# 

Trusselskatalog

*dcis-Transport, TRAFIKSTYRELSEN*

*vERSION 2.0 (ÆNDRINGSHISTORIK FINDES I VEJLEDNINGEN)*

Trusselskatalog

[Angreb på eller fejl i industrikontrolsystemer (ICS/SCADA) 3](#_Toc148944424)

[Cyberspionage mod forretningskritiske data 5](#_Toc148944425)

[Ransomwareangreb mod forretningskritiske enheder og systemer 6](#_Toc148944426)

[Tab af ydelser fra leverandør 8](#_Toc148944427)

[Tab af internetforbindelse i længere tid 10](#_Toc148944428)

[Brand eller større vandskade i kontrolrum/kritiske tekniske anlæg 11](#_Toc148944429)

[Insider: Indvirkning på driftskritiske IT-systemer 12](#_Toc148944430)

[Kompromittering af driftskritiske kommunikationssystemer 13](#_Toc148944431)

[Omfattende DDoS-angreb 14](#_Toc148944432)

[Kompromittering og/eller tab af kritiske cloud-services 15](#_Toc148944433)

[Udløb af licenser (end-of-life/end-of-support) 16](#_Toc148944434)

[Uautoriseret digital adgang til lukkede systemer/netværk 17](#_Toc148944435)

[Phishing, BEC-scams mm. 18](#_Toc148944436)

[Website defacement attack 19](#_Toc148944437)

|  |  |
| --- | --- |
| Angreb på eller fejl i industrikontrolsystemer (ICS/SCADA) OT  *Cyberattack on industrial control systems (ICS/SCADA)* | |
| **Risikoidentificering** *Risk identification* | |
| Trussel *Threat* | Virksomheden rammes af et omfattende cyberangreb på industrikontrolsystemer, der styrer, regulerer og/eller overvåger virksomhedens forretningskritiske OT. Cyberangrebet kan være foretaget af en hacker, der opportunistisk forsøger at finde sårbarheder eller af en ondsindet ekstern aktør mhp. økonomisk vinding eller med et politisk motiv.  Ved fejl i industrikontrolsystemer menes der, at systemer ikke fungerer som forventet eller fejler fuldstændigt. |
| Årsag *Cause* | Industrikontrolsystemer er måske ikke tilstrækkeligt beskyttede, fx ved forbindelser med andre systemer med svagere adgangsstyring eller fordi forhold på *remote sites* muliggør adgang til systemerne.  Det kan også være sket gennem en softwareopdatering, som ikke har været tilstrækkelig gennemtestet inden implementering i virksomhedens systemer. |
| Mulige konsekvenser *Potential consequences* | Et omfattende cyberangreb kan indebære at de data, som vises på kontrolskærme mv., ikke er korrekte i forhold til, hvad aktuelle fysiske målinger og signaler ville have vist eller at systemer generelt ikke opfører sig som ventet.  Som følge heraf kan de ikke bruges, hvilket medfører driftsmæssige forstyrrelser; enten afbrydelse af drift eller væsentligt nedsat funktion.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed, 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *Consider the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden regler for tilslutning af fremmede medier til jeres industrikontrolsystemer? * Vurdér virksomhedens netværkssegmentering af industrikontrolsystemerne. Er der unødvendige forbindelser til SCADA’en/ICS? * Vurdér i hvilket omfang virksomheden foretager *patching* eller andre forbedringer af monitoreringssystemet for industrikontrolsystemer. I hvor høj grad testes *patches*, inden de implementeres? Er der behov for at se systemopdateringer i lukkede sandkassemiljøer, inden de implementeres i driftssystemer? Er det vurderet, om behovet er lige væsentligt for alle systemer eller er visse systemer mere kritiske på dette område? * Har virksomheden systemer til detektion af uønsket indtrængen i industrikontrolsystemer (ICS)? * Har virksomheden en beredskabsplan? Indeholder planen procedurer for, hvordan cyberangreb anmeldes til politi og indrapporteres til myndighederne? Indeholder planen procedurer for, hvis patches skaber uforudsete ændringer i OT-systemer?   **Tekniske foranstaltninger/technical measures**   * Har virksomheden identificeret alle forbindelser til SCADA/ICS-netværk? Og testet sikkerheden af forbindelserne? * Vurdér om virksomhedens genoprettelsesplan omfatter tiltag, såsom blokering af brugerkonti, også systemkonti, skift af passwords mv. * Vurdér i hvilket omfang virksomheden har sikret de fysiske forhold for *remote sites*, som er forbundet til SCADA/ICS? * Vurdér, om cyberangreb på industrikontrolsystemer kan forårsage fysiske skader på tekniske anlæg. * I hvilket omfang har virksomheden brug for, og adgang til offline medier, som kan geninstallere software på jeres udstyr? * Kan der skaffes virtuel eller fysisk adgang til industrikontrolsystemer via interne eller eksterne kommunikationskanaler? * Bliver der logget/dokumenteret aktivitet og adgang til kontrolsystemer mhp. efterforskning eller sikring af beviser? * Medfører brugen af back-up systemer eller data begrænsninger driftsmæssige begrænsninger? Fx nedsat kapacitet eller hastighed?   **Adfærdsmæssige foranstaltninger/behavioral measures**   * (Overvej selv yderligere foranstaltninger) | |

|  |  |
| --- | --- |
| Cyberspionage mod forretningskritiske data IT  *Cyberespionage on business-critical data* | |
| **Risikoidentificering** *Risk identification* | |
| Trussel *Threat* | Ondsindede aktører (private eller statsstøttede aktører) infiltrerer jeres netværk/systemer med software som i al hemmelighed ”trækker” fortrolige og/eller forretningskritiske data fra virksomhedens systemer. Forretningskritisk data i denne sammenhæng kan f.eks. være sikkerhedsplaner, persondata, beredskabsplaner og/eller konfigurationsdata til forretningskritiske systemer. |
| Årsag *Cause* | Mulige årsager kan være, at kritiske data/systemer ikke er tilstrækkeligt beskyttede, fx pga. mangelfuld kryptering, fejlkonfiguration, at netværkstrafikken på IT-systemerne ikke er tilstrækkeligt overvåget eller at en medarbejder utilsigtet trykker på et inficeret link. Angrebet kan også være foregået hos en leverandør. |
| Mulige konsekvenser *Potential consequences* | Et spionageangreb resulterer i uvedkommendes adgang til data, som er forretningskritiske og/eller fortrolige.  Adgangen leder til at fortroligheden og integriteten i information og/eller data kompromitteres med indvirkning på virksomhedens drift og sikkerhed. En ondsindet aktør får f.eks. adgang til kunders persondata eller virksomhedens kontrakter med leverandører.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed (egen og kunder), 2. Drift (egen og kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *Consider the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden et overblik over kritiske forretningsdata og systemer, herunder digital opbevaring, procedurer for opdatering samt hvilke medarbejdere, der har adgang hertil? * Har virksomheden taget stilling til hvorvidt de kritiske forretningsdata skal være tilgængelige på maskiner med opkobling til internet? * Har virksomheden overblik over leverandører, også af hardware og software? * Har virksomheden risikovurderet brugen af ovenstående leverandører, herunder om kontrollen af leverandør er tilstrækkelig? * Har virksomheden etableret (aktiv) overvågning af netværkstrafik på IT-systemerne, både for den administrative og den operationelle del? * Har virksomheden overvejet indvirkningen på samarbejdspartnere ved et spionageangreb?   **Tekniske foranstaltninger/technical measures**   * Vurdér om virksomheden deler og modtager viden om trusler ift. spionage mod kritiske data. * Har virksomheden etableret andre foranstaltninger/tiltag for at mitigere konsekvenserne og eller sandsynligheden af et spionageangreb, antivirus mv.? * Bliver der logget eller på andre måder dokumenteret aktivitet og adgange til kritisk data mhp. efterforskning? * Er der back-up’s på kritiske data samt procedurer for at opdatere disse? * Hvor lang tid tager genetablering? Er evt. forsinkelser medregnede i genetableringsplaner?   **Adfærdsmæssige foranstaltninger/behavioral measures**   * Vurdér om virksomheden i tilstrækkeligt omfang gennemfører awareness-kampagner? | |

|  |  |
| --- | --- |
| Ransomwareangreb mod forretningskritiske enheder og systemer IT/OT  *Ransomware attack against business-critical units and systems* | |
| **Risikoidentificering** *Risk identification* | |
| Trussel *Threat* | Flere af virksomhedens forretnings-kritiske systemer krypteres pludselig, og I mister adgangen hertil. |
| Årsag *Cause* | Ondsindede aktører udnytter en sårbarhed i virksomhedens *Remote Access Tool* (RAT) til at skabe sig en *backdoor* til jeres forretningskritiske systemer. |
| Mulige konsekvenser *Potential consequences* | Truslen kan resultere i, at kritisk personale ikke kan tilgå systemer, herunder administrative it-systemer (fx mails og ip-telefoni), dokumenter mv. som er nødvendige for at udføre forretningskritiske opgaver. Eksempler på konsekvenser kan være, at virksomheden ikke kan opretholde driften helt eller delvist over for kunder.  Hackere har desuden efterladt instruktioner om, at jeres systemer forbliver utilgængelige medmindre virksomheden betaler en løsesum i Bitcoin.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed (egen og kunders), 2. Drift (egen og kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *Consider the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden kortlagt den eventuelle sammenhæng mellem administrative it-miljøer og andre operationelle systemer, herunder OT-miljøer? Kan et angreb spredes på tværs af de to miljøer? * Vurdér i hvilket omfang administrative systemer og processer er kritiske for den daglige drift. * Vurdér hvorvidt virksomheden kan blive tvunget til at lukke dele eller hele driften ned for at undgå spredning til OT-siden. * Vurder fysisk beskyttelse af administrative systemer, herunder adgang via portable telefoner, computer, tablets, mv.? * Kan virksomhedens interne og eksterne kommunikationskanaler opretholdes ved et omfattende cyberangreb? * Har virksomheden en plan for genoprettelse af forretningskritiske enheder og systemer? * Kan beredskabsplaner og sikkerhedsplaner tilgås uden adgang til digitale systemer? * Har virksomheden risikovurderet behovet for aftale med et incident response team? * Eksisterer der tydelige handlingsplaner ift. håndtering af krav om løsesum? Har virksomheden en beredskabsplan? * Har virksomhedens topledelse overvejet, hvorvidt man betaler løsesum eller ej i tilfælde af et ransomware-angreb? * Vurder om aktivering og inddragelse af virksomhedens krisestab for håndtering af krav om løsesum og betaling er nødvendig og hvordan dette foregår? Hvem bør indgå i staben i et sådan scenarie? Hvem skal forhandle med dem? * Vurder om virksomheden har en klar aftale med et forsikringsselskab om, hvad der er omfattet og ikke omfattet?   **Tekniske foranstaltninger/technical measures**   * Har virksomheden indkøbt og anvender antivirus og mailfiltre til at tjekke indkomne mails for tegn på spam, phishing eller malware? * Har virksomheden en proces og ressourcer til at håndtere indrapporteringer om phishingforsøg fra medarbejdere? * Vurder mulighederne for øjeblikkeligt at lukke ned for inficerede computere, f.eks. via. en ”kill-switch”. * Har virksomheden taget backup af forretningskritiske enheder og systemer? * Foretager virksomheden logning af ovennævnte enheder og systemer? * Har virksomheden gennemgået den information om virksomheden, som er offentlig tilgængelig/søgbar på internettet? Det kan være medarbejdere med offentlige e-mails, sociale medier, men også detaljegraden af oplysninger om jeres virksomhed. * Vurdér om virksomheden løbende sikkerhedsopdaterer systemer og enheder? * Har virksomheden overvejet at bruge application control-løsninger, så kun autoriserede programmer kan aktiveres? * Vurdér om virksomheden begrænser antallet af medarbejdere med lokale administratorrettigheder. * Vurdér i hvilket omfang virksomheden anvender multi-faktor autentifikation.   **Adfærdsmæssige foranstaltninger/behavioral measures**   * Vurdér om virksomheden i tilstrækkeligt omfang gennemfører awareness træning af medarbejdere? | |

|  |  |
| --- | --- |
| Tab af ydelser fra leverandør IT  *Loss of services as a result of supplier failure* | |
| **Risikoidentificering** *Risk identification* | |
| Trussel *Threat* | Virksomhedens forretningskritiske systemer og enheder kompromitteres gennem et cyberangreb hos jeres leverandører.  Leverandører er attraktive mål for ondsindede aktører, da leverandører kan have adgang til eller drifter dele af virksomheders kritiske netværk og data. |
| Årsag *Cause* | Mulige årsager kan være, at virksomheden ikke har alternative løsninger til de ydelser eller systemer, som leverandører yder. Årsager kan også være, at kontrakter med leverandører ikke stiller tilstrækkelige krav ift. fortrolighed, integritet og tilgængelighed, fx ift. nedetider eller sikkerhedsforanstaltninger. |
| Mulige konsekvenser *Potential consequences* | Virksomhedens leverandør(er) kan ikke længere yde services, som er kritiske for virksomhedens drift og forretning. Det kan fx resultere i, at medarbejdere ikke længere har adgang til vigtige cloudbaserede løsninger eller anden data og software, som er kritiske for virksomhedens drift og forretning.  Driftsmæssige forstyrrelser kan være nedsat effektivitet eller at driften helt må afbrydes i en periode med både gener for passagerer og økonomiske tab som følge.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed (egen og kunders), 2. Drift (egen og kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *Consider the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden et overblik over forretningskritiske systemer og data, der ydes eller helt driftes af leverandører? * Har virksomheden overblik over leverandørens brug af underleverandører hvad angår forretningskritiske systemer og data? * Vurder om der er indgået aftale om at virksomheden skal have foretaget audits, enten ved ekstern audit eller ved virksomheden selv? * Vurder om virksomheden stiller krav til leverandørens modenhed? * Vurder om virksomheden stiller krav til leverandøren omkring medarbejderes integritet og baggrund, der håndterer forretningskritiske systemer og data? * Opdateres og afprøves leverandørens efterlevelse af kravene løbende ud fra jeres gældende risikovurdering? * Har virksomheden vurderet leverandørens evne til at håndtere en hændelse? * Har virksomheden overvejet aftaler med andre virksomheder, hvor man kan låne kapacitet af hinanden i tilfælde af tab af leverandør? * Er der overblik over leverandørers adgang til fysiske anlæg? * Omfatter beredskabsplanen procedurer for nedbrud af forrentningskritiske systemer i medfør af et tab leverandørydelser?   **Tekniske foranstaltninger/technical measures**   * Vurdér hvorvidt ejerskab til kildekode og dokumentation af egenudviklede (via leverandør) applikationer, protokoller eller andet er tilstrækkelig sikret. * Vurdér om de serviceydelser og tjenester som ydes af leverandør kan udnyttes som en ”indgang” til andre af virksomhedens ”in-house” systemer, OT, m.v. * Vurder om virksomhedens aftaler med leverandører stiller krav til overvågning, logning, af aktivitet, mv. mhp. efterforskning? * Vurder om virksomheden stiller tilstrækkelige sikringskrav i aftaler med leverandører ift. tilgængelighed, fortrolighed og integritet, fx ift. nedetid, logning og back-up-løsninger.   **Adfærdsmæssige foranstaltninger/behavioral measures**   * Stiller virksomheden krav til medarbejder-awareness ved leverandører? | |

|  |  |
| --- | --- |
| Tab af internetforbindelse i længere tid IT/OT  *Loss of internet connection for an extended period of time* | |
| **Risikoidentificering** *Risk identification* | |
| Trussel *Threat* | Scenariet omhandler et cyberangreb mod virksomhedens internetforbindelse, der medfører at virksomheden ikke har internetforbindelse i længere tid.  Fælles services og tjenester kan være attraktive mål for ondsindede aktører da et cyberangreb potentielt kan ramme bredt og få stor indvirkning på virksomheders drift på tværs af flere sektorer. |
| Årsag *Cause* | Årsagen til tab af internetforbindelse kan være både interne og eksterne. Eksternt ved generelt tab af internetforbindelse i lokalområdet. Internt ved at en sårbarhed i et legacy-system i virksomheden udnyttes af en ondsindet aktør for at stoppe internetadgangen. |
| Mulige konsekvenser *Potential consequences* | Tab af internetforbindelse i længere tid kan medføre at medarbejdere, kunder og andre esterne samarbejdspartners ikke har adgang til virksomhedens systemer.  Dette kan få driftsmæssige konsekvenser som forsinkelser eller delvise afbrydelser af transportydelser.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed (egen og kunders), 2. Drift (egen og kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *Consider the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden alternative internetforsyninger, såsom mobile netværk eller aftaler med serviceudbydere om alternative tilkoblinger? * Vurdér hvor længe driftskritiske system(er) kan opretholdes uden adgang til internet. * Vurdér konsekvenser af et internetnedbrud for resten af virksomheden (administrative systemer, mv.). * Vurdér om et tab af internetforbindelse har indvirkning på fysiske forhold, herunder sikringstiltag som adgangskort m.v. * Er der adgang til beredskabsplanen og tilhørende action cards, bilag, mv. ved tab af internetforbindelse? * Omfatter beredskabsplanen håndtering af tab af internetforbindelse, herunder prioritering ifm. genetablering ved nedsat kapacitet? * Vurdér i hvilket omfang virksomhedens kommunikationskanaler påvirkes ved et tab af internetforbindelse.   **Tekniske foranstaltninger/technical measures**   * Påvirkes virksomhedens overvågnings- og logningssystemer af tab af internetforbindelse? * Vurdér om tab af internetforbindelse kan påvirke adgang til eller styring af tekniske anlæg.   **Adfærdsmæssige foranstaltninger/behavioral measures**   * Er medarbejderne trænede til at håndtere en situation, hvor internetforbindelsen er tabt? | |

|  |  |  |
| --- | --- | --- |
| Brand eller større vandskade i kontrolrum/kritiske tekniske anlæg OT  *Fire in control room/critical technical installations* | | |
| **Risikoidentificering** *Risk identification* | | |
| Trussel *Threat* | | En brand eller oversvømmelse skader virksomhedens kontrolrum eller kritiske tekniske anlæg.  Skaderne bevirker, at medarbejdere må evt. evakueres ligesom en stor del af inventaret, herunder computere, skærme, ledninger og kabler, bliver brand- og sodskadet eller vandskadet.  Eventuelt tilstødende bygninger bliver ligeledes skadet i større omfang. |
| Årsag *Cause* | | Mulige årsager handler om fysisk sikring af de bygninger, hvor kontrolrum og dataservere er placerede samt risici for bygninger i tilslutning til de rum. Årsager kan fx være placering af servereanlæg i nærheden af brandfarlige installationer og misvedligeholdte brandsluknings-installationer eller at servere er placeret således, at risikokoen for vandskader er til stede. |
| Mulige konsekvenser *Potential consequences* | | Skader på kontrolrum/ og kritiske tekniske anlæg kan indebære tab af tilgængelighed af centrale systemer og data i længere tid.  Dette kan have omfattende økonomiske konsekvenser men også driftsmæssige konsekvenser i perioden for genetablering af systemer og aktiveringstid for evt. backup systemer.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed (egen og kunders), 2. Drift (egen og kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *Consider the following measures* | | |
| **Organisatoriske foranstaltninger/Organizational measures**   * Har virksomheden et overblik over hvilke kritiske systemer ift. kerneydelser og sikkerhed, der er afhængige af kontrolrummet/ eller tekniske anlæg? * Hvad er konsekvensen for virksomhedens kritiske systemer, som understøtter kernedrift og sikkerhed, hvis størstedelen af kontrolrummet, er brændt ned eller beskadiget? * Vurdér om sikring af fysiske forhold er optimal ift. brand, herunder om der er foranstaltninger på plads, som mindsker konsekvenserne ved en omfattende hændelse i kontrolrummet, fx brandalarmer. * Vurdér om sikring af fysiske forhold er optimal ift. oversvømmelse, herunder om kritiske anlæg er placeret i kælder eller er hævet fra gulvet eller om der er fugtighedsmåler til stede i rummet. * Er der genoprettelsesplaner på plads i tilfælde af en omfattende skade på kontrolrum? * Kan hændelsen medføre, at virksomheden tager alternative løsninger for IT-systemer i brug, som kompromitterer fortroligheden og/eller integriteten for kritiske systemer eller informationer? * Vurdér om fysiske skader kan have effekt på andre virksomheder/eksterne parter og/eller transportydelser i sektoren, fx i nærliggende bygninger.   **Tekniske foranstaltninger/Technical measures**   * Kan fysiske forhold ved de tekniske anlæg medføre en øget risiko for skader på datarum og kontrolcenter? * Kan kommunikationssystemer påvirkes af brand- eller vandskader på kontrolrum / og tekniske anlæg? * Er evt. back-up løsninger fysiske adskilte fra de systemer og data man normalt bruger? F.eks. cloudbaseret? * Kan overvågningssystemer blive påvirkede af skader på kontrolrum og? Er der alternative systemer eller procedurer, der kan bruges under genetableringsperioden?   **Adfærdsmæssige foranstaltninger/behavioral measures**   * (Overvej selv yderligere foranstaltninger) | | |
| Insider: Indvirkning på driftskritiske IT-systemer IT  *Insider: Threat to critical IT-systems* | | |
| **Risikoidentificering** *Risk identification* | | |
| **Trussel** *threat* | En insider med lovlig adgang til virksomhedens forretningskritiske systemer, intellektuelle ejendom eller lignende, udøver bevidst eller ubevidst skadelig adfærd på virksomheden. Insideren kan fx midlertidigt afbryde adgangen til et system, stjæle data med henblik på økonomisk vinding eller destruere systemer eller kildedata. Den ubevidste insider kan fx blive narret til at oplyse sin adgangskode. | |
| **Årsag** *Cause* | En insider har legitim adgang til virksomhedens fortrolige systemer, hvilket i kombination med et motiv - f.eks. politisk, økonomisk eller påvirkning fra en ekstern aktør - kan medføre skade på virksomheden.  Økonomisk vinding som motiv kan fx bestå i, at en person anvender sine netværksprivilegier ift. virksomhedens industrikontrolsystemer og kopierer diagnostik fra systemerne mhp. salg af de fortrolige oplysninger. Personligt motiv kan f.eks. være et ønske om at volde skade på virksomheden som hævn for opsigelse eller lign. | |
| **Mulige konsekvenser** *Potential consequence* | Konsekvenserne kan være tab af tilgængelighed, fortrolighed eller integritet. Insiderens motiv i kombination med adgang til og viden om kritiske systemer og data er styrende for omfanget af evt. konsekvenser.  I den mindst alvorlige del af skalaen er fx konsekvenserne ved afbrudt adgang til systemer (ændring af centrale adgangskoder) eller tyverier, der medfør et mindre økonomisk tab. Mere alvorlige scenarier kan fx være videresalg af oplysninger til ondsindede aktører, der har kapacitet til at udføre avancerede angreb på virksomheden.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed, 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy | |
| **Overvej bl.a. nedenstående foranstaltninger** *Discuss the following measures* | | |
| **Organisatoriske foranstaltninger/Organizational measures**   * Vurdér om virksomheden har et overblik over medarbejderes adgang til driftskritiske IT-systemer, samt om adgangen til hele eller dele af systemerne er styret ud fra medarbejdernes behov for at kunne løse sine arbejdsopgaver. * Vurdér medarbejdernes kendskab til virksomhedens informationssikkerhedspolitik; kender medarbejderne til risikoen forbundet med fx læk af data samt virksomhedens overvågning over uønsket aktivitet? * Har virksomheden tilsvarende oversigter over medarbejderes fysiske adgang, fx til datacenter og kontrolrum eller til fysisk opbevarede data samt er denne optimalt begrænset? * Kan interne kommunikationssystemer udnyttes af en insider til at sikre sig adgang til mere kritisk data? Har virksomheden tydelige procedurer for hvilke systemer, der må bruges for at dele eller opbevare kritiske data?   **Tekniske foranstaltninger/Technical measures**   * Vurdér om virksomheden er i stand til at opdage, om en insider bevidst eller ubevidst kan have kompromitteret driftskritiske IT-systemer (både fysisk og digitalt), samt om medarbejderne er bekendt med, hvordan evt. mistanke skal rapporteres.   **Adfærdsmæssige foranstaltninger/Behavioral measures**   * Gennemfører virksomheden awareness-træning for medarbejdere med adgang til forretningskritiske systemer, data mv. over for trusler som spear-phising og malware? | | |

|  |  |
| --- | --- |
| Kompromittering af driftskritiske kommunikationssystemer IT/OT  *Compromise of critical communication systems* | |
| **Risikoidentificering** *Risk identification* | |
| **Trussel** *Threat* | Virksomheden rammes af en kompromittering eller anden forstyrrelse af GPS-baserede systemer, radarsystemer el.lign., som bruges til drifts- og sikkerhedskritisk kommunikation.  En stor del af transportsektorens kommunikationsteknologi baseres i dag på internetbaserede teknologier. Trådløs kommunikation sker i dag ikke længere nødvendigvis gennem lukkede systemer og dedikerede frekvenser. I nogle tilfælde skyldes det, at hidtidige proprietære systemer ikke længere udvikles, ikke længere er fit for purpose og/eller ændringer af systemer er sket for at bringe omkostninger ned. |
| **Årsag** *Cause* | Fx manglende beskyttelse af driftskritiske kommunikationssystemer eller mangelfuld segmentering mellem kritiske- og ikke kritiske kommunikationssystemer. |
| **Mulige konsekvenser** *Potential consequence* | Konsekvenser kan omhandle udfald og unøjagtigheder i GPS-baserede kommunikation ml. trafikstyring og virksomhedens transporttjenester.  Udfaldet kan true driftsafviklingen og medføre forsinkelser eller trafikstop eller i værste fald true passager- og medarbejdersikkerhed.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed, 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *discuss the use of the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden et løbende overblik over systemer, som understøtter drifts- og sikkerhedskritisk kommunikation? * Har virksomheden krypteret og/eller iværksat andre tiltag for at beskytte den drifts- og sikkerhedskritiske kommunikation? * Vurdér om fysiske forhold (fx afstand mellem security og områder med offentlig adgang) udgør en risiko for kompromittering kritiske systemer.   **Tekniske foranstaltninger/Technical measures**   * Medfør evt. aktivering af alternative kommunikationssystemer en øget risiko for tab af fortrolighed? * Vurdér i hvilket omfang virksomheden har alternative kommunikationskanaler, samt hvordan aktivering af disse påvirker drift og effektivitet. * Har virksomheden foranstaltninger på plads til at opdage hændelser i opløbet? * I hvilket omfang har virksomheden indført logning?   **Adfærdsmæssige foranstaltninger/Behavioral measures**   * (Overvej selv yderligere foranstaltninger) | |

|  |  |
| --- | --- |
| Omfattende DDoS-angreb IT  *Widespread DDoS-attack* | |
| **Risikoidentificering** *Risk identification* | |
| **Trussel** *Threat* | Ondsindede aktører udfører et omfattende overbelastningsangreb (DDoS-angreb) og rammer virksomhedens hjemmesider og/eller andre internetvendte services.  DDoS-angreb kan fx forstyrre driften og pålideligheden af virksomhedens ydelser ved fx at gøre billetsalg eller hjemmesider utilgængelige. |
| **Årsag** *Cause* | Årsager kan være netværkskomponenter, herunder firewall og routere, som ikke er opdateret, mangel på aftale med alternativ internetudbyder eller virksomhedens egen manglende evne til at differentiere mellem skadelig angrebstrafik og legitim driftstrafik. |
| **Mulige konsekvenser** *Potential consequence* | Hændelsen kan medføre, at netværk overbelastes samt tilgængeligheden af hjemmesider kompromitteres og ikke kan tilgås.  I sidste ende kan hændelsen have afledte konsekvenser, der kan resultere i driftsmæssige forstyrrelser; enten ved afbrydelse af drift eller nedsat kapacitet, økonomisk tab for virksomheden eller påvirke andre forretningskritiske systemer.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed, 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| Overvej bl.a. nedenstående foranstaltninger *discuss the use of the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden gjort sig overvejelser om afledte konsekvenser af et DDoS-angreb rettet mod en hjemmeside eller anden offentligt anvendt tjeneste, f.eks. virksomhedens mulighed for at anvende e-mail internt pga. en belastet mailserver? * Hvordan sikres, at relevante medarbejdere i virksomheden er bekendt med beredskabsplanen, herunder kontakt til og kendskab til aftaler med internetleverandør? * Har virksomheden nærmere overblik over, hvilke DDoS-forsvarsmidler virksomhedens internetleverandør stiller til rådighed? * Har virksomheden tilkøbt ekstra IP-adresser eller aftale om ekstra separate internetadgange, der kan anvendes alternativt, hvis den primære IP-adresse eller internetadgang bliver blokeret?   **Tekniske foranstaltninger/Technical measures**   * Hvordan monitoreres netværk og applikationer for hurtigt at kunne erkende et angreb, herunder have normalt billede af internet-båndbredde (tilgængeligt og brugt)? * Er virksomheden i stand til at differentiere mellem skadelig angrebstrafik og legitim driftstrafik? * Hvordan sikrer virksomheden, at alle netværkskomponenter, herunder firewall, routere og spamfiltre, er opdateret til seneste *patch*? * Kan et DDoS-angreb på hjemmesiden overbelaste netværkskomponenter, fx firewalls eller en router og dermed afbryde og forstyrre adgang til VPN eller E-mail? * Har virksomheden forberedt en nødforside på hjemmesiden eller alternativ hostet forside/informationsside? * Har virksomheden gjort sig overvejelser om anvendelse af cloud-hosting af hjemmesiden?   **Adfærdsmæssige foranstaltninger/Behavioral measures**   * (Overvej selv yderligere foranstaltninger) | |

|  |  |
| --- | --- |
| Kompromittering og/eller tab af kritiske cloud-services IT  *Compromise and/or loss of cloud services* | |
| **Risikoidentificering** *Risk identification* | |
| **Trussel** *Threat* | Et cyberangreb foretaget af en ondsindet aktør rammer virksomhedens cloud-baserede kritiske services, herunder eksempelvis backups. |
| **Årsag** *Cause* | Årsager kan være fejlkonfigurationer, manglende kryptering og logning, hvortil ondsindede aktører formår at udnytte disse sårbarheder i cloud-miljøet. |
| **Mulige konsekvenser** *Potential consequence* | En kompromittering af cloud-services kan give ondsindede aktører adgang til fortrolige og/eller forretningskritiske data, mens et tab af cloud-services kan medføre at medarbejdere mv. ikke har adgang til vigtige dele af virksomhedens systemer eller at backup af systemer ikke er tilgængelige, når der er behov.  I sidste ende kan hændelsen have afledte konsekvenser, der kan resultere i driftsmæssige forstyrrelser; enten ved afbrydelse af drift eller nedsat kapacitet, økonomisk tab for virksomheden eller på anden vis påvirke andre forretningskritiske systemer.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed, 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *discuss use of the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden et overblik over forretningskritiske systemer og data, der driftes via cloud-services? * Har virksomheden overblik over, hvilke medarbejdere, der benytter sig af eller har adgang til cloud-services? * Vurder om virksomhedens cloud-services er baseret på standard løsninger eller løsninger, der kan tilpasses virksomhedens sikkerhedskrav? * Har virksomheden fastlagt sikkerhedskrav til leverandøren fx ift. kryptering af data, sårbarhedsscanninger, sikring mod fejlkonfigurationer, GDPR, nedetid og back-up-løsninger? * Stiller aftalen med leverandør af cloud-services krav til overvågning, logning, af aktivitet, mv. mhp. efterforskning? * Fører virksomheden tilstrækkelig kontrol med leverandøren af cloud-løsninger ift. de fastlagte sikkerhedskrav? * Opdateres og afprøves leverandørens efterlevelse af kravene løbende ud fra gældende risikovurdering? * Har leverandøren dokumentation på de sikkerhedsmæssige tiltag, eksempelvis ved certificeringer, revisionsrapporter, sikkerhedslogs eller dokumentation fra en uafhængig tredjepart? * Har virksomheden gjort sig overvejelser om andre afledte konsekvenser ved kompromittering eller tab af cloud-services? Kan det i værste fald få indvirkning på passager- og medarbejdersikkerhed?   **Tekniske foranstaltninger/Technical measures**   * Har virksomheden en eller mange aftaler med udbydere af cloud-services eller er services ”spredt ud” og driftes af flere udbydere, der potentielt kan mindske konsekvenserne af et angreb? * Vurdér om cloud-services kan udnyttes som en ”indgang” til virksomhedens andre ”in-house” systemer, OT, m.v. eller på anden vis få konsekvenser for tilgængelighed, fortrolighed og integritet, fx ift. kritiske data og forretningskritiske systemer? * Omfatter beredskabsplanen et nedbrud af forretningskritiske systemer forårsaget af en kompromittering eller et tab af cloud-services?   **Adfærdsmæssige foranstaltninger/Behavioral measures**   * Er medarbejderes adgangssikkerhed ift. cloud-services understøttet, fx af en multifaktor autentifikationsproces? | |

|  |  |
| --- | --- |
| Udløb af licenser (end-of-life/end-of-support) IT/OT  *Expiration of licences* | |
| **Risikoidentificering** *Risk identification* | |
| **Trussel** *Threat* | En eller flere licenser til software, hardware eller lign., som er en del af jeres forretningskritiske systemer, er løbet ud (end-of-life og/eller end-of-support). |
| **Årsag** *Cause* | Årsager kan være gammel, men nødvendig teknologi, utilstrækkelig licensstyring, herunder en bevidst eller ubevidst tilsidesættelse af forlængelse af licenser pba. økonomiske hensyn, mangelfuld leverandørstyring eller ugennemsigtige kontrakter. |
| **Mulige konsekvenser** *Potential consequence* | Udløb af licenser kan resultere i at software ikke kan opdateres. Manglende opdateringer kan lede til sårbarheder i jeres systemer, der kan udnyttes af ondsindede aktører.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed, 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *discuss use of the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden overblik over licenser og hvor længe de er aktive? Er de kategoriseret ud fra kritikalitet? * Eksisterer der en virksomhedspolitik for tildeling af licenser?   **Tekniske foranstaltninger/Technical measures**   * Foretages der løbende licens-audits? Fx af eksterne eller interne reviews? Manuel audit vs. Scanningsprogrammer? * Har I etableret en software asset management funktion til overvågning af softwarelicenser? * Hvor hurtigt kan en udløbet licens(er) evt. genaktiveres?   **Adfærdsmæssige foranstaltninger/Behavioral measures**   * Har I overblik over hvilke typer af brugere (fx evt. light users), der interagerer med licensen? og hvilken adgang brugerne har? | |

|  |  |
| --- | --- |
| Uautoriseret digital adgang til lukkede systemer/netværk IT/OT  Unauthorized access to non-public systems | |
| **Risikoidentificering** *Risk identification* | |
| **Trussel** *Threat* | En ondsindet aktør hacker sig (teknologisk) adgang til et lukket netværk, system eller lign i virksomheden og udnytter adgangen som en ”gateway” til at trænge ind på interne lukkede systemer og/eller netværk.  Den uautoriserede digitale adgang kan være muliggjort af, at den ondsindede aktør lovligt kan opholde sig fysisk i nærheden af nogle af virksomhedens ellers lukkede systemer og netværk. |
| **Årsag** *Cause* | Årsagen kan være mangelfuld fysisk sikring og overvågning, herunder videoovervågning og overvågning af netværk mhp. at detektere indtrængen fra uvedkommende. |
| **Mulige konsekvenser** *Potential consequence* | Konsekvenserne kan være tab af tilgængelighed, fortrolighed og/eller integritet.  Ondsindede aktører kan få adgang til fortrolige og/eller forretningskritiske systemer og i sidste ende kan hændelsen have afledte konsekvenser, der kan resultere i driftsmæssige forstyrrelser eller økonomisk tab for virksomheden.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed, 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *discuss use of the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden regler for tilslutning af fremmede medier til jeres lukkede netværk? * Vurdér om virksomhedens genoprettelsesplan omfatter tiltag, såsom blokering af brugerkonti, også systemkonti, skift af passwords mv. * Kan virksomheden på tilstrækkelig vis detektere evt. uvedkommendes uautoriserede adgang, eller forsøg herpå, til lukkede systemer? * Vurdér i hvilket omfang virksomheden foretager *patching* eller andre forbedringer af monitoreringssystemet? * Har virksomheden lavet backup og beredskabsplan i tilfælde af et destruktivt cyberangreb? Og indeholder planen procedurer for, hvordan cyberangreb anmeldes til politi og indrapporteres til myndighederne?   **Tekniske foranstaltninger/Technical measures**   * Har virksomheden testet sikkerheden af forbindelserne mellem lukkede/lokale netværk? * Vurdér virksomhedens netværkssegmentering, fx mellem offentligt tilgængelige netværk og lukkede netværk. Er der unødvendige forbindelser til jeres lukkede netværk? * Vurdér i hvilket omfang virksomheden har sikret de fysiske forhold for jeres lukkede netværk, som er inden for fysisk rækkevidde af offentligheden? * Bliver der logget eller på andre måder dokumenteret aktivitet og adgang mhp. efterforskning eller sikring af beviser?   **Adfærdsmæssige foranstaltninger/Behavioral measures**   * (Overvej selv yderligere foranstaltninger) | |

|  |  |
| --- | --- |
| Phishing, BEC-scams mm. IT  Phishing and BEC-scams | |
| **Risikoidentificering** *Risk identification* | |
| **Trussel** *Threat* | En ondsindet aktør får gennem omhyggelig research identificeret et potentielt offer, som de bruger til at få adgang til interne systemer såsom mailprogram, og kan derfra udgive sig for at være en intern medarbejder. Bemærk, at denne trussel er instrumental af natur og kan derfor være katalysator eller udslagsgivende for andre trusler i dette katalog. |
| **Årsag** *Cause* | Årsagen kan være mangelfuld it-sikkerhedsbevidsthed eller cyberhygiejne fra medarbejderne, som derved bliver et mål for phishing e.l. |
| **Mulige konsekvenser** *Potential consequence* | Konsekvenserne kan være tab af fortrolighed og/eller integritet. Samtidig kan der være tale om store økonomiske konsekvenser, hvis hændelsen ikke opdages i tide. Ved at udgive sig som en medarbejder, kan den ondsindede aktør lave forespørgsler om pengeoverførsler eller betaling af falske faktura.  Hvis virksomheden ikke har foranstaltninger i form af to-faktor godkendelser på loginsystemer generelt, så kan den indledende hændelse brede sig til et væld af andre interne systemer, hvor den ondsindede aktør dermed vil have adgang.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed (egen), 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *discuss use of the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden informeret medarbejderne omkring konsekvenserne ved phishing og BEC-scams (Business Email Compromise)? * Er der implementeret procedurer, som modvirker BEC-scams og anden phishing, eksempelvis personlig eller fysisk verifikation ved pengeoverførsler?   **Tekniske foranstaltninger/Technical measures**   * Har virksomheden indført foranstaltninger som eksempelvis to-faktor godkendelse ifm. større pengeoverførelser? Er to-faktor godkendelse generelt implementeret i virksomheden? * Har virksomheden oprettet muligheden for at indrapportere forsøg på phishing til et centralt sted? Er det kun ift. mails eller omfatter det også sms’er og telefonopkald? * Bliver mails eller links sendt i mail kontrolleret mod kendte phishingaktører inden medarbejderne modtager dem?   **Adfærdsmæssige foranstaltninger/Behavioral measures**   * Er medarbejderne trænede i at opdage og håndtere forsøg på phishing, såsom at klikke på suspekte links mm? Holdes denne træning ved lige? * Er medarbejderne trænede i god sikkerhedsadfærd på internettet, eksempelvis hvilke oplysninger man deler mv, for at modvirke eksempelvis spear phishing? * (Overvej selv yderligere foranstaltninger) | |

|  |  |
| --- | --- |
| Website defacement attack IT  Website defacement attack | |
| **Risikoidentificering** *Risk identification* | |
| **Trussel** *Threat* | En ondsindet aktør får adgang til virksomhedens hjemmeside og ændrer det visuelle eller tekstuelle på siden – typisk med et politisk budskab eller information om at hjemmesiden er blevet hacket. |
| **Årsag** *Cause* | Årsagen kan være medarbejdere, som ubevidst gennem phishing giver ondsindede aktører adgang til loginoplysninger til virksomhedens hjemmeside. Adgangen kan også skaffes gennem brute force eller ved at udnytte kendte svagheder i plugins eller addons. |
| **Mulige konsekvenser** *Potential consequence* | Konsekvensen kan ramme virksomhedens omdømme, men det er også muligt for ondsindede aktører at få adgang til andre systemer, hvis en webside ikke er tilstrækkeligt sikkert konstrueret. Der er derfor mulige tab af oplysninger, som kan have andre større driftsmæssige og økonomiske konsekvenser.  **Overvej farens mulige konsekvenser for:**  1. Sikkerhed, 2. Drift (kunder), 3. Økonomi, 4. Omdømme, 5. Privacy |
| **Overvej bl.a. nedenstående foranstaltninger** *discuss use of the following measures* | |
| **Organisatoriske foranstaltninger/organizational measures**   * Har virksomheden informeret medarbejderne omkring konsekvenserne ved phishing? * Har virksomheden en politik eller principper omkring adgangs- og rettighedsstyring på systemer, så medarbejdere kun har den adgang, de reelt har behov for? * Er reglerne for kodeord og andre loginoplysninger tilstrækkelige? Og bliver det løbende opdaterede, så de er de er tidssvarende til eksempelvis brute force-angreb?   **Tekniske foranstaltninger/Technical measures**   * Har virksomheden vurderet behovet og brugen af eksterne plugins og add-ons, som aktører kan benytte til at skabe adgang til websiden? Udføres der patching på disse plugins? * Er websiden krypteret?   **Adfærdsmæssige foranstaltninger/Behavioral measures**   * Er medarbejderne trænede i at opdage og håndtere forsøg på phishing, såsom at klikke på suspekte links mm? Holdes denne træning ved lige? * (Overvej selv yderligere foranstaltninger) | |