

Verslag KPT-webinar

‘Cybersecurity bij tunnels: Verantwoordelijkheden, compliance en dilemma's’

Datum 17 september 2026
Tijd 12.00-13.30 uur
Locatie digitaal vanuit de COB-studio
Deelnemers > 75 personen



Opening en introductie KPT

Harry de Haan, coördinator van het KPT opent het webinar en heet alle deelnemers en in het bijzonder de sprekers **Cedric Both (Datadigest)** en **Marc van der Zandt (Safesecur)** van harte welkom. Na enkele huishoudelijke mededelingen en een korte toelichting op het KPT geeft Harry het woord aan Jan Kuchel, expert van het KPT, die de sprekers voorstelt en vervolgens ook het woord geeft. De presentatie is terug te vinden via [de KPT-website](#).

Tijdens het webinar konden vragen gesteld worden. Deze zijn na afloop van de presentaties behandeld. Ook de vragen die wegens tijdgebrek niet tijdens de webinar beantwoord konden worden, zijn in dit verslag meegenomen. Onderstaand volgt een weergave van deze vragen en antwoorden.

Vragen en antwoorden:

Vraag 1:

Vanuit het perspectief van de veiligheidsbeambte bestaat er een duidelijke relatie tussen safety en security binnen het cyberdomein. Waar security zich primair richt op de beveiliging, gaat safety ook over de aantoonbare kwaliteit, van software, IT- en OT-systemen. In de praktijk is er daarom sprake van een aanzienlijke overlap tussen beide gebieden.

Bij het werken met IT- en OT-systemen moet rekening worden gehouden met de specifieke risico's van de omgeving waarin deze systemen worden toegepast.

Bij tunnelveiligheid wil je niet dat er dingen gebeuren waardoor de tunnel niet meer veilig is: dat het systeem platgaat, wordt gelekt of geblokkeerd. Dit geldt ook voor fysieke beveiliging – beveiliging van de tunnel – en de systemen die de veiligheid in de tunnel moeten waarborgen. De tunnel moet blijven werken, maar wel veilig. Veiligheid is hier heel breed: voor het wegverkeer, voor de gebruikers etc., maar ook veilig voor aanvallen van buitenaf. In de praktijk proberen we een goede mix te maken tussen de maatregelen die je kunt toepassen, zodat het werkbaar blijft. We kijken ook hoe de gelaagdheid is: wel of niet aan een externe toegang. De rode draad daarin is: probeer het niet te complex te maken, waardoor de veiligheid van het object in het geding komt. Er moet een balans zijn.

Vraag 2 – aanvullend op vraag 1:

Het gaat nadrukkelijk ook om aantoonbare kwaliteit van software en IT/OT hardware.

De aantoonbare kwaliteit van software en IT/OT hardware is één van de belangrijkste uitdagingen.

Datadigest maakt verschillende oplossingen voor verschillende tunnels, dit betreft een stukje maatwerk software. Als je niets doet met het ontwerpproces en de documentatie van deze oplossing wordt het een black box.

Een van de belangrijkste thema's is openheid van zaken. Er zijn allerlei mogelijkheden dat stukje software te toetsen. ISO-normen zoals de ISO 27001 kunnen daarbij ondersteunen

Meenemen in projecten waar software gemaakt wordt, stel de vraag of de software veilig is en voldoet aan de richtlijnen. Achteraf dat laten testen is ingewikkelder. Het begint aan de voorkant. Weet wie de leverancier is en vraag of een rapportage kan worden opgeleverd waarin staat dat de software getest en veilig is. Dit is ook nieuw in de norm opgenomen.

Vraag 3 – aanvullend op vraag 1:

Hoe ontwerp je voor de combinatie van een fysiek incident én een cyberaanval die bijvoorbeeld CCTV, communicatiesystemen, ventilatie of verkeerssturing beïnvloedt? Is daar een 'worst credible scenario' voor?

Er wordt veel waarde gehecht aan het ontwerpproces van tunnelveiligheidsmaatregelen.

Cybersecurity dient in het werkproces meegenomen te worden om van daaruit een veilige tunnel te maken. Dit was vaak een hekkensluiter, maar de hedendaagse tendens is dat cybersecurity steeds vaker in de hele keten wordt meegenomen, zodat dit in het proces geborgd is (Security en Safety by design).

Bij de risicoanalyse komt altijd aan de orde of je met security en safety te maken hebt.

Vraag 4:

Is er een norm of methodiek die borgt dat patches niet alleen de security verbetert, maar ook aantoont dat de werking van het systeem erachter in orde blijft?

Mijn ervaring is dat een patch soms toch ook inhoudelijke effecten heeft die niet voorzien waren.

Ja, dat is de IEC 62443-2-3

Vraag 5:

Het idee van quick wins wordt begrepen. Maar is het niet beter om eerst te kijken naar de grootste risico's en daar als eerste iets aan te doen?

Risico's staat als tweede genoemd. Risico's zijn te identificeren als je weet wat je assets zijn. In de praktijk zien we vaak dat nog niet de hele keten en alle assets in kaart zijn. Misschien zijn er grotere risico's.

Vraag 6:

Vraagsteller merkt op het een gevaarlijke raad te vinden om zonder meer pentesten (PEN-test=penetratietest door een ethisch hacker) een goed idee te noemen. Door ongecontroleerd pentesten in een OT-omgeving te doen, kan je toch heel de boel lam leggen. Dus controleer zeker de kennis en kunde van de partij die je het laat doen.

Aangeraden wordt de pentesten niet ongecontroleerd te doen en een kader mee te geven: wat mag wel en wat mag niet. Daarnaast is het van belang om indirect betrokkenen zoals een verkeersleiding of onderhoudspartijen in te lichten wat er gedaan wordt. Mocht er dan onverhoopt iets gebeuren, kan er meteen geacteerd worden. Zie binnen ISO 27001 de normparagrafen 8-34: die gaan over bovengenoemde vraag.

Aangevuld wordt dat de ISO 27001 is opgezet voor IT-systemen en de ISA/IEC 62443 voor OT-systemen. Overigens is de ISA/IEC 62.443-1 een set van documenten waarin niet alleen technische eisen van componenten zijn beschreven, maar waarin ook een plan is opgenomen om een hele organisatie cybersecure te maken. Waaronder ook de relatie tussen opdrachtgevers, systeemintegratie en leveranciers.

De normen waren er al voor de cybersecuritybeveiligingswet: binnen de ISO 27001 ben je vrij om allerlei beheersmaatregelen toe te voegen, voor zover jouw industrie dat vereist of voor zover je dat zelf van belang vindt.

Vraag 7:

Is een tunnelbeheerder verplicht om een gespecialiseerde partij in te schakelen?

Het is niet verplicht een gespecialiseerde partij in te schakelen. Met de juiste kennis kun je het zelf optuigen. Wel kan het toetsen door een expert verbeterpunten opleveren. Zeker iemand die het auditproces zelf uitvoert is een goede raadgever.

Vraag 8:

Een algemene – maatschappelijke – vraag:

Moeten we geen NL-breed-landelijk securitybeleid hebben? Eisen stellen aan voertuigen, verkeerslichten en bruggen?

Heel goed dat momenteel cybersecurity in tunnels de nodige aandacht heeft.

Veel geld gaat op aan het cybersecure maken van de infrastructuur/tunnel als object/asset zelf.

Er komen echter steeds meer connected voertuigen, Chinese auto's en bussen in Nederland. In Noorwegen is een issue ontdekt dat deze op afstand te stoppen zijn. Met meerdere van dit soort

voertuigen kan dit ook. Dit is een andere bedreiging en zo kunnen we veel blinde vlekken hebben. We willen anticiperen op nieuwe bedreigingen, maar hoe verleggen we de focus naar breder in het netwerk, zodat de risico's vollediger zijn?

Dit is één van de dingen die te weinig gedaan worden, veel zaken zijn versnipperd. Een platform als het KPT helpt om deze versnipperingen bij elkaar te brengen. Wat je ziet is dat bijvoorbeeld de RDW een type auto goedkeurt, maar niet nadenkt over mogelijke cybersecurity consequenties (is ook niet gevraagd). Er hoeft alleen gekeken te worden of de auto fysiek veilig is. Het is goed als er in bredere zin naar gekeken wordt, dat gebeurt steeds meer. Spreker noemt een praktijkvoorbeeld waarbij private overheidspartijen samenwerken om ons te beschermen tegen DDOS-aanvallen van buitenaf. In dat platform wordt kennis gedeeld om aanvallen met elkaar tegen te gaan.

Vraag 9:

Gesteld wordt dat bepaalde zaken 'slechts operationeel' zijn: als voorbeeld wordt een toltunnel genoemd. Maakt de NIS dit onderscheid? Voor een tunnelbeheerder van een toltunnel, kan het belang van tolheffing heel groot zijn. En privacy speelt hier ook een rol, er zijn wellicht gegevens van klanten geregistreerd.

Geadviseerd wordt om vanuit je risicoanalyse je eigen proportionaliteit te bepalen. Nooddeuren bijvoorbeeld moeten het altijd blijven doen, dit kan levensbedreigend zijn en dat gaat altijd voor andere prio's. Als een tolpoortje even open moet staan, hebben we daar niet zoveel pijn van.

Opmerking/vraag 10:

Binnen een risico-gestuurde aanpak is een hack één van de risico's waardoor de tunnel niet veilig is, net als slecht onderhoud, of uitvallende onderdelen. Het totaal aan maatregelen bepaalt het risico op uitval.

Goede toevoeging.

Vraag 11:

Is het ook duidelijk voor opdrachtgever/nemer wanneer CSIR2.0 (2.4) en CSIR3.0 (3.4) gebruikt moet worden? CSIR3.0 (3.4) is primair bruikbaar gemaakt voor alle BAW (Bestuursakkoord Water) partners. Is de tunnel 2.0 (2.4)?

Dit is typisch iets Nederlands, er zijn veel varianten van CSIR, sommige daarvan zijn toepasbaar gemaakt voor bepaalde doelgroepen. De vorige variant is iets generieker over tunnels etc. Versie 3.0 is niet per definitie een vervanger, meer een aanvulling.

Rode draad: beheersmaatregelen en andere zaken zijn relatief uniform, maar vandaag de dag meer toepasbaar per sector. Het zou mooi zijn een tunnelvariant te hebben.

Vraag 12:

Er wordt veel gesproken over de ISO 27001, dat is voornamelijk de organisatorische sturing. De normen IEC 62443 zijn vooral bruikbaar voor een scada en PLC-omgeving.

Tendens is de twee werelden meer bij elkaar te brengen. Vroeger was het meer OT gerelateerd, nu wordt gekeken naar verschillende normen en hoe die aan te vullen. De puzzel wordt steeds groter en complexer en alle puzzelstukjes zijn nodig.

Per sector zijn er verschillende NEN-normen. Het is belangrijk deze samen te brengen en bewustwording te creëren. ISO 27001 als framework is aangegeven om antwoord te geven op de vraag hoe je laagdrempelig kan beginnen met compliance. Met andere normen kan je vervolgens de diepte in op de individuele beheersmaatregelen.

Het webinar werd afgesloten met dank aan de sprekers en alle deelnemers.