|  |  |  |
| --- | --- | --- |
| Utfärdad: 30.1.2023 | Träder i kraft:  30.1.2023 | Giltighetstid:  tills vidare |
| Lagstiftning som anvisningen baserar sig på: | | |
| Ändringsuppgifter:  Version 1.0, utfärdad 29.6.2020, träder i kraft 1.7.2020  Version 1.1, utfärdad 1.2.2023   * Kapitel 1–2: Mindre ändringar för att främja förståelsen * Kapitel 3: Uppdaterat för att motsvara lägesbilden för 2022 * Kapitel 3.1: Hänvisningar till bland annat 244 a § i lagen om tjänster inom elektronisk kommunikation, TS50701, Traficoms anvisning om anmälan om störningar i spårtrafiken och Cybermätaren lades till. Beskrivningen av kommande reglering och internationella nätverk för cybersäkerhet i spårtrafiken uppdaterades. * Kapitel 3.2–3.3: Mindre ändringar, ingen väsentlig inverkan på innehållet. * Kapitel 4: För nya OT-system rekommenderas användning av TS50701 och för befintliga system serien IEC 62443. För IT-system rekommenderas i första hand användning av ISO/IEC 27001, alternativ referensram exempelvis Cybermätaren. I ledningssystemet ISO/IEC 27001 kan även OT-miljöer inkluderas genom att man även tillämpar standarder för OT-system. Med ovanstående referensramar kunde punkterna i kapitel 4.1–4.11 i denna rekommendation ersättas till överlappande delar. * Kapitel 4.1–4.11 i rekommendationen uppdaterades för att motsvara åtminstone målnivå 1 enligt Cybermätaren. Tidigare rekommendationer har bevarats till de delar som de motsvarar Cybermätaren. Flera nya rekommendationer lades till. * De hanteringsmetoder som beskrivs i rekommendationen och verktyget Cybermätaren finns som bilagor. | | |

REKOMMENDATION OM FRÄMJANDE AV CYBERSÄKERHET   
I SPÅRTRAFIKEN  
  
Innehåll

**1.** **Rekommendationens syfte och tillämpningsområde** 3

**2. Begrepp inom cybersäkerhet** 3

**3. Cybersäkerhet i spårtrafiken** 5

3.1 Reglering av cybersäkerhet inom spårtrafiken 6

3.1.1 Nuläge 6

3.1.2 Framtiden 6

3.2 Cybersäkerhetshot och -risker i spårtrafiken 7

3.3 Exempel på cybersäkerhetshot och metoder för att hantera dem 9

**4. Rekommendationer om utvecklingen av cybersäkerheten i spårtrafiken** 12

4.1 Cybersäkerhet som en del av säkerhetsledningen och säkerhetskulturen 12

4.2 Skydd av kritiska tjänster 13

4.3 Hantering av egendom, förändringar och konfigurationer 14

4.4 Hantering av hot och sårbarheter 14

4.5 Riskhantering 14

4.6 Identitetshantering och åtkomstkontroll 15

4.7 Lägesbild 15

4.8 Hantering av händelser och störningar samt verksamhetens kontinuitet 16

4.9 Hantering av risker i partnernätverket 16

4.10 Personalledning och -utveckling 17

4.11 Cybersäkerhetsarkitektur 17

4.12 Ökning av samarbete 18

**5.** **Bilagor, ytterligare information och informationskällor** 18

**Tabeller**

1. Viktiga termer som används i rekommendationen (s. 4)

2. Indelningen av cyberrisker inom spårtrafiken i huvudklasser (s. 8)

3. Exempel på cyberhot i spårtrafiken (s. 10)

4. Exempel på granskning av cybersäkerhetshändelser i anknytning till tågföring (s.11)

5. Exempel på granskning av cybersäkerhetshändelser i anknytning till underhåll (s.11)

**Bilagor**

1. Metoder för hantering av cybersäkerheten enligt rekommendationen i tabellformat

2. Version 2.0 av Cybersäkerhetscentrets verktyg Cybermätaren med en hänvisning till denna rekommendation

# **Rekommendationens syfte och tillämpningsområde**

Denna rekommendation syftar till att främja den övergripande utvecklingen av cybersäkerheten inom spårtrafiken och säkerställa verksamhetens kontinuitet. Syftet är att öka:

* spårtrafikaktörernas medvetenhet om cybersäkerhet,
* spårtrafikaktörernas förståelse för cybersäkerhetsrisker och -angrepp,
* spårtrafikaktörernas beredskap och ansvarsfulla skydd mot cyberhot som riktar sig till den egna verksamheten med hjälp av riskhantering och
* samarbetet mellan spårtrafikaktörerna, så att nivån på det totala skyddet av spårtrafiken och dess system kan höjas.

Målet är att främja förmågan för de organisationer och myndigheter som deltar i verksamheten för järnvägssystemet och stadsspårtrafikens system att upptäcka och identifiera olika cybersäkerhetshändelser som påverkar spårtrafiken samt skydda sig mot och återhämta sig från dem så snabbt som möjligt.

Rekommendationen är indelad i två delar. Kapitel 1–3 fungerar som inledning. Syftet med inledningen är att leda läsaren till att främja cybersäkerhet och för honom eller henne åskådliggöra mångfalden av cybersäkerhetshot inom spårtrafiken. I kapitel 4 beskrivs Transport- och kommunikationsverkets rekommendationer till spårtrafikens aktörer om hur de förbereder sig för cybersäkerhetshot och om olika åtgärder för att hantera cybersäkerhetsrisker. Bilagorna till rekommendationen innehåller punkterna i kapitel 4 i tabellformat och syftar till att främja rekommendationens användbarhet.

Rekommendationen är avsedd att fungera som ett konkret hjälpmedel vid utveckling av cybersäkerheten. Hur respektive aktör uppfyller rekommendationerna i kapitel 4 beror därför på såväl arten och omfattningen av aktörens verksamhet som de åtgärder som aktören redan har genomfört för att utveckla cybersäkerheten. Det viktigaste är att varje spårtrafikaktör bearbetar rekommendationerna med den egna verksamheten och verksamhetsmiljön i åtanke.

Rekommendationen är avsedd för både järnvägssystemet och stadsspårtrafikens system. Rekommendationen är i huvudsak utarbetad med tanke på järnvägssystemet, men de begrepp, utmaningar och hanteringsmetoder inom cybersäkerhet som beskrivs i rekommendationen kan mycket väl tillämpas även på stadsspårtrafiken. Exemplen i rekommendationen baserar sig till stor del på järnvägssystemet, men går att använda för att beskriva cybersäkerheten även i stadsspårtrafikens system.

2020 års version av rekommendationen utarbetades som ett tjänstearbete vid Transport- och kommunikationsverket, och i beredningen av den hördes spårtrafikens aktörer. Uppdateringen av rekommendationen år 2022 gjordes likaså som ett tjänstearbete vid Transport- och kommunikationsverket. Uppdateringen av rekommendationen år 2022 kunde kommenteras av utvalda aktörer hösten 2022 och av samtliga aktörer inom spårtrafiken i november 2022.

# **2. Begrepp inom cybersäkerhet**

Termer som rör informations- och cybersäkerhet definieras tämligen uttömmande i den [ordlista om cybersäkerhet](https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf) som Säkerhetskommittén, som verkar i anknytning till försvarsministeriet, har utarbetat. För tydlighetens skull används i denna rekommendation i regel termen cybersäkerhet, trots att det på en del ställen kunde vara ändamålsenligt att hänvisa till informationssäkerhet.[[1]](#footnote-2)

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Sårbarhet** | En sårbarhet kan vara vilken som helst svaghet som möjliggör uppkomst av en skada eller som kan användas för att orsaka en skada. Det kan finnas sårbarheter i operativa system, informationssystem, processer och mänsklig aktivitet. Sårbarheterna kan bero på till exempel processerna, arkitekturen eller planeringen, konfigurationen och underhållet, fysiskt intrång, program- och produktutveckling i ett system, kommunikation och datanät samt brist på övning och medvetenhet. |
| **Cyberhot** | Ett cyberhot avser en orsak till en eventuell icke-önskad skadlig händelse eller utvecklingsgång, som riktar sig till cybermiljön och som när den förverkligas äventyrar funktioner som är beroende av den. Förutom av genomförda informationssäkerhetshot kan cyberhot även orsakas av handlingar som genomförs i digitala kommunikationsmiljöer eller operativa system och som äventyrar samhällets säkerhet. Cyberhot kan komma från inhemska aktörer eller från utlandet. |
| **Cyberrisk** | En cyberrisk avser en kombination av ett hot som utnyttjar en sårbarhet, eventuella händelser och konsekvenser samt sannolikheterna för dem. Riskerna kan hanteras med hjälp av metoder för riskhantering. |
| **Cybermiljö** | En cybermiljö är en verksamhetsmiljö som består av ett eller flera digitala informationssystem. Typiskt för cybermiljöer är lagring, redigering och överföring av data och information med hjälp av kommunikationsnät. Ett typiskt drag för cybermiljöer inom spårtrafiken är dessutom geografisk spridning, styrning av apparater med hjälp av operativa system samt vikten av integriteten för och tillgången till data. Miljön inkluderar även fysiska strukturer för behandling av data och information. |
| **Cyber-** **säkerhet** | Cybersäkerhet är ett måltillstånd där man kan lita på cybermiljön och dess verksamhet säkerställs. Cybersäkerheten omfattar åtgärder genom vilka man proaktivt kan hantera och vid behov tolerera olika slags cyberhot och effekterna av dem. Störningar i cybermiljöns verksamhet orsakas ofta av genomförda informationssäkerhetshot och därför är informationssäkerhet en viktig faktor i strävan efter cybersäkerhet. Förutom med hjälp av informationssäkerhet strävar man efter cybersäkerhet även med hjälp av bland annat åtgärder som syftar till att trygga de funktioner i den fysiska världen som är beroende av den cybermiljö som drabbats av störningar. När man med informationssäkerhet avser tillgänglighet, integritet och konfidentialitet för data, avser cybersäkerhet säkerheten för det digitala och uppkopplade samhället eller den digitala och uppkopplade organisationen och säkerhetens inverkan på dess funktioner. |
| **Informations-** **säkerhet** | Med informationssäkerhet avses arrangemang som syftar till att säkerställa datas tillgänglighet, integritet och konfidentialitet. Tillgänglighet innebär att information kan användas vid önskade tidpunkter. Integritet innebär att informationen stämmer överens med den ursprungliga informationen, och konfidentialitet att ingen obehörig får tillgång till den. Arrangemang för informationssäkerhet är till exempel passerkontroll, låsning av lokaler, säker förvaring och förstörelse av dokument, kryptering och säkerhetskopiering av information samt användning av brandväggar, antivirusprogram och certifikat. Informationssäkerhet omfattar bland annat tryggande av data, apparater, programvaror, datakommunikationen och verksamheten. Med informationssäkerhet och datasäkerhet kan även avses förhållanden där informationssäkerhetsriskerna är under kontroll. |
| **OT, operativ teknik** | Med operativ teknik (OT, operational technology) avses programmerbara digitala system och apparater som interagerar med en fysisk miljö eller som styr apparater som interagerar med en fysisk miljö.  Med hjälp av OT-system hanteras exempelvis infrastruktur i trafiknätet och rullande materiel, såsom trafikering, signalering, kraftkällor, kommunikation och stationsledning. |
| **IT, informationsteknik** | Med informationsteknik (IT, information technology) avses IT-system som stöder affärsverksamheten samt IT-system som stöder operativa system och tillhandahåller en anslutning för de operativa systemen.  Exempel: passagerarinformation, förarens terminalapplikationer, system för uppföljning av transporter, kontrollsystem för trafikledning, allmänt använda metoder för dataöverföring (till exempel WLAN-nät) samt informations- och kommunikationssystem. |

*Tabell 1. Viktiga termer som används i rekommendationen*

# **3. Cybersäkerhet i spårtrafiken**

I och med harmoniseringen och digitaliseringen av det europeiska järnvägssystemet har systemet blivit enhetligare och öppnare, men möjligtvis även med sårbart. Rysslands anfallskrig i Ukraina har bekräftat att järnvägssystemet är en viktig del av den kritiska infrastrukturen i samhället. Under 2022 observerades flera cybersäkerhetsstörningar som riktades mot järnvägssystemet i Ukraina, Belarus och EU-området. Dessa faktorer har lett till ett ökat antal cybersäkerhetsrisker inom spårtrafiken. Förbättringen av spårtrafikens effektivitet bygger i stor utsträckning på digitaliseringen, och uppnåendet av de fördelar som framtidens digitaliseringsmål medför förutsätter en stark basnivå för cybersäkerheten.

Jämfört med järnvägstrafiken är stadsspårtrafikens system klart mer begränsade geografiskt sett. På grund av mängden resenärer och resor kan effekterna av störningar dock ha stor samhällelig betydelse. Även stadsspårtrafikens system har runt om i världen blivit föremål för cybersäkerhetsangrepp med konsekvenser på systemens funktion och driftssäkerhet. Störningar kan även inverka på trafiksäkerheten.

Inom spårtrafiken kan cyberriskerna realiseras på många olika sätt. Cybersäkerhetsrisker kan realiseras oavsiktligt, men även avsiktligt, varvid de som genomför dem kan vara enskilda personer, nätverk, organisationer eller statliga aktörer. För att identifiera hot krävs att alla hotfaktorer beaktas, oavsett om de har orsakats av naturen eller människan, om de är olyckor eller avsiktligt orsakade. En organisation kan bli offer för ett cybersäkerhetsangrepp som är uttryckligen riktat mot den. En organisation kan även bli offer för ett oriktat cybersäkerhetsangrepp om det till exempel finns en sårbarhet i dess system som är lätt att upptäcka och utnyttja. Man vet att oriktade angrepp sker oftare än riktade angrepp, och även ett oriktat angrepp kan vara skadligt för organisationens verksamhet. Källan till ett cybersäkerhetshot, det vill säga den aktör som strävar efter att orsaka skada, kan även vara en annan aktör än den som genomför cybersäkerhetsangreppet. Genomförande aktörer kan finnas både inom organisationen, bland konkurrenter eller underleverantörer och bland kriminella, terrorister eller hackare. Traficoms servicehelhet för spårtrafiken upprätthåller en lägesbild över de cyberstörningar inom spårtrafiken som rapporterats i offentligheten.

Genomförda cybersäkerhetsstörningar kan ha stora negativa effekter på spårtrafiken. Det är sannolikt att cybersäkerhetsstörningarna leder till försämrad tillgång till tjänster, extra arbete och skador på ryktet, men de kan även leda till tillbud och till och med olyckor. I denna rekommendation behandlas cybersäkerhet därför särskilt med tanke på säkerheten i kritiska system.

Eftersom järnvägssystemet i allt högre grad är ett enda enhetligt system, kan en genomförd cybersäkerhetsstörning leda till störningar som påverkar till och med hela systemet och det statliga bannätet. På motsvarande sätt är det möjligt att en cybersäkerhetsstörning helt kan slå ut exempelvis metrotrafikens system. Därför bör cybersäkerheten främjas på ett systembaserat sätt och i samarbete. Endast på så sätt kan man förhindra en situation där ett helt system lider på grund av en sårbarhet i ett enda delområde. Betydande störningar i spårtrafiken kan även ha indirekta effekter på funktionen hos andra trafikformer och annan kritisk samhällsinfrastruktur.

Vid främjande av cybersäkerhet är det viktigt att förstå att cybersäkerheten är en del av säkerheten i spårtrafiksystemet och att den inte ska upplevas eller behandlas som en separat helhet.

Cybersäkerheten i spårtrafiksystemet regleras i NIS-direktivet gällande säkerheten i EU:s nätverks- och informationssystem[[2]](#footnote-3) ([EU:s nätverks- och informationssäkerhetsdirektiv](https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016L1148&from=SV), (EU) 2016/1148). Den regleras dock inte uttömmande i järnvägstrafikens egen EU-reglering och beaktas inte i exempelvis de bedömningskriterier som styr innehållet i järnvägstrafikens säkerhetsledningssystem. Även om järnvägsaktörernas säkerhetsledningssystem baserar sig på EU:s reglering av järnvägarna, rekommenderar man att cybersäkerheten inkluderas i aktörens säkerhetsledningssystem eller system för hantering av säkerheten.

## 3.1 Reglering av cybersäkerhet inom spårtrafiken

### 3.1.1 Nuläge

Utvecklingen av regleringen av cybersäkerheten inom spårtrafiken väntas fortsätta. 169 § i spårtrafiklagen har i över fyra år redan innehållit bestämmelser om skyldigheten att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten. Bestämmelsen gäller tills vidare endast förvaltare av statens bannät och tillhandahållare av trafikledningstjänster. Bakgrunden till den är NIS-direktivet. [244 a § i lagen om tjänster inom elektronisk kommunikation](https://finlex.fi/sv/laki/ajantasa/2014/20140917#O9L29P244a) ålägger de viktigaste aktörerna för spårtrafiksystemet, såsom förvaltare av statens bannät och tillhandahållare av trafikledningstjänster, att under vissa förutsättningar och för ett sådant till ett allmänt kommunikationsnät anslutet separat nät identifiera och dokumentera de kritiska delarna av nätet och de nätverksenheter som används i det samt bedöma hur man försäkrar sig om att användningen av nätverksenheterna inte utgör något hot mot den nationella säkerheten eller försvaret. Bakgrunden till skyldigheten är EU:s 5G toolbox[[3]](#footnote-4) och oron över informationssäkerheten i 5G-nät.

Spårtrafiklagen innehåller även en mer allmän skyldighet att anmäla uppgifter som behövs för att skapa en lägesbild. 172 § i lagen gäller både järnvägsoperatörer, bannätsförvaltare, bolag som tillhandahåller trafikledningstjänster och aktörer som ansvarar för trafikledningen i bannätet för stadsspårtrafiken, vilka utan dröjsmål till Traficom ska anmäla sådana händelser som de fått kännedom om och som kan påverka skapandet av en lägesbild. År 2022 utfärdade Traficom instruktioner för hur man ska förfara i enlighet med paragrafen ([Anvisning om anmälan om störningar i spårtrafiken](https://www.traficom.fi/sites/default/files/media/regulation/H%C3%A4iri%C3%B6ilmoitusohje%20valmis.pdf), på finska). Paragrafen kan anses innehålla även en skyldighet att anmäla cybersäkerhetshot och -störningar. Alla aktörer inom spårtrafiken rekommenderas att inte tveka att anmäla störningar i cybersäkerheten till Cybersäkerhetscentret och servicehelheten Spårtrafik vid Traficom. Det enklaste sättet att anmäla är med följande elektroniska blankett: [https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=sv&RetUrl=https%3A//www.traficom.fi/fi/asioi-kanssamme](https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=sv&amp;amp;RetUrl=https%3A//www.traficom.fi/fi/asioi-kanssamme)

Utöver i spårtrafiklagen beaktas cybersäkerheten även i Traficoms föreskrift om ordnande av beredskapsplanering ([TRAFICOM/308489/03.04.04.00/2019](https://www.traficom.fi/sv/aktuellt/nya-foreskriften-ordnande-av-beredskapsplanering-i-transportsystemet)). Föreskriften förutsätter bland annat att bannätsförvaltare i sin beredskapsplan ska beskriva sin cybermiljö. Föreskriften gäller både förvaltare av statens bannät och förvaltare av ett privat bannät. Dessutom ska förvaltaren av statens bannät och den som tillhandahåller dess trafikledningstjänster beakta vilka händelser och hot som hotar cybermiljön när de beskriver genom vilka förfaranden de säkerställer att järnvägstrafiken sköts i enlighet med beredskapens målnivåer. Föreskriften blev tillämplig den 1 juni 2021 efter en övergångstid. Traficom har med anknytning till föreskriften även utfärdat en anvisning om utarbetande av en beredskapsplan.[[4]](#footnote-5)

### 3.1.2 Framtiden

Regleringen, standardiseringen och instruktionerna beträffande cybersäkerheten inom spårtrafiken utvecklas hos flera olika aktörer. Av den kommande EU-regleringen är det så kallade [NIS2-direktivet](https://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1672915693202&uri=CELEX%3A32022L2555) (EU) 2022/2555 om cybersäkerhet i kritiska tjänster i samhället det viktigaste. Direktivet publicerades den 27 december 2022 och preciserar kraven för hanteringen av cybersäkerhetsrisker i kritiska samhällstjänster. Reformen av NIS2-direktivet gäller även tillverkningssektorn för spårtrafikområdet. År 2022 publicerade standardiseringsorganisationen CENELEC den tekniska specifikationen för cybersäkerhet inom spårtrafiken, [TS50701](https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID5/5/1012872.html.stx). Utifrån den tekniska specifikationen utvecklar standardiseringsorganisationen IEC en internationell cybersäkerhetsstandard för järnvägarna ([IEC:s projektgrupp](https://www.iec.ch/ords/f?p=103:14:319535360914374::::FSP_ORG_ID:28802)). IEC har för avsikt att publicera cybersäkerhetsstandarden för järnvägssystemet den 31 juli 2025. Cybersäkerhetscentret vid Traficom deltar i verksamheten i gruppen för informationsutbyte om cybersäkerheten för Europas järnvägar, [ER-ISAC](https://er.isacs.eu/). ER-ISAC har tillsammans med EU:s cybersäkerhetsbyrå Enisa publicerat en anvisning om tillämpningen av TS50701. Traficom är medlem i Enisas grupp för spårtrafiken, Transport Resilience and Security Expert Group (TRANSSEC). Enisa har årligen publicerat utredningar om cybersäkerheten i spårtrafiksystemet. Därtill deltar Traficom och Polisstyrelsen i säkerhetsgrupperna Expert Group on Land Transport Security (Landsec) och Rail Passanger Security Platform (Railsec) för landtrafiken och järnvägarna som lyder under EU-kommissionen. I grupperna delar man information om cybersäkerheten inom spårtrafiken och utarbetar rekommendationer. Alla aktörer inom spårtrafiken har möjlighet att påverka utvecklingen av cybersäkerheten inom sektorn. Trafikledsverket är medlem i den internationella järnvägsunionen UIC, som haft som mål att aktivera sin cybersäkerhetsgrupp i slutet av 2022. UIC deltog i projektet CYRAIL, som 2018 publicerade en cybersäkerhets[rekommendation](https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf) om ledning och signalering. Trafikledsverket är även medlem i European Rail Infrastructure Managers (EIM) cybersäkerhetsgrupp och i arbetsgruppen för cybersäkerhet inom användargruppen (EUG) av det europeiska trafikstyrningssystemet för järnväg (ERMTS). EUG utreder exempelvis hanteringen av certifikat i nyckelhanteringssystemet ERTMS online. Därtill ska statsrådets principbeslut om förbättring av informationssäkerheten och dataskyddet inom kritiska samhällssektorer beaktas. Genomförande av åtgärderna i beslutet skulle ålägga aktörer att bland annat definiera kritiska data- och datakommunikationstekniska funktioner samt använda ISO 27001-certifiering.[[5]](#footnote-6)

Även Europeiska unionens järnvägsbyrå har redan vidtagit åtgärder som behövs för att reglera cybersäkerheten inom järnvägssektorn. Arbetet omfattar till att börja med utveckling av en tredje nivå (L3) i det europeiska trafikstyrningssystemet för järnväg ERTMS (European Rail Traffic Management System). I arbetet beaktas även resultaten av Shif2Rail-konsortiets projekt. Europeiska unionens järnvägsbyrå har för avsikt att i större utsträckning framöver inkludera cybersäkerhet i ramverket för den europeiska spårtrafiksregleringen och att i arbetet beakta bland annat CENELEC:s specifikation TS50701 railway applications – Cybersecurity.

Cybersäkerhetens allt större betydelse i EU-regleringen av spårtrafiken torde under de närmaste åren påverka hanteringen av cybersäkerhetsfrågor som rör järnvägssystemet. Beträffande stadsspårtrafiken är däremot inga motsvarande förändringar att vänta, varför hanteringen av cybersäkerhetsfrågor som rör stadsspårtrafikens system även framöver torde bli kvar inom den nationella styrningen.

## 3.2 Cybersäkerhetshot och -risker i spårtrafiken

Det viktigaste i fråga om cybersäkerhet är att hantera cybersäkerhetsriskerna. Sårbarheter och deras effekter kan hanteras och minskas genom att man identifierar och åtgärdar dem. Förekomsten av en sårbarhet leder dock inte automatiskt till en skada, utan skadan uppkommer först när det hot som utnyttjar sårbarheten realiseras. Om sårbarheten inte är förknippad med något hot om utnyttjande förutsätter den inte nödvändigtvis att man tar till någon hanteringsmetod, men den borde ändå identifieras och följas upp, så att eventuella förändringar kan upptäckas. Ett hot innebär något som kan orsaka en eventuell icke-önskad skadlig händelse, och hot kan hanteras genom att bedöma vilka risker de utgör. Risker i sin tur kan hanteras med hjälp av metoder för riskhantering.

Med hantering av cyberrisker avses identifiering och bedömning av risker samt val, utveckling och genomförande av alternativ för att hantera riskerna. Riskhantering gäller alla eventuella risker för organisationen och reaktionerna på dem. Cybersäkerhetsrisker ingår i helheten riskhantering. Riskhanteringen som helhet är en systematisk och fortgående tankeprocess, som återspeglar organisationens värden och består av, förutom identifiering, hantering och bedömning, även kontinuerlig samordning, undersökning av riskernas utveckling, omvärdering av riskerna, korrigerande åtgärder, kommunikation och rapportering. I synnerhet ur riskhanteringens perspektiv är cyberrisker förknippade med tidlöshet, rumslöshet och svårigheten att beräkna skadeersättningar.

Cyberrisker kan delas in i fyra huvudkategorier: mänsklig aktivitet, systemstörningar och tekniska fel, misslyckade interna processer samt externa händelser. Huvudkategorierna i sin tur kan delas in i underkategorier, som åskådliggör de operationella åtgärder som orsakar riskerna. Med tanke på cyberriskerna som helhet är det viktigt att tänka på att cyberrisker ofta korrelerar med varandra och att en risk när den realiseras kan orsaka en serie händelser som utlöser flera risker.[[6]](#footnote-7)

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Mänsklig aktivitet | 2. Systemstörningar och -fel | 3. Misslyckade interna funktioner | 4. Externa händelser |
| 1.1 Oavsiktlighet  Skador Fel Försummelser | 2.1 Utrustning  Kapacitet Prestanda Underhåll Obsolescens | 3.1 Planering och genomförande av verksamheten  Funktionens förlopp Dokumentering av funktionen Roller och ansvar Anmälningar och larm Informationsflöde Växande problem Serviceavtal Överföring av uppgifter | 4.1 Katastrofer  Väderfenomen Bränder Översvämningar Jordbävningar Oroligheter Olyckor Pandemier |
| 1.2 Avsiktlighet  Bedrägerier Sabotage Stölder Vandalism | 2.2 Programvara  Förenlighet Hantering av konfigurationen Hantering av förändringar  Säkerhetsinställningar Programmeringspraxis Testning | 3.2 Övervakning av  verksamheten  Övervakning av verksamhetsmiljön Indikatorer Regelbunden egenkontroll Verksamhetens ägarskap | 4.2 Lagstiftningsmässiga problem  Efterlevnad av reglering Regleringens funktion Rättegångar |
| 1.3 Bristande funktion  Färdigheter Kunskaper Ledning Tillgänglighet | 2.3 System  Planering Tekniska krav Integration Komplexitet | 3.3 Stödfunktioner  Personalförvaltning Finansiering Utvecklings- och utbildningsverksamhet Anskaffning | 4.3 Problem i affärsverksamheten  Störningar hos underleverantörer Marknadsförhållanden Ekonomisk situation |
|  |  |  | 4.4 Beroendeförhållanden  El-, vatten- och telekommunikationsnät Räddningsväsendet Reservkraft Transport |

*Tabell 2. Indelningen av cyberrisker inom spårtrafiken i huvudklasser. Bygger på Cebula & Youngs verk (2010).*

Cyberrisker kan i vidare bemärkelse betraktas som operationella risker som rör information och teknologi och som påverkar konfidentialiteten, tillgängligheten eller integriteten för information eller ett system. En cyberrisk anses därför omfatta alla de risker som leder till ekonomisk förlust, avbrott i verksamheten eller att organisationens anseende skadas eller som påverkar organisationens konkreta verksamhet. När en cyberrisk realiseras kan skadorna i värsta fall vara ekonomiskt och mänskligt sett omfattande.

För såväl järnvägssystemets som stadsspårtrafikens del består cybermiljön för spårtrafiken av två separata helheter: informationssystemen och de operativa systemen. Informationssystem och operativa system länkas i allt högre grad till varandra, vilket ställer nya krav på hanteringen av cyberrisker. Traditionellt har cybersäkerhet beaktats i större utsträckning i informationssystem, och först under de senaste åren har man allt mer fått upp ögonen för cybersäkerhetsfrågor i operativa system. Även de tekniska lösningarna i OT-system börjar numera närma sig de tekniska lösningarna i IT-system.

En lång livslängd på de system som används och delvis även systemens åldrande är karakteristiskt för spårtrafiken. Vissa delar av systemen har använts i årtionden, medan andra har förbättrats längs vägen, vilket gör systemen både utmanande och sårbara med tanke på cybersäkerheten. Det faktum att beaktandet av cybersäkerhet ökar i så långsam takt på den operativa sidan och den geografiska spridningen ökar spårtrafikens mottaglighet för cyberhot. I hanteringen av cyberrisker är det viktigt att utveckla samarbetet mellan informationssystemens och de operativa systemens aktörer. Dessutom är det viktigt att ägna uppmärksamhet åt att skydda systemen, skydda den information och de data som finns i systemen samt sörja för säkerheten för datakommunikationen i och mellan systemen.

Det som gör hanteringen av cybersäkerhetsrisker utmanande är att mängden cybersäkerhetsrisker ökar och att riskerna blir mångsidigare i takt med att spårtrafikens funktioner och system utvecklas och digitaliseras. En fullständig säkring av den digitala världen är däremot omöjlig, varför uppmärksamhet bör ägnas även åt exempelvis organisationens mognad att upptäcka cybersäkerhetshot.

Uppmärksamhet bör ägnas åt identifiering och avvärjning av cyberhot både när befintliga system uppdateras och i nya system med början från planeringsfasen. Beställar- och aktörsorganisationer har ett stort ansvar i förverkligandet av cybersäkerheten. I synnerhet innan ändrade eller nya system tas i bruk är det viktigt att konstatera att systemen också är cybersäkra och att användarna av dem har rutiner för att sörja för cybersäkerheten under systemens hela livscykel. Eftersom många leveransavtal inom spårtrafiken är långa och många av dem har upprättats i en tid då man inte fokuserade på cybersäkerhetsfrågor, är det viktigt att komma överens om kraven på cybersäkerhet även när gamla avtal uppdateras eller förnyas.

## 3.3 Exempel på cybersäkerhetshot och metoder för att hantera dem

I följande tabell beskrivs olika typer av cyberrisker som kan rikta sig mot spårtrafiken och som spårtrafikaktörerna ska beakta i riskhanteringen. Cyberriskerna i tabellen är dock endast exempel, och varje spårtrafikaktör bör på egen hand bedöma de cyberrisker som hänför sig till den egna verksamheten och vilka kritiska system som bör beaktas i utvecklandet av cybersäkerheten.

|  |  |  |
| --- | --- | --- |
| **Cyberrisk** | **Exempel (hot)** | **Aktörer som hotet gäller** |
| **Risker som hänför sig till datorställverksutrustning** | Dataöverföringen från trafikledningen bryts och kommandona förmedlas inte på önskat sätt till datorställverksutrustningen exempelvis på grund av en kabel som gått av i samband med banarbeten. | Trafikledningen, bannätsförvaltare, järnvägsoperatörer |
| **Risker i gränssnitten mellan trafikledningssystem och ställverk** | Ett avbrott eller en störning i dataöverföringen mellan datorerna och de reläställverk som de styr. | Trafikledningen, bannätsförvaltare, järnvägsoperatörer |
| **Risker i gränssnitten mellan trafikledningssystem och datorställverk** | Kommandona i det fjärrstyrningssystem som trafikledaren använder förmedlas inte korrekt till datorställverket. | Trafikledningen, bannätsförvaltare, järnvägsoperatörer |
| **Risker som hänför sig till integriteten och tillförlitligheten hos information i trafikledningssystem** | Informationsinnehållet som används faller sönder på grund av exempelvis en hackers åtgärder så att man inte kan lita på eller använda informationen i systemen. | Trafikledningen, bannätsförvaltare, järnvägsoperatörer |
| **Risker i trafikledningssystem som baserar sig på källkod** | En skadlig kod laddas upp i källkoden och kommer in i trafikledningssystemet samt aktiveras till exempel i samband med att systemet uppdateras. | Trafikledningen, bannätsförvaltare, järnvägsoperatörer |
| **Risker som hänför sig till anslutningen av trafikledningssystem till det allmänna nätet** | Icke önskade uppdateringar eller konfigurationsändringar i systemen görs avsiktligt via det allmänna nätet eller så bryts kontakten till det allmänna nätet. | Trafikledningen, bannätsförvaltare, järnvägsoperatörer |
| **Risker som hänför sig till gränssnitt för sammankoppling av IT- och OT-system samt anslutning till det allmänna nätet** | IT- och OT-system kopplas till varandra och till det allmänna nätet, varvid OT-systemens integritet kan äventyras. | Trafikledningen, bannätsförvaltare, järnvägsoperatörer |
| **Risker som hänför sig till tryggandet av elförsörjningen** | En störning inträffar i stamnätet som hindrar elöverföringen till matningsstationer eller från en matningsstation till bannätet, eller så gör någon olagligt intrång i övervakningssystemen för elektrifierade järnvägar. | Bannätsförvaltare, trafikledningen |
| **Risker som hänför sig till telematiska**  **system** | Någon kommer åt att avsiktligt störa utrop eller informationsskärmar. | Bannätsförvaltare, järnvägsoperatörer |
| **Risker som hänför sig till komponenter** | I en komponent (till exempel ett microchip eller en telefon) inkluderas avsiktligt en faktor som orsakar störningar även utanför komponenten. | Trafikledningen, järnvägsoperatörer (materiel) |
| **Risker som hänför sig till apparaters interoperabilitet** | Kompatibiliteten mellan anordningar för passerkontroll störs på grund av till exempel programvaruuppdateringar eller dåligt planerade utvecklingsprojekt. | Trafikledningen, bannätsförvaltare, järnvägsoperatörer |
| **Cyberrisker som hänför sig till rullande materiel** | Passerkontroll för rullande materiel eller andra funktioner störs så att det inte är säkert att använda materielen. | Järnvägsoperatörer, underhållare av materiel |
| **Kapning av system** | Systemens funktion störs eller måste avbrytas till följd av en kapning för att säkerheten ska kunna säkerställas. | Alla aktörer inom spårtrafiken |
| **Risker som beror på personalen** | En anställd eller någon som tidigare varit anställd orsakar antingen avsiktligt eller av okunnighet störningar i systemen. I synnerhet farliga kombinationer av arbetsuppgifter. | Alla aktörer inom spårtrafiken |
| **Risker som beror på underleverantörer** | Samma som ovan, men aktören är en underleverantör. | Alla spårtrafikaktörer som använder sig av underleverantörer |
| **Risker som beror på**  **tjänsternas användare** | Samma som ovan, men aktören är användaren av tjänsten. | Alla spårtrafikaktörer som tillhandahåller tjänster |

*Tabell 3. Exempel på cyberhot i spårtrafiken*

Vid en detaljerad granskning och analys av cybersäkerhetsscenarion kan till exempel en så kallad bow tie-analys användas.[[7]](#footnote-8) Följande tabell visar exempel på enskilda cybersäkerhetshändelser som bearbetats med hjälp av en bow tie-analys. Samtidigt fungerar tabellerna som exempel på funktioner som kan orsaka en cybersäkerhetshändelse, för hur man redan i förväg kan skydda sig mot händelserna och, om en händelse inträffar trots skyddet, på vilka dess återställande skydd samt konsekvenser är.

Exemplen har utarbetats i en cybersäkerhetsworkshop för spårtrafiken som Traficom ordnade den 11 mars 2020, där man testade om bow tie-modellen kunde vara till nytta vid närmare granskning av cybersäkerhetshändelser och för att förstå vilka alla beroendeförhållanden som kan anknyta till en enskild händelse.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TÅGFÖRING** | | | | | |
| **Funktion** | **Utlösande faktor** | **Händelse/tillbud** | **Hindrande eller förebyggande skydd** | **Återställande**  **skydd** | **Händelsens**  **konsekvenser** |
| Fysiskt skydd | Intrång i utrymmen för säkerhetsanordningar | Fjärrstyrningen lamslås | Övningar, utbildningar, revisioner | Användning av backuppsystem,  trafiken stoppas eller  begränsas | Tågföringen  förhindras |
| Skydd | Hackning via nätet |
| Skydd | Skadlig programvara | Olycka |
| Backupsystem | Backuppsystemet kraschar |

*Tabell 4. Exempel på granskning av cybersäkerhetshändelser i anknytning till tågföring*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UNDERHÅLL** | | | | | |
| **Funktion** | **Utlösande faktor** | **Händelse/tillbud** | **Hindrande eller förebyggande skydd** | **Återställande**  **skydd** | **Händelsens**  **konsekvenser** |
| Avtalsmässigt problem | Bristfälligt underleverantörsavtal | En underleverantör påverkar systemet i samband med underhåll | God beredning samt uppdatering av avtalet vid behov, kompetenta avtalsförhandlare | Det som orsakat skadan och orsaken till den avlägsnas och isoleras, backupsystemen i ordning, ansvaren och arbetsbeskrivningarna i ordning, snabb reaktion på felet, kommunikationsfärdigheterna i ordning | Systemet  lamslås |
| Avtalsmässigt problem | Avtalsbrott | Avtalspåföljderna i ordning, övervakning, sekretessavtal |
| Onda avsikter | Avsiktlighet från den som utför arbetet | Utredning av tjänsteleverantörens bakgrund, tidigare referenser, avtalsbestämmelser, tjänstebeskrivningarna i ordning, regelbundna kontroller | Olycka eller tillbud |
| Brister i  övervakningen | Ingen övervakning av underleverantörer, övervakningen fungerar inte | Fördelning av  ansvaret för övervakningen | Skador på ryktet |

*Tabell 5. Exempel på granskning av cybersäkerhetshändelser i anknytning till underhåll*

# **4. Rekommendationer om utvecklingen av cybersäkerheten i spårtrafiken**

Detta kapitel innehåller en sammanställning av Transport- och kommunikationsverkets rekommendationer för utveckling av cybersäkerheten. Rekommendationerna presenteras även i tabellformat i en separat bilaga. Genom hurdana åtgärder respektive aktör borde försöka uppfylla de givna rekommendationerna beror på arten och omfattningen av spårtrafikaktörens verksamhet.

Transport- och kommunikationsverket rekommenderar att man i nya delar av operativ teknik (OT) i spårtrafiksystemet tillämpar den tekniska specifikationen TS50701 Railway Applications – Cybersecurity och senare den standard som utvecklas utifrån specifikationen. Ämbetsverket rekommenderar att man beträffande befintliga OT-system fortsätter att följa standardserien IEC 62443 avsedd för säkerhet inom industriautomation om systemen har utvecklats utifrån den.

Alla aktörer inom spårtrafiksystemet rekommenderas att bedöma och mäta nivån på sin organisations cybersäkerhet. Beträffande befintliga administrativa IT-system rekommenderas i första hand tillämpning av ledningssystemstandarden för cybersäkerhet ISO/IEC 27001:2022[[8]](#footnote-9). Med hjälp av ledningssystemet för informationssäkerhet ISO/IEC 27001 är det möjligt att även administrera OT-miljöer, på vilka man dessutom tillämpar ovan nämnda standarder för OT-miljöer.[[9]](#footnote-10) En annan alternativ referensram kan vara exempelvis den avgiftsfria och svenskspråkiga [Cybermätaren](https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren)[[10]](#footnote-11), som upprätthålls av Cybersäkerhetscentret. När Cybermätaren används som referensram rekommenderas alla spårtrafikaktörer att nå målnivå 1. Tillhandahållare av kritiska tjänster i spårtrafiksystemet (NIS-aktörer) rekommenderas att nå målnivå 2. Som bilaga till denna rekommendation finns version 2.0 av bedömningsverktyget Cybermätaren, som innehåller hänvisningar till rekommendationerna i kapitel 4.1–4.11.

Genom att tillämpa ovanstående referensramar kan rekommendationerna i kapitel 4.1–4.11 nedan ersättas till de delar som kraven enligt den valda referensramen är minst lika krävande. Kapitel 4.12 i denna rekommendation beskriver ökning av samarbetet inom spårtrafiksystemet. I sammanställningen av kapitel 4.1–4.11 i rekommendationen har målnivå 1 i Cybermätaren tillämpats, men några av punkterna ställer högre krav än målnivå 1. Cybermätaren bygger på referensramarna för cybersäkerhet NIST Cybersecurity Framework och Cybersecurity Capability Maturity Model (C2M2), som även den tidigare rekommendationen om främjande av cybersäkerhet inom spårtrafiken baserade sig på och som uppdaterats genom denna rekommendation. Även de arkitektoniska ramarna för digital säkerhet ([DTARK](https://wiki.dvv.fi/display/DTARK/)), som Myndigheten för digitalisering och befolkningsdata (MDB) publicerat, bygger på ramverket NIST Cybersecurity Framework. DTARK lämpar sig väl för planering av cybersäkerheten, men ramverket är inte i första hand avsett för bedömning och mätning av nivån på cybersäkerheten.

## 4.1 Cybersäkerhet som en del av säkerhetsledningen och säkerhetskulturen

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna inkluderar ledning av cybersäkerhet i sitt säkerhetsledningssystem eller säkerhetshanteringssystem, eller, om inget av dessa finns, i det allmänna ledningssystemet. Cybersäkerheten främjas i så stor utsträckning som möjligt med hjälp av verksamhetsmodeller som är en viktig del av utvecklingen av den övriga verksamheten (riskbedömning, egenkontroll och så vidare). För detta ändamål ska aktörerna:

* Definiera en cybersäkerhetsstrategi till exempel som en del av säkerhetsledningssystemet samt säkerställa stödet från organisationens ledning och styrelse eller ledningsgrupp för att genomföra målen i enlighet med cybersäkerhetsstrategin.
  + Cybersäkerhetsstrategin ska inkludera åtminstone en lista över cybersäkerhetsmålen och en plan för genomförandet av dem.
  + Dokumentera cybersäkerhetsstrategin och -målen. Strategin och målen ska vara i linje med organisationens allmänna mål och riskerna för kritisk infrastruktur.
* Beakta cybersäkerheten i planer som rör verksamhetens kontinuitet och se till att cybersäkerhetsstrategin och planerna för verksamhetens kontinuitet är sammanjämkade med varandra.
* Anvisa resurser (personer, finansiering och verktyg) för att starta cybersäkerhetshanteringen.
* Definiera och dokumentera ansvaren och samarbetsmodellerna i fråga om cybersäkerheten så att de omfattar organisationen och övriga aktörer med anknytning till verksamheten, med hänsyn till att cybersäkerheten inom spårtrafiksystemet är en heltäckande kedja som löper genom infrastruktur som ägs av flera olika aktörer.

## 4.2 Skydd av kritiska tjänster

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna erkänner sin roll i logistikkedjan, som är en samhällskritisk tjänst, och hanterar riskerna enligt den. Kritiska tjänster och deras beroendeförhållanden ska identifieras och hanteras samt effekterna av cyberstörningar minimeras. För detta ändamål ska aktörerna:

* Definiera och dokumentera tjänster som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet.
* Definiera och dokumentera data som behövs för produktionen av tjänster som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet.
* Definiera och dokumentera processer som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet.
* Definiera och dokumentera objekt att skydda, det vill säga informationssystem som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet samt operativa system och data, såsom trafikledningssystem inklusive funktioner.
* Definiera och dokumentera system och funktioner som är väsentliga med tanke på lägesbilden och övervakningen av kritiska system, tjänster och apparater.
* I organisationens säkerhetshantering och policyer införliva alla resurser som behövs för produktionen av de tjänster som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet (data, processer, lokaler, apparater och leveranskedjor).
* I organisationens policyer för riskhantering införliva alla resurser som behövs för produktionen av de tjänster som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet (data, processer, lokaler, apparater och leveranskedjor).
* Göra upp en plan för hanteringen av cybersäkerhetshändelser och -störningar som omfattar alla tjänster som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet.
  + Planen är omfattande och innehåller en beskrivning av sannolika verkningar av kända angreppsmetoder.
  + Personal som deltar i hanteringen av cybersäkerhetshändelser och -störningar har tillägnat sig och förstår hanteringsplanen.
  + Planen har dokumenterats och delats ut till alla relevanta berörda parter.

## 4.3 Hantering av egendom, förändringar och konfigurationer

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna har kontroll över sin IT- och OT-egendom. Med egendom avses apparater, programvaror och information som är viktiga med tanke på funktionerna. För detta ändamål ska aktörerna:

* Upprätta ett register över apparater och programvaror som är viktiga med tanke på spårtrafikens kontinuitet och säkerhet.
* Upprätta ett register över informationsresurser som är viktiga med tanke på spårtrafikens kontinuitet och säkerhet, till exempel aktörers kapacitetshantering och kunduppgifter som hänför sig till branschen samt standardinställningar för apparater och programvaror.
* Skapa etablerade standardinställningar för konfigurationerna av apparater, programvaror och informationsresurser.
* Utvärdera och inhämta godkännande av ändringar i registrerade apparater, programvaror och informationsresurser innan de genomförs.
  + Föra loggar över ändringar i registrerade apparater, programvaror och informationsresurser.
* Skapa metoder för att hålla fasta programvaror uppdaterade (till exempel programuppdateringar).
* Skapa metoder för fjärrövervakning, -administration och -uppdatering av kritiska apparater.

## 4.4 Hantering av hot och sårbarheter

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna fastställer rutiner för att upptäcka, identifiera, analysera och hantera cybersäkerhetshot och sårbarheter samt svara på dem genom att beakta hoten mot spårtrafikens kontinuitet och säkerhet. För detta ändamål ska aktörerna:

* Identifiera lämpliga informationskällor för identifiering av sårbarheter.
  + Samla in och tolka uppgifter om sårbarheter för verksamheten.
  + Genomföra sårbarhetsbedömningar.
  + Ingripa i sårbarheter som är av betydelse för verksamheten genom att till exempel öka övervakningen eller installera korrigerande uppdateringar.
  + Med hjälp av sårbarhetsbedömningar ta reda på vilka områden i de system som används som är mottagliga för cybersäkerhetsangrepp med beaktande av bland annat systemens gränssnitt och beroendeförhållanden.
* Identifiera lämpliga informationskällor för identifiering av hot.
  + Samla in och tolka uppgifter om hot för verksamheten.
  + Ingripa i hot som är av betydelse för verksamheten genom att till exempel öka övervakningen eller följa hotens utveckling.
    - Med riskbaserad rättidighet följa och övervaka cybersäkerhetshot och hanteringen av dem i operativa system och informationssystem, så att man kan reagera på dem i ett så tidigt skede som möjligt.
  + Sörja för skyddet av objekt som hänför sig till rutiner, system och människor och som är utsatta för cybersäkerhetshot under hela deras livscykel.
  + Beakta observerade cybersäkerhetshot under systemens hela livscykel, med början från fastställandet av kraven när anskaffningen av systemen planeras.

## 4.5 Riskhantering

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna upprättar ett riskhanteringssystem som omfattar hela organisationen för att möjliggöra identifiering, analys och minskning av cybersäkerhetsrisker samt uppföljning av dem med beaktande av affärsenheter, dotterbolag, sammanlänkade infrastrukturer och övriga intressenter i relation till riskerna för spårtrafikens kontinuitet och säkerhet. För detta ändamål ska aktörerna:

* Systematiskt leda riskhanteringen i fråga om cybersäkerhet.
* Identifiera cybersäkerhetsrisker genom att kartlägga risker mot rutiner, system och människor samt utnyttja kontinuerlig riskbedömning.
* Prioritera cybersäkerhetsriskerna på basis av deras beräknade effekter.
* Reagera på cybersäkerhetsriskerna och cybersäkerhetsriskkategorierna genom att till exempel minska, godkänna, undvika eller överföra dem.
* Komma överens om godtagbara risknivåer och fastställa genom vilka åtgärder organisationen ska skyddas och vilka åtgärder som vid ett eventuellt angrepp ska vidtas för att upptäcka, analysera och avvärja angreppet samt återställa verksamheten efter angreppet.
* Beakta cybersäkerhetsriskerna när beslut fattas.
  + Beakta observerade cybersäkerhetsrisker under systemens hela livscykel, med början från fastställandet av kraven när anskaffningen av systemen planeras.
  + Planera livscykelhanteringen av systemen som helhet och säkerställa att eventuella kvarstående risker godkänns på ett kontrollerat och medvetet sätt.

## 4.6 Identitetshantering och åtkomstkontroll

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna fastställer rutiner för hantering av användarbehörigheter och åtkomstkontroll beträffande fysiska lokaler, informationssystem och operativa system med beaktande av interna och externa personer, men även andra aktörer (apparater, system och programvaruprocesser) genom att ägna särskild uppmärksamhet åt fjärranslutningar. För detta ändamål ska aktörerna:

* Anvisa separata identiteter för arbetstagare och andra enheter (såsom processer och apparater som behöver åtkomst till apparater, programvaror och informationsresurser som hör till funktionerna) samt bedöma de anvisade identiteternas nödvändighet.
  + Dela ut uppgifter om åtkomstbehörigheter såsom lösenord, smartkort eller nycklar till arbetstagare och andra enheter.
  + Ta identiteterna ur bruk när de inte längre behövs.
* Använda metoder för tillsyn av hanteringen av logiska användningsrättigheter (i datasystem).
  + Ta bort rättigheterna när de inte längre behövs.
* Använda metoder för övervakning av den fysiska åtkomstkontrollen (till exempel stängsel, lås eller skyltar).
  + Ta bort åtkomsträttigheterna när de inte längre behövs.
  + Föra loggar över åtkomsträttigheterna.
* Starkare identifiering eller flerfaktorsautentisering krävs för användnings- och åtkomsträttigheter som är förknippade med högre risk (exempelvis hanterings- och administratörskoder, delade koder och distansförbindelser).

## 4.7 Lägesbild

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna definierar funktioner och teknik som ska användas för insamling och analys av operativa data och cybersäkerhetsdata, framlyftande, beskrivning och utnyttjande av larm för skapandet av en lägesbild över organisationens verksamhet och nivån på cybersäkerheten. För detta ändamål ska aktörerna:

* Samla in logginformation om apparater, programvaror och informationsresurser som är viktiga med tanke på spårtrafikens kontinuitet och säkerhet.
* Följa upp och analysera information som samlats in via loggar och andra källor.
  + Övervaka IT- och OT-miljöer med tanke på avvikande aktivitet och eventuella cybersäkerhetshändelser.
* Fastställa rutiner för att skapa och upprätthålla en lägesbild över cybersäkerheten som uppdateras regelbundet samt för att informera om den.
  + Sammanställa tillsynsinformation för att skapa en operativ lägesbild för aktören.
  + Berika lägesbilden med andra tillämpliga uppgifter från organisationen, till exempel visuella observationer.

## 4.8 Hantering av händelser och störningar samt verksamhetens kontinuitet

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna upprättar planer, processer och tekniker att använda för att upptäcka och analysera händelser och avvikelser som anknyter till cybersäkerheten samt svara på och återställa sig från dem i relation till riskerna för spårtrafikens kontinuitet och säkerhet. För detta ändamål ska aktörerna:

* Fastställa rutiner för anmälan om cybersäkerhetshändelser och -avvikelser till personer eller rollinnehavare som fastställts på förhand samt föra logg över händelserna och avvikelserna.
* Utarbeta kriterier för definitionen av cybersäkerhetsstörningar.
  + Analysera cybersäkerhetshändelser så att analysen stöder definitionen av eventuella cybersäkerhetsstörningar.
* Identifiera lämpliga arbetstagare och anvisa dem roller för att reagera på cybersäkerhetshändelser och -störningar.
  + Reagera på cybersäkerhetshändelser och -störningar så att man begränsar effekten på funktionen och återställer verksamheten till det normala.
  + Cybersäkerhetsstörningar rapporteras till Transport- och kommunikationsverkets Cybersäkerhetscenter och enhet för spårtrafik samt exempelvis L-ISAC-gruppen.
  + Informationssäkerhetsincidenter och försök till sådana anmäls till polisen när man misstänker brott.
* Upprätta en återhämtningsplan för systemen som hänför sig till verksamheten och en kontinuitetsplan för funktionen, där man beaktar organisationens metoder för att fortsätta verksamheten vid störningar samt dess möjligheter att säkerställa tillhandahållandet av tjänster som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet.
  + Säkerhetskopiera uppgifterna och testa säkerhetskopiorna.
  + Identifiera de IT- och OT-apparater som behöver reservdelar och som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet.
* Inom den egna organisationen och tillsammans med andra aktörer i transportsystemet öva för att testa kontinuitetsplanerna, svara på cybersäkerhetshändelser och -avvikelser samt kartlägga sårbarheter.

## 4.9 Hantering av risker i partnernätverket

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna fastställer rutiner för hantering av leveranskedjan och externa beroendeförhållanden genom vilka man kan hantera cybersäkerhetsrisker i tjänsterna och skyddade objekt som är beroende av externa aktörer i relation till riskerna för spårtrafikens kontinuitet och säkerhet. För detta ändamål ska aktörerna:

* Identifiera betydande IT- och OT-beroenden i partnernätverket, inklusive de partner som ansvarar för att operera funktionerna.
  + Identifiera de aktörer i partnernätverket som äger, administrerar eller på annat sätt har tillgång till apparater, programvaror eller informationsresurser som är viktiga för funktionen.
* Vid valet av aktörer och andra aktörer i partnernätverket beakta en bedömning av deras cybersäkerhetskompetens.
* Vid valet av produkter och tjänster beakta en bedömning av deras cyberförmågor.
  + Säkerställa säkerheten för de system som anskaffas genom att i anskaffningsskedet ställa nödvändiga cybersäkerhetskrav både på systemet som anskaffas och på leverantörens cybersäkerhetsnivå.
* Genom avtal säkerställa att cybersäkerhetsåtgärderna av aktörerna i partnernätverket är tillräckliga och anpassa dem till den egna organisationens verksamhetsmodeller för cybersäkerhet.
* Som en del av godkännandetestningen konstateras genom testning av säkerheten att de mest kritiska apparater, informationsresurser och system som anskaffas är säkra innan de tas i bruk.

## 4.10 Personalledning och -utveckling

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna definierar och upprätthåller planer, processer, teknik och kontroller för att skapa en cybersäkerhetskultur samt garantera lämplig och kunnig personal i relation till riskerna för spårtrafikens driftsäkerhet och säkerhet samt aktörernas egna mål. För detta ändamål ska aktörerna:

* Identifiera de ansvar som hänför sig till cybersäkerheten och utse en ansvarig person eller ansvariga personer i organisationen.
* Genom att erbjuda de ansvariga personerna utbildning i cybersäkerhet säkerställa att det i organisationen finns tillräcklig cybersäkerhetskompetens med tanke på arten och omfattningen av dess verksamhet samt att kompetensen upprätthålls och utvecklas.
* Säkerställa att de ansvariga personerna är förtrogna med aktörens operativa system och system som rör trafikeringen samt att de förstår de cybersäkerhetsrisker som är förknippade med systemen och arbetar för att minimera dem. De ansvariga personerna är förtrogna med lagstiftning och standarder som gäller cybersäkerhet samt kan säkerställa att dessa beaktas och iakttas i organisationen.
* Identifiera kraven på kunskaper, färdigheter och förmågor i anknytning till cybersäkerhet samt eventuella brister i dessa med tanke på både nuvarande och framtida behov.
* Utbilda även den övriga personalen och vid behov även underleverantörerna i cybersäkerhetsfrågor samt se till att medvetenheten om cybersäkerhet förbättras i organisationen.
* Definiera rutiner för bakgrundskontroller och utnämnande av arbetstagare och leverantörer till uppgifter, där de har åtkomst till skyddade objekt som hänför sig till tillhandahållandet av tjänster som är kritiska med tanke på spårtrafikens kontinuitet och säkerhet.
  + I förfaranden för avslutande av en anställning beaktas cybersäkerheten.

## 4.11 Cybersäkerhetsarkitektur

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna skapar och upprätthåller strukturer med hjälp av vilka de hanterar och styr organisationernas cybersäkerhetskontroller och -processer samt annan cybersäkerhetsverksamhet i relation till både riskerna för organisationens egendom och de mål som organisationen ställt upp. För detta ändamål ska aktörerna:

* Utarbeta en strategi för cybersäkerhetsarkitekturen i fråga om integriteten för och tillgången till kritiska system samt skyddade data genom att ägna särskild uppmärksamhet åt planerings- och användningsprinciperna för säkerhetsanordningar samt det fysiska skyddet och övervakningen av datacentraler.
* Skilja organisationens IT-nätverk från OT-nätverken exempelvis genom segmentering samt bedöma behovet av att dubblera nätverken och genomföra nödvändiga dubbleringar av dem.
* Använda mekanismer för skydd av cybersäkerheten för apparater, förbindelser, programvaror och informationsresurser som är viktiga för verksamheten.
* I högprioriterade apparater och programvaror säkerställa det programvarubaserade skyddet av programvaror som utvecklas internt och tredje parters lösningar under programvarornas hela livscykel, från anskaffningen och användningen till avskaffandet av programvarorna genom att i synnerhet se till att principerna för säker programvaruutveckling iakttas.
  + Beakta principerna för säker programvaruutveckling även i andra än högprioriterade system.
* Skydda känslig information på basis av identifieringen och klassificeringen av den information som behandlas.
  + När det gäller utvalda typer av information även sörja för skyddet av all övrig information.
  + När det gäller utvalda typer av information även sörja för skyddet av all information som är under överföring.

## 4.12 Ökning av samarbete

Transport- och kommunikationsverket rekommenderar att spårtrafikaktörerna samarbetar för att höja nivån på det totala skyddet i spårtrafiksystemet. För detta ändamål ska aktörerna:

* För den egna organisationen fastställa rutiner för samarbete för att utveckla cybersäkerheten och främja hanteringen av cybersäkerhetsrisker tillsammans med övriga aktörer inom branschen samt myndigheterna.
* I samarbete med övriga aktörer inom branschen sörja för cybersäkerheten och sträva efter att harmonisera rutinerna och nivån på skyddet, till exempel mellan dem som använder samma system eller gemensamma gränssnitt.
* Förmedla information om cybersäkerhetshot, -risker och -angrepp till övriga aktörer och samarbetsnätverk inom spårtrafiken för att skapa och dela en gemensam lägesbild.
* Sprida god praxis för att utveckla cybersäkerheten.
* Bidra till en god utveckling av cybersäkerhetsregleringen, bland annat i tekniska specifikationer för interoperabilitet.
* Se till att lyfta fram cybersäkerhetsfrågor i avtal mellan organisationer och på olika synliga ställen.

# **Bilagor, ytterligare information och informationskällor**

Bilaga 1: Metoder för hantering av cybersäkerheten enligt rekommendationen i tabellformat

Bilaga 2: Cybersäkerhetscentrets verktyg Cybermätaren med en hänvisning till denna rekommendation

Reglering

* NIS1-direktivet ([https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016L1148&from=SV](https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016L1148&amp;amp;from=SV))
* NIS2-direktivet ([https://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1672915693202&uri=CELEX%3A32022L2555](https://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1672915693202&amp;amp;uri=CELEX%3A32022L2555))
* Spårtrafiklagen 169 § (<https://finlex.fi/sv/laki/ajantasa/2018/20181302#L22P169>)
* Lagen om tjänster inom elektronisk kommunikation 244 a § (<https://finlex.fi/sv/laki/ajantasa/2014/20140917#O9L29P244a>)

Nationella myndigheter

* Traficoms föreskrift om ordnande av beredskapsplanering (<https://www.traficom.fi/sv/aktuellt/nya-foreskriften-ordnande-av-beredskapsplanering-i-transportsystemet>)
* Traficoms anvisning om anmälan om störningar i spårtrafiken (på finska) (<https://www.traficom.fi/sites/default/files/media/regulation/H%C3%A4iri%C3%B6ilmoitusohje%20valmis.pdf>)
* Webbplatsen för Cybersäkerhetscentret vid Transport- och kommunikationsverket (<https://www.kyberturvallisuuskeskus.fi/sv>)
  + Anvisningar och guider (<https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider>)
  + Cybermätaren (<https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren>)
  + Blankett för NIS-anmälan (anmälan om informationssäkerhetsincidenter) ([https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=sv&RetUrl=https%3A//www.traficom.fi/fi/asioi-kanssamme](https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx?langid=sv&amp;amp;RetUrl=https%3A//www.traficom.fi/fi/asioi-kanssamme))
* Statsrådets principbeslut om förbättring av informationssäkerheten och dataskyddet inom kritiska samhällssektorer (på finska) (<https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82>)
* Myndighetens för digitalisering och befolkningsdata (MDB) arkitektoniska ramar för digital säkerhet (DTARK) (på finska) (<https://wiki.dvv.fi/display/DTARK/>)

Standardisering

* IEC-standardisering för cybersäkerheten i järnvägssystemet (<https://www.iec.ch/ords/f?p=103:14:319535360914374::::FSP_ORG_ID:28802>)
* ISA 62443, Security for Industrial Automation and Control Systems
* CENELEC (<https://www.cenelec.eu/>)
  + CLC/TS 50701:2021:en Railway applications – Cybersecurity (<https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID5/5/1012872.html.stx>)
* NIST Cyber Security Framework, referensram för cybersäkerhet (<https://www.nist.gov/cyberframework>)
* NIST 800-82r2, anvisning för cybersäkerhet i ledningssystem för industrin (<https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final>)
* ISO/IEC 27001:2022:fi Informationssäkerhet, cybersäkerhet och dataskydd. Ledningssystem för informationssäkerhet. Krav. ([https://online.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stxISO/IEC 27002](https://online.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stxISO/IEC%2027002))
* SFS-EN ISO/IEC 27002:2022 Informationssäkerhet, cybersäkerhet och dataskydd. Metoder för hantering av informationssäkerhet. (<https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/1172534.html.stx>)
* ISO/IEC 27005, Riskhantering för informationssäkerhet. (<https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/738504.html.stx>)
* Cybersecurity Capability Maturity Model (C2M2) (<https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>)

Övriga

* Ordlista om cybersäkerhet (<https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/>)
* Webbplatsen för EU:s cybersäkerhetsbyrå Enisa (<https://www.enisa.europa.eu/>)
  + Hotmiljön i fråga om cybersäkerhet (<https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends>)
* Europeiska kommissionens publikation om instrument för cybersäkerhet i trafiken <https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en>
* EU 5G toolbox (<https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security>)
* Gruppen för informationsutbyte om cybersäkerheten för Europas järnvägar (ER-ISAC) (<https://er.isacs.eu/>)
* CYRail (<https://cyrail.eu/>). Se även CYRail Recommendations on cybersecurity of rail signalling and communication systems (<https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf>)
* Storbritanniens strategi Rail Cyber Security Strategy ([https://www.raildeliverygroup.com/component/arkhive/?task=file.download&id=469772253](https://www.raildeliverygroup.com/component/arkhive/?task=file.download&amp;amp;id=469772253))
* Exempel på en bow tie-analys, det vill säga en olycksfjärilsanalys ([https://www.traficom.fi/sites/default/files/media/file/Guidance for FSTD operators.pdf](https://www.traficom.fi/sites/default/files/media/file/Guidance%20for%20FSTD%20operators.pdf))
* Cebula, James J. & Young, Lisa R. 2010. A Taxonomy of Operational Cyber Security Risks. Carnegie Mellon University

Godkänd 30.1.2023

Kaisa Sainio   
Direktör

Ville Lahti

Specialsakkunnig

1. Definitionerna i tabell 1 är i huvudsak från Säkerhetskommitténs ordlista om cybersäkerhet, men en del av dem har kompletterats med termer som används i utrikesministeriets cybersäkerhetsstrategi för spårtrafiken och anpassats efter spårtrafiken (se kapitel 5 Ytterligare information och informationskällor) [↑](#footnote-ref-2)
2. https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016L1148&from=SV [↑](#footnote-ref-3)
3. <https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security> [↑](#footnote-ref-4)
4. <https://www.traficom.fi/sv/foreskrifter/anvisning-utarbetande-av-beredskapsplan-spartrafik> [↑](#footnote-ref-5)
5. <https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82> [↑](#footnote-ref-6)
6. Tabellen bygger på Cebula & Youngs (2010) tabell över operationella cyberrisker. [↑](#footnote-ref-7)
7. Till exempel IEC 31010:2019 Riskhantering. Metoder för riskbedömning. B.4.2 Olycksfjärilsanalys (bow tie analysis) och s. 22 i <https://www.traficom.fi/sites/default/files/media/file/Guidance%20for%20FSTD%20operators.pdf> [↑](#footnote-ref-8)
8. <https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID5/2/1155761.html.stx> [↑](#footnote-ref-9)
9. Traficom har inte befogenhet att kräva certifiering enligt ISO/IEC 27001 av aktörer, trots att ett krav på certifiering finns i till exempel Danmark. Traficom utövar riskbaserad tillsyn över aktörerna, och anskaffning av certifikatet skulle minska behovet av Traficoms tillsyn. [↑](#footnote-ref-10)
10. <https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren> [↑](#footnote-ref-11)