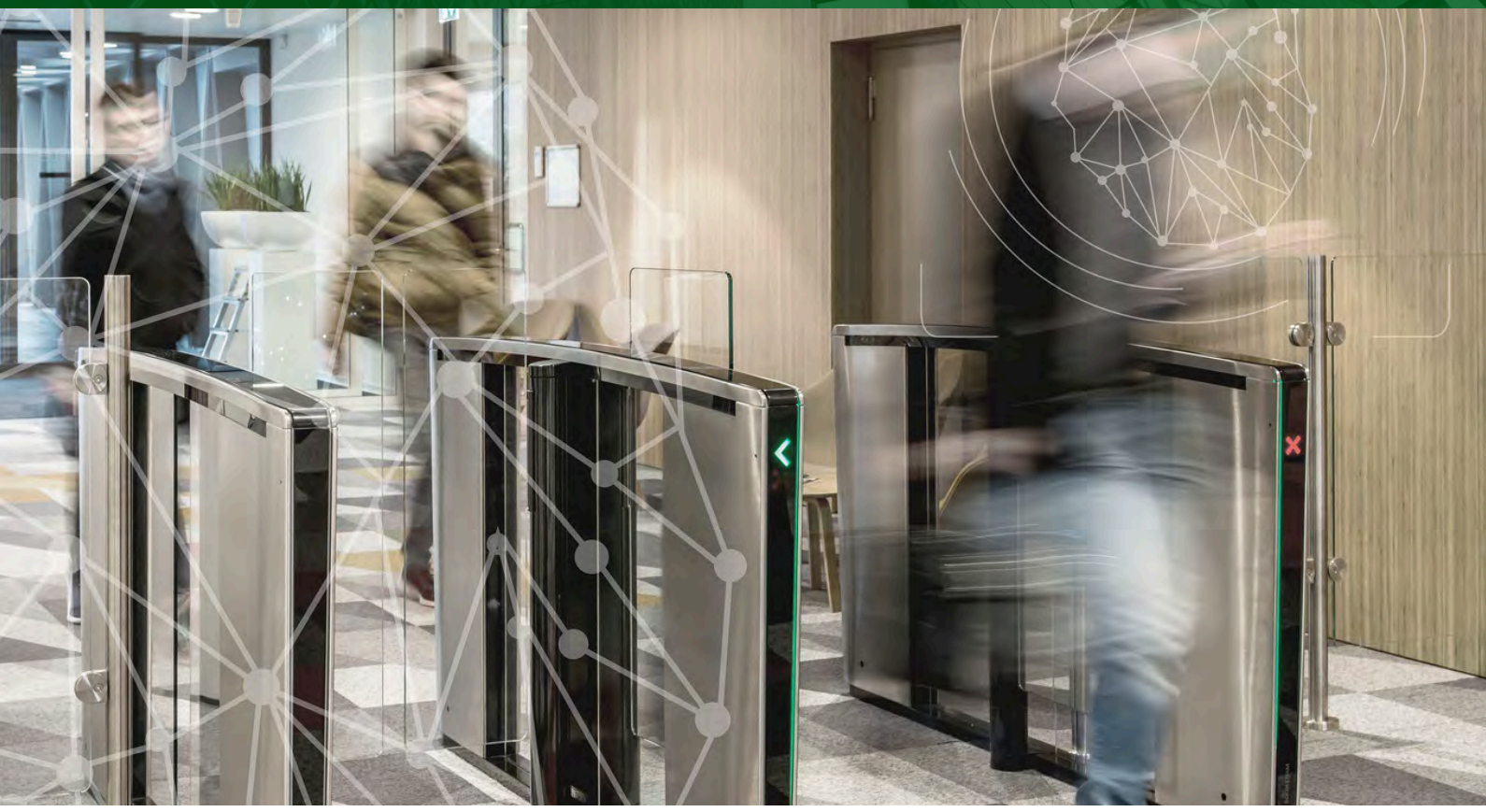
BEVEILIGINGS ENTREES

TRENDRAPPORT

2025.



BEVEILIGINGSOPLOSSINGEN VOOR ENTREES VAN MORGEN.

BOON EDAM
YOUR **ENTRY** EXPERTS.

INTRODUCTIE.

In een wereld die wordt gekenmerkt door toenemende polarisatie, technologische vooruitgang, extremisme en groeiend wantrouwen, zijn de eisen voor gebouwbeveiliging aanzienlijk aangescherpt. Sectoren die voorheen slechts beperkte bescherming nodig hadden, krijgen nu te maken met verhoogde risico's. De dreiging beperkt zich allang niet meer tot overheidsinstellingen en datacenters. Dit rapport verkent de actuele ontwikkelingen op het gebied van beveiligingsentrees en biedt inzicht in hoe u voorbereid blijft op een steeds onvoorspelbaarder veiligheidslandschap.

"Nu de maatschappij streeft naar barrièrevrije en gastvrije omgevingen, vraagt de harde realiteit om robuuste beveiligingsmaatregelen die toegankelijkheid in balans brengen met bescherming."

Douwe Jolles
PRODUCTMANAGER - DOOR SYSTEMS

INDEX

1 CYBER SECURITY ONTMOET FYSIEKE BEVEILIGING.

De noodzaak voor een samenhangende benadering van beveiliging is urgenter dan ooit. Organisaties in uiteenlopende sectoren - van datacenters en overheidsgebouwen tot kritieke infrastructuur en bedrijfshoofdkantoren - staan aan de vooravond van een nieuw tijdperk in beveiligingsstrategie. In een steeds meer verbonden wereld draait beveiliging niet langer alleen om het voorkomen van ongeautoriseerde toegang of het beschermen van digitale systemen. Het gaat om het naadloos integreren van beide componenten in één alomvattende, uniforme verdedigingslijn.

Zero Trust-architectuur

Dit beveiligingsmodel is gebaseerd op het principe van minimale toegangsrechten. Gebruikers en apparaten krijgen uitsluitend toegang tot de bronnen die noodzakelijk zijn voor hun rol - en niets meer dan dat. Het Zero Trust-model maakt het voor kwaadwillenden aanzienlijk moeilijker om systemen te compromitteren of vertrouwelijke informatie te onderscheppen, doordat het aantal toegangswegen strikt wordt beperkt. Deze benadering is met name van belang in omgevingen waar uiterst gevoelige en waardevolle gegevens worden beheerd, zoals in datacenters. In zulke omgevingen moet elke interactie met zowel fysieke als digitale middelen worden geverifieerd op basis van geldige toegangsrechten.

De lat hoger leggen voor cybersecurity

Nieuwe EU-regelgeving verandert de normen voor cyberbeveiliging ingrijpend, met directe gevolgen voor beveiligingsentrees en toegangscontrolesystemen. De NIS2-richtlijn en de Cyber Resilience Act (CRA) hebben beide als doel de digitale weerbaarheid te vergroten, elk vanuit een ander perspectief.

NIS2 is gericht op het versterken van de beveiliging van essentiële diensten en kritieke infrastructuur. Sectoren zoals energie, gezondheidszorg en transport moeten hun cyberbeveiligingsmaatregelen structureel aanscherpen. Denk hierbij aan strenger risicobeheer, beveiliging van de toeleveringsketen en verplicht melden van cyberincidenten. Organisaties die eind 2024 niet aan deze vereisten voldoen, riskeren forse boetes en reputatieschade.

De **Cyber Resilience Act** verplicht producten met digitale componenten, zoals toegangscontrolesystemen en beveiligingsproducten met IoT-functionaliteit, te voldoen aan strengere cyberbeveiligingsnormen. Fabrikanten moeten beveiliging integreren in het ontwerp en de ontwikkeling van hun producten, zorgen voor doorlopend onderhoud en beveiligingsupdates, en in sommige gevallen externe certificering laten uitvoeren voor risicovolle producten alvorens deze op de EU-markt toegelaten worden. Producten die aan deze eisen voldoen, ontvangen de CE-markering. Dit vergemakkelijkt voor bedrijven het herkennen van oplossingen die aantoonbaar voldoen aan de gestelde veiligheidsnormen.

In samenhang markeren NIS2 en de CRA een nieuwe standaard voor cyberbeveiliging. Ze waarborgen dat zowel de infrastructuur als de fysieke toegangsproducten die deze beschermen, weerbaar zijn tegen digitale dreigingen.

Beveiligingsecosystemen

In het complexe beveiligingslandschap van vandaag moet het beveiligingsecosysteem van een gebouw bestaan uit een geïntegreerde mix van hoge, middelhoge en lage beveiligingsniveaus. Elke laag vervult een specifieke functie: het beveiligen van het gebouw, het beschermen van kritieke middelen en het gecontroleerd verlenen van toegang.

Hoewel cybersecurity vaak centraal staat in discussies over het beschermen van gevoelige omgevingen, is fysieke beveiliging minstens zo cruciaal, met name in faciliteiten zoals datacenters. Directe fysieke toegang tot een server kan zelfs de best ingerichte digitale verdedigingslinies, zoals firewalls, omzeilen en leiden tot ernstige datalekken. Dit benadrukt de noodzaak van een nauwe afstemming tussen fysieke en digitale beveiligingsmaatregelen.

Zones met een **hoge beveiliging**, zoals serverruimtes, vereisen een combinatie van geautomatiseerde fysieke beveiligingsoplossingen, waaronder biometrische verificatie en gecodeerde communicatieprotocollen. Deze maatregelen blokkeren ongeautoriseerde toegang en sluiten aan op cybersecuritystrategieën door snelle wijziging van toegangsrechten mogelijk te maken bij een dreiging.

Gebieden met **middelhoge beveiliging**, zoals administratieve afdelingen, maken gebruik van technologieën zoals beveiligingspoortjes met geavanceerde sensoren. Deze bieden vlotte toegang voor geautoriseerd personeel en vormen tegelijkertijd een fysieke barrière tegen ongewenste indringers.

Ruimten met **lage beveiliging**, zoals publieke lobby's, zijn ontworpen met de nadruk op toegankelijkheid en uitstraling, zonder concessies te doen aan de basisbeveiliging. Bewaakte toegangen zorgen hier voor een gecontroleerde doorstroming van bezoekers.

Deze gelaagde aanpak weerspiegelt principes uit de cybersecurity, zoals multifactorauthenticatie: net zoals digitale systemen meerdere beschermingsniveaus vereisen, vragen fysieke ruimtes om complementaire beveiligingslagen. Als één maatregel faalt, blijft de rest actief om de veiligheid te waarborgen.

Een effectieve beveiligingsaanpak vereist dat cybersecurity best practices worden doorvertaald naar fysieke systemen. Denk aan het implementeren van versleutelde communicatie, regelmatige software-updates en toegangscontrolesystemen die bestand zijn tegen cyberaanvallen.

Door fysieke en digitale beveiligingsoplossingen te verenigen in één samenhangend ecosysteem, creëren organisaties veilige, toekomstbestendige omgevingen. Deze aanpak biedt niet alleen stevige bescherming, maar bewaakt ook de balans tussen veiligheid, functionaliteit en gastvrijheid.

Indringers buiten houden is de eerste verdedigingslinie. Zodra een indringer via een toegangspunt een gebouw binnendringt, worden alle andere beveiligingsmaatregelen reactief. Het voorkomen van een beveiligingslek begint dus bij de entree."

Security Operations Centre

Een Security Operations Centre (SOC) is een centrale eenheid die verantwoordelijk is voor de continue monitoring, detectie, analyse en afhandeling van cybersecuritydreigingen. Het primaire doel is het beschermen van netwerken, systemen, applicaties en gevoelige informatie tegen digitale aanvallen, en daarmee het waarborgen van de algehele beveiliging van de organisatie.

Het SOC is 24/7 operationeel om permanente monitoring te waarborgen en het risico op datalekken, cyberaanvallen of ongewenste toegang te beperken. Organisaties richten hun SOC in op basis van eigen behoeften en capaciteit. Veelvoorkomende varianten zijn interne SOC's, die maximale controle bieden maar forse investeringen vragen. Managed SOC's, beheerd door externe specialisten, bieden expertise zonder interne belasting.

2 EXPLOSIE- EN INSLAGWERENDHEID.

Het veranderende dreigingsbeeld leidt tot een toenemende vraag naar geavanceerde gebouwbeveiliging binnen een steeds breder spectrum van sectoren. Traditionele sectoren zoals overheden, financiële instellingen en datacenters hebben al langer een sterke focus op beveiliging. Tegenwoordig dwingen nieuwe risico's ook sectoren als mediabedrijven en commerciële organisaties om hun beveiligingsmaatregelen fors op te schalen.

Risico's zoals vandalisme, terrorisme, extremisme en maatschappelijke polarisatie veranderen de manier waarop organisaties naar gebouwbeveiliging kijken. Materialen die bestand zijn tegen explosies en inslagen worden daarbij steeds vaker ingezet als cruciaal onderdeel van moderne beveiligingsoplossingen.

Materiaalinnovatie

Nu organisaties meer inzetten op het voorkomen van dreigingen, krijgen explosie- en impactbestendige entrees een hogere prioriteit. Het toenemende gebruik van geavanceerde materialen in gebouwgevels benadrukt de noodzaak van robuuste fysieke barrières die inspelen op veranderende veiligheidsrisico's.

Materialen zoals polycarbonaat (licht van gewicht en slagvast), versterkt staal en veiligheidsglas worden steeds vaker toegepast in moderne beveiligingssystemen. Ze zijn ontwikkeld om de energie van explosies of inslagen te absorberen en te verspreiden, en vormen duurzame barrières die schade beperken. Door samen te werken met materiaalspecialisten integreren fabrikanten geavanceerde technologie in hun toegangsproducten, wat de weerstand tegen zowel gerichte aanvallen als onbedoelde impact versterkt.

Beveiligingsentrees worden ontworpen om ook zware inbreuken te weerstaan, of die nu plaatsvinden met gereedschap of voertuigen. Onderdelen zoals anti-ramelementen, versterkte kozijnen en geavanceerde verankeringssystemen zorgen voor robuuste bescherming en vormen de eerste verdedigingslinie van een gebouw.

Daarnaast neemt het gebruik van kogelwerend glas toe in sectoren die voorheen als minder risicovol golden. Dit glas is ontwikkeld om de energie van inslagen op hoge snelheid op te vangen en af te voeren en biedt gerichte bescherming tegen vandalisme, brandstichting en gewelddadige aanvallen.

Economische gevolgen van downtime

De financiële impact van verstoringen door explosies of geforceerde toegang kan groot zijn en reikt vaak verder dan alleen fysieke schade. Bedrijven kunnen worden getroffen door operationele stilstand, verlies van goederen of data en schade aan hun reputatie, vooral in sectoren waar uitval direct het vertrouwen en de omzet raakt. Steeds meer organisaties erkennen daarom het belang van beschermende toegangsproducten als vast onderdeel van hun beveiligingsstrategie. Deze oplossingen spelen een sleutelrol in het waarborgen van bedrijfscontinuïteit.

Balans tussen toegankelijkheid en veiligheid

Omdat de samenleving steeds meer belang hecht aan openheid en toegankelijkheid, is een zorgvuldige balans nodig tussen gastvrije gebouwomgevingen en effectieve beveiliging. Dat vraagt om innovatieve oplossingen die geavanceerde beveiligingsfuncties integreren zonder concessies te doen aan transparantie of esthetiek. Gebouwen moeten niet alleen veilig en weerbaar zijn, maar ook passen binnen bredere maatschappelijke waarden. Alleen dan ontstaat een omgeving die bescherming biedt in een onvoorspelbare wereld, zonder afbreuk te doen aan de beleving van gebruikers en bezoekers.

3

AI.

Kunstmatige intelligentie (AI) blijft een sleutelrol spelen binnen de ontwikkeling van beveiligde toegangsoplossingen. Hoewel AI soms als hype wordt gezien, groeit het strategisch belang ervan gestaag en verandert het fundamenteel hoe beveiliging wordt ingericht en toegepast.

Toepassingen zoals voorspellende analyse, dreigingsdetectie en de automatisering van repetitieve processen blijken bijzonder waardevol. Dankzij het vermogen om grote hoeveelheden data te verwerken en te duiden, is AI bij uitstek geschikt voor complexe omgevingen zoals luchthavens, zorginstellingen en bedrijfsgebouwen. Hier draagt het bij aan de schaalbare en efficiënte beveiliging die moderne organisaties vereisen.

Voorspellende analyse en detectie van bedreigingen

Een van de meest betekenisvolle toepassingen van AI in beveiliging is voorspellende analyse en dreigings-detectie. Traditionele systemen werken vaak reactief: ze treden pas in werking nadat een incident heeft plaatsgevonden. AI maakt een meer proactieve benadering mogelijk door continu toegangscontrole-gegevens en andere beveiligingsinformatie te analyseren.

AI-gestuurde systemen herkennen trends en afwijkingen die kunnen wijzen op een dreiging. In plaats van te vertrouwen op menselijke waarneming, markeert AI automatisch verdachte patronen, beoordeelt het risico en levert het direct bruikbare inzichten. Dit versnelt de respons en stelt beveiligingsteams in staat om in te grijpen vóórdat een situatie uit de hand loopt.

WIST U DAT?

De wereldwijde markt voor AI in cybersecurity zal naar verwachting 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. Bron: https://www.mordorintelligence.com/industry-reports/artificial-intelligence-in-security-market

AI-aangedreven innovaties in toegangsoplossingen

De integratie van AI in toegangsoplossingen zoals draaideuren en beveiligingspoortjes markeert het begin van een nieuw tijdperk van intelligente beveiliging. AI kan piekmomenten voorspellen, functionaliteit automatisch aanpassen en een efficiënte doorstroming faciliteren zonder in te leveren op veiligheid. Dit verhoogt zowel de beveiliging als het gebruiksgemak en draagt bij aan een optimale gebruikerservaring binnen de operationele kaders.

Ook biometrische verificatie ontwikkelt zich snel. Naast herkenning via vingerafdruk of gezicht worden geavanceerde technieken zoals aderpatroonanalyse en hartslagidentificatie toegepast in high security omgevingen. Deze innovaties versterken de toegangscontrole en maken een soepele toegang mogelijk voor geautoriseerde personen.

Duurzame innovatie

Machine learning-systemen vereisen aanzienlijke rekenkracht. Daarom is het essentieel om het energieverbruik en de CO_2-voetafdruk ervan zorgvuldig te beheersen. Het ontwikkelen van energiezuinige modellen, het optimaliseren van infrastructuur en het inzetten van hernieuwbare energiebronnen zijn cruciale stappen om de ecologische impact van AI-technologieën te verkleinen. Door hierin te investeren, dragen organisaties bij aan zowel technologische vooruitgang als verantwoord milieubeheer.

Ethische toepassing

AI-systemen moeten bovendien eerlijk en transparant worden ontworpen. Vooroordelen in machine learning kunnen leiden tot eenzijdige, onethische uitkomsten en het vertrouwen in technologie aantasten. Om dit te voorkomen, is het belangrijk om te werken met diverse en representatieve datasets, transparante algoritmen en voortdurende toetsing. Tegelijkertijd moet er een zorgvuldige balans worden gevonden tussen beveiliging en privacy, zodat veiligheid niet ten koste gaat van individuele rechten.

Het menselijke element: beslissingen versterken met AI

Hoewel AI krachtige mogelijkheden biedt, blijven mensen onmisbaar binnen effectieve beveiligingsoplossingen. De combinatie van machine learning en menselijk inzicht leidt tot beter onderbouwde beslissingen. AI kan patronen herkennen en processen versnellen, maar menselijk toezicht is nodig om interpretaties te maken en ethische afwegingen te garanderen. Er bestaat nog altijd terughoudendheid om beslissingen volledig aan AI over te laten zonder menselijk toezicht om die beslissingen te valideren.

AI is er niet om mensen te vervangen, maar om hen te versterken. Door routinetaken te automatiseren, dreigingen sneller te signaleren en responsprocessen te verbeteren, stelt AI beveiligingsteams in staat zich te richten op hun kerntaak: het beschermen van mensen, middelen en gebouwen.

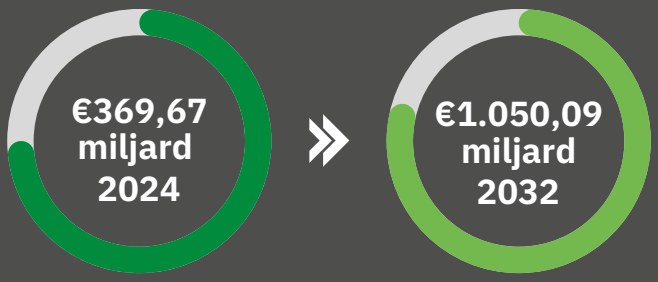
De krachtigste beveiligingsstrategieën ontstaan door samenwerking. AI neemt het zware werk van data-analyse en automatisering over, terwijl mensen context, ervaring en beoordelingsvermogen toevoegen. Die wisselwerking vormt de basis van slimme, betrouwbare en toekomstbestendige beveiliging.

4 DUURZAAMHEID.

De vraag naar duurzame en milieubewuste oplossingen wordt steeds belangrijker binnen de beveiligingssector nu organisaties meer verantwoordelijkheid nemen voor hun ecologische impact. Hoewel veiligheid de kern blijft, groeit het besef dat duurzaamheid een integraal onderdeel is van toekomstgerichte strategieën. Bedrijven zoeken in toenemende mate naar oplossingen die sterke beveiligingsprestaties combineren met energie-efficiëntie en een lagere milieu-impact. Deze ontwikkeling weerspiegelt een bredere verschuiving naar verantwoord ondernemen, waarin beveiliging en duurzaamheid hand in hand gaan.

Echte duurzaamheid gaat niet alleen over recyclen of hergebruiken; het begint met het ontwerpen van producten die zo betrouwbaar zijn dat die stappen 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

Modernisering is een duurzame en kostenefficiënte manier om bestaande beveiligingsentrees te upgraden. Het verhoogt de veiligheid en functionaliteit zonder dat volledige vervanging nodig is. Door installaties langer mee te laten gaan, beperken moderniseringen zowel afval als verstoringen in de bedrijfsvoering.

We onderscheiden twee vormen van modernisering, elk afgestemd op specifieke wensen en functionele eisen:

- Een **modernisering** verbetert de prestaties of functionaliteit van een bestaande oplossing zonder de basisconstructie aan te passen. Denk aan het vervangen van sensoren of het verfijnen van toegangscontrole. Zo kunnen organisaties voldoen aan nieuwe eisen, terwijl de oorspronkelijke installatie behouden blijft.

- Een **upgrade** gaat een stap verder en omvat ingrijpende aanpassingen aan technologie, materialen of functies. Dit resulteert vaak in een herclassificatie van het product. Voorbeelden zijn het integreren van nieuwe technologieën of het vervangen van cruciale componenten om te voldoen aan strengere beveiligingsnormen.

Energie-efficiëntie en milieuvriendelijke materialen

Moderne beveiligingsoplossingen zijn uitgerust met energiezuinige motoren, IoT-componenten met laag energieverbruik en slimme sensoren die hun werking automatisch afstemmen op realtime gebruik. Deze technologieën verlagen het energieverbruik en verhogen de operationele efficiëntie. Draaideuren dragen bovendien bij aan klimaatbeheersing doordat ze luchtstromen beperken, wat ze geschikt maakt voor duurzame bouwprojecten en certificeringen zoals LEED.

Daarnaast worden niet-giftige materialen steeds vaker standaard toegepast in het ontwerp van beveiligingsentrees. Al deze elementen versterken de duurzaamheidsambities van organisaties en maken het mogelijk om beveiligingsinvesteringen te koppelen aan bredere MVO-doelstellingen.

Bouwen voor de lange termijn

Duurzame oplossingen beperken afval door de behoefte aan frequente vervanging te verminderen. Organisaties kiezen steeds vaker voor strategieën die gericht zijn op levensduur, betrouwbaarheid en een zo gering mogelijke milieu-impact. Het gaat daarbij niet alleen om de uitdagingen van vandaag, maar om het bouwen aan oplossingen die generaties meegaan. Investeren in degelijk ontworpen, hoogwaardige producten levert langdurige prestaties, betrouwbare beveiliging en een consistente gebruikerservaring die toekomstbestendig is.

5 HET BUREN EFFECT.

Beveiliging beheren in gebouwen met meerdere huurders

In multi-tenant gebouwen wordt de beveiligingsbehoefte van één organisatie vaak beïnvloed door de activiteiten van andere gebruikers. Of u nu gebouwbeheerder of huurder bent: het is essentieel om rekening te houden met de impact van omliggende bedrijven op uw eigen veiligheidsaanpak. Beveiligingsrisico's stoppen niet bij de eigen voordeur. Een incident bij een aangrenzende huurder, zoals criminaliteit, protesten of andere verstoringen, kan directe gevolgen hebben voor uw organisatie. Dit zogenoemde bureneffect benadrukt het belang van onderlinge afstemming en samenwerking binnen gedeelde gebouwomgevingen.

Balans vinden tussen uiteenlopende behoeften

Gebouwen met meerdere huurders functioneren als dynamische gemeenschappen, waarin elke organisatie eigen eisen en voorkeuren heeft. Waar de ene huurder strenge beveiliging verlangt, kiest een ander juist bewust voor openheid en gedeelde voorzieningen om zakelijke synergie te bevorderen. Die verscheidenheid kan spanningen veroorzaken, vooral wanneer belangen uiteenlopen. Een zorgvuldige positionering van fysieke beveiligingsoplossingen, met oog voor zowel veiligheid als toegankelijkheid, stelt gebouwbeheerders in staat om een evenwichtige, werkbare omgeving te realiseren voor alle betrokken partijen.

De opkomst van huren

Binnen het commercieel vastgoed is een duidelijke trend zichtbaar: steeds meer grote organisaties kiezen voor huur in plaats van eigendom. Deze verschuiving naar gedeeld gebruik maakt gebouwen mogelijk kwetsbaarder voor beveiligingsrisico's vanuit omliggende huurders, zeker wanneer de bezetting toeneemt en eigendomsstructuren veranderen. Voor zowel gebouwbeheerders als huurders is het daarom van belang om te investeren in flexibele beveiligingsoplossingen die kunnen meebewegen met veranderende gebruikspatronen en bezettingsdynamiek.

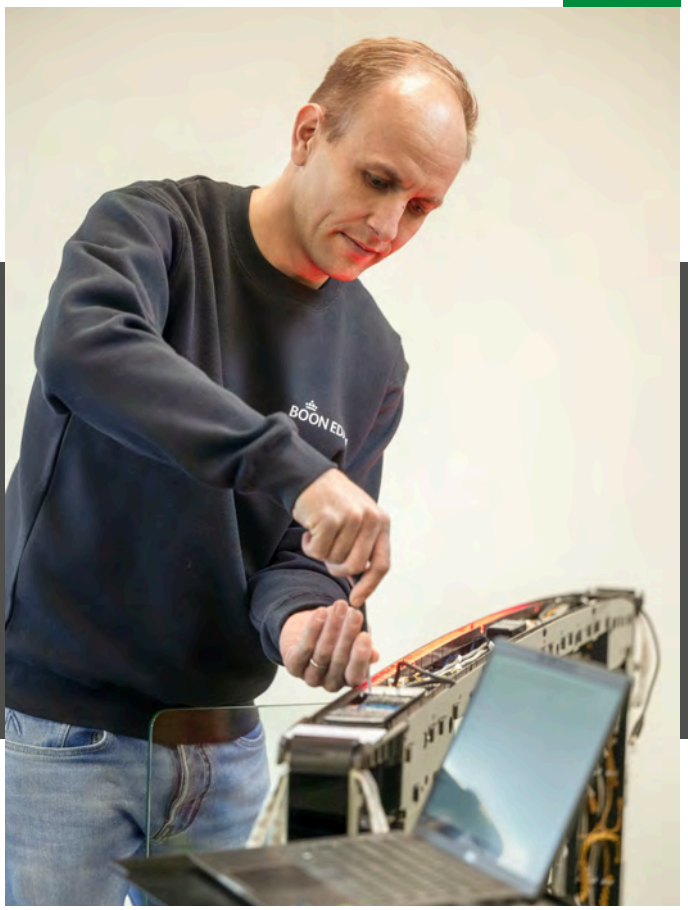
Bedreigingen van binnenuit de organisatie

Hoewel externe dreigingen vaak centraal staan in beveiligingsdiscussies, zijn interne risico's minstens zo relevant. Ontevreden medewerkers of oud-werknemers met achtergebleven toegangsrechten kunnen bestaande kwetsbaarheden benutten. Om dit te voorkomen, hebben organisaties schaalbare oplossingen nodig waarmee toegangsrechten snel en flexibel kunnen worden aangepast of ingetrokken - vergelijkbaar met het beheer van gebruikersaccounts in digitale systemen zoals Microsoft-omgevingen.

Het inzetten van fysieke barrières, zoals Speedlanes op specifieke verdiepingen, voegt een extra beveiligingslaag toe. In combinatie met digitale maatregelen zoals multifactorauthenticatie ontstaat zo een geïntegreerd verdedigingssysteem. Het vermogen om snel te reageren op nieuwe dreigingen, zowel fysiek als digitaal, is een onderscheidend kenmerk van veerkrachtige en toekomstbestendige organisaties.

6 IOT EN REALTIME MONITORING.

De integratie van Internet of Things (IoT)-systemen verandert fundamenteel hoe organisaties omgaan met fysieke en digitale dreigingen. Door innovatieve technologie in te zetten, kunnen bedrijven continu toezicht houden en realtime risico's detecteren en daarop reageren.



Wat is IoT?

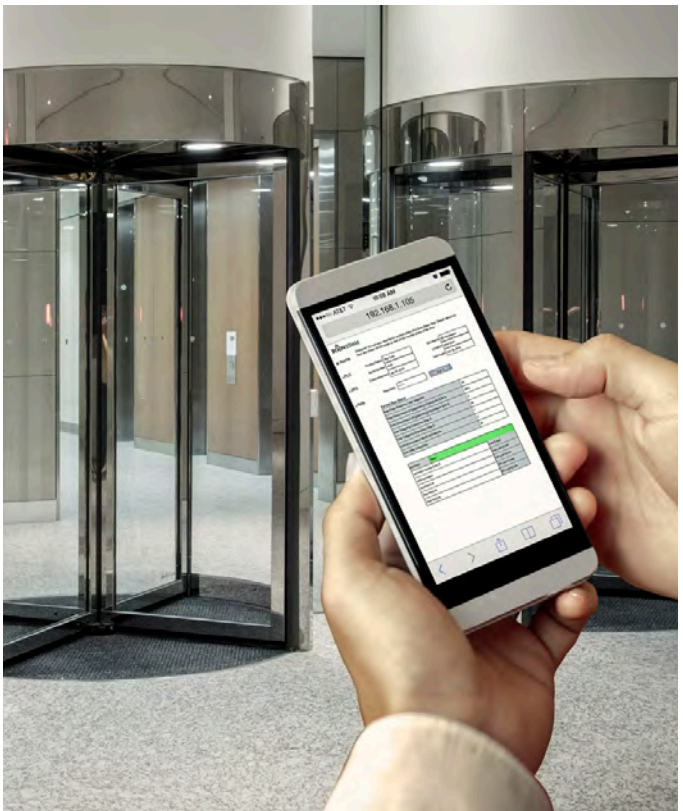
IoT verwijst naar een netwerk van onderling verbonden fysieke apparaten die zijn uitgerust met sensoren, software en andere technologie. Deze apparaten verzamelen gegevens en sturen deze direct via internet door, waardoor slimmere automatisering en beter onderbouwde beslissingen mogelijk worden. Binnen de beveiliging omvatten IoT-toepassingen onder meer realtime monitoring, toegangscontrole en voorspellend onderhoud van toegangsoplossingen.

Open Supervised Device Protocol (OSDP)

De digitalisering van hardware verandert ook de manier waarop producten worden geïntegreerd met toegangscontrolesystemen. Dit resulteert in hogere efficiëntie en eenvoudiger beheer. Voorheen waren meerdere kabels nodig voor stroomvoorziening, communicatie en aansturing, wat leidde tot complexe bedrading en uitdagingen bij installatie en onderhoud.

Nieuwe standaarden, zoals OSDP, vereenvoudigen dit proces door digitale communicatie via een enkele kabel mogelijk te maken. In plaats van meerdere datalijnen kan één verbinding meerdere functies uitvoeren, waardoor de fysieke infrastructuur aanzienlijk wordt gereduceerd.

Door deze verbeterde connectiviteit werken producten uit verschillende systemen, zoals toegangscontrole, gebouwbeheer en brandveiligheid, nu naadloos samen op één uniform platform. Dit vermindert complexiteit, verkleint de kans op fouten tijdens installatie en onderhoud, versnelt de ingebruikname en verbetert het algehele systeembeheer. Zo ontstaan soepelere processen en meer inzicht in de beveiligingsomgeving.



Verbeterd toezicht en monitoring

IoT-systemen bieden organisaties uitgebreide 24/7 monitoring. Sensoren, camera's en verbonden apparaten werken samen in een naadloze gegevensstroom, waardoor een volledig beeld ontstaat van realtime beveiligingsgebeurtenissen. Dit hoge niveau van zichtbaarheid stelt beveiligingsteams in staat potentiële dreigingen snel te signaleren en te beoordelen, zodat zij mogelijke inbreuken altijd een stap voor blijven.

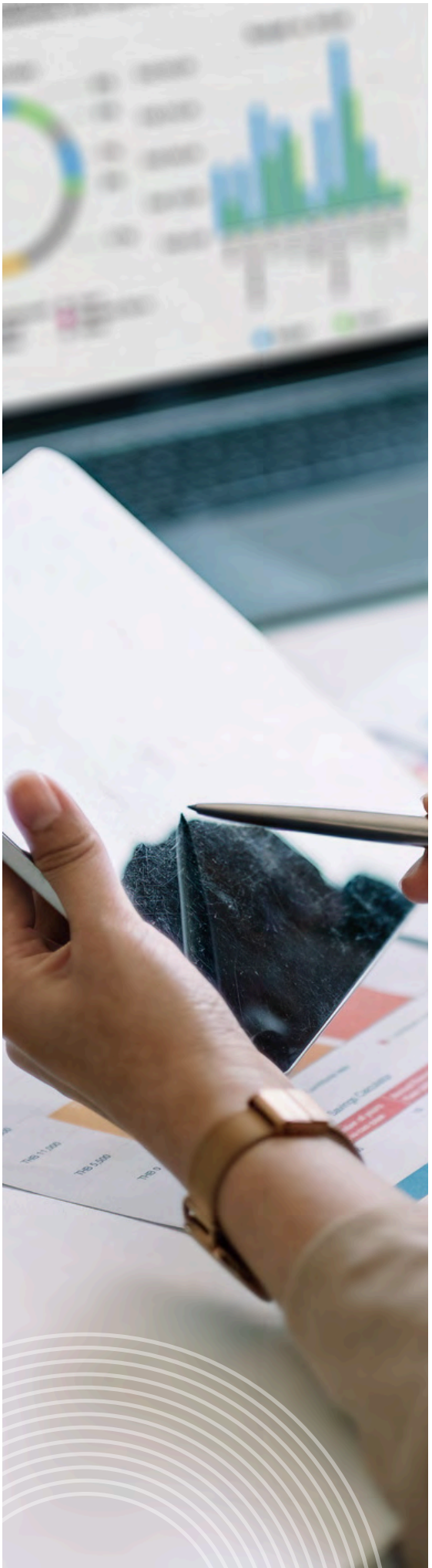
Remote monitoring en voorspellend onderhoud

In een steeds verder digitaliserende wereld speelt IoT een cruciale rol in het optimaliseren van toegangsbeheer. Met remote monitoring kunnen gebouwbeheerders de status en prestaties van toegangsproducten, zoals draaideuren, beveiligingsdraaideuren, sluizen en beveiligingspoortjes, realtime volgen via geavanceerde sensoren en veilige software-integraties. Deze continue connectiviteit biedt direct inzicht in de conditie van installaties.

Voorspellend onderhoud, ondersteund door IoT en machine learning, tilt dit naar een hoger niveau. Door datapatronen te analyseren, kan het systeem mogelijke storingen voorspellen voordat ze optreden. In plaats van pas in te grijpen bij een defect, worden slijtage, afwijkingen en ongebruikelijke patronen vroegtijdig herkend. Zo kunnen servicebeurten proactief en doelgericht worden ingepland.

Deze werkwijze minimaliseert ongeplande uitval, optimaliseert onderhoudscycli en verlengt de levensduur van belangrijke componenten. Organisaties besparen daarmee op spoedreparaties en onnodige servicebezoeken, terwijl de beschikbaarheid van beveiligingsentrees toeneemt.

Naast operationele voordelen leveren remote monitoring en voorspellend onderhoud waardevolle, data gedreven inzichten op. Op basis van gebruiksgegevens kunnen gebouwbeheerders gerichte keuzes maken om het beheer te verbeteren en de gebruikerservaring te optimaliseren. Zo blijven toegangsproducten betrouwbaar, veilig en afgestemd op de specifieke behoeften van iedere locatie.



TOEKOMST-VOORUIT.

Amine Bouchareb

PRODUCTMANAGER - SECURITY ACCESS

De toegangsoplossingen van Boon Edam zijn ontworpen met het oog op de toekomst. Ze combineren geavanceerde beveiligingstechnologie met flexibele, ruimtebesparende ontwerpen die zowel veiligheid als gastvrijheid ondersteunen, volledig afgestemd op de steeds veranderende eisen en normen in moderne beveiliging.

Met decennialange ervaring en een innovatieve visie leveren wij oplossingen die eigendommen beschermen, de gebruikerservaring optimaliseren en blijvend betrouwbaar zijn.

De toekomst van beveiligingsentrees ligt in naadloze integratie: een omgeving waarin fysieke en digitale beveiliging samenkomen, met aandacht voor duurzaamheid en technologische innovatie.

Organisaties die proactief op deze ontwikkelingen inspelen, zijn beter voorbereid op een steeds complexer dreigingslandschap.

“De toekomst van beveiligings-entrees ligt in naadloze integratie.”

WERELDWIJD AANWEZIG.

Wij zijn al ruim 150 jaar actief in de productie van premium esthetische en beveiligde toegangsoplossingen in Nederland, 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.nl/contact

Boon Edam Nederland B.V.
T +31 (0) 299 38 08 08
E info@boonedam.nl
W www.boonedam.nl

BOON EDAM
YOUR **ENTRY** EXPERTS.