L‘évolution du contrôle d‘accès :

conseils pour les projets de bureaux connectés

Contenu

AVANT-PROPOS

Il ne fait aucun doute que la demande de solutions de contrôle d'accès intelligentes est en hausse, mais ce qui constitue le meilleur contrôle d'accès de sa catégorie dans les immeubles de bureaux connectés évolue constamment à mesure que la technologie se développe et que les attentes des employés de bureau changent.

Si vous êtes un intégrateur ou un installateur de systèmes travaillant sur un projet de bureau ou de bâtiment commercial, à quoi devez-vous penser lorsque vous décidez de la solution de contrôle d'accès à privilégier ? Avec tant de facteurs à prendre en compte, quelles doivent être vos priorités ?

En tant que leader mondial des systèmes de Visiophonie IP, 2N travaille aux côtés de ses clients et partenaires dans le monde entier, pour les aider à trouver la bonne solution pour leurs projets de bureaux. Cette expérience pratique ne fait pas seulement de nous des experts en solutions de contrôle d'accès, elle nous donne également un aperçu étonnant des priorités qui guident les décisions des clients en matière de contrôle d'accès - une compréhension qui a également été éclairée par une enquête que nous avons menée l'année dernière auprès des distributeurs, des intégrateurs de systèmes et des installateurs opérant dans la région EMEA, en Asie-Pacifique ainsi que sur le continent américain.

Ce livre blanc est conçu pour résumer les idées les plus pertinentes. Il se concentrera sur les avantages des systèmes, vous aidera à comprendre les dernières technologies disponibles et vous expliquera ce que vous devez prendre en compte pour être certain de choisir des solutions qui pourront évoluer avec vous au cours des dix prochaines années.

Nous espérons que vous y trouverez une lecture informative, agréable et, surtout, utile sur le plan pratique.

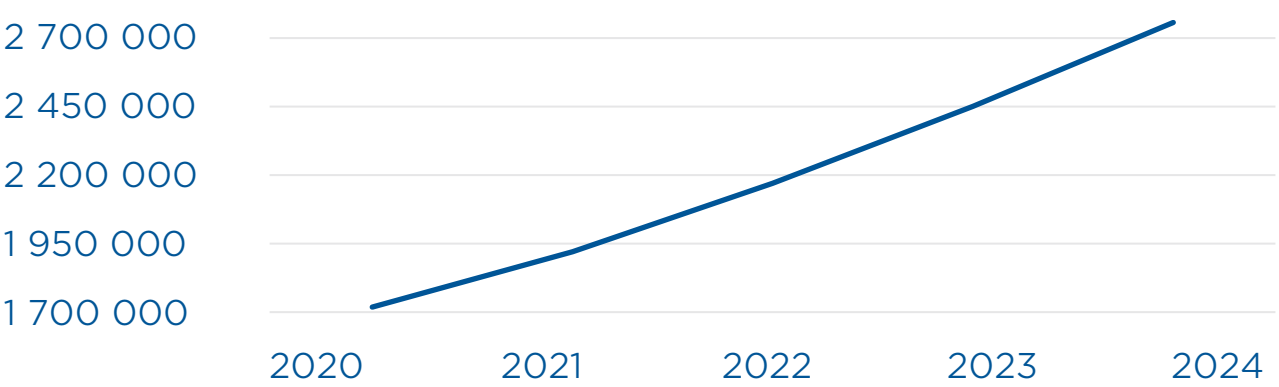
Michal Kratochvíl
PDG de 2N Telekomunikace

En ce qui concerne les immeubles de bureaux connectés, qu'est ce que l'on entend par „contrôle d'accès intelligent" ?

D'après notre expérience et l'enquête que nous avons menée auprès des professionnels du secteur, les gestionnaires d'immeubles de bureaux perçoivent de plus en plus la valeur commerciale que peut apporter un système de contrôle d'accès intelligent - même si le contrôle d'accès ne représente que 0,1 % du coût total de la construction d'un bâtiment.

Le contrôle d'accès intelligent peut cependant se présenter sous différentes formes. Quels sont donc les choix que nos clients font et, surtout, pourquoi les font-ils ?

Augmentation prévue des ventes de contrôleurs IP dans le monde[1]



[1] Base de données OMDIA sur le contrôle d'accès - 2020

01

OMDIA prévoit que les ventes de contrôleurs IP dans le monde augmenteront de plus de 12,5 % en moyenne chaque année au cours des quatre prochaines années (voir ci-dessus). De plus en plus de personnes adoptent les avantages de la technologie IP, notamment pour la rapidité d'installation, les fonctions avancées et la gestion à distance, qui permettent aux installateurs et aux intégrateurs de gagner un temps considérable.

02

Selon notre expérience, il existe un désir croissant de répondre aux attentes des employés de bureau qui souhaitent un accès rapide et pratique via leurs smartphones.
La plupart de nos installations sont désormais équipées d'un lecteur Bluetooth qui permet aux employés de bureaux d'éliminer les cartes d'accès et d'utiliser leur téléphone portable comme moyen d'identification pour entrer.

03

Nos clients sont de plus en plus nombreux à vouloir connecter leur solution de contrôle d'accès aux systèmes de sécurité et aux caméras, afin de renforcer la sécurité et de permettre à l'administrateur de contrôler plus facilement l'ensemble de l'immeuble de bureaux depuis un emplacement central.

04

D'une manière qui n'était pas universellement vraie il y a quelques années, nous constatons une compréhension généralisée du fait que l'indice de dépense d'énergie d'un bâtiment est un facteur déterminant dans l'évaluation de son efficacité.
La cyber-résilience est tout aussi importante que la sécurité physique. Les deux doivent donc être pris en compte de manière égale.

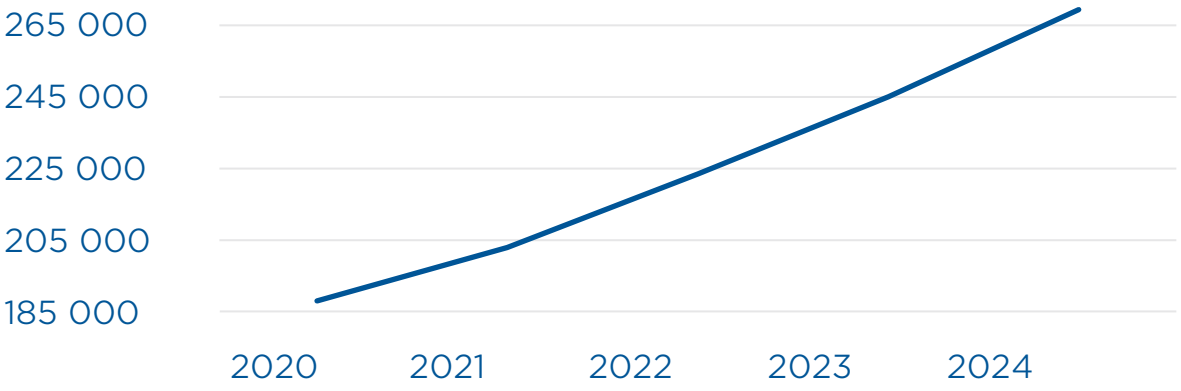
À l'heure actuelle, ce sont là quelques-uns des facteurs les plus importants qui définissent ce que les clients entendent par „contrôle d'accès intelligent".

Les pages qui suivent examinent chacun de ces domaines de manière plus détaillée, en transmettant davantage l'expertise de 2N à l'avant-garde du contrôle d'accès.

Technologie IP „Edge“ - l‘intelligence au service de vos projets de contrôle d‘accès

Un „dispositif IP Edge“ combine un contrôleur de porte en IP traditionnel et un lecteur intelligent (Bluetooth, biométrie, RFID, Clavier) en un seul et même dispositif autonome. Les données 2020 de l‘OMDIA Access Control Intelligence Database montrent que les dispositifs „Edge“ vont continuer à gagner en popularité au cours des prochaines années :

Augmentation prévue des ventes d‘appareils « Edge » dans le monde entier



Pourquoi ?
Quels sont les avantages des „appareil IP Edge“ ?

01 Toute l‘intelligence de la décision à la porte

Nos lecteurs intelligents sont livrés avec un contrôleur déjà intégré. Ils fonctionnent de manière autonome et sans serveur, ce qui signifie qu‘il n‘y a pas de point de défaillance unique - si un appareil est endommagé, une seule porte est affectée.

02 Installation rapide et économique

La plupart des immeubles de bureaux sont déjà équipés d‘un câblage IP, et l‘installateur n‘a donc pas besoin de passer des heures sur place. La prise en charge du PoE signifie que vous n‘avez besoin que d‘un seul câble UTP pour la connexion et l‘alimentation. Cela permet de gagner du temps lors de l‘installation et d‘économiser sur le câblage.

[1] Base de données OMDIA sur le contrôle d‘accès - 2020

03 Protocoles ouverts permettant l'intégration de systèmes tiers.

Tirez parti des protocoles ouverts tels que HTTP, SIP, ONVIF, RTSP et des API ouvertes pour connecter les produits 2N avec la gestion vidéo, la sécurité et la gestion du temps de présence.

04 Infrastructure de réseau évolutive offrant des solutions à l'épreuve du temps.

Se connecter aux anciennes solutions d'entrée avec plusieurs dispositifs nouveaux est coûteux prend du temps. Les systèmes basés sur l'IP, en revanche, sont extensibles à l'infini, et vous ne serez jamais confronté à des impasses dans votre installation.

05 Gestion à distance efficace depuis n'importe où

Proposez une aide immédiate à vos clients sans avoir à vous déplacer.
Connectez-vous aux dispositifs 2N via l'interface web et gérez-les à distance. La communication est, bien entendu, cryptée et 100% sécurisée.

06 Des fonctionnalités intelligentes pour une meilleure expérience utilisateur

Les interphones IP sont capables de détecter les mouvements, d'envoyer des notifications au système de surveillance, d'enregistrer le flux vidéo et de diffuser un signal d'avertissement. Ils permettent également au locataire d'ouvrir les portes à l'aide de son smartphone, même lorsqu'il n'est pas chez lui.

07 Des devis simples pour vos projets

Vous devez proposer une solution pour protéger 15 portes dans un bâtiment ? Oubliez la recherche et le calcul des bons contrôleurs, la réflexion sur les interfaces propriétaires et le câblage compliqué.
Demandez simplement le prix de 15 unités d'accès 2N. Aucune autre information n'est nécessaire.

> Les dispositifs Edge sont la pierre angulaire d'une solution complète de contrôle d'accès, de l'entrée du garage à l'entrée des bureaux et des salles de réunion, en passant par les portes d'entrée principale et arrière, la réception, l'ascenseur. Tous les appareils „communiquent" entre eux et sont gérés comme un système .
>
> Luca Passini, PDG de CWS

ÉTUDE DE CAS

Technologie IP „Edge“ : l‘intelligence au service de l‘environnement Vos projets de contrôle d‘accès

Client

Melittaklinic, une maison de retraite privée et un centre de réadaptation à Bolzano, en Italie.

Espace

Un complexe neuf, équipé selon les normes internationales les plus strictes et pouvant accueillir plus de 160 résidents et patients.

Priorités du projet

Une solution simple et intuitive pour le personnel et les résidents, une intégration transparente avec la plateforme de positionnement intérieur de CWS et évolutive pour s‘adapter à l’arrivée de nouveaux résidents, une gestion, une configuration et une installation faciles.

Solution

Des interphones 2N® IP Verso avec un clavier tactile ont été installés à chacune des entrées afin de sécuriser l‘accès au complexe.

300 lecteurs RFID 2N® Access Unit 2.0 ont été installés à l‘entrée de chaque chambre, ainsi qu‘à la piscine, aux salles de sport et aux autres installations de réhabilitation.

En plus des cartes RFID, un téléphone portable peut être utilisé pour l‘identification. Le personnel et les résidents ont seulement besoin de l‘application 2N® Mobile Key, qui transforme leur smartphone en carte d‘accès.

L‘intégration simple avec la plateforme de positionnement intérieur CWS a permis de connecter tous les interphones et unités d‘accès 2N au système de vidéosurveillance et de contrôle.

Si l‘un des résidents de la Villa Melitta tombe, son bracelet Bluetooth envoie une alerte ainsi que sa localisation au système de GTB Livion, qui est immédiatement transmis aux smartphones du personnel. Il envoie également une commande http à l‘unité d‘accès 2N afin que la porte reste ouverte pour le personnel.

La configuration et la gestion de l‘ensemble du système sont assurées par 2N® Access Commander et peuvent être effectuées à distance.

Luca Passini

PDG de CWS

La sécurité et le confort de nos résidents sont notre priorité absolue, et le contrôle d'accès est une considération très importante.

Les dispositifs d'accès 2N sont magnifiquement conçus et contribuent à protéger la vie privée de nos résidents ainsi que leur sécurité. L'intégration avec le système BMS Livion nous aide à les garder en sécurité.

Vous voulez en savoir plus sur la technologie IP 'edge' ?

Tomáš Vystavěl

Chef des produits

Vystavel@2n.cz

Nous constatons une croissance significative de l‘intérêt pour les identifiants mobiles dans les bureaux, en partie à cause de la pandémie.

Quels sont les facteurs déterminant le succès ou l‘échec des systèmes d‘accès mobiles ?

Les systèmes d‘accès par téléphone mobile sont sur le marché depuis un certain temps - le plus souvent, les solutions sont basées sur la technologie Bluetooth Low Energy ou NFC et elles sont proposées par de plus en plus d‘entreprises dans le monde. Cela signifie que nous avons souvent eu l‘occasion de voir les avantages par rapport aux cartes RFID traditionnelles. Nous avons également une très bonne compréhension des raisons pour lesquelles certains systèmes réussissent et d‘autres échouent.

Sur la base de notre expérience, voici les trois facteurs fondamentaux qui déterminent la réussite des projets mobiles :

01 Vitesse

Combien de temps l‘utilisateur doit-il attendre après son authentification avant que la porte ne s‘ouvre ?

02 Fiabilité

La porte s‘ouvrira-t-elle de manière fiable du premier coup ? Ou l‘utilisateur doit-il essayer d‘ouvrir la porte plusieurs fois ?

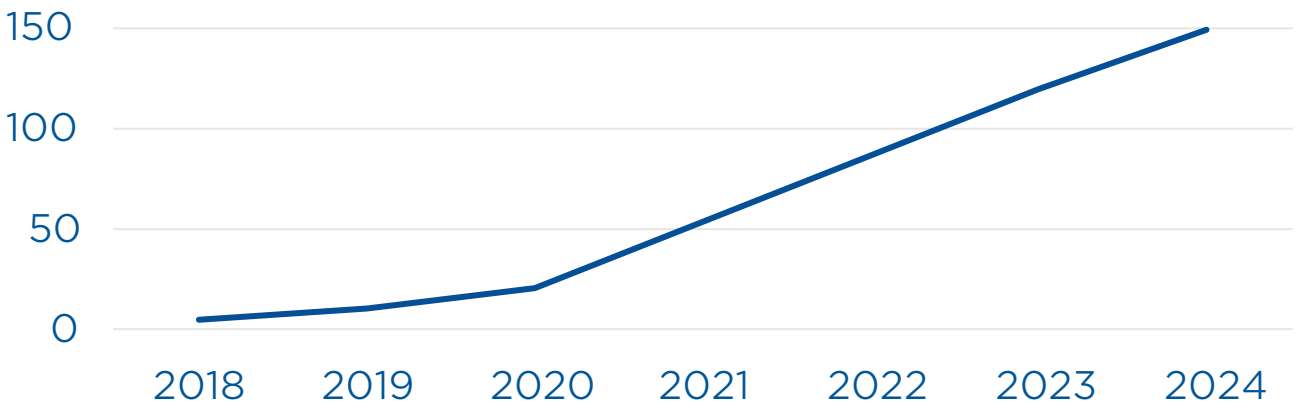
03 Sécurité

Comment s‘assurer qu‘un téléphone posé à proximité sur une table ne donne pas accès à une personne non autorisée ?

Bien que les deux tiers des administrateurs de bureau cherchent activement à introduire des systèmes de gestion de l‘information dans leurs bureaux, pour le contrôle d‘accès „sans contact“, il est absolument essentiel de choisir le bon fournisseur si vous voulez profiter de tous les avantages du Contrôle d’accès mobiles.

Le secteur prévoit une croissance exponentielle des dispositifs d'identification mobiles au cours des prochaines années :

Téléchargements annuels de dispositifs d'identification mobiles dans le monde (millions)[1]



> Les dispositifs d'identification mobiles représentent actuellement un pourcentage relativement faible du total (4,7 %), mais ce marché est appelé à connaître une croissance dynamique après 2020.
>
> Enquête sur le service d'information sur le contrôle d'accès d'Omdia, 2020

[1] Base de données OMDIA sur le contrôle d'accès - 2020

LA DEMANDE DES EMPLOYÉS DE BUREAU

De nos jours, les gens cherchent à réaliser de plus en plus de chose avec leur smartphone. Les paiements par smartphone ont augmenté de 67 % cette année avec le COVID-19, et les cartes de fidélité des magasins sont remplacées par des applications, car personne ne veut se plus se promener avec autant de cartes dans son portefeuille. Il en va de même pour le contrôle d'accès. Pourquoi transporter des cartes ou des badges supplémentaires, alors que l'application 2N® Mobile Key peut transformer votre téléphone en carte d'accès ?

41 % des employés de bureau déclarent désormais que leur choix préféré pour stocker des informations d'identification est leur smartphone ou leur montre connectée.[2]

SÉCURITÉ

Aucune technologie de contrôle d'accès, aussi pratique soit-elle, ne peut faire de compromis sur la sécurité. Heureusement, les dispositifs d'identification mobiles de 2N utilisent des normes de cryptage de „qualité gouvernementale" (AES128). Ils évitent également que les employés de bureau perdent leurs cartes physiques, ce qui est relativement fréquent :

41 % d'entre eux ont signalé la perte ou le vol de leurs clés, de leurs cartes ou de leurs porte-clés[2].

34 % ont laissé quelqu'un emprunter leurs clés, leurs cartes ou leurs porte-clés.[2]

FLEXIBILITÉ

Les identifiants mobiles donnent aux administrateurs la possibilité de contrôler l'accès à l'ensemble du bâtiment, et pas seulement aux entrées principales, équipées d'interphones vidéo. Les lecteurs Bluetooth tels que la 2N® Access Unit 2.0 sont relativement peu coûteux et peuvent être facilement déployés pour contrôler l'accès à des pièces ou des zones individuelles.

COÛT / COMMODITÉ POUR LES ADMINISTRATEURS

€ 5-10 Le coût typique des cartes à puce (bien qu'elles puissent aller jusqu'au double).

Leur remplacement coûte également de l'argent, contrairement aux dispositifs d'identification mobiles. Le facteur commodité est aussi à prendre en compte. Les identifiants mobiles peuvent être rapidement générés et délivrés à distance à l'utilisateur. Ils peuvent être facilement remplacés en cas de perte ou de vol du téléphone.

SANS CONTACT

L'attention se porte sur la technologie sans contact pour rendre les bureaux plus sûrs lorsque les employés commencent à revenir. Le „mode tactile" de 2N, par exemple, évite le contact avec la peau et réduit les risques de sécurité pour les utilisateurs finaux.

[Les identifiants mobiles] seront particulièrement intéressants pour les propriétaires de bâtiments fréquentés par des visiteurs et des entrepreneurs de passage... [au lieu de] réémettre les mêmes dispositifs d'identification physiques à de multiples entrées, une pratique qui peut être considérée comme insalubre dans le sillage du COVID-19 1 [1].

MIGRATION PROGRESSIVE AU COURS DU TEMPS

La gamme de lecteurs 2N propose des options d'appareil à technologie d'accès multiples. En choisissant notre lecteur RFID et Bluetooth, ou codes PIN et Bluetooth, les administrateurs peuvent migrer vers du Contrôle d'accès Mobile plus pratiques au fil du temps, sans qu'il ne soit nécessaire de faire ce changement du jour au lendemain pour chaque personne utilisant le lecteur.

[1] OMDIA Access Control Intelligence Database – 2020 [2] Nexkey's 2020 Access Control Trends Review
[3] Statista Digital Market Outlook

ÉTUDE DE CAS

Nous constatons une croissance significative de l'intérêt pour les identifiants mobiles dans les bureaux, en partie motivés par la pandémie

Client

Albion Cars, un concessionnaire Jaguar et Land Rover a récemment ouvert à Prague.

Espace

4 000m2, comprenant le plus grand showroom de République tchèque, des installations d'entretien et un espace de vente extérieur. Le plus grand showroom et service de la République tchèque est basé sur le concept global de ces deux marques britanniques, en mettant l'accent sur les points suivants.

Nombre d'employés

100+

Priorités du projet

Design luxueux, système d'entrée sans clé, facile à gérer, à configurer et à installer.

Solution

40 unités d'accès 2N® Bluetooth et RFID ont été installées aux entrées. Les utilisateurs n'ont besoin que de l'application 2N® Mobile Key, qui transforme leur smartphone en carte d'accès.

Les interphones 2N® IP Verso ont été choisis pour les entrées principales, quatre d'entre eux étant installés sur chaque site. L'IP Verso a été choisi principalement en raison de sa modularité, de son design luxueux et de ses fonctionnalités.

L'application 2N® Mobile Video, permet de recevoir l'appel à distance des visiteurs via les interphones et de leur ouvrir ensuite la porte.

La configuration et la gestion du système d'accès complet sont assurées par le logiciel 2N® Access Commander. Grâce à l'interface utilisateur graphique, les autorisations d'accès et les fonctions spécifiques sont définies de manière centralisé, par exemple pour déterminer qui a accès à certaines zones. En temps voulu, il sera également possible d'ajouter un système de gestion de présences qui enregistre le temps de présence des employés et peut être consulté via l'interface web ou exporté vers un fichier XLS ou CSV.

Karel Stolejda,
PDG et propriétaire
d'Albion Cars

Dans le passé, nous avons eu des problèmes de perte de cartes d'accès, nous avons donc cherché une solution pour résoudre ce problème. Pour cette raison, nous avons opté pour la solution 2N qui nous permet de passer à un tout nouveau système via la technologie Bluetooth.

Vous voulez savoir comment 2N peut vous aider avec une solution mobile ?

Gareth Robinson
Chef produit
Robinson@2n.cz

ACCENT SUR LA CYBERSÉCURITÉ

Le Hiscox Cyber Readiness Report 2020 a interrogé 5 569 professionnels responsables de la stratégie de cybersécurité de leur organisation dans huit pays d'Europe et d'Amérique du Nord. Elle a mis en évidence l'importance accrue accordée par les entreprises - des plus grandes aux plus petites - à la prévention des cyberattaques :

39 %

Augmentation des dépenses en matière de cybersécurité entre 2020 et 2019.

1.8 MILLIARD DE DOLLARS

Les cyber-pertes totales parmi les entreprises touchées (en hausse par rapport à 1,2 milliard de dollars en 2019).

$ 57,000

Impact financier médian sur les personnes touchées par un cyber-événement (presque six fois plus élevé qu'en 2019).

Přístupové systémy nebyly vždy řešeny s ohledem na kybernetickou bezpečnost. Vzhledem k potenciálnímu dopadu kybernetických útoků se však jeví jako zásadní zvolit systém, který zahrnuje šifrování k ochraně komunikace, autorizuje přístup k zařízení, jeho API a zamezuje neoprávněným vstupům.

> Les systèmes de contrôle d'accès n'ont pas toujours été une priorité en matière de cybersécurité, mais compte tenu de l'impact potentiel des cyberattaques sur les entreprises, il est essentiel de choisir un système qui inclut l'utilisation du cryptage pour protéger la communication entre les appareils, sécurise l'accès au dispositif et à son API et garantit l'absence de portes dérobées à des „fins de maintenance".
>
> Tomáš Vystavěl, chef des produits, 2N Telekomunikace

Quelles sont les 5 principales menaces de cybersécurité auxquelles sont confrontés les bâtiments commerciaux et comment protéger nos appareils de contrôle d'accès contre ces menaces ?

01 Attaque de type „Man-in-the-middle“ (MitM)

Attaque au cours de laquelle un pirate se connecte à un réseau et écoute les communications entre les terminaux (par exemple, le code d'ouverture de la porte, le mot de passe de connexion du terminal).

Notre protection contre les MitM ?

Nous prenons en charge des protocoles tels que HTTPS, TLS, SIPS ou SRTP.

02 Connexion non autorisée au réseau LAN

L'interphone ou le lecteur peut être installé à l'extérieur du bâtiment (c'est-à-dire sur un mur extérieur) et il existe un risque potentiel que quelqu'un casse l'interphone et utilise le câble UTP pour se connecter au réseau LAN.

Notre protection contre les connexions non autorisées au réseau LAN ?

Nous utilisons un protocole 802.1x qui nécessite une autorisation du dispositif par rapport au serveur (vous devez connaître votre nom, votre mot de passe, votre adresse MAC, etc.) pour vous connecter. La sécurité physique étant une condition préalable à une cybersécurité fiable, les dispositifs 2N intègrent également un commutateur d'autoprotection. Si quelqu'un tente de les ouvrir, une alarme se déclenche et une vidéo commence à être enregistrée.

03 Mot de passe / attaque par dictionnaire“

Une attaque où un pirate tente de deviner le mot de passe pour entrer dans l'appareil (il utilise un générateur de mot de passe et essaie différentes options).

Notre protection contre les attaques par mot de passe ?

L'installateur doit d'abord remplacer le mot de passe par défaut par un nouveau mot de passe fort (huit caractères) juste après la première connexion à l'appareil. Nous disposons ensuite d'un mécanisme de protection qui fait que si vous entrez le mot de passe de façon incorrecte trois fois, vous devez attendre. 30 secondes avant de pouvoir entrer à nouveau.

04 Empêcher les vues non autorisées de la caméra des interphones

Il arrive souvent que les caméras IP soient installées avec un mot de passe par défaut, et n'importe qui peut s'y connecter et regarder ce qui se passe.

Notre protection contre les vues non autorisées de la caméra de l'interphone ?

Sur nos interphones IP, vous pouvez définir un accès autorisé au flux RTSP - c'est-à-dire à la caméra (pour un aperçu, vous devez connaître l'adresse IP, le nom et le mot de passe) - ou un accès uniquement depuis une adresse IP spécifique.

05 Attaques de logiciels malveillants contre les appareils mobiles

Les pirates s'intéressent de plus en plus aux attaques contre les smartphones, qu'il s'agisse de vol d'identifiants, de surveillance ou de publicité malveillante.

Notre protection contre les attaques de logiciels malveillants sur les appareils mobiles ?

Notre communication est cryptée par deux types de chiffrement : RSA-1024 (couplage) et AES-128 (communication proprement dite lors de la tentative d'ouverture de la porte). En outre, il existe d'autres mécanismes spéciaux qui empêchent le vol non autorisé des identifiants mobiles par un tiers.

2N CHECKLIST

Comment protéger les immeubles de bureaux intelligents, les données critiques et la sécurité contre les pirates et les intrus ?

- ☐ Choisissez une solution de sécurité fiable et sur mesure, spécialement conçue pour les environnements ICS, qui assure la sécurité de votre réseau à tout moment.
- ☐ Créez un réseau indépendant - dédié exclusivement aux appareils qui traitent des informations sensibles ; utilisez le réseau local virtuel (VLAN) et assurez-vous que les fabricants des appareils ou des logiciels installés utilisent par défaut des protocoles de mise en œuvre tels que HTTPS, TLS, SIPS ou SRTP.
- ☐ Créez différents comptes avec des privilèges différents : un utilisateur ne pourra apporter que des modifications liées à ses tâches spécifiques, tandis que l'administrateur disposera de privilèges plus importants pour gérer le bâtiment et tous les comptes associés.
- ☐ Mettez régulièrement le firmware à jour : il est important d'installer la dernière version du firmware sur les appareils pour limiter les risques liés aux cyberattaque. Chaque nouvelle version corrige les bugs trouvés sur le logiciel en mettant en œuvre les derniers correctifs de sécurité.
- ☐ Utilisez des mots de passe complexes et renforcés d'au moins huit caractères et composés d'une combinaison de chiffres, de lettres et de symboles.
- ☐ Effectuez des audits de sécurité réguliers de l'infrastructure informatique afin d'identifier et d'éliminer les éventuelles vulnérabilités.
- ☐ Formez l'équipe de sécurité chargée de protéger l'infrastructure informatique du bâtiment aux menaces les plus courantes et à la manière d'y faire face. En outre, les employés doivent être formés à être sceptiques à propos de pratiquement tout.
- ☐ Consultez le 2N Hardening Guide, qui fournit des conseils techniques à toute personne impliquée dans l'installation / l'intégration des dispositifs 2N pour garantir qu'ils sont sûrs et qu'ils font partie d'une sécurité réseau complète. Le Hardening Guide traite également de l'évolution des différents types de menace.

La cybersécurité est l'un des principaux défis auxquels sont confrontées les organisations aujourd'hui. Il est essentiel que les systèmes de sécurité et de contrôle d'accès en réseau offrent aux clients la solution la plus sûre possible. Afin de maîtriser la complexité croissante, il est de la plus haute importance d'accorder une attention particulière à l'assurance qualité du logiciel du produit.

Carsten Pinnow,
Expert en sécurité informatique basé à Berlin

Vous voulez en savoir plus sur l'approche de 2N en matière de cybersécurité ?

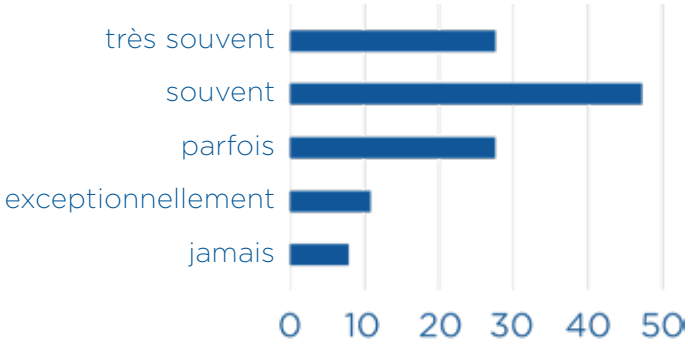
Lukáš Psota

Responsable du marketing produit
Psota@2n.cz

DES INTÉGRATIONS

D'après une enquête 2N menée auprès de plus de 120 distributeurs, intégrateurs de systèmes et installateurs opérant dans le monde entier en 2020, le passage à un système offrant de meilleures options d'intégration est l'une des principales motivations pour la mise à jour d'un système de contrôle d'accès existant.

Combien de fois le passage à un système offrant de meilleures options d'intégration est-il une motivation pour mettre à jour un système existant ?



Le passage à un système plus facilement interopérable est la troisième motivation la plus courante pour la mise à jour d'un système existant, après „le passage vers un système offrant des fonctionnalités plus avancées" et „le passage à un système IP".

Les „capacités d'intégration" arrivent également en troisième position sur une liste de 14 facteurs qui motivent les intégrateurs et les installateurs à utiliser 2N pour le contrôle d'accès, derrière la „fiabilité" et la „disponibilité du support".

Vous voulez en savoir plus sur les intégrations intelligentes ?

Radka Talianová

Responsable des partenaires technologiques
Talianova@2n.cz

Si vous tenez à ce que votre système soit entièrement intégré dans une solution complète, quels sont les points à prendre en compte ?

Dans un premier temps, votre système devra être basé sur la technologie IP et les normes/protocoles ouverts tels que : Le protocole de signalisation SIP pour la communication vocale sur IP (VoIP), RTSP (une norme largement reconnue pour le streaming audio/vidéo), ONVIF S (conçu pour les dispositifs vidéo basés sur l'IP qui peuvent envoyer des données vidéo sur un réseau IP) et API (un intermédiaire logiciel qui permet à deux applications de dialoguer entre elles).

Ensuite, vous souhaiterez sans doute que votre système soit connecté au VMS (Video Management System), qui relie le système d'accès aux caméras de sécurité, en contrôlant les appareils et en enregistrant les flux vidéo. Cela vous permet de zoomer ou de passer d'une caméra à l'autre pour suivre les mouvements d'une personne qui vous préoccupe, sans que celle-ci ne se rende compte qu'elle est filmée. Outre la prévention des incidents en temps réel, la possibilité de relier les journaux d'accès et les informations sur les utilisateurs à la vidéo enregistrée peut s'avérer essentielle pour identifier les auteurs après coup.

Troisièmement, vous voudrez des intégrations pour soutenir les plans d'urgence. La connexion du système d'accès aux alarmes et aux systèmes de sonorisation peut par exemple s'avérer vitale pour assurer la sécurité des personnes en cas de verrouillage ou d'urgence, lorsque les gens doivent être évacués rapidement d'un bâtiment.

Les intégrations ne concernent pas seulement les pires scénarios. Ils sont également efficaces et pratiques et vous aident à faire une bonne première impression sur les visiteurs. Vous pouvez aussi gérer et transférer tous les appels de l'interphone via une seule et même interface joliment conçue à la réception, ou encore économiser sur les coûts en supprimant complètement la réception, en gérant l'accès simplement via une application et un téléphone mobile („Réception à distance").

L'interconnexion des produits 2N avec différents systèmes vous permet de faire toutes ces choses, et nous nous sommes appliqués à rendre l'intégration incroyablement simple à mettre en place et à gérer.

> Nous allons voir de plus en plus d'intégrations de ce type car ce sont les solutions les plus innovantes et les plus efficaces qui existent. Les partenariats solides nous aident à nous développer en nous permettant de répondre à la demande croissante de solutions d'accès plus intelligentes et plus complètes.
>
> Michal Kratochvíl, PDG de 2N Telekomunikace

DES INTÉGRATIONS INTELLIGENTES ÉTUDE DE CAS

Développement d'un centre de sécurité totalement unifié dans une université américaine de premier plan.

Client	Université de Binghamton, Université de l'État de New York
Espace	Un campus de 930 acres comprenant 120 bâtiments, dont huit communautés résidentielles, sept collèges et écoles, trois bibliothèques, un complexe théâtral et un musée d'art - avec d'autres travaux de construction en préparation.
Nombre d'employés	L'université accueille plus de 18 000 étudiants.
Priorités du projet	Intégrer pleinement la sécurité du campus afin que les répartiteurs et la police du campus puissent gérer les incidents au moment où ils se produisent, et pas seulement réagir après coup.
Solution	La première étape a consisté à installer un système de gestion vidéo (VMS) Genetec Omnicast™. Plus de 1 500 caméras de sécurité Axis ont ensuite été intégrées au système, ainsi que des interphones vidéo IP de 2N, qui sont intégrés à trois modules du centre de sécurité Genetec : Synergis (contrôle d'accès), Sipelia (PBX) et Omnicast (VMS). Les interphones intègrent une caméra supplémentaire avec un angle de vue spécial, le signal étant envoyé directement au VMS. La sécurité de l'université pourra ainsi facilement synchroniser les séquences vidéo horodatées pour vérifier qui entre et sort d'un bâtiment. Cette capacité, combinée aux segments de reconnaissance de plaques d'immatriculation et de voix sur IP de Genetec, permettra d'obtenir un centre de sécurité complètement unifié. Alors que la solution de sécurité continue de se développer, l'université de Binghamton prévoit également de remplacer ses boîtiers d'appel d'urgence situés le long des allées du campus par des interphones vidéo IP de 2N.

DES INTÉGRATIONS INTELLIGENTES
ÉTUDE DE CAS

Une entreprise de logistique spécialisée dans le conditionnement de légumes exotiques à Den Hoorn

Espace	Un immeuble de bureaux intelligent de sept étages
Nombre d'employés	Sept entreprises se partagent le complexe, travaillant sur les différents étages
Priorités du projet	Technologie de pointe, fiabilité des produits et conception de haute qualité
Solution	L'interphone audiovisuel 2N® IP Verso a été choisi pour les portes d'entrée car il offre une modularité unique, un design luxueux et des capacités améliorées. L'interphone est doté d'un écran tactile numérique avec des lecteurs Bluetooth / RFID, permettant d'utiliser les téléphones portables pour l'identification. Les employés de bureau n'ont besoin que de l'application 2N® Mobile Key installée sur leur smartphone. Les unités d'accès 2N® Bluetooth & RFID ont été installées aux portes de chaque bureau, y compris les salles de réunion, les salles de serveurs et le parking. La configuration du système est assurée par 2N® Access Commander, logiciel professionnel de gestion du contrôle d'accès. Grâce à une seule interface, il permet d'administrer et de configurer en masse les autorisations d'accès pour plusieurs entreprises d'un même bâtiment. L'intégration simple au système CUCM (Cisco Unified Communication Manager) permet de connecter les interphones 2N au système de téléphonie IP. Cette connexion assure une communication flexible avec l'ouverture de la porte à distance, y compris la configuration des interphones 2N à l'aide de l'auto-provisioning.

2N TELEKOMUNIKACE a.s., Modřanská 621, 143 01 Praha 4, Česká republika,
+420 261 301 500, sales@2n.cz, www.2n.cz

Version : 1.0 Publié : Février 2021