BEVEILIGINGS INGANGEN

TRENDRAPPORT

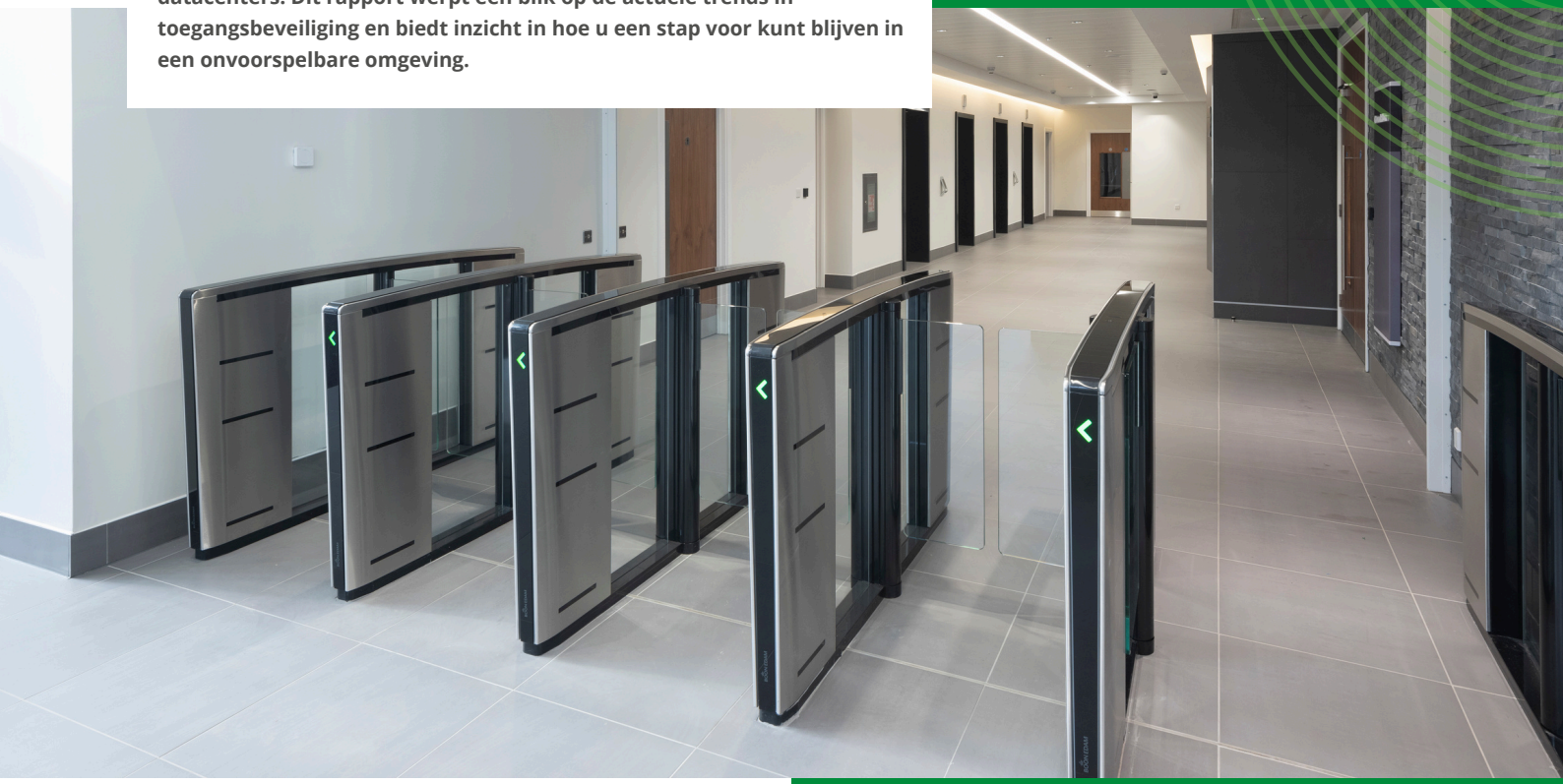
2025.

BEVEILIGINGSOPLOSSINGEN VOOR DE INKOM VAN MORGEN.

BOON EDAM
YOUR **ENTRY** EXPERTS.

INTRODUCTIE.

De vereisten voor de beveiliging van gebouwen zijn aanzienlijk toegenomen in een wereld die steeds meer gekenmerkt wordt door polarisatie, technologische vooruitgang, extremisme en een groeiend wantrouwen. Sectoren die voorheen slechts een beperkte beveiliging nodig hadden, worden vandaag geconfronteerd met verhoogde risico's. De bedreigingen beperken zich niet langer tot overheidsgebouwen of datacenters. Dit rapport werpt een blik op de actuele trends in toegangsbeveiliging en biedt inzicht in hoe u een stap voor kunt blijven in een onvoorspelbare omgeving.



"Terwijl de samenleving streeft naar drempelloze en gastvrije omgevingen, dwingt de harde realiteit ons tot robuuste beveiligingsmaatregelen die toegankelijkheid en veiligheid met elkaar in evenwicht brengen."

Douwe Jolles
PRODUCTMANAGER - DOOR SYSTEMS

INDEX

1 CYBER SECURITY ONTMOET FYSIEKE BEVEILIGING.

Het combineren van cyber security met fysieke beveiliging luidt een nieuw tijdperk in van beschermingsstrategieën voor organisaties in uiteenlopende sectoren, zoals datacenters, overheidsgebouwen, kritieke infrastructuur en hoofdzetels van bedrijven. In onze verbonden wereld draait beveiliging niet langer enkel om het blokkeren van ongeoorloofde toegang of het beschermen van digitale systemen – het gaat om de naadloze combinatie van beide in één omvattende en uniforme verdedigingsstrategie.

Zero Trust-architectuur

Dit beveiligingsmodel steunt op het principe van 'least privilege' (minimale toegangsrechten). Het houdt in dat gebruikers en toestellen enkel toegang krijgen tot de specifieke bronnen die zij nodig hebben voor hun rol – en niets meer. Zero Trust maakt het aanzienlijk moeilijker voor kwaadwilligen om systemen te compromitteren of gevoelige gegevens te ontvreemden, doordat het de toegangspunten strikt beperkt. Deze aanpak is cruciaal in omgevingen waar uiterst gevoelige en waardevolle informatie wordt verwerkt, zoals datacenters. In zulke omgevingen moet elke interactie met fysieke én digitale middelen worden geverifieerd op basis van vooraf gedefinieerde toegangsrechten.

Cyberveiligheid naar een hoger niveau tillen

Nieuwe Europese regelgeving verandert de normen voor cyberveiligheid, met directe gevolgen voor inkombeveiliging en toegangscontrolesystemen. De NIS2-richtlijn en de Cyber Resilience Act (CRA) zijn beide gericht op het versterken van de cyberveiligheid, maar leggen de focus op verschillende aspecten.

De NIS2-richtlijn is bedoeld om essentiële diensten en kritieke infrastructuur beter te beveiligen. Sectoren zoals energie, gezondheidszorg en transport zullen daarom strengere maatregelen op het vlak van cyberveiligheid moeten invoeren. Deze omvatten onder meer een versterkt risicobeheer, een betere beveiliging van de toeleveringsketen en een verscherpte meldingsplicht bij cyberincidenten. Organisaties die tegen eind 2024 niet in regel zijn, riskeren zware geldboetes en reputatieschade.

De Cyber Resilience Act verplicht dat producten met digitale componenten – zoals toegangscontrolesystemen, IoT-compatibele beveiligingsdeuren, speedgates en tourniquetdeuren met digitale integraties – moeten voldoen aan verhoogde normen op het vlak van cyberveiligheid. Fabrikanten worden geacht beveiliging te integreren in het ontwerp van hun producten, evenals in het onderhoud en de continue updates ervan. Voor bepaalde risicovolle producten is bovendien een certificatie door een externe instantie vereist, nog vóór ze op de Europese markt gebracht mogen worden. Producten die aan deze normen beantwoorden, ontvangen een CE-markering, wat het voor bedrijven eenvoudiger maakt om conforme oplossingen te herkennen.

Samen vormen deze regelgevingen een nieuwe standaard voor cyberveiligheid. Ze zorgen ervoor dat zowel de infrastructuur als de fysieke producten die worden ingezet voor beveiliging, beter bestand zijn tegen digitale dreigingen.

Beveiligingsecosystemen

In het complexe beveiligingslandschap van vandaag moet het beveiligingsecosysteem van een gebouw een mix van hoge, middelhoge en lage beveiligingsmaatregelen integreren om tot een dynamische en onderling verbonden verdediging te komen. Elke beveiligingslaag vervult een specifiek doel: het gebouw veilig houden, waardevolle activa beschermen en tegelijk toegang verlenen waar dat nodig is.

Hoewel cybersecurity vaak de meeste aandacht krijgt in discussies over de bescherming van gevoelige omgevingen, is fysieke beveiliging minstens even belangrijk – zeker voor infrastructuren zoals datacenters. Wanneer iemand met kwaad opzet fysieke toegang verkrijgt tot een server, kan zelfs de meest geavanceerde firewall worden omzeild, met mogelijk catastrofale datalekken tot gevolg. Dit benadrukt hoe essentieel het is om fysieke en digitale beveiligingsoplossingen op elkaar af te stemmen.

Zones met een hoog beveiligingsniveau, zoals serverruimtes, vereisen geautomatiseerde fysieke beveiligingsoplossingen die geïntegreerd zijn met biometrische authenticatie en gecodeerde communicatieprotocollen. Deze maatregelen voorkomen ongeoorloofde toegang en ondersteunen de cybersecuritystrategie door snelle wijzigingen in toegangsrechten mogelijk te maken, waarmee bedreigingen in realtime kunnen worden beperkt.

Ruimtes met een gemiddeld beveiligingsniveau, zoals administratieve afdelingen, hebben baat bij technologieën zoals beveiligingspoortjes met geavanceerde sensoren. Deze garanderen vlotte toegang voor gemachtigd personeel en ontmoedigen ongeoorloofde pogingen. In zones met een lager beveiligingsniveau, zoals openbare onthaalruimtes, ligt de focus op esthetiek en toegankelijkheid, terwijl een basisbeveiliging wordt gegarandeerd via bewaakte toegangscontrolepunten.

Deze ecosysteembenadering weerspiegelt principes uit de cybersecurity, zoals multifactorauthenticatie. Net zoals digitale systemen gelaagd beveiligd zijn om gevoelige data te beschermen, vereisen fysieke omgevingen meerdere, elkaar aanvullende beveiligingslagen. Elke laag verzekert dat bij het falen van één verdedigingslinie, andere actief blijven om cruciale activa te beschermen.

Om fysieke beveiliging doeltreffend te houden, is het essentieel om cybersecurity-best practices te integreren. Dit omvat onder andere het gebruik van gecodeerde communicatieprotocollen, het uitvoeren van regelmatige software-updates en het inzetten van toegangscontrolesystemen die bestand zijn tegen cyberaanvallen.

Door een beveiligingsecosysteem te ontwerpen waarin digitale en fysieke beveiliging naadloos samenwerken, kunnen organisaties veilige en operationele omgevingen creëren die bestand zijn tegen de uitdagingen van vandaag. Deze aanpak biedt niet enkel een robuuste bescherming, maar ook een evenwicht tussen toegankelijkheid en veiligheid – en draagt zo bij aan een gastvrije omgeving.

“Indringers buiten houden is de eerste verdedigingslinie. Wanneer een indringer erin slaagt om via de toegangspunten een gebouw binnen te dringen, worden alle andere beveiligingsmaatregelen pas achteraf geactiveerd. Het voorkomen van een beveiligingsinbreuk begint dan ook bij de inkom.”

Security Operations Centre

Een Security Operations Centre (SOC) is een gecentraliseerde eenheid die instaat voor de realtime monitoring, detectie, analyse en respons op cyberveiligheidsdreigingen. Het voornaamste doel is om de beveiligingspositie van een organisatie te handhaven door netwerken, systemen, applicaties en gevoelige gegevens te beschermen tegen digitale dreigingen.

Een SOC is 24/7 actief om continue bewaking te verzekeren en het risico op datalekken, cyberaanvallen of ongeoorloofde toegang tot een minimum te beperken. Organisaties richten hun SOC in op basis van hun specifieke noden en beschikbare middelen. De meest voorkomende vormen zijn interne SOC's, die volledige controle bieden over alle beveiligingsactiviteiten, maar een aanzienlijke investering in personeel en technologie vergen. Daarnaast zijn er beheerde SOC's (of uitbestede SOC's), die worden gerund door externe dienstverleners met gespecialiseerde expertise.

2 EXPLOSIE- EN INSLAG WEERSTAND.

Het veranderende beveiligingslandschap leidt tot een toenemende vraag naar verbeterde gebouwbeveiliging in een bredere waaier aan sectoren. Traditionele sectoren zoals overheidsinstellingen, banken en datacenters hebben al lange tijd veiligheid hoog op de agenda staan. Vandaag zorgen nieuwe dreigingen ervoor dat ook andere sectoren – zoals mediabedrijven en commerciële organisaties – hun beschermingsmaatregelen aanzienlijk versterken.

Toenemende risico's zoals vandalisme, terrorisme, extremistische groeperingen en maatschappelijke polarisatie beïnvloeden de manier waarop gebouwen beveiligd worden. Explosie- en inslagbestendige materialen zijn uitgegroeid tot essentiële componenten van moderne beveiligingsoplossingen.

Materiaalinnovatie

Nu bedrijven steeds meer inzetten op het voorkomen van bedreigingen, krijgen explosie- en impactbestendige inkomoplossingen een hogere prioriteit. Het toenemend gebruik van geavanceerde materialen in gevelconstructies onderstreept de nood aan sterkere barrières om in te spelen op de veranderende veiligheidsrisico's.

Materialen zoals polycarbonaatlagen – gewaardeerd om hun lichte gewicht en slagvaste eigenschappen – versterkt staal en veiligheidsglas worden steeds vaker geïntegreerd in moderne beveiligingssystemen. Deze materialen zijn ontworpen om de energie van explosies of projectielen op te vangen en te verspreiden, waardoor ze duurzame barrières vormen die schade aanzienlijk beperken. Door samen te werken met specialisten in materiaalkunde integreren fabrikanten geavanceerde technologieën in hun toegangsoplossingen. Dit verhoogt de weerbaarheid tegen zowel doelgerichte aanvallen als onbedoelde impact.

Beveiligde inkomoplossingen worden ook ontwikkeld om krachtige inbraakpogingen te weerstaan, ongeacht of deze worden uitgevoerd met werktuigen of voertuigen. Componenten zoals anti-ramelementen, verstevigde kaders en geavanceerde verankeringssystemen zorgen voor een robuuste bescherming en vormen de eerste verdedigingslinie van een gebouw.

Daarnaast wint kogelwerend glas aan populariteit in sectoren die tot voor kort als laag risico werden beschouwd. Dit type glas is ontworpen om de energie van inslagen met hoge snelheid te absorberen en te verspreiden, en biedt zo essentiële bescherming tegen vandalisme, brandstichting en gewelddadige aanvallen.

Economische gevolgen van downtime

De financiële impact van verstoringen door explosies of geforceerde toegang kan bijzonder zwaar doorwegen en reikt vaak verder dan louter fysieke schade. Operationele onderbrekingen, verlies van materiaal of data en reputatieschade kunnen organisaties ernstig treffen – zeker in sectoren waar downtime een directe impact heeft op klantvertrouwen en omzet. Steeds meer organisaties geven dan ook prioriteit aan beschermende toegangsoplossingen als een essentieel onderdeel van hun beveiligingsstrategie. Ze erkennen daarbij de cruciale rol die deze systemen spelen in het waarborgen van de bedrijfscontinuïteit.

Balans tussen toegankelijkheid en veiligheid

In een samenleving die steeds meer inzet op openheid en toegankelijkheid, is het belangrijk om een zorgvuldig evenwicht te vinden tussen het creëren van gastvrije gebouwomgevingen en het aanpakken van dringende beveiligingsdreigingen. Dit evenwicht vraagt om innovatieve oplossingen die geavanceerde beveiligingsfuncties combineren met openheid en esthetiek. Organisaties moeten gebouwen ontwerpen die niet alleen veilig en veerkrachtig zijn, maar ook aansluiten bij bredere maatschappelijke waarden. Zo dragen ze bij aan een leef- en werkomgeving waarin mensen en eigendommen beschermd zijn – ook in een steeds onvoorspelbaardere wereld.

3

AI.

Kunstmatige intelligentie (AI) blijft een sleutelfactor binnen de wereld van beveiligde toegangsoplossingen. Hoewel AI soms als overgewaardeerd wordt bestempeld, blijft het transformerende potentieel ervan toenemen. Het verandert fundamenteel de manier waarop beveiliging benaderd en toegepast wordt.

Concreet toepasbare AI-oplossingen, zoals voorspellende analyses, dreigingsdetectie en de automatisering van tijdrovende processen, zijn van onschatbare waarde. Dankzij de capaciteit om grote hoeveelheden gegevens te verwerken en te interpreteren, is AI bijzonder geschikt voor het beheren van complexe locaties zoals luchthavens, ziekenhuizen en bedrijfsomgevingen. In dergelijke contexten levert AI geavanceerde inzichten en efficiëntie die essentieel zijn om veiligheid op schaal te garanderen.

Voorspellende analyse en detectie van bedreigingen

Een van de meest impactvolle toepassingen van AI binnen beveiliging situeert zich in voorspellende analyses en dreigingsdetectie. Traditionele beveiligingssystemen zijn vaak reactief van aard: ze treden pas in werking nadat een incident zich heeft voorgedaan. AI doorbreekt dit patroon door een proactieve benadering mogelijk te maken. Door toegangscontrolegegevens en andere beveiligingsinputs in realtime te analyseren, kunnen AI-gestuurde systemen patronen en afwijkingen herkennen die wijzen op een potentiële dreiging.

In plaats van te wachten tot menselijke operatoren deze signalen opmerken, markeren AI-systemen ze automatisch, bepalen ze de prioriteit op basis van het risiconiveau en leveren ze bruikbare inzichten aan. Dit resulteert in snellere reacties en stelt beveiligingsteams in staat om in te grijpen vóór een situatie uit de hand loopt.

WIST JE DAT?

De wereldwijde markt voor AI in cybersecurity naar verwachting zal groeien van 22,22 miljard euro in 2024 tot 52,81 miljard euro in 2029, met een samengestelde jaarlijkse groei (CAGR) van 19,02%*

*Mordor Intelligence. (2024). Rapport over kunstmatige intelligentie in de beveiligingsmarkt. Opgehaald van https://www.mordorintelligence.com/industry-reports/artificial-intelligence-in-security-market

AI-aangedreven innovaties in toegangsoplossingen

De integratie van AI in inkomoplossingen zoals tourniquetdeuren en beveiligingspoortjes luidt een nieuw tijdperk van intelligente beveiliging in. AI kan piekmomenten voorspellen, functionaliteiten dynamisch aanpassen en een efficiënte doorstroming garanderen zonder afbreuk te doen aan de veiligheid. Deze mogelijkheden versterken zowel de beveiliging als het gebruiksgemak, en zorgen voor een optimale gebruikerservaring die tegelijk voldoet aan de operationele vereisten.

Ook biometrische authenticatie heeft een nieuwe dimensie gekregen. Naast traditionele methoden zoals vingerafdruk- en gezichtsherkenning worden nu ook geavanceerde technieken zoals aderpatroonanalyse en hartslagherkenning toegepast bij streng beveiligde toegangen. Deze innovaties optimaliseren de toegangscontrole in gevoelige zones en garanderen tegelijk een vlotte doorstroming voor geautoriseerd personeel.

Duurzame innovatie

Machine learning-systemen vereisen aanzienlijke rekenkracht, waardoor hun energieverbruik en CO_2-voetafdruk zorgvuldig beheerd moeten worden. Het ontwikkelen van energie-efficiënte modellen, het optimaliseren van de infrastructuur en het inzetten van hernieuwbare energiebronnen zijn cruciale stappen om de ecologische voetafdruk van AI-technologieën te verkleinen. Door deze maatregelen prioriteit te geven, kunnen organisaties ervoor zorgen dat de vooruitgang van AI zowel technologische innovatie als milieubeheer ten goede komt.

Ethische toepassing

Machine learning-modellen moeten ontworpen en geïmplementeerd worden zonder vooroordelen. Vooroordelen binnen AI kunnen leiden tot subjectieve en onethische uitkomsten, wat ongelijkheden bestendigt en het vertrouwen in de technologie aantast. Om dit te vermijden, moeten organisaties prioriteit geven aan diverse en representatieve datasets, transparante algoritmen en voortdurende evaluatie. Tegelijk is het essentieel om beveiliging in evenwicht te brengen met privacyoverwegingen, zodat de zoektocht naar veiligheid geen inbreuk maakt op individuele rechten of persoonlijke levenssfeer.

Het menselijke element: beslissingen versterken met AI

Hoewel artificiële intelligentie een enorme kracht biedt, blijven mensen centraal staan in doeltreffende beveiligingsoplossingen. Betere beslissingen worden genomen wanneer inzichten uit machine learning worden gecombineerd met menselijk beoordelingsvermogen. De samenwerking tussen AI en menselijke expertise vormt een krachtig systeem dat in staat is om complexe beveiligingsuitdagingen aan te pakken. Er blijft immers een duidelijke terughoudendheid om volledig op AI te vertrouwen voor besluitvorming zonder menselijke supervisie om die beslissingen te valideren.

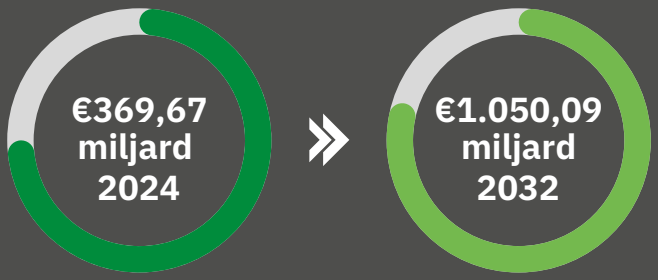
Uiteindelijk draait AI niet om het vervangen van mensen, maar om het versterken van hun mogelijkheden. Door routinetaken te automatiseren, de detectie van bedreigingen te verbeteren en de reactiemogelijkheden te optimaliseren, stelt AI beveiligingsteams in staat zich te focussen op hun kerntaak: het beschermen van mensen, eigendommen en omgevingen. Ondanks de vele voordelen vormt AI geen vervanging voor menselijke expertise. Beveiligingsprofessionals brengen kritisch denkvermogen, intuïtie en contextueel inzicht mee die AI niet kan evenaren. De meest doeltreffende beveiligingsstrategieën steunen dan ook op deze samenwerking tussen mens en AI, waarbij AI het zware werk van data-analyse en automatisatie voor zijn rekening neemt, terwijl mensen de inzichten interpreteren en weloverwogen beslissingen nemen.

4 DUURZAAMHEID.

De vraag naar duurzame en milieuvriendelijke oplossingen wordt steeds belangrijker in de beveiligingssector, aangezien organisaties meer verantwoordelijkheid willen opnemen op het vlak van milieubeheer. Hoewel beveiliging de primaire focus blijft, groeit het besef dat duurzaamheid een rol speelt in langetermijnstrategieën van ondernemingen. Steeds meer bedrijven zijn op zoek naar oplossingen die beveiligingsprestaties verzoenen met energie-efficiëntie en ecologische impact, wat wijst op een verschuiving naar een meer verantwoorde manier van zakendoen.

Echte duurzaamheid draait niet alleen om recycleren of hergebruik; ze begint bij het ontwerpen van producten die zó betrouwbaar zijn dat die stappen slechts secundair worden."

Amine Bouchareb
PRODUCTMANAGER - SECURITY ACCESS



In 2024 werd de wereldwijde markt voor groene bouwmaterialen geschat op ongeveer 369,67 miljard euro.

Naar verwachting zal dit bedrag in 2032 € 1.050,09 miljard bedragen, met een samengestelde jaarlijkse groei (CAGR) van 12,3%.

Het aanpassen van beveiligingsingangen

Retrofits vormen een duurzame en kostenefficiënte manier om bestaande beveiligingsingangen te moderniseren. Ze verhogen de veiligheid en efficiëntie zonder dat een volledige vervanging noodzakelijk is. Door de levensduur van installaties te verlengen, helpen retrofits afval te beperken en operationele onderbrekingen te minimaliseren.

We onderscheiden twee vormen van retrofits, elk afgestemd op specifieke behoeften en vereisten:

- **Een retrofit** verbetert de prestaties of functionaliteit van een bestaand systeem, zonder de kerncomponenten aan te passen. Denk bijvoorbeeld aan het vervangen van sensoren of het verfijnen van toegangscontrole. Zo kunnen organisaties inspelen op nieuwe vereisten, terwijl ze hun bestaande installatie behouden.

- **Een upgrade** gaat verder en houdt ingrijpende aanpassingen in op vlak van technologie, materiaal of functionaliteit. Dit resulteert vaak in een nieuwe productclassificatie. Voorbeelden zijn het integreren van geavanceerde technologieën of het vervangen van cruciale onderdelen om te voldoen aan strengere beveiligingsnormen.

Energie-efficiëntie en milieuvriendelijke materialen

Moderne beveiligingsproducten zijn vandaag uitgerust met energie-efficiënte motoren, IoT-componenten met een laag energieverbruik en slimme sensoren die hun werking afstemmen op realtime gebruik. Deze innovaties verlagen het energieverbruik en verhogen de algemene efficiëntie van beveiligingssystemen. Tourniquetdeuren dragen bovendien bij aan het reguleren van het binnenklimaat door luchtuitwisseling te beperken, wat hen bijzonder geschikt maakt voor groene bouwprojecten en energiezuinige certificeringen zoals LEED. Daarnaast worden niet-giftige materialen stilaan een standaard in het ontwerp van beveiligingsingangen.

Al deze elementen ondersteunen duurzaamheid en sluiten aan bij de doelstellingen van maatschappelijk verantwoord ondernemen. Zo kunnen bedrijven hun investeringen in beveiliging beter afstemmen op hun duurzaamheidsdoelstellingen.

Bouwen voor de lange termijn

Duurzame oplossingen beperken afval door de nood aan frequente vervangingen tot een minimum te herleiden. Bedrijven nemen afstand van snelle oplossingen en kiezen voor strategieën die levensduur, betrouwbaarheid en minimale milieu-impact centraal stellen. Het gaat hierbij niet alleen om de uitdagingen van vandaag, maar om bouwen met het oog op de komende honderd jaar en daarna. Investeren in vakkundig vervaardigde, hoogwaardige producten garandeert langdurige prestaties, optimale beveiliging en een naadloze gebruikerservaring die de tand des tijds doorstaat.

5 HET BURENEFFECT.

Beveiliging beheren in gebouwen met meerdere huurders

In gebouwen met meerdere huurders wordt de beveiligingsbehoefte van één organisatie vaak beïnvloed door de activiteiten van naburige bedrijven. Of u nu gebouwbeheerder of huurder bent, het is essentieel om rekening te houden met de impact van omliggende ondernemingen en gebruikers op uw eigen werking. Beveiligingsuitdagingen beperken zich niet langer tot afzonderlijke organisaties. Een incident bij een aangrenzende huurder – zoals criminaliteit, betogingen of andere verstoringen – kan rechtstreeks gevolgen hebben voor uw veiligheid. Dit fenomeen staat bekend als 'het bureneffect' en benadrukt het belang van samenwerking in moderne gedeelde omgevingen.

Balans vinden tussen uiteenlopende behoeften

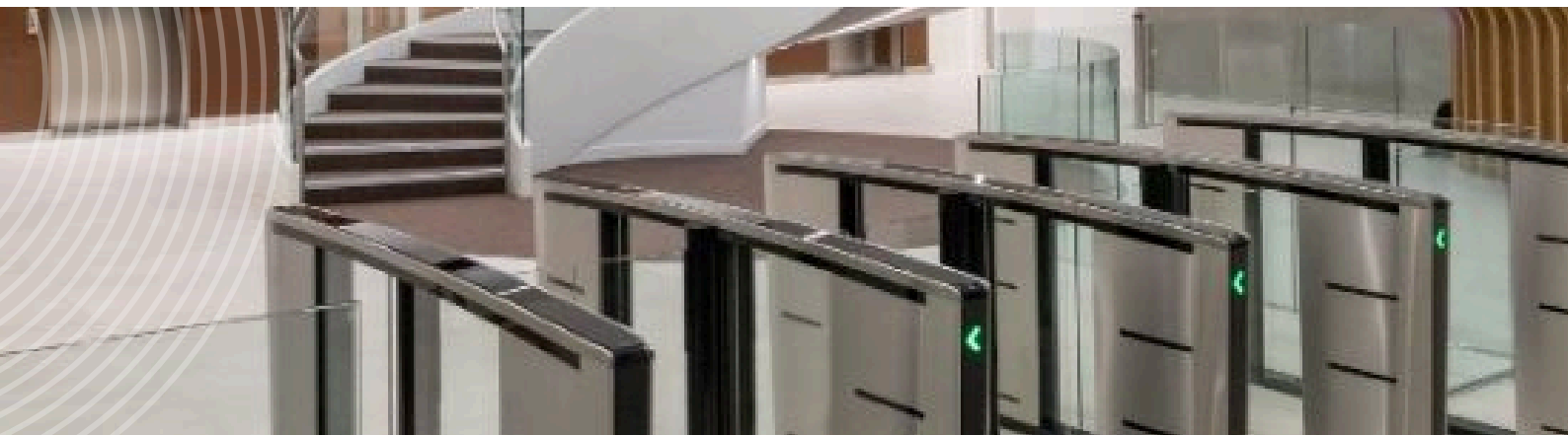
Gebouwen met meerdere huurders functioneren als dynamische gemeenschappen, waarbij elke organisatie eigen noden en verwachtingen heeft. Terwijl sommige bedrijven nood hebben aan strengere beveiliging, kiezen andere bewust voor een gedeelde omgeving omwille van zakelijke synergieën. Deze diversiteit kan spanningen veroorzaken, zeker wanneer belangen met elkaar in conflict komen. Een doordachte positionering van fysieke beveiligingsoplossingen – met aandacht voor zowel veiligheid als gastvrijheid – helpt gebouwbeheerders om een werkbare en evenwichtige omgeving te creëren.

De opkomst van huren

Trends in commercieel vastgoed tonen een verschuiving van eigendom naar huur. Grote organisaties kiezen er steeds vaker voor om ruimtes te leasen in plaats van ze volledig in eigendom te nemen. Deze evolutie kan gebouwen kwetsbaarder maken voor beveiligingsrisico's afkomstig van naburige huurders, zeker naarmate de personeelsrotatie toeneemt en eigendomsstructuren complexer worden. Het is dan ook cruciaal voor gebouwbeheerders en huurders om te investeren in flexibele beveiligingsoplossingen die zich kunnen aanpassen aan veranderende bezettingspatronen.

Bedreigingen van binnenuit de organisatie

Hoewel externe bedreigingen vaak de meeste aandacht krijgen in discussies, zijn interne risico's minstens even belangrijk. Ontevreden werknemers of voormalige medewerkers met behouden toegangsrechten kunnen bestaande kwetsbaarheden misbruiken. Om deze risico's te beperken, hebben organisaties nood aan flexibele en schaalbare oplossingen die het snel wijzigen of intrekken van toegangsrechten vergemakkelijken – vergelijkbaar met het beheer van inloggegevens in digitale omgevingen zoals Microsoft-systemen. Het installeren van fysieke barrières, zoals Speedlanes op specifieke verdiepingen, biedt een extra beveiligingslaag binnen gebouwen. Deze maatregelen maken deel uit van een gelaagd verdedigingssysteem, in combinatie met multifactorauthenticatie voor digitale toegang. De capaciteit om zich snel aan te passen aan opkomende bedreigingen – zowel fysiek als digitaal – is wat goed beveiligde organisaties onderscheidt van kwetsbare.



6 IOT EN REALTIME MONITORING.

De integratie van Internet of Things (IoT)-systemen verandert fundamenteel de manier waarop organisaties omgaan met fysieke en digitale dreigingen. Door gebruik te maken van innovatieve technologieën kunnen bedrijven voortdurend toezicht houden, wat realtime detectie van risico's en directe respons mogelijk maakt.

Wat is IoT?

IoT verwijst naar een netwerk van onderling verbonden fysieke toestellen die uitgerust zijn met sensoren, software en andere technologieën. Door gegevens te verzamelen en onmiddellijk via het internet door te sturen, ondersteunen deze toestellen intelligente automatisering en doordachte besluitvorming. Binnen de beveiliging omvatten IoT-toepassingen onder meer realtime monitoring, toegangscontrole en voorspellend onderhoud van inkomoplossingen.

Open Supervised Device Protocol (OSDP)

De digitalisering van hardware verandert de manier waarop producten worden geïntegreerd met toegangscontrolesystemen, wat leidt tot meer efficiëntie en gebruiksgemak. Traditioneel vereiste de aansluiting van toestellen op dergelijke systemen meerdere kabels voor stroomvoorziening, communicatie en aansturing, wat resulteerde in complexe bekabelingsopstellingen en uitdagingen bij installatie en onderhoud.

Ontwikkelingen zoals OSDP vereenvoudigen dit proces door digitale communicatie tussen toestellen mogelijk te maken via een enkelvoudige kabelverbinding. In plaats van meerdere datakabels is nu één enkele verbinding voldoende om verschillende functies te ondersteunen, waardoor de fysieke infrastructuur aanzienlijk wordt gereduceerd.

Dankzij deze verbeterde connectiviteit werken producten uit uiteenlopende systemen – zoals toegangscontrole, gebouwbeheer en branddetectie – nu vlot samen op één uniform platform.

Door de complexiteit te verlagen en het risico op fouten tijdens installatie en onderhoud te beperken, worden werkzaamheden vereenvoudigd, de insteltijd verkort en het algemene systeembeheer verbeterd. Dit bevordert vlottere besluitvorming en betere controle.

Verbeterd toezicht en monitoring

IoT-systemen bieden organisaties uitgebreide 24/7 monitoringcapaciteiten. Sensoren, camera's en verbonden toestellen werken samen in een naadloze gegevensstroom en verschaffen een volledig overzicht van realtime beveiligingsgebeurtenissen. Dit niveau van zichtbaarheid stelt beveiligingsteams in staat om potentiële dreigingen snel te detecteren en te evalueren, zodat ze steeds een stap voor blijven op mogelijke inbreuken.

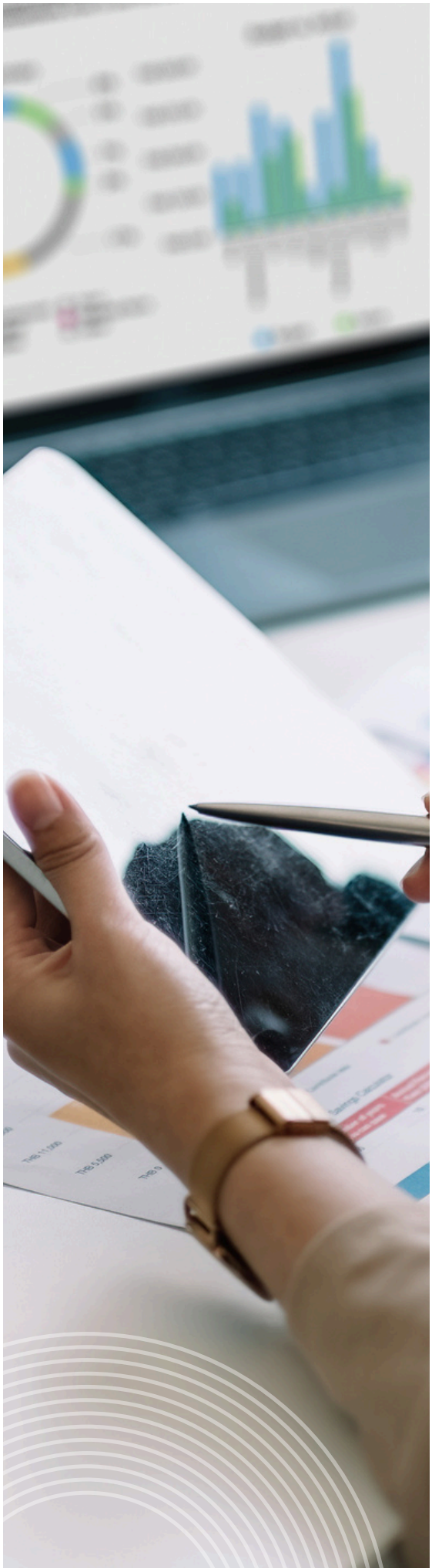
Remote monitoring en voorspellend onderhoud

In een steeds digitaler wordende wereld speelt IoT een sleutelrol in het optimaliseren van toegangsbeheer. Dankzij remote monitoring kunnen gebouwbeheerders de status en prestaties van toegangsproducten – zoals tourniquetdeuren, beveiligingstourniquetdeuren, toegangssassen en beveiligingspoortjes – in realtime opvolgen via geavanceerde sensoren en beveiligde software-integraties. Deze continue connectiviteit biedt direct inzicht in de toestand van installaties.

Voorspellend onderhoud, ondersteund door IoT en machine learning, tilt dit naar een hoger niveau. Door het analyseren van datapatronen voorspelt het systeem potentiële defecten nog vóór ze zich voordoen. In plaats van reactief in te grijpen bij storingen, worden slijtage, afwijkingen en ongewoon gebruik vroegtijdig gedetecteerd. Hierdoor kunnen onderhoudsbeurten proactief en doelgericht ingepland worden.

Deze aanpak minimaliseert ongeplande stilstand, optimaliseert onderhoudsschema's en verlengt de levensduur van kritieke componenten. Zo besparen organisaties op dringende herstellingen en overbodige service-interventies – terwijl ze tegelijk de beschikbaarheid van hun beveiligingsingangen verhogen.

Naast operationele voordelen bieden remote monitoring en voorspellend onderhoud waardevolle, datagestuurde inzichten. Gebouwbeheerders kunnen op basis van gebruiksdata gerichte beslissingen nemen om het gebouwbeheer te optimaliseren en de gebruikerservaring te verbeteren. Op die manier blijven toegangsproducten betrouwbaar, veilig en afgestemd op de specifieke behoeften van elke locatie.



TOEKOMST-VOORUIT.

Amine Bouchareb

PRODUCTMANAGER - SECURITY ACCESS

De inkomoplossingen van Boon Edam zijn ontworpen met het oog op de toekomst. Ze combineren geavanceerde beveiligingstechnologie met flexibele, ruimtebesparende ontwerpen die zowel veiligheid als gastvrijheid garanderen – volledig afgestemd op de voortdurend evoluerende eisen en normen van hedendaagse beveiliging.

Met decennialange ervaring en een innovatieve visie bieden wij oplossingen die eigendommen beschermen, de gebruikerservaring optimaliseren en betrouwbaar presteren.

De toekomst van beveiligingsingangen ligt in een naadloze integratie – waar fysieke en digitale beveiliging samenkomen, met aandacht voor duurzaamheid en technologische vooruitgang.

Organisaties die proactief inspelen op deze evoluties zijn beter gewapend tegen een steeds complexer wordend dreigingslandschap.

De toekomst van beveiligingsingangen ligt in naadloze integratie.

WERELDWIJD AANWEZIG.

Wij zijn al 150 jaar actief in de productie van premium esthetische en beveiligde toegangsoplossingen in Europa, de Verenigde Staten en China. Wij kunnen vol vertrouwen zeggen dat onze vestigingen wereldwijd te vinden zijn. In landen zonder eigen Boon Edam-vestiging werkt onze Global Export divisie samen met exclusieve distributeurs of biedt ze directe verkoop en services. Door onze wereldwijde aanwezigheid hebben wij uitgebreide kennis van lokale markten en hun unieke toegangseisen.

Bezoek onze website om een Boon Edam expert in uw regio te vinden: **www.boonedam.be/contact**

Boon Edam Belux B.V.
T +32 14 21 67 17
E be.service@boonedam.com
W www.boonedam.be

BOON EDAM
YOUR **ENTRY** EXPERTS.