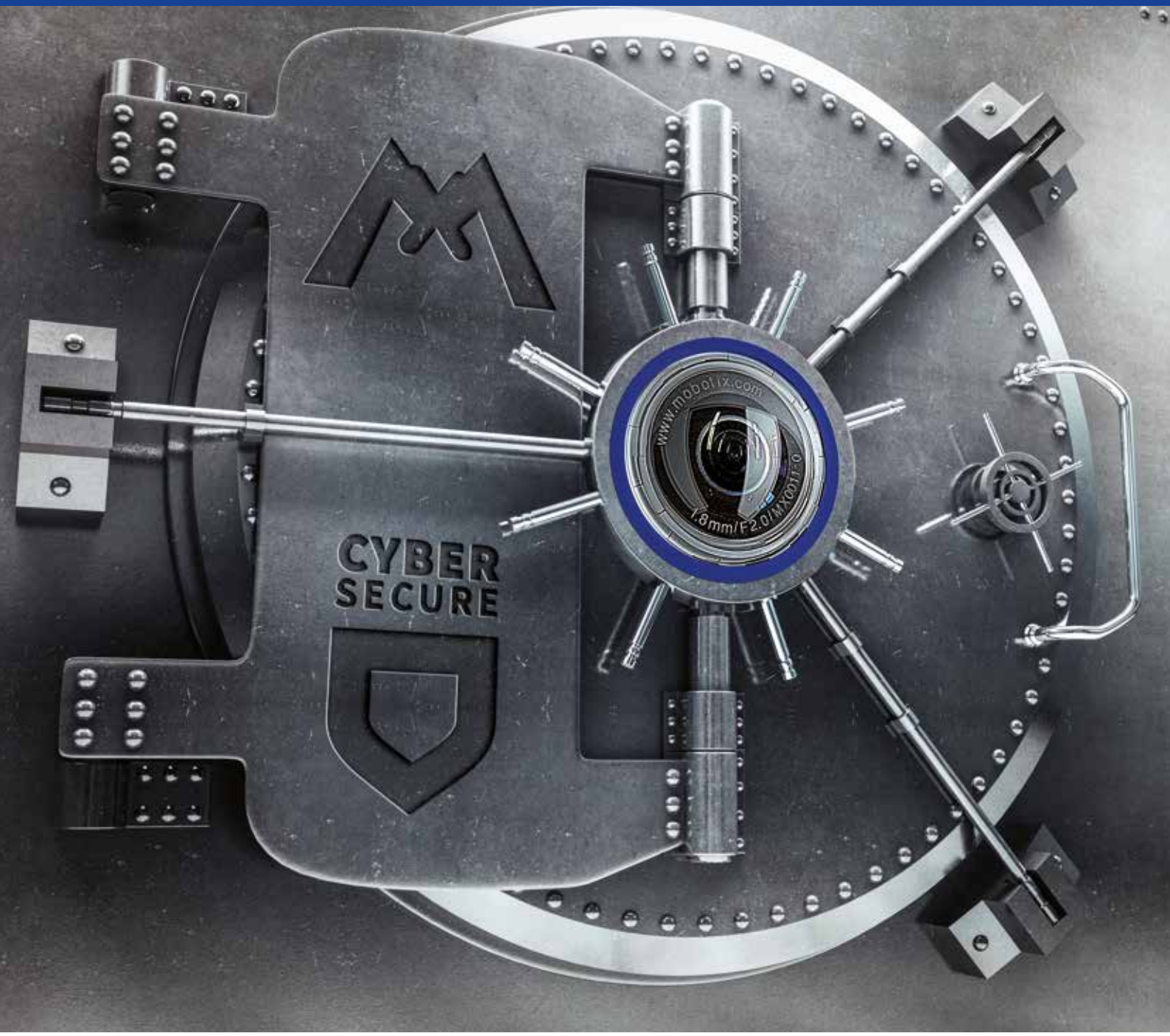
L’importance de la cybersécurité dans les systèmes de vidéosurveillance

Livre blanc



BeyondHumanVision

MOBOTIX

Introduction

L'utilisation de la vidéo dans les domaines de la prévention, du contrôle industriel, de la santé et de la sécurité a une incidence positive sur la vie de milliards d'individus chaque jour. D'une famille flânant dans un centre commercial sous l'œil vigilant d'un système CCTV aux responsables utilisant la vidéo à distance pour détecter les défauts sur une ligne de production, en passant par les parents inquiets surveillant le sommeil de leur bébé, la vidéosurveillance est présente dans chaque aspect de notre vie.

Principaux facteurs de croissance		
1	Incidence des problèmes de sécurité	58 %
2	Pertinence des analyses vidéo	51 %
3	Accessibilité des réseaux IP	50 %

Le développement des secteurs de l'information, de la communication et des technologies a accéléré le recours à la vidéo pour la surveillance et autres applications. Si autrefois une image de vidéosurveillance exigeait la présence d'un opérateur pour évaluer une situation et prendre une décision, l'imagerie vidéo est aujourd'hui de plus en plus associée à d'autres types de données sensorielles comme la température, le son, le mouvement et des systèmes d'intelligence artificielle capables de déclencher automatiquement les alarmes et procédures. De simple outil de réception passif, la vidéo est devenue un dispositif automatisé et intelligent pouvant exécuter des tâches à partir de l'observation des faits.

Des exemples simples, comme l'identification des plaques minéralogiques pour les politiques de tarification routière ou certains dispositifs sophistiqués capables de détecter des défauts mineurs sur les machines avant une panne, ne sont que la pointe de l'iceberg. Même dans des applications courantes comme la surveillance des commerces, les nouvelles technologies ajoutent des éléments tels que le comptage de personnes et l'analyse des comportements d'achat qui facilitent l'agencement des magasins et la conception de nouveaux centres commerciaux.

La demande est en forte croissance. Selon Cisco, les applications vidéo à des fins professionnelles et de divertissement représenteront 79 % du trafic internet à l'horizon 2020[1]. En outre, il est de plus en plus facile de créer des vidéos grâce aux petites caméras moins élaborées mais à faible coût qui existent sur le marché. Le transfert vidéo depuis la source gagne également en simplicité avec l'extension de la connectivité internet et les réseaux mobiles à plus grande vitesse. La vidéo, notamment la vidéosurveillance, est largement perçue comme une avancée sociétale majeure pour lutter contre la criminalité et accroître la liberté des personnes en rendant les environnements plus sûrs. Cependant, cette omniprésence de la vidéo s'accompagne d'attaques de plus en plus virulentes de la part des criminels, terroristes et groupes d'action qui exploitent et perturbent les plateformes de vidéosurveillance pour servir leurs intentions malveillantes.

Risques des systèmes de vidéosurveillance et IOT non contrôlés

Auparavant, les attaques contre les réseaux de vidéosurveillance étaient rares en raison de la nature privée des transmissions filaires en boucle entre les sites surveillés et les salles de contrôle. D'autre part, la configuration matérielle primaire de l'infrastructure vidéo avec transmission par câble coaxial évitait tout risque d'attaque en surface. Les temps ont changé et, désormais, les caméras vidéo modernes sont pilotées par des logiciels connectés à un capteur d'image numérique. L'arrivée de caméras à faible coût gérées en ligne a facilité l'accessibilité aux systèmes de vidéosurveillance sur les réseaux IP.

De la même façon que les détaillants et fournisseurs de service sont confrontés aux vols de données de cartes bancaires et autres informations de valeur, la complexité et la nature changeante des processus informatiques augmentent la vulnérabilité des protocoles et des règles d'authentification. Le problème n'est pas nouveau. Depuis plus de dix ans, les experts de la sécurité[2] ont découvert des vulnérabilités dans les caméras qui affectent les grandes marques internationales comme les acteurs régionaux avec une liste croissante d'incidents, notamment :

- Les failles de sécurité dans les comptes utilisateur par défaut qui permettent d'obtenir le mot de passe administrateur.
- Le contournement des données d'authentification de l'utilisateur à l'aide d'identifiants codés incorporés dans le périphérique en tant que « backdoor » (porte dérobée) par le fabricant.
- L'exécution de code arbitraire sur le périphérique sans authentification par exploitation des vulnérabilités du gestionnaire de paquet du protocole RTSP (Real Time Streaming Protocol).
- Les failles de sécurité qui permettent de contourner l'authentification de l'opérateur de la caméra et d'accéder directement aux fichiers de configuration.
- Les failles de sécurité qui permettent à un pirate de réinitialiser le mot de passe d'accès au périphérique afin de modifier les fichiers de configuration et obtenir l'accès aux fonctions principales de la caméra.
- Les attaques directes contre les caméras qui permettent aux tiers d'intercepter les flux vidéo transmis en direct sur les réseaux privés ou par connexion internet.

Des millions de périphériques sont concernés par ces vulnérabilités et affectent de nombreux distributeurs de technologie sous licence. Alors que des correctifs sont régulièrement publiés par les grands fournisseurs à la réputation établie, nombre de revendeurs plus modestes ont tendance à ignorer le problème. Même lorsque des correctifs sont disponibles, le processus de mise à jour reste manuel et la plupart des exploitants de plateformes de vidéosurveillance ne sont pas informés de leur publication. Le problème concerne d'autant plus les particuliers dont les systèmes de vidéosurveillance grand public proposés dans le commerce n'ont toujours pas reçu de correctifs.

Attaques ciblées et botnets

Même si cela rappelle le scénario de films hollywoodiens à succès, la probabilité qu'un système complet de vidéosurveillance d'un site sensible soit détruit ne relève pas de la fiction. De nombreux revendeurs d'applications de vidéosurveillance réutilisent les mêmes bases de données logicielles qui gèrent des éléments comme le streaming, l'authentification utilisateur et le transfert des vidéos sur les supports de stockage. Il est dès lors facile à des agresseurs qualifiés de préparer leurs attaques, voire de provoquer la terreur et la panique.

La transversalité des réseaux est une autre opportunité pour les cybercriminels de s'introduire dans un périphérique associé, une caméra par exemple, puis de l'utiliser comme point d'authentification pour accéder à d'autres ressources connectées. Bien que les protections réseau soient généralement conçues pour bloquer ce type d'attaque, la hausse de la demande en caméras et autres périphériques IoT (internet des objets) dotés de processus intelligents augmente le risque d'intrusion. Mais les attaques contre les caméras elles-mêmes ne sont pas le seul problème. Récemment, des caméras ont été détournées et utilisées comme moyen de lancer des attaques par déni de service distribué (DDoS).

Une attaque DDoS massive due en partie au botnet Mirai a affecté Twitter, Amazon, Tumblr, Reddit, Spotify et Netflix en octobre 2016. Comme l'a observé Allison Nixon, experte en sécurité et directrice de recherche chez Flashpoint, le botnet a essentiellement affecté les caméras IP et enregistreurs vidéo numériques (DVR) fabriqués par la société technologique chinoise XiongMai Technologies. Les composants fabriqués par XiongMai approvisionnent les fournisseurs grand public et se retrouvent par centaines de milliers dans des produits d'entrée de gamme comme autant de cybermenaces potentielles.[3]

Gouvernements, régulation et législation internationale

Selon Gartner, Cisco et d'autres spécialistes du secteur, l'explosion des objets connectés, qui devraient représenter entre 25 et 50 milliards[4] d'unités d'ici 2020, est un véritable casse-tête pour les gouvernements et les régulateurs internationaux. Contrairement aux transmetteurs radio, aux stations de télévision et aux véhicules à moteur, il n'existe pratiquement pas de législation relative aux objets connectés à Internet. Les normes de sécurité applicables à ces objets n'ont toujours pas été définies. Or, que faire quand un appareil est piraté ou utilisé pour attaquer un tiers ? Dans la plupart des régions, le droit pénal est adapté à la cybercriminalité lorsque l'agresseur et la victime sont identifiés. Mais avec le développement des applications autonomes, le risque que des périphériques non sécurisés soient le siège d'attaques virales comme ce fut le cas des ordinateurs de bureau pourrait réapparaître sur des dispositifs, comme les réseaux de caméras de vidéosurveillance, pour lesquels il existe peu de moyens de détecter le problème ou de remédier rapidement à la situation.

Mise en jeu potentielle des responsabilités pénales et financières

Se pose également l'épineux problème de la responsabilité. L'installation de systèmes de vidéosurveillance réduit généralement les coûts d'assurance et augmente les chances d'arrêter les délinquants. Toutefois, si un système de vidéosurveillance devient inopérant en raison d'une faille de sécurité et qu'un délit est commis et non enregistré par la caméra, les assureurs peuvent refuser d'indemniser les dommages par manquement aux conditions d'application des garanties. Dans ce cas, la victime est-elle fondée à poursuivre en justice le fabricant de la caméra ? Quid du fournisseur dans le cadre d'un contrat de maintenance d'un système CCTV ? Et en cas d'incident portant atteinte à la sécurité publique, la responsabilité de l'État est-elle engagée ? Les vulnérabilités des systèmes, tels que la vidéosurveillance, soulèvent de nombreuses questions et les cas d'écoles sont encore peu nombreux, si bien que l'incertitude règne sur le marché.

Protection de la vie privée

Si les questions de responsabilité pénale et financière liées au piratage des dispositifs de vidéosurveillance font encore débat, les pays développés ont pour la plupart intégré dans leur droit la protection de la vie privée des

citoyens. À part quelques différences d'un pays à l'autre, toutes les données à caractère personnel relatives à la santé, aux finances, à l'orientation sexuelle, aux opinions politiques et à divers autres aspects doivent être recueillies et conservées dans des conditions optimales de sécurité. Cette obligation s'applique également aux données vidéo. Par exemple, les enregistrements vidéo concernant un patient se rendant dans une clinique psychiatrique ou à un rassemblement politique doivent être conservés en sécurité et en dehors du domaine public. En cas de cyberattaque contre un dispositif ou un réseau de vidéosurveillance, il existe un risque très élevé que les informations privées - images et autres données - ciblent des personnes en particulier et soient volées puis diffusées sans autorisation. Ceci porterait atteinte aux droits des utilisateurs à la protection de la vie privée par l'intermédiaire du système et pourrait entraîner des poursuites légales à l'encontre de la personne responsable du traitement des données personnelles.

Action des gouvernements

Les gouvernements confrontés à ces questions sont en attente de clarifications face aux risques que représente l'émergence des appareils IoT. En Europe, les hauts responsables de la Commission européenne proposent de créer une procédure de certification pour les dispositifs relevant de « l'Internet des Objets » (IoT) visant à garantir la protection des utilisateurs. La Commission a également soutenu la création d'un groupement nommé « Alliance pour l'innovation dans le domaine de l'Internet des Objets » qui rassemble plusieurs grands fournisseurs de produits technologiques dans les secteurs de l'énergie, de l'automobile et de la santé, avec pour mission d'élaborer un ensemble de règles de bonnes pratiques. Aux Etats-Unis, le département de la sécurité intérieure a publié un guide des principes stratégiques relatifs à la sécurité de l'Internet des Objets[5]. Parmi les différents sujets traités, ce guide rassemble certains principes fondamentaux comme l'intégration des paramètres de sécurité dès la phase de conception, la promotion des mises à jour de sécurité et la gestion des vulnérabilités, en donnant la priorité aux mesures de sécurité en fonction de leur impact potentiel. Il n'existe pourtant toujours pas de consensus général ou de recommandations de l'industrie, comme c'est le cas avec les normes PCI-DSS dans le secteur des cartes de paiement. En conséquence, la sécurité des objets connectés est encadrée pays par pays et relève d'une réglementation succincte dont la portée et l'efficacité sont très variables.

L'approche de MOBOTIX

En tant que leader du secteur de la vidéosurveillance numérique, MOBOTIX marque là aussi sa différence en développant ses propres logiciels en interne. Nous sommes ainsi en mesure de proposer des produits sophistiqués dont les performances en matière de sécurité sont particulièrement appréciables. En contrôlant la chaîne de développement, MOBOTIX est moins exposé aux incidents de sécurité résultant de logiciels et de matériel tiers mal conçus. Dans les domaines où nous appliquons les normes de l'industrie largement adoptées telles que le protocole ONVIF, nos procédures en place assurent la publication immédiate des correctifs à mesure de leur disponibilité. Comme le même logiciel est utilisé pour tous les modèles de caméra MOBOTIX, ce processus continu de mise à jour et de sécurisation du firmware facilite la gestion des caméras pour nos clients internationaux.

En matière de sécurité, la recherche de l'excellence dès la phase de conception motive l'entreprise depuis sa création et se manifeste dans de nombreux domaines :

Sécurisation des systèmes d'exploitation et mises à jour

L'approche de MOBOTIX pour la sécurité de ses caméras s'exprime dès la conception du système d'exploitation et des couches applicatives. Tous les périphériques MOBOTIX sont construits sur une architecture Linux modifiée et sécurisée qui supprime les services et modules standard. Les modules Linux critiques, tels que l'authentification, sont entièrement recréés par les ingénieurs MOBOTIX afin d'éliminer les risques de vulnérabilité aux intrusions et techniques d'injection de code classiques. Ce logiciel d'exploitation, qui n'est pas open source, est protégé par des procédures de sécurité supplémentaires. En outre, chaque mise à jour du firmware du périphérique et des composants logiciels est chiffrée et signée numériquement pour éviter les tentatives d'altération.

Configuration sécurisée des caméras

L'accès à l'interface de configuration de la caméra n'est octroyé qu'aux utilisateurs autorisés. Par mesure de sécurité, la création et l'application de privilèges différents par groupes d'utilisateurs relève d'un processus interne à chaque système. En pratique, les mots de passe utilisateur ne sont jamais enregistrés en clair dans les caméras MOBOTIX, mais sont hachés grâce à un algorithme de hachage unidirectionnel puissant (SHA-512). Même si le fichier de configuration tombait entre de mauvaises mains, la récupération du mot de passe en clair s'avèrerait quasiment impossible. Les services sous OS Linux non essentiels sont désactivés pour limiter les intrusions potentielles et prévenir les attaques, et il n'existe aucun telnet ou « mot de passe maître » non documenté. Une caméra MOBOTIX est accessible et configurable via son interface utilisateur graphique (GUI) Web. Les mots de passe peuvent être conservés dans des systèmes de gestion des privilèges d'accès comme BeyondTrust et CyberArk dont la sécurité peut être renforcée par protocole d'authentification à deux facteurs.

Communications réseau et périphérique sécurisées

Toutes les données échangées sur le réseau entre les hôtes et chaque caméra MOBOTIX peuvent être chiffrées pour en garantir la confidentialité et l'intégrité pendant la transmission. Les protocoles HTTPS (SSL/TLS) et les certificats sont tous pris en charge par défaut en conformité avec les bonnes pratiques recommandées par les principaux experts de la sécurité comme le SANS Institute. MOBOTIX offre également un support intégré pour la gestion des certificats X.509 spécifiques pour chaque caméra et autorité de certificat racine afin que les entreprises puissent inclure dans le protocole de sécurité de leurs périphériques les caméras et portiers vidéo authentifiés via des systèmes comme OpenVPN. En d'autres termes, si une caméra est volée ou piratée, il sera impossible au criminel d'utiliser les identifiants dans l'appareil pour s'emparer du reste des caméras du réseau.

Enregistrement interne sécurisé et protection contre les modifications

Tous les enregistrements générés par la caméra peuvent être chiffrés avant leur stockage, en commençant par la mémoire tampon circulaire qui utilise la carte SD intégrée dans chaque caméra. MOBOTIX a développé un système de fichiers sécurisés grâce auquel, si une caméra est volée ou piratée, les vidéos enregistrées et encore présentes dans l'appareil ne peuvent pas être récupérées sans avoir obtenu au préalable les droits administrateur, eux-mêmes protégés par les processus de sécurisation de la configuration décrits précédemment. Chaque image produite par une caméra MOBOTIX peut être signée numériquement au moyen de certificats personnalisés pour prévenir

toute altération ; ceci garantit l'acceptation des enregistrements comme moyen de preuve lors d'une procédure pénale.

Fonctionnalités de sécurité	✗	MOBOTIX
HTTPS (SSL/TLS) et certificats	✓	✓
Authentification HTTP Digest	✓	✓
Listes de contrôle d'accès	✓	✓
Utilisateurs et groupes avec droits personnalisés	⚠	✓
Détection d'intrusion	✗	✓
Protection contre les robots	✗	✓
Enregistrements chiffrés	✗	✓
Vidéos et messages chiffrés	✗	✓
Client VPN	✗	✓

Détection d'intrusion

Malgré le nombre de systèmes et de processus de sécurité en place, il serait imprudent de croire que les caméras MOBOTIX sont à l'abri de tentatives malveillantes. C'est pourquoi MOBOTIX a adopté des mesures renforcées pour détecter de telles attaques. Chaque caméra ou portier vidéo intègre des composants de détection d'intrusion qui signalent sur un canal crypté toute connexion non autorisée ou attaque en force. En outre, des notifications peuvent être envoyées en cas d'échecs successifs de tentatives de connexion et l'adresse IP en cause peut être bloquée automatiquement.

Synthèse

L'usage croissant de la vidéosurveillance et d'autres applications vidéo dans le domaine de la santé, de la sécurité et des procédés industriels ne montre aucun signe de ralentissement. Alors que ces dispositifs deviennent incontournables, d'autres processus tels que le contrôle d'accès, la surveillance de l'environnement et les systèmes d'analyse comme la reconnaissance faciale seront de plus en plus ciblés par les cybercriminels.

Les prescripteurs de systèmes de vidéosurveillance, les opérateurs de services voire les régulateurs devront étendre les contrôles en matière de sécurité dans le cadre de leur devoir de vigilance envers les citoyens et de leurs obligations légales présentes et à venir. En tant que professionnels du secteur, des leaders comme MOBOTIX ont identifié ces problèmes et s'investissent activement dans l'intégration logicielle et matériel et composants de sécurité dès les premiers stades de la conception.

Cependant, la sécurisation des périphériques n'a de sens que si l'environnement global est protégé. Il ne sert à rien de verrouiller la porte si la fenêtre reste ouverte. À ce titre, les prescripteurs et opérateurs de vidéosurveillance ainsi que les réseaux IoT étendus doivent évaluer d'autres éléments comme le réseau sous-jacent, l'infrastructure de stockage et, surtout, l'élément humain qui est souvent le maillon faible de la chaîne. Plusieurs groupements d'industriels comme le SANS Institute ont élaboré des recommandations utiles, notamment les Contrôles critiques de sécurité développés par le Centre pour la sécurité sur Internet (CIS). Il s'agit d'un ensemble de mesures de cyberdéfense proposées comme moyens ciblés et efficaces pour stopper les attaques les plus dangereuses qui se répandent aujourd'hui.[6]

À l'avenir, il est clair que la sécurité des périphériques et des plateformes va devenir un facteur clé dans les grands projets vidéo et, à mesure que la prise de conscience des enjeux de l'IoT s'amplifie, MOBOTIX est prêt à coopérer avec ses pairs, ses clients et les services gouvernementaux afin de protéger les technologies et les systèmes essentiels qui contribuent à rendre la société plus sûre pour chacun d'entre nous.

Références

https://www.coresecurity.com/system/files/publications/2016/05/corelabs-ipcams-research-falcon-riva.pdf

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Sources

[1]https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.

[2]html https://www.coresecurity.com/advisories/hikvision-ip-cameras-multiple-vulnerabilities

[3]https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

[4]http://www.telecomtv.com/articles/iot/internet-of-things-to-reach-25-billion-devices-within-five-years-11931/

[5]https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[6]https://uk.sans.org/critical-security-controls

MOBOTIX développe et fabrique des systèmes vidéo IP ainsi que des logiciels de gestion d'analyse vidéo depuis l'année 2000 en Allemagne.

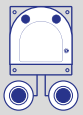
MOBOTIX se distingue par son **niveau élevé de fiabilité**. Toutes les caméras extérieures sont soumises à un test de résistance aux températures comprises entre -30 °C et +60 °C (-22 °F et +140 °F). Dépourvues de composants supplémentaires, de dispositif de chauffage ou de refroidissement ainsi que de pièces mobiles (par exemple des diaphragmes automatiques), elles ne nécessitent quasiment aucun entretien.

MOBOTIX fournit un **paquet parfaitement cohérent**, à commencer par la carte microSD pour la gestion du stockage et l'audio HD (microphone et haut-parleur) avec la téléphonie VoIP, sans oublier l'analyse vidéo, un système de gestion vidéo professionnel et un logiciel de détection de déplacements réduisant les fausses alertes.

L'architecture décentralisée signifie qu'aucun ordinateur central n'est nécessaire et que la charge réseau est minime. Les caméras intelligentes de MOBOTIX traitent et stockent les données d'images elles-mêmes, déclenchent des événements et, en cas d'accès à distance, gèrent le taux de rafraîchissement et la résolution de l'image en fonction de la bande passante disponible.

Les **capteurs Moonlight 6 MP** accompagnés de la **technologie d'imagerie thermique** garantissent une détection fiable des objets en mouvement, même dans des conditions de luminosité extrêmes et sur de longues distances. Cela permet par conséquent de couvrir de larges zones avec seulement quelques caméras. Exige moins de câbles d'alimentation, d'infrastructure informatique et de sources de lumière supplémentaires. Toutes les caméras MOBOTIX sont alimentées via PoE standard et ne consomment pas plus de 4 ou 5 watts.

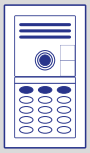
Un système vidéo IP intelligent de MOBOTIX vous permet de **réduire vos coûts globaux**. L'investissement est rentabilisé en très peu de temps et le logiciel et les mises à jour gratuits garantissent un investissement à l'épreuve du futur.

Double optique d'extérieur			Thermique	
M16 AllroundDual	S16 FlexMount	D16 DualDome	M16 Thermal	S16 DualThermal
				
Robuste pour conditions extrêmes	Caméra double flexible	Caméra double modulaire	Thermique double	Thermique double

Optique simple d'extérieur			
M26 Allround	S26 FlexMount	Q26 Hemispheric	D26 Dôme
			
Robuste pour conditions extrêmes	Discrète, analyse vidéo	Discrète, analyse vidéo	Modulaire, dôme fixe

Intérieur			
i26 panoramique	c26 Hemispheric	p26 Allround	v26 MiniDome
			
180° hemispheric	Discrète, analyse vidéo	Caméra modulaire de plafond	Caméra anti-vandalisme

Modules de porte			MxDisplay+
Caméra	BellRFID	Clavier	Poste terminal
			

Kits de porte			
Double cadre		Triple cadre	
			

FR_11/17

MOBOTIX AG
Kaiserstrasse
D-67722 Langmeil
Tél. : +49 6302 9816-103
Fax : +49 6302 9816-190
sales@mobotix.com
www.mobotix.com

MOBOTIX