Cybersecurity tunnels

Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Over cybersecurity is weliswaar veel informatie beschikbaar, maar vaak is het moeilijk hierin de juiste weg te vinden en goede afwegingen te maken. Het COB-netwerk heeft daarom voor (tunnel)beheerders een handreiking over cybersecurity opgesteld. Hiermee kan de beheerder de digitale weerbaarheid van zijn object beoordelen en zijn processen op het gebied van cybersecurity optimaliseren.

Gezien de snelle ontwikkelingen op het gebied van cybersecurity is de handreiking opgezet als digitaal groeiboek. Hierdoor kan de inhoud bijvoorbeeld worden aangevuld met specifieke aspecten voor het bestuurlijke kader en voor andere projectfases, zoals het ontwerp.

De handreiking is gratis online te raadplegen op
www.cob.nl/groeiboek/cybersecurity

Cybersecurity tunnels

Handreiking voor (tunnel)beheerders

Hoewel de handreiking gericht is op de (tunnel)beheerder, is de inhoud breed toepasbaar en biedt de handreiking informatie voor alle betrokken partijen binnen de tunnelsector en voor alle projectfases.

Beheerders van tunnels en andere objecten willen dat het object veilig gebruikt kan worden en dat dit ook in de toekomst zo blijft. Cyberaanvallen kunnen enorme schade met zich meebrengen, en dan gaat het niet alleen om kosten. De bedrijfscontinuïteit van vitale en niet-vitale processen kan grote maatschappelijke gevolgen hebben, waarbij ook de veiligheid van mensen in het geding kan zijn.

Het doel van deze handreiking is de (tunnel)beheerder kennis te laten nemen van de verschillende aspecten van cybersecurity. In de handreiking wordt een risicogestuurde aanpak beschreven die de (tunnel)beheerder in staat stelt de weerbaarheid van zijn object te beoordelen en zijn processen zodanig te optimaliseren dat tijdig de juiste maatregelen worden genomen om cybersecurity-incidenten te voorkomen of te beheersen en eventueel opgetreden effecten bij incidenten te mitigeren. De aanpak bestaat uit zes stappen die telkens herhaald worden:

1. **Inventariseren van de situatie/het ontwerp**
   De basis voor het inventariseren van de situatie en de te definiëren maatregelen is het concept van een integrale gelaagde beveiliging, *defense in depth*. Elke beveiligingslaag vertegenwoordigt een deel van het geheel. Omdat de onderdelen per laag verschillen, zijn ook de te nemen maatregelen verschillend. Het nemen van verschillende maatregelen zorgt ervoor dat een zwakte in de ene laag gecompenseerd kan worden door een maatregel in een andere laag. Door voor elke laag een adequate beveiliging te creëren, ontstaat een beveiligingsconcept dat opeenvolgend zorgt voor de beveiliging van de kern. Het voordeel van deze stapeling van beveiligingslagen is dat de kans op een verstoring van het geheel kleiner wordt doordat er verschillende beveiligingen moeten falen om het geheel te doen falen.

2. **Opstellen van de risicoanalyse**
   Na de inventarisatie van alle onderdelen vindt de risicoanalyse plaats. Per dreiging wordt de kans op het optreden ervan bepaald en wordt berekend wat de gevolgschade is als het daadwerkelijk misgaat. De risico's die zijn geïnventariseerd, worden bij de risicoanalyse gekwantificeerd door de kans op optreden en de gevolgen daarvan te combineren: risico = kans x impact. Daarna wordt ook gekeken naar de mogelijke maatregelen.

3. **Keuze van de te nemen maatregelen**
   Uit de risicoanalyse volgt een lijst waaruit blijkt welke gevolgen bepaalde maatregelen hebben op het optreden van gebeurtenissen. Het nemen van de juiste (combinatie van) maatregelen, vergt een zorgvuldige afweging. In de handreiking worden maatregelen beschreven voor drie belangrijke thema's: de mens (taken, bevoegdheden, verantwoordelijkheden), de organisatie (procedures, assets, beheer en onderhoud) en de techniek (fysieke beveiliging, hardware, software).

4. **Evalueren van de restrisico's en acceptatie restrisico's**
   Zodra de maatregelen zijn geselecteerd, wordt opnieuw per onderdeel bekeken wat de (rest)risico's zijn als de maatregelen worden uitgevoerd: welk effect (inclusief de kans daarop) blijft over als alle beheersmaatregelen zijn genomen? Het restrisico moet bestuurlijk of op directieniveau worden geaccepteerd.

5. **Uitvoeren van de maatregelen**
   De geselecteerde maatregelen moeten uiteraard worden geïmplementeerd. Dit gebeurt onder verantwoordelijkheid van de directie; de juiste uitvoering is de verantwoordelijkheid van de beheerder. Het is bijvoorbeeld een taak van de beheerder om te bepalen wanneer en onder welke voorwaarden de implementatie kan plaatsvinden.

6. **Borgen cybersecurity**
   Een belangrijk en vaak onderbelicht aspect is het documenteren van de maatregel(en). Na de implementatie moeten maatregelen in de organisatie geborgd worden om het bereikte niveau van cybersecurity te handhaven. Het is de verantwoordelijkheid van de beheerder om dit proces te leiden. Voor niet-technische aspecten (organisatie, personeel, procedures) kan er bijvoorbeeld controle door eigen medewerkers plaatsvinden of een externe auditor worden ingeschakeld. Omdat de techniek met betrekking tot cybersecurity specialistisch is, is het van groot belang dat de borging hiervan bewaakt wordt door cybersecurityspecialisten. Uiteraard in opdracht van de tunnelbeheerder en het bevoegd gezag. Voor uitbesteed werk is het van groot belang dat de externe partij alle procedures en maatregelen volgt die voor de interne organisatie gelden.

De handreiking is gratis online te raadplegen op
www.cob.nl/groeiboek/cybersecurity

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik