DIGITAL REALTY

Whitepaper

Dit is waarom fysieke security van datacenters net zo belangrijk is als cybersecurity

Introductie

In ons digitale tijdperk vormen IT-systemen de ruggengraat van vrijwel elke organisatie. Datacenters zijn de fysieke locatie waar de IT systemen staan met belangrijke software en waar gevoelige bedrijfsgegevens zijn opgeslagen. Datacenters zijn daarom al langere tijd een doelwit voor cybercriminelen. Gelukkig zijn steeds meer organisaties zich ervan bewust dat ze hun cybersecurity op orde moeten hebben om cybercriminelen te weren en hun gevoelige bedrijfsgegevens te beschermen. En dat is maar goed ook, want in 2021 hebben gemiddeld meer dan 10% van Nederlandse organisaties al te maken gehad met een cybersecurity incident waardoor de ICT niet meer te gebruiken was. Vooral de gezondheidszorg en de financiële sector hebben veel last gehad.

Er is veel aandacht voor de digitale kant van cybercrime waardoor organisaties zich minder bewust zijn van de fysieke aspecten van cybercrime. Denk hierbij aan Social Engineering, waarbij hackers zich voordoen als medewerkers van een bedrijf om fysieke toegang te krijgen tot systemen, waarna ze vanuit die systemen hun cybercrime kunnen voortzetten.

Omdat de fysieke security van datacenters vaak onderbelicht is, richten we ons in deze whitepaper op de verborgen wereld van fysieke beveiliging bij datacenters. Zo gaan we dieper in op de fysieke bedreigingen wanneer een datacenter niet goed beveiligd is en bespreken we welke fysieke beveiligingslagen van belang zijn om deze bedreigingen te voorkomen. We sluiten af met de technologische ontwikkelingen en trends in fysieke security van datacenters.

Dit zijn de meest voorkomende fysieke bedreigingen voor datacenters

Datacenters staan bloot aan verschillende bedreigingen die de fysieke veiligheid en beschikbaarheid van gegevens in gevaar kunnen brengen. We bespreken de meest voorkomende fysieke bedreigingen en de bedreigingen waar u wellicht nog niet eerder bij stilgestaan hebt.

Menselijke fouten

Hoe goed u uw medewerkers ook traint, fouten maken blijft menselijk. Denk aan situaties waarin medewerkers hun toegangspas verliezen of deze vergeten in te leveren bij vertrek, een deur open laten staan of per ongeluk de verkeerde kabel lostrekken (in tegenstelling tot hackers die dit met opzet doen). Het gevaar van deze menselijke fouten is dat het makkelijker wordt voor ongeautoriseerde personen om een datacenter te betreden, schade aan te richten en data met vertrouwelijke informatie te stelen die opgeslagen staan op een server.

Datadiefstal door eigen medewerkers

Het is voor een medewerker vaak eenvoudiger om data te stelen dan voor een cybercrimineel. Voor een medewerker zit de uitdaging hem enkel nog in het ongezien wegloodsen van de gevoelige bedrijfsgegevens. Waarom stelen medewerkers deze data? Dit kan verschillende oorzaken hebben. Zo kan een medewerker data doorverkopen aan hackers of concurrenten. Daarnaast kan het ook gaan om een ontevreden medewerker die wraak wil nemen op zijn of haar werkgever. Een andere oorzaak voor het stelen van data is dat een medewerker bedreigd wordt of dat één van hun naasten bedreigd of zelfs gegijzeld wordt.

Natuurrampen

Natuurrampen kunnen desastreuze gevolgen hebben voor datacenters. Denk bijvoorbeeld aan datacenters met het risico op waterschade door overstromingen en orkanen. Daarnaast is de hardware in datacenters vaak gevoelig voor extreme temperaturen en vochtigheid. Als een datacenter niet de juiste koeling en luchtregeling heeft, kan dit problemen als downtime en kortere levensduur veroorzaken. En wanneer een datacenter niet goed is uitgerust tegen brand, kan dit zich eenvoudig door een datacenter verspreiden en onomkeerbare schade aan de opslagruimte veroorzaken. De gevolgen? Downtime, dataverlies en kosten voor de aanschaf van nieuwe systemen.

Werkzaamheden

Wanneer er graafwerkzaamheden in de buurt plaatsvinden, kan dit bijvoorbeeld stroomuitval veroorzaken. Wanneer telecommunicatielijnen geraakt worden, kunnen verbindingen met de buitenwereld verloren gaan. Of het nu gaat om werkzaamheden of een natuurramp, datacenters die niet goed zijn uitgerust met back-up apparatuur en generatoren zijn kwetsbaar voor stroomuitval. Datacenters kunnen niet werken zonder connectiviteit en stroom, dus stroomuitval vormt een grote bedreiging voor de continuïteit van bedrijfsprocessen.

De fysieke beveiliging van datacenters

Om fysieke bedreigingen van datacenters te voorkomen, is een robuuste fysieke beveiliging nodig. Organisaties die een eigen (privaat) datacenter hebben, moeten enorme kosten maken om net zo goed beveiligd te zijn als commerciële datacenters. Er bestaan beveiligingsstandaarden voor hoe de fysieke beveiliging moet worden geregeld om als “professioneel” gezien te worden. We lichten hiervoor de belangrijkste aspecten toe.

Beveiliging en omheining van het terrein

Het terrein waarop het gebouw van een datacenter staat is omringd door hekken. Deze hekken kunnen voorzien zijn van toegangscontrolesystemen zoals kaartlezers.Daarnaast wordt er vaak een bewaker ingezet die zich bevindt in een kiosk en toegang kan geven via een slagboom. Op deze manier is een datacenter in staat om de komst van medewerkers en bezoekers te reguleren.

Cameratoezicht

Cameratoezicht voor real-time surveillance wordt gebruikt om activiteiten rondom toegangspunten van een datacenter vast te leggen. Dit dient niet alleen als afschrikmiddel, maar biedt ook een audittrail (een systeem dat automatisch stapsgewijs alle uitgevoerde activiteiten voor een onderzoek gedetailleerd vastlegt en opslaat) in het geval van een beveiligingsincident. Daarnaast worden er binnen het datacenter ook camera’s gebruikt om goed in de gaten te houden wat er gebeurt in de verschillende ruimtes.

Een strenge toegangscontrole binnen het gebouw

Medewerkers dragen vaak smartcards die toegang geven tot specifieke gebieden binnen het datacenter. Deze kunnen worden ingetrokken als een medewerker de organisatie verlaat of zijn autorisatie verliest. Deze toegangsrechten kunnen worden ingesteld op basis van tijd, waardoor medewerkers alleen toegang hebben tot het datacenter tijdens hun normale werkuren. Dit beperkt de kans op ongeoorloofde toegang buiten reguliere werktijden.

Daarnaast wordt er ook hier gebruikgemaakt van biometrische identificatie in de vorm van vingerafdrukscanners en gezichtsherkenningssystemen. Deze methoden zorgen voor een zeer nauwkeurige vorm van identificatie en verkleinen de kans op ongeautoriseerde toegang.

Toegangspanelen voor bijvoorbeeld deuren kunnen ook worden beveiligd met persoonlijke identificatienummers (PIN) of wachtwoorden. Dit voegt een extra laag van beveiliging toe en vereist dat geautoriseerde personen zowel een fysieke kaart als een persoonlijk identificatiemiddel gebruiken.

Alarm- en detectiesystemen

Een Very Early Smoke Detection Apparatus (VESDA) is een geavanceerd rookdetectiesysteem dat is ontworpen om vroegtijdig een waarschuwing te geven voor mogelijke brandincidenten. In tegenstelling tot traditionele rookmelders (die reageren op zichtbare rookdeeltjes), gebruiken VESDA-systemen een geavanceerde technologie om rook te detecteren in de vroegste stadia, vaak nog voordat er sprake is van een kritieke situatie.

Daarnaast is het met de nieuwste alarm- en detectiesystemen mogelijk om via speciale sensoren zeer kleine gewichtsveranderingen te detecteren. Een medewerker of bezoeker wordt door sensoren gewogen voordat hij of zij een bepaalde ruimte ingaat en wanneer deze persoon de ruimte verlaat. Wordt er gewichtsveranderingen gedetecteerd? Dan gaat het alarm af en wordt deze persoon gecontroleerd door bewakers.

Het ontwerp van een datacenter

Door al deze beveiligingslagen te implementeren, kunnen datacenters zich beter beschermen tegen fysieke bedreigingen. Het ontwerp van een datacenter is dan ook heel bewust opgebouwd uit deze verschillende beveiligingslagen:

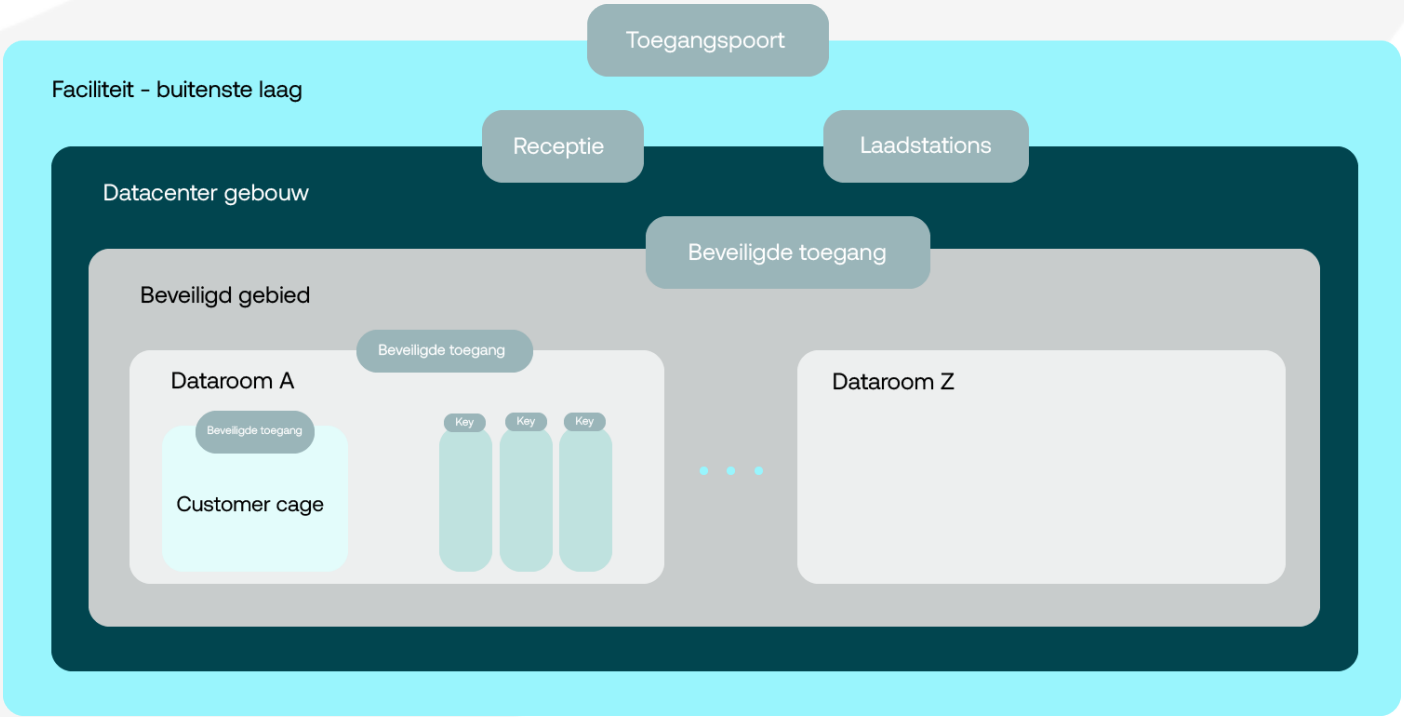
1. Faciliteit - buitenste laag: Door de beveiligde toegangspoort betreedt een medewerker of bezoeker het terrein waarop het gebouw van het datacenter staat.

2. Datacenter gebouw en receptie: Een medewerker of bezoeker treedt het gebouw binnen en meldt zich bij de receptie en krijgt een toegangspas of gaat onder begeleiding verder. Er wordt een logboek bijgehouden om vast te leggen wie er binnenkomt en vertrekt.

3. Beveiligd gebied: Vervolgens treedt de bezoeker of de medewerker het datacenter gebouw binnen. Deze laag heeft beveiligde deuren en sluizen om de toegang van personen te reguleren. Deze deuren kunnen biometrische scanners, kaartlezers, of andere toegangscontrolesystemen bevatten. Sluizen helpen ook bij het voorkomen van ongeautoriseerde toegang doordat slechts één deur tegelijk opengaat. Dit minimaliseert het risico van ongeautoriseerde personen die binnenglippen.

4. Data rooms: In de volgende laag bevinden zich de streng beveiligde datarooms met een beveiligde customer cage waarin er ruimte is voor meerdere servers van een specifieke organisatie.

5. Customer racks: In de data rooms staan µ customer racks die elk afzonderlijk afgesloten en beveiligd zijn. In de racks staat de computer-, netwerk- en opslagsystemen waarop de IT systemen actief zijn. Deze racks kunnen ook weer met extra fysieke veiligheidsmaatregelen uitgerust worden, zoals camera's en biometrische identificatie.



Technologische ontwikkelingen en trends in fysieke security

Welke opkomende technologieën en trends zijn er die de fysieke beveiliging van datacenters transformeren?

- **Betere beveiligingsstandaarden dankzij NEN-EN 50600**: steeds meer datacenters werken met de NEN-EN 50600 normenreeks om zo effectief mogelijk datacenters en serverruimtes op te zetten. Deze normenreeks geeft onder andere inzicht in het ontwerpproces: van het bepalen van een strategie tot het uitvoeren ervan.
- **Kunstmatige intelligentie (AI) en machine learning**: deze technologieën maken geavanceerde beveiligingsanalyses mogelijk, waardoor realtime bedreigingsdetectie en -preventie verbeteren. Denk aan objectherkenning, biometrische identificatie en integratie van sensoren en IoT-apparaten.
- **Zero-trust-beveiliging**: een beveiligingsmodel dat de traditionele beveiliging verlegt en ervoor zorgt dat niets als vanzelfsprekend wordt beschouwd in een tijd waarin cyberdreigingen evolueren.
- **Nano drone security**: deze compacte drones hebben geavanceerde beeldtechnologie en zijn vrijwel niet detecteerbaar.
- **Bescherming tegen usb-sticks**: een extra laag materiaal om een rack of cage heen die zodanig klein is dat er geen usb-stick doorheen past.

Deze technologische trends bieden nieuwe mogelijkheden om datacenters te beveiligen en te anticiperen op toekomstige uitdagingen. Goed beveiligde datacenters als die van Digital Realty passen dit soort nieuwe technologieën toe om te kunnen garanderen dat ze goed beveiligd blijven.

Zo helpt Digital Realty

Door uw fysieke beveiliging van uw datacenter uit te besteden, kunt u zich meer richten op uw kernactiviteiten en strategieën, waardoor u zich minder zorgen hoeft te maken over de complexiteiten van fysieke beveiliging. Wat zijn de belangrijkste redenen om uw fysieke beveiliging uit te besteden aan Digital Realty? We zetten het voor u op een rij:

- **Minder hoge kosten**: wanneer u uw eigen datacenter fysiek wilt beveiligen, kan dit hoge kosten met zich meebrengen. Het is een hele investering om geavanceerde beveiligingsinfrastructuur, zoals biometrische scanners, toegangscontrolesystemen, bewakingscamera's, en beveiligde deuren aan te schaffen. Daarnaast kan dit ook erg ingewikkeld zijn om uit te zoeken.
- **Geen tijdrovende installaties en configuraties:** u moet niet alleen betalen voor de aanschaf van systemen, maar ook voor de installatie en configuratie ervan. Het onderhouden van geavanceerde beveiligingssystemen vereist regelmatig inspecties, software-updates en reparaties.
- **Werven en trainen van beveiligingspersoneel:** Het aannemen en trainen van beveiligingspersoneel dat bekwaam is in het beheren van geavanceerde beveiligingstechnologieën kan kostbaar zijn. Bovendien moet u rekening houden met doorlopende salarissen, voordelen en training van dit personeel.
- **Voldoen aan de wet- en regelgeving**: Datacenters moeten voldoen aan strikte regelgeving op het gebied van gegevensbeveiliging. Het implementeren en handhaven van maatregelen om aan deze regelgeving te voldoen, zoals GDPR of andere lokale wet- en regelgeving, kan extra kosten met zich meebrengen.
- **Schaalbaarheid en flexibiliteit:** De behoefte aan schaalbaarheid en flexibiliteit in beveiligingsoplossingen kan leiden tot hogere kosten. Als de vraag naar beveiligingsfuncties toeneemt of afneemt, kan het aanpassen van interne systemen complex en duur zijn. Digital Realty kan gemakkelijk opschalen of afschalen op basis van de behoeften van de organisatie, waardoor we flexibeler zijn dan interne beveiligingsoplossingen.

Digital Realty is gespecialiseerd in het bieden van beveiligingsdiensten en heeft vaak toegang tot de nieuwste technologieën en beste praktijken op het gebied van beveiliging. Door beveiliging uit te besteden, profiteert een organisatie van de expertise van onze gespecialiseerde diensten.

Meer weten?

Wilt u meer weten over het uitbesteden van de fysieke beveiliging van datacenters? Bent u benieuwd hoe Digital Realty hierbij kan helpen? Bel dan gerust naar +31 (0)20 880 77 00 of stuur een e-mail naar salesnl@digitalreality.com. Wij leren u graag kennen!