

Cybersecurity lifecycle

Nederland kent een uitgebreide weg- en waterinfrastructuur, waarvan digitalisering en technologische vooruitgang essentiële onderdelen zijn. Daarom is cybersecurity een onmisbaar aspect geworden in de lifecycle van deze infrastructuur. Van planning en ontwerp tot exploitatie en onderhoud, in elk stadium moet rekening worden gehouden met potentiële cyberdreigingen. Dit om de veiligheid, betrouwbaarheid en continuïteit van kritieke voorzieningen te waarborgen.

Het is cruciaal om vanaf de eerste stadia van infrastructuurontwikkeling cybersecurity te integreren in het ontwerp- en planningsproces. Potentiële risico's dienen te worden geïdentificeerd en robuuste beveiligingsmaatregelen geïmplementeerd om cyberincidenten te voorkomen. Dit in overeenstemming met het belang van de betreffende infrastructuur. Bij Hudson Cybertec zien we dat als in dit stadium geen duidelijke onderbouwing komt voor de classificatie van het object, dit in de latere fasen leidt tot onvoorziene risico's en extra kosten. Een gedegen en onderbouwde inschatting van de classificatie en het benodigde cybersecurity-weerstands niveau is dan ook essentieel. Door vanaf het begin cybersecurity mee te nemen, kunnen ontwerpers en ingenieurs ervoor zorgen dat systemen voor verkeersmanagement, bruggen, sluizen en tunnels op het juiste niveau weerbaar zijn tegen cyberdreigingen.

Tijdens de bouw en implementatie van infrastructuurprojecten is een zorgvuldige controle van de digitale componenten cruciaal. Dit omvat het beveiligen van de software en hardware, en het trainen van personeel in best practices voor cybersecurity en zorg voor de juiste procedures. Deze maatregelen kunnen de kans op cyberincidenten tijdens de bouwfase minimaliseren, wat essentieel is om vertragingen en extra kosten te voorkomen.

Eenmaal operationeel moeten weg- en waterinfrastructuur voortdurend worden onderhouden om cyberbeveiligingsrisico's te beheersen. Dit is essentieel om te kunnen reageren op nieuwe dreigingen. Bij afloop van contracten is een goede overdracht van de verantwoordelijkheid voor cybersecurity van groot belang. Daarbij dient niet alleen de vertrouwelijke informatie over het object veilig te worden gedeeld, maar moet ook het beheer van de digitale infrastructuur naadloos worden overgedragen aan de nieuwe onderhoudspartij.

Door cybersecurity gedurende de gehele lifecycle centraal te stellen, kan de integriteit, beschikbaarheid en veiligheid van essentiële infrastructuur worden gewaarborgd.

Jeroen van Schijndel

Technisch consultant, Hudson Cybertec

