BIJ COMELIT ZIJN UW GEGEVENS ECHT VEILIG.

Iets wat fysiek is, is makkelijk te beschermen: je kunt het afsluiten in een kamer, vastketenen aan je bureau of een reserve-exemplaar kopen.
De beveiliging van informatie is echter **veel lastiger**: het kan op meerdere plaatsen zijn opgeslagen, in **enkele seconden** naar de andere kant van de planeet worden getransporteerd, of worden **gestolen** zonder dat je er weet van hebt.

COMELIT®
WITH • YOU • ALWAYS

CCTV & Cybersecurity

ONS BEDRIJF ALS GARANTIE VOOR DE VEILIGHEID VAN UW GEGEVENS

ZIJN UW GEGEVENS ECHT VEILIG? WAT KAN ER GEBEUREN MET DE MILJOENEN GEGEVENS DIE DOOR UW SERVERS WORDEN VERWERKT? WIE IS ER VERANTWOORDELIJK VOOR DEZE VEILIGHEID? DIT ZIJN ENKELE VRAGEN DIE U KUNT STELLEN ALS U OP ZOEK BENT NAAR EEN GOED EN BETROUWBAAR CAMERABEWAKINGSSYSTEEM.

+81 %

DE PERCENTUELE GROEI VAN SERIEUZE AANVALLEN OP HET PUBLIEKE DOMEIN (MET EEN SYSTEEMEFFECT OP ALLE GEBIEDEN VAN ONZE SAMENLEVING, VAN POLITIE TOT ECONOMIE) IN DE AFGELOPEN 4 JAAR.

Het tijdperk waarin we momenteel leven kan absoluut 'het informatietijdperk' worden genoemd. Meer dan ooit hebben we, dankzij de technologische **ontwikkelingen** de beschikking over eindeloze hoeveelheden verschillende soorten gegevens afkomstig van diverse apparaten waarmee we, zodra ze geanalyseerd en verwerkt zijn, over informatie beschikken waarmee we ons gedrag en dat van andere kunnen voorspellen.

Juist daarom zijn **cybersecurity** en de **bescherming van gevoelige gegevens** zeer actuele en belangrijke thema's en vormen ze bovendien een steeds grotere **zorg** voor zowel bedrijven als particulieren. Het is geen toeval dat sinds 2018 tot nu toe cyberaanvallen **met 81% zijn toegenomen**, waarbij niet alleen particulieren werden getroffen, maar in veel gevallen vooral complete financiële instellingen, omroeporganisatie, particuliere bedrijven, openbare instellingen en basisdiensten zoals postkantoren, luchthavens en stations.

Een groot deel van de beveiliging van publieke of particuliere infrastructuren is gebaseerd op **camerabewakingssystemen**.
Tot een aantal jaren geleden kon het hacken van hun protocollen onvoorstelbaar ernstige gevolgen hebben.

Beveiliging en bescherming tegen cyberaanvallen is daarom het '**nieuwe normaal**' geworden waar de markt om vraagt. Dat is de reden waarom alle grote spelers – ook wij – bezig zijn met het ontwikkelen en invoeren van **steeds effectievere tegenmaatregelen**, door het introduceren van firmware, shields en geavanceerde protocollen om de normen voor informatiebeveiliging te verhogen.

Maar als we het echt willen hebben over de veiligheid van de gegevens en videofeeds van iedereen, zowel van personen en burgers als consumenten, moet er eerst een belangrijke vraag worden gesteld die een helder en transparant antwoord vereist: **hoe kan een fabrikant de betrouwbaarheid en veiligheid van zijn producten garanderen?**
We weten allemaal dat er in de wereld een aantal landen zijn die verschillende fabrikanten van camerabewakingssystemen van hun markt **weren**. Een voorbeeld daarvan zijn de **Verenigde Staten** die in 2018, met de goedkeuring van de federale wet **NDAA** - ondertekend door Trump en daarna bevestigd door Biden – federale

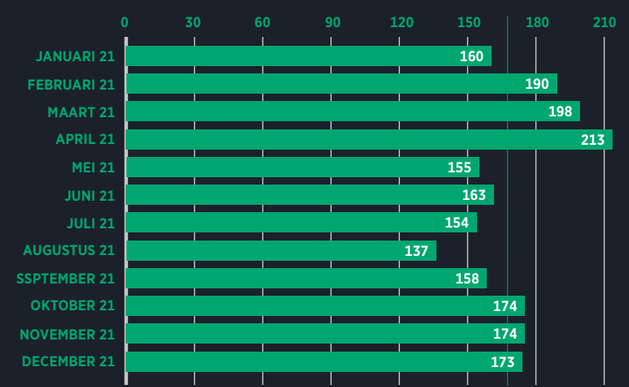
NDAA COMPLIANT

GDPR COMPLIANT

Meer weten over de NDAA

[in het Engels]
PAG 283-285

In 2021 heeft Clusit* 2.049 serieuze cyberaanvallen in het publieke domein geanalyseerd, met een maandgemiddelde van 171 aanvallen. Dit is de hoogste waarde ooit gemeten en komt overeen met een stijging van bijna 10% ten opzichte van het jaar daarvoor. De schade voor 2021 werd (op wereldschaal) geschat op 6 biljoen dollar.



*Italiaanse vereniging voor informatiebeveiliging, een non-profitorganisatie die op 4 juli 2000 in Milaan is opgericht.

agentschappen en hun aanbesteders **verbiedt** telecommunicatie- of camerabewakingsapparatuur en onderdelen hiervan te gebruiken of te kopen die zijn vervaardigd door een aantal van de grootste fabrikanten ter wereld, waaronder zeer bekende merken, ook in België..
Dit zijn kritieke kwesties **die Comelit in geen enkel opzicht raken**. In tegendeel. **We zijn Italiaans**, we zijn een particulier bedrijf, zonder enige staatsdeelneming. **We hebben geen verplichtingen jegens anderen**, anders dan onze aandeelhouders. We hebben derhalve **geen enkel belang of verplichting om de gegevens te delen** die door onze servers worden verwerkt.

En dat niet alleen. Hoewel het duidelijk is dat bijna alle camerabewakingstechnologie 'made in China' is - net als de smartphone in onze tas of de pc op ons bureau -, kunnen wij garanderen dat onze systemen uitsluitend onderdelen bevatten die **in geen enkel land op een blacklist staan.**

Wij zijn minder kwetsbaar. We zijn een Italiaans particulier bedrijf zonder staatsinmenging en zonder belang of verplichting om de gegevens aan derden te verstrekken.

De producten van Comelit maken gebruiken van een eigen protocol en onze eigen servers in Europa. Bovendien zijn ze volledig ONVIF-compliant: dat wil zeggen dat volledige compatibiliteit met producten van andere fabrikanten is gegarandeerd.

Daarnaast is de infrastructuur van onze cloud-server voor gegevensoverdracht- en opslag Europees, **onze eigendom** en wordt hij beheerd **in samenwerking met 's werelds grootste cloud provider, Amazon AWS**, die 36% van de markt in handen heeft. Onze servers bevinden zich in Frankfurt, in Duitsland, worden beveiligd door de beste informatiebeveiligingssystemen, zijn voor niemand toegankelijk, om welke reden dan ook, en er worden voortdurend back-ups gemaakt.

Garanderen dat uw gegevens en uw video's echt compleet veilig zijn, is voor Comelit **een bron van trots en een ethisch engagement**. Een garantie die geen optionele eis zou moeten zijn, maar een onschendbaar basisrecht voor iedereen.

MIRKO BONADEI
Chief Architect Officer van de Comelit Group S.p.A.

Een gevaar waarop Comelit goed is voorbereid.

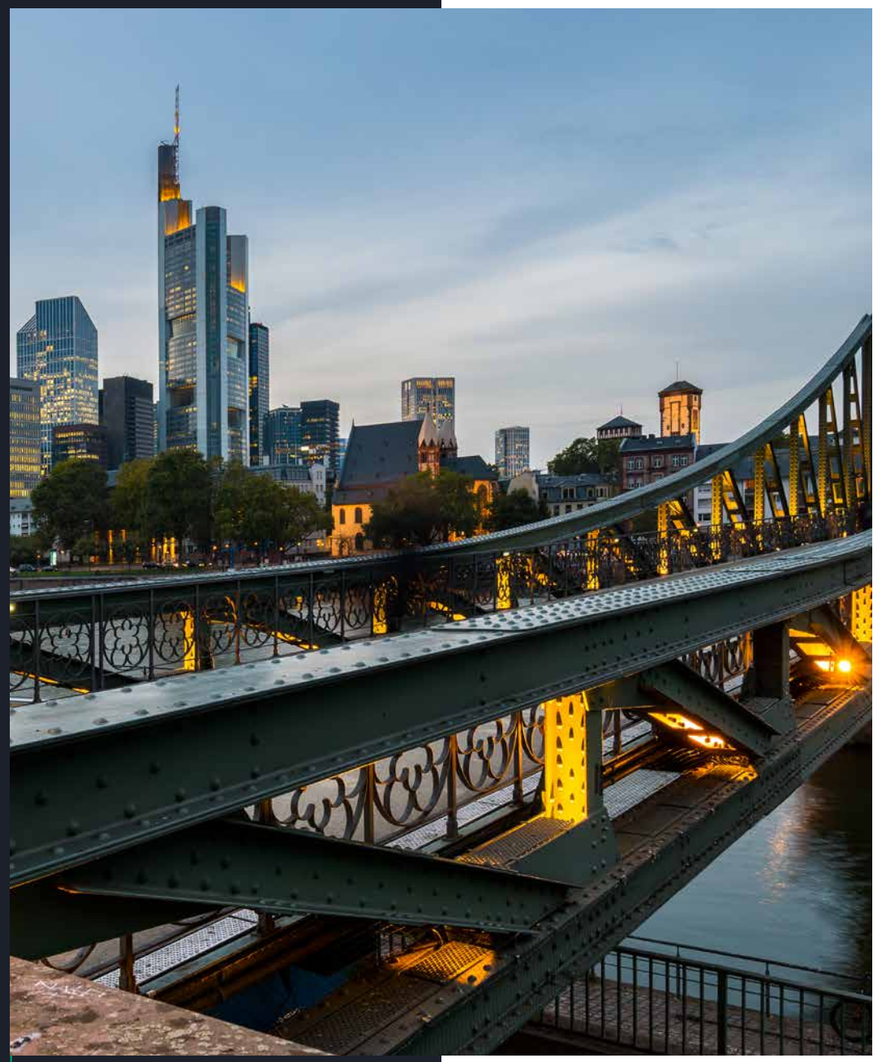
Bij Comelit is cybersecurity een **topprioriteit** en we doen onze **uiterste best** om onze systemen veiliger te maken door middel van steeds strengere protocollen. Hiervoor hebben we **geïnvesteerd in middelen en talent** en hebben we een reeks acties opgezet om de best mogelijke oplossing te implementeren: Ten eerste **controleren we de bewerkingen door derden** – de productleveranciers - door met hogere standaarden te werken dan die gewoonlijk worden gehanteerd. Vervolgens hebben we een **nieuw platform** Cloud Comelit gecreëerd dat zich in Europa bevindt, in Frankfurt, met zeer strenge beveiligingsprotocollen en hebben we back-up en disaster recovery-systemen geïmplementeerd en deze multiregionaal gemaakt, omdat de **redundantie** van de systemen ervoor zorgt dat de gegevens beschikbaar blijven, ook bij onverwachte gebeurtenissen. Verder hebben we een **monitoring van de activiteiten** van het platform gerealiseerd door middel van **AI**-systemen die de toegang tot en de activiteiten van de accounts op het platform controleren en die niet alleen indringers kunnen detecteren, d.w.z. pogingen tot ongeautoriseerde toegang, maar ook **gedrag** dat niet in overeenstemming is met de autorisaties van individuele accounts, waardoor iemand een **geautoriseerd** account zou kunnen gebruiken om handelingen uit te voeren die dat type account normaal gesproken niet uitvoert, d.w.z. handelingen die buiten het patroon vallen, waarbij de gebeurtenis wordt gedetecteerd en gesignaleerd.
Niet alleen de operators/accounts worden voortdurend gecontroleerd, maar ook de infrastructuur zelf wordt regelmatig getest via een **vulnerability test** om te controleren of het **beveiligingsniveau** nog steeds afdoende is voor nieuwe mogelijke bedreigingen. De **drie principes van informatiebeveiliging** zijn **betrouwbaarheid**, in de zin dat de gegevens alleen toegankelijk zijn voor wie hiertoe daadwerkelijk bevoegd is, **integriteit** wat betekent dat de gegevens worden bewaard zonder dat ze gemanipuleerd worden, en tevens **beschikbaarheid**,wat betekent dat de gegevens zo snel mogelijk toegankelijk en beschikbaar dienen te zijn.
Indien de infrastructuur van Comelit om een bepaalde reden zou "omvallen" of beschadigd zou raken, dan wordt deze **automatisch** voor 99% gereconstrueerd, zodat interventie en menselijke fouten tot een minimum blijven beperkt.

Onze Cloud CCTV-dienst: nu veiliger dan ooit.

Het vertrouwen van de klant staat centraal bij Comelit en we weten dat u ons vertrouwt om uw **meest kritische en gevoelige activa te beschermen: uw gegevens.** Onze camera's en videorecorders gebruiken speciale firmware om maximale bescherming te garanderen, zowel wat betreft cyberveiligheid als gegevensbescherming. Comelit-producten maken gebruik van gecodeerdecommunicatieprotocollen, vergrendeling van telnet-poorten, gecodeerde configuratiebestanden, versleuteling van opslaggegevens en back-ups. Maar is dit alles voldoende om computerveiligheid en gegevensbescherming te garanderen? **Wij zijn nog een stap verder gegaan!**

We hebben de beveiliging van de gegevens van onze klanten nog verder verhoogd door gebruik te maken van de infrastructuur en clouddiensten van **Amazon Web Services** (AWS), het meest uitgebreide en veilige cloudplatform dat momenteel beschikbaar is. Met behulp **van de AWS-clouddiensten** bieden de videobewakingsdiensten van Comelit u de hoogste normen voor veerkracht, cyberveiligheid en bescherming van gevoelige en persoonlijke gegevens in overeenstemming met de Europese privacyregelgeving. De infrastructuur, gebaseerd op het gebruik van zeer betrouwbare en schaalbare serverloze technologieën, wordt systematisch onderworpen aan:

- **Kwetsbaarheidsbeoordeling voor het opsporen van veiligheidslekken in software, de afhankelijkheden ervan en netwerkconfiguraties**
- **Monitoring met tools voor kunstmatige intelligentie die algoritmen voor patroonherkenning gebruiken om frauduleus gedrag en aanvallen op te sporen**
- **Bewaking met tools die Machine Learning en pattern matching gebruiken om gevoelige gegevens te identificeren en privacy en beveiliging te beschermen door best practices op het gebied van beveiliging af te dwingen**
- **Intelligente dreigingsdetectie met bescherming tegen DDoS-aanvallen op de transportlaag (lvl 4 ISO OSI)**



DE GEGEVENS WORDEN OPGESLAGEN IN EUROPA EN VOLDOEN AAN DE EU-VOORSCHRIFTEN INZAKE PRIVACY, OVERDRAAGBAARHEID EN DIGITALE SOEVEREINITEIT.

Amazon Web Services

Al **meer dan 15 jaar** is AWS het meest uitgebreide en breed toegepaste cloudplatform ter wereld. AWS heeft zijn diensten gestaag uitgebreid om vrijwel elke workload in de cloud te ondersteunen en heeft nu meer dan **200 uitgebreide diensten** voor compute, storage, databases, netwerken, analytics, robotica, machine learning en artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual en augmented reality (VR en AR), media en applicatieontwikkeling. Miljoenen klanten - waaronder de snelst groeiende start-ups, de grootste ondernemingen en grote overheidsinstellingen - vertrouwen op AWS om hun infrastructuur te verbeteren, wendbaarder te worden en aan de hoogste veiligheidseisen te voldoen..

Redundantie: Alle gegevensbronnen zijn redundant om een hoge betrouwbaarheid en lage failover-tijden te garanderen.

Encryptie: Alle gegevensbronnen worden gecodeerd met symmetrische coderingssleutels die worden beheerd op FIPS 140-2-conforme hardwarebeveiligingsmodules.

Slot: De gegevensbronnen zijn niet openbaar toegankelijk om een extra beveiligingslaag te bieden.

Back-up: Back-ups van alle gegevensbronnen en schijven worden voortdurend gegenereerd, opgeslagen op gecodeerde omgevingen en verspreid over verschillende en verafgelegen geografische locaties.

Amazon Inspector: Dankzij de Amazon Inspector dienst is er automatisch en continu beheer van de beoordeling van kwetsbaarheden voor het opsporen van beveiligingslekken in software, de afhankelijkheden ervan en netwerkconfiguraties.

Amazon GuardDuty: dienst voor bedreigingsdetectie die voortdurend AWS-accounts en workloads controleert op kwaadaardige activiteiten en gedetailleerde beveiligingsresultaten retourneert voor zicht op herstel.

Amazon Macie: Monitoring met tools die ML en pattern matching gebruiken om gevoelige gegevens te identificeren en privacy en beveiliging te beschermen door best practices af te dwingen.

Amazon Cloudwatch: Monitoringdienst die gedetailleerde gegevens en informatie levert die nuttig zijn voor het bewaken van toepassingen, het reageren op prestatieveranderingen in het hele systeem en het optimaliseren van het gebruik van resources.

Amazon Shield: Infrastructuur beschermd door een Intelligent Threat Detection tool met bescherming tegen DDoS-aanvallen tot niveau 4 van het ISO OSI-model.

15

FOR OVER 15 YEARS, AMAZON WEB SERVICES (AWS) HAS BEEN THE MOST COMPREHENSIVE AND WIDELY ADOPTED CLOUD PLATFORM IN THE WORLD.

Ons aanbod

TWEE SERIES, ÉÉN OPLOSSING.

Het huidige aanbod van Comelit bestaat uit twee **productseries**: de serie NEXT en de serie ADVANCE.

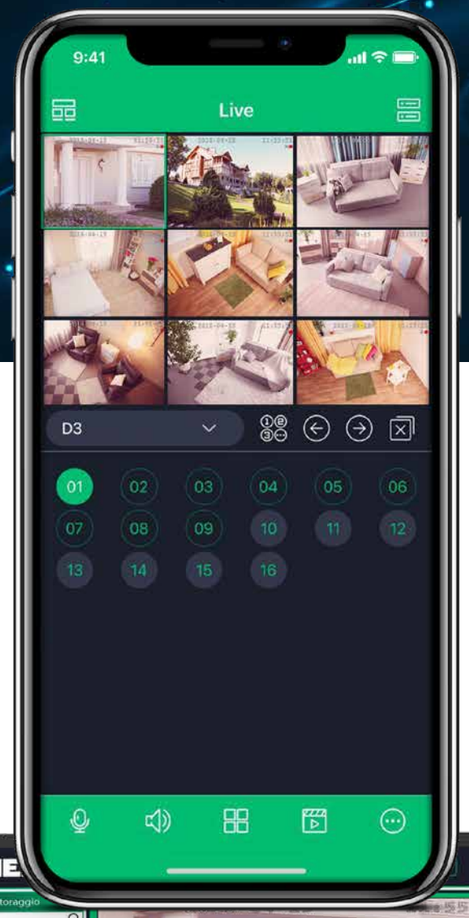
De serie Next bestaat uit technologisch geavanceerde producten: camera's met diverse behuizingen, lenzen en sensoren met resoluties tot 4K, opname-apparatuur tot 32 ch, kortom ideaal voor kleine en middelgrote installaties.

De serie Advance biedt daarentegen het beste op het gebied van Deep video analysis (DVA), video-analysefuncties die onderscheid kunnen maken tussen mensen, voertuigen, fietsen, motoren, target telfuncties, heatmap, van gezichtsherkenning tot de analyse van metagegevens (DVA 2.0), videorecorders tot 128 ch en platformproducten met opslagservers en beheerservers voor het realiseren van installaties tot max. 30.000 ch. Ideaal voor middelgrote en grote installaties en om aan elke eis te kunnen voldoen.

DE SERIE NEXT EN DE SERIE ADVANCE WORDEN BEHEERD VIA EEN ENKEL PLATFORM, EEN ENKELE APP EN SLECHTS ÉÉN VMS. HIERDOOR IS ELKE COMBINATIE TUSSEN DE SERIES MOGELIJK, ZODAT HET CAMERABEWAKINGSSYSTEEM NOG MEER OP MAAT IS GEMAAKT, EN AAN ELKE TECHNOLOGISCHE EN ECONOMISCHE EIS KAN VOLDOEN.

Dankzij de video-analysefuncties kan het camerabewakingssyteem **veel meer** dan alleen video's opnemen en afspelen.

Het is mogelijk eigendommen te **beschermen** tegen diefstal, gebeurtenissen kunnen sneller worden gevonden en er wordt direct een pushmelding of e-mail ontvangen. Naast de meest gebruikelijke video-analysefuncties, zoals perimeterbeveiliging, zijn ook marketinganalyses mogelijk dankzij de verschillende functies voor het herkennen van geslacht, leeftijd, voertuigidentificatie en rijrichting.



COMELIT

- RETAIL
- SCHOOLGEBOUWEN
- TRANSPORT
- OPENBARE RUIMTES
- HOTELS
- BEDRIJVEN
- WONINGEN
- BANKEN

Comelit.

ALWAYS.

Sinds 1956 schrijven we geschiedenis op het gebied van video-deurintercomsystemen en dragen we in belangrijke mate bij aan de **continue** ontwikkeling ervan. De ervaring die we in deze specifieke sector hebben opgedaan om te kunnen inspelen op de **vraag** naar eenvoud, betrouwbaarheid en multifunctionaliteit in de installatiewereld, heeft in de loop der jaren gezorgd voor een flinke groei, waardoor we op **internationaal niveau toonaangevend** zijn geworden.

Onze **waarden** en onze **ondernemersvisie** vormen het fundament waarop we ons management en onze internationale organisatie hebben opgebouwd, met **9 vestigingen** in het buitenland, meer dan **800 werknemers** en een commerciële aanwezigheid in **meer dan 90 landen**.

Naast video-deurintercomsystemen ontwerpen, realiseren we ook systemen voor inbraakbeveiliging, camerabewaking, huisautomatisering, branddetectie en toegangscontrole en presenteren we ons als één unieke deskundige partner voor de beveiliging van personen en ruimtes.

With You. Always.

ONZE BELOFTE, ONS STREVEN.

Altijd dichtbij, betekent voor ons bij **Comelit** dat we naar de behoeften van onze klanten luisteren, mee zoeken naar oplossingen, de zekerheid bieden van een constante service, altijd de kwaliteit van onze producten en systemen garanderen en een breed assortiment aanbieden met een ruime beschikbaarheid. Omdat het succes en de tevredenheid van elke **professionele installateur** die voor Comelit kiest, het doel is van onze dagelijkse inspanningen. **With You. Always.**

MyComelit.

U KUNT NIET MEER ZONDER.

Eenvoudig, **direct** en **op maat**. MyComelit maakt dankzij alle beschikbare diensten het werk van alle **professionals een stuk eenvoudiger**: installateurs, ontwerpers, systeemintegratoren, veiligheidsmanagers, gebouwbeheerders, groothandels en architecten.

my COMELIT

Download on the App Store

GET IT ON Google Play

- Raadpleeg in een oogwenk alle technische en commerciële informatie en toepassingen van onze producten (catalogi, handleidingen, technische informatiebladen, enz.).
- Blijf op de hoogte van de nieuwste ontwikkelingen op uw vakgebied: acties, trainingen online en op locatie, services, nieuwe producten en nog veel meer.
- Configureer uw video-deurintercom-systemen in slechts een paar stappen en bewaar ze op uw persoonlijke pagina.
- Vraag direct een offerte aan via de configurator en raadpleeg al uw offertes in het speciale gedeelte.
- Vraag technische en commerciële ondersteuning aan voor het ontwerp van een installatie.
- Beheer en controleer uw verbonden systemen en ontvang meldingen over de status van de geïnstalleerde producten om bij storingen snel te kunnen ingrijpen.
- Configureer de namen van het Ultra deurstation (in de versies Touch of met digitaal namenregister) via bluetooth-verbinding.

code
2G32001253

COMELIT

Kleinewinkellaan 24
1853 Grimbergen
BELGIUM NV/SA
www.comelitgroup.com