VIDÉOSURVEILLANCE

40 % des caméras ont un risque cyber

© Getty images

Une étude réalisée par Genetec révèle que près de quatre caméras de vidéosurveillance sur dix présentent un risque de cybersécurité dû à un micrologiciel obsolète.

Cette étude* montre par ailleurs que jusqu'à 68,4 % des caméras de sécurité d'une entreprise, soit près de sept sur dix, n'ont ainsi pas été mises à jour avec la dernière version disponible de leur micrologiciel.
Lorsqu'on déploie la dernière version d'un micrologiciel, ce n'est pas seulement pour pouvoir profiter de nouvelles fonctionnalités intéressantes, mais également pour bénéficier, dès leur disponibilité, des dernières mesures de protection en matière de cybersécurité – une étape cruciale pour assurer la résilience d'une entreprise face aux cyberattaques.

© DR

« Nos données indiquent que 53,9 des caméras dotées d'un micrologiciel obsolète présentent des vulnérabilités de cybersécurité connues. »

MATHIEU CHEVALIER, LEAD SECURITY ARCHITECT CHEZ GENETEC

Des vulnérabilités de cybersécurité connues

Toujours selon Genetec, près d'une entreprise sur quatre (23 %) n'utilise pas de mots de passe uniques sur ses caméras de sécurité, mais le même mot de passe pour toutes les caméras d'un même fabricant. Il suffit d'une seule caméra compromise pour offrir un point d'accès facile aux pirates informatiques.
Jusqu'à récemment, les caméras IP étaient livrées avec des paramètres de sécurité par défaut, y compris au niveau des informations de connexion administrateur, par ailleurs souvent accessibles au public sur les sites Web des fabricants. La plupart des fabricants de caméras demandent désormais aux utilisateurs de définir de nouveaux mots de passe et identifiants administrateur lors de l'installation. Mais les entreprises, les villes et les institutions gouvernementales disposant d'équipements plus anciens n'ont bien souvent jamais mis à jour leurs mots de passe, compromettant potentiellement les autres données et systèmes critiques qui se trouvent sur leur réseau.

23 %
C'est le pourcentage d'entreprises qui n'utilisent pas de mots de passe uniques sur ses caméras de sécurité.

Une seule caméra suffit...

« Notre étude montre que, malheureusement, l'approche informatique qui consiste à "configurer et oublier" reste répandue, mettant en danger la sécurité de toute une entreprise et la vie privée des individus. Il suffit d'une seule caméra avec un micrologiciel obsolète ou un mot de passe par défaut pour créer une faille dans laquelle un attaquant peut s'engouffrer et compromettre l'ensemble du réseau. Il est essentiel que les entreprises soient aussi proactives dans la mise à jour de leurs systèmes de sécurité physique que dans celle de leurs réseaux informatiques », conclut Mathieu Chevalier, Lead Security Architect chez Genetec. ■

** L'étude a été menée sur un échantillon de 44763 caméras connectées àdes systèmes prenant part au programme facultatif d'amélioration des produits de Genetec.*