CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod jernbanesektoren

1. udgave februar 2021
Seneste opdatering juni 2022

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

2. udgave juni 2022.

Cybertruslen mod jernbanesektoren

Formålet med denne trusselsvurdering er at redegøre for cybertruslen mod den danske jernbanesektor. Trusselsvurderingen kan blandt andet bruges i sektorens videre arbejde med risikovurderinger. Målgruppen for trusselsvurderingen er primært ledelsen og it-medarbejdere hos jernbaneoperatører og infrastrukturforvaltere.

Trusselsvurderingen er blevet opdateret i juni 2022 med et tilpasset kapitel om truslen fra cyberaktivisme som følge af en ændring af trusselsniveauet beskrevet i CFCS' vurdering "CFCS hæver trusselsniveauet for cyberaktivisme mod Danmark fra LAV til MIDDEL" udgivet d. 18. maj 2022. Trusselsniveauet for cyberaktivisme er hævet fra **LAV** til **MIDDEL**. Den øvrige tekst er uændret.

Hovedvurdering

- Truslen fra cyberkriminalitet mod jernbanesektoren følger det generelle niveau for cybertruslen mod Danmark og er **MEGET HØJ**. Det betyder, at det er meget sandsynligt, at virksomheder eller myndigheder i jernbanesektoren bliver ramt af forsøg på cyberkriminalitet. Den største trussel kommer fra ransomware-angreb, men sektoren oplever for eksempel også cyberangreb mod underleverandører og forsøg på spear-phishing.

- Truslen fra cyberspionage mod den danske jernbanesektor er **HØJ**. Det betyder, at det er sandsynligt, at sektoren vil blive udsat for forsøg på cyberspionage. Fremmede stater kan eksempelvis have en interesse i at kompromittere organisationer i jernbanesektoren i forbindelse med større udbud.

- Truslen fra cyberaktivisme er hævet fra **LAV** til **MIDDEL**. CFCS har hævet trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine. Det er muligt, at særligt pro-russiske hackere vil gå efter mål i Danmark, herunder mål i jernbanesektoren.

- Truslen fra destruktive cyberangreb mod den danske jernbanesektor er **LAV**. Det betyder, at det er mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod samfundsvigtig dansk infrastruktur, herunder den danske jernbanesektor.

- Truslen fra cyberterror mod den danske jernbanesektor er **INGEN**. Militante ekstremister har i få tilfælde ytret intentioner om at udføre cyberterror, men de har ikke kapacitet til dette på nuværende tidspunkt.

Om trusselsvurderingen

Trusselsvurderingen beskriver cybertruslen mod den danske jernbanesektor. Vurderingen analyserer dermed truslen mod danske passager- og godsoperatører samt infrastrukturforvaltere, herunder letbaner, metroer og privatbaner.

Vurderingen tager afsæt i analyser af danske og internationale eksempler på cyberangreb mod operatører og infrastrukturforvaltere. Det sammenholdes med viden om trusselsaktørers kapacitet og intention. Trusselsvurderingen er udarbejdet i samarbejde med organisationer i jernbanesektoren.

Trusselsvurderingen beskriver det aktuelle trusselsbillede på kort sigt. Det svarer til en varslingshorisont på op til to år. Da cybertruslen er dynamisk, kan trusselsbilledet på nogle områder ændre sig pludseligt. Det gælder både generelt og specifikt for jernbanesektoren. Vurderingen anvender Forsvarets Efterretningstjenestes trusselsniveauer og sandsynlighedsgrader, der er forklaret i slutningen af vurderingen.

Den største trussel mod jernbanesektoren er cyberkriminalitet. Her udgør ransomware den mest alvorlige trussel mod jernbanesektoren som helhed, da ransomware-angreb fortsat er en populær angrebsmetode på tværs af de samfundsvigtige sektorer. Desuden kan et veludført ransomware-angreb potentielt medføre alvorlige økonomiske konsekvenser og i værste tilfælde driftsforstyrrelser for jernbaneaktørerne. Derudover udgør angreb via underleverandører, Business Email Compromise-scams (BEC-scams) og forsøg med spear-phishing også en væsentlig trussel for aktører i sektoren.

Cyberkriminalitet

Truslen fra cyberkriminalitet mod jernbanesektoren er **MEGET HØJ.** Truslen mod sektoren følger det generelle trusselsniveau for cyberkriminalitet mod Danmark. Det betyder, at CFCS vurderer, at det er meget sandsynligt, at sektoren vil blive ramt af angreb fra cyberkriminelle indenfor trusselsvurderingens varslingshorisont på to år.

Truslen kommer fra økonomisk motiverede kriminelle enkeltpersoner og netværk. Angrebene er som udgangspunkt opportunistiske. Aktørerne er derfor også interesserede i at kompromittere den danske jernbanesektor, hvis et angreb kan udnyttes til økonomisk vinding.

Derudover underbygges truslens høje niveau af udviklingen blandt de cyberkriminelle, hvor der i højere grad end tidligere samarbejdes og udveksles tjenester indbyrdes under markedslignende vilkår. Det kaldes Crime-as-a-service. Crime-as-a-service gør det muligt for kriminelle mod betaling at anskaffe sig adgange, værktøjer og infrastruktur, som de bruger i cyberangreb, frem for at udvikle selv. Samarbejdet øger specialiseringen og effektiviteten i det cyberkriminelle miljø, hvilket skaber robuste og organiserede forsyningskæder, der blandt andet understøtter målrettede ransomware-angreb.

Alvorlige ransomware-angreb truer jernbanesektoren

Ransomware udgør en alvorlig trussel mod sektoren. Ransomware er nemlig fortsat et populært værktøj blandt cyberkriminelle, som angriber på tværs af de samfundsvigtige sektorer. Derudover er ransomware-angreb mod jernbanesektoren alvorlige, da de i værste tilfælde kan forsage driftsforstyrelser og forsinkelser i den kritiske infrastruktur.

Ransomware-angreb foregår ved, at cyberkriminelle først skaffer sig adgang til en organisations netværk. Derefter krypterer de organisationens data, så de ikke længere er tilgængelige. På den måde tager de cyberkriminelle organisationens data, systemer og enheder som gidsler. Efterfølgende kræver hackerne løsepenge udbetalt i kryptovaluta for at dekryptere de låste data.

Nogle cyberkriminelle netværk går målrettet efter store organisationer, fordi angreb mod disse er mere profitable. Store operatører og infrastrukturforvaltere er interessante mål for disse cyberkriminelle netværk, da de ofte indtager samfundskritiske funktioner. Derfor forventer hackerne, at sådanne myndigheder og virksomheder er mere villige til at betale en meget stor løsesum.

Jernbanens legacy-systemer skaber risici

En særlig udfordring hos transportsektoren, herunder jernbanesektoren, er, at der fortsat anvendes et stort antal legacy-systemer. Legacy-systemer kan være sårbare overfor cyberangreb. Det skyldes blandt andet, at systemerne ofte er udviklet inden, der var tænkt på cybersikkerhed. Det betyder, at det er kompliceret eller meget omkostningstungt at opdatere eller udskifte systemerne. Endelig er det nogle gange ikke muligt at opdatere systemerne eller gøre dem it-sikre i forhold til nutidige standarder. Dermed udgør legacy-systemer en potentiel angrebsflade, som går på tværs af de forskellige former for cybertrusler.

Angrebene er målrettede i den forstand, at hackere bruger tid på først at kompromittere offeret for derefter at bevæge sig videre ind i offerets IT-systemer, for at kunne skabe størst mulig skade. Der kan derfor gå dage mellem hackernes indledende kompromittering af offeret og den endelige deployering af ransomware. Det er desuden sandsynligt, at nogle kriminelle hackere sælger den indledende kompromittering videre til andre kriminelle hackere.

Det er dog ikke kun de store og samfundsvigtige aktører, der er relevante mål for cyberkriminelle. CFCS er bekendt med, at cyberkriminelle også er gået efter små eller mellemstore virksomheder i transportsektoren i Danmark. Det skyldes, at de cyberkriminelle søger bredt efter sårbarheder blandt alle slags virksomheder. I sidste ende handler det om, hvor de lettest kan sikre sig en udbetaling i form af løsepenge.

I starten af 2020 fortalte det amerikanske anlægsfirma RailWorks Corporation, at de var blevet ramt af et ransomware-angreb. Under angrebet, som anlægsfirmaet kaldte et sofistikeret cyberangreb, lykkedes det hackerne at kompromittere virksomhedens systemer og plante malware. Derudover kom hackerne i besiddelse af personfølsomme data om medarbejdere, tidligere medarbejdere og underleverandører.

Cyberangreb mod leverandører kan være en let vej ind

Leverandører er attraktive mål for hackere, da kompromittering af en leverandør på én gang kan give adgang til mange organisationer, til leverandørens kundedata eller adgang til væsentlige dele af en sektors infrastruktur. Leverandører leverer blandt andet centrale services, herunder cloud-løsninger, datalagertjenester og andre it-serviceydelser.

Leverandører har ofte uhindret adgang til mange af deres kunders netværk og data. Ved blot at kompromittere én leverandør kan en aktør potentielt få mulighed for at bevæge sig uhindret på tværs af adskillige kunders netværk og data. Derfor sker cyberangreb imod leverandører med forskellige motiver som for eksempel spionage eller økonomisk vinding.

Verdens største cyberangreb skete via en leverandør

I december 2020 opdagede sikkerhedsfirmaet FireEye et af de mest omfattende offentligt kendte cyberangreb nogensinde.

Angrebet blev udført ved, at hackere kompromitterede virksomheden SolarWinds, som leverer software til organisationer verden over. Hackerne tilføjede i foråret 2020 ondsindet kode i legitime opdateringer til SolarWinds' software Orion. Op imod 18.000 kunder verden over downloadede de kompromitterede opdateringer. Den ondsindede kode gav hackerne en indledende adgang til ofrenes systemer, som de kunne udnytte yderligere.

CFCS har kendskab til, at omkring 30 organisationer i Danmark har anvendt den kompromitterede version af Orion og dermed har fået installeret en bagdør i deres netværk.

CFCS har kendskab til flere tilfælde af cyberangreb mod leverandører til jernbanesektoren i Danmark. Eksempelvis blev en underleverandør til Aarhus Letbane i 2020 udsat for et større hackerangreb. Her stjal bagmændene store mængder data fra underleverandøren inkl. information om letbanen.

Derudover oplevede Metroselskabet i 2020, at flere medarbejdere modtog mistænkelige mails fra en velkendt underleverandør, som indeholdt malware. Det viste sig, at en mailkorrespondance med underleverandøren var blevet kompromitteret af kriminelle hackere, der havde sendt mails til Metroselskabet fra leverandørens legitime mailkonto. Det var derfor svært for medarbejderne hos Metroselskabet at regne ud, at der var tale om et angrebsforsøg. Metroselskabet fik imidlertid afværget angrebet. Denne angrebsmetode er udbredt på tværs af sektorer og kaldes e-mail thread hijacking. Her kompromitterer hackerne en mailkonto hos en samarbejdspartner og udsender svar på igangværende mailkorrespondancer til ofrets kontakter. De inficerede mails kommer derfor fra en troværdig afsender og i naturlig forlængelse af allerede etablerede samtaler.

Andre udbredte angrebsmetoder er også effektive

En anden metode, som de kriminelle hackere kan anvende imod den danske jernbanesektor, er spear-phishing, der fortsat er en udbredt angrebsmetode. Spear-phishing minder om almindelige phishingforsøg, men adskiller sig ved, at modtagerne ikke er tilfældige, men udvalgte. Hackerne anvender ofte social engineering for at målrette indholdet til den enkelte modtager. Mails er typisk udformet, så de virker særligt relevante, overbevisende og troværdige for modtageren. Det kan eksempelvis være ved at anvende modtagerens navn, personspecifik information eller andre oplysninger, som er fundet ved forudgående rekognoscering.

Bedrageri i form af såkaldte BEC-scams er fortsat en trussel på tværs af sektorer. BEC-scams har til formål at franarre virksomheder og myndigheder penge via bedrageriske mails, der indeholder instrukser om at gennemføre pengeoverførsler til aktøren. For at udnytte medarbejdernes loyalitet udgiver de kriminelle sig typisk for at være en ledende medarbejder i organisationen. Bedrageri af denne type kaldes derfor også ofte for CEO-fraud eller direktørsvindel. BEC-scams kan medføre betydelige økonomiske tab for den berørte virksomhed eller myndighed.

CFCS har kendskab til forsøg på BEC-scams i jernbanesektoren i Danmark. Virksomheden Keolis, som står for driften af Århus Letbane, og som skal stå for den daglige drift af Odense Letbane, har for eksempel oplevet, at en højtstående medarbejder blev kompromitteret, muligvis med det formål at anvende personens information eller konto til at udføre BEC-scams mod ansatte i virksomheden. Medarbejderen reagerede dog hurtigt og angrebet blev afværget.

Truslen fra bevidste og ubevidste insidere

Der er en potentiel insidertrussel i alle organisationer. Det gælder også i jernbanesektoren. Organisationers sikkerhedsmekanismer beskytter ofte ikke mod insidere, som er i stand til at udføre deres handlinger alene ved at bruge deres legitime it-adgange.

Insidere kan inddeles i ubevidste og bevidste insidere. De ubevidste insidere er medarbejdere, der ikke er klar over, at deres adfærd kan være skadelig for

organisationen. Bevidste insidere er medarbejdere, som bevidst overtræder organisationens sikkerhedspolitikker for egen vinding skyld eller med det formål at skade organisationen.

CFCS vurderer, at ubevidste insidere er involverede i op mod halvdelen af sikkerhedshændelserne i en organisation.

Cyberspionage

Truslen fra cyberspionage mod jernbanessektoren er **HØJ.** Det generelle niveau for cyberspionage mod Danmark er meget høj, da fremmede stater vedholdende forsøger at stjæle information fra staten og flere sektorer. CFCS har ikke kendskab til et ligeså højt aktivitetsniveau mod jernbanesektoren, men vurderer, at fremmede stater både har intention om og kapacitet til at udføre cyberspionage mod dele af sektoren.

Cyberspionage bruges aktivt af flere lande, herunder Rusland og Kina, til at fremme nationale handlemuligheder og undgå strategiske overraskelser i et foranderligt udenrigspolitisk miljø. Hvor cyberkriminalitet i høj grad er drevet af grupper med et profitmotiv, er cyberspionage drevet af statsstøttede grupper, som ønsker adgang til viden. Det kan være viden om udvikling af nye omkostningstunge teknologier, dual-use-teknologier, passagerlister samt information, der kan have relevante overlap til andre sektorer.

I det omfang at dele af transportsektoren støtter dansk forsvar eller andre landes militær, eksempelvis transport af militært personel til missioner i udlandet eller militær brug af civile trafikknudepunkter, såsom lufthavne, havne og jernbaner, kan dette have fremmede staters interesse.

Statsstøttede grupper kan også have interesse for udbudsprocesser i jernbanebranchen. I udlandet har der været eksempler, hvor hackergrupper har forsøgt at tilgå information hos jernbaneoperatører forud for store udbud. Mellem februar og marts 2018 angreb hackere flere agenturer forbundet til Kuala Lumpur-Singapore high-speed rail-projektet. På det tidspunkt var flere kinesiske firmaer i gang med at byde på projektet. De kinesiske firmaer konkurrerede mod japanske og sydkoreanske virksomheder. Det er desuden muligt, at statsstøttede hackere udførte rekognoscering mod California High-speed Rail Authority forud for et større udbud i 2017.

Kinas nye silkevej

Kina er en aktiv og avanceret cyberaktør, der råder over omfattende kapaciteter til at udføre cyberspionage og destruktive cyberangreb. Kinas cyberkapaciteter er primært underlagt efterretningstjenesterne og det kinesiske militær, der i de seneste år har styrket cyberområdet.

Kina har med deres "Made in China 2025" program identificeret ti essentielle industrier, hvor de i fremtiden ønsker at indtage førende roller. Her er den nye silkerute et helt centralt element. Silkeruten skal sikre, at Kina har et stærkt handelsnetværk over hele verden med stærke og stabile transportmuligheder. Derfor har Kina vist stor interesse for jernbaneudbud og jernbanevirksomhed over hele verden, herunder også i Europa.

Kina har flere gange vist interesse for dansk infrastruktur - herunder også jernbanevirksomhed. I 2018 henvendte China Railway Tunnel Group, som er et datterselskab til det statsejede China Railway Group, sig til Helsingborg kommune. De ønskede at anlægge en ni kilometer lang jernbanetunnel mellem Helsingborg og Helsingør. Derudover skulle der anlægges en tunnel til biltrafik på 14-15 kilometer, som skulle knyttes til Helsingørmotorvejen ved Snekkersten.

Trafik-, Bygge- og Boligstyrelsen, Vejdirektoratet og Trafikverket undersøger i øjeblikket mulighederne for en fast forbindelse mellem Helsingør og Helsingborg. Denne undersøgelse er imidlertid uafhængig af det kinesiske tilbud.

I oktober 2015 forsøgte hackere at stjæle sikkerhedsinformation fra Japan Railways Hokkaido via selskabets administrative netværk. Hackerne sendte spear phishing-mails, som leverede ransomware af typen Emdivi RAT. Herefter forsøgte hackerne at hive information ud af systemet, blandt andet om forebyggelse af jernbanekriminalitet, jernbanekommunikationssystemer, sikkerhedsprocedurer og sikkerhedsinformation. Forsøget mislykkedes imidlertid og hackerne fik ikke informationen.

Cyberaktivisme

Truslen fra cyberaktivisme mod jernbanesektoren er **MIDDEL**. Det betyder, at det er muligt, at jernbanesektoren vil blive ramt af aktivistiske cyberangreb inden for de næste to år.

CFCS har hævet trusselsniveauet på baggrund af aktivistiske cyberangreb udført mod europæiske NATO-lande i forbindelse med krigen i Ukraine. På globalt plan er antallet af aktivistiske cyberangreb faldet de seneste år, men Ruslands invasion af Ukraine har skabt stor opmærksomhed i dele af det aktivistiske miljø. Hvor cyberaktivistiske angreb indledningsvist fandt sted i direkte forlængelse af krigen og var fokuseret mod Rusland, Ukraine og Belarus, har cyberaktivistiske angreb sidenhen også ramt europæiske NATO-lande, herunder aktører i transportsektoren.

Når trusselsniveauet for cyberaktivisme er hævet på grund af konkrete aktiviteter udført af pro-russiske cyberaktivister i forbindelse med krigen i Ukraine, betyder det ligeledes, at niveauet kan ændre sig igen med kort varsel afhængigt af krigens udvikling.

Cyberaktivisme er typisk drevet af ideologiske eller politiske motiver, og cyberaktivister fokuserer ofte på personer eller organisationer, de opfatter som modstandere af deres sag. Cyberaktivister kan få stor opmærksomhed på deres sag, hvis det lykkes at angribe jernbanevirksomheders hjemmesider, da disse typisk har mange besøgende. Ligeledes har informations- og afgangsskærme på stationer og banegårde en høj grad af synlighed, og de kan derfor være interessante mål for cyberaktivister.

Cyberaktivister angriber jernbanen i Belarus
I slutningen af januar 2022 offentliggjorde den cyberaktivistiske gruppe Cyber Partisans i et Twitter-opslag, at de ved hjælp af ransomware havde stoppet dele af den statslige togdrift i Belarus. Løsesummen for at udlevere dekrypteringsnøglen til den driftsansvarlige virksomhed var, at 50 politiske fanger skulle løslades, samt at russiske troppers tilstedeværelse på belarusissk territorium skulle forhindres.

Da Rusland kort efter havde igangsat invasionen af Ukraine, lavede Cyber Partisans endnu et aktivistisk angreb rettet mod jernbanen i Belarus. Denne gang krypterede de dele af jernbanens routing- og switching-komponenter, hvilket forstyrrede signalsystemerne og betød, at man måtte gå over til manuel drift. Målet var at forsinke russiske troppetransporter fra Belarus.

Flere aktører i jernbanebranchen fortæller, at chikane og cyberaktivisme står højt på deres dagsorden, når det kommer til cybersikkerhed. Dette gælder særligt angrebsformen DDoS-angreb, også kaldet overbelastningsangreb. DDoS-angreb foregår ved, at hackere udnytter kompromitterede computere til at generere usædvanligt store mængder datatrafik mod en hjemmeside eller et netværk. Formålet er at gøre hjemmesiden eller netværket utilgængeligt for legitim trafik, mens angrebet

står på. DDoS-angreb kan være alvorlige, hvis de rettes mod de kundevendte flader som rejseplaner, ankomst- og afgangsopdateringer samt billetsystemer. Denne form for angreb kan have en skadelig effekt på jernbanevirksomhedernes omdømme i offentligheden, pga. manglende tilgængelighed af de ramte kundevendte systemer.

DSB blev i september 2019 udsat for et DDoS-angreb, der gjorde flere dele af DSB's online services, blandt andet billetsalg via DSB app'en og DSB's hjemmeside, utilgængelig i flere timer. Tidligere har DDoS-angreb mod DSB i 2013 og 2018 også haft negative konsekvenser for DSB. Også i udlandet er der set eksempler på DDoS-angreb. Eksempelvis medførte et DDoS-angreb mod jernbaneoperatøren Trafikverket i Sverige i 2017 store forsinkelser.

Destruktive cyberangreb

Truslen fra destruktive cyberangreb mod jernbanesektoren er **LAV.**

CFCS definerer et destruktivt cyberangreb som et cyberangreb, hvor den forventede effekt er død, personskade, betydelig skade på fysiske objekter eller ødelæggelse eller forandring af informationer, data eller software, så de ikke kan anvendes uden væsentlig genopretning.

Langt de fleste af de destruktive cyberangreb, der har fundet sted indtil nu, har ødelagt data. Det er sket ved, at hackeren har slettet eller krypteret data uden mulighed for at genskabe dem. Destruktive cyberangreb er selv inden for denne brede definition relativt sjældne.

En række lande opbygger cyberkapaciteter, der kan bruges destruktivt mod samfundsvigtig infrastruktur, såsom jernbanessektoren, i forbindelse med en militær eller skærpet politisk konflikt. En del af denne opbygning består i cyberspionage, der bruges til at kortlægge kritisk infrastruktur.

Det er på kort sigt mindre sandsynligt, at fremmede stater har intention om at rette destruktive cyberangreb mod den danske jernbanesektor. Truslen kan dog ændre sig, hvis Danmark kommer i seriøs konflikt med lande, der har kapacitet til at udføre destruktive cyberangreb.

I udlandet er jernbanesektoren blevet ramt af destruktive cyberangreb, som i mindre grad forstyrrede sektorens tilgængelighed. I 2017 blev flere jernbanevirksomheder i udlandet ramt af NotPetya-angrebet, der var et destruktivt cyberangreb forklædt som ransomware. Senere i 2017 ramte den såkaldte BadRabbit-malware blandt andet metroen i Ukraines hovedstad Kiev.

Cyberterror

Truslen fra cyberterror mod jernbanesektoren i Danmark er **INGEN**. Det betyder, at det er usandsynligt, at jernbanesektoren vil blive udsat for forsøg på cyberterror inden for de næste to år.

CFCS definerer cyberterror som cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror. Det vil sige cyberangreb, der forårsager fysisk skade på mennesker eller materiel eller skaber omfattende forstyrrelser af samfundsvigtig infrastruktur.

CFCS vurderer, at selvom militante ekstremister i få tilfælde har ytret interesse for at udføre cyberterror, forudsætter denne type alvorlige cyberangreb tekniske evner og organisatoriske ressourcer, som de militante ekstremister ikke har.

Det nye signalsystem - ERTMS

Det nye fælleseuropæiske standardsystem European Rail Traffic Management System (ERTMS) skal planmæssigt udrulles i Europa frem mod 2030. I Danmark har man allerede udrullet systemet på flere strækninger, og det forventes, at signalsystemet er færdigudrullet i hele landet i 2030.

Med ERTMS signalsystemets indførelse foregår styringen af togene ikke længere via fysiske signaler på siden af banen men via et digitalt system med højere grad af centralisering. Derfor vil kompromitteringer af systemerne potentielt få større konsekvenser end i dag, da det vil være muligt at lave større og geografisk bredere forstyrrelse end tidligere.

ERTMS baserede signalsystemer er designet til at være et fejlsikre. Den generelle filosofi bag systemet er, at toget stopper, hvis der opstår usikkerheder i forhold til indkomne signaler. Derfor er det svært at forårsage en togulykke via systemet. Det er imidlertid muligt at udnytte denne sikkerhedsforanstaltning og skabe en situation, hvor man tvinger toget til stop. Dermed kan for eksempel et velplanlagt DDoS-angreb forårsage forstyrrelser og passagergener.

Da det nye signalsystem er baseret på en europæisk standard, skabes der nogle nye sikkerhedsudfordringer på cybersikkerhedsområdet. Det skyldes, at en fælles europæisk standard gør det muligt for hackere at bruge viden om sårbarheder registeret i andre europæiske lande og overføre denne viden til det danske system. Det var tidligere kun muligt i meget begrænset omfang, da de nationale systemer i langt højere grad varierede. Desuden er det nu muligt for en hacker i udlandet at nærlæse de overordnede specifikationerne for dele det danske system, da den information fremgår af de offentligt tilgængelige standarder for ERTMS.

I 2014 oplevede en amerikansk jernbanevirksomhed, at udenlandske hackere lavede et cyberangreb, hvor de forstyrrede signalerne via firmaets operative systemer. Det medførte, at der var forsinkelser over flere dage. Der var i dette tilfælde ikke tale om det europæiske standardsystem ERTMS, men angrebet viser, at det er muligt at angribe en jernbanevirksomhed via centralstyrede signalsystemer.

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og plan-lægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynligheder i analyser

Andre relevante publikationer

Center for Cybersikkerhed (CFCS) udgiver løbende vejledninger og trusselsvurderinger. Nedenfor er fremhævet en række produkter af særlig relevans for jernbanesektoren. Alle produkterne er tilgængelige på CFCS' hjemmeside.

Truslen fra bevidste og ubevidste insidere
CFCS og PET har udarbejdet trusselsvurderingen 'Cybertruslen fra bevidste og ubevidste insidere'. I trusselsvurderingen kan du læse mere om truslen og anbefalinger til mitigerende tiltag. Læs vurderingen her:

Trusselsvurdering om truslen mod leverandører
Trusselsvurderingen "Cyberangreb mod leverandører" beskriver cybertruslen mod leverandører. Læs vurderingen her:

Vejledning om leverandørstyring
Vejledningen "Informationssikkerhed i leverandørforhold" indeholder en række forslag til, hvordan styringen af forholdet mellem organisationer og leverandører kan varetages. Læs vejledningen her:

Truslen fra phishing-mails
Trusselsvurderingen "Cybertruslen fra phishing-mails" går i dybden med, hvordan hackere benytter phishing- og spear-phishing-mails i deres forsøg på at kompromittere virksomheder eller franarre dem følsomme oplysninger. Læs vurderingen her:

Vejledning til at imødegå phishing
Vejledningen "Phishing: Beskyt organisationen mod phishingangreb" henvender sig til ledelsen og kommer med en række konkrete anbefalinger, der kan bidrage til organisationernes arbejde med at beskytte sig mod phishing-angreb. Læs vejledningen her:

Samarbejde mellem cyberkriminelle
Trusselsvurderingen "Drømmer cyberkriminelle om tillidsfulde relationer?" beskriver, hvordan veletablerede samarbejdsrelationer, arbejdsdeling og udveksling af tjenester i det kriminelle miljø bidrager til den meget høje trussel fra cyberkriminalitet i almindelighed og målrettede ransomware-angreb i særdeleshed. Læs vurderingen her:

Truslen fra målrettede ransomware-angreb
Trusselsvurderingen "Digitale gidseltagere på storvildtjagt" beskriver truslen fra såkaldte målrettede ransomware-angreb, der kan have alvorlige konsekvenser for en organisation. Læs vurderingen her:

Vejledning om at imødegå ransomware-angreb
Vejledningen 'Reducér risikoen for ransomware' giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Vejledningen giver desuden råd til, hvordan et ransomware-angreb kan håndteres, når skaden er sket. Læs vejledningen her:

Hvordan målrettede ransomware-angreb foregår skridt for skridt
Undersøgelsesrapporten 'Anatomien af målrettede ransomware-angreb' går i dybden med, hvordan sådanne angreb foregår. Rapporten indeholder konkrete råd til, hvordan angrebene kan imødegås. Læs rapporten her:

Cyberangreb mod HR-afdelinger
Trusselsvurderingen "HR-afdelinger rammes også af målrettede cyberangreb" belyser, hvordan hackere forsøger at bruge HR-afdelinger som en nem vej ind i organisationer. Vurderingen indeholder også anbefalinger til, hvordan organisationer kan understøtte deres HR-afdelinger med både tekniske tiltag og awareness. Læs vurderingen her: