7 MEILLEURES PRATIQUES EN MATIÈRE DE CYBERSÉCURITÉ

CONSERVER LES LOGICIELS À JOUR

UTILISER DES MOTS DE PASSE FORTS

DES COMPTES DIFFÉRENTS POUR DES RÔLES DIFFÉRENTS

LIMITER L'EXPOSITION À INTERNET

SÉCURISER VOTRE RÉSEAU

CHOISIR LE BON FOURNISSEUR DE SERVICES DE TÉLÉGESTION

SÉCURISER L'ÉCOSYSTÈME IOT

CYBER SECURITY by 2N

2N

An Axis company

CONSERVER LES LOGICIELS À JOUR

Il est inévitable d‘utiliser des appareils dotés de versions de logiciels à jour afin de réduire les risques éventuels de cybersécurité. Lorsqu‘un fabricant découvre un bug logiciel potentiel, il le corrige dans la version suivante du logiciel. **L‘installation de mises à jour logicielles vous permettra d‘utiliser les correctifs de sécurité pour toutes les vulnérabilités récemment découvertes.**

2N
An Axis company

UTILISER DES MOTS DE PASSE FORTS

Le moins que vous puissiez faire en tant qu'utilisateur, c'est de créer un **mot de passe complexe qui ne sera pas facile à pirater.** Le mot de passe idéal devra comporter au moins six caractères. Il doit combiner des chiffres, des lettres et des symboles. De toute évidence, utiliser des mots de passe faciles à deviner comme la date de votre anniversaire ou le nom de votre ville natale n'est pas recommandé. Si vous parvenez à créer un mot de passe fort, très bien. Mais **évitez de partager vos identifiants** avec d'autres utilisateurs. Même si vous suivez ces règles, il est bon de **changer votre mot de passe** de temps en temps.

2N
An Axis company

DES COMPTES DIFFÉRENTS POUR DES RÔLES DIFFÉRENTS

Il est important d'avoir **plusieurs comptes avec des privilèges différents.** Un utilisateur ne pourra effectuer que les modifications liées à ses tâches professionnelles spécifiques. Encore une fois, même pour ce type de compte, vous ne devrez pas partager votre mot de passe avec quelqu'un d'autre. De cette façon, vous réduisez au minimum les risques de diffusion de vos informations d'identification sécurisées dans toute l'entreprise.

2N
An Axis company

LIMITER L‘EXPOSITION À INTERNET

Pour éviter les logiciels malveillants, utilisez des **pare-feu basés sur des routeurs** capables de rejeter le trafic suspect avant qu‘il n‘arrive sur le réseau. Bien entendu, il est impensable de se déconnecter complètement d‘Internet. Il est cependant important d‘être prudent et **de protéger le réseau avec un mot de passe fort.** Les pirates scannent constamment internet à la recherche de machines qui sont exposées. Si vous voulez savoir ce qui est ouvert au réseau à partir des appareils que vous utilisez, vous rendez-vous sur www.shodan.io et vérifiez-le par vous-même. Plus vous retirez de dispositifs avec une exposition directe à l‘internet, plus vous réduisez les risques. N‘oubliez pas non plus de toujours activer uniquement les fonctions nécessaires du produit.

2N
An Axis company

SÉCURISER VOTRE RÉSEAU

a) Créer un réseau indépendant, dédié uniquement aux appareils contenant des informations sensibles. Rendez physiquement impossible l‘accès au réseau en disposant de commutateurs séparés.

b) Utilisez un **réseau local virtuel (VLAN).** Le VLAN contient des réseaux isolés au sein du centre de données et chaque réseau est un domaine de diffusion distinct.

c) Il est également très utile de sécuriser le réseau grâce au **protocole IEEE 802.1X.** Il empêchera les appareils non autorisés d‘accéder au réseau local.

d) Vérifiez que les fabricants des appareils ou des logiciels que vous utilisez mettent en œuvre des **protocoles tels que HTTPS, TLS, SIPS ou SRTP,** activés par défaut. Cela permet également d‘éviter les cyber-attaques de type „Man in the middle“.

2N
An Axis company

CHOISIR LE BON FOURNISSEUR DE SERVICES DE TÉLÉGESTION

Il est très utile de **gérer tous les sites d‘installation à partir d‘un seul compte.** Peu importe où se trouvent vos sites d‘installation, vous pourrez y accéder à distance depuis le confort de votre bureau. Cela peut sembler risqué, compte tenu de tous les dangers d‘exposition des appareils à l‘Internet décrits ci-dessus. Recherchez un fournisseur de gestion à distance, dont le service est basé sur un service de cloud sécurisé. Dans ce cas, **vous n‘aurez plus à utiliser des pare-feu basés sur des routeurs ou à des tunnels.** Le service basé sur le cloud **établira lui-même une communication cryptée.**

2N
An Axis company

SÉCURISER L'ÉCOSYSTÈME IOT

Créer un **réseau séparé pour les appareils IoT,** choisir un **mot de passe de routeur fort** pour protéger le réseau, **ne jamais installer de nouveaux appareils électroniques sans en vérifier le fabricant,** ne pas autoriser de fonctionnalités inutiles sur les appareils et **mettre à jour régulièrement les firmwares et les logiciels.**

2N
An Axis company