Protéger votre système de vidéosurveillance contre les cyberattaques

Conseils pour évaluer la cybersécurité de votre solution vidéo

Par Todd Robinson,
chef de produit, Fixed Recorder Appliances

Les attaques récentes et médiatisées contre des systèmes de vidéosurveillance ont souligné l'importance de choisir une technologie vidéo qui soit sûre en termes de cybersécurité.

Les retombées d'un piratage peuvent être dévastatrices, rendre publiques des données hautement sensibles sur Internet, réduire la confiance des clients, et augmenter le risque de litiges et les responsabilités financières.

Il est impératif que les entreprises choisissent des produits auxquels elles peuvent faire confiance, et des fabricants qui ont une réputation établie dans la cybersécurité et les mesures de protection des données. Parfois, cela implique de s'informer plus en profondeur, et d'examiner les antécédents, la R&D et les processus de fabrication des produits d'une entreprise.

Voici quelques éléments importants à prendre en compte lors de l'évaluation d'une solution de vidéosurveillance du point de vue de la cybersécurité :

Todd Robinson

Qu'est-ce qui est chiffré et qu'est-ce qui ne l'est pas ?

Si de nombreux systèmes de vidéosurveillance offrent un cryptage en transit, qui empêche des tiers d'accéder aux données pendant leur transmission en les gardant cryptées jusqu'à ce qu'elles atteignent leur point d'arrivée, le cryptage complet de bout en bout est le niveau de protection le plus élevé pour vos données. Les données n'incluent pas seulement la vidéo et l'audio, mais incluent également des métadonnées telles que les données GPS, les données du panneau d'alarme, les données d'analyse, les données de point de vente ou les données de transaction GAB.

Le cryptage complet de bout en bout va au-delà du simple cryptage en transit et inclut le cryptage au repos afin que chaque aspect de vos données soit protégé. Le cryptage au repos est le processus de cryptage des données stockées sur un support physique. Avec un cryptage complet de bout en bout, les données sont cryptées à la fois lors de leur passage de la caméra à l'enregistreur et de l'enregistreur au logiciel client, ainsi que sur les supports physiques de stockage.

Comme des niveaux de cryptage plus élevés peuvent parfois avoir un impact sur les performances du processeur, il faut demander à votre fournisseur de vidéo de trouver le bon équilibre pour vos besoins.

Sécurité du système d'exploitation (OS)

Il y a beaucoup de débats concernant la sécurité de Linux par rapport aux systèmes d'exploitation Windows (OS) pour les enregistreurs vidéo sur réseau (NVR). Bien que n'importe quel système puisse être attaqué en dernier ressort, je dirais qu'un appareil avec un système d'exploitation Linux intégré est plus sûr lorsqu'il a été personnalisé dans le seul but d'enregistrer de la vidéo. Le système d'exploitation basé sur Linux dans les enregistreurs March Networks, par exemple, est renforcé, supprimant les services inutiles, de sorte qu'il y a moins de possibilités de cyberattaques.

De plus, lorsqu'un système d'exploitation basé sur Linux est personnalisé, il ne dépend pas d'un tiers pour les mises à jour de sécurité, et il n'y a aucun risque de mises à jour système appliquées automatiquement qui pourraient avoir un impact négatif sur le système. Il y a également un contrôle plus strict sur ce à quoi une application a accès, ce qui complique l'accès au système pour les logiciels malveillants. Et pour renforcer encore la sécurité, Linux dispose d'un large groupe de développeurs de son code OS en open source, ce qui augmente la probabilité que toute faille de sécurité soit rapidement repérée.

Qui a accès au système ?

L'attaque très médiatisée qui a eu lieu plus tôt ce mois-ci impliquait l'utilisation d'un compte «Super-admin», où une personne avait un accès illimité à toutes les caméras du système basé sur le cloud. De toute évidence, ce type d'accès illimité constitue une menace pour la sécurité, alors discutez avec votre fournisseur de vidéo de ses politiques en matière de droits des utilisateurs et d'accès. (Soit dit en passant, March Networks ne propose pas de mode super-utilisateur ou super-administrateur qui pourrait accéder à tous les systèmes de nos clients).

Que ce soit dans le cloud ou sur site, un bon fournisseur de vidéo doit offrir des contrôles stricts sur les droits et la gestion des utilisateurs, permettant aux administrateurs de créer des profils très spécifiques qui donnent ou restreignent l'accès aux personnes utilisant le système. Cela garantit que les employés juniors ou débutants ne voient que ce dont ils ont besoin pour faire leur travail ; cela permet également aux administrateurs système de vérifier l'accès des utilisateurs et de voir qui a accédé à quoi et quand.

Protection par mot de passe

La sécurité des mots de passe semble simple, mais il est étonnant de constater le nombre d'intrusions liées à la perte ou au vol de mots de passe. Un bon fournisseur de vidéosurveillance n'utilisera pas de mots de passe fixes ou codés en dur sur ses appareils, et encouragera également les changements de mot de passe fréquents et la création de mots de passe complexes.

Avec les enregistreurs de March Networks, par exemple, chaque client reçoit un mot de passe individuel à usage unique pour la configuration initiale. Ils sont ensuite invités à remplacer ce mot de passe par un mot de passe complexe à plusieurs caractères.

Recherche active des menaces

Étant donné que les cybermenaces évoluent constamment, il est important de considérer quelles autres fonctionnalités peuvent être intégrées à votre solution de vidéosurveillance pour vous avertir en cas d'attaque potentielle.

Certains systèmes intègrent des alertes de sécurité et des alarmes. Vous recevrez donc une alerte en cas de tentatives inhabituelles d'accès à l'enregistreur, telles que des échecs de connexion répétés ou une attaque potentielle de déni de service distribué (DDoS).

Le choix d'un fournisseur de vidéosurveillance qui surveille en permanence les vulnérabilités et communique toutes les informations nécessaires est également essentiel afin que les problèmes puissent être résolus avant qu'une attaque ne se produise. Le programme de mises à jour et d'avis de sécurité de March Networks évalue les vulnérabilités, détermine comment elles affectent les produits ou logiciels que vous utilisez et vous alerte afin qu'elles puissent être corrigées.

Pour en savoir plus sur la cybersécurité de la vidéosurveillance, visitez : www.marchnetworks.com/products-services/video-surveillance-cybersecurity/

March Networks® aide les organisations à transformer la vidéo en intelligence commerciale grâce à l'intégration de la vidéosurveillance, d'analyses et de données provenant de systèmes d'entreprise et d'appareils IoT. Des entreprises du monde entier utilisent nos solutions pour améliorer l'efficacité et la conformité, réduire les pertes et les risques, améliorer le service client, et être plus compétitives. Avec une présence établie dans la sécurité vidéo et la mise en réseau, March Networks est également reconnu comme le leader de la gestion vidéo de classe entreprise et des services hébergés.

Amérique du Nord 1 800 563 5564
Amérique du Sud . . . . . +5255 5259 9511
Europe . . . . . +39 0362 17935
Asie . . . . . +65 6818 0963
Australie et Nouvelle Zélande . . . . . +61 1300 089 419
Moyen-Orient et Afrique 971 4 399 5525

marchnetworks.com