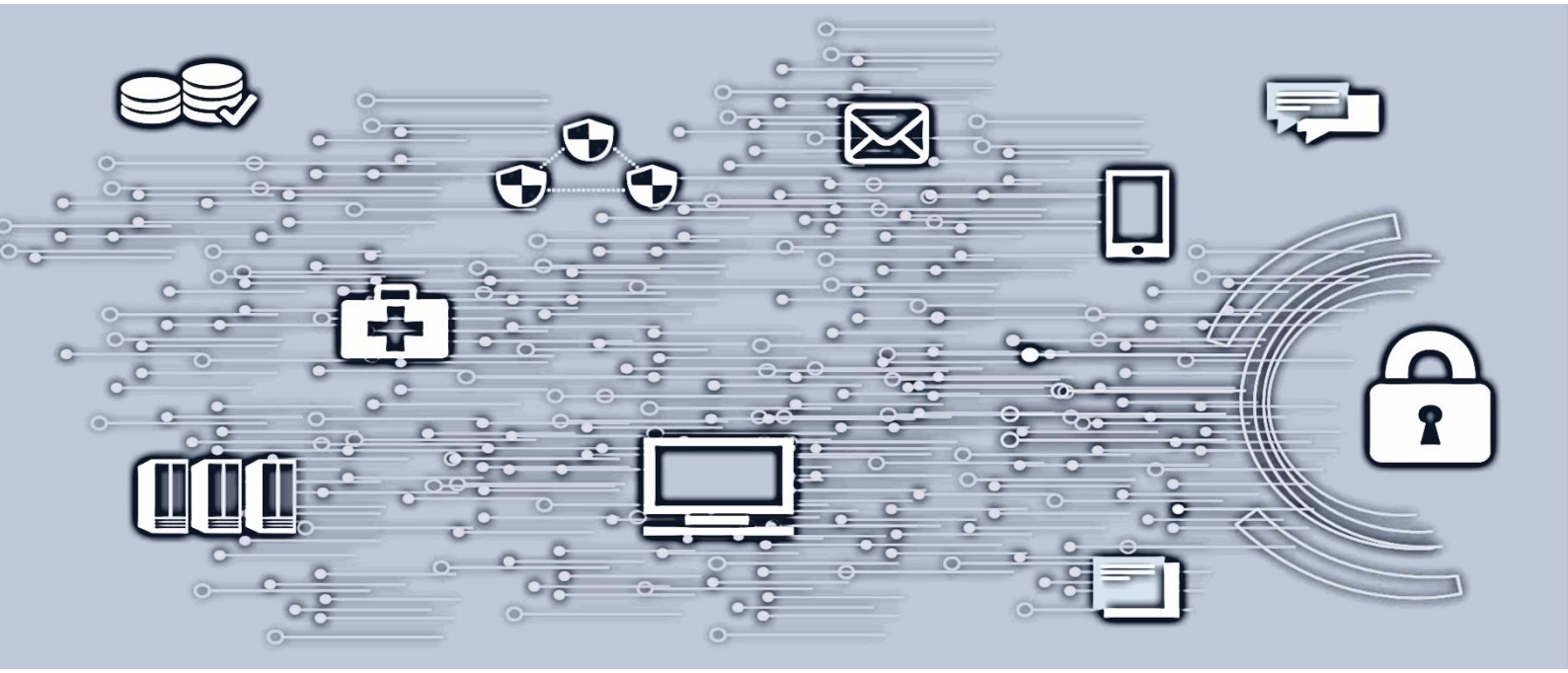
SYKEHUSPARTNER

NO-47 – Sikkerhetskrav til tjenester i DMZ



Innhold

Versjon	Dato	Godkjent av
1.0	2021-02-15	ISMB
1.1	2021-08-17	ISMB
1.2	2022-06-15	Christian Jacobsen
1.3	2024-05-13	Thor Milde

1. Bakgrunn

Hensikten med dokumentet er å ha et sterkt fundament for å kunne ha en robust og sikker DMZ-sone. En DMZ eller demilitarisert sone i datanettverk er et fysisk eller logisk subnet som offentliggjør en organisasjons offentlige tjenere mot internett. Hensikten er å sørge for at en trusselaktør ikke skal få tilgang til hele bedriftens nettverk dersom vedkommende greier å bryte seg inn på server(e) som er tilgjengelig fra internett.

Det vil stilles strenge krav til å kunne publisere tjenester i DMZ. For at tjenester kan publiseres i DMZ skal alle krav være oppfylt. Avdeling sikkerhet er kvalitetssjekker av at kravene har blitt oppfylt. Denne sjekken gjøres når tjenesten er klar til å publiseres i DMZ før man åpner tilgjengelighet fra internett.

Det er tjenesteansvarlig per tjeneste som er ansvarlig for at sikkerhetskravene blir iverksatt og eventuelle avvik blir dokumentert i systemdokumentasjonen. Det betyr ikke at det er tjenesteansvarlig som skal utføre alle disse oppgavene, se kapittel 3. Det er hensiktsmessig å samarbeide med applikasjonsansvarlig når man gjennomgår sikkerhetskravene.

2. Krav

1) Tjenesten skal være risikovurdert og ha løsningsdesign. Løsningsdesign og risikovurdering skal være akseptert av HF og SP.

2) Tjenesten skal ha aktiv forvaltning og tydelig eierskap. Hvem som er systemeier, skal også defineres og verifiseres årlig. Systemeier xxHF, Systemansvarlig xxHF og Tjenesteansvarlig SP.

3) Operativsystem, applikasjonsrammeverk og databaseteknologi som er «end of life» fra produsent tillates ikke. Det skal årlig verifiseres at tjenesten ikke inneholder EOL-komponenter.

4) Tjenestens komponenter skal defineres i UCMDB og IPAM- Disse skal alltid samsvare. UCMDB skal gi treff på den eksternekseponerte IP-adressen til tjenesten samt interne adresser. UCMDB er et oversiktsverktøy som alle tjenester skal være modellert i. IPAM er et verktøy som inneholder IP plan for Helse Sør-Øst, og benyttes til å holde oversikt over alle nettverk som etableres.

5) Alle servere i DMZ skal overvåkes (SCOM/SCCM/utvidet SCOM).

6) Trafikk til tjenesten skal dekrypteres og avtappes i klartekst til Sikkerhetsplattformen i «internettmottaket», eller på annet egnet sted.

7) Alle servere som inngår i tjenesten skal ha installert agent for sårbarhetsscanning, og avrapportering skal verifiseres.

8) Alle servere som inngår i tjenesten skal ha installert agent for sikkerhetsmonitorering, og avrapportering skal verifiseres.

9) Alle servere som inngår i tjenesten skal ha installert agent for skadevarebeskyttelse, og avrapportering skal verifiseres.

10) Dersom trafikken til tjenesten underveis får omskrevet kilde-ip adresse, eksempelvis gjennom reverse proxy, skal det sørges for at "X-Forwarded-For" blir tilført i kommunikasjonen og loggført av applikasjonen og/eller serveren som mottar trafikken.

11) Alle servere som inngår i tjenesten skal ha installert Splunk agent for loggavlevering, samt IIS-logger. Avrapportering skal verifiseres. Hensiktsmessig loggnivå skal være etablert, slik at kravene i «NO-19 - Sikkerhetsprinsipper og -krav for IKT-infrastruktur og applikasjoner», etterfølges for tilstrekkelig sporbarhet og deteksjonsevne. Det må avleveres informasjon om vesentlige tjenestespesifikke logginnslag som skal monitoreres og varsles.

12) Servere skal tillate at sikkerhetspatcher installeres, fortrinnsvis gjennom «autopatch».

13) Applikasjonen skal ha Applikasjonslagpatching.

14) Det skal ikke initieres kommunikasjon fra DMZ inn til foretakenes- eller sentral infrastruktur. Dette gjelder også fra intern DMZ-sone. Avvik fra dette skal risikovurderes individuelt. Om slik trafikk finnes, skal den gjøres leselig og sporbar i Sikkerhetsplattformen.

15) Tjenesten skal stå bak reverse proxy. Servere som står bak reverse proxy skal også etableres i DMZ miljøet.

16) Webapplikasjoner skal ha Web Application Firewall (WAF) implementert.

17) Tjenesten skal ha dokumentert penetrasjonstest og akseptert restrisiko. Aksept skal gis av informasjonssikkerhetsleder SPHF. Ved vesentlige endringer av tjenesten stilles det krav om ny penetrasjonstest av tjenesten. Dette er primært endringer som påvirker sikkerhetsfunksjonalitet, og innføring av nye funksjoner som tidligere sikkerhetsfunksjoner ikke har dekket. Det er Tjenesteansvarlig som bærer ansvaret av dette, Avdeling Sikkerhet kan gi anbefalinger angående behov.

18) Brannmurendringer skal sendes inn av Applikasjonsdrift vha. tjenesteansvarlig og dokumentasjon nevnt ovenfor skal vedlegges i change. Ferdig utfylt NO-47skal også vedlegges aktuell change med kommentarer til hvert enkelt krav.

19) Det er Sykehuspartner HF v/tjenesteansvarlige for DMZ, aktuell tjeneste og avdeling sikkerhet som skal godkjenne at informasjonssystemer kan produksjonsettes i Sykehuspartner HFs DMZ.

3. Fremgangsmåte

Fremgangsmåte er nummerert i henhold til kapittel 2.

1) Informasjon angående risikovurdering og løsningsdesign finnes her
2) Dette skal dokumenteres i risikovurdering/løsningsdesign
3) Definisjoner av EOL-begreper finnes her
4) Rutine for UCMDB-registrering finnes i KM19384. IPAM eies av Datakommunikasjon, ta kontakt med dem, slik at de kan definere tjenesten (se køkoordinator i Aktive Roller)
5) Bestillingsrutine for overvåkning finnes her. Se også sikkerhetsprinsipper om overvåkning punkt 2.3.6.1 – 2.3.6.7
6) Tjenesteansvarlig tar kontakt med Datakom og verifiserer mottak med CERT. Se køkoordinator her. For at bestillingen skal være så komplett som mulig ønsker CERT følgende: Eksponeringspunkt IP, hostname, om det er en IIS-server og når tidspunktet for penetrasjonstesten av tjenesten foregikk (tidspunkt gjelder dersom det er gjort en nyere penetrasjonstest)
7) Tjenesteansvarlig tar kontakt med CERT og verifiserer mottak. Bestillingen gjøres til 765000. Se køkoordinator her
8) Tjenesteansvarlig tar kontakt med CERT og verifiserer mottak. Se køkoordinator her
9) Tjenesteansvarlig tar kontakt med CERT drift og verifiserer mottak. Bestillingen gjøres til 765000. Se køkoordinator her
10) Tjenesteansvarlig tar kontakt med AppDrift AIS og verifiserer mottak. Bestillingen gjøres til 712300. Se køkoordinator her
11) Tjenesteansvarlig tar kontakt med AppDrift AIS og verifiserer mottak. Bestillingen gjøres til 712300. Se køkoordinator her
12) Tjenesteansvarlig tar kontakt med 711500 Operativsystem
13) Se risikovurdering
14) Se løsningsdesign og trafikkinitiering
15) Ta kontakt med Tilgangskontroll 719200
16) Tjenesteansvarlig tar kontakt med Tilgangskontroll og bestiller WAF-oppsett. Bestillingen settes til 719200. Logging fra denne tjenesten må verifiseres ref. punkt 10 og 11
17) Bestilling av penetrasjonstest finnes her
18) Rutine for bestilling av brannmursendringer finnes her

19) Tjenesteansvarlig presenterer nødvendige verifikasjoner til avdeling sikkerhet som godkjenner publisering i DMZ dersom alle krav er oppfylt. Unntak skal være risikovurdert og godkjent

4. Unntak

Dersom tjenesten inneholder avvik fra kravene som er satt, skal disse godkjennes av virksomhetsdirektør for den aktuelle tjenesten. Avvikene skal risikovurderes og dokumenteres i ROS-dokumentet til den aktuelle tjenesten.

5. Kvittering

Krav	**Kommentar TA/AA (Tasknummer, change og andre verifikasjoner eksempelvis e-postvedlegg)**	**Verifisering TA DMZ**
1. Tjenesten skal være risikovurdert og ha løsningsdesign. Løsningsdesign og risikovurdering skal være akseptert av HF og SP.		
2. Tjenesten skal ha aktiv forvaltning og tydelig eierskap. Hvem som er systemeier, skal også defineres og verifiseres årlig. Systemeier xxHF, Systemansvarlig xxHF og Tjenesteansvarlig SP.		
3. Operativsystem, applikasjonsrammeverk og databaseteknologi som er «end of life» fra produsent tillates ikke. Det skal årlig verifiseres at tjenesten ikke inneholder EOL-komponenter.		
4. Tjenestens komponenter skal defineres i UCMDB og IPAM- Disse skal alltid samsvare. UCMDB skal gi treff på den eksterneksponerte IP-adressen til tjenesten samt interne adresser. UCMDB er et oversiktsverktøy som alle tjenester skal være modellert i. IPAM er et verktøy som inneholder IP		

	plan for Helse Sør-Øst, og benyttes til å holde oversikt over alle nettverk som etableres.		
5.	Alle servere i DMZ skal overvåkes (SCOM/SCCM/utvidet SCOM).		
6.	Trafikk til tjenesten skal dekrypteres og avtappes i klartekst til Sikkerhetsplattformen i «internettmottaket», eller på annet egnet sted.		
7.	Alle servere som inngår i tjenesten skal ha installert agent for sårbarhetsscanning, og avrapportering skal verifiseres.		
8.	Alle servere som inngår i tjenesten skal ha installert agent for sikkerhetsmonitorering, og avrapportering skal verifiseres.		
9.	Alle servere som inngår i tjenesten skal ha installert agent for skadevarebeskyttelse, og avrapportering skal verifiseres.		
10.	Dersom trafikken til tjenesten underveis får omskrevet kilde-ip adresse, eksempelvis gjennom reverse proxy, skal det sørges for at "X-Forwarded-For" blir tilført i kommunikasjonen og loggført av applikasjonen og/eller serveren som mottar trafikken.		
11.	Alle servere som inngår i tjenesten skal ha installert Splunk agent for loggavlevering, og avrapportering skal verifiseres. Hensiktsmessig loggnivå skal være etablert, slik at kravene i «NO-19 - Sikkerhetsprinsipper og -krav for IKT-infrastruktur og applikasjoner», etterfølges for tilstrekkelig sporbarhet		

og deteksjonsevne. Det må avleveres informasjon om vesentlige tjenestespesifikke logginnslag som skal monitoreres og varsles.		
12. Servere skal tillate at sikkerhetspatcher installeres, fortrinnsvis gjennom «autopatch».		
13. Applikasjonen skal ha Applikasjonslagspatching.		
14. Det skal ikke initieres kommunikasjon fra DMZ inn til foretakenes- eller sentral infrastruktur. Dette gjelder også fra intern DMZ-sone. Avvik fra dette skal risikovurderes individuelt. Om slik trafikk finnes, skal den gjøres leselig og sporbar i Sikkerhetsplattformen.		
15. Tjenesten skal stå bak reverse proxy. Servere som står bak reverse proxy skal også etableres i DMZ miljøet.		
16. Webapplikasjoner skal ha Web Application Firewall (WAF) implementert.		
17. Tjenesten skal ha dokumentert penetrasjonstest og akseptert restrisiko. Aksept skal gis av informasjonssikkerhetsleder SPHF. Ved vesentlige endringer av tjenesten stilles det krav om ny penetrasjonstest av tjenesten. Dette er primært endringer som påvirker sikkerhetsfunksjonalitet, og innføring av nye funksjoner som tidligere sikkerhetsfunksjoner ikke har dekket. Det er Tjenesteansvarlig som bærer ansvaret av dette, Avdeling Sikkerhet kan gi anbefalinger angående behov.		
18. Brannmurendringer skal sendes inn av		

	Applikasjonsdrift vha. tjenesteansvarlig og dokumentasjon nevnt ovenfor skal vedlegges i change. Ferdig utfylt NO-47 skal også vedlegges aktuell change med kommentarer til hvert enkelt krav.		
19.	Det er Sykehuspartner HF v/tjenesteansvarlige for DMZ, aktuell tjeneste og avdeling sikkerhet som skal godkjenne at informasjonssystemer kan produksjonsettes i Sykehuspartner HFs DMZ.		

6. Referanser

NO-19 - Sikkerhetsprinsipper og krav for IKT-infrastruktur og applikasjoner (sykehuspartner.no)

Regional policy for publiserings- og publikumstjenester og domener (helse-sorost.no)