

Een veilig datacenter begint met een goed beveiligd terrein. Heeft u gedacht aan deze 7 veiligheidsfactoren?

Datacenters vormen het hart van de digitale infrastructuur. Onze huidige manier van leven is ervan afhankelijk. Daarom is het zaak dat datacenters goed beveiligd worden. Dat begint bij de beveiliging van het terrein. In dit blog legt Robbert van Ham, Productmanager bij Heras, uit welke factoren een rol spelen. En hoe u het terrein van uw datacenter voorbereidt op diverse beveiligingsrisico's.

Lorem Datacenters spelen een vitale rol in ons bestaan, daarom is het belangrijk dat ze 24/7 optimaal beveiligd zijn. Om de meest effectieve beschermingswijze te bepalen, moeten we eerst de beveiligingsbehoefte achterhalen. Dat doen we door een aantal vragen te beantwoorden en mogelijke scenario's uit te denken.

1. Voldoet bestaande beveiliging?

Allereerst kijken we naar al aanwezige beveiliging. We onderzoeken of eventueel bestaande oplossingen uw datacenter voldoende bescherming bieden. En of de beveiliging klopt als geheel. Dat wil zeggen: zijn er zwakke punten? En is het terrein ingedeeld in sluitende veiligheidszones?

2. Het gebruik in kaart brengen

Daarnaast is het belangrijk om te weten hoeveel bewegingen er dagelijks op uw terrein plaatsvinden. Hoeveel bezoekers krijgt u, hoeveel medewerkers zijn er dagelijks en hoeveel leveranciers rijden er af en aan? Als we die bewegingsstromen in kaart hebben gebracht, onderzoeken we aan welke vereisten de beveiligingsoplossingen moet voldoen.

3. De toegang onder controle

Een belangrijk onderdeel van de beveiliging is de toegangsverlening. Wie komt het terrein op? Hoe weet u ten alle tijden wie zich allemaal op het terrein bevindt? Moeten mensen zich van tevoren aanmelden? Is er bijvoorbeeld behoefte aan een sluis waarin mensen gescreend worden? En welke toegangsooplossingen passen daarbij?

4. Een gepaste uitstraling

Vervolgens bespreken we welke uitstraling de beveiliging moet hebben. Moeten de beschermingsmiddelen afschrikken? Of ontvangt u regelmatig bezoekers in uw datacenter en wilt u een nette open uitstraling behouden? Of is uw datacenter juist erg onopvallend en wilt u die uitstraling niet verstoren door zeer zware beveiligingsoplossingen?

Bij verschillende uitgangspunten passen verschillende oplossingen. Wilt u maximaal afschrikken, dan gaan we bijvoorbeeld voor hoge staalplaathekken met prikkeldraad. Zoekt u naar een veilige oplossing met een vriendelijkere uitstraling, dan zetten we bijvoorbeeld onopvallende camera's in en een spijlenhekwerk waarin detectie op basis van trillingen verstopt zit.

5. Oog voor de omgeving

Daarnaast hebben we aandacht voor de ligging van uw datacenter. Welke gevolgen hebben omgevingsfactoren op de veiligheid van uw terrein? Ligt er bijvoorbeeld water dat een natuurlijke barrière tegen indringers vormt? Is er een woonwijk in de buurt die de maximale hoogte van uw hekwerk beperkt? Of grenst uw datacenter aan wegen die het potentiële indringers gemakkelijk maken uw terrein te benaderen?

6. Optimale integratie met aanvullende beveiliging

We zoeken altijd naar optimale aansluiting bij uw overige beveiligingsmaatregelen. We houden rekening met de alarmopvolging door bijvoorbeeld een externe meldkamer. We zorgen dan dat de beveiligingsmaatregelen indringers vertragen zodat beveiligers tijd hebben om te reageren. En als er beveiligers aanwezig zijn op uw terrein, richten we een portiersloge in met beeldschermen waarop zij het hele terrein overzien.

7. Rekening houden met alle scenario's

We zetten bovendien op een rij tegen welke scenario's uw terreinbeveiliging bestand moet zijn. Zijn er in het verleden veiligheidsinbreuken geweest? Welke scenario's zijn er redelijkerwijs te verwachten? En wat betekent dat voor de beveiliging van uw terrein? Sommige datacenters zijn bijvoorbeeld gevoelig voor activistische uitingen. Andere moeten bestand zijn tegen extreme situaties, zoals voertuigen die met hoge snelheid op de afbakening inrijden. In dat geval kiezen we voor 'crash-rated' oplossingen of roadblocks.

Combineer alle factoren voor een gepaste oplossing

De beveiliging van uw datacenter begint bij uw terrein. En daar komt dus heel wat bij kijken! In dit blog las u slechts een paar van de vele factoren die een rol spelen. Samen bepalen deze factoren welke oplossingen bij uw datacenter passen. In een volgend blog leest u meer over die oplossingen. Daarin geeft mijn collega Jan van Putten voorbeelden van drie beveiligingsscenario's die verschillen in zwaarte.