La Cyber-Lettre de la GENDARMERIE RÉGION GRAND EST

Octobre 2026

🔐 Quand les accès des prestataires deviennent une porte d'entrée

DIFFUSION LIBRE

Vous êtes responsable d'une structure professionnelle. Certains de vos équipements sont connectés à Internet afin de permettre à un prestataire externe d'assurer leur maintenance à distance. Tout fonctionne correctement. Un technicien peut surveiller les installations, vérifier certains paramètres et intervenir sans avoir à se déplacer.

Une question se pose : que pourrait faire un cybercriminel qui parviendrait à s'emparer du compte de ce technicien ? 👀 Pourrait-il uniquement accéder au matériel administré à distance ? Pourrait-il également avoir accès à d'autres équipements informatiques ? C'est précisément en s'interrogeant sur ces sujets que débute la réflexion relative aux droits d'accès accordés aux prestataires externes.

Pour intervenir à distance, Ces derniers disposent de comptes spécifiques permettant à leurs techniciens de se connecter aux installations de plusieurs établissements.

La compromission des identifiants d'un technicien par vol de mot de passe expose le système à des risques majeurs. En l'absence d'une gestion stricte des accès, un attaquant peut usurper cette identité pour s'infiltrer dans les équipements autorisés. Un cloisonnement réseau insuffisant peut en outre lui permettre de réaliser des mouvements latéraux vers d'autres environnements critiques.

Par exemple :

- Les équipements électriques ;
- Les systèmes de supervision technique ;
- Certains serveurs ou postes informatiques ;
- D'autres équipements connectés sur un même réseau.

⚠️ **Un accès prévu pour la maintenance peut devenir un point d'entrée pour une cyberattaque.**

🔐 Le principe du moindre privilège. Chaque utilisateur doit disposer uniquement des droits nécessaires à l'exécution de sa mission.

→ Vous ne donnez pas le code d'accès à votre coffre fort au technicien qui vient réviser votre chaudière…

Prenons trois exemples :

🔴 Situation à risque : Un technicien chargé de la maintenance d'un équipement donné dispose également de droits d'administration sur l'ensemble du réseau de la structure.

🟠 Situation à surveiller : Un prestataire conserve ses accès après la fin de son contrat ou après le départ d'un de ses techniciens.

🟢 Bonne pratique : Le prestataire dispose d'un compte nominatif, limité aux équipements concernés. Son accès est sécurisé, cloisonné, surveillé et désactivé lorsqu'il n'est plus nécessaire.

Un prestataire doit pouvoir effectuer son travail correctement sans être pour cela autorisé à avoir accès à l'ensemble du réseau informatique de son client.

👀 COMMENT RECONNAÎTRE LES RISQUES ?

Lorsqu'un prestataire intervient dans votre entreprise, posez-vous les bonnes questions :

🔎 Qui possède un accès à distance à mes équipements ?
🔎 Les comptes sont-ils individuels ou partagés entre plusieurs techniciens ?
🔎 Les droits accordés sont-ils limités à la mission confiée ?
🔎 Un compte prestataire peut-il accéder à d'autres réseaux ou équipements ?
🔎 Les connexions sont-elles protégées par une authentification multi-facteurs (MFA) ?
🔎 Les accès sont-ils supprimés à la fin du contrat ?
🔎 Qui contrôle les opérations réalisées à distance ?
💡 **Si vous n'avez pas les réponses à ces questions, il est temps de faire le point sur vos accès.**

🛡️ LES BONS RÉFLEXES

✅ 1. Recensez les accès. Identifiez tous les prestataires disposant d'un accès à vos systèmes.
✅ 2. Limitez les droits. Accordez uniquement les autorisations nécessaires à chaque intervention.
✅ 3. Cloisonnez les réseaux. Séparez les équipements techniques des serveurs et du réseau global.
✅ 4. Sécurisez les connexions. Privilégiez les comptes nominatifs, l'authentification multi-facteurs et les solutions d'accès distantes sécurisées.
✅ 5. Limitez la durée des accès. Vérifiez et désactivez les comptes qui ne sont plus nécessaires.
✅ 6. Contrôlez régulièrement les habilitations. Vérifiez les droits après un changement de prestataire ou le départ d'un intervenant.
✅ 7. Surveillez les connexions. Conservez les journaux permettant d'identifier les accès et les opérations inhabituelles.

+ D' INFO

Vous êtes victime ?

Appelez immédiatement le 📞**17** ou 💻 contacter :

LE 17 CYBER

Une cyberattaque, échangez avec un cybergendarme - 24h/24 7j/7
https://17cyber.gouv.fr/

LA BRIGADE NUMÉRIQUE

Échangez avec un gendarme 24h/24 7j/7

LA CNIL

Prévenir en cas de fuite de données personnelles, réelle ou supposée.

CYBERMALVEILLANCE

Pour vous faire assister, vous informer ou vous former
www.cybermalveillance.gouv.fr

GRAND EST CYBERSECURITE

Assistance cyberattaque gratuite
Tel : 0 970 512 525
www.cybersecurite.grandest.fr

L'ANSSI

Assiste les entités essentielles et les entités importantes, fournit des guides
https://cyber.gouv.fr

THÉSÉE

Déposer plainte en ligne pour les victimes d'e-escroqueries

APPLICATION MA SÉCURITÉ

Trouver des informations de prévention et les démarches en ligne.



Vous souhaitez joindre un Référent Cyber
de la Région de Gendarmerie du Grand-Est
prevention-ggdXX@gendarmerie.interieur.gouv.fr
(Remplacez les XX par votre département)

01010010 01001001 01010011 01000011 01001000