GUIDE DU TÉLÉTRAVAIL À DESTINATION DES PME

Administrateur informatique : nos conseils pour vous aider à sécuriser le travail des employés à distance

Alors que la pandémie actuelle de COVID-19 fait rage et force bon nombre d'employés à travailler de chez eux, une question subsiste : votre entreprise peut-elle rester à la fois productive ET protégée ? De nombreuses grandes sociétés telles que Google et Microsoft ont adopté cette transition sans trop de heurts. Toutefois, pour des PME, la situation s'avère parfois tout à fait différente.

Le télétravail n'est malheureusement pas l'affaire de tous et ne peut être envisagé que par une petite partie d'entre nous. De manière plus pragmatique, il concerne avant tout les échanges par messagerie électronique et d'autres tâches non-opérationnelles. Il semble donc primordial de vous assurer que vos infrastructures et politiques informatiques soient correctement paramétrées pour assurer la continuité de vos services.

Pré-requis

Voici les exigences les plus élémentaires et incontournables dont les employés auront besoin à distance pour rester productifs :

- Un ordinateur
- Une connexion Internet efficace
- Des applications de visioconférence et de discussion
- Un coin bureau dédié (si possible)
- En option, un téléphone
- De la discipline et de la motivation intérieure
- Une routine stricte

En plus de leur configuration habituelle, les entreprises et organisations doivent également se préparer, avec leurs employés, **à une augmentation des menaces en matière de cybersécurité** liées au travail à distance.

Quels sont les principaux défis à relever en la matière ?

1. La sécurité matérielle des appareils de l'entreprise
2. La sécurité informatique de l'entreprise depuis le domicile des employés
3. L'environnement technologique domestique
4. L'accès au réseau et aux systèmes de l'entreprise
5. Les outils collaboratifs et les méthodes d'autorisation
6. L'entraînement à la cybersécurité
7. La gestion de crise

1 La sécurité matérielle des appareils de l'entreprise

Les employés exposent davantage les appareils de l'entreprise à des risques lorsque ceux-ci sont utilisés en dehors des bureaux. Ces derniers doivent donc impérativement être protégés contre les vols et les pertes. Voici quelques astuces et conseils pour vous aider à sécuriser tous les outils de l'entreprise.

- **Déconnectez-vous systématiquement** —lorsque vous n'utilisez pas votre matériel, que vous soyez chez vous ou à l'extérieur. Cela vous évitera par exemple un e-mail envoyé inopinément par votre enfant à votre directeur ou à un client lorsque vous avez le dos tourné.
- **Optez pour une politique de mot de passe intransigeante** — définissez des délais d'inactivité et interdisez les mots de passe sur les posts-it ! (Car oui, les gens continuent de faire ce genre de choses)
- **Ne laissez jamais l'appareil sous surveillance** ou exposé publiquement. Si vous le mettez dans votre voiture, alors il doit être rangé dans le coffre !

NOTRE CONSEIL :

Full-disk encryption simple mais très efficace qui vous permet de chiffrer en un clin d'œil les données de l'entreprise dans le cas où un appareil tomberait entre de mauvaises mains.

2 La sécurité informatique de l'entreprise depuis le domicile des employés

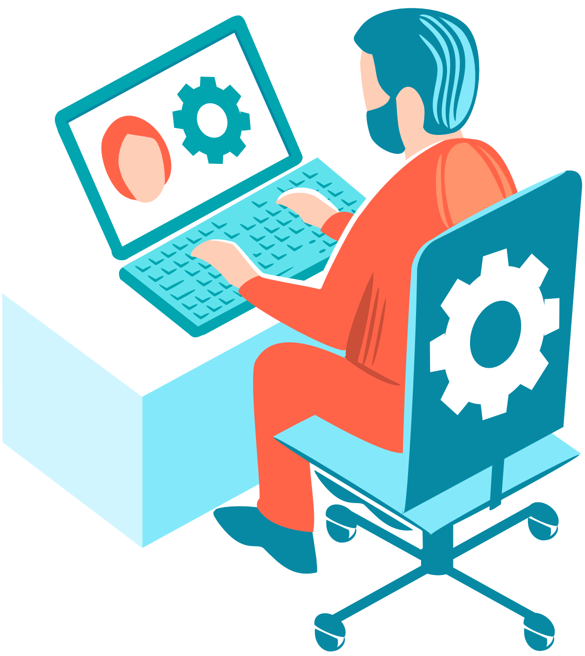
Maintenant que vos employés sont seuls chez eux, votre visibilité quant à ce qui se déroule sur leur ordinateur est très limitée et ce d'autant plus si vous n'êtes pas habitués à administrer des appareils à distance.
C'est donc précisément le moment pour en apprendre davantage sur les bénéfices d'une administration à distance et ainsi diminuer drastiquement le nombre de problèmes informatiques à solutionner.

L'utilisation de l'administration à distance vous fera gagner du temps :

- Configurez et maintenez très simplement tous les systèmes à jour. En une seule fois, sans avoir besoin de passer d'un appareil à l'autre !
- Programmez des tâches, définissez des politiques et exécutez-les selon les groupes d'employés
- Recevez des notifications en temps réel au sujet d'incidents et intervenez immédiatement lorsque le problème apparaît.

NOTRE CONSEIL :

Si vous possédez jusqu'à 250 appareils, vous pouvez très facilement administrer votre parc d'ordinateurs grâce à la console cloud-based. Son activation se fait en quelques minutes seulement.



3 L'environnement technologique domestique

Demandez aux employés de vérifier leur environnement technologique domestique avant d'y connecter leurs outils de travail, afin d'identifier d'éventuelles vulnérabilités. Il existe des failles au sujet de l'Internet des Objets (IdO ou IoT en anglais), c'est donc le moment idéal pour les salariés de prendre des mesures pour sécuriser ces appareils à l'aide de mots de passe robustes mais aussi de mettre à jour tous leurs logiciels vers les dernières versions existantes.

Vous pouvez également suggérer (voire obliger) vos effectifs à utiliser une application de gestion et de surveillance domestique avant qu'ils ne connectent leurs outils professionnels sur leur réseau personnel. L'analyse ou le monitoring mettra ainsi en évidence les appareils possédant des vulnérabilités, des logiciels qui n'auraient pas été mis à jour ou des mots de passe par défaut qui doivent être modifiés.

4 L'accès au réseau et aux systèmes de l'entreprise

Déterminez si vos employés ont besoin d'accéder au réseau interne de l'entreprise ou si un accès aux services sur le cloud et à la messagerie électronique est suffisant. À vous également de définir si l'employé pourra obtenir, de chez lui, le même accès aux données sensibles que depuis son poste de travail officiel.

Si l'accès au réseau interne de l'entreprise est nécessaire :

- Il est fortement recommandé d'utiliser uniquement les appareils propriétaires de l'entreprise, de manière à ce que chaque outil soit administré par l'équipe informatique et bénéficie d'une technologie de sécurité.
- **Utilisez toujours un VPN pour que les employés puissent se connecter à distance** au réseau interne de l'entreprise. Cela permettra d'éviter les attaques dites de "l'homme du milieu" depuis des emplacements distants. Gardez en tête qu'avec le télétravail, bon nombre de données circulent sur les réseaux publics.
- **Contrôlez l'utilisation des périphériques externes** tels que les outils USB et appareils amovibles.
- Beaucoup de gens travaillent de chez eux et deviennent ainsi des cibles idéales d'hameçonnage ou d'arnaques par e-mails. **Vous pouvez garder les ordinateurs de vos employés à l'abri de ce type de cyberattaques** grâce aux solutions de cloud-sandboxing.
- Limitez les possibilités de stockage, de téléchargement ou de copie de données. Une violation de données peut survenir depuis n'importe quel ordinateur contenant des données sensibles de l'entreprise.
- Envisagez l'utilisation de machines virtuelles pour fournir un accès. Cela peut s'avérer plus difficile à mettre en place mais c'est une solution efficace sur le long terme.

Dans le cas où certains (ou tous vos) employés utiliseraient leur propre ordinateur pour accéder à leur messagerie électronique ou aux services cloud, assurez-vous que la politique de sécurité appliquée soit la même que s'il s'agissait d'un appareil de l'entreprise et ce notamment en termes de solution anti-malware, pare-feu, etc. **Si nécessaire, vous pouvez fournir une solution de sécurité identique à celle utilisée sur les ordinateurs de l'entreprise.** En cas de besoin concernant des licences supplémentaires, contactez votre éditeur de sécurité : il est fort probable qu'il ait déjà envisagé une solution adéquate pour répondre à l'urgence de la situation.

NOTRE CONSEIL

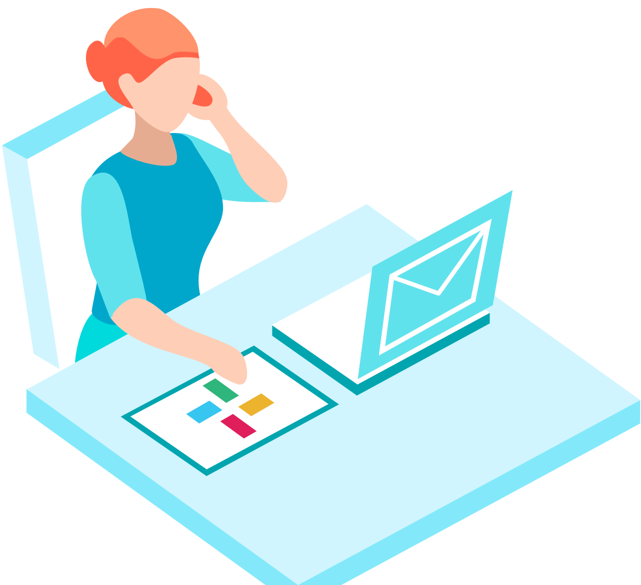
L'authentification multifacteur (MFA) permet de vous assurer que l'accès, qu'il soit à destination des services du cloud ou à l'ensemble du réseau interne, n'est possible que pour les utilisateurs autorisés. Dans la mesure du possible, utilisez un système basé sur une application ou un jeton d'authentification en vue de générer des codes à usage unique qui autoriseront l'accès.

5 Les outils collaboratifs et les méthodes d'autorisation

Il peut sembler étrange de rassembler ces deux sujets sous le même paragraphe, toutefois l'un peut véritablement vous aider à protéger l'autre d'éventuels problèmes.

- Fournissez un accès aux discussions et visioconférences de manière à ce que les employés puissent communiquer entre eux. Cela leur permettra d'avoir des outils utiles à leur disposition et surtout de garder un lien social avec leurs collègues.
- Utilisez les outils collaboratifs pour protéger les employés des instructions ou transactions malveillantes. Les cybercriminels profiteront certainement du fait que les effectifs soient en télétravail pour tenter des attaques BEC (Business Email Compromise) Ce type de procédé consiste à envoyer une fausse demande à traiter en urgence par l'employé au sujet d'un transfert d'argent. Du fait de la distance, le salarié ne peut pas faire valider la demande en "face-à-face" à son responsable.

Assurez-vous donc d'utiliser les systèmes de discussion instantanée ou de vidéoconférence comme étape officielle de validation "en personne", même à distance !



6 L'entraînement à la cybersécurité

Nous avons déjà identifié de nombreuses arnaques ayant pour sujet le COVID-19, dont notamment des fausses informations, des escroqueries au sujet de vaccins ou même de masques. Lorsque les employés travaillent depuis leur domicile, la tentation peut être plus grande pour eux de cliquer sur un lien ou de regarder une vidéo car ils ne sont pas soumis aux regards des autres collègues.

NOTRE CONSEIL :

Une formation à la sensibilisation sur la cybersécurité devrait être une obligation annuelle pour chaque employé. Avec la situation actuelle, il pourrait être intéressant de mettre en place un apprentissage sur-mesure destiné aux salariés, à suivre de manière obligatoire.

7 La gestion de crise

Malgré l'urgence de fournir un accès distant, ne sacrifiez pas la cybersécurité ni même la capacité de gérer les systèmes et appareils. La possibilité d'aider les utilisateurs à distance est essentielle pour vous assurer des opérations fluides et sans heurts, en particulier si les utilisateurs sont mis en quarantaine pour des raisons de santé. Les salariés en télétravail doivent disposer de protocoles de communication clairs pour obtenir de l'aide du support informatique ou pour une gestion de crise. Ce peut être le cas si par exemple, ils rencontrent des problèmes inhabituels qui pourraient être liés à une violation de données.

Nous avons tendance à penser qu'en un claquement de doigt, n'importe quel employé saura s'adapter efficacement au travail à distance. Or l'apprentissage du télétravail ne va pas de soi et il est fort probable que vos employés aient besoin non seulement d'un temps d'adaptation, mais aussi et surtout de directives et d'aide.

ESET peut vous aider !

Sécuriser le travail à distance et les défis qui en découlent sont des sujets sur lesquels ESET peut vous épauler. Voici quelques-unes de nos solutions qui vous aideront à protéger votre entreprise sans rogner sur la productivité en ces temps incertains.

Administration à distance

ESET Cloud Administrator

Solution de sécurité gérée depuis le cloud pour une capacité maximale de 250 postes. Elle permet de gagner du temps, d'économiser du budget et de simplifier la protection de votre réseau.

- Installation et déploiement en quelques minutes
- Aucune installation de matériel ou de logiciel supplémentaire
- Accès centralisé à la gestion de sécurité du réseau
- Accessible en toute sécurité depuis n'importe où via un navigateur web

Découvrez cette solution dès maintenant !

Protection des appareils

ESET Endpoint Protection

Technologie de sécurité multicouche, apprentissage automatique et expertise humaine, associés à une gestion automatisée de la sécurité.

- Protection simple à exécuter avec une gestion à distance basée sur le cloud
- Technologie efficace pour protéger des attaques ciblées, de celles sans fichier et des ransomwares
- Module Full Disk Encryption

Découvrez cette solution dès maintenant !

Accès sécurisé

ESET Secure Authentication

Une façon simple et efficace pour les entreprises de toutes tailles d'implémenter l'authentification multifacteur sur les systèmes les plus couramment utilisés. Cette technologie vous permet notamment de :

- Prévenir les violations de données
- Répondre aux exigences du RGPD
- Administrer centralement la solution depuis votre navigateur
- Utiliser votre téléphone ou des tokens d'authentification (HW tokens)

Découvrez cette solution dès maintenant !

Pour plus d'informations sur nos solutions de travail à distance, rendez-vous sur notre PAGE WEB dédiée