Riktlinje för hantering av cybersäkerhetsincidenter

Omfattning

Målgrupp för denna riktlinje är Region Västerbottens särskilda sjukvårdsledning (regional särskild sjukvårdsledning-RSSL) som hanterar inträffade cybersäkerhetsincidenter som är av sådan dignitet att de kan orsaka betydande påverkan[1] på hälso- och sjukvården, patientsäkerhet eller generera omfattande ekonomisk skada för regionen.

Även TiB (Tjänsteperson i beredskap) och IT:s insatsledare omfattas av riktlinjen då dessa funktioner ansvarar för den initiala hanteringen av inträffade cybersäkerhetsincidenter och behöver agera före RSSL är etablerad.

Avgränsning

Riktlinjen omfattar inte ett förebyggande arbete inom området IT säkerhet (så som exempelvis det strategiska arbetet med säkerhetsuppdateringar, behörighetsförvaltning) utan avser enbart hanteringen av konstaterade cybersäkerhetsincidenter.

Riktlinjen innehåller inga beskrivningar avseende reservrutiner/avbrottsplaner, det arbetet bedrivs inom ramen för kontinuitetshantering.[2]

Bakgrund

Metoder och verktyg för cyberangrepp utvecklas ständigt och förändras i takt med teknikutvecklingen. Oftast använder sig angriparen av de enklast möjliga tillvägagångssätten för att uppnå önskat resultat. Det finns ett flertal metoder som används vid cyberangrepp exempelvis phising (nätfiske), identitetsstölder, ransomware, angrepp mot mobiler, angrepp mot sakernas internet, angrepp mot publikt exponerade tjänster, så kallade vattenhålsangrepp eller angrepp mot mjukvaruleverantörer. Bland de svenska mål som utsätts för cyberangrepp finns samhällsviktiga verksamheter[3] som är väsentlige för samhällets grundläggande funktionalitet.

Hotbild

De cyberhot som riktas mot Sverige och som utgörs av illvilliga individer och/eller grupperingar är mångfacetterade och kan kopplas till både statliga aktörer och kriminella grupper. Hälso- och sjukvårdssektorn har visat sig vara ett särskilt attraktivt mål för cyberangrepp. Detta då medicinska data är mycket högt värderat och kan användas för utpressning (ransomware). Så som andra sektorer i samhället har även hälso- och sjukvårdssektorn moderniserats med innovativa IT-lösningar såsom

[1] Med betydande påverkan avses incidenter som kan medföra eller medför skador på regionens informationstillgångar (exempelvis kärnsystem för vården eller patientuppgifter) och som inte är ringa i effekt eller i tid.

[2] Kontinuitetshantering handlar om förmågan att upprätthålla verksamhet trots störningar och avbrott, oplanerade och planerade. Genom kontinuitetsplanering/reservrutiner klarar verksamheten av att leverera samhällsviktiga tjänster. Kontinuitetshantering ska genomföras för regionens samhällsviktiga verksamheter.

[3] Samhällsviktig verksamhet omfattar de verksamheter, anläggningar, noder, infrastrukturer och tjänster som är av avgörande betydelse för att upprätthålla viktiga samhällsfunktioner

uppkopplad medicinteknisk utrustning eller olika system med vårdregister som är sammankopplade och uppkopplade till internet. Detta bidrar till en ökad sårbarhet avseende cyberangrepp. Enligt Myndigheten för samhällsskydd och beredskap (MSB) har både offentlig och privat verksamhet i Sverige drabbats av cyberangrepp i synnerhet ransomware-attacker under 2020 dvs under Coronapandemin. När sjukvården är under ett pressat läge, där personalen är hård belastat skulle ett sådant angrepp kunna få omfattande konsekvenser. I detta avseende förtydliga MSB vikten av att hålla fast vi etablerade it-säkerhetsprocesser och rutiner dvs. ett löpande underhåll som är nödvändigt för att skydda systemen.

Syfte

Syftet med riktlinjen är att beskriva de uppgifter som den regionala särskilda sjukvårdsledningen behöver genomföra vid hantering av inträffade cybersäkerhetsincidenter. Åtgärder som beskrivs är av övergripande karaktär, dvs ska tillämpas oavsett typ av cyberangrepp och/eller konsekvenser. Dokumentet ska ge en inriktning vid hantering av konstaterade cybersäkerhetsincidenter.
Riktlinjen ska även vara utgångspunkt vid framtagande av verksamhetsspecifika rutiner och/eller processer inom berörda basenheter.

Lagar och andra krav

Viktiga lagar och föreskrifter kopplat till området:

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8)
- Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
- SOSFS 2013:22 Socialstyrelsens föreskrifter och allmänna råd om katastrofmedicinsk beredskap
- SOSFS 2008:1 Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården

Ansvar och befogenheter

IT Västerbotten

Nödvändiga åtgärder för att minska eller begränsa skada vid inträffat incident. Det kan vara att isolera eller stänga ner funktionalitet, verksamhetssystem eller delar av nätverket. Åtgärder skall skyndsamt meddelas av IT:s insatsledare till TiB eller RSSL om dessa får stor påverkan i regionens kärnverksamhet.

Informationssäkerhetsfunktionen

Informationssäkerhetsfunktionen svarar för Region Västerbottens övergripande Informationssäkerhetsarbete. Informationssäkerhetssamordnaren stöttar verksamheternas arbete under incidenten. Funktionen ansvarar för att informationssäkerhetsincidenter anmäls till tillsynsmyndigheten (CERT).[4]

Teknisk förvaltande verksamheter

Tekniskt förvaltande verksamheter har ett ansvar för att i sina ledningssystem upprätta rutiner för att minska eller begränsa skada, rapportera misstänkta incidenter till IT:s insatsledare, och underlätta insamling av bevis för den teknik som de förvaltar.

Tjänsteperson i beredskap (TiB)

Vid inträffat incident avgör TiB i samråd med IT:s insatsledare om händelsen ska betecknas som en särskild händelse och har mandat att aktivera den särskilda sjukvårdsledningen i adekvat beredskapsläge (för mer information se plan för kris- och katastrofmedicinsk beredskap).

Sjukvårdsledaren inom den särskilda sjukvårdsledningen

Särskild sjukvårdsledning upprättas när incidenten bedöms vara så omfattande eller krävande att regionens resurser måste organiseras, ledas och användas på särskilt sätt. Sjukvårdsledaren i den särskilda sjukvårdsledningen är beslutsfattare och leder insatsen. Medicinsk ansvarig fattar det medicinska inriktningsbeslutet och ansvarar vid behov för medicinska prioriteringar och åtgärder (för mer information se plan för regional kris- och katastrofmedicinsk beredskap).

[4] Incidentrapportering av betydande informationssäkerhetsincidenter beskrivs i särskild rutin.

Beskrivning/Genomförande

Rapportering och eskalering efter behov sker enligt ordinarie rutiner för IT säkerhetsincidenter.

Cybersäkerhetsincidenter ska så långt som möjligt hanteras inom linjeorganisationen dvs. den ordinarie organisationen. När resurserna inte räcker till eller behöver samordnas och inriktas på ett särskilt sätt aktiveras särskild sjukvårdsledning. Incidentens allvarlighetsgrad och dess konsekvenser är avgörande för bedömningen om händelsen bedöms som särskild eller inte.

Oavsett allvarlighetsgrad så ska alltid följande åtgärder vidtas.

Uppgifter/åtgärder

- **Betala aldrig kravet på lösensumma. Det finns inga garantier att system återställs eller filer dekrypteras.**
- Isolera smittade enheter i syfte att hindra att fler verksamheter/system blir utsatta.
- Vid behov beslutar om prioriteringar mellan verksamheter
- Uppmana berörda verksamheter att övergå till reservrutiner/avbrottsplaner för att kunna upprätthålla verksamheten på en tolerabel nivå.
- Cyberangrepp kan pågå under längre tid, beakta därför tidsaspekter och planera för uthållighet.
- Säkerställa och samla in bevis.
- Samordnade kommunikationsinsatser både inom och utanför regionen i lämplig kanal. Observera att sedvanliga kommunikationskanaler så som intranätet, e-post, chefskanalen mm möjligtvis inte kommer vara tillgängliga.
- Beakta eventuell sekretess, exempelvis i kommunikationsinsatser.
- Rapporteringsskyldighet - Anmäl händelsen i ett tidigt skede, tex. Polisanmälan. Incidentrapportering till myndigheter efter bedömning av incidentens art, detta görs enligt NIS-direktivet eller enligt säkerhetsskyddslagen.
- Vid behov kontakta MSB/CERT-SE för stöd i hanteringen.
- Säkerställ i utredningen att angreppet är åtgärdat och att angriparen inte har fortsatt tillgång till IT-miljön genom behörigheter och/eller skadlig kod i systemet. (Knyter an till första punkten)
- Innan återställning av säkerhetskopior sker, säkerställ att kopiorna inte också har drabbats.

Utarbetat av

Verksamhetsrepresentanter krisberedskap, IT, informationssäkerhet, fastighet, CMTS

Referenser och förändringar

Avsnittet placeras sist i dokumentet och hanteras av systemet

Dokumentinformation
Referenser: Nej
Förändringar sedan senaste utgåva: