NEDIK

Aux membres de l'ASF
Association suisse du froid

Zurich, le 12 novembre 2026

Cyberattaques contre des installations frigorifiques commerciales – informations importantes et mesures immédiates

Mesdames, Messieurs,

Depuis la mi-octobre, des installations frigorifiques commerciales sont la cible d'attaques ciblées via Internet dans plusieurs pays européens et désormais aussi en Suisse. Les attaquants prennent le contrôle de la commande, coupent le refroidissement et font chauffer les installations, parfois bien au-delà de 50 °C. Les conséquences sont des marchandises avariées et des dégâts matériels. De plus en plus de petites entreprises sont également touchées.

La condition préalable à de telles attaques est que la commande de l'installation frigorifique soit accessible via un accès réseau, par exemple depuis Internet. Les attaquants peuvent s'en prendre de manière ciblée aux paramètres du système de commande et les modifier, de sorte que l'installation ne refroidisse plus, mais chauffe.

Mesures recommandées

- Accès Internet et accès à distance : Si l'installation dispose d'un accès réseau ou d'un accès Internet, il convient de vérifier avec la personne responsable technique si la commande peut être déconnectée du réseau jusqu'à nouvel examen. La commande ne doit pas être directement accessible depuis Internet. L'accès à distance aux installations ne devrait se faire que par un accès réseau sécurisé. Si cela n'est pas possible à court terme, déconnectez la commande du réseau jusqu'à ce que vous ayez pris des mesures appropriées. Le refroidissement continue en général de fonctionner localement.
- Données d'accès à l'installation frigorifique : Assurez-vous que l'accès à votre système répond aux standards de sécurité actuels (p. ex. remplacer les mots de passe par défaut, définir des mots de passe individuels et robustes, utiliser si possible l'authentification à deux facteurs et vérifier les accès des prestataires).
- Sécuriser les appareils : Assurez-vous, avec le fabricant ou la personne spécialisée compétente, que votre installation est à jour. Cela comprend l'installation de logiciels à jour, le remplacement des appareils qui ne bénéficient plus du support du fabricant ou leur exploitation dans un réseau distinct et isolé, séparé de l'informatique de bureau. L'installation de mises à jour à elle seule ne suffit pas.
- Garantir une alarme de température indépendante : Définir des seuils et faire passer l'alarme (p. ex. par SMS) par un appareil indépendant de la commande. Une personne responsable doit être joignable et connaître le plan d'urgence (refroidissement de remplacement ou de secours).
- Élaborer un concept de sécurité : Comme de nouvelles vulnérabilités sont régulièrement découvertes, il est important d'élaborer un concept de sécurité avec le spécialiste informatique.

En cas de soupçon d'attaque

Faites immédiatement appel à l'entreprise du froid et au spécialiste informatique, exploitez l'installation manuellement si possible, conservez les traces numériques (journaux, paramètres) et ne réinitialisez pas l'appareil. Signalez immédiatement l'incident à la police : en cas de dommage en cours, via le numéro d'urgence 117, sinon auprès de votre poste de police local.

L'Office fédéral de la cybersécurité (OFCS) a publié un avertissement contenant d'autres mesures de protection : www.bacs.admin.ch/fr/warnung-kuehlanlagen-fr.

Pour d'autres informations sur la cybercriminalité, consultez cybercrimepolice.ch/fr.

Meilleures salutations
Votre police / NEDIK (Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung)