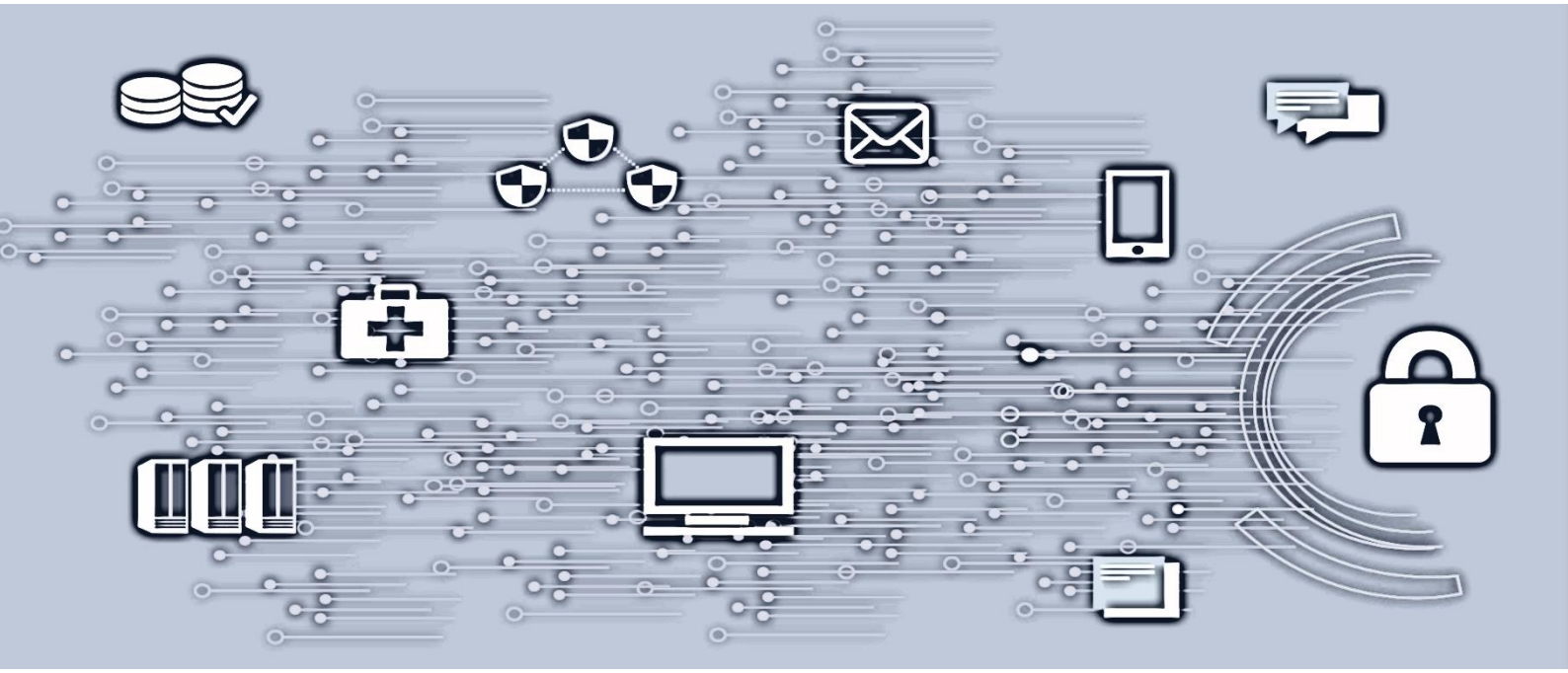
SYKEHUSPARTNER

VPN mv. mot tredjepart



Innhold

Versjon	Dato	Godkjent av
1.0	2014-02-08	Christian Jacobsen
1.1	2015-02-06	Christian Jacobsen
1.2	2022-03-05	Christian Jacobsen

1. Bakgrunn

Sykehuspartner HF mottar ulike henvendelser om nettverksmessig åpning av krypterte forbindelser mot en tredjepart. Henvendelsene kommer både fra ansatte i Sykehuspartner HF og ved helseforetakene. Eksempler på slike henvendelser kan dreie seg om åpning av VPN, SSH eller andre interaktive, krypterte kommunikasjonskanaler mot samarbeidende virksomheter, eller private formål som utdanningsinstitusjoner.

2. Problemstilling

Henvendelsene omhandler en nettverksmessig åpning for å konsumere tjenester hos en tredjepart som på en eller annen måte har kryptert datatransitt, enten med tradisjonell VPN, SSH, proprietære skjermdelingsverktøy eller lignende. Hovedregelen er likevel at det ved slik kommunikasjon opprettes en kryptert tunnel fra den ansattes PC direkte mot tredjepart.

Hensikten med krypteringen er fra leverandøren å ivareta konfidensialitet under datatransitt, men valget av kryptering innebærer også at Sykehuspartner HF mister kontrollen over innholdet i datakommunikasjonen, og mister derfor evnen til nettverksmessig å beskytte mot ondsinnet kode, tilsiktet datainnbrudd eller tilsiktet eller utilsiktet utlevering av informasjon.

Tredjepartsnettverket og dets informasjonssikkerhet vil alltid være en ukjent faktor for oss, uavhengig av hvilket tillitsnivå vi har til eieren.

Likevel vet vi at mange leverandører krever bruk av kryptert transitt for konsumering av deres tjenester, og behovene for konfidensiell kommunikasjon mot tredjepart kan være nødvendig. Eksempelvis tillater vi – og oppfordrer – til bruk av HTTPS som også er en metode for å realisere en kryptert datatransitt mellom intern klient og tredjepart.

Sykehuspartner må derfor legge til rette for en mest mulig balansert sikring.

3. Hovedregel for VPN mv.

Den manglende kontrollen som krypterte tunneler mot en tredjepart utgjør, medfører en negativ endring i risikobildet. På bakgrunn av dette skal slike krypterte forbindelser være stengt.

Hovedregelen er altså at henvendelser om åpning av kryptert tunnel mot tredjepart skal avvises med begrunnelsen gitt i dette dokumentet.

4. Unntak

Unntak skal fremgå av en risikovurdering, som skal aksepteres både av dataansvarlig, og når dette er noen andre enn Sykehuspartner HF, skal Sykehuspartner HF i tråd med oppdraget som ansvarlig for IKT-infrastruktur gjennomføre en uavhengig vurdering og godkjenning av unntaket.

Ved unntak skal det tilrettelegges for trafikk-monitorering, enten ved bruk av dekryptering i brannmur eller på annen hensiktsmessig måte som særskilt avtapping til Sykehuspartner HFs sikkerhetsplattform.