Livre blanc

Risques de cybersécurité des anciens systèmes de contrôle d'accès

Genetec

Sommaire


1 2 3
4 5 6
7 9

Résumé

Dans de nombreuses entreprises, les systèmes de contrôle d'accès datent de 15 ans ou plus. Les systèmes de contrôle d'accès plus anciens peuvent sembler fonctionner suffisamment bien pour permettre aux employés d'entrer et de sortir, mais ce type de technologie traditionnelle peut être vulnérable aux cybermenaces.

De nouvelles solutions de contrôle d'accès mieux cybersécurisées offrent un chiffrement de bout en bout et une authentification avancée, ainsi que d'autres fonctionnalités permettant de se défendre contre les cyberattaques et les logiciels malveillants. Une approche moderne et unifiée du contrôle d'accès peut renforcer la résilience de votre organisation face aux cybermenaces, tout en offrant bien plus de valeur que le simple verrouillage et déverrouillage des portes.

1

Présentation

Partout dans le monde, des cybercriminels ingénieux recherchent les failles de sécurité pour accéder à des installations, des systèmes de surveillance et des données sensibles qu'ils peuvent ensuite revendre sur le marché noir ou utiliser dans le but d'extorquer une entreprise. Et les victimes paient un lourd tribut ; le coût moyen d'une violation de données est passé de 3,86 millions de dollars (USD) en 2020 à 4,24 millions de dollars (USD) en 2021[1], mais le coût peut parfois se chiffrer en dizaines de millions. En 2021, une entreprise a été invitée à payer une rançon de 70 millions de dollars[2], le montant le plus élevé jamais demandé lors d'une cyberattaque.

Les ordinateurs et les serveurs ne sont pas les seuls appareils vulnérables aux cybermenaces. Tout appareil connecté à Internet ou à votre réseau local peut constituer un point faible en matière de cybersécurité.

Les vulnérabilités des anciens systèmes de contrôle d'accès peuvent introduire des faiblesses de cybersécurité qui mettent votre entreprise en danger. Les cybermenaces émergentes peuvent cibler ces vulnérabilités à tous les niveaux : identifiants, contrôleurs, serveurs ou postes de travail.

Si un pirate informatique pénètre dans votre réseau afin d'accéder à des données sensibles – informations propriétaires ou données privées de clients, par exemple – l'impact d'une faille de cybersécurité dans votre système de contrôle d'accès peut causer des dommages allant bien au-delà de vos portes. Cela peut non seulement avoir un impact sur vos revenus, mais aussi sur votre réputation et celle de vos employés, sur la vie privée de vos clients, etc.

Vous devez protéger ce qui vous protège. C'est pourquoi les entreprises, les gouvernements, les établissements d'enseignement et les organismes de sécurité publique délaissent les solutions propriétaires au profit de solutions de contrôle d'accès sécurisées. Ils recherchent une plateforme de sécurité physique unifiée dans une optique de cybersécurité.

[1] https://www.ibm.com/security/data-breach
[2] https://www.welives`ecurity.com/2021/09/30/eset-threat-report-t22021/

Si un pirate informatique pénètre dans votre réseau afin d'accéder à des données sensibles – informations propriétaires ou données privées de clients, par exemple – l'impact d'une faille de cybersécurité dans votre système de contrôle d'accès peut causer des dommages allant bien au-delà de vos portes.

2

Faiblesses des anciens systèmes de contrôle d'accès en matière de cybersécurité

À l'heure actuelle, la plupart des systèmes de contrôle d'accès sont basés sur le protocole Internet (IP), et connectés à un réseau local via Internet. Les systèmes sur IP sont puissants, mais les anciens systèmes manquent de fonctionnalités de cybersécurité essentielles servant à se défendre contre les cybermenaces en constante évolution.

La robustesse de votre système de contrôle d'accès ne peut dépasser celle de son maillon le plus faible. Les cybercriminels peuvent exploiter les faiblesses des identifiants des systèmes de contrôle d'accès, des contrôleurs, des serveurs ou des postes de travail connectés au réseau. Une fois que quelqu'un a piraté votre réseau, il peut prendre le contrôle d'autres systèmes du bâtiment, consulter ou voler des informations sensibles contenues dans des enregistrements internes, ou lancer des attaques conçues pour mettre hors ligne des systèmes stratégiques.

Voici une sélection de menaces de cybersécurité courantes ciblant les systèmes de contrôle d'accès :

- **Attaques de type « homme du milieu »** : le cybercriminel accède à un réseau pour récupérer des informations échangées entre des appareils, telles que des codes d'ouverture de porte ou des identifiants et mots de passe d'appareils.
- **Skimming et attaque par relais** : le criminel utilise son lecteur pour obtenir et cloner les informations figurant sur le badge de sa victime, sans son consentement.
- **Attaques de contrôleur** : un criminel écrase le micrologiciel du contrôleur pour rendre l'appareil inopérant.

Une fois que quelqu'un a piraté votre réseau, il peut prendre le contrôle d'autres systèmes du bâtiment, consulter ou voler des informations sensibles contenues dans des enregistrements internes, ou lancer des attaques conçues pour mettre hors ligne des systèmes stratégiques.

3

Vulnérabilités des identifiants

Les systèmes de contrôle d'accès s'appuient sur les identifiants des utilisateurs afin de déterminer qui est autorisé ou non à accéder à des zones spécifiques. Ces systèmes ont recours à de nombreux types d'identifiants : codes PIN, applications pour smartphone, empreintes digitales et badges ou cartes.

Les cybercriminels peuvent voler les identifiants des utilisateurs lors d'attaques par skimming. Ils utilisent alors leur propre lecteur non autorisé pour accéder à des informations à l'insu de l'utilisateur. Sinon, en accédant à votre réseau, ils peuvent intercepter les données d'identification envoyées sur celui-ci et les stocker afin s'en servir ultérieurement. Ils peuvent exploiter ces données pour « usurper » ou cloner certains types de cartes-clés ou de porte-clés plus anciens, encore largement utilisés. De nombreux anciens types d'identifiants, tels que les cartes de proximité, peuvent être copiés très facilement à l'aide d'un appareil bon marché disponible sur Internet.

Certains identifiants, couramment utilisés dans les systèmes de contrôle d'accès traditionnels basés sur des cartes de proximité à bande magnétique et 125 kHz, présentent également des vulnérabilités connues. Un grand nombre d'entre elles communiquent via le protocole Weigand, devenu la norme du secteur depuis son invention en 1974. Malheureusement, les pirates ont appris à trafiquer les lecteurs de carte couramment utilisés avec ce type de système afin de récupérer des informations sensibles.

Les communications Wiegand étant unidirectionnelles, en cas de sabotage du lecteur, le contrôleur n'en est pas informé à moins d'être branché à un interrupteur de sabotage. Les données envoyées via un système de type Wiegand sont également non chiffrées. De ce fait, même en ayant recours à des identifiants sécurisés, il devient posible de récupérer des informations sensibles.

Pour atténuer le risque d'attaques de type « homme du milieu », recherchez un système doté d'un protocole bidirectionnel sécurisé entre le lecteur et le contrôleur, tel que OSDP2. Ainsi, si un individu tente de voler des identifiants en altérant le lecteur ou en le remplaçant par un lecteur frauduleux, il ne pourra récupérer aucune information sensible. Le protocole bidirectionnel informera également l'opérateur de la tentative de sabotage du système, afin que votre équipe de sécurité puisse intervenir rapidement et neutraliser la menace.

Cependant, la vulnérabilité la plus courante concernant les identifiants reste l’erreur humaine. Pensez aux codes PIN ou aux badges que l'on partage, aux cartes que l'on perd, aux portes qu'on tient ouvertes pour laisser entrer quelqu'un.

Cependant, la vulnérabilité la plus courante concernant les identifiants reste l’erreur humaine. Le partage de codes PIN ou de porte-clés, la perte de cartes-clés, ou encore le fait de tenir des portes ouvertes sont autant d'événements anodins qui peuvent avoir un impact important sur la sécurité de votre bâtiment.

Opter pour des identifiants sécurisés avancés ou pour la biométrie est la meilleure approche pour minimiser les vulnérabilités des identifiants. Le renforcement de la cyberhygiène peut également contribuer à réduire les risques liés à l’erreur humaine. Assurez-vous que tout le personnel bénéficie d'une formation, de messages et de rappels favorisant une culture de travail qui encourage et consolide une bonne cyberhygiène. Cette exigence doit s’étendre aux partenaires avec lesquels vous travaillez, car une violation de leur côté pourrait également avoir un impact sur votre sécurité. Demandez à tous les éditeurs de logiciels partenaires de vous expliquer en détail les mesures qu’ils prennent pour s’assurer que leur personnel respecte les bonnes pratiques de cyberhygiène. Intégrez la cybersécurité dans les exigences de vos appels d'offre lorsque vous recherchez de nouveaux partenaires logiciels ou fournisseurs d’équipements connectés au réseau.

La gestion des droits d’accès est également sujette aux erreurs si la gestion et le suivi des informations se font manuellement. Choisissez des partenaires de sécurité capables de fournir une solution unifiée pour gérer les droits d’accès en fonction du rôle et du statut des utilisateurs, et non de leur identité. Cela vous permet alors de mettre à niveau, de rétrograder, d’ajouter ou d’annuler automatiquement des droits d’accès pour des groupes de personnes en fonction de l’évolution des besoins. C'est notamment utile en cas de congé maternité, de changement de poste ou de départ de l'entreprise. Lorsque le statut de l’employé change dans la base de données associée, ses droits d’accès changent également : ainsi, vous pouvez éliminer le risque que quelqu’un utilise une ancienne carte-clé pour entrer dans des zones auxquelles il n’a plus accès. Ce système vous permet également de révoquer rapidement l’accès en cas de perte ou de vol de la carte-clé, ou de tout autre identifiant d’une personne.

4

Vulnérabilités des contrôleurs

Les contrôleurs interprètent les identifiants du lecteur et les comparent à une liste blanche synchronisée depuis le serveur de contrôle d'accès. Si les identifiants correspondent, il envoie un signal à la serrure de la porte pour ouvrir ou refuser l'accès.

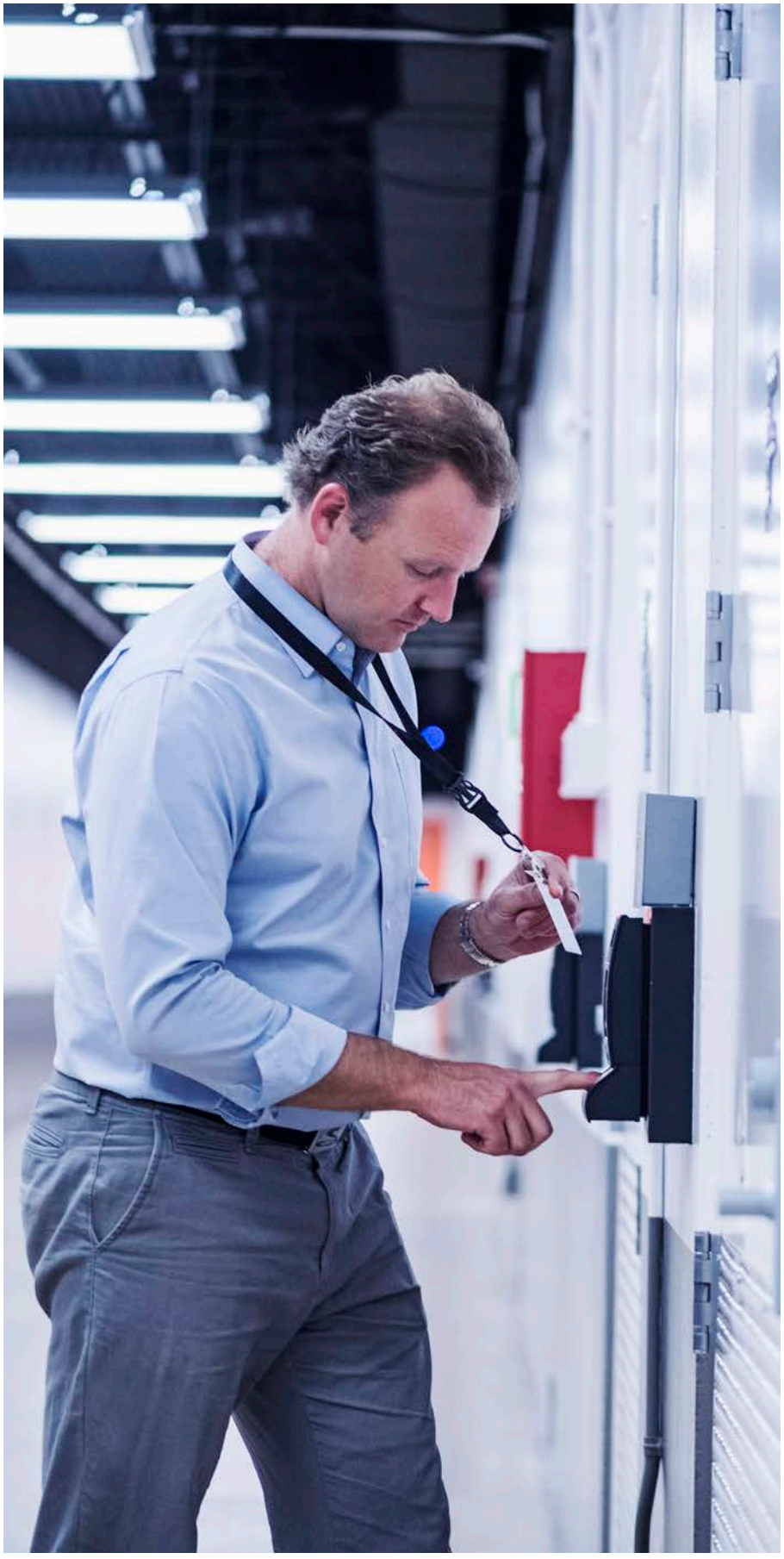
Un cryptage ou un mot de passe faible pourrait permettre à des cybercriminels d'accéder à vos contrôleurs, et donc d'obtenir les clés de votre installation.

Les systèmes de contrôle d'accès modernes utilisent un outil intelligent de gestion des certificats pour authentifier le contrôleur et garantir des communications sécurisées entre le serveur de contrôle d'accès et le contrôleur. L'authentification confirme qu'un contrôleur autorisé est connecté à un serveur légitime dont il reçoit les instructions. Pour sécuriser les communications entre les deux composants, il est recommandé de chiffrer les communications en utilisant le protocole Transport Layer Security (TLS) versions 1.2 et supérieures.

Les contrôleurs nécessitent des mises à jour régulières du micrologiciel pour assurer une sécurité optimale. Il est important de veiller à ce que votre équipe de sécurité vérifie régulièrement les mises à jour ou confie cette tâche à un tiers ou à un fournisseur réputé afin qu'elles soient installées rapidement.

Enfin, une mesure simple mais importante à prendre pour sécuriser vos contrôleurs est de s'assurer que les mots de passe par défaut ont été remplacés par quelque chose d'unique qui ne peut pas être facilement deviné. Une autre bonne pratique consiste à disposer d'un système de gestion des mots de passe qui modifie automatiquement et régulièrement les mots de passe utilisés entre les dispositifs.

Les contrôleurs nécessitent des mises à jour régulières du micrologiciel afin de garantir leur sécurité. Il est important que votre équipe de sécurité vérifie régulièrement les mises à jour afin qu'elles soient installées rapidement.



5

Vulnérabilités des serveurs ou des postes de travail

Les serveurs stockent et gèrent la liste des identifiants approuvés des individus et communiquent avec les contrôleurs pour authentifier les données d'identification. Ces informations doivent être transmises sur un réseau. Si les données ne sont pas chiffrées, les cybercriminels qui accèdent au réseau peuvent voler des identifiants et d'autres données sensibles.

Les données d'identification recueillies par les lecteurs et stockées dans les serveurs doivent être protégées par de puissantes méthodes de chiffrement, d'authentification et d'autorisation. Voici une liste des vulnérabilités les plus courantes que l'on retrouve au niveau des serveurs :

- Utilisateurs non autorisés exploitant des méthodes d'authentification faibles
- Autorisations utilisateur trop généreuses, qui permettent aux utilisateurs d'accéder à des données qui devraient être restreintes, ou d'apporter des modifications non autorisées au système
- La manière dont le serveur gère l'authentification des utilisateurs et veille à ce que seules les personnes autorisées puissent afficher les informations sensibles

Les données d'identification recueillies par les lecteurs et stockées dans les serveurs doivent être protégées par de puissantes méthodes de chiffrement, d'authentification et d'autorisation.

6

Bonnes pratiques de cybersécurité pour les systèmes de contrôle d'accès

La technologie de contrôle d'accès a subi une énorme transformation ces dernières années. Ce marché traditionnellement propriétaire est aujourd'hui plus ouvert. Les clients ne dépendent pas toujours d'un seul fournisseur et, par conséquent, les entreprises développent des produits et services plus innovants. Ces nouvelles solutions, davantage cybersécurisées, offrent un chiffrement de bout en bout et une authentification avancée, ainsi que d'autres fonctionnalités pour se défendre contre les cyberattaques et les logiciels malveillants.

Pour améliorer la cybersécurité de votre réseau

- Mettez à niveau votre système : les systèmes traditionnels n'ont pas été conçus pour faire face aux menaces d'aujourd'hui
- Utilisez des identifiants sécurisés, intelligents et/ou mobiles, et les derniers protocoles de communication afin de sécuriser les données envoyées sur Internet
- Formez vos employés afin de leur enseigner les bonnes pratiques de cybersécurité et rappelez-leur régulièrement de mettre à jour leurs mots de passe
- Faites appel à un système de gestion des identités pour garantir que les utilisateurs ne puissent accéder qu'aux zones et aux données associées à leur rôle et à leur statut actuel
- Mettez en place des réseaux locaux distincts pour les appareils qui stockent ou partagent des informations hautement sensibles, afin qu'elles ne soient pas accessibles à partir de votre réseau habituel
- Choisissez un fournisseur de sécurité capable de démontrer sa conformité avec les cadres de contrôle de sécurité établis

De nombreuses entreprises préfèrent une approche hybride afin de pouvoir tirer parti de la flexibilité et de l'évolutivité des logiciels et des options de stockage de données dans le cloud, tout en conservant certains serveurs gérés en local.

- Assurez-vous que votre système de contrôle d'accès utilise des méthodes de chiffrement de données éprouvées ainsi qu'une authentification en plusieurs étapes
- Collaborez avec un partenaire qui dispose d'une équipe dédiée à la surveillance des cybermenaces, et veillez à ce que les logiciels soient mis à jour fréquemment et que les correctifs soient appliqués, si nécessaire

Vous n'avez pas à choisir entre une solution cloud et une solution sur site. De nombreuses entreprises préfèrent une approche hybride afin de pouvoir tirer parti de la flexibilité et de l'évolutivité des logiciels et des options de stockage de données dans le cloud, tout en conservant certains serveurs gérés en local.

7

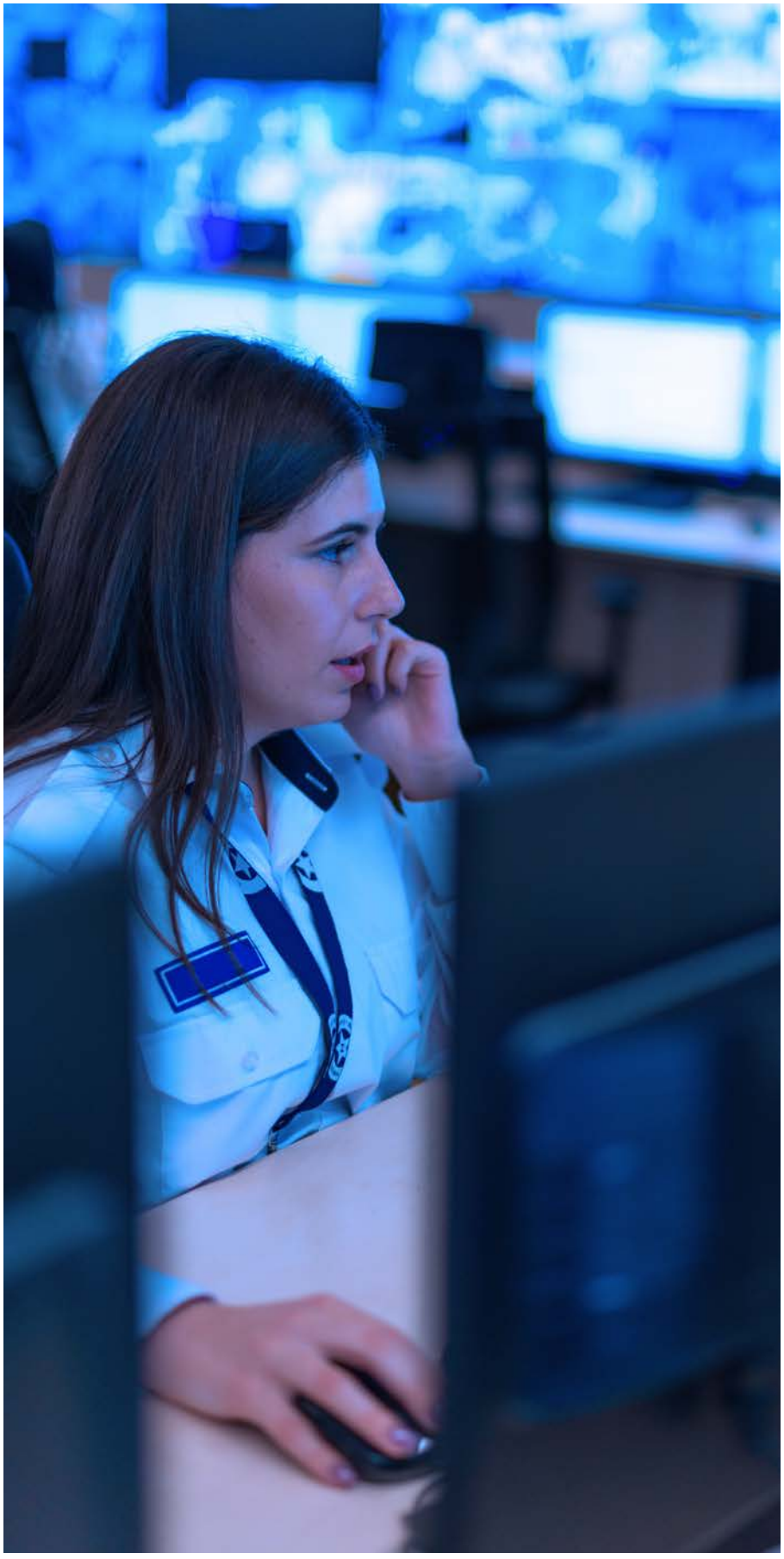
Les systèmes de contrôle d'accès modernes vont plus loin que la cybersécurité

Un système de contrôle d'accès unifié, qui s'appuie sur les dernières normes de cybersécurité pour protéger les communications, les serveurs et les données tels que Genetec Security Center Synergis, peut mieux protéger les actifs et le personnel d'une organisation. Mais il peut également améliorer les opérations et la prise de décision, au-delà du simple verrouillage et déverrouillage des portes. En choisissant un système de contrôle d'accès sur IP à architecture ouverte, les organisations ont la possibilité de passer à tout moment à la dernière technologie prise en charge, d'évoluer à leur propre rythme et de travailler dans les limites de leur budget.

Le système de contrôle d'accès Synergis[MC] répond aux dernières normes de cybersécurité pour sécuriser les communications, serveurs et données à tous les niveaux de votre architecture. Grâce à la protection avancée s'étendant du badge d'accès au logiciel, vous pouvez gérer l'accès à vos locaux en toute confiance en sachant qu'ils resteront à l'abri des regards indiscrets.

Genetec[MC] Security Center est une plateforme à architecture ouverte qui unifie la vidéosurveillance sur IP, le contrôle d'accès, la reconnaissance automatique des plaques d'immatriculation (RAPI), les communications et les analyses. Genetec développe également des solutions et des services dans le cloud, conçus pour améliorer la sécurité et apporter plus d'intelligence opérationnelle aux organismes gouvernementaux, aux entreprises, au transport et aux communautés dans lesquelles nous vivons.

Security Center est une plateforme à architecture ouverte qui unifie la vidéosurveillance sur IP, le contrôle d'accès, la reconnaissance automatique des plaques d'immatriculation (RAPI), les communications et les analyses.



8

Les systèmes de contrôle d'accès modernes offrent des avantages qui vont au-delà du verrouillage et du déverrouillage des portes

Les systèmes de contrôle d'accès plus récents et mieux cybersécurisés comme Synergis peuvent faire bien plus que simplement verrouiller et déverrouiller les portes selon des horaires précis. Ils peuvent utiliser la richesse des données recueillies par les systèmes de contrôle d'accès et les combiner avec des données provenant d'autres sources pour mettre en lumière de nouvelles informations utiles qui peuvent vous aider à améliorer les opérations quotidiennes ainsi que la sécurité. Par conséquent, le retour sur investissement de ces systèmes est bien plus important.

Synergis va au-delà des portes pour libérer de nouvelles informations qui contribuent à améliorer vos opérations quotidiennes. En tant que système véritablement ouvert, il se connecte à une liste toujours plus grande de dispositifs de contrôle d'accès tiers. Il agrège et affiche les données dans un format dynamique pour vous permettre de mieux gérer vos opérations.

Par exemple, pendant la pandémie de COVID, les clients de Synergis ont pu installer rapidement et facilement de nouveaux lecteurs biométriques qui ont permis de réduire le besoin de contact physique, afin de limiter la propagation des germes. Ils ont également pu utiliser les données du système de contrôle d'accès pour prendre en charge la recherche de cas contacts, ainsi que pour gérer les niveaux d'occupation et les exigences de distanciation physique mis en place par les autorités de santé publique.

De la gestion de l'occupation en temps réel à la surveillance des infrastructures distantes, Synergis peut vous aider à protéger vos opérations, et pas seulement vos portes.

Les systèmes de contrôle d'accès récupèrent un très grand nombre de données, mais elles sont difficiles à collecter et à interpréter avec les systèmes plus anciens. Les tableaux de bord de Synergis offrent une vue unifiée de tous vos systèmes de sécurité et données de capteurs, afin que vous puissiez repérer les tendances et prendre des décisions opérationnelles proactives plutôt que réactives.

De la gestion de l'occupation en temps réel à la surveillance des infrastructures distantes, Synergis peut vous aider à protéger vos opérations, et pas seulement vos portes. Vous pouvez vous adapter à l'évolution des besoins en ajustant facilement les paramètres du logiciel, ou en ajoutant/modernisant les équipements, sans avoir à modifier l'ensemble du système. Vous pouvez utiliser les données de contrôle d'accès pour activer l'automatisation du bâtiment, pour éteindre les lumières, par exemple, ou régler le chauffage et la climatisation en l'absence de personnes dans les locaux. Vous pouvez également mieux comprendre les zones des bâtiments les plus utilisées, afin de savoir si vous avez besoin d'autant d'espace.

9

Conclusion

Un système de contrôle d'accès unifié, qui s'appuie sur les dernières normes de cybersécurité pour protéger les communications, les serveurs et les données tels que Security Center Synergis, peut mieux protéger les actifs et le personnel d'une organisation. Mais il peut également améliorer les opérations commerciales et la prise de décision, au-delà du simple verrouillage et déverrouillage des portes. En choisissant un système de contrôle d'accès sur IP à architecture ouverte, les organisations ont la possibilité de passer à tout moment à la dernière technologie prise en charge, d'évoluer à leur propre rythme et de travailler dans les limites de leur budget.

Vous voulez aller plus loin ?

Téléchargez notre liste des 7 éléments à prendre en compte lors de la migration vers un système de contrôle d'accès sur IP.

Obtenir la liste

Genetec Inc. est une société de technologie innovante, qui dispose d'une large gamme de solutions englobant la sécurité, l'intelligence et les opérations. Son produit phare, Genetec[MC] Security Center, est une plateforme de sécurité physique sur IP qui unifie la vidéosurveillance, le contrôle d'accès, la reconnaissance automatique des plaques d'immatriculation (RAPI), les communications et l'analyse. Genetec développe également des solutions et des services dans le cloud, conçus pour améliorer la sécurité et apporter plus d'intelligence opérationnelle aux organismes gouvernementaux, aux entreprises, au transport et aux communautés dans lesquelles nous vivons. Fondée en 1997 et basée à Montréal au Canada, Genetec répond aux besoins de ses clients internationaux par l'intermédiaire d'un vaste réseau de revendeurs, d'intégrateurs, de partenaires certifiés et de consultants répartis dans plus de 159 pays.

Vidéosurveillance : bénéficiez d'une meilleure appréciation de la situation et renforcez la sécurité de votre ville grâce au partage de caméras entre agences et entreprises, qui permet de disposer d'une vision opérationnelle commune et de réduire le délai d'intervention en cas d'incident.

Contrôle d'accès : renforcez la sécurité de votre entreprise, réagissez efficacement aux menaces et prenez des décisions plus pertinentes et plus rapides grâce à une plateforme sur IP unifiée, que ce soit pour déployer un nouveau système de contrôle d'accès ou mettre à jour une installation existante.

Reconnaissance automatique des plaques d'immatriculation : automatisez la détection des véhicules présentant un intérêt particulier, appliquez plus efficacement les règles de stationnement et accélérez les enquêtes de sécurité publique grâce à la fonctionnalité de partage des données de plaques d'immatriculation avec les agences et entreprises partenaires de votre choix, tout en respectant la propriété et la confidentialité de ces données.

Assistance aux décisions opérationnelles : améliorez la gestion des incidents et la prise de décisions grâce à des flux opérationnels avancés, qui guident les opérateurs tout au long de procédures basées sur des politiques, depuis les alertes situationnelles jusqu'à l'exportation d'une compilation détaillée du dossier.

Gestion des dossiers d'enquête : simplifiez votre gestion de dossiers et accélérez vos enquêtes grâce à une plateforme offrant la possibilité de centraliser les preuves numériques et de collaborer en toute sécurité avec les enquêteurs, les agences externes et le public.

Services Cloud : étendez les capacités de votre système de sécurité sur site et réduisez vos coûts informatiques grâce à des services Cloud à la demande hautement évolutifs, qui permettent à votre ville de faire plus facilement face à l'évolution rapide des exigences de sécurité, tout en gagnant en efficacité.

Genetec Inc.
genetec.com/emplacements
info@genetec.com
@genetec

MISE À JOUR : 15-NOV-2022