ELEKTRONISCH TOEGANGSBEHEER TRENDRAPPORT

POWERED BY

FEDERATIE VEILIG NEDERLAND

Federatie
Veilig Nederland
Technologie in brandveiligheid & beveiliging

Inhoudsopgave

Voorwoord

De huidige systemen voor toegangsbeheer vinden hun oorsprong als elektronisch alternatief van traditionele sluitsystemen met fysieke sleutels. Een voordeel was vooral dat een pas in tegenstelling tot een sleutel ongeldig gemaakt kan worden bij verlies of diefstal. Later werden meer voordelen benut, zoals het instellen van tijdelijke of eenmalige toegangsrechten. Inmiddels zijn we een generatie verder en maakt toegangsbeheer een ontwikkeling door die past bij het veranderende gebruik van zakelijk vastgoed.

Het kantoorgebouw met vaste werkplekken begint een zeldzaamheid te worden en het werken op kantoor is ook allang niet meer vanzelfsprekend. De coronapandemie leerde ons dat thuiswerken en vergaderen via Teams en Zoom veel efficiencyvoordelen kunnen opleveren en dat daarom ook na de pandemie op deze wijze gewerkt zal blijven worden. Dit leidt vooral in de kantorenmarkt tot een sterk groeiende vraag naar flexibel te gebruiken huisvesting. Een belangrijk element daarbij: sluitend toegangsbeheer. In een gebouw dat wisselend wordt gebruikt door meerdere organisaties vormt dat een redelijke uitdaging. Technisch is er altijd wel een oplossing te vinden, maar een en ander moet ook organisatorisch goed geregeld kunnen worden. Het ligt daarom voor de hand dat toegangsbeheer steeds meer als dienst zal worden gevraagd en niet meer als product. Zo kan iedere organisatie in het gebouw – virtueel gezien – haar eigen toegangssysteem beheren en bepalen wie, waar en wanneer naar binnen mag. Technologie die dit mogelijk maakt, is sinds enkele jaren bij verschillende fabrikanten en importeurs beschikbaar en verwacht wordt dat deze al over enkele jaren een marktaandeel van ruim 50% zal hebben.

Zo zijn er meer trends. Wat organisaties op het moment sterk bezighoudt, zijn de flink gestegen beheerkosten van gebouwen. Vooral de explosief toegenomen energiekosten spelen daarin een rol, maar ook de kosten voor algemeen onderhoud stijgen met dubbele cijfers. Dat zorgt voor een snel toenemende interesse in slimme gebouwen, waarin geen energie verspild wordt met het verwarmen, koelen of verlichten van lege ruimten. Elektronisch toegangsbeheer draagt hier in belangrijke mate bij aan een efficiënter gebruik van het gebouw, in dit voorbeeld door flexibele werkplekken zoveel mogelijk te concentreren. Als maar de helft van de werknemers aanwezig is, hoeft ook maar de helft van het gebouw energie te verbruiken.

Naast fysiek toegangsbeheer is digitaal toegangsbeheer voor organisaties nog veel belangrijker. Het valt te betreuren dat deze twee disciplines nog vaak gescheiden werelden zijn. Een effectieve beveiliging is alleen mogelijk als de toegang tot gebouwen en computernetwerken integraal geregeld wordt. Technisch kan dit, maar organisatorisch gebeurt het vaak niet, omdat fysiek toegangsbeheer als iets voor het facilitymanagement wordt beschouwd, terwijl digitaal toegangsbeheer aan de afdeling ICT wordt overgelaten. Het gaat hier om mensen die ‘verschillende talen’ spreken, wat de samenwerking niet ten goede komt. Daarom is het aan te bevelen om de verantwoordelijkheid voor toegangsbeheer hoger in de organisatie te leggen, zodat één afdeling bepaalt wie, waar en wanneer toegang krijgt tot welke ruimtes en ICT-systemen. En dat beperkt zich niet tot één gebouw.

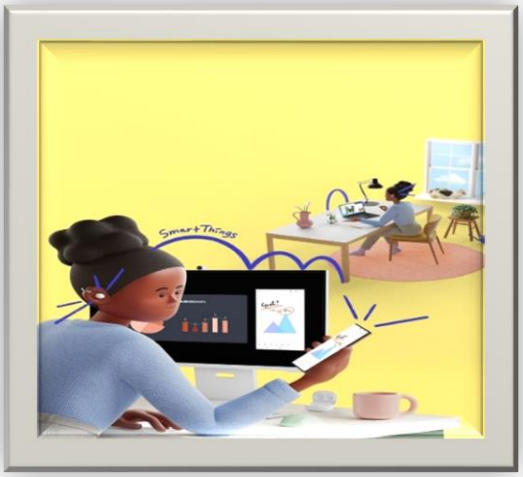
Een laatste trend vormt het stijgend aantal alternatieven voor elektronische toegangspassen. Een daarvan is de smartphone. Gebruikers raken die minder snel kwijt dan pasjes, ze worden minder snel ‘uitgeleend’ en ze bieden extra beveiligingsmogelijkheden, zoals tweefactor-authenticatie. Een ander is biometrie. Deze technologie wordt nu nog vooral bij zeer hoge risico’s gebruikt, maar door de adoptie ervan in het dagelijks verkeer – bijvoorbeeld voor het ontgrendelen van smartphones – is de verwachting dat deuren ook steeds vaker geopend zullen worden met een vingerafdruk of irisscan. Behalve extra veiligheid, biedt dit ook meer gebruikersgemak en zeker dat laatste is bepalend voor de acceptatiegraad. Regelgeving vertraagt de invoering van biometrie, maar naar mate biometrie meer gemeengoed wordt, zal op dit gebied ook steeds meer mogelijk worden.

Samenvattend kunnen we stellen dat toegangsbeheer op dit moment een razendsnelle evolutie doormaakt en dat dit rapport daarin een meer dan welkom inzicht verschaft.

Boele Staal
voorzitter Federatie Veilig Nederland
15 februari 2023

Federatie Veilig Nederland
Zilverstraat 69
2718RP Zoetermeer
info@federatieveilignederland.nl
www.federatieveilignederland.nl

1. EXECUTIVE SUMMARY



De nieuwe werkorganisatie en ETB

Hybride werkmodellen, zowel thuis- als op kantoor werken, zijn tegenwoordig de norm: 96% van alle bedrijven met meer dan 100 medewerkers biedt dit nu aan. De verschuiving van vaste naar flexibele werkplekken, van vaste naar inwisselbare vergaderzalen en het heroverwegen/verlagen van aantal vierkante kantoormeters is een toptrend die de beveiligingsindustrie en dus elektronisch toegangsbeheer domineert in 2022 en verder.

ETB in een volatiele, gepolariseerde wereld

Bedrijven dreigen nog meer in de knel te komen nu de oorlog in Oekraïne voortduurt en aardgas en andere energiebronnen nog duurder of zelfs schaars kunnen worden.

De ontwikkeling van de (verwachte) bedrijfsinvesteringen is weinig hoopvol. De CPB-raming voor 2022 is met 4,5% positief, in 2023 wordt echter -0,3% verwacht.

De voortdurende problemen in de toeleveringsketen zorgen ook voor meer uitdagingen voor bedrijven in de elektronische toegangsmarkt. Halfgeleidertekorten, wereldwijde logistieke knelpunten en bijbehorende kostenstijgingen zullen van invloed zijn op alles, van lezers en bedieningspanelen tot sensoren en detectoren.

ETB-markt: volwassen en sterk evoluerend

ID-badges worden nog steeds wijdverbreid gebruikt , 60% van de organisaties gebruikt ze voor toegangscontrole doeleinden. De progressie van mobiele en biometrische technologie, QR-codes en automatisch kenteken-herkenningssystemen is echter groot. 30% van de bedrijven gebruikt op kleine of grote schaal elektronische toegang op basis van biometrische eigenschappen.

Contactloos en toegang door middel van een mobiel device

46% van de bedrijven plaatst mobiele toegang in de top drie van functies die ze nodig zouden hebben in een nieuw systeem. Nog eens 28% gaf aan dat ze ofwel bezig waren met het upgraden naar mobiele technologie, of dat al hebben gedaan. De technologie is al jaren volwassen, de adoptie lijkt nu groter te worden.

Steeds vaker kiezen gebruikers van ETB-systemen om hun kaarten geheel of gedeeltelijk te gaan vervangen door een oplossing waarmee een lezer bediend kan worden met een smartphone. Naar de gebruiker wordt dan een zogenaamde virtuele kaart verzonden. Het beheer wordt hiermee een stuk flexibeler. Niet ongewoon zijn de “hybride oplossingen” waarbij traditionele toegangspassen worden gecombineerd met mobile access.

ETB in de Cloud

Elektronisch toegangsbeheer oplossingen in een **hosted Cloud omgeving** lopen redelijk in de pas met de penetratie van de overige ICT-systemen binnen de klantorganisaties. De schatting van de leden van de elektronisch toegangsbeheer sectie van de Federatie Veilig Nederland is dat ongeveer 70% van alle organisaties dit gebruiken.

De penetratie van **elektronisch toegangsbeheer as een service uit de Cloud (ACaaS)** daartegen blijft achter. Leveranciers en installateurs van elektronisch toegangscontrolesystemen schatten in dat Elektronisch toegangsbeheer in de Cloud of te wel Access Control as a Service (ACaaS) ongeveer 25% van de markt behelst. Alle partijen zijn echter eensgezind dat binnen 3-4 jaar de penetratie van Access Control as a Service (ACaaS) 40% - 50% van de markt zal behelzen.

ETB en Cybersecurity: twee handen op een buik

Integratie van veiligheid, zowel fysieke als cyber, is onontbeerlijk en vereist een cultuuromslag. Een shift van silo-afdelingen met aparte financieringsbronnen en strategieën naar een van inclusieve en samenwerkende organisatie. Fysieke beveiliging hardware kan een 'toegangspoort' voor cyber-fysieke bedreigingen zijn waardoor een grotere stijging van de vraag voor meer geïntegreerde systemen binnen slimme gebouwen wordt verwacht. 44% van de bedrijven denkt dat slimme gebouwen een belangrijke trend is, die van invloed is op de ETB- sector in de komende jaren.

Duurzaamheid

Er is een groeiende consensus dat eindgebruikers in samenwerking met hun leveranciers duurzaamheid tot een hoeksteen van hun zakelijke beslissingen en activiteiten willen maken. In de komende jaren is de verwachting dat de focus op duurzaamheid zal toenemen. Leveranciers gaan zich meer richten op digitale oplossingen, waaronder end-to-end mobiele en multi-applicatietechnologieën om de voetafdruk van de sector verkleinen.

INLEIDING

Toegangscontrole is van groot belang voor bedrijven en organisaties. Het precies weten wie, waar en wanneer naar binnen mag in een gebouw is natuurlijk van cruciaal belang om de veiligheid te waarborgen. Elektronisch toegangsbeheer zorgt dat de security en safety van gebruikers van locaties zo klantvriendelijk mogelijk gewaarborgd wordt. Wat is de huidige stand van zaken op dit gebied en wat kunnen we verwachten in de toekomst?

Ilisia Marketingservice namens en in opdracht van de sectie Elektronisch Toegangsbeheer van de Federatie Veilig Nederland heeft zorggedragen voor een antwoord op de bovenstaande vragen middels dit trendrapport. De resultaten van dit rapport zijn tot stand gekomen op basis van twee onderdelen:

- **Literatuurstudie**: via deskresearch brachten we de huidige stand van zaken van elektronisch toegangsbeheer in kaart en inventariseerde wij de verschillende, relevante, trends op het gebied van veiligheid, safety en arbeidsorganisatie.

- **Kwalitatieve interviews** met 12 directieleden van leden van de sectie Elektronisch Toegangsbeheer van de Federatie Veilig Nederland over de bovenstaande ontwikkelingen alsmede hun visie over de toekomst van de elektronisch toegangsbeheermarkt.

2. ELEKTRONISCHE TOEGANGSBEHEERMARKT

1.1 Marktafbakening

Elektronisch toegangsbeheer is het proces en bijbehorend technisch systeem dat het **optimaal** en **klantvriendelijk** organiseren van de toegankelijkheid van een terrein, gebouw of ruimte geautomatiseerd en gecontroleerd mogelijk maakt. Daarbij wordt potentieel misbruik of oneigenlijke toegang zoveel mogelijk beperkt. Dit kan zowel een standalone systeem zijn, alsook een systeem gecombineerd met andere safety en securitysystemen.

Voor de opzet van moderne elektronische toegangsbeheersystemen wordt veelal gebruik gemaakt van de zogenaamde OBE-maatregelen of te wel organisatorische-, bouwkundige- en elektronische maatregelen. Door verbreding van de functionaliteit van elektronisch toegangsbeheer ervaren meer en meer gebruikers/eigenaren van dergelijke systemen dat de investering zich sneller terugverdient en de eigen business case verbetert.

2.2 Omvang gebruikersmarkt

Concreet worden elektronische toegangscontrole systemen gebruikt in (CBS, 2022) (NVM, 2022):

- Ongeveer **665.000 bedrijven** met medewerkers en een fysieke vestiging

- Ongeveer **15.000 kantoorgebouwen** met meer dan 47.310.000 m² kantoorruimte
- **3.774 bedrijventerreinen** waar meer dan 66.000 bedrijven in gevestigd zijn

- Ongeveer **258.000 zorginstellingen** in Nederland waaronder,
  - 314 Ziekenhuizen
  - 1022 Verpleeghuizen

- Ongeveer **8.130 onderwijsinstellingen** in Nederland waaronder
  - 6.660 basisscholen
  - 1.440 voortgezet onderwijsinstellingen
  - 62 MBO instellingen en
  - 57 hogere onderwijsinstellingen

- Ongeveer 1.421.000 leerlingen (primair) en 934.000 (voortgezet en hoger) leerlingen

- Ongeveer **9.280 accommodaties** met in totaal 1.400.000bedden (> 4 bedden per vestiging
  - Waaronder 1.590 vakantieterreinen met 342.000slaaplaatsen

- Ongeveer **1.200 culturele en muziekfestivals** met in totaal 24.300.000 bezoekers

3. HUIDIGE STAAT ELEKTRONISCH TOEGANGSBEHEER

3.1 Soort toegangsbeheertechnologie en -systemen in gebruik

Er is weinig twijfel dat toegangscontroletechnologie de afgelopen 10 jaar sterk geëvolueerd is. De progressie van mobiele en biometrische technologie, QR-codes en automatisch kenteken-herkenningssystemen is groot. Naast de al enige tijd beschikbare elektronische systemen met ID-kaarten en Bluetooth-apparaten, biedt dit eindgebruikers nu talloze opties om uit te kiezen.

Het is geen verrassing dat ID-badges nog steeds wijdverbreid worden gebruikt, uit ons onderzoek blijkt dat 60% van de organisaties ze gebruikt voor toegangscontrole doeleinden (wat doet de overige 40%?. Tijd- en aanwezigheidssystemen, waar medewerkers kunnen in- en uitchecken van werk voor salarisadministratie en andere administratieve functies worden door 50% van de bedrijven gebruikt, terwijl nog 49% gebruik van parking/gatecontrole systemen maakt (IFSEC, 2022).

Gebruikte toegangsbeheertechnologie/systemen	Marktpenetratie
Identificatie middel (ID badge)	60%
Tijd & aanwezigheid controle	50%
Parking/gatecontrole systemen	49%
Mobiele identificatie	32%
Biometrische identificatie	30%
Beveiligersrondes applicaties	28%
Kentekenherkenning systemen	25%

Interessant is verder het feit dat 30% van de respondenten (IFSEC, 2022) aangeeft biometrische lezers te gebruiken. Het is onwaarschijnlijk dat de meeste organisaties biometrische gegevens standaard in hun hele bedrijf gebruiken. De technologie wordt nog steeds gebruikt om gebieden met een hogere prioriteit te beschermen.

Bijna 32% van de eindgebruikers geeft aan dat ze niet wisten welke elektronische toegangsbeheer technologie hun organisatie gebruikte. Een indicatie dat gebouwbeheerteams niet altijd op de hoogte van de specifieke kenmerken van hun oplossing zijn.

3.2 Tevredenheid gebruikers met huidige oplossing

Over het algemeen zijn beveiligings- en facility managers van mening dat hun huidige oplossing voor elektronische toegangsbeheer op zijn minst voldoet aan de essentiële eisen, waarbij de meerderheid aangeeft dat ze voldoen aan de huidige vereisten of deze overtreffen. 12% antwoordde dat hun huidige oplossing niet voldeed aan de gestelde eisen.

	Effectiviteit huidige elektronische toegangsbeheeroplossing	Geschatte marktpenetratie
	Voldoet aan de essentiële eisen	47%
	Voldoet aan alle eisen	33%
	Voldoet niet	12%
	Overtreft alle eisen	3%
	Voldoet aan alle huidige **en** geplande eisen	5%

Technologie en op IP gebaseerde oplossingen blijven zich in een snel tempo ontwikkelen - om nog maar te zwijgen van kwetsbaarheden in oudere, verouderde systemen. Het onderhouden en bijtijds upgraden van de elektronische toegangsbeheer oplossingen van bedrijven is essentieel. De 2022 EMEA resultaten (IFSEC, 2022) op het gebied van de ouderdom van de belangrijkste componenten van een elektronisch toegangsbeheer oplossing zien er als volgt uit:

Ouderdom componenten huidige elektronische toegangsbeheeroplossing			
	> 3 jaar	3 – 6 jaar	< 6 jaar
Componenten	42%	39%	19%
Software	46%	39%	15%

De bovenstaande cijfers zijn gebaseerd op interviews met beveiligingsmanagers/directeuren, CISO- en CSO-rollen en facility managers/directeuren. Deze functies betreffen over het algemeen besluitvormers, of degenen die invloed hebben op beslissingen over de keuze van de toegangscontroleoplossing die hun bedrijf gebruikt.

De respondenten zijn werkzaam binnen een brede dwarsdoorsnede van sectoren, waaronder die uit de telecommunicatie, professionele dienstverlening, overheid, onderwijs, bankieren/financiën, gezondheidszorg en handel. Daarnaast werken de respondenten ook in verschillende bedrijfsgroottes, hoewel organisaties met minder dan 500 werknemers iets meer dan de helft (52%)

van de ondervraagden uitmaken. Ongeveer 15% van de respondenten werkte in organisaties met meer dan 10.000 werknemers, wat erop wijst dat ook grote nationale of multinationale ondernemingen goed vertegenwoordigd zijn.

3.3 “Real time” locatie medewerkers en bezoekers

Elktronische toegangsbeheersystemen worden gebruikt voor het in kaart brengen van de locatie (binnen de bedrijfsgebouwen) van zowel de eigen medewerkers als de bezoekers. Daarnaast kunnen systemen voor “real time tracking” gebruikt worden.

Een derde (35%) van de respondenten (IFSEC, 2022) geeft aan de locatie van medewerkers en bezoekers “real time” te kennen. Nog eens 35% antwoordde dat ze, door middel van hun elektronisch toegangsbeheersysteem, het aantal personen kenden, maar niet de “real time” locatie. 23%, meestal kleinere bedrijven, wisten noch de locatie noch het aantal bewoners. Dit geeft aan dat kleinere bedrijven niet per se waarde in investeringen in “real time” locatiebewaking zien.

Het gebruik van “real time” locatieservices is nog steeds relatief laag. Het gebruik zal naar verwachting groeien naarmate de trend naar intelligentere gebouwen zich voortzet. Er is een groot verschil is in de manier waarop bezoekers worden gecontroleerd in vergelijking met werknemers. Organisaties gebruiken liever een papieren rooster (33%) om bezoekers te monitoren, terwijl zij meer geavanceerde toegangscontrolesystemen voor personeel gebruiken (39%).

4. ELEKTRONISCH TOEGANGSBEHEERMARKT BINNEN EEN COMPLEXE, VOLATIELE OMGEVING

4.1 Impact energiecrisis en Oekraïne oorlog

Bedrijven dreigen nog meer in de knel te komen nu de oorlog in Oekraïne voortduurt en aardgas en andere energiebronnen duurder of zelfs schaars worden. De hoge energiefacturen, de stijgende inflatie en de verwachte terugvallende economische groei zorgen voor grote onzekerheid.

De vooruitzichten voor de Nederlandse economie in de periode 2022-2023 zijn diffuus. Het Centraal Plan Bureau (CPB) berekent in haar augustus 2022 raming dat het BBP in 2022 met 4,5% groeit om in 2023 naar 1,1% terug te vallen (CPB, 2022).

De inflatie stijgt naar verwachting in 2022 naar een duizelingwekkende 11,4% en naar verwachting een 4,5% in 2023. Belangrijk voor de elektronische toegangsmarkt is de ontwikkeling van de (verwachte) bedrijfsinvesteringen. De CPB-verwachting is weinig hoopgevend; de raming voor 2022 is met 4,5% positief, in 2023 wordt echter -0,3% verwacht.

De voortdurende problemen in de toeleveringsketen zorgen ook voor meer uitdagingen voor bedrijven in de elektronische toegangsmarkt. Halfgeleidertekorten, wereldwijde logistieke knelpunten en bijbehorende kostenstijgingen zullen van invloed zijn op alles, van lezers en bedieningspanelen tot sensoren en detectoren.

4.2 Impact corona op elektronische toegangsmarkt

Ondernemers en instellingen hebben de afgelopen 2 jaar veel ervaring opgedaan en weten welke preventieve maatregelen en interventies het beste in de praktijk werken. De samenleving zo open en veilig mogelijk houden – dat is het uitgangspunt van de corona langetermijnstrategie van het kabinet.

De economie is krachtig hersteld in 2022, na de forse krimp van het bruto binnenlands product (bbp) in 2020 met 3,7% en de verwachte faillissementengolf bleef uit (CBS, 2022).

De impact van de pandemie op de elektronische toegangsmarkt wordt eigenlijk zichtbaar op het gebied van de contactloze oplossingen en het aantal structureel thuiswerkende medewerkers, waarover straks meer.

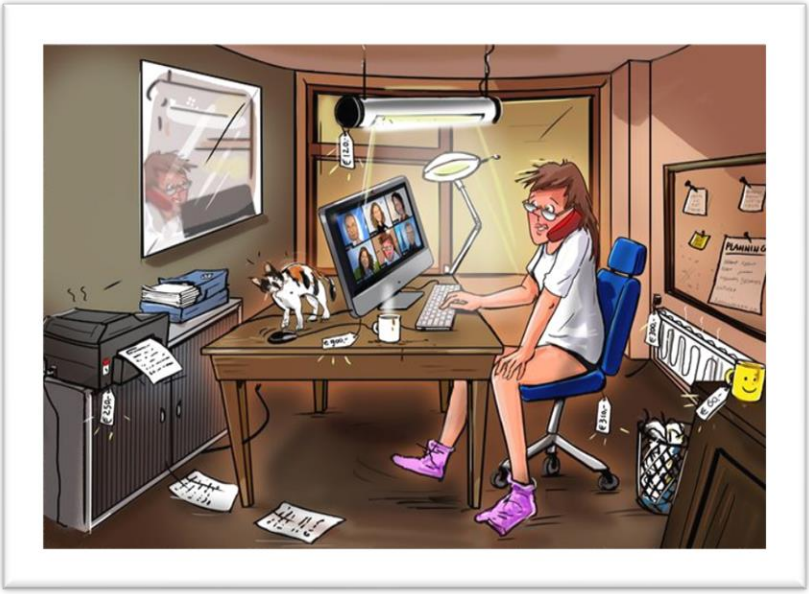
4.3 Opmars van contactloos oplossingen

Experts (WRR, KNAW, 2022) hebben betoogd dat veel 'trends' werden versneld door de pandemie eerder dan nieuw gecreëerd te zijn. Integratie en werken op afstand, alsmede contactloze oplossingen zijn hier voorbeelden van. Contactloze oplossingen waren al vóór 2019 beschikbaar maar door de pandemie werden ze voor veel organisaties 'bedrijf kritisch'.

Organisaties in de gezondheidzorg, voedingsindustrie en recreatie hebben al voor de pandemie aangedrongen op contactloze oplossingen, waar het gros van kantoor- en residentiële gebouwen dit als "nice" en niet "need to have" zagen. Een vijfde van het EMEA-rapport respondenten claimt nu dat contactloze technologie de grootste impact op het verbeteren van hun fysieke toegangscontrole is.

Nog eens 43% van de respondenten bestempelt contactloze oplossingen als een van de top drie vereiste functionaliteiten van een nieuw toegangscontrolesysteem.

De invloed van de pandemie ziet men terug in de uitspraak van 32% van de respondenten dat 'contactloze functionaliteit introductie' een van de 3 belangrijkste "drivers" voor de volgende fysieke toegangscontrolesysteem upgrade is.



4.4 Het thuiswerken en elektronisch toegangsbeheer

Hybride werkmodellen zijn tegenwoordig de norm en een zero-trust-benadering voor iedereen is een toptrend die de beveiligingsindustrie domineert in 2022 en verder. Medewerkers werken dus afwisselend zowel thuis als op kantoor waarbij iedereen, directie en medewerkers, op dezelfde (cyber)veilige wijze gefaciliteerd worden.

Functionarissen zijn belast met enerzijds het waarborgen van een veilige omgeving voor degenen die terugkeren naar kantoor en anderzijds met veilig identiteits- en toegangsbeheer voor degenen die op afstand werken. Zij zijn op zoek naar best practices die dit mogelijk maken. Touchless-oplossingen, gegevensbescherming en technologieën voor bezoekersbeheer zorgen voor gezonde en veilige on-site-omgevingen, terwijl multi-factor authenticatie-oplossingen centraal staan voor toepassingen op afstand.

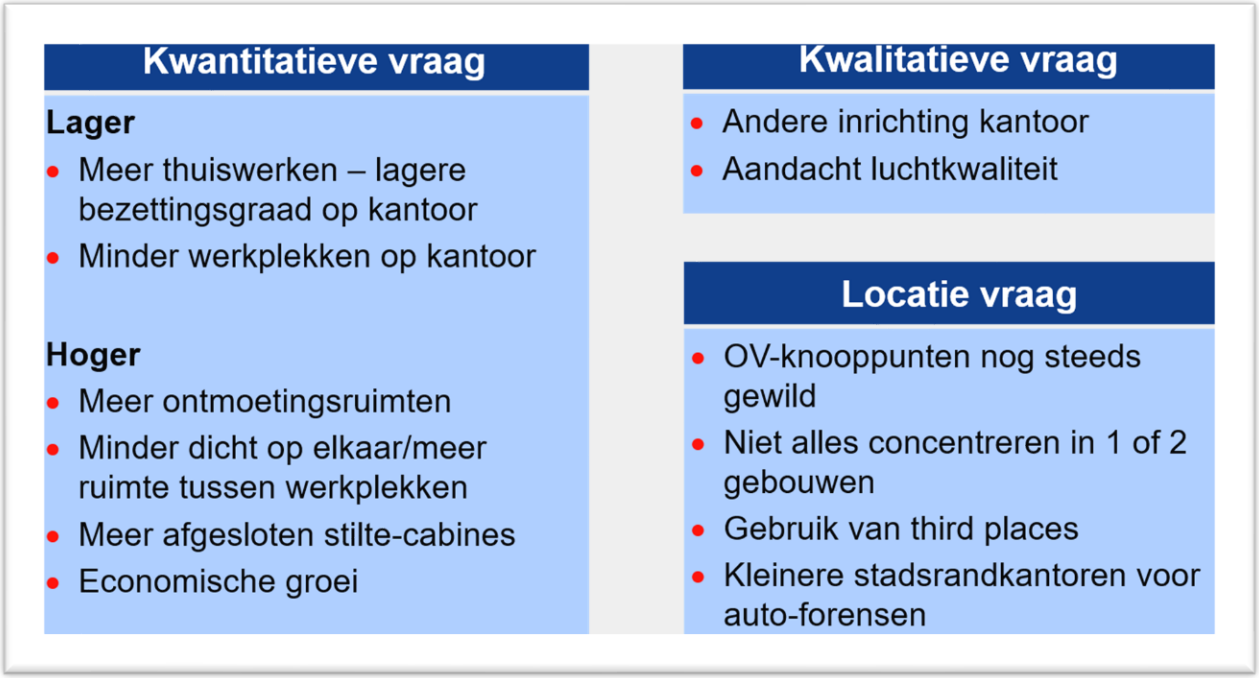
Onderzoeksresultaten over de ontwikkelingen op het aantal **structureel** thuiswerkende medewerkers wijzen uit naar een grote, blijvende, groei. 25% van de organisaties in de non-profit sector (regionale overheid en zorg) en de dienstverlenende sectoren melden een sterke groei (meer dan 50%) van het aantal structureel thuiswerkende medewerkers (Ilisia, 2021).

Consequenties voor de kantorenmarkt

De verschuiving van vaste naar flexibele werkplekken, van vaste naar inwisselbare vergaderzalen en het heroverwegen/verlagen van aantal vierkante kantoormeters zal zeker doorgaan maar in kleine stappen en zeker niet als vervolg van disruptieve werking van de coronapandemie (STEC, 2021) (Ilisia, 2021).

De komende vijf jaar wordt er een lichte daling voor de kantorenmarkt verwacht (STEC, 2021). De kantoorruimte wordt anders ingericht: zo is er meer behoefte aan individuele werkplekken waar men zich op kantoor kan afzonderen en is er meer aandacht voor de interne luchtkwaliteit van kantoren.

Met inbegrip van het feit dat élk bedrijf zijn eigen afweging maakt en dat er met betrekking van de toekomst van corona nog behoorlijk wat onzekerheid is, hieronder door Buck Consultants International (Buck Consultants, 2021) een voorzichtige inschatting voor de Nederlandse kantorenmarkt:



De geschetste ontwikkelingen genereren zowel kansen als bedreigingen voor de elektronische toegangsbeheermarkt. In de tabel op de volgende pagina worden deze schematisch weergegeven.

KANSEN	BEDREIGINGEN
Geen vaste bezetting meer in de panden, de sociale controle is lager waardoor gevoel van onveiligheid toeneemt. Een adequate beveiliging is dan een vereiste waaronder ETB	Door lagere bezettingsgraden van gebouwen en daardoor minder aanwezigheid van personeel betekent minder toezicht.
Het afsluiten van gebouwdelen en ruimtes wordt belangrijker. Hier zal naar onze verwachting geïnvesteerd gaan worden in uitbreidingen op toegangsbeheer	Focus eerst op het opstarten van de core activiteiten en dus niet direct budget klaar staan voor nieuwe infrastructuur
Flexibeler werken betekent meer behoefte aan flexwerkplekken en meeting ruimtes. Er komt dus meer vraag naar toegangscontrole en sleutel management van remote sites.	Levertijden en prijzen zullen stijgen doordat grondstoffen duurder worden.
Werkgevers willen toch echt wel dat de werknemer wekelijks minimaal een aantal uren op kantoor werkt. Een toegangscontrole systeem kan straks heel eenvoudig bijhouden hoeveel uur iemand op kantoor geweest is. Daarnaast denk ik aan een soort werkplekreservatiesysteem dat sowieso gekoppeld kan/zal worden met een elektronisch toegangscontrolesysteem	
Kantoorgebouwen die omgebouwd gaan worden tot appartementencomplexen dienen ook voorzien te worden van toegangscontrole en deurintercom, en vooral het laatste is een grote groeimarkt.	
Combinatie van toegangscontrolesystemen met andere systemen zoals inbraakdetectiesystemen, video met bijkomende een managementsoftware om de verschillende systemen naadloos met elkaar te laten samenwerken.	

4.5 Slimme gebouwen

Het anders inrichten van de kantoorruimte wordt daarnaast noodzakelijk door de voortdurende evolutie van slimme gebouwen welke zeker een grote impact zal hebben op elektronisch toegangsbeheersystemen.

De term “smart building” wordt nog vaak als relatief vaag ervaren omdat er meer nodig is dan alleen bewakings- en technologiesensoren om een gebouw slim te maken.

In plaats daarvan moet een faciliteit deze technologie gebruiken om voordelen en efficiëntie voor gebruikers te creëren.

Dit geschreven hebbende, gelooft meer dan de helft (51%) van de respondenten (IFSEC, 2022)dat slimme gebouwen de toekomst van elektronisch toegangsbeheer zullen bepalen. Gerelateerde slimme technologieën als kunstmatige intelligentie (AI), Internet of Things, locatieservices en energie-efficiëntie zullen een sleutelrol spelen bij het intelligenter maken van een gebouw.

Een slim gebouw zal waarschijnlijk veel van deze technologieën gebruiken, zoals IoT-apparaten die met elkaar communiceren, locatieservices die “real time” bezettingsbewaking bieden en AI waarmee eindgebruikers beter geïnformeerde beslissingen kunnen nemen over de beveiliging en efficiëntie van een gebouw. De oplossing voor toegangscontrole zou ook worden geïntegreerd in dit intelligente gebouwbeheersysteem, op voorwaarde dat dit veilig kan.

5. INTEGRATIE FYSIEKE EN DIGITALE BEVEILIGING: BITTERE NOODZAAK

Fysieke en digitale beveiliging zijn van oudsher gescheiden (CAP GEMINI, 2021). In toenemende mate voeren echter criminelen en overige kwaadwilligen gecombineerde aanvallen uit op fysieke en digitale beveiliging of kiezen de zwakste schakel van een van de twee.

In 2018 een medewerker van een IT-bedrijf kwam voor regulier onderhoud bij een Britse bank. In werkelijkheid was hij een crimineel die malafide IT-apparatuur en software binnen de IT-infrastructuur van de bank installeerde om vervolgens op afstand € 1,5 miljoen te stelen (CSO.com, 2018).

Ook Nederland heeft ervaring met soortgelijke voorvallen. Eveneens in 2018 richtten enkele Russische inlichtingenofficieren hun pijlen op het gebouw van de organisatie voor het verbod op chemische wapens (OPCW). Hiervoor benaderden zij het OPCW-fysiek als bezoekers om vervolgens het WIFI-netwerk van het OPCW te hacken (Government.nl, 2018).

5.1 Uitdagingen bij het integreren van fysieke en digitale beveiliging

De grootste uitdagingen zijn van organisatorisch aard. Beveiliging is meestal op verschillende plekken binnen de organisatie gelegd. Digitale beveiliging, cybersecurity, ligt op het bord van de ICT-afdeling.

De fysieke beveiliging is de verantwoordelijkheid van de afdeling facilitaire zaken en is meestal uitbesteed aan derde partijen.

De afstand van beide afdelingen tot het hoogste management is ook verschillend. In het licht van de enorme toename van cybersecurity aanvallen, in het bijzonder “ransomware” aanvallen, is de aandacht van het hoogste management voor cybersecurity enorm toegenomen en als zodanig zijn de communicatielijnen met de ICT-afdeling aanzienlijk korter geworden. In het geval van fysieke beveiliging blijft de afstand tot het hogere management groter. Daardoor is er vaak onvoldoende budget voor een adequate en up-to-date elektronische toegangsbeheer oplossing.

(ID) Data en hun organisatie is ook een grote uitdaging.

Een uitdaging die gepaard gaat met het gescheiden organiseren van fysieke en digitale beveiliging is het hebben van meerdere bronnen van identiteitsgegevens. Deze gegevens zijn essentieel om te bepalen of een individu fysieke toegang tot een gebouw en/of digitale toegang tot informatiesystemen van de organisatie heeft.

Binnen veel organisaties worden aldus identiteiten in meerdere plekken opgeslagen. Vaak bevatten deze identiteitssystemen verschillenden data. Volgens het ene systeem zou een medewerkers toegang tot meerdere gebouwen mogen hebben, terwijl het HR-systeem aangeeft dat deze medewerker uit dienst is.

Bij organisaties met een bepaalde mate van integratie van identiteitsdata gaat het voornamelijk over data integratie voor de eigen medewerkers. Voor gasten en externe partijen is er vaak een apart systeem. ***Het is dus – ook hier - noodzakelijk om beveiliging centraal aan te sturen met commitment van hogere management.*** Een integrale aanpak zorgt voor een verbetering van de beveiliging en verlaging van bedrijfsrisico’s.

De leden van de elektronische toegangsbeheer sectie van de Federatie Veilig Nederland geven aan dat het ‘cyber veilig’ maken en houden van de ETB-systemen steeds belangrijker wordt. Software (update) services zijn ingevoerd en worden gemeengoed. De ICT-afdeling van de klant dient bij het proces betrokken te worden om gezamenlijk de juiste stappen tijdens de implementatie van het ETB-systeem te zetten.

5.2 Integratie elektronisch toegangsbeheer met overige informatiesystemen

Aangezien het elektronisch toegangsbeheersysteem een wezenlijk onderdeel van het totale veiligheidsplatform van een gebouw of terrein is wordt het al lang geïntegreerd in het algemene facility managementsysteem (FMS).

De leden van de elektronische toegangsbeheer sectie schatten dat dit een feit bij ongeveer 50% van alle bedrijven is in Nederland en groeit naar verwachting tot 60% in 2025.

Hetzelfde beeld wordt geschetst voor de integratie van het elektronisch toegangsbeheersysteem met het algemene building managementsysteem (BMS). Volgens de schatting van de leden van de elektronische toegangsbeheersectie is dit een feit bij ongeveer 50% van alle bedrijven in Nederland en groeit naar verwachting tot 70% in 2025.

De mate van integratie van het elektronisch toegangsbeheer systeem met specifieke informatiesystemen zoals Human Resources (HR), Customer Relations (CRM) of logistiek/warehouse systemen is in het algemeen nog laag. Volgens de schatting van de leden van de elektronische toegangsbeheersectie is bijvoorbeeld bij ongeveer 10% van de bedrijven het elektronische toegangsbeheersysteem geïntegreerd met het VMS-systeem en naar verwachting groeit dit tot 20% in 2025.

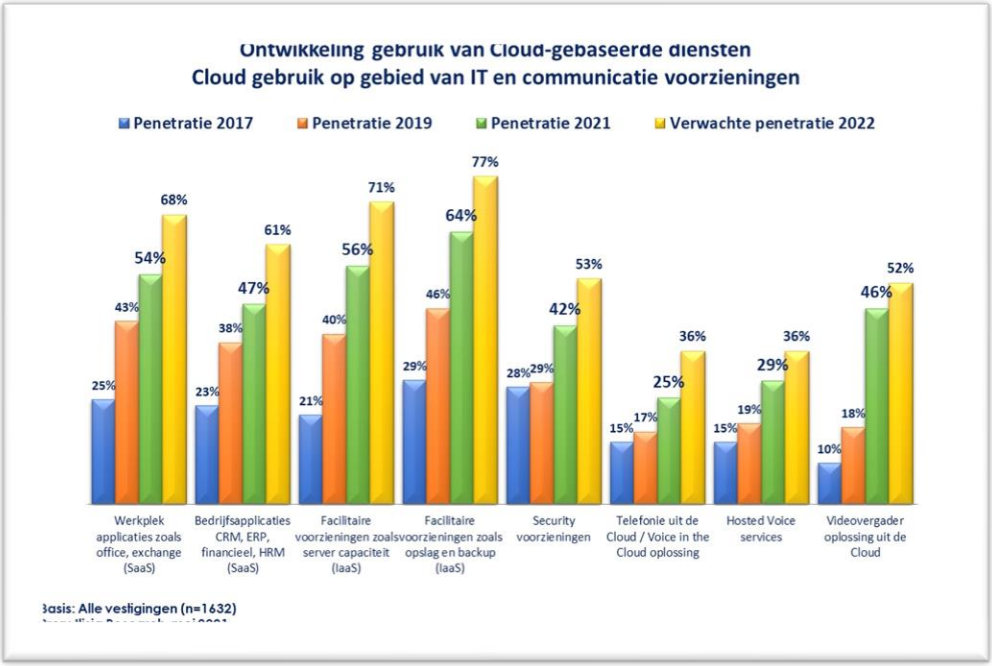
Momenteel speelt de vraag naar totale integratie binnen de grote bedrijven die gebruik van “grotere”, complexe elektronisch toegangsbeheersystemen maken. Bij de MKB-bedrijven wil men vooral een oplossing die makkelijk te gebruiken is wanneer men het nodig heeft.

Naast het integraal beheren van informatiesystemen is er bijkomend de trend om dit op afstand te doen zodat een probleem sneller opgelost kan worden. Daardoor verwachten verschillende systemintegrators dat hun operationele kosten verlaagd worden met als resultaat uiteindelijk een gunstiger kostenplaatje voor de eindgebruiker. Dit laatste zal allicht ook een grotere rol gaan spelen in het beheer van het systeem waarbij er duidelijke afspraken tussen de systemintegrator en de eindgebruiker vastgelegd dienen te worden.

Elektronisch toegangsbeheersystemen met integratiemogelijkheden worden tevens betaalbaarder. Een voorbeeld ervan is toegangscontrole gecombineerd met video. Aan de hand van een toegangscontrolegebeurtenis kunnen videobeelden heel eenvoudig terugkeken worden. “Video analytics”, automatisch een deur openen wanneer iemand richting die deur loopt, een deur sluiten wanneer een verplaatsing afgerond is zijn een paar voorbeelden waarvan systemintegrators verwachten dat dit meer en meer gevraagd zal worden.

6. ELEKTRONISCH TOEGANGSBEHEER ‘AS A SERVICE’

6.1 Cloud is mainstream geworden



De tijd dat Clouddiensten alleen maar voor perifere IT-voorzieningen werden ingezet is al lang voorbij. Steeds vaker schakelen organisaties Cloud leveranciers in voor hun ‘core’-ICT voorzieningen.

De onderstaande grafiek, uit de jaarlijkse Convergentie monitor van Ilisia Research weergeeft de huidige stand van zaken m.b.t. Cloud (Ilisia, 2021).

6.2 Hosten en de Cloud

Een belangrijk onderdeel van de discussie over elektronisch toegangsbeheer als een service uit de Cloud (ACaaS) spitst zich toe op de vraag of er gebruik wordt gemaakt van een hosting in de Cloud model of de Cloud?

Hosting in de Cloud is het model waarbij het centrale IT-systeem, de server en de database, en het onderhoud daarvan worden uitbesteed aan een datacenter. Het systeem zelf verandert niet, maar bepaalde componenten en services worden bij de klant weggehaald.

Bedrijven die gebruik maken van **dit model p**laatsen de eigen private ICT-omgeving dus bij een externe partij. De ETB-oplossing is nog afgeschermd, meestal via VPN-verbindingen.

'As a Service' s een containerbegrip voor onlinedienstverlening waarbij de zorg voor data, beschikbaarheid en schaalbaarheid worden uitbesteed en als een dienst wordt ingekocht. Bedrijven die **elektronische toegangsbeheer uit de Cloud** hebben, maken gebruik van verschillende externe datacenters. De infrastructuur, updates et cetera wordt gereed gemaakt voor meerdere klanten en er wordt altijd gebruik van openbare internetverbindingen gemaakt.

Elektronisch toegangsbeheer oplossingen in een **hosted Cloud omgeving** (geen ACaaS) lopen redelijk in de pas met de penetratie van de overige ICT-systemen binnen de klantorganisaties. De schatting van de leden van de elektronisch toegangsbeheer sectie van de Federatie Veilig Nederland komt ongeveer op 70% uit.

6.3 Elektronisch toegangsbeheer as a service (ACaaS)

De penetratie van elektronisch toegangsbeheer as een service uit de Cloud (ACaaS) daartegen blijft achter. Leveranciers van elektronisch toegangscontrole systemen en installateurs schatten in dat Elektronisch toegangsbeheer in de Cloud of te wel Access Control as a Service (ACaaS) ongeveer 25% van de markt behelst. Alle partijen zijn echter eensgezind dat binnen 3-4 jaar de penetratie van Access Control as a Service (ACaaS) 40% - 50% van de markt zal behelzen.

Sommige systemintegrators geven aan dat Access Control as a Service (ACaaS) op dit moment door kleinere organisaties wordt omarmd.

Zij constateren echter dat de functionaliteit en integratiemogelijkheden van ACaaS oplossingen blijft momenteel wel achter bij traditionele systemen.

Tegelijkertijd wordt er geconstateerd dat veel bedrijven inmiddels gewend zijn om hun data in de Cloud te zetten. Zij zijn minder bang om servers in de Cloud te zetten en/of Clouddiensten af te nemen.

In high security omgevingen is een "dedicated eiland oplossing" om geen enkele invloed van buitenaf mogelijk te maken nog steeds de regel. In die gevallen wordt de elektronische beveiliging dan ook vaak als gebouw gebonden oplossing gezien met extreem veiligheidsbelang. De verwachting is echter dat ook hier op afzienbare tijd verandering in zal komen.

ACaaS is een populaire oplossing voor organisaties die kiezen voor ontzorgen en graag continu up-to-date willen blijven. Veel aanbieders in de markt leveren nu nog vaak beperkte functionaliteit en de beveiliging van zowel data als de apparatuur op locatie verdienen extra aandacht. De verwachting is dat ontwikkelingen op het gebied van functionaliteit en veiligheid elkaar in de komende jaren snel zullen opvolgen. Dat maakt ACaaS beschikbaar voor een steeds grotere groep afnemers.

7. BIOMETRIE

7.1 Biometrie is gemeengoed geworden

Een vingerafdruk om je smartphone te ontgrendelen. Een creditcardbetaling doen met een selfie. Een telefoonabonnement verlengen op basis van je stemgeluid. Biometrie is het herkennen van individuen door middel van een lichaamskenmerk en met behulp van informatietechnologie en biedt allerlei kansen om consumentendienstverlening snel en makkelijk te maken. Tegelijkertijd breidt het toepassingsgebied van biometrie zich uit. Want in een anonieme, digitale samenleving is het belang van persoonsherkenning groter dan ooit.

Biometrische identificatie toepassingen zijn naast vingerafdrukken, irisscans, scans van het gezicht en de handpalmen. En voor steeds meer toepassingen worden biometrische verificatiemethoden ingezet zoals het Nederlandse paspoort welke inmiddels voorzien van een vingerafdruk is. De Amerikaanse grenscontrole kom je niet meer door zonder het afgeven van je vingerafdruk en irisscan. En op meerdere luchthavens, waaronder Schiphol, is men bezig om reizigers met behulp van een eenmalige gelaatsscan snel door het proces te leiden.

Er bestaat wel degelijk weerstand tegen het gebruik van biometrie als authenticatiemiddel. Mensen staan niet graag hun biometrische gegevens af, vooral niet aan commerciële partijen. De bereidheid om biometrische gegevens te gebruiken voor het betalen in webshops, voor het gebruiken van apps en het zoeken via Google is nog steeds beperkt.

De veiligheid van opgeslagen data is een veelgenoemd zorgpunt. Als een biometrisch gegeven in verkeerde handen valt, zijn de gevolgen niet te overzien. In tegenstelling tot een wachtwoord kan een vingerafdruk of irisscan nu eenmaal niet gewijzigd worden.

Bovendien worden databanken steeds meer, zelfs internationaal, gekoppeld. Bij identiteitsdiefstal kan daardoor een heel scala aan persoonsgegevens op straat komen te liggen.

Capgemini in haar Trends in Veiligheid rapport (CAP GEMINI, 2021) signaleert dat de acceptatie van biometrie toeneemt. De zorgen om privacy en veiligheid over apps, smartphones en webshops zijn nog relatief beperkt. Het gebruik van de vingerafdruk om de mobiele telefoon te ontgrendelen is nu de dominante manier geworden.

Bij high securityklanten staat biometrie absoluut niet ter discussie en wordt breed toegepast. Wel vergt het soms overredingskracht bij werknemersvertegenwoordigingen (OR) om biometrie in te voeren.

Reactie respondent:

"Nu biometrie op smartphones gemeengoed is geworden is de acceptatiegraad op individueel niveau enorm gestegen. Toepassing en vastlegging door werkgevers daarentegen stuit op verzet en tegenstand. Dit is een eigenaardige contradictie waar wij niet direct een verklaring voor hebben. Het lijkt op de privacy discussie: iedereen maakt zich daar bedrijfsmatig zorgen over maar deelt vervolgens in het privédomein alles via social media. "

Experts zijn het erover eens dat voor de adequate beveiliging van biometrische toepassingen een complex samenspel van techniek, organisatie en procedures nodig is, met voldoende aandacht voor de menselijke factor.

Reactie respondent:

"Belangrijk is steeds dat de eerste registratie en verificatie van de biometrische gegevens goed verlopen, waarbij een two- factor verification zeker kan helpen. Dan combineer je bijvoorbeeld iets wat je weet, zoals een wachtwoord, met iets wat je bent, zoals een vingerafdruk. Dat maakt de kans op fouten en hacks kleiner. Helaas krijg je al wel al snel een trade-off: want hoe beter de beveiliging, hoe minder het gebruiksgemak."

De leden van de elektronische toegangsbeheer sectie van de Federatie Veilig Nederland schatten de penetratie van biometrische readers in Nederland als volgt:

Gebruikte biometrische oplossing	Geschatte marktpenetratie
Vingerafdruk lezers	12%
Gezichtsherkenning lezers	10%
Irisscan lezers	6%
Palmader / vingerader lezers	1%

7.2 Privacywetgeving en biometrie

In de Algemene verordening gegevensbescherming (AVG) worden “biometrische gegevens met het oog op de unieke identificatie van een persoon” gezien als “bijzondere persoonsgegevens”. Het verwerken van bijzondere persoonsgegevens is verboden tenzij sprake is van een uitzondering.

Voor de praktijk betekent dat dit dat er een beperkt aantal uitzonderingen beschikbaar is. De belangrijkste daarvan voor de praktijk van de elektronische beheersystemen zijn wettelijke grondslag en veel belangrijker

Reactie respondent:

“AVG is terecht een dominant onderwerp bij toepassing van biometrie. Wij hebben door middel van een eigen data protectie functionaris (DP-officer) de dienstverlening opgetuigd voor onze klanten om het proces van AVG goed het hoofd te bieden”.

uitdrukkelijke toestemming van de gebruiker. Kortom: werkgevers kunnen gewoon toestemming vragen voor het verwerken van biometrische gegevens zolang zij daarnaast een redelijk alternatief bieden.

Reactie respondenten:

"Er is zeker en vast een markt voor biometrische identificatie maar stel vast dat dit momenteel ook een nicheproduct is. Daarnaast kan ik me ook voorstellen dat met het hele COVID-19 gebeuren klanten op zoek gaan naar contactloze oplossingen. Biometrische identificatie via vingerafdruk zal hierdoor onder druk komen staan. Irisscan oplossingen waarbij geen aanraking noodzakelijk is worden steeds meer gevraagd".

De toekomst belooft een gestage groei van de toepassing van biometrie, maar men dient er goed op te letten of gegevens wel zorgvuldig worden opgeslagen en gebruikt. Experts vragen zich af of de wetgever er op tijd bij is met wet- en regelgeving om misbruik te voorkomen. Vaak ontstaat het besef dat iets wettelijk geregeld moet worden pas als er eerst iets echt is misgegaan.

Reactie respondenten:

"Biometrie is een groeiende markt, gebruikers vragen naar stabiele goedwerkende oplossingen en hebben hier budget voor. Er is dringend nood aan een duidelijkere wetgeving hierrond zodat kwalitatieve fabrikanten hun producten kunnen laten certificeren. Zo kunnen gebruikers een leidraad hebben voor de selectie van hun apparaten. Nu loopt de wetgeving

8. MOBIELE TECHNOLOGIE EN ELEKTRONISCH TOEGANGSBEHEER

8.1 Mobiele apparatuur is gemeengoed geworden

Mobiele apparatuur (smartphones en tablets) is in de afgelopen jaren gemeengoed geworden in zakelijke omgevingen. Dit heeft natuurlijk een rechtstreeks verband met het aandeel bedrijven dat medewerkers met een (deels) mobiele functie kent en het aantal bedrijven die mobiele devices aan hun medewerkers ter beschikking stellen.

Het aandeel medewerkers in Nederland met een deels mobiele functie is ongeveer 50%. Het overgrote deel van de bedrijven kent medewerkers die gebruik maken van smartphone en/of tablet. Het percentage van alle medewerkers dat een smartphone voor zakelijk gebruik heeft, al is het deels in eigendom van de gebruiker, groeit wel in 2021 naar 69% (Ilisia, 2021).

Het percentage bedrijven dat tablets aan hun medewerkers verstrekt/vergoedt blijft in 2021 stabiel op ongeveer 48%. Het percentage medewerkers met een tablet/IPad van de zaak daalt wel van 36% in 2019 naar 32% in 2021. De meeste medewerkers met een mobiele device zijn nog steeds werkzaam binnen kleinere/middelgrote bedrijven binnen de dienstverlenende en non-profit sectoren.

8.2 Mobiele toegang

Hoewel het gebruik van mobiele devices voor toegangscontrole slechts een paar jaar geleden nog in de relatieve kinderschoenen stond, verwacht de meerderheid van de respondenten uit het 2022 EMEA rapport van IFSEC een versnelling van de invoering van mobiele inloggegevens binnen organisaties. Dit zal een dramatische impact op de ontwikkeling van toegangscontrolesoftware op mobiel toepassingen hebben.

De vraag is er wel en wordt alsmaar groter. Verschillende systemintegrators melden dat bij de meeste nieuwe aanvragen een belangrijke wens toegang door middel van een mobiele device is. Steeds vaker kiezen gebruikers van ETB-systemen om hun kaarten geheel of gedeeltelijk te gaan vervangen door een oplossing waarmee een lezer bediend kan worden met een smartphone. Naar de gebruiker wordt dan een zogenaamde virtuele kaart verzonden. Het beheer wordt hiermee een stuk flexibeler. Niet ongewoon zijn de “hybride oplossingen” waarbij traditionele toegangspassen worden gecombineerd met mobile access.

Meer dan de helft (52%) van de eindgebruikers (IFSEC, 2022) gelooft dat mobiele toegang of applicaties een van de belangrijkste trends zal zijn om de toekomst van toegangscontrole vorm te geven. Nog eens 46% plaatste mobiele toegang in de top drie van functies die ze nodig zouden hebben in een nieuw systeem, terwijl 28% van de respondenten aangaf dat ze ofwel bezig waren met het upgraden naar mobiele technologie, of dat al hebben gedaan. Zelfs degenen die nog moeten upgraden, erkenden de behoefte aan mobiele lezers.

Dit geschreven hebbende blijft een feit dat toegangsverlening met mobiele apparaten in Nederland al jaren als een belofte boven de markt hangt. Volgens schatting van de leveranciers en installateurs van elektronische toegangsbeheersystemen behelst dit momenteel 10% van alle ETB-systemen en naar verwachting groei dit percentage tot 25% in 2025. De technologie is al jaren volwassen, de adoptie echter blijft sterk achter.

Reactie respondent:

Dit is een groeiende markt merken wij. Steeds vaker als klanten een nieuw ETB-systeem aanschaffen of hun oude leestechnologie gaan vervangen kiezen ze voor een smartphone als identificatiemiddel. Vaak wel in combinatie met een lezer die nog steeds de vertrouwde kaart of druppel kan gebruiken voor gebruikers die niet willen dat hun privé telefoon een zakelijke functie krijgt. Vaak laat de werkgever de keuze aan de medewerker. Als men een kaart of druppel gebruikt wordt ook deze vervangen voor een veilig exemplaar. Procentueel gezien zien we dat bij 5% van de lezers er gekozen wordt voor een lezer die met smartphones overweg kan om de smartphone gelijk al te gaan inzetten of omdat ze dit wellicht in de toekomst willen gaan doen. We dienen er wel bij stil te staan dat bij sommige oplossingen het beheer van de virtuele kaarten een goede voorbereiding en veel werk met zich mee kan brengen

.

9. APPENDIX

IDENTIFICATIEMIDDELEN ELEKTRONISCHE TOEGANGSSYSTEMEN

Toegangscontrolesystemen maken gebruik van herkenning via identificatiemiddelen. Het is daarom van belang om bij de uiteindelijke keuze voor een toegangscontrolesysteem ook goed te kijken welke identificatiemiddelen het beste bij de organisatie passen, nu en in de toekomst. Want identificatie kan op diverse manieren en met verschillende middelen, variërend van een pincode, een toegangspas, de steeds vaker gebruikte mobiele telefoon, tot aan het gebruik van biometrische gegevens. De belangrijkste identificatiemiddelen zijn:

- **Pincode**

Een eenvoudige manier om deuren te openen is het gebruik van een pincode. Vooral zorginstellingen en winkels passen deze vorm van toegangsverlening vaak toe.

- **Toegangspas**

De meeste toegangscontrolesystemen maken gebruik van fysieke informatiedragers in de vorm van kaarten, passen, druppels en tags.

- **Barcode**

Voor bezoekersmanagement waarbij gebruikersgemak voorop staat, zijn toegangskaarten met daarop een barcode een goede keuze.

- **Contact smartcards**

Contact smartcards met daarin een chip worden vaak toegepast voor de toegang tot IT-apparaten zoals laptops.

- **Mobiele telefoon**

Een recente ontwikkeling is dat de mobiele telefoon fungeert als toegangspas. Daarbij wordt gebruikgemaakt van de volgende twee technologieën:

- **Near Field Communication (NFC)**

NFC is vergelijkbaar met RFID, maar er zijn specifieke kenmerken zoals gebruikersgemak, leesafstand en duurzaamheid die afhangen van hoe NFC is geïmplementeerd in het toegangscontrolesysteem.

Bij het gebruik van NFC zit er een uniek ID-nummer in de mobiele telefoon. Dit kan hardware matig door het in het toestel zelf of in de simkaart te monteren. Een andere mogelijkheid is het gebruik van gastkaartemulatie waarbij een softwarematige versleuteling wordt gebruikt.

- **Bluetooth Low Energy (BLE)**

BLE is een draadloos signaal voor de korte afstand, maar wel met een groter bereik dan NFC. Voordelen van deze technologie zijn het gebruikersgemak, de mogelijke combinatie met RFID-kaarttechnologie en de leesafstand van enkele meters. Bovendien is gebruik met zowel Android als iPhone mogelijk. Nadeel is dat er een grote variatie aan mobiele telefoons is waardoor compatibiliteitsproblemen kunnen ontstaan.

➢ Biometrie

De voor toegangscontrole meest gebruikte biometrische technologieën zijn:

Vingerafdruk

Bij een vingerafdruk worden de lijnen en patronen (minutia) van de vingers gemeten, gecodeerd en opgeslagen. Bij een controle van een tweede scan, wordt de uitkomst hiervan vergeleken met de opgeslagen uitkomst. Als deze overeenkomt, of voldoende overeenkomt is er een match.

Vingerader

Door de vinger van een persoon aan de achterkant te verlichten worden de vingeraders zichtbaar. Dit patroon wordt opgeslagen en later vergeleken bij verificatie.

Vingergeometrie

Bij vingergeometrie wordt de vorm van de vingers gemeten. Alle maten van geometrische kenmerken worden hierbij geregistreerd.

Handgeometrie

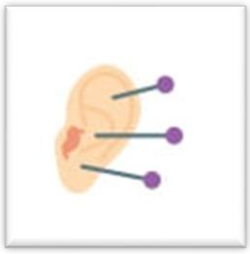
Handgeometrie vergelijkt de breedte van de hand, de lengte van de vingers en het verschil in lengte tussen de vingers gebruikt.

Gezichtsherkenning

Ruimte tussen de ogen, breedte neus, afstand van neus tot ogen. Bijna alle kenmerken die een afstand of positie kennen worden gemeten en gecontroleerd. In feite is het niet veel anders dan het registreren van een vingerafdruk, met andere herkenningspunten.

DNA

DNA de blauwdruk van het menselijk lichaam. DNA wordt gebruikt in de medische wereld en is niet geschikt als een ‘snelle test’ in toegangsomgevingen.



Oor

De vorm, maat en bochten van het oor worden geregistreerd voor herkenning.

Ogen – Iris

Het oog wordt geanalyseerd voor herkenning om te bepalen of toegang is toegestaan.

Ogen – Retina

Het netvlies (retina) is een lichtgevoelige laag achterin het oog.

10. BRONNEN

Gebruikte bronnen

1. IFSEC global, The state of physical access control in EMEA business, 2022
2. DNB, Economische vooruitzichten & ontwikkelingen, juni 2022
3. CPB, Raming PPB, september 2022
4. CBS, Statline BBP, productie en bestedingen, september 2022
5. CBS, Eurostat1e kwartaal 2020 (2e kwartaal) – 2022 (4e kwartaal) Faillissementen
6. Rabo Research, Economisch kwartaalbericht, juni 2022
7. Convergentie monitor van Ilisia Marketingservice: grootschalig, jaarlijks terugkerend onderzoek op het gebied van ICT-ontwikkelingen en trends op basis van 1.600 interviews met ICT verantwoordelijke, mei 2021
8. Rabobank, Impact corona op kantorenmarkt, juli 2021
9. Buck consultants International, Impact thuiswerken op Nederlandse kantorenmarkt, juni 2021
10. Kennisinstituut voor mobiliteit, Effecten corona op mobiliteit, juni 2022
11. Cap Gemini, Trends in Veiligheid 2021
12. Cso.com.au/artikel, 527083
13. Government.nl/nieuws/2018, NIVD disrupts Russische operatie tegen OPCW
14. IT Trendsonderzoek van Supply Value, augustus 2020
15. Security magazine, 2016
16. Sarb Sembhi & James Willison, 'The Role of a Converged Security Centre in a Smart Building', https://www.ifsecglobal.com/smart-buildings/the-role-of-a-converged-security-centre-in-a-smart-building/
17. Agenda-arbeidsveiligheid-2050/Ministerie SZW

Aanbevolen bronnen

Bronnen over de nieuwe werkorganisatie

- Het rapport Duurzame inzetbaarheid in perspectief van (TNO) laat zien hoe het werknemers op de arbeidsmarkt vergaat en welke toekomstige acties nodig zijn. Focus ligt op recente data en ontwikkelde duurzaam inzetbare interventies.
- Het rapport Kennisagenda 2019-2022 van het ministerie van SZW geeft inzicht in relevante ontwikkelingen op de arbeidsmarkt de komende jaren.
- Het boek van de Nederlandse Vereniging voor Veiligheidskunde (NVVK) Gedrag en Veiligheid (redactie Frank Guldemond) biedt veiligheidskundigen met kennis over veilig werkgedrag en een veilige werkcultuur.

Bronnen over technologische ontwikkelingen

- Het rapport Gebruik biomonitoring en sensoring binnen de arbeidsomstandigheden (TNO) geeft inzicht in praktische en ethische overwegingen over dit onderwerp.
- Het rapport Occupational safety and health in 2040 van de European Trade Institute (ETUI) kijkt naar de lange termijn vooruitzichten voor betere en strategische beslissingen over veiligheid en gezondheid op het werk (OSH) in de Europese Unie.
- Het rapport Foresight new health and safety risks with digitalisation by 2025 presenteert de eindresultaten over ontwikkelingen in digitale technologieën en de veranderingen in waar, wanneer en hoe het werk wordt gedaan.
- Het rapport De toekomst van sensing voor veiligheid plaatst sensing voor veiligheid in een maatschappelijke context.
- Het rapport Het verhaal van Digitaal (Platform voor de Informatiesamenleving) laat zien welke rol digitale ontwikkelingen invloed hebben op de werkvloer.
- Het rapport Vitaal vakmanschap (TNO) gaat in op de invloed van technologische ontwikkelingen op de voortdurend veranderende arbeidsvraag en arbeidsaanbod.
- Het rapport Opportunity's and challenges of the industrial internet (PWC Industry 4.0) beschrijft hoe industriële bedrijven de digitale transformatie kunnen vormen en welke nieuwe mogelijkheden voor groei deze bieden.

COLOFON

Deze editie van het Trendrapport Elektronisch Toegangsbeheer is tot stand gekomen door medewerking van de leden van de sectie Elektronisch Toegangsbeheer, onderdeel van de ondernemersvereniging Federatie Veilig Nederland.

OVER DE FEDERATIE VEILIG NEDERLAND

De vereniging Federatie Veilig Nederland is een professionele ondernemersvereniging met een groot aantal leden, allemaal gespecialiseerde bedrijven met oplossingen voor vele brandveiligheids- en beveiligingsvraagstukken. De vereniging behartigt de algemene, economische, commerciële en strategische belangen van haar leden. Federatie Veilig Nederland is in 1969 opgericht en staat voor kwaliteitsbedrijven, duidelijke taal, een sterke organisatie en meerwaarde voor haar leden. Deskundige ondersteuning, dienstverlening en belangenbehartiging staan hoog in het vaandel.

De leden van de Federatie zijn actief in één of beide van de onderstaande vakgebieden:

- Brandveiligheid (FireSafety); en
- Beveiliging (Security)

Binnen deze vakgebieden zijn leden actief die zich richten op specifieke disciplines met eigen specialismen en oplossingen voor (brand)veiligheidsvraagstukken.

<table>
<tr><th>BRANDVEILIGHEID</th><th>BEVEILIGING</th></tr>
<tr><td>BOUWKUNDIG
RookBeheersingsSystemen</td><td>BOUWKUNDIG
Hang- en Sluitwerk (VHS)</td></tr>
<tr><td>REPRESSIE
Blusmiddelen
Blussystemen (SB)
Sprinklertechniek (VSI)</td><td>SIGNALERING
Inbraak, Detectie & Alarmtransmissie
Elektronisch Toegangsbeheer (ETB)
Videospecialisten (CCTV/VSS)</td></tr>
<tr><td>PREVENTIE
Branddetectie, -componenten & OAS
Rook- en CO-melders
Noodverlichting</td><td>SYSTEMEN
Bouwplaats Beveiliging
Integrated Solutions (System Integrators)</td></tr>
<tr><td colspan="2">TOEZICHT
Monitoring and Alarm Receiving Centre (MARC’s)</td></tr>
</table>

De technische beveiligingsindustrie in cijfers:

Ruim 180 bedrijven, ruim 11.000 medewerkers.
Een gezamenlijke omzet van EUR 1.65 miljard (Bron: Illisia 2021).

DE SECTIE ELEKTRONISCH TOEGANGSBEHEER

De leden van de sectie leveren effectieve toepassingen voor toegangscontrole en werken aan regelgeving om de sector als geheel naar een nog hoger plan te tillen. Door verbreding van de functionaliteit van elektronisch toegangsbeheer ervaren meer en meer gebruikers/eigenaren van dergelijke systemen dat de investering zich sneller terugverdient.

De volgende bedrijven hebben meegewerkt aan de totstandkoming van dit trendrapport en zijn allen lid van de ondernemersvereniging Federatie Veilig Nederland.

Leden ETB – Federatie Veilig Nederland in 2023

BEDRIJFSNAAM	WEBADRES
ARAS Security B.V.	https://www.aras.nl
ASSA ABLOY Nederland B.V.	https://www.assaabloy.nl
Axis Communications	https://www.axis.com
Carrier F&S (Aritech)	https://www.carrier.com
CDVI	https://www.cdvibenelux.com
EAL B.V.	https://www.eal.nl
Honeywell Building Solutions	https://www.honeywell.com
Interflex Allegion BV	https://www.interflex.nl
Nedap Security Management	https://www.nedapsecurity.com
Nsecure	https://www.nsecure.nl
Paxton Benelux B.V.	https://www.paxton-access.com
Siemens Nederland N.V.	https://www.new.siemens.com
SmartSD	https://www.smartsd.com
Transquest	https://www.transquest.eu
Traka / NoRisk Keymanagement	https://www.traka.com

Federatie
Veilig Nederland

Federatie Veilig Nederland
Zilverstraat 69
2718RP Zoetermeer
info@federatieveilignederland.nl
www.federatieveilignederland.nl

Federatie Veilig Nederland
Zilverstraat 69
2718RP Zoetermeer
info@federatieveilignederland.nl
www.federatieveilignederland.nl