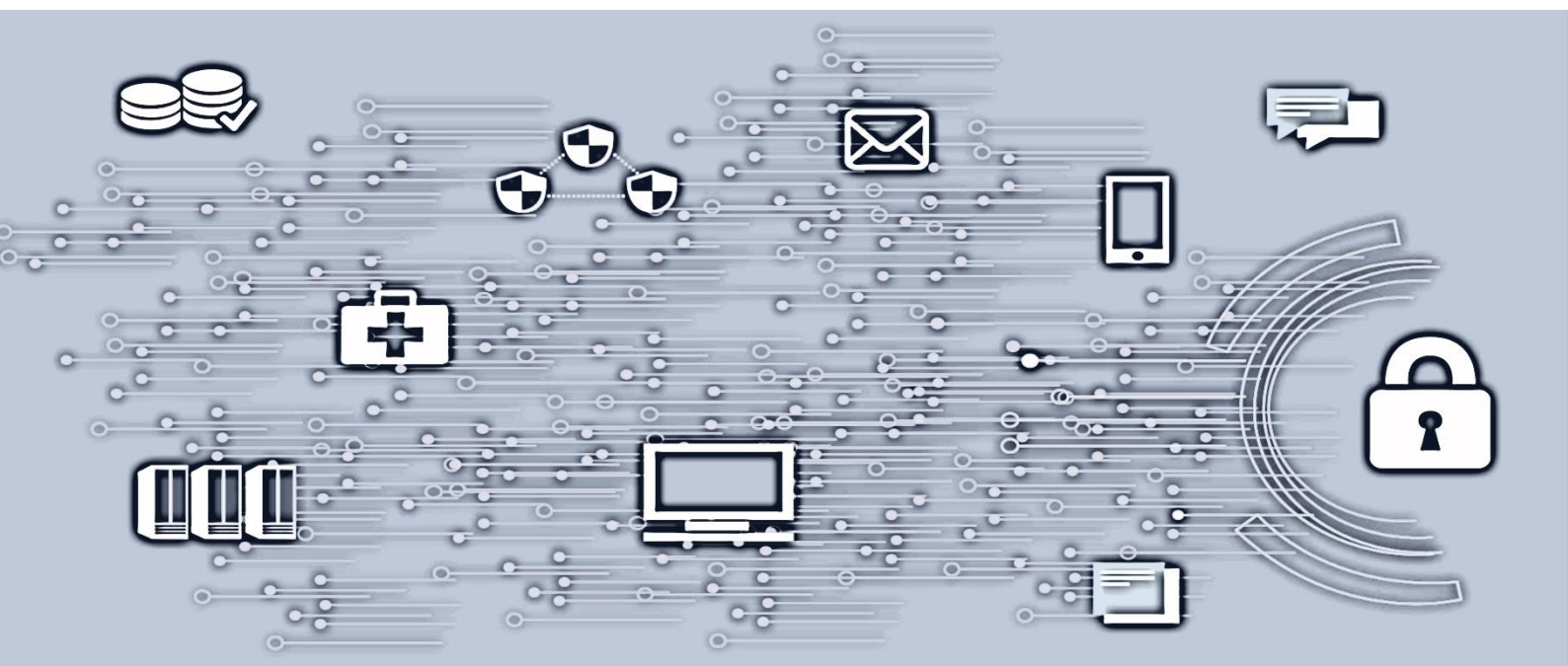


Blokkering av URL-kategorier og dekoding av HTTPS



Innhold

1.	Bakgrunn	3
2.	Teknisk implementering av blokkering og dekoding.....	3
3.	Vurdering av personvern og alternative sikkerhetskontroller.....	5

Versjon	Dato	Godkjent av
1.0	2014-10-03	Christian Jacobsen
1.1	2015-02-06	Christian Jacobsen
1.2	2015-10-08	Christian Jacobsen
1.3	2022-02-24	Christian Jacobsen

1. Bakgrunn

Sykehuspartner HF er gitt ansvar for informasjonssikkerhet i IKT-infrastrukturen, og skal sørge for tilfredsstillende informasjonssikkerhet. Som et ledd i dette, og for å understøtte regionens overordnede sikkerhetsstrategi med fokus på deteksjon, har Sykehuspartner HF implementert teknologi som medfører mulighet for å blokkere tilgang til uønskede nettsider, samt å dekryptere datastrømmer for å gjennomføre sikkerhetsinspeksjon av innholdet, med det uttrykkelige formål å forhindre eller oppklare sikkerhetshendelser.

Sikkerhetstiltaket innebærer at eksterne webserveres digitale sertifikat byttes ut med Sykehuspartner HF's egne sertifikater, og det er disse som presenteres brukeren. Brukeren får da kodet datastrømmen mellom seg selv og sensor, hvor det dekodes for innholdsinspeksjon. Data kodes deretter igjen med den eksterne webserverens digitale sertifikat, og går kodet til opprinnelig mottaker. Datastrømmen er altså kun dekodet på sensoren. Uten denne implementeringen ville det ikke vært mulig å forhindre eller detektere informasjonssikkerhetsbrudd i krypterte datastrømmer.

Når det avdekkes sikkerhetsbrudd, logges et lite sett med dekodet data sammen med IP-adresse, og kan med letthet sammenstilles med andre loggkilder, for å håndtere den uønskede hendelsen.

2. Teknisk implementering av blokkering og dekoding

Dette kapittelet gir en oversikt over de pr. tid gjeldende nettsidekategoriene fra Sykehuspartner HF's applikasjonsbrannmurleverandør, og Sykehuspartner HF's beslutning mht. hvorvidt URL-kategorien er åpen (tillat), blokkert (stengt, unntak må søkes om), og hvorvidt innholdet skal dekrypteres eller ikke.

Kategorier	Status	Skal dekrypteres
Abortion	Åpen	NEI
Abused Drugs	Blokkert	N/A
Adult	Blokkert	N/A
Alcohol and Tobacco	Åpen	JA
Auctions	Åpen	JA
Business and Economy	Åpen	JA
Command and Control	Blokkert	N/A
Computer and Internet Info	Åpen	JA
Content Delivery Networks	Åpen	JA
Copyright Infringement	Blokkert	N/A
Cryptocurrency	Blokkert	N/A
Dating	Åpen	JA
Dynamic DNS	Åpen	JA
Educational Institutions	Åpen	NEI
Entertainment and Arts	Åpen	JA
Extremism	Blokkert	N/A
Financial Services	Åpen	NEI
Gambling	Blokkert	N/A
Games	Blokkert	N/A
Government	Åpen	NEI
Grayware	Blokkert	N/A
Hacking	Blokkert	N/A
Health and Medicine	Åpen	NEI
Home and Garden	Åpen	JA

Hunting and Fishing	Åpen	JA
Insufficient Content	Åpen	JA
Internet Communications and Telephony	Åpen	JA
Internet Portals	Åpen	JA
Job Search	Åpen	JA
Legal	Åpen	JA
Malware	Blokkert	N/A
Military	Åpen	JA
Motor Vehicles	Åpen	JA
Music	Åpen	JA
Newly Registered Domain*	Blokkert	N/A
News	Åpen	JA
Not-resolved	Blokkert	N/A
Nudity	Blokkert	N/A
Online Storage and Backup	Blokkert	N/A
Parked	Blokkert	N/A
Peer-to-Peer	Blokkert	N/A
Personal Sites and Blogs	Åpen	JA
Philosophy and Political Advocacy	Åpen	JA
Phishing	Blokkert	N/A
Private IP Addresses	Åpen	JA
Proxy Avoidance and Anonymizers	Blokkert	N/A
Questionable	Blokkert	N/A
Real Estate	Åpen	JA
Recreation and Hobbies	Åpen	JA
Reference and Research	Åpen	JA
Religion	Åpen	NEI
Search Engines	Åpen	JA
Sex Education	Åpen	JA
Shareware and Freeware	Blokkert	N/A
Shopping	Åpen	JA
Social Networking	Blokkert	N/A
Society	Åpen	JA
Sports	Åpen	JA
Stock Advice and Tools	Åpen	JA
Streaming Media	Åpen	JA
Swimsuits and Intimate Apparel	Åpen	JA
Training and Tools	Åpen	JA
Translation	Åpen	JA
Travel	Åpen	JA
Unknown	Blokkert	N/A
Weapons	Blokkert	N/A
Web Advertisements	Blokkert	N/A
Web Hosting	Åpen	JA
Web-based Email	Blokkert	N/A

3. Vurdering av personvern og alternative sikkerhetskontroller

Arbeidsgiver er pålagt å ivareta tilfredsstillende informasjonssikkerhet, og skal med dette implementere tekniske og organisatoriske sikkerhetstiltak.

Det ligger i krypteringens natur at datastrømmen ikke kan analyseres uten dekoding («dekryptering»). Kryptering benyttes for å bevare konfidensialitet ved å gjøre datastrømmen uleselig for andre enn den opprinnelige mottakeren. Dekodingen omgår dette ved å bytte det digitale sertifikatet, og en datastrøm som før var uleselig, har da blitt leselig. Uten å dekode datastrømmen, er det ikke mulig å inspisere innholdet for ondsinnet kode eller annet uønsket innhold. Det er derfor heller ikke mulig for Sykehuspartner å etablere kompenserende kontroller for å ivareta informasjonssikkerheten.

Det er ikke hensiktsmessig eller ønskelig å stenge for bruk av HTTPS, da dette anses å være nødvendig for å utføre virksomhetsmessig kommunikasjon.

Ansatte i Helse Sør-Øst har mulighet til å bruke arbeidsgivers IKT-utstyr til et begrenset privat omfang. Ansatte kan fritt velge ikke å benytte virksomhetens IKT-utstyr til private formål.

Det er besluttet at dekoding av HTTPS-trafikk er et forholdsmessig tiltak for å balansere virksomhetens behov for kontroll mot den ansattes behov for fortrolighet i e-kommunikasjon. Dette oppnås bl.a. ved at bestemte URL-kategorier som kan anses å være inngripende eller sensitive fra den ansattes perspektiv, unntas fra dekoding.