



CHECKLIST

Sécuriser le télétravail et les accès distants

La checklist pour fermer les portes d'entrée les plus exploitées : RDP exposé, VPN non protégés, MFA absent, postes et réseaux domestiques.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~11 min Édition 2026 sedona-ai.com

Le télétravail n'est pas un risque en soi : le risque, c'est l'accès distant mal configuré. Un poste RDP laissé ouvert sur Internet, un VPN sans double authentification, un ordinateur familial partagé — voilà les portes que les attaquants ouvrent en premier. Cette checklist réunit les recommandations de l'ANSSI, de Cybermalveillance.gouv.fr et de la CISA en un plan d'action clair pour dirigeants de PME et ETI. Objectif : verrouiller vos accès distants sans freiner vos équipes.

À retenir

- Ne jamais exposer le RDP (port 3389) directement sur Internet : le faire transiter par un VPN, un bureau virtuel (VDI) ou une passerelle, avec authentification préalable.
- Le MFA est la mesure de référence sur tous les accès distants (VPN, RDP, messagerie) — privilégier le MFA résistant au phishing (clés FIDO2) sur les comptes critiques.
- Les équipements d'accès distant en périphérie (VPN, passerelles) sont devenus une cible majeure : leur exploitation via vulnérabilité pèse 22 % des compromissions par ce vecteur, contre ~3 % un an plus tôt (Verizon DBIR 2025).
- Séparer strictement usages pro et perso : pas de messagerie personnelle sur le poste pro, pas de données pro sur un appareil personnel.
- Maintenir VPN, passerelles et postes à jour des correctifs, déployer un antivirus professionnel et centraliser la journalisation.
- La première étape concrète : savoir ce qui est réellement exposé sur Internet à votre nom — un scan de surface révèle les services (dont RDP) visibles depuis l'extérieur.

01 Pourquoi le télétravail élargit votre surface d'attaque

Le travail à distance déporte vos accès hors du périmètre maîtrisé de l'entreprise : réseaux domestiques, ordinateurs partagés, connexions ouvertes vers votre système d'information. Chaque accès distant mal protégé devient une porte d'entrée. Les attaquants l'ont compris et ciblent désormais massivement les équipements qui rendent le télétravail possible.

22 %

des compromissions par exploitation de vulnérabilité visent les équipements d'accès distant en périphérie (VPN, passerelles), contre environ 3 % l'année précédente — une multiplication par huit.

Verizon, 2025 Data Breach Investigations Report (DBIR)

Deux vecteurs d'entrée dominant

Selon le Verizon DBIR 2025, l'abus d'identifiants reste le premier vecteur d'accès initial aux violations, devant l'exploitation de vulnérabilités (environ 20 % des vecteurs). Traduction concrète : protéger vos identifiants (MFA) et corriger vos accès distants exposés couvre l'essentiel du risque télétravail.

02 Accès distants : bannir le RDP exposé sur Internet

Le RDP (Remote Desktop Protocol, port 3389) est l'un des services les plus ciblés lorsqu'il est directement accessible depuis Internet. La règle, partagée par l'ANSSI et la CISA, est sans ambiguïté : ne jamais l'exposer en direct. Il doit transiter par un tunnel authentifié. Attention : il ne s'agit pas d'interdire le RDP, mais de le protéger derrière un accès contrôlé.

Pratique	Verdict	Recommandation ANSSI / CISA
RDP (port 3389) exposé directement sur Internet	À proscrire	Ne jamais exposer en direct : faire transiter par VPN, bureau virtuel (VDI) ou passerelle d'accès distant, avec authentification préalable avant tout accès au poste interne.
RDP accessible via VPN ou VDI	Acceptable si durci	Authentifier l'utilisateur avant l'ouverture de session ; activer la Network Level Authentication (NLA), qui vérifie l'identité avant l'établissement complet de la session.
RDP en usage interne uniquement	Toléré	Restreindre les sources autorisées, exiger le MFA sur les comptes concernés, maintenir les postes à jour.

Les rançongiciels adorent les services exposés

Une part significative des rançongiciels traités par Cybermalveillance.gouv.fr provient de l'exploitation de failles sur des accès exposés sur Internet — RDP, VPN, NAS. Fermer ces portes est la mesure de prévention la plus rentable.

03 MFA partout, résistant au phishing sur les accès critiques

L'authentification multifacteur (MFA) est la mesure de référence pour protéger les accès distants. La CISA recommande de l'appliquer sur toutes les connexions VPN et sur le RDP. Sur les comptes les plus sensibles, visez un MFA résistant au phishing (clés physiques FIDO2/U2F) : les codes reçus par SMS sont désormais jugés insuffisants face aux attaques d'hameçonnage modernes.

- ☐ MFA activé sur toutes les connexions VPN et tous les accès distants (RDP, messagerie, outils SaaS métier).
- ☐ MFA résistant au phishing (clés FIDO2/U2F) déployé sur les comptes à privilèges et les accès les plus critiques.
- ☐ À défaut de MFA sur un VPN, mots de passe d'au moins 15 caractères pour les télétravailleurs — mesure d'appoint, jamais un équivalent au MFA (recommandation CISA).
- ☐ OTP par SMS évité comme facteur unique de secours sur les accès sensibles.
- ☐ Procédure de récupération de compte elle-même protégée (pas de contournement du MFA par un simple e-mail).

04 Sécuriser les postes et les réseaux domestiques

Le poste de travail à distance et le réseau depuis lequel il se connecte échappent au contrôle du bureau. On les ramène dans le périmètre par des mesures simples et systématiques, en s'appuyant sur des équipements maîtrisés par l'entreprise plutôt que sur le matériel personnel.

- ☐ Postes fournis et administrés par l'entreprise, chiffrement du disque activé, verrouillage automatique de session.
- ☐ Antivirus professionnel déployé sur tous les postes de télétravail (recommandation Cybermalveillance.gouv.fr).
- ☐ Connexions systématiquement établies via VPN (ou solution d'accès équivalente) vers le système d'information.
- ☐ Correctifs de sécurité appliqués sans délai sur les postes, les VPN et les équipements réseau (recommandation CISA).
- ☐ Box domestique durcie : mot de passe d'administration modifié, Wi-Fi en WPA2/WPA3, firmware à jour.
- ☐ Sauvegardes des données professionnelles hors du poste, testées régulièrement.

Le réseau public : jamais sans tunnel

Gare, hôtel, café : sur un réseau non maîtrisé, aucune connexion professionnelle sans VPN actif. Sécuriser les flux générés par le travail à distance est l'un des grands volets du guide ANSSI sur le nomadisme numérique.

05 Cloisonner les usages et traiter à part les comptes à privilèges

Le mélange des usages est une source majeure d'incidents : un e-mail personnel piégé ouvert sur le poste pro, un fichier professionnel copié sur un ordinateur familial. La séparation stricte, recommandée par Cybermalveillance.gouv.fr, limite fortement la propagation d'une compromission.

- ☐ Pas de messagerie ou de navigation personnelle sur le poste professionnel.
- ☐ Pas de stockage de données professionnelles sur un équipement personnel (clé USB, ordinateur familial, cloud perso).
- ☐ Comptes à privilèges (administrateurs, comptes techniques) traités à part : accès dédié, MFA renforcé, jamais utilisés pour la bureautique courante.

- ☐ Droits accordés au strict nécessaire (moindre privilège), revus régulièrement — notamment aux départs.
- ☐ Comptes inactifs et accès temporaires désactivés sans délai.

06 Sensibiliser, journaliser, superviser

La technique ne suffit pas : l'hameçonnage vise directement vos collaborateurs à distance, moins entourés qu'au bureau. En parallèle, la journalisation centralisée permet de détecter une intrusion et d'en comprendre le déroulé — indispensable en cas d'incident.

- ☐ Sensibilisation régulière au phishing et aux réflexes en télétravail (que faire en cas de doute, qui alerter).
- ☐ Procédure claire de signalement d'un incident, connue de tous et accessible à distance.
- ☐ Journalisation des accès distants (VPN, RDP, authentications) centralisée et conservée.
- ☐ Supervision des connexions : alertes sur les accès anormaux (horaires, géographie, échecs répétés).
- ☐ Test régulier de la réaction : une simulation d'hameçonnage mesure la vigilance réelle des équipes.

07 Le cadre de référence : ANSSI et CISA

Deux référentiels structurent la sécurisation du télétravail. Le guide ANSSI « Recommandations sur le nomadisme numérique » (version 2.0, novembre 2023) aborde trois grands volets : la gestion des accès distants, le contrôle des flux de données et la sécurisation des équipements de connexion. Il est accompagné d'un outil d'aide à la priorisation, OASIS. Le guide #StopRansomware de la CISA détaille, lui, les mesures sur le RDP, le VPN et le MFA.

Des recommandations, pas une obligation

L'ANSSI précise que le guide sur le nomadisme numérique n'a pas de valeur normative : ce sont des recommandations, pas une contrainte réglementaire. Elles restent la meilleure boussole pour prioriser vos efforts.

08 Vérifier ce qui est réellement exposé

Toutes ces mesures supposent de savoir ce qui est visible depuis l'extérieur à votre nom. Un RDP oublié, un VPN obsolète, un service de test laissé ouvert : ces angles morts ne se voient pas de l'intérieur. Sedona Radar analyse ce que votre domaine expose sur Internet et recense les services

accessibles — dont le RDP, dans le détail inclus dès le plan Starter — pour transformer cette checklist en plan d'action.

Commencez par un état des lieux

Le plan Discovery de Sedona Radar offre un scan gratuit (un scan à vie), qui compte en 45 minutes environ (médiane mesurée) les ports ouverts du domaine que vous indiquez ; le détail (RDP, VPN...) est inclus dès le plan Starter. C'est le point de départ le plus rapide pour repérer les portes ouvertes.

§ Sources

1. ANSSI — Recommandations sur le nomadisme numérique (guide télétravail/mobilité) — <https://cyber.gouv.fr/publications/recommandations-sur-le-nomadisme-numerique>
2. cyber.gouv.fr — Guide nomadisme numérique (miroir messervices) — <https://messervices.cyber.gouv.fr/guides/recommandations-sur-le-nomadisme-numerique>
3. Cybermalveillance.gouv.fr — Recommandations de sécurité informatique pour le télétravail — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail>
4. Cybermalveillance.gouv.fr — Rançongiciels : fiche réflexe — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiels-ransomwares>
5. CERT-FR (ANSSI) — Panorama de la cybermenace 2025 — <https://www.cert.ssi.gouv.fr/cti/CERTFR-2026-CTI-002/>
6. CISA — #StopRansomware Guide — <https://www.cisa.gov/stopransomware/ransomware-guide>
7. Verizon — 2025 Data Breach Investigations Report (DBIR) — <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>
8. Shodan Blog — Trends in Internet Exposure (RDP exposé) — <https://blog.shodan.io/trends-in-internet-exposure/>

Quels services exposez-vous sans le savoir ?

Le scan gratuit de Sedona Radar compte les ports ouverts de votre domaine ; le détail (RDP, VPN...) est inclus dès le plan Starter. Un état des lieux clair pour prioriser cette checklist.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit