2);

b. De server is opgenomen in het centrale beheer door IT&DI voor updates en patching (SCCM/Ansible) van het besturingssysteem en centraal beheerde componenten.

2.9 TECHNISCH SPECIFIEKE EISEN

a. De webapplicatie moet een recente pentest hebben ondergaan. Hoog risicobevindingen moeten gedocumenteerd & opgelost zijn;

b. De webapplicatie is opgenomen in de internet.nl scans en het systeem voldoet aan de eisen zoals beschreven in Bijlage A;

c. Foutmeldingen worden dusdanig ingericht dat het geen informatie kan prijsgeven zoals gebruiker bestaat niet, database niet bekend, rechtstreekse foutmeldingen uit de backend, geen meldingen in de console;

d. Directories zijn niet doorzoekbaar vanuit de webapplicatie.

3. HANDHAVING

Handhaving van dit beleid is essentieel om de beveiliging van het LUMC-netwerk en -gegevens te waarborgen. Webapplicaties die niet voldoen aan de vereisten van dit beleid, krijgen geen toestemming voor firewalldoorgang of kunnen hun toestemming voor firewalldoorgang verliezen. Dit betekent dat de applicatie niet meer toegankelijk zal zijn vanuit externe netwerken totdat de beveiligingsproblemen zijn verholpen en de applicatie opnieuw is goedgekeurd.

BIJLAGE A.

Eis	Toelichting
HTTPS	De website is uitsluitend bereikbaar via HTTPS, verzoeken via HTTP worden verwezen naar HTTPS.
HTTP-compressie	Niet toegestaan
HSTS	`max-age=31536000; includeSubDomains; preload`
TLS-verie	Minimaal 1.2

Ciphers (algoritmeselecties)	Uitsluitend onderstaande ciphers zijn toegestaan. De voorkeur gaat uit naar de implementatie van TLS 1.3.
	
	`TLS 1.3`
	`TLS_AES_256_GCM_SHA384`
	`TLS_CHACHA20_POLY1305_SHA256`
	`TLS_AES_128_GCM_SHA256`
	`TLS_AES_128_CCM_SHA256`
	
	`TLS 1.2`
	`ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256`
	`ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
	`ECDHE_ECDSA_WITH_AES_256_CCM`
	`ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
	`ECDHE_ECDSA_WITH_AES_128_CCM`
	`ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`
	`ECDHE_RSA_WITH_AES_256_GCM_SHA384`
	`ECDHE_RSA_WITH_AES_128_GCM_SHA256`

Sleuteluitwisselings-parameters	Uitsluitend de onderstaande elliptische krommen zijn toegestaan:
	`Secp512r1`
	`secp384r1`
	`secp256r1`
	`curve 448`
	`curve 25519`
	`BrainpoolP521r1`
	`BrainpoolP5384r1`
	`BrainpoolP256r1`

Hashfunctie voor sleuteluitwisseling	Het gebruik van een veilige hashfunctie voor sleuteluitwisseling is verplicht middels:

	SHA-256 SHA-384 SHA-512
TLS-compressie	Niet toegestaan
Insecure renegotiation	Niet toegestaan (n.v.t. in TLS 1.3)
Client-initiated renegotiation	Niet toegestaan (n.v.t. in TLS 1.3)
0-RTT	Niet toegestaan (n.v.t. in TLS 1.3)
OCSP stapling	Optioneel, bij voorkeur wel
Vertrouwensketen van certificaat	Verplicht

Publieke sleutel van certificaat	Uitsluitend de onderstaande elliptische curves zijn toegestaan:
	`secp384r1`
	`secp256r1`
	`curve 448`
	`curve 25519`
	
	Lengte van RSA-sleutels
	`4096 bit (of beter)`

Handtekening van certificaat	Het gebruik van een veilige hashfunctie voor certificaatondertekening is verplicht middels: SHA-256 SHA-384 SHA-512
Domeinnaam	De domeinnaam van de website komt overeen met de domeinnaam op het websitecertificaat
DANE	Optioneel
X-Frame-Options	Optioneel vanwege de verplichting van Content-Security-Policy
X-Content-Options	`nosniff`
Content-Security-Policy	1. `default-src` moet gedefinieerd zijn, zodat er een restrictieve default fallback policy bestaat voor door jouw website gebruikte bron-typen waarvoor geen specifieke policy is gedefinieerd. De waarde dient of `'none'` of `'self'` te zijn. Aanvullend kunnen de domeinnaam zelf, of zijn super-domeinnaam of sub-domeinnaam gedefinieerd worden. Naast deze waarden kan `'report-sample'` als waarde zijn ingesteld als je wil dat in de 'violation reports' code-voorbeelden worden opgenomen. Verder staan we `https:` toe, hoewel je dat niet nodig hebt als je je aan de onderstaande regels houdt. 2. `frame-src` moet worden gebruikt (hetzij per definitie of via de fallback naar `child-src` en `default-src`) en moet de waarde `'self'`, `'none'` of een specifieke URL hebben, zodat externe bronnen die in jouw website worden geladen verhinderd wordt om andere bronnen te framen of te embedden met behulp van HTML-elementen zoals `<frame>` en `<iframe>`.

	3. `frame-ancestors` moet gedefinieerd zijn en moet de waarde `'none'`, `'self'`, of een specifieke URL, zodat andere websites verhinderd wordt om jouw website te framen of te embedden met behulp van HTML-elementen zoals `<frame>`, `<iframe>`, `<object>`, `<embed>`, of `<applet>`. 4. `unsafe-inline`, `unsafe-eval` en `unsafe-hashes` zijn niet toegestaan, omdat deze XSS-aanvallen mogelijk maken. 5. `data:` is niet toegestaan in `default-src`, `script-src` en `object-src`, omdat dit XSS-aanvallen mogelijk maakt. 6. `http:` is niet toegestaan als schema, omdat dit het mogelijk maakt dat bronnen worden gedownload over een onveilige verbinding. Gebruik in plaats daarvan `https:`. 7. `*` (wildcard voor het schema- en host-gedeelte van een URL) is niet toegestaan, omdat daardoor iedere externe bron is toegestaan. 8. `127.0.0.1` is niet toegestaan, omdat dit aanvallen via content injection mogelijk maakt in een gecompromitteerd systeem.
Referrer-Policy	Toegestane policy-waarden: 1. Geen gevoelige informatie naar derde-partijen • `no-referrer` • `same-origin` 2. Gevoelige informatie naar derde-partijen alleen via beveiligde verbindingen (HTTPS) • `strict-origin` • `strict-origin-when-cross-origin`
Security.txt	Het bestaan van een up-to-date security.txt bestand in de directory .well-known is verplicht. Een actuele versie is te vinden op: `https://www.lumc.nl/.well-known/security.txt`