MAGAZINE CYBERSÉCURITÉ AXIS COMMUNICATIONS

Partenaires en protection

ÉCLAIRAGES ET INSPIRATION DU MARCHÉ DE LA CYBERSÉCURITÉ

Par ici >

AXIS COMMUNICATIONS

INTRODUCTION

Un cadre de protection robuste

Comme vous le savez peut-être, il n'existe pas de solution unique aux problématiques de cybersécurité, ni de cybersécurité absolue intégrée à un produit. La cybersécurité est plutôt une question de partenariats de confiance, où tous les acteurs concernés, du sous-traitant au fabricant, des installateurs-intégrateurs aux utilisateurs finaux, ont un rôle important à jouer. C'est aussi une question de processus continu plutôt que d'accomplissement ponctuel.

Pour votre mission de partenaire responsable de cybersécurité, nous avons réuni cette série d'articles, de conseils et de sources d'inspiration. Nous espérons que ces informations vous guideront dans vos efforts de maintien de la cybersécurité et qu'elles vous seront profitables.

Mais avant de tourner la page, nous tenons à vous présenter rapidement le cadre de gestion du risque du NIST (National Institute of Standards and Technology). La sécurité porte fondamentalement sur la gestion du risque. Un bon point de départ consiste donc à évaluer les risques pour votre activité en termes probabilistes, puis leur potentiel destructeur selon un cadre de gestion du risque, dont il existe de nombreuses variantes.

Axis a choisi d'adopter une approche cybersécurité régie par le cadre du NIST. Utilisées dans le monde entier, les directives du NIST conviennent non seulement aux grandes organisations, mais également aux petites et moyennes entreprises. Même si votre organisation utilise un autre cadre de référence, il est probablement compatible avec celui du NIST.

Le cadre du NIST est articulé autour de cinq piliers : identification, protection, détection, réponse et récupération. Pour en savoir plus sur chaque pilier, notre rôle en tant que partenaire cybersécurité et vos propres rôles, consultez notre site web à l'adresse www.axis.com/cybersecurity.

Nous espérons que vous apprécierez le magazine !

SOMMAIRE

Cybersécurité : leçons à tirer de la sécurité physique

La plupart d'entre nous se représentent facilement les risques de sécurité physique. Une porte non verrouillée accroît le risque d'accès d'intrus. La visibilité de biens précieux augmente le risque de vol. Les erreurs et les accidents peuvent porter préjudice aux personnes, aux biens et aux objets.

La sécurité physique et la cybersécurité sont généralement abordées de la même manière. Que vous soyez responsable de la sécurité physique ou de la cybersécurité de votre entreprise, vous devez appliquer les mêmes principes :

- Identifier et classifier vos actifs et vos ressources (quoi protéger)
- Identifier les menaces plausibles (protéger de qui/quoi)
- Identifier les vulnérabilités plausibles que peuvent exploiter les menaces (probabilité)
- Identifier les coûts attendus en cas d'événement préjudiciable (conséquences)

Le risque est souvent défini comme la probabilité d'une menace multipliée par le résultat négatif qu'elle engendre. Une fois le risque déterminé, vous devez savoir quelles mesures vous êtes prêt à prendre pour éviter les effets négatifs.

Inventoriez vos actifs et ressources

Dans le domaine des systèmes vidéo, la ressource évidente à protéger est le flux vidéo des caméras. L'actif correspond aux enregistrements vidéo dans le système de gestion vidéo (VMS). L'accès est habituellement contrôlé en fonction de privilèges utilisateurs. Les autres actifs à considérer sont les comptes et les mots de passe des utilisateurs, les configurations, le système d'exploitation, les firmwares et les logiciels, ainsi que les dispositifs connectés au réseau.

En savoir plus >

Panorama des menaces potentielles

La première étape de votre programme de protection consiste à connaître les cybermenaces qui vous concernent. La confidentialité, l'intégrité et la disponibilité sont des éléments clés d'un système informatique. Un événement préjudiciable à l'un de ces éléments est un incident de sécurité. Dans les pages suivantes, nous faisons le point sur les cybermenaces les plus courantes et les vulnérabilités qu'elles exploitent.

Les trois cybermenaces les plus courantes en vidéosurveillance

1. Naïveté et erreur humaine
2. Détournement délibéré du système
3. Altération physique et sabotage

En savoir plus >

1 Naïveté et erreur humaine

Quelle que soit la qualité de la technologie ajoutée pour protéger votre réseau, si un attaquant peut conduire une seule personne à cliquer sur un lien douteux dans un e-mail, l'intrusion est actée. Pour les cybercriminels, cette méthode d'attaque est donc privilégiée, car elle est la plus facile. Plusieurs types d'erreur humaine peuvent ouvrir la voie à une cyberattaque :

- **Ingénierie sociale :** lorsqu'un utilisateur est forcé, par manipulation psychologique, à commettre des erreurs de sécurité ou à transmettre des informations sensibles. Le phishing et le « scareware » sont des exemples d'ingénierie sociale.
- **Mauvais usage des mots de passe :** notamment la non-application de mots de passe complexes ou l'absence de protection et/ou de mise à jour appropriée des mots de passe.
- **Gestion négligente de composants critiques :** perte ou mauvais placement d'un objet permettant d'accéder au système. Carte d'accès, téléphones, ordinateurs portables et documents en sont des exemples.
- **Mauvaise gestion du système :** non-installation des mises à jour système et des correctifs de sécurité.
- **Améliorations infructueuses :** la résolution d'un problème par quelqu'un se traduit par une baisse des performances du système.

Vulnérabilités et erreur humaine

Certaines des vulnérabilités les plus communes dues à une erreur humaine découlent d'un manque de sensibilisation à la cybersécurité et de l'absence de politiques et de procédures de long terme de gestion du risque. Pour atténuer le risque d'erreur humaine, l'ensemble du personnel d'une organisation doit être formé aux bonnes pratiques de cybersécurité. Vous devez également restreindre l'accès à la vidéo et les autorisations critiques à un nombre limité de personnes dans votre logiciel VMS.

En savoir plus >

Détournement délibéré du système

2

Une autre cybermenace trop répandue est le détournement délibéré de votre système vidéo par des utilisateurs disposant d'un accès légitime. Parmi les types de détournement intentionnel :

- Accès non autorisé et manipulation des services et ressources du système
- Vol de données
- Dommages délibérés au système

Vulnérabilités et détournements intentionnels

La mise en œuvre de politiques et de procédures de long terme de gestion du risque est essentielle pour faciliter la gestion des vulnérabilités et atténuer la menace d'un mauvais usage délibéré du système. Une approbation formalisée des utilisateurs disposant d'autorisations d'accès à des données sensibles doit être en place, tout comme la limitation de leur nombre. Les dispositifs doivent être associés à des comptes distincts pour l'administration et pour les clients d'exploitation au quotidien (c'est-à-dire les logiciels VMS), et ils doivent utiliser un compte provisoire pour la maintenance et le dépannage. Si ces trois comptes étaient identiques, le mot de passe pourrait se propager facilement dans l'entreprise et ouvrir la voie à une mauvaise utilisation délibérée ou accidentelle.

En savoir plus >

3

Altération physique ou sabotage

La protection physique des systèmes informatiques est capitale du point de vue de la cybersécurité :

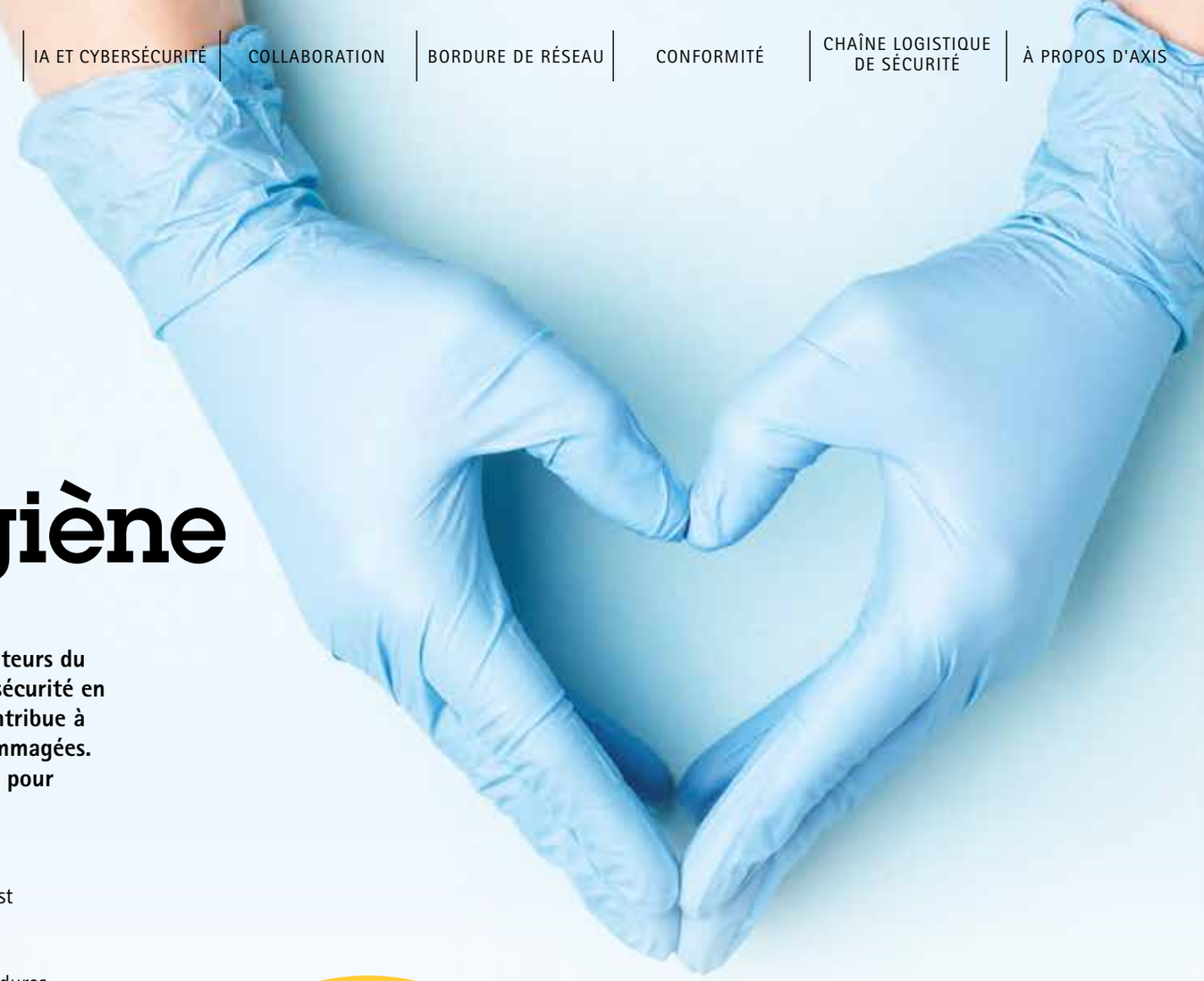
- Les équipements physiquement accessibles peuvent être trafiqués.
- Les équipements physiquement accessibles peuvent être volés.
- Les câbles exposés peuvent être débranchés, réacheminés ou coupés.

Vulnérabilités et menaces physiques

Les caméras elles-mêmes ne courent pas seulement le risque de sabotage : elles peuvent aussi exposer les câbles réseau, qui peuvent servir de moyen d'introduction sur le réseau. D'autres vulnérabilités courantes sources de cybermenaces concernent les équipements réseau, par exemple les serveurs et les switches situés dans des locaux non verrouillés, les caméras facilement accessibles sans boîtier de protection ou les câbles non protégés par des murs ou des conduits.

Les conséquences sont ailleurs

Les systèmes vidéo ne traitent pas de transactions financières ou de données clients. Une attaque sur un système vidéo peut donc être difficile à monétiser et manquer d'intérêt pour les organisations cybercriminelles. Cependant, un système compromis peut devenir une menace pour les autres systèmes. L'estimation des coûts est donc délicate. Malheureusement, les entreprises les découvrent souvent à leurs dépens. La protection est comme la qualité : il faut en payer le prix. Un achat économique peut se révéler beaucoup plus coûteux sur le long terme.



Maintien d'une bonne cyber-hygiène

La cyber-hygiène se rapporte aux pratiques et aux étapes que suivent les utilisateurs du système et des dispositifs pour maintenir l'intégrité du système et renforcer la sécurité en ligne. Souvent intégrée à des procédures internes globales, la cyber-hygiène contribue à protéger les identités et autres informations susceptibles d'être volées ou endommagées. Comme l'hygiène corporelle, la cyber-hygiène doit être pratiquée régulièrement pour compenser la dégradation naturelle et les menaces courantes.

Avantages d'une bonne cyber-hygiène

La mise en place de procédures régulières de cyber-hygiène pour vos dispositifs et logiciels est profitable à la maintenance et à la sécurité.

- La maintenance veille à la performance optimale des dispositifs et logiciels. Les fichiers fragmentés et les programmes obsolètes augmentent le risque de vulnérabilités. Les procédures de maintenance permettent d'identifier rapidement ces problèmes et peuvent éviter les problèmes graves. Un système soumis à une maintenance rigoureuse est généralement moins vulnérable aux risques de cybersécurité.
- Entre les hackers et les usurpateurs d'identité, les virus et les malwares intelligents, les entreprises représentent une cible permanente. En anticipant les menaces et en appliquant de bonnes pratiques de cyber-hygiène, il est possible de détecter les risques très tôt, de mieux s'y préparer ou d'éviter qu'ils se concrétisent.

Comme l'hygiène corporelle, la cyber-hygiène doit être pratiquée régulièrement

En savoir plus >

Mots de passe complexes et uniques

Cela peut sembler évident, mais la méthode d'accès non autorisé la plus courante des cybercriminels à votre système est due à l'utilisation de mots de passe faibles. La plupart des dispositifs IP sont livrés avec des mots de passe et des paramètres par défaut. Il est donc indispensable de les changer immédiatement en suivant la politique informatique ou générale de l'entreprise. Les entreprises doivent mettre en place un système efficace de gestion de mots de passe, qui doivent être complexes et uniques (minimum 8 caractères), changés régulièrement et jamais communiqués d'un site à l'autre. Les politiques de mots de passe ne sont pas du ressort des systèmes informatiques. Les entreprises doivent s'assurer que leur personnel est formé et sensibilisé aux bonnes pratiques internes en matière de mots de passe. Il est également conseillé d'utiliser des certificats pour crypter les mots de passe et noms d'utilisateur.

Un mot de passe composé d'un seul nom, commun ou propre, ou d'une série de chiffres est piratable en quelques secondes, quelle que soit sa longueur.

Déploiement et installation de dispositifs selon la politique informatique ou de sécurité réseau

Lors du déploiement des dispositifs, vous devez systématiquement désactiver les services inutilisés. Pour les cybercriminels, c'est en effet un moyen d'attaque simple pour installer des applications malveillantes. La désactivation des services inutilisés et l'installation d'applications fiables seulement réduisent le risque d'exploitation d'une vulnérabilité système par un attaquant. Par ailleurs, l'installation physique des dispositifs doit être conforme et ne jamais exposer les prises réseau et fentes pour carte SD au public.

En savoir plus >

Rôles et responsabilités clairs

Il convient d'établir des règles et des procédures claires pour que les utilisateurs disposent des droits d'accès correspondant à leur domaine de responsabilité. Les entreprises doivent respecter le principe des « comptes de moindres privilèges », où les utilisateurs ont seulement accès aux ressources relevant de leur mission. L'utilisation des comptes par défaut est à proscrire. Si vous utilisez des comptes temporaires à des fins de maintenance, veillez à les éliminer une fois l'intervention terminée.

Ne vous fiez jamais aux paramètres par défaut d'un dispositif, notamment le mot de passe. Les ID et mots de passe par défaut des comptes d'administrateur sont facilement identifiables pour les dispositifs courants par une simple recherche sur Google, un jeu d'enfant pour les hackers. Veillez à activer et à configurer les services de protection du dispositif et à n'utiliser les paramètres par défaut qu'à des fins de démonstration.

61 %
des salariés mélangent activités personnelles et professionnelles sur leurs appareils

80 %
des salariés admettent utiliser des applications SaaS (Software-as-a-Service) non approuvées au travail

75 %
des intrusions réseau exploitaient des identifiants faibles ou volés

En savoir plus >

Firmwares disponibles les plus récents

Vos dispositifs exécutent-ils les derniers firmwares disponibles ? Les défauts et les bugs dans les systèmes et les dispositifs placent les entreprises à la merci des attaques. Ils peuvent permettre aux hackers de voler des clés privées de serveur ou des mots de passe utilisateur. Un plan formalisé de gestion des mises à jour de firmwares/logiciels doit être en place pour s'assurer que les dispositifs réseau exécutent toujours les firmwares et correctifs de sécurité les plus récents.

Analyse de risque

Combien votre entreprise doit-elle dépenser à la protection de ses actifs ? En analysant les menaces potentielles internes et externes, ainsi que les conséquences si vos actifs majeurs sont endommagés ou perdus, vous pouvez prioriser vos efforts pour les protéger. Il existe également des cadres de gestion du cyber-risque, comme celui du NIST (National Institute of Standards and Technology) , qui peut aider à la mise en place de procédures et de consignes pour gérer les risques.

Le nombre d'intrusions signalées a fortement augmenté en 2019, avec plus de

8,5 milliards d'enregistrements

exposés, soit trois fois plus qu'en 2018*

*IBM X-Force Threat Intelligence Index 2020 : éclairages sur la protection des systèmes et les menaces potentielles

En savoir plus >

Chaîne logistique : quel est son degré de sécurité ?

Par une collaboration étroite avec l'ensemble de votre chaîne logistique, vous pouvez mieux cerner les menaces possibles qu'encourent votre réseau et les dispositifs connectés. Aujourd'hui, de nombreux fabricants informatiques proposent des bonnes pratiques formalisées ou des guides pour durcir la sécurité de leurs dispositifs sur votre réseau, ainsi que des documents sur la sécurité de la chaîne logistique. Si cette documentation n'est pas disponible, il convient d'aborder le sujet avec votre fabricant ou de trouver d'autres documents utilisateur. Les dispositifs doivent respecter votre politique informatique, aussi bien au niveau individuel que pour le système dans son ensemble.

Utilisez toujours des connexions chiffrées

Quel que soit votre secteur d'activité, toutes les données doivent faire l'objet d'un chiffrement sécurisé. De plus, tous les réseaux, même locaux ou « internes », doivent utiliser des connexions chiffrées. Des protocoles d'authentification s'assurent que les informations sont chiffrées avant leur transmission sur le réseau, réduisant ainsi le risque d'attaques dans lesquelles du code malveillant « écoute » les transmissions non chiffrées.

Protocoles sécurisés

- L'authentification HTTP Digest (accès) est l'une des méthodes convenues que peut utiliser un serveur Web pour confirmer les identifiants et l'identité d'un utilisateur, comme le mot de passe et le nom d'utilisateur
- HTTPS (HyperText Transfer Protocol Secure) est le protocole de chiffrement de données le plus courant. HTTPS est identique à HTTP, sauf que les données transmises font l'objet d'un chiffrement supplémentaire SSL (Secure Sockets Layer) ou TLS (Transport Layer Security)
- Le protocole SRTP (Secure Real-Time Transport Protocol) chiffre le flux vidéo pour renforcer la protection de la vidéo elle-même. Si vous utilisez un logiciel VMS ou des cartes SD pour le stockage local de la vidéo, un chiffrement s'impose également.

En savoir plus >

Sécurisation du périmètre du réseau

Savez-vous comment fonctionnent vos pare-feu et vos filtres ? Par la sécurisation de votre réseau à partir du backbone, vous pouvez mieux soutenir d'autres initiatives d'application de bonnes pratiques de sécurité. L'utilisation de la segmentation réseau, par exemple sous forme de VLAN (Virtual Local Area Network), sur les dispositifs de sécurité peut réduire le risque d'interception d'informations sensibles et d'attaque ciblée sur des serveurs et équipements réseau. En complément, des listes de contrôle d'accès (ACL) peuvent contribuer à limiter les transmissions malveillantes sur le réseau. Avant d'investir dans de nouveaux équipements, demandez à votre fournisseur une liste des ports réseau pour vérifier que la solution sera fonctionnelle dans l'ensemble du réseau.

La maintenance régulière d'un système est cruciale pour son intégrité générale

Maintenance de vos systèmes et processus

La maintenance régulière d'un système est cruciale pour son intégrité générale. Les dispositifs et les journaux système doivent être examinés régulièrement pour détecter toute tentative d'accès non autorisé. Aujourd'hui, le monde technologique progresse à grande vitesse : mises à jour, fonctionnalités et bonnes pratiques sont publiées en permanence. C'est pourquoi vous devez documenter les procédures de maintenance pour que tout le monde comprenne les processus.

Un logiciel de gestion des dispositifs comme AXIS Device Manager peut aider les entreprises à constituer rapidement un inventaire complet en temps réel de tous les dispositifs et logiciels connectés au réseau. Ce logiciel analyse l'ensemble du réseau et capture toutes les informations clés, y compris numéro de modèle, adresses IP et MAC, version de firmware et statut des certificats.

Le rôle critique d'une gestion efficace du cycle de vie

Un réseau est seulement aussi sûr que les dispositifs qui le composent. De plus, alors que les entreprises adoptent des pratiques de protection multiniveaux pour sécuriser leur réseau, elles doivent également disposer de moyens efficaces pour gérer le cycle de vie de leurs ressources physiques. En revanche, elles négligent souvent de mettre à jour les logiciels, même lorsque de nouveaux firmwares sont disponibles. Généralement, c'est parce qu'elles n'ont pas une vue complète de toutes les technologies de leur réseau.

Un dispositif, deux durées de vie

Le cycle de vie associé aux dispositifs pilotés par logiciel se divise en deux types.

1. Durée de vie fonctionnelle du dispositif, ou durée réaliste pendant laquelle un dispositif peut fonctionner. Par exemple, une caméra réseau possède une durée de vie fonctionnelle de 10 à 15 ans.

2. Cycle de vie économique du dispositif : combien de temps avant qu'il commence à coûter plus cher en maintenance que l'adoption de nouvelles technologies plus performantes ? Alors qu'une caméra IP peut rester opérationnelle pendant 15 ans, sa durée de vie réelle sera plus courte en raison de l'évolution rapide de l'environnement de cybersécurité.

D'après le commissariat à l'information du Royaume-Uni (ICO)

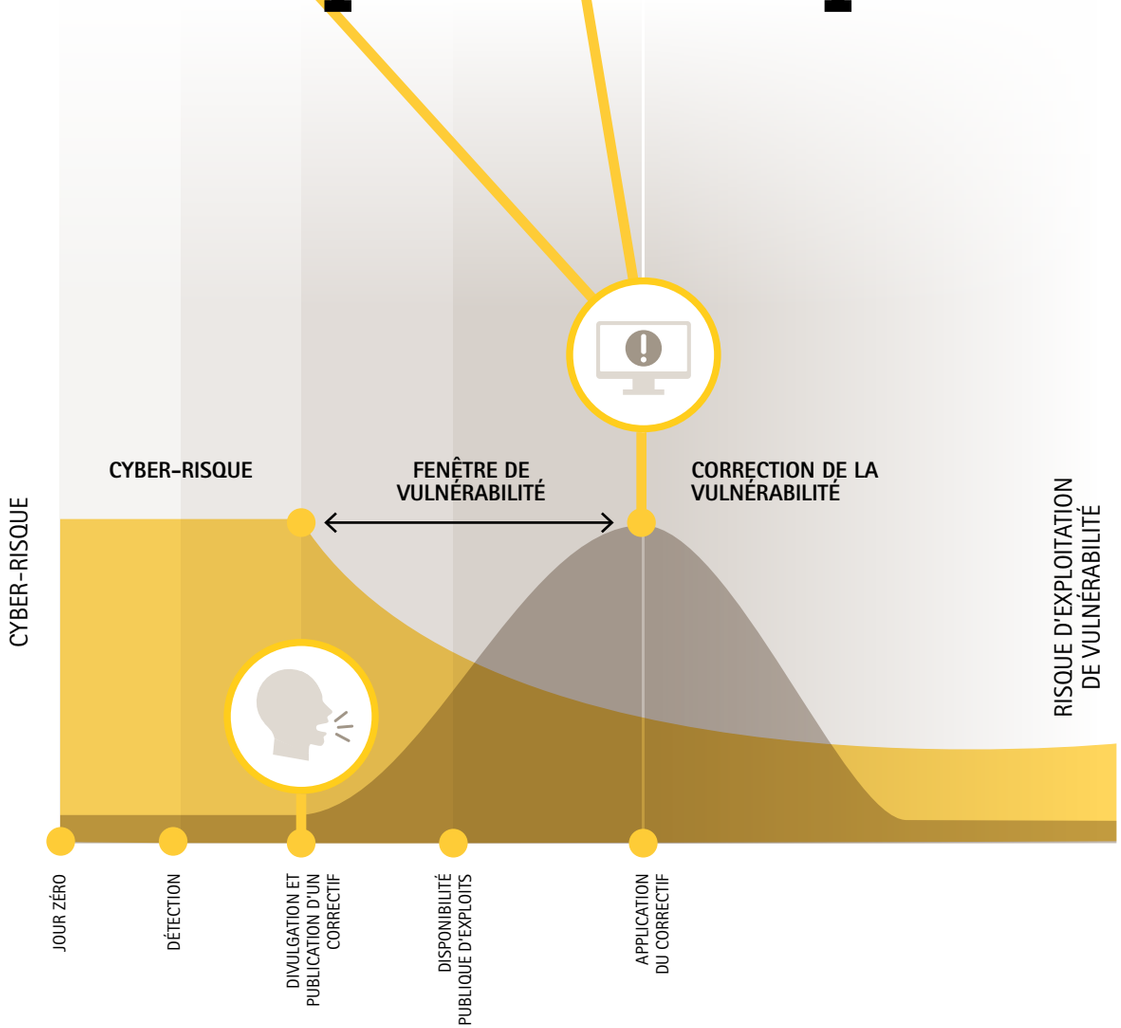
« 60 % des intrusions concernaient des vulnérabilités pour lesquels un correctif était disponible, mais qui n'a pas été appliqué. »

Gérez vos ressources de manière proactive

La gestion du cycle de vie se rapporte à la gestion efficace du cycle de vie fonctionnel et économique des ressources physiques. Les entreprises ont besoin d'une vue d'ensemble claire de toutes les technologies déployées pour pouvoir garder un œil sur leurs réseaux et leurs données critiques, mais aussi vérifier qu'ils sont protégés des menaces et des vulnérabilités.

En savoir plus >

Croiser les doigts n'est pas une option



Tous les dispositifs technologiques, des caméras réseau aux logiciels VMS, doivent être mis à jour et corrigés régulièrement pour éviter l'exploitation des vulnérabilités connues et le contournement des moyens de protection existants.

Les mises à jour et les correctifs restent le meilleur moyen de renforcer la cybersécurité. Cependant, ils ne sont pas toujours disponibles pour les anciennes technologies, notamment celles que le fabricant ne prend plus en charge. Or, du point de vue de la cybersécurité, les anciennes technologies non corrigées posent le plus grand risque. Les entreprises doivent impérativement rester informées des menaces en cours et toujours respecter les bonnes pratiques de cybersécurité les plus récentes. Un dispositif négligé peut facilement devenir une proie facile pour les attaquants.

Préparez-vous face aux menaces

Une gestion efficace du cycle de vie peut aider les entreprises à préserver la sécurité de leur activité. De plus, elle contribue à mieux préparer l'avenir. Cela suppose de situer les risques et de rester informé des domaines susceptibles d'être exploités à des fins malveillantes. Cette considération s'adresse particulièrement aux systèmes de sécurité, car si une caméra de surveillance réseau tombe en panne, les conséquences peuvent être désastreuses.

Les dispositifs physiques doivent être à jour

Les fabricants publient régulièrement des mises à jour de firmware et des correctifs de sécurité qui résolvent les vulnérabilités, les bugs et d'autres problèmes de performance pour préserver la stabilité et la sécurité du système. Même si les entreprises saisissent l'importance des correctifs pour les systèmes d'exploitation et les applications, elles négligent souvent de mettre à jour les firmwares qu'exécutent les matériels. Ces dispositifs ainsi exposés aux cyberattaques peuvent entraîner la perte de précieuses données clients ou de lourdes amendes pour non-conformité de la part du régulateur.

En savoir plus >

Gestion rationalisée du cycle de vie

Un programme structuré de gestion du cycle de vie aide les entreprises à mieux préparer l'avenir. Il recourt aux technologies les plus adaptées et les plus récentes pour minimiser les menaces de sécurité et les vulnérabilités. Un logiciel de gestion des dispositifs comme AXIS Device Manager peut automatiser cette tâche et permettre aux entreprises de gérer efficacement leurs ressources.

Principe de fonctionnement

Un logiciel de gestion des dispositifs peut rapidement constituer un inventaire complet en temps réel de la totalité des caméras, encodeurs et dispositifs de contrôle d'accès, audio et autres connectés au réseau. Il peut analyser l'ensemble du réseau et, lorsqu'un dispositif nouveau ou mis à jour est détecté, il en capture toutes les informations clés, y compris numéro de modèle, adresses IP et MAC, version de firmware et statut des certificats.

Tour d'horizon complet

Un panorama très détaillé de tous les écosystèmes réseau permet d'appliquer plus facilement des pratiques et politiques de gestion du cycle de vie sur tous les dispositifs et de gérer en toute sécurité les tâches majeures d'installation, déploiement, configuration, sécurité et maintenance.

Gains de temps et de ressources

Un logiciel de gestion des dispositifs permet aux entreprises d'économiser beaucoup de temps et de stress dans la gestion du cyber-risque. Ce type de logiciel peut servir à la maintenance du système de plusieurs manières :

- Déploiement simultané des changements système, mises à jour de firmware et nouveaux certificats à tous les dispositifs concernés.
- Création ou reconfiguration des paramètres de sécurité, puis déploiement sur l'ensemble de votre réseau pour que tous les dispositifs respectent les pratiques et politiques de sécurité les plus récentes.
- Contrôle que tous les dispositifs exécutent la version de firmware la plus récente et la plus sûre.
- Gestion des niveaux de privilèges utilisateur sur l'ensemble du réseau et configuration des changements.

En savoir plus >

Informations en temps réel

Les outils de gestion des dispositifs offrent aux entreprises des éclairages en temps réel sur l'état de leur écosystème. Par exemple, vous pouvez voir les dispositifs à jour des correctifs, mises à jour de firmware et certificats les plus récents. Vous saurez également lorsqu'un dispositif est signalé pour retrait si le fabricant ne le prend plus en charge. Ces précieuses informations peuvent vous aider à déterminer si un malware pourrait éventuellement infecter vos dispositifs. Vous avez accès à toutes les informations nécessaires pour résoudre une multitude d'autres problèmes de vulnérabilités avant qu'elles ne compromettent votre réseau.

Sécurité proactive de l'écosystème

L'automatisation des processus de gestion des dispositifs permet de protéger les réseaux des menaces et des vulnérabilités. Les entreprises doivent néanmoins s'assurer qu'elles respectent des politiques et bonnes pratiques sérieuses de sécurité. Par exemple, votre entreprise applique-t-elle des politiques concernant la complexité des mots de passe et la fréquence de leur changement ? La bonne pratique de désactivation des services inutiles pour réduire la surface d'attaque est-elle appliquée ? À quelle fréquence la détection des vulnérabilités des dispositifs est-elle effectuée ? Appliquez-vous des procédures pour évaluer le niveau de risque lorsqu'un fabricant publie des failles de sécurité connues ? Ce sont là des questions à se poser pour pouvoir identifier et appliquer des mesures de protection proactive de votre écosystème réseau.

Réseaux Zero-Trust : de quoi s'agit-il ?

Les réseaux sont de plus en plus vulnérables. Ils sont menacés non seulement par les nombreuses attaques de plus en plus sophistiquées, mais aussi par la croissance vertigineuse des dispositifs connectés, chacun offrant un nouveau point d'accès possible au réseau. Pour y remédier, le concept de « Zero-Trust » a émergé, décliné en réseau et architectures Zero-Trust. Les fabricants de matériels, Axis compris, doivent impérativement se préparer aux environnements Zero-Trust. Ils seront là plus tôt qu'on ne le pense.

Ne faites confiance à rien ni personne sur le réseau

Comme son nom l'indique, la posture par défaut d'un réseau Zero-Trust consiste à ne se fier à aucune entité qui s'y connecte, qu'elle soit humaine ou matérielle en apparence. Peu importe où elle se trouve et ses modalités de connexion. La philosophie prépondérante des réseaux Zero-Trust est donc la suivante : ne jamais faire confiance, toujours vérifier.

Accordez l'accès minimal nécessaire

L'identité d'une quelconque entité qui accède au réseau ou qui s'y trouve est vérifiée plusieurs fois de différentes manières, en fonction de son comportement et de la sensibilité des données auxquelles elle accède sur le réseau. À la base, il est octroyé aux entités l'accès minimal nécessaire pour exécuter leurs tâches.

La posture par défaut d'un réseau Zero-Trust consiste à ne se fier à aucune entité qui s'y connecte.

En savoir plus >

3 raisons pour lesquelles un pare-feu n'est pas suffisant

Auparavant, les entreprises s'assuraient que leur pare-feu soit le plus robuste possible, mais cette méthode devient problématique pour plusieurs raisons.

1 Le préjudice potentiel est élevé

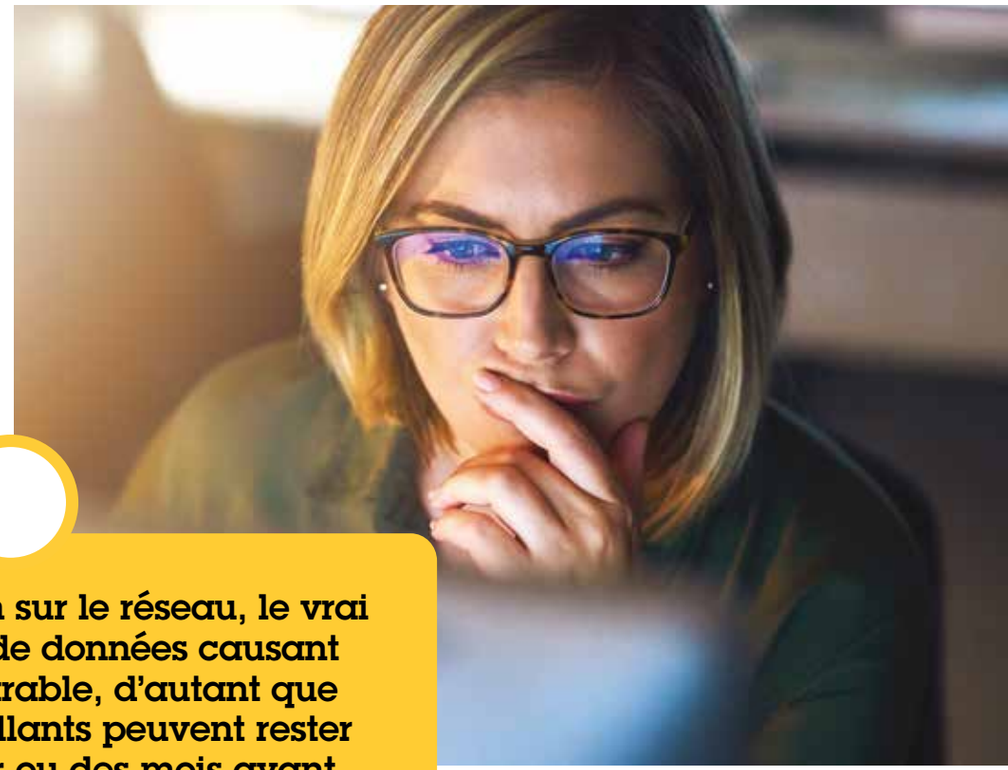
Même si un pare-feu a vocation à sécuriser les accès réseau, un pirate capable de s'introduire dans le pare-feu peut ensuite circuler assez librement sur le réseau.

2 Un pare-feu ne suffit plus

En raison du nombre considérable de dispositifs connectés au réseau, la protection périmétrique du réseau par une seule solution n'est plus envisageable.

3 Avantages de réseaux plus « perméables »

L'utilisation de services cloud au-delà du réseau et les avantages d'une interconnexion transparente des systèmes des clients et des fournisseurs ont changé la nature de la sécurité réseau.



> **« Après une intrusion sur le réseau, le vrai risque est la perte de données causant un préjudice irréparable, d'autant que des acteurs malveillants peuvent rester actifs des semaines ou des mois avant d'être détectés (s'ils le sont).**
>
> Wayne Dorris, Directeur régional Architecture et ingénierie chez Axis Communications

En savoir plus >

Principe du Zero-Trust

La méthode Zero-Trust emploie des techniques comme la sécurité périmétrique granulaire et la micro-segmentation du réseau. La première repose sur les utilisateurs et les dispositifs. Elle utilise leurs emplacements physiques et d'autres données d'identification pour déterminer si leurs identifiants peuvent justifier leur accès au réseau. La deuxième porte sur l'application de niveaux de sécurité variables en fonction des portions du réseau où résident des données plus critiques.

Niveau supplémentaire de sécurité

En accordant aux utilisateurs l'autorisation d'accéder uniquement aux portions du réseau et aux données nécessaires à leur mission, l'avantage pour la sécurité est évident. Néanmoins, le signalement des anomalies de comportement associées à ces identités offre un niveau de sécurité supplémentaire. Par exemple, un administrateur réseau peut disposer d'un accès étendu pour la maintenance des serveurs de R&D ou de finance.

Alerte de sécurité

Une alerte de sécurité se déclencherait si les identifiants de ce même administrateur réseau étaient utilisés en pleine nuit pour télécharger certains fichiers ou données critiques et les sortir du réseau. Dans un réseau Zero-Trust, soit une authentification supplémentaire confirme la légitimité de l'opération, soit l'activité anormale est signalée en temps réel au centre opérationnel de sécurité pour examen.

Des anomalies de comportement peuvent signaler le vol d'identifiants de sécurité, le ressentiment d'un collaborateur ou une activité d'espionnage d'entreprise.

En savoir plus >

Visite du moteur de politiques...

Au cœur de tous les réseaux Zero-Trust réside un moteur de politiques : ce logiciel permet aux entreprises de créer, contrôler et appliquer des règles sur les modalités d'accès aux données et ressources réseau. Les moteurs de politiques exploitent un ensemble de fonctions d'analyse réseau et de règles programmées pour accorder les autorisations par rôle en fonction d'un certain nombre de facteurs.

Oui ou non à chaque demande

En termes simples, le moteur de politiques compare chaque demande d'accès réseau et son contexte à la politique, puis informe l'applicateur sur la légitimité ou non de la demande. Dans un réseau Zero-Trust, le moteur de politiques définit et applique des politiques d'accès et de sécurité des données à tous les modèles d'hébergement, sites, utilisateurs et dispositifs.

Définition et application de règles

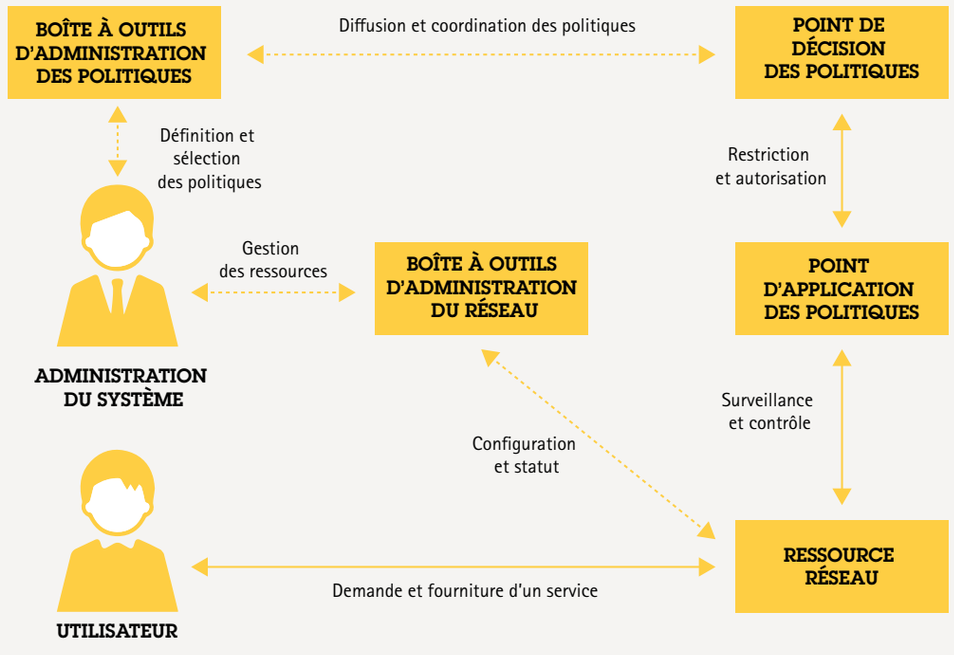
Pour qu'un moteur de politiques fonctionne, les entreprises doivent définir soigneusement les règles et politiques dans les équipements de contrôle de sécurité essentiels, comme les pare-feux nouvelle génération (NGFW), les passerelles de sécurité e-mail et cloud et les logiciels de prévention de la perte des données (DLP). Ensemble, ces contrôles se conjuguent pour appliquer les micro-segmentations réseau au-delà des modèles d'hébergement et des sites.

Modalités d'accès aux données et ressources réseau

Avec les moteurs de politiques, vous pouvez :

- créer des règles
- contrôler les règles
- appliquer les règles

Vue d'ensemble des moteurs de politiques



Moteurs de politiques actuels et futurs

Actuellement, la définition des politiques peut être nécessaire dans la console de gestion de chaque solution. Cependant, l'intégration toujours plus poussée des consoles peut favoriser la définition et l'actualisation automatiques des politiques sur tous les produits.

La gestion des identités et des accès, l'authentification multifacteurs, les notifications push, les autorisations de fichiers, le chiffrement et l'orchestration de la sécurité jouent tous un rôle dans la conception d'architectures réseau Zero-Trust.

En savoir plus >

Zero-Trust et vidéosurveillance

Les entités qui se connectent à un réseau peuvent évidemment être des utilisateurs, mais aujourd'hui, les connexions réseau proviennent majoritairement des dispositifs. C'est notamment le cas des caméras de surveillance réseau et des dispositifs connectés associés. Alors que les entreprises se tournent vers les architectures réseau Zero-Trust, les dispositifs réseau devront se plier au principe « ne jamais faire confiance, toujours vérifier ».

Quelle ironie !

Ce serait un comble si une caméra de surveillance, dont la vocation est la sécurité physique des entreprises, engendrait une vulnérabilité. Là encore, les méthodes traditionnelles de sécurité des dispositifs ne suffisent plus. De la même manière que les acteurs malveillants peuvent voler les identifiants d'accès d'un collaborateur, ils peuvent compromettre le certificat de sécurité des dispositifs. Dans un réseau Zero-Trust, de nouvelles approches sont nécessaires pour que les dispositifs démontrent leur légitimité sur le réseau.

Solution apparemment surprenante

Une technologie capable de fournir une racine de confiance infalsifiable pour les appareils connectés est la « blockchain ». Pour beaucoup, la blockchain est associée aux crypto-monnaies, qui lui confèrent une réputation sulfureuse. Mais en soi, la blockchain est un registre ouvert et distribué capable d'enregistrer efficacement les transactions entre deux parties de manière vérifiable et indélébile. En recourant à des blockchains privées pour l'utilisation de racines matérielles de confiance, les entreprises peuvent donc établir des clés de confiance inviolables dans les dispositifs.

Les prévisions suggèrent plus de

75 milliards

d'objets IoT en service d'ici 2025

Principe de la blockchain

De par la construction de la blockchain, aucune opération sur les données de la chaîne n'est modifiable sans accord des nœuds de consensus de toutes les transactions antérieures, qui sont toutes liées de manière cryptographique. Par conséquent, si des clés de confiance pour les parties identifiables d'un dispositif sont créées dans la blockchain, cela crée des identifiants inviolables pour le dispositif lui-même.

Course à l'armement IA dans le cyberespace

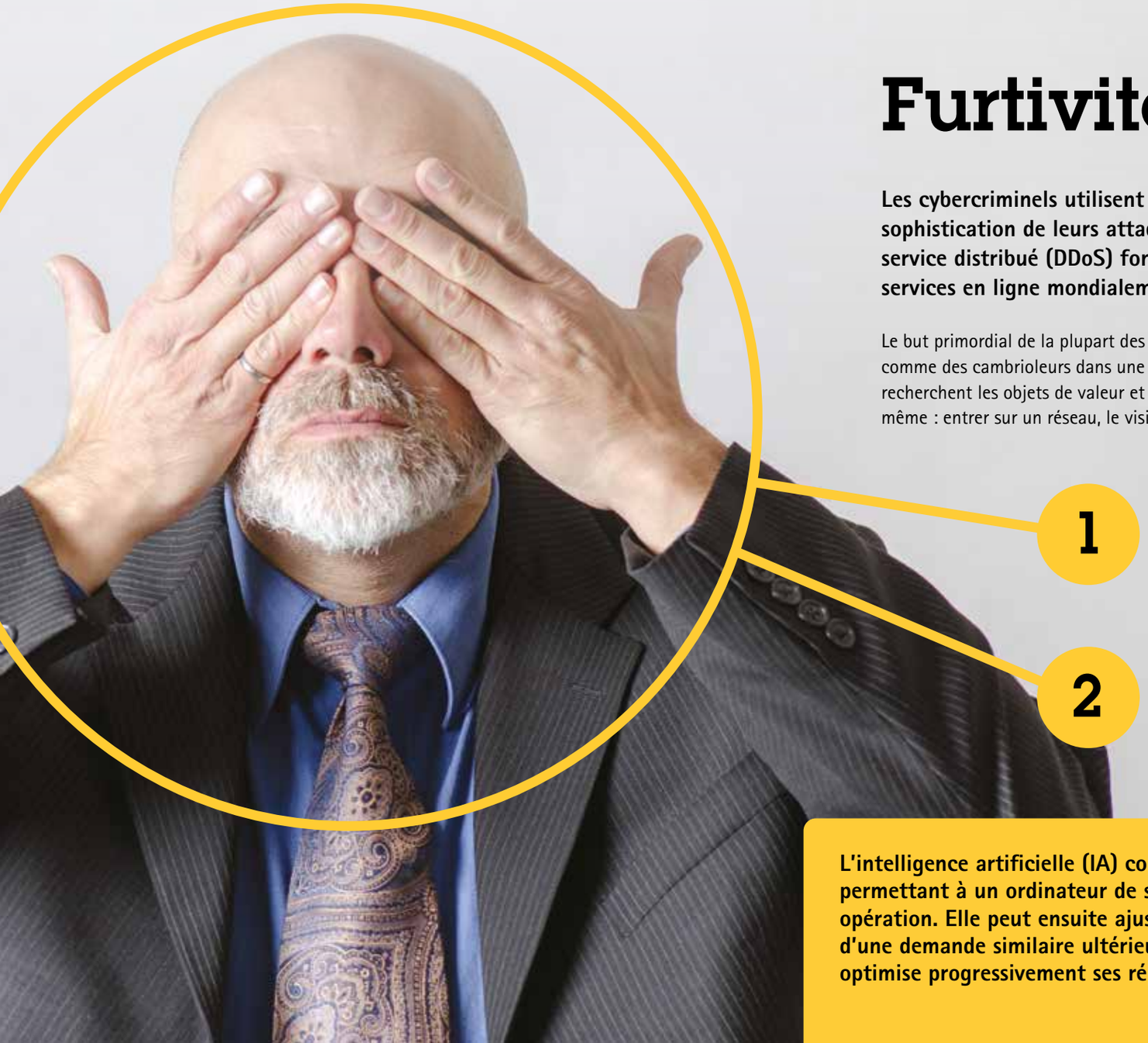
Dans tout progrès technologique, les acteurs malveillants ne tardent pas à étudier son potentiel pour leurs visées délictueuses. Lorsque des cybercriminels planifient des attaques par ransomware ou le vol d'informations financières, ou que des États cherchent à perturber les infrastructures critiques d'adversaires (ou pire), les nouvelles technologies peuvent renforcer leur force de frappe.

Ces organisations sont aussi bien financées qu'une activité légitime. Elles peuvent innover dans leur exploitation des nouvelles technologies comme l'intelligence artificielle (IA), le machine learning (ML) et le deep learning (DL). De plus, elles ne s'encombrent pas de morale, d'éthique ou du respect des lois et réglementations nationales ou internationales.

Elles étudieront simplement les opportunités que cette technologie leur apporte pour atteindre leurs objectifs criminels.

Les nouvelles technologies, y compris l'IA, se fraieront toujours un chemin jusqu'aux mains de criminels. **Heureusement, elles peuvent aussi servir de défense pour les entreprises ciblées.**

En savoir plus >



Furtivité et dissimulation

Les cybercriminels utilisent de plus en plus l'intelligence artificielle pour accroître la sophistication de leurs attaques sur les réseaux. Les attaques à grande échelle par déni de service distribué (DDoS) font souvent les gros titres car elles désactivent des sites web et services en ligne mondialement connus. Comment sont-elles possibles ?

Le but primordial de la plupart des cybercriminels est de rester indétectables le plus longtemps possible. Ils agissent comme des cambrioleurs dans une maison. Ils passent d'une pièce à l'autre en évitant les caméras et les alarmes, recherchent les objets de valeur et s'en vont aussi discrètement qu'ils sont entrés. Les cybercriminels opèrent de même : entrer sur un réseau, le visiter et partir sans être détectés.

1

Une méthode consiste à ressembler à un utilisateur légitime du réseau, humain ou dispositif. C'est là où l'IA et le ML deviennent de nouvelles armes redoutables. Grâce à ces technologies, les cybercriminels apprennent les comportements des utilisateurs et des dispositifs sur le réseau, développent rapidement de nouveaux malwares et stratégies de phishing, puis les déploient à une échelle gigantesque.

2

Cependant, le moyen le plus simple de pénétrer sur un réseau reste le même : pousser un utilisateur légitime à cliquer sur un lien pour ouvrir une porte. Un faux message du patron, au ton et au style presque identiques à un vrai, est souvent la clé d'entrée la plus efficace.

L'intelligence artificielle (IA) consiste en un ensemble d'algorithmes permettant à un ordinateur de stocker et d'analyser le résultat d'une opération. Elle peut ensuite ajuster cette opération en conséquence lors d'une demande similaire ultérieure. Au fil de milliers de demandes, elle optimise progressivement ses réponses et ses actions.

En savoir plus >

Tous les chemins mènent à Rome

Les cybercriminels recourent à une multitude d'outils d'IA tout au long de l'attaque, depuis les « chatbots » qui interagissent avec les utilisateurs au travers de profils de réseaux sociaux falsifiés, jusqu'aux réseaux neuronaux qui identifient les données les plus précieuses à extraire.

Une fois l'accès au réseau acquis, une telle technique est le déplacement latéral. Cette technique est fondamentale car le point d'accès au réseau, par exemple un dispositif non sécurisé dans une succursale, est rarement la destination finale convoitée.

Petit à petit, l'intrus progresse vers des zones beaucoup plus sensibles du réseau, récupérant des identifiants utilisateur au passage, notamment ceux des administrateurs réseau, qui leur fournissent une clé passe-partout d'accès au réseau.

En savoir plus >

IT et OT : un lien préoccupant

Avec la montée en flèche des dispositifs connectés et de l'Internet des objets (IoT) dans le monde, les risques augmentent en conséquence, d'autant que le réseau IT devient plus étroitement intégré à l'environnement opérationnel (OT).

Pour simplifier, le réseau informatique (IT) gère la circulation des informations numériques. De leur côté, les technologies d'exploitation (OT) gèrent le fonctionnement des procédés physiques, des machines et des actifs tangibles d'une entreprise ou d'un site donné. Pour les acteurs malveillants dont l'objectif est la perturbation et la destruction au lieu du vol, l'accès à l'OT est primordial. Inutile de déployer des trésors d'imagination pour saisir le préjudice potentiel en cas d'accès aux machines d'une centrale électrique, d'une raffinerie ou d'un hôpital.

En savoir plus >

Place aux détectives

L'exploitation potentielle de l'IA par les cybercriminels fait froid dans le dos. Cependant, ces mêmes technologies sont tout aussi disponibles à ceux dont la mission est de protéger les réseaux des intrusions. Or à plusieurs titres, les défenseurs prennent l'avantage sur les attaquants.

À plusieurs titres, les défenseurs prennent l'avantage sur les attaquants.

DARKTRACE

Darktrace est une entreprise reconnue d'envergure mondiale, spécialiste de l'IA appliquée à la cybersécurité. Naturellement, elle saisit parfaitement l'enjeu de l'exploitation grandissante de l'IA par les groupes criminels. Darktrace innove en permanence dans l'IA et le ML pour garder une longueur d'avance sur les cyber-malfaiteurs.

En savoir plus >

l'IA comme outil de défense et d'attaque

Entretien avec Jeff Cornelius, de Darktrace

Dans les pages suivantes, Jeff Cornelius, Vice-président exécutif de Darktrace, nous révèle comment son entreprise utilise l'IA et le ML pour garder une longueur d'avance sur les cybercriminels.

Q **Le tableau est-il si sombre ?**

« D'abord, malgré l'impression que les médias peuvent propager, le développement en IA et ML est loin d'être aisé ! Et même si l'adversaire est puissant parmi les groupes criminels et les états cherchant à perpétrer des cyberattaques, plusieurs éléments jouent en notre faveur.

« Le premier d'entre eux est que nous pouvons voir toute l'activité sur le réseau, du fait de l'accès que nous fournissent nos clients. Elle sert à comprendre le comportement de chaque dispositif et utilisateur. Au contraire, les acteurs malveillants ne pourront jamais compter que sur une vue partielle de l'activité. Toutes les actions qu'ils entreprennent à partir d'une tête de pont initiale est un pas presque en aveugle dans un environnement qu'on connaît, contrairement à eux.

« Leurs buts englobent des activités que l'entreprise n'exécute normalement pas. Notre premier objectif consiste à identifier et à répondre aux anomalies de comportement sur le réseau. La portée de notre action doit être vaste, car nous ne savons ni quand, ni où un adversaire peut frapper, pas plus que ses buts ou ses méthodes. »

En savoir plus >

Une analogie parlante

Entretien avec Jeff Cornelius, de Darktrace

Q

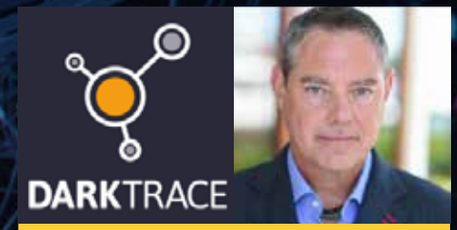
Pouvez-vous développer ?

« Pour établir un parallèle, quelqu'un qui étudie mes déplacements quotidiens à l'extérieur de chez moi parviendra à une vue assez détaillée de mes habitudes : mes horaires de sortie quotidiens, mon itinéraire pour aller au travail, où je déjeune, etc. Ils reproduiraient sans doute assez fidèlement ces aspects de ma vie.

« Mais en l'absence de vue chez moi, s'ils essaient de reproduire mes goûts au petit-déjeuner, ils commettraient certainement une erreur facilement détectable par un parent proche comme une anomalie. Il existe généralement un certain nombre d'informations disponibles sur Internet pour cibler une personne par un message astucieux de harponnage, mais une fois entrés, ils restent assis à la table. »

En savoir plus >

Machine learning supervisé…



Entretien avec Jeff Cornelius, de Darktrace

Q **Parlez-nous du machine learning.**

« Il y a une distinction importante à faire entre le ML supervisé et le ML non supervisé. Dans le premier, les ordinateurs sont entraînés avec un ensemble de données connues. Ils se réfèrent constamment à ces données pour vérifier si le résultat enregistré est celui attendu.

« En termes de cybersécurité, les modèles d'apprentissage se basent sur les malwares connus. Et c'est là où se joue la course entre criminels et cybersécurité : les acteurs malveillants utilisent le ML pour créer de nouvelles versions de malware, qui augmentent à un rythme exponentiel. Les entreprises de cybersécurité tentent de suivre la cadence en élaborant de nouveaux modèles de défense par ML supervisé. C'est un peu comme un correcteur d'orthographe qui tente de rester à jour alors que de nouveaux mots et langues surgissent chaque jour. Et la tâche se complique toujours plus pour rester dans la course.

En savoir plus >

...et machine learning non supervisé

Entretien avec Jeff Cornelius, de Darktrace

Q

N'y a-t-il pas un autre moyen ?

« Si. Au lieu de se baser sur les connaissances acquises des menaces passées, les algorithmes de ML non supervisé classifient les données de manière autonome et détectent des schémas récurrents. Ils analysent les données réseau à grande échelle et exécutent des milliards de calculs de probabilités en fonction des éléments qu'ils détectent. De là, ils établissent un modèle des comportements « normaux » sur le réseau concerné, au niveau des dispositifs, des utilisateurs ou des groupes des uns ou des autres. Ils peuvent ensuite détecter des écarts par rapport à ce « schéma de vie » évolutif, qui peuvent signaler une menace émergente. Ce système d'alerte précoce nous permet de garder une longueur d'avance sur les cybercriminels et les acteurs malveillants. »

L'union fait la force pour neutraliser les cybermenaces

La protection des entreprises, des établissements, de nos infrastructures critiques et de nos villes n'est pas la mission d'une seule personne. Il n'y a ni solution miracle, ni solution unique. Au contraire, le maintien d'un niveau acceptable de cybersécurité doit être le résultat de la collaboration d'une longue liste d'acteurs impliqués, y compris les utilisateurs finaux.

Instauration d'une culture cybersécurité

Là encore, l'union fait la force. Vous devez considérer chaque collaborateur de votre entreprise comme un membre de votre équipe de cybersécurité. Plusieurs pistes :

- Investir dans la formation du personnel à la cybersécurité
- Sensibiliser les nouveaux embauchés à cette question
- Encourager les dirigeants à mettre en place des politiques de cybersécurité
- S'informer et communiquer en permanence les cybermenaces émergentes
- Évaluer la cybersécurité comme critère de sélection lors de l'acquisition d'équipements réseau
- Mettre en place une politique BYOD (bring your own device)
- Élaborer et appliquer une stratégie de réponse aux incidents de cybersécurité

Si tous les acteurs de votre entreprise s'approprient vos plans de cybersécurité, vous êtes en bien meilleure posture pour garantir la sécurité de votre réseau et vos dispositifs.

En savoir plus >

Partage des responsabilités

La cybersécurité tourne autour des produits, des personnes, de la technologie et des processus en cours. La participation de tous est clairement une nécessité pour que tous les maillons de la chaîne de cybersécurité soient aussi solides que possible. La cybersécurité est une responsabilité partagée qui impose à tous les acteurs, y compris les utilisateurs finaux, d'œuvrer dans ce sens :

Intégrateurs et installateurs

Ils doivent s'assurer que tous les équipements installés sont dotés des derniers correctifs et mises à jour, et qu'ils exécutent un outil antivirus performant. Ils doivent également participer à l'effort mutuel avec les acteurs concernés dans l'établissement d'une stratégie efficace concernant les mots de passe, la gestion des accès distants et la maintenance des logiciels et des dispositifs connectés au fil du temps.

Distributeurs

Pour les distributeurs, qui ne manipulent pas directement les produits, la cybersécurité est relativement simple. En revanche, les distributeurs à valeur ajoutée doivent tenir compte des mêmes considérations que les intégrateurs et les installateurs, notamment lorsqu'ils achètent des équipements d'un fabricant pour les commercialiser sous une autre marque (ou la leur). La transparence est fondamentale, et l'origine des équipements doit être claire.

Consultants

Ils contribuent à spécifier les systèmes et les calendriers de maintenance sur toute leur durée de vie. Ils doivent faire preuve de transparence quant aux éventuels coûts associés. La problématique des équipements OEM/ODM, où les responsabilités de cybersécurité sont souvent floues, doit faire partie de la discussion générale autour de la cybersécurité.

Fabricants de dispositifs

C'est là où commence la cybersécurité. Les fabricants doivent appliquer les bonnes pratiques de cybersécurité dans la conception, le développement et les tests pour minimiser le risque de défaut. Des fonctions de sécurité intégrée, des processeurs développés en interne et le contrôle rigoureux de leur chaîne logistique sont aussi des aspects importants. Tout comme la fourniture d'outils abordables de gestion automatique des dispositifs et la communication des vulnérabilités connues aux canaux de distribution et aux partenaires.

Chercheurs

Ils découvrent souvent les vulnérabilités des dispositifs. Si la vulnérabilité n'est pas intentionnelle, le chercheur informe généralement le fabricant pour lui donner la possibilité de la corriger avant la publication. En revanche, si une vulnérabilité critique est intentionnelle, ils alertent plutôt le public pour sensibiliser les utilisateurs.

Utilisateurs finaux

Comme chaque entreprise a des besoins spécifiques et uniques en cybersécurité, il n'existe pas de configuration universelle en la matière. Néanmoins, un ensemble de politiques de sécurité informatique doit être en place pour définir l'étendue de la sécurité nécessaire. L'élimination des comptes par défaut, l'utilisation de mots de passe uniques et complexes, stockés de manière sûre et changés régulièrement, l'attribution d'autorisations différenciées et l'installation systématique des correctifs et des mises à jour ne sont que quelques-unes des procédures à appliquer.

En savoir plus >

Partenaires en protection

Ce n'est que par la collaboration que nous pouvons mieux nous préparer à répondre aux cybermenaces en constante évolution et rester en mesure de réagir vite en cas d'attaque. Tous les intervenants concernés ont un rôle à jouer pour veiller au bon déroulement de toutes les étapes du déploiement de solutions sécurisées : de la fabrication des dispositifs à leur gestion et leur maintenance, en passant par la conception et l'installation du système. C'est ainsi que nous restons vigilants.

Cybersécurité, gage de confiance en bordure de réseau

État des lieux en bordure de réseau

Alors que 2021 s'écoule, on observe une dynamique de fond en faveur de l'informatique en bordure de réseau (« Edge computing »). Le fait que des milliards d'objets **IoT** sont déjà connectés au réseau et que ce chiffre **augmente rapidement** n'est pas nouveau. Mais la nature et les demandes de ces dispositifs soulèvent de sérieux défis de cybersécurité.

IoT

L'IoT (Internet des objets) se rapporte à un réseau de dispositifs connectés à Internet, capables de communiquer entre eux. Ils englobent entre autres les smartphones et les « wearables », les compteurs connectés ou les machines industrielles intelligentes. Ces objets connectés utilisent des capteurs et des processeurs pour collecter et analyser les données acquises dans leur environnement et déclencher des actions en conséquence.

Croissance rapide

D'ici à 2025, les prévisions suggèrent que plus de 75 milliards d'objets connectés seront en service. Ce chiffre représente presque le triple de la base IoT existante en 2019.

En savoir plus >

État des lieux en bordure de réseau

> On observe une tendance en faveur du traitement des données et de l'analyse au niveau de la caméra elle-même.

En termes simples, les « objets » connectés au réseau doivent de plus en plus être capables de détecter instantanément une situation, prendre une décision et déclencher une action.

Les véhicules autonomes sont un exemple évident

Communicant avec l'environnement extérieur (par ex. feux de circulation) ou avec des capteurs de détection du risque (par ex. un objet qui surgit devant la voiture), les décisions doivent être calculées en une fraction de seconde. Or, la transmission par le réseau des données de la voiture jusqu'à un datacenter pour traitement et analyse, puis le retour d'une décision sur l'action à effectuer, prend trop de temps.

Mêmes impératifs pour la vidéosurveillance

L'adoption d'une approche proactive plutôt que réactive (prévention des incidents plutôt que réponse a posteriori) suppose de déporter davantage de traitement des données et d'analyse vers la caméra elle-même. Mais l'augmentation des dispositifs en bordure de réseau, qui jouent un rôle croissant dans la sécurité et la protection, se traduit par plusieurs conséquences, que nous présentons dans les pages suivantes.

En savoir plus >

Puissance maison dans des dispositifs dédiés

Des matériels et logiciels dédiés et optimisés, conçus pour une application donnée, sont indispensables pour accompagner le développement de l'Edge computing. Les objets connectés devront posséder une puissance de calcul supérieure. Leur conception et leur fabrication devront répondre à un but précis et intégrer la cybersécurité dès la plaque de silicium.

C'est là où les processeurs intégrés propriétaires prennent tout leur sens. Par exemple, les dispositifs Axis utilisent un système processeur intégré (System-on-chip) conçu en interne, qui les protège des cyberattaques, telles que les mises à jour de firmware malveillant qui ouvre une « porte dérobée ». Dans sa dernière version, le processeur ARTPEC-7 est conçu spécialement pour les besoins actuels et futurs en vidéosurveillance, dans une optique de sécurité d'abord.

Spécialement destiné à la vidéosurveillance, le tout dernier processeur Axis ARTPEC-7 embarque plus de 50 fois les performances de l'original. Comme Axis contrôle la conception et la fabrication de son propre processeur, il peut créer les produits les plus adaptés aux besoins des clients, mais aussi répondre aux besoins de facteurs externes en évolution, tels que les cybermenaces de sécurité.

> **ARTPEC-7 nous permet de fournir des caméras réseau offrant une excellente qualité d'image et des performances de pointe, efficaces en bande passante et capables d'exécuter des analyses en bordure de réseau.**
>
> Stefan Lundberg, Expert ingénieur chez Axis Communications

En savoir plus >

Vers un Edge Computing de confiance

La confiance se décline sous plusieurs formes.

- **Avoir confiance dans le fait que les entreprises collecteront et utiliseront nos données de manière responsable**
- **Avoir confiance dans le fait que les dispositifs et les données sont protégés contre les cybercriminels**
- **La confiance dans l'exactitude des données et dans le fait que la technologie fonctionnera comme prévu**

La bordure de réseau sera le point auquel cette confiance s'établit ou se détruit.

La confiance tout au long de la chaîne logistique sera déterminante. Même si l'incorporation de processeurs-espions dans les matériels eux-mêmes est une possibilité relativement lointaine, il serait relativement simple d'installer une « porte dérobée » d'espionnage dans un dispositif, par une actualisation du firmware postérieure à l'étape de fabrication.

En savoir plus >

Vers un Edge Computing de confiance

Les questions relatives à la confidentialité restent un débat d'actualité de par le monde. Alors que les technologies comme l'anonymisation et le masquage dynamique peuvent servir en bordure de réseau pour protéger la confidentialité, les méthodologies et réglementations restent hétérogènes selon les régions et les pays. L'examen du cadre juridique international restera une tâche continue pour les entreprises opérant dans le domaine de la surveillance.

La cybersécurité s'impose plus que jamais

Alors que le traitement et l'analyse des données sont amenés à se généraliser dans le dispositif lui-même, la cybersécurité devient un enjeu critique. Malgré un environnement où les cyberattaques sont de plus en plus fréquentes et sophistiquées, de nombreuses entreprises négligent encore de déployer les mises à niveau de firmware les plus basiques. Fondamentalement, un système sécurisé doit associer la gestion de chaque dispositif et la gestion complète du cycle de vie de l'ensemble de la solution de surveillance, grâce à des politiques claires concernant les matériels, les logiciels et les utilisateurs.

Le risque de la non-conformité

Ces dernières années, des entreprises comme British Airways et Mariott International ont encouru de fortes amendes pour infraction aux réglementations. La crainte des amendes a fait l'effet d'une onde de choc parmi les entreprises, qui se répercute sur les budgets qu'elles affectent à la cybersécurité.

Les entreprises sont également menacées par d'autres attaques ciblées, comme le ransomware, le malware et le phishing. Elles peuvent se concrétiser par des pannes de systèmes, des pertes de données, des perturbations opérationnelles, une mauvaise publicité, une perte de clients et une chute du chiffre d'affaires.

Plusieurs aspects de conformité

On imagine souvent que la conformité se rapporte au respect des réglementations nationales et des normes internationales. Cependant, il ne s'agit que d'un aspect. Les entreprises doivent également mettre en place et respecter des contrôles et des bonnes pratiques internes, tout en veillant à ce que leurs partenaires les respectent également.

Il incombe désormais aux entreprises de s'assurer que les données de leurs clients sont convenablement protégées.

Trois domaines à prendre en compte :

1. **Conformité réglementaire**
   Règlements nationaux comme le RGPD et normes et cadres internationaux comme ISO ou NIST
2. **Conformité interne**
   Politiques et bonnes pratiques internes à l'entreprise
3. **Conformité externe**
   Conformité dans la chaîne logistique

En savoir plus >

Notre obligation : respecter la loi

Les lois sur la protection des données, telles que le Règlement général sur la protection des données (RGPD) de l'UE, sont destinées à réglementer l'exploitation des informations personnelles des consommateurs par les entreprises, les organismes ou les États. En termes de cybersécurité, ces lois sont souvent étroitement liées aux solutions de sécurité en place dans l'entreprise.

Le RGPD est un règlement européen, mais la plupart des entreprises mondialisées doivent s'y conformer d'une manière ou d'une autre. Par exemple, les entreprises américaines qui stockent des données dans l'UE doivent respecter le RGPD. De même, si une entreprise passe un contrat avec un tiers qui utilise le traitement des données, les deux parties doivent également se conformer au RGPD. Aux États-Unis, les 50 États ont adopté des réglementations distinctes sur la protection des données, qui compliquent les activités inter-États.

La gouvernance interne coûte plus cher

Les hackers ne piratent pas des normes. Ils étudient une entreprise et déterminent leurs vulnérabilités propres et les points où elles sont exposées. Les entreprises pourraient facilement dépenser tout leur budget à la cybersécurité. Cependant, l'objectif doit consister à assurer une protection suffisante qui n'entrave pas l'innovation. C'est un équilibre à trouver, qui dépend du goût du risque de l'entreprise. Certaines d'entre elles appliquent des contrôles encore plus rigoureux que ceux exigés par la loi. En effet, en cas de compromission de sécurité, les entreprises doivent démontrer qu'elles ont pris les bonnes mesures pour protéger l'activité.

Conformité dans la chaîne logistique

Les entreprises avec des chaînes logistiques complexes auront aussi d'autres exigences de conformité. Par exemple, les entreprises européennes qui traitent avec le gouvernement des États-Unis doivent respecter des normes comme le programme CMMC (Cybersecurity Maturity Model Certification), qui impose un audit de certification de la gestion interne des procédures de cybersécurité. Dans le pire des cas, des entreprises tierces (par ex. fournisseurs) peuvent aussi être partiellement responsables de non-conformité et donc supporter un pourcentage des amendes.

Sans pour autant négliger l'importance des obligations externes, l'application de politiques internes plus strictes dans l'entreprise est conseillée. Car au final, c'est à l'entreprise qu'il incombe de garantir la conformité et la protection des données contre toute intrusion.

En savoir plus >

Quelles réglementations dans votre cas ?

Le maintien de la conformité exige un travail permanent. Les réglementations de cybersécurité et de gestion des données qui s'appliquent à votre entreprise dépendent généralement de son secteur d'activité. Cependant, plusieurs règlements concernent une multitude de secteurs d'activité et de pays.

Les entreprises doivent régulièrement examiner les nouvelles directives et les évolutions qui pourraient aboutir à une législation. Par l'examen des menaces et des attaques actuelles, ainsi que la compréhension des nouvelles lois et réglementations de conformité en vigueur, les entreprises peuvent déterminer les changements qu'elles doivent apporter pour passer les nouveaux contrôles de conformité.

Audits de cybersécurité

Après l'identification des réglementations que doit respecter votre entreprise, vous devez évaluer votre situation en matière de conformité générale. Un audit interne de cybersécurité vous permet d'évaluer les procédures de gouvernance de la sécurité informatique de votre entreprise. En général, les entreprises doivent mener un audit de cybersécurité chaque année. Néanmoins, il est recommandé d'évaluer en continu tous les contrôles pour pouvoir combler en temps utile les éventuelles failles. Les entreprises ont également intérêt à formaliser ces procédures d'évaluation continue des contrôles de sécurité, dont elles pourront se servir aux audits suivants.

Quelques pistes à considérer lors d'un audit de cybersécurité :

- **Gestion du risque :** Quelle procédure applique votre entreprise pour identifier et gérer les risques associés à la conformité réglementaire ? Par exemple, comment communiquez-vous les risques et comment vérifiez-vous qu'ils sont évalués ?
- **Procédure d'audit interne :** Les entreprises doivent établir un processus d'audit interne pour évaluer régulièrement la conformité. Par exemple, quelles sont les procédures en place pour identifier, évaluer et gérer les changements apportés aux pratiques de cybersécurité ?
- **Formation sécurité et confidentialité :** Vos collaborateurs sont-ils responsabilisés et adéquatement formés pour identifier les risques de sécurité informatique ? Par exemple, proposez-vous une formation sur les e-mails de phishing ? Un tel programme de formation n'est qu'un aspect du sujet. Des contrôles internes détermineront l'efficacité de la formation. Dans les domaines à risque élevé, l'entreprise peut choisir d'effectuer des contrôles chaque trimestre plutôt que chaque année.

En savoir plus >

Suivi de la conformité

Le résultat d'un audit interne peut servir à créer un plan de suivi de la conformité. Ce plan permettra d'évaluer en continu les efforts de conformité générale d'une entreprise et de prendre en compte tous les risques identifiés pendant l'audit. Les risques doivent être priorisés en fonction de la menace qu'ils représentent pour votre entreprise. L'évaluation des contrôles de conformité en place dans votre entreprise permet d'identifier les éventuels écarts réglementaires dans vos contrôles de cybersécurité.

Pour établir les responsabilités du suivi des risques de cybersécurité, les rôles doivent être attribués en fonction de l'expertise nécessaire. Il est possible d'optimiser ces affectations en se demandant quelles personnes disposent des compétences nécessaires et quelles activités de surveillance du risque peuvent être combinées.

Êtes-vous à jour ?

En général, les fabricants publient régulièrement des mises à jour de firmware pour corriger des vulnérabilités et lorsqu'une nouvelle législation entre en vigueur. En parallèle, un panorama clair de tous les dispositifs et du statut de leur cycle de vie est tout aussi important pour se préparer lorsque la prise en charge d'un produit se termine. Des outils de gestion des dispositifs comme AXIS Device Manager peuvent aider à vérifier que les produits sont à jour et conformes aux exigences de conformité. Ces outils envoient des notifications sur le renouvellement des licences, les dates de maintenance ou les agréments. De plus, si les audits l'exigent, ces outils peuvent également fournir la documentation nécessaire.

Démontrez votre degré de conformité

Les clients demandent souvent aux fabricants de dispositifs de remplir des questionnaires sur leur degré de cybersécurité. Les entreprises doivent répondre à des questions concernant leurs plans de continuité, leurs modalités de mise en œuvre des certifications et leurs procédures de protection des données sur le réseau. Si toutes ces informations sont déjà prêtes, les entreprises peuvent tranquilliser leurs clients en démontrant rapidement la rigueur de leur organisation.

> **« Le coût de la non-conformité est très élevé. Si vous pensez que la conformité coûte cher, essayez la non-conformité.**
>
> **Paul McNulty, ancien procureur général adjoint des USA**
> **https://youattest.com/**

En savoir plus >

Documentation, formalisation

La documentation est un élément central pour démontrer le respect des réglementations. Vos politiques internes peuvent inclure des réponses aux questions suivantes :

- Comment justifiez-vous ce que vous enregistrez ?
- Affichez-vous des panneaux informant le public qu'il est surveillé ?
- Votre surveillance filme-t-elle des personnes ? Leur vie privée est dès lors exposée, les conséquences doivent être prises en compte et documentées. Qui a accès à la vidéo ?
- Comment les données sont-elles stockées et pour combien de temps ? Le stockage des données est-il sécurisé physiquement et informatiquement ? Comment garantissez-vous l'élimination des vidéos anciennes ?

Vous devez également inclure de la documentation sur certains scénarios particuliers. Par exemple, comment la traiter une intrusion : qui est responsable du contrôle des données et quelles sont les procédures en place ? De plus, il est recommandé de tenir informés les conseils réglementaires de toute défaillance identifiée pendant les audits internes et des programmes mis en œuvre par l'entreprise pour éliminer ces écarts.

La conformité est une cible mouvante

Comme les lois et réglementations évoluent régulièrement, il faut admettre que même les plans de suivi de la conformité les plus rigoureux ne vous protègent pas complètement d'amendes réglementaires. Les entreprises doivent contrôler en permanence leur conformité et être en mesure de la démontrer sans hésitation.

L'heure est venue d'agir

La conformité est incontestablement une composante essentielle de la cybersécurité et les préoccupations qui l'entourent sont là pour durer. Les entreprises et les consommateurs prennent conscience de la menace, en réalisant que leurs systèmes et leurs données sont vulnérables aux attaques s'ils n'agissent pas rapidement. Alors que les entreprises veulent continuer d'innover et de se développer sans frein, elles doivent néanmoins minimiser les risques que pose la cybercriminalité. De leur côté, les consommateurs veulent que leurs données restent protégées et que les entreprises avec lesquelles ils traitent disposent des moyens de le faire. La question des réglementations nationales ne peut être résolue que par une approche collaborative, où fournisseurs, fabricants et utilisateurs finaux assument tous la responsabilité d'une cybersécurité efficace. Cette démarche aboutira à minimiser le risque d'une faille de sécurité préjudiciable.

La conformité est incontestablement une composante essentielle de la cybersécurité et les préoccupations qui l'entourent sont là pour durer.

Que faut-il savoir sur son fournisseur en surveillance et ses sous-traitants ?

Les risques de sécurité sont toujours présents. De nouvelles menaces émergent et leur nature peut évoluer à tout moment. Les entreprises doivent savoir que le fournisseur de leur système évalue en continu ces risques et les neutralise, non seulement sur ses propres sites, mais aussi sur ceux de ses sous-traitants.

Les entreprises se limitent souvent à la façon dont leurs fournisseurs participent à la cybersécurité. Mais qu'en est-il des sous-traitants du fournisseur ? Comment les fournisseurs gèrent-ils toute leur chaîne logistique et veillent-ils à la sécurité de tous leurs produits, du composant au produit fini ?

Votre fournisseur s'attache-t-il à minimiser les risques de sécurité ?

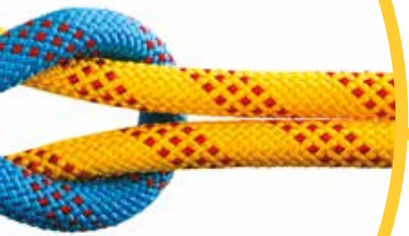
- Les produits qu'il conçoit et fabrique sont-ils sécurisés par une protection intégrée ?
- Partage-t-il des connaissances et des outils pour mettre en place des moyens de protection ?
- Propose-t-il une réaction rapide et des mises à jour gratuites en cas de détection d'une nouvelle vulnérabilité ?
- Contrôle-t-il toute sa chaîne d'approvisionnement, du composant au produit fini ?

« Comment les fournisseurs contrôlent-ils l'ensemble de leur chaîne logistique ? »

En savoir plus >

À la recherche du bon partenaire

La sécurité de la chaîne logistique débute par un choix éclairé de partenaires selon un processus d'évaluation rigoureux. Ce processus doit comporter pour chaque candidat une analyse de ses processus de gestion qualité et de ses pratiques durables. A minima, elle doit être certifiée ISO 9001 ou IATF 16949 par un organisme indépendant.



Évaluation des sous-traitants

Votre fournisseur doit également évaluer les processus de gestion du risque de ses sous-traitants, ainsi que leurs installations et procédés de production. Des visites de sites, suivies d'audits sur site, permettront d'évaluer si l'entreprise répond aux critères et normes définis pour la qualification de fournisseur agréé. Dans le cadre de l'évaluation d'un nouveau partenaire potentiel de la chaîne logistique, les fournisseurs doivent mener une analyse approfondie de la situation financière et du tour de table de l'entreprise.

Sous-traitants stratégiques

Avec les sous-traitants de composants critiques et les partenaires fabricants, les relations sont généralement étroites et durables. Ce sont des acteurs stratégiques avec lesquels votre fournisseur codirige les projets et le développement, définit des objectifs et prend des engagements mutuels à long terme. La collaboration et la communication sont donc intenses et quotidiennes, avec de fréquentes visites sur site.

Tous les composants critiques faisant partie des produits de votre fournisseur doivent être approvisionnés directement à partir de sous-traitants stratégiques et entreposés en interne. Les composants non critiques peuvent être achetés par les partenaires fabricants eux-mêmes, mais uniquement auprès de fournisseurs appartenant à la liste de fournisseurs agréés.

Quel degré de sécurité dans la production de votre fournisseur ?

- Est-ce qu'il définit et contrôle les procédés de fabrication ?
- Est-ce qu'il développe et produit des équipements de production critiques ?
- Votre fournisseur propose-t-il un système de test des composants, modules et produits pendant la production, accompagné de logiciels, d'ordinateurs de test et d'autres structures informatiques physiques ?
- Votre fournisseur collecte-t-il les données de production 24 h/7 j pour l'analyse en temps réel des données, l'évaluation des risques de sécurité et l'application de plans de correction ?

En savoir plus >

Audit de votre fournisseur

Le meilleur moyen pour votre fournisseur de garantir la conformité de ses sous-traitants au cahier des charges spécifié consiste à mener des audits réguliers sur site, annuellement ou tous les deux ans.

Les audits doivent évaluer plusieurs aspects importants :

- Conformité des procédures, y compris documentation
- Sécurité des installations
- Manipulation physique en usine
- Gestion d'inventaire
- Moyens de production
- Contrôle qualité
- Traçabilité

Un examen trimestriel de l'activité est également un bon moyen de suivre la performance par rapport aux attentes. Pour les sous-traitants stratégiques, il est recommandé de mener ces évaluations au niveau de la direction.

Sécurité physique

Tous les sites de la chaîne d'approvisionnement, du fournisseur de composants au centre de distribution, doivent satisfaire les exigences rigoureuses concernant la sécurité des installations :

- Les accès et les sorties doivent être gardés en permanence, des contrôles d'accès et un registre des visiteurs doivent être tenus à jour et archivés. Certaines zones peuvent exiger une surveillance continue, voire des agents de sécurité pour sécuriser l'installation et les alentours.
- Des portiques doivent être en place pour détecter les objets ou matières indésirables.
- Le transport doit être assuré uniquement par des transporteurs de bonne réputation, qui appliquent des réglementations et des contrôles de sécurité rigoureux. Les chauffeurs et les poids-lourds doivent être soumis aux règles de sécurité à l'enlèvement et à la livraison.
- Tout le fret aérien doit être passé aux rayons X. Il arrive souvent que les marchandises soient dans un emballage inviolable au point d'origine pour détecter toute manipulation ultérieure.
- Les marchandises entrantes et sortantes sont souvent surveillées et documentées par des caméras CCTV.

En savoir plus >

Transfert des données et sécurité informatique

Le transfert de données sur le réseau de la chaîne logistique doit être protégé par des protocoles de sécurité au moyen de méthodes de chiffrement et d'authentification. Les sous-traitants et les partenaires doivent maintenir un niveau élevé de sécurité informatique pour réduire les risques d'une éventuelle faille dans la chaîne logistique.

Votre fournisseur doit adopter une approche systématique d'identification et de gestion des informations sensibles de l'entreprise. Ce système doit englober le personnel, les procédures, les systèmes informatiques et les sites physiques. Il doit respecter la norme ISO 27001 et le Règlement général sur la protection des données (RGPD) de l'UE. Ces dispositions renforceront la sensibilisation et l'efficacité de la gestion du risque.

Sécurité du personnel

Il est essentiel de savoir qui vous embauchez, non seulement en termes de compétences, formation et expérience professionnelle, mais aussi dans une perspective de sécurité. Chez Axis par exemple, la qualité et la sécurité des procédures de recrutement sont strictes : elles englobent vérification d'identité, demandes de références et contrôle des antécédents avant l'embauche. Les nouveaux embauchés et les consultants doivent signer un accord de confidentialité qui protège la propriété intellectuelle et d'autres informations sensibles, pendant l'occupation du poste et après leur départ.

Responsabilisez votre personnel et réduisez les risques

Chez Axis, nous veillons à sensibiliser le personnel à l'importance de la sécurité informatique. Nous estimons que des collaborateurs responsabilisés disposent des informations nécessaires pour savoir ce qu'ils ont à faire et connaître les risques existants. Chaque collaborateur Axis est associé à l'engagement envers une sécurité et une confiance effectives. L'ensemble du personnel suit une formation sur la sensibilisation à la sécurité informatique, qui l'incite à faire preuve de prudence et de vigilance. L'accès aux informations, aux systèmes et aux ressources est contrôlé et accordé uniquement aux collaborateurs qui en ont besoin pour accomplir leur mission. Le personnel des sous-traitants et partenaires fabricants d'Axis partage les informations, les systèmes et les ressources avec Axis.

En savoir plus >

Intégrité des produits

Comme tous les produits, les dispositifs de surveillance doivent fonctionner comme prévu et leur intégrité doit être maintenue. Pour ce faire, les composants matériels et le firmware du produit doivent être efficacement protégés de toute modification ou manipulation non autorisée pendant son cheminement sur la chaîne logistique.

Contrôles qualité

Avec ses sous-traitants et partenaires fabricants, Axis applique une multitude de contrôles qualité pour protéger l'intégrité de ses produits. Les composants proviennent toujours d'un fournisseur de la liste des fournisseurs agréés, selon le cahier des charges Axis. Le fournisseur ne peut pas modifier les spécifications, les consignes d'intervention ou les documents d'inspection qualité sans l'accord d'Axis. Tous les changements approuvés doivent être documentés et consignés.

Traçabilité

Un processus de gestion des marchandises veille toujours à leur état et révèle tout écart susceptible de mettre en jeu la qualité. Les sous-traitants et partenaires fabricants doivent appliquer un système de traçage pour garantir la traçabilité des lots produits, depuis les marchandises entrantes jusqu'aux composants finis. Pendant la production, le composant physique subit une multitude de tests pour vérifier la conformité et détecter tout défaut.

Détection des composants contrefaits

Une inspection optique automatisée permet de vérifier l'absence de composant contrefait. Axis met au point et produit ses moyens de production critiques, ainsi que le système pour tester les composants, modules et produits à différents stades de fabrication. Ce processus réduit le risque de sabotage. Mesure de sécurité supplémentaire : toutes les données de test sont communiquées à Axis 24 h/7 j, de sorte que les modifications non autorisées sont immédiatement identifiées.

Pourquoi Axis ?

Des solutions pour un monde plus sûr et plus intelligent

Une qualité omniprésente : Tous nos produits sont soumis à des essais approfondis, gage de sérénité pour nos clients.

Technologies innovantes : Nous associons les technologies et l'imagination humaine pour renforcer les performances et la simplicité d'utilisation. Basées sur des standards ouverts, nos technologies sont flexibles, évolutives et faciles à intégrer.

Développement durable à tous les niveaux : Axis est résolument engagé envers un développement écoresponsable avec l'utilisation de matériaux durables. Par exemple, 80 % des caméras et encodeurs Axis ne contiennent pas de PVC.

À la pointe de la cybersécurité : Nous surveillons en permanence les menaces et leurs conséquences pour prendre rapidement les mesures qui s'imposent. Même après l'installation, nous continuons de renforcer la cybersécurité de nos dispositifs par des mises à niveau, des mises à jour et des modernisations.

Présence mondiale, expertise locale : Axis possède la plus grande base au monde de produits vidéo sur IP installés et des collaborateurs dans plus de 50 pays. Nous partageons nos perspectives et nos expériences, en restant informés des dernières nouveautés.

Le pouvoir des partenariats : Le modèle de partenariat d'Axis en fait la marque de caméras la plus intégrée du marché.

À propos d'Axis Communications

En concevant des solutions réseau qui améliorent la sécurité et permettent le développement de nouvelles façons de travailler, Axis contribue à un monde plus sûr et plus clairvoyant. Leader technologique de la vidéo sur IP, Axis propose des produits et services axés sur la vidéosurveillance, l'analyse vidéo, le contrôle d'accès, l'interphonie et les systèmes audio. L'entreprise emploie plus de 3800 personnes dans plus de 50 pays et collabore avec des partenaires du monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984, son siège est situé à Lund en Suède.

Pour en savoir plus, visitez notre site web www.axis.com.