

powered by  AWS

AVEC COMELIT, VOS DONNÉES SONT VRAIMENT PROTÉGÉES.

Un objet physique est facile à protéger : il suffit de l'enfermer dans une pièce, de l'attacher au bureau ou d'en acheter un de rechange.

Les informations représentent un **problème majeur** : elles peuvent exister dans plusieurs lieux, être transportées en **quelques secondes** de l'autre côté de la planète ou **volées** à votre insu.


WITH • YOU • ALWAYS

Vidéoprotection & Cybersécurité

NOTRE ENGAGEMENT AU SERVICE DE LA GARANTIE DE VOS DONNÉES

VOS DONNÉES SONT-ELLES VRAIMENT PROTÉGÉES ? QUE PEUT-IL ARRIVER AUX MILLIONS DE DONNÉES QUI PASSENT PAR LES SERVEURS ? QUI EST RESPONSABLE DE CETTE SÉCURITÉ ? TELLES SONT LES VRAIES QUESTIONS À SE POSER AVANT DE CHOISIR UN SYSTÈME DE VIDÉOPROTECTION.

L'époque dans laquelle nous vivons peut certainement être appelée « l'ère des données ». Grâce au **développement** de la technologie, nous pouvons désormais disposer de volumes presque infinis de données de diverse nature et provenant de multiples dispositifs qui, une fois analysés et traités, nous permettent d'obtenir des informations permettant de prévoir notre propre comportement et celui des autres.

télévision, des entreprises privées, des institutions publiques et des services primaires tels que les bureaux de poste, les aéroports et les gares

La sécurité de nos infrastructures, qu'elles soient publiques ou privées, repose en grande partie sur les **systèmes de vidéoprotection**.



Il y a quelques années encore, une violation de leurs protocoles aurait pu avoir des conséquences d'une gravité inimaginable.

La sécurité et la protection contre les cyberattaques sont donc devenues la « **nouvelle normalité** » qui est demandée par le marché. C'est pourquoi tous les grands acteurs, dont nous faisons partie, s'efforcent de développer et d'adopter des **contre-mesures toujours plus efficaces**, en introduisant des firmwares, des boucliers et des protocoles évolués, dans le but de peaufiner les normes de sécurité informatique.

Mais, si nous voulons vraiment parler de sécurité des données et des flux vidéo de chacun d'entre nous, en tant qu'individus et citoyens ou consommateurs, il y a une question en amont qui exige une réponse claire et transparente : **quelle garantie un fabricant est en mesure de fournir en matière de fiabilité et de sécurité?**

Nous savons tous que plusieurs pays dans le monde entier ont **banni** de leurs marchés plusieurs fabricants de systèmes de vidéoprotection. L'un d'entre eux sont les **États-Unis** qui, avec l'approbation de la loi fédérale

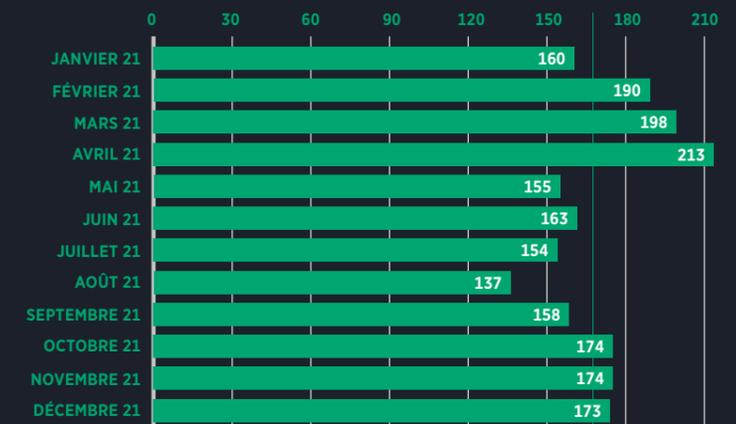


En savoir plus sur la NDA A



[En anglais]
PAG 283-285

En 2021, le Clusit* a analysé **2.049** des cyberattaques graves du domaine public, pour une moyenne mensuelle de **171** attaques. Il s'agit de la valeur la plus élevée jamais enregistrée, qui correspond à une augmentation proche de **10 %** par rapport à l'année précédente. Les dommages en 2021 ont été estimés (à l'échelle mondiale) à **6 000** milliards de dollars.



*Association italienne pour la sécurité informatique, une organisation sans but lucratif créée à Milan le 4 juillet 2000.

+81 %

C'EST L'AUGMENTATION DU POURCENTAGE D'ATTAQUES GRAVES DE DOMAINE PUBLIC (AYANT UN IMPACT SYSTÉMIQUE SUR TOUS LES ASPECTS DE LA SOCIÉTÉ, DE LA POLITIQUE À L'ÉCONOMIE) AU COURS DES 4 DERNIÈRES ANNÉES

C'est précisément pour cette raison que la **cyber sécurité** et la **protection des données sensibles** sont des sujets d'actualité et d'importance capitale, et qu'elles constituent un motif de **préoccupation** croissant, tant pour les entreprises que pour les particuliers. Ce n'est pas une coïncidence si, de 2018 à ce jour, les cyberattaques dans le monde entier ont **progressé de 81 %**, au détriment des particuliers mais, surtout, en parvenant à paralyser, dans de nombreux cas, des institutions financières entières, des chaînes de



NDAA , en 2018 - signée par Trump et confirmée par la suite par Biden - interdit aux agences fédérales et à leurs sous-traitants d'utiliser et d'acheter des équipements et des composants de télécommunication et de vidéoprotection fabriqués par certains des plus grands producteurs du monde, y compris des marques bien connues en Belgique.

Tout ceci est une criticité qui ne concerne en aucun cas Comelit. Bien au contraire. Nous sommes italiens, nous sommes une entreprise privée sans participation de l'État. Nous n'avons pas d'obligations envers qui que ce soit, si ce n'est envers nos actionnaires. Et nous n'avons, par conséquent, aucun intérêt ni aucune obligation de partager les données qui transitent par nos serveurs.

Pas seulement. Même s'il est évident que la quasi-totalité de la technologie de vidéoprotection est « made in China » - tout comme le smartphone

Nous ne faisons pas partie de la vulnérabilité. Nous sommes une société italienne, sans participation de l'État et sans intérêt ni obligation de transmettre les données que nous collectons.



Les produits Comelit utilisent un protocole propriétaire et nos propres serveurs sont situés en Europe. En outre, ils sont entièrement conformes à la norme ONVIF, c'est-à-dire qu'ils garantissent une compatibilité totale avec les produits d'autres fabricants.

dans notre poche ou le PC sur notre bureau -, nous pouvons garantir que nos systèmes intègrent des composants qui ne figurent dans aucune liste noire d'aucun pays.

En outre, notre infrastructure server-cloud pour le transfert et le stockage des données est européenne, nous appartient et est gérée en partenariat avec le plus important cloud provider du monde, Amazon AWS, qui détient 36 % du marché. Nos serveurs sont basés à Francfort, en Allemagne, sont protégés par les meilleurs systèmes de sécurité informatique et, en plus de n'être accessibles par personne pour quelque raison que ce soit, sont constamment sauvegardés.

Pouvoir garantir que vos données et vos vidéos sont effectivement totalement sécurisés est une source de fierté pour Comelit ainsi qu'un engagement éthique. Une garantie qui ne devrait pas être une exigence optionnelle, mais un droit inviolable pour tous.



MIRKO BONA DEI
Architecte en chef de Comelit Group S.p.A.

Un danger par rapport auquel Comelit n'est pas prise au dépourvu.

Chez Comelit, la cyber-sécurité est une **priorité**, nous déployons **tous nos efforts** pour rendre nos systèmes de plus en plus sûrs grâce à des protocoles toujours plus rigoureux. Pour ce faire, nous avons **investi des ressources et des talents** et mis en place une série d'actions pour mettre en œuvre la meilleure solution possible : En premier lieu, nous avons **limité les opérations effectuées par des tiers** - les fournisseurs de produits - en exigeant des normes plus pointues que celles normalement utilisées. Par la suite, nous avons créé une **nouvelle plateforme Cloud Comelit** située en Europe, à Francfort, avec des protocoles de sécurité très élevés et après avoir mis en place des systèmes de sauvegarde et de reprise après sinistre en les rendant multi-régionaux, parce que la **redondance** des systèmes permet de maintenir la disponibilité des données même en cas d'événements imprévus. Nous avons activé la **surveillance des activités** de la plateforme grâce à des systèmes d'**intelligence artificielle** qui contrôlent l'accès et l'activité des

comptes sur la plateforme et sont capables de détecter non seulement les intrusions, à savoir les tentatives d'accès non autorisés, mais aussi les **comportements** qui ne sont pas alignés sur les autorisations des comptes individuels, de sorte que si quelqu'un devait utiliser un compte **autorisé** pour effectuer des opérations que ce type de compte ne fait normalement pas, à savoir des opérations hors modèle, l'événement serait détecté et signalé. Non seulement les opérateurs/comptes sont constamment surveillés, mais l'infrastructure elle-même est régulièrement soumise à un **vulnerability test** pour vérifier si le **niveau de sécurité** est adapté aux

nouvelles menaces possibles. Les **trois principes de la sécurité informatique** sont la **confidentialité**, en ce sens que l'accès aux données doit être permis aux personnes réellement autorisées, l'**intégrité**, ce qui signifie que les données doivent être conservées sans être manipulées, mais aussi la **disponibilité**, les données devant être accessibles et disponibles le plus rapidement possible.

Si, pour quelque raison que ce soit, l'infrastructure Comelit devait « tomber », être endommagée, elle peut être reconstruite de **manière automatique** à 99 %, ce qui réduit au minimum les interventions humaines et les erreurs.





Notre site service Cloud CCTV: désormais plus sûr que jamais.

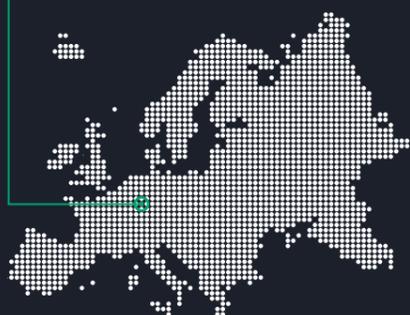
La confiance des clients est au cœur de l'activité de Comelit et nous savons que vous nous faites confiance pour protéger vos actifs **les plus critiques et les plus sensibles : vos données**. Nos caméras et enregistreurs vidéo utilisent un micrologiciel spécial pour garantir une protection maximale en termes de cybersécurité et de protection des données. Les produits Comelit utilisent des protocoles de communication cryptés, le verrouillage des ports telnet, des fichiers de configuration cryptés, le cryptage des données de stockage et des sauvegardes. Mais tout cela est-il suffisant pour garantir la sécurité informatique et la protection des données ? **Nous avons fait un pas**

de plus ! Nous avons encore renforcé la sécurité des données de nos clients en utilisant l'infrastructure et les services cloud **d'Amazon Web Services (AWS)**, la plateforme cloud la plus complète et la plus sûre actuellement disponible. En utilisant **les services cloud d'AWS**, les services de vidéosurveillance de Comelit vous offrent les normes les plus élevées en matière de résilience, de cybersécurité et de protection des données sensibles et personnelles, conformément à la réglementation européenne sur la vie privée. L'infrastructure, basée sur l'utilisation de technologies serverless hautement fiables et évolutives, est systématiquement soumise à :

- **évaluation des vulnérabilités pour détecter les failles de sécurité dans les logiciels, leurs dépendances et les configurations de réseau**
- **Surveillance à l'aide d'outils d'intelligence artificielle qui utilisent des algorithmes de reconnaissance des patrons pour détecter les comportements frauduleux et les attaques.**
- **Surveillance à l'aide d'outils qui utilisent l'apprentissage automatique et la comparaison de modèles pour identifier les données sensibles et protéger la vie privée et la sécurité en appliquant les meilleures pratiques en matière de sécurité.**
- **Détection intelligente des menaces avec protection contre les attaques DDoS au niveau de la couche transport (niveau 4 de l'ISO OSI).**



LES DONNÉES SONT STOCKÉES EN EUROPE ET SONT CONFORMES À LA RÉGLEMENTATION EUROPÉENNE EN MATIÈRE DE CONFIDENTIALITÉ, DE PORTABILITÉ ET DE NUMÉRISATION. SOVEREIGNTY.



Amazon Web Services

Depuis **plus de 15 ans**, AWS est la plateforme cloud la plus complète et la plus largement adoptée au monde. AWS n'a cessé d'étendre ses services pour prendre en charge pratiquement toutes les charges de travail dans le cloud et propose désormais plus de **200 services complets** pour le calcul, le stockage, les bases de données, la mise en réseau, l'analytique, la robotique, l'apprentissage automatique et l'intelligence artificielle (IA), l'Internet des objets (IoT), le mobile, la sécurité, l'hybride, la réalité virtuelle et augmentée (VR et AR), les médias, ainsi que le développement. Des millions de clients - dont les start-ups à la croissance la plus rapide, les plus grandes entreprises et les principales agences gouvernementales - comptent sur AWS pour améliorer leur infrastructure, devenir plus agiles et répondre aux exigences de sécurité les plus élevées.



Redondance : Toutes les sources de données sont redondantes pour garantir une grande fiabilité et des temps de basculement réduits.



Cryptage : Toutes les sources de données sont cryptées avec des clés de cryptage symétriques gérées sur des modules de sécurité matériels conformes à la norme FIPS 140-2.



Verrouillage : Les sources de données ne sont pas accessibles au public afin de fournir une couche supplémentaire de sécurité.



Sauvegarde : Des sauvegardes de toutes les sources de données et des disques sont constamment générées, stockées dans des environnements cryptés et réparties sur des sites géographiques différents et éloignés.



Amazon Inspector : Grâce au service Amazon Inspector, il existe une gestion automatique et continue de l'évaluation des vulnérabilités pour la détection des failles de sécurité dans les logiciels, leurs dépendances et les configurations réseau.



Amazon GuardDuty : service de détection des menaces qui surveille en permanence les comptes AWS et les charges de travail à la recherche d'activités malveillantes, et renvoie des résultats de sécurité détaillés pour une visibilité des mesures correctives.



Amazon Macie : Surveillance à l'aide d'outils utilisant le ML et le pattern matching pour identifier les données sensibles et protéger la vie privée et la sécurité en appliquant les meilleures pratiques.



Amazon Cloudwatch : Service de surveillance qui fournit des données et des informations détaillées utiles pour surveiller les applications, réagir aux changements de performance à l'échelle du système et optimiser l'utilisation des ressources.



Amazon Shield : Infrastructure protégée par un outil de détection intelligente des menaces avec une protection contre les attaques DDoS jusqu'au niveau 4 du modèle ISO OSI.

15

DEPUIS PLUS DE 15 ANS, AMAZON WEB SERVICES (AWS) EST LA PLATEFORME DE CLOUD COMPUTING LA PLUS COMPLÈTE ET LA PLUS LARGEMENT ADOPTÉE AU MONDE.

Notre offre

DEUX GAMMES, UNE SEULE SOLUTION.

L'offre actuelle de Comelit se compose de deux **gammes de produits** : la série NEXT et la série ADVANCE.

La série Next se compose de produits à la pointe de la technologie : caméras avec différents boîtiers, optiques et capteurs avec des résolutions allant jusqu'à 4K, enregistreurs jusqu'à 32 ch, l'idéal pour les petites et moyennes installations.

La série Advance offre les plus hauts niveaux en termes d'analyse vidéo approfondie (DVA), de

fonctions d'analyse vidéo en mesure de distinguer un homme, un véhicule, un vélo et une moto, de fonctions de comptage de cibles, de cartes thermiques, de la reconnaissance des visages à l'analyse des métadonnées (DVA 2.0), d'enregistreurs vidéo jusqu'à 128 ch et de produits de plateforme avec des serveurs de stockage et de gestion pouvant atteindre 30 000 ch. Idéal pour les moyennes et grandes installations et pour répondre à tous types de demande.

LA SÉRIE NEXT ET LA SÉRIE ADVANCE SONT GÉRÉES PAR UNE SEULE PLATEFORME, UNE SEULE APPLICATION ET UN UNIQUE VMS. CELA PERMET DE CONJUGUER LES SÉRIES POUR RENDRE LE SYSTÈME DE VIDÉOPROTECTION TOUJOURS PLUS PERSONNALISÉ, RÉPONDANT À TOUS LES BESOINS, TANT TECHNOLOGIQUES QU'ÉCONOMIQUES.

Les fonctions de vidéo analyse permettent à l'installation de vidéoprotection d'aller **au-delà des limites** de la simple visualisation et de l'enregistrement vidéo.

Elles permettent de **protéger** la propriété contre les intrusions, de rechercher plus rapidement des événements, de recevoir immédiatement des notifications push et e-mail. Outre les fonctions d'analyse vidéo les plus courantes telles que la protection du périmètre, il est également possible de faire de l'analyse marketing, grâce aux différentes fonctions de reconnaissance du sexe, de l'âge, d'identification du véhicule et du sens de marche.



Comelit.

DEPUIS TOUJOURS.

Depuis 1956, nous écrivons l'histoire des systèmes d'interphonie et de vidéophonie et nous avons largement contribué à leur évolution **constante**. L'expérience acquise dans ce secteur spécifique pour répondre aux **nécessités** de simplicité, fiabilité et multifonctionnalité du monde de l'installation nous a permis d'évoluer au fil des ans et de devenir une **référence internationale** reconnue.



Nos **valeurs** et notre **vision** d'entreprise sont les fondements sur lesquels nous avons développé une gestion et une organisation structurée à l'échelle mondiale, avec **10 filiales** étrangères, plus de **830 collaborateurs** et une présence commerciale dans **plus de 90 pays**.

Parallèlement aux systèmes de vidéophonie, nous concevons et construisons aujourd'hui des systèmes d'alarme anti-intrusion, de vidéoprotection, de domotique, de détection d'incendie et de contrôle d'accès, ce qui fait de nous un partenaire unique et compétent pour la protection des personnes et des biens.

With You. Always.

NOTRE PROMESSE, NOTRE ENGAGEMENT.

Être **aux côtés** des personnes qui choisissent Comelit pour leurs clients est notre **engagement** quotidien. Cet engagement se traduit par la recherche et le développement constants de nouvelles solutions faciles à installer et aux prestations évoluées, par le conseil et **l'assistance** quotidienne, par téléphone et sur le terrain, par la proposition de produits et de systèmes fiables et de haute qualité, par **l'accompagnement à chaque étape de votre travail**. With You. Always. Parce que **votre succès est aussi notre succès** tout comme la satisfaction de vos clients est notre satisfaction.



MyComelit.

L'APPLI DONT VOUS NE POURREZ PLUS VOUS PASSER.



Simple, immédiate et personnalisée. MyComelit simplifie le travail de tous les **professionnels du secteur** grâce à tous les services qu'elle met à leur disposition : installateurs, concepteurs, intégrateurs de système, responsables de la sécurité, syndics de copropriété et architectes.



- Consultez rapidement toutes les informations techniques, commerciales et d'application (catalogues, manuels, fiches techniques, etc.).
- Restez au courant de toutes les nouvelles qui vous sont destinées : promotions, cours de formation en ligne et sur site, services, nouveaux produits et bien plus encore.
- Configurez vos systèmes de portier vidéo en quelques étapes seulement et enregistrez-les dans votre espace privé.
- Demandez une offre directement dans le configurateur et consultez toutes vos offres dans la section dédiée.
- Demandez de l'assistance technique et commerciale pour la conception d'un système.
- Gérez et surveillez vos systèmes connectés et recevez des notifications sur l'état des produits installés pour intervenir rapidement en cas d'anomalies.
- Configurez les noms de la platine Ultra (en version Touch ou Répertoire numérique) via la connexion Bluetooth.



Download on the
App Store

GET IT ON
Google Play



COMELIT

Kleinewinkellaan 24
1853 Grimbergen
BELGIUM
www.comelitgroup.com



Les marques et dénominations commerciales figurant dans cette publication appartiennent à leurs propriétaires respectifs.
Les dimensions des produits illustrés sont fournies à titre indicatif.



code
2G32001246