

VPN et accès distants : ouvrir sans exposer

RDP, VPN, prise en main à distance : chaque porte ouverte vers l'intérieur doit être blindée. Le mode d'emploi.

10 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/vpn-acces-distant

Télétravail, maintenance, multi-sites : l'entreprise moderne a besoin d'accès distants. Mais chaque porte ouverte vers l'intérieur du réseau est aussi une porte pour les attaquants — les accès distants mal protégés sont, avec le phishing, la première cause d'intrusion en PME. Ce guide passe en revue les types d'accès, leurs pièges et la manière de les ouvrir proprement.

1. Les trois familles d'accès distant

Le VPN : le tunnel chiffré

Le VPN d'entreprise crée un tunnel chiffré entre le poste distant et votre réseau : l'utilisateur travaille comme s'il était au bureau. C'est la solution de référence — à condition d'être à jour (les failles de VPN sont massivement exploitées), protégée par MFA, et limitée : chaque utilisateur n'accède qu'aux ressources dont il a besoin, pas à tout le réseau.

Le bureau à distance (RDP)

RDP permet de prendre la main sur un poste ou un serveur Windows. Exposé directement sur Internet, c'est l'erreur la plus exploitée qui soit : des robots testent en permanence des millions de mots de passe sur les ports RDP ouverts. La règle est simple et sans exception : jamais de RDP accessible depuis Internet — toujours derrière un VPN.

Les outils de prise en main (TeamViewer, AnyDesk...)

Pratiques pour le dépannage, ils deviennent dangereux installés en accès permanent non surveillé : compte du prestataire compromis = accès direct à vos postes. À encadrer : version à jour, mot de passe fort + MFA sur le compte, accès sur demande plutôt que permanent, et liste tenue à jour de qui peut se connecter à quoi.

ATTENTION

Les faux dépanneurs exploitent ces mêmes outils : un appel « du support Microsoft » ou « de votre banque » vous fait installer AnyDesk, et l'escroc vide le compte sous vos yeux. Aucun support légitime ne vous appelle spontanément pour prendre la main sur votre machine. On raccroche.

2. Le socle non négociable

- MFA sur tous les accès distants, sans exception — la mesure qui neutralise l'essentiel des attaques par identifiants volés
- Équipements d'accès (pare-feu, VPN) à jour en priorité absolue : exposés à Internet, leurs failles sont exploitées en heures
- Comptes nominatifs et journaux de connexion conservés : qui s'est connecté, quand, d'où

- Moindre privilège : le VPN du comptable ouvre la compta, pas les serveurs
- Coupure automatique des sessions inactives et blocage après échecs répétés
- Revue régulière : chaque accès distant qui ne sert plus se ferme

3. Les prestataires : vos accès distants les plus sensibles

L'accès de maintenance de votre prestataire (informatique, photocopieur, caisse, chauffage...) est un accès distant comme un autre — souvent avec des droits élevés, et hors de votre vue.

- Recenser tous les accès prestataires existants — il y en a toujours plus qu'on ne croit
- Un compte dédié par prestataire, jamais de compte administrateur partagé
- MFA imposée contractuellement, et accès activé à la demande quand c'est possible
- Couper l'accès à la fin du contrat — le classique oublié

4. Aller plus loin : vers le « zero trust »

Le modèle traditionnel « une fois dans le réseau, on est de confiance » vieillit mal : un seul poste compromis contamine tout. L'approche moderne — dite zero trust — vérifie chaque accès à chaque ressource (identité + état du poste + contexte), au lieu d'ouvrir grand le réseau. Concrètement, pour une PME, cela commence par des briques simples : applications publiées individuellement plutôt que VPN « tout réseau », SSO avec MFA, et vérification de l'état de santé du poste avant connexion. C'est la direction que prennent les outils grand public professionnels (Microsoft Entra, solutions ZTNA).

L'essentiel à retenir

- 01 Activer la MFA sur tous les accès distants, VPN compris
- 02 Ne jamais exposer RDP directement sur Internet
- 03 Mettre à jour pare-feu et VPN en priorité absolue
- 04 Encadrer les outils de prise en main à distance (MFA, accès sur demande)
- 05 Recenser et limiter les accès des prestataires, les couper en fin de contrat
- 06 Conserver et consulter les journaux de connexion

Questions fréquentes

Le VPN ralentit le travail à distance. Des solutions ?

Souvent, le goulot est le débit montant de la connexion du bureau, ou un VPN qui fait transiter TOUT le trafic (y compris YouTube) par l'entreprise. Les réponses : le « split tunneling » bien configuré (seul le trafic professionnel passe par le tunnel), un lien Internet adapté au nombre de télétravailleurs, ou la bascule des outils vers le cloud — qui supprime le besoin de VPN pour ces usages.

Un VPN grand public (NordVPN...) protège-t-il l'entreprise ?

Non — ce n'est pas le même objet : ces services chiffrent votre navigation vers Internet (utile sur un Wi-Fi public), mais ne donnent aucun accès à votre réseau d'entreprise et n'apportent aucun contrôle à l'employeur. L'accès aux ressources internes passe par un VPN d'entreprise que vous administrez.

Comment savoir si notre RDP est exposé sur Internet ?

Votre prestataire le vérifie en quelques minutes (scan de vos adresses IP publiques, port 3389 et voisins). Des services comme Shodan montrent ce que les attaquants voient de vous. Si un RDP exposé est découvert : fermeture immédiate, bascule derrière VPN, et vérification des journaux — il a probablement déjà été testé.

Faut-il autoriser l'accès distant depuis les appareils personnels ?

Le moins possible : un poste que vous ne maîtrisez pas (mises à jour ? antivirus ? qui d'autre l'utilise ?) devient le maillon faible du tunnel. Si c'est inévitable, limitez au strict nécessaire via des applications publiées ou un bureau virtuel, sans montage des lecteurs ni copie de fichiers locaux.

Pour aller plus loin

ANSSI — recommandations sur le nomadisme numérique — cyber.gouv.fr/publications/recommandations-sur-le-nomadisme-numerique

Cybermalveillance.gouv.fr — sécuriser le télétravail — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-teletravail

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr