Dr.WEB®
Depuis 1992

PROTÉGEZ VOTRE UNIVERS

Sécurité et télétravail

pour assurer la sécurité
de l'information lors du passage
des employés au télétravail

Passez ce document à votre administrateur système

Liste des tâches assurant la sécurité de l'information lors du passage des employés au travail à distance

Avant de procéder au télétravail :

Action	Statut
Préparez une liste des logiciels recommandés à installer sur les ordinateurs des employés, et faites-la approuver par la direction. Portez-le à la connaissance de chaque employé qui va travailler à distance.	
Préparez les packages d'installation des produits recommandés pour les employés et mettez-les dans un emplacement accessible avec des marches à suivre relatives à leur installation, ainsi que les configurations recommandées et les listes de plugins. Assurez-vous que les programmes sont téléchargés, installés et configurés correctement.	
Recommandez aux employés d'utiliser des mots de passe forts, si besoin, aidez-les à choisir ou modifier leurs mots de passe.	
Recommandez aux employés d'installer les mises à jour de sécurité pour les OS utilisés ainsi que pour les applications, aidez-les si nécessaire. Vérifiez si la tâche est accomplie.	
Assurez-vous que les services de l'entreprise sont accessibles en dehors du bureau. Vérifiez si la connexion est bonne pour que vos employés puissent faire du télétravail.	
Réduisez au minimum le nombre de services disponibles en dehors des bureaux de l'entreprise. Il est à noter que chacun d'entre eux est une éventuelle cible d'attaque. Si possible, désactivez les processus opérationnels non sécurisés, ceux que vous pouvez temporairement abandonner. Effectuez une analyse de vos ressources à la recherche de vulnérabilités, préparez-vous à des attaques DDoS.	
Si vous n'êtes pas sûr que tous les employés respectent les mesures de sécurité adoptées, évitez qu'ils manipulent des données sensibles afin de minimiser les risques.	
Pour éviter de recevoir et envoyer des messages infectés, faites en sorte que vos employés puissent utiliser le serveur de messagerie de l'entreprise.	
Assurez une analyse antivirus du courrier au niveau du serveur de messagerie à la recherche de programmes malveillants et de spams.	
Installez les outils de protection sur les dispositifs de télétravail - un antivirus, un antispam, un pare-feu, un outil de restriction d'accès aux ressources non sécurisées. Si l'installation et la configuration distantes des outils de protection n'est pas possible, donnez à vos employés des packages d'installation des outils de protection, des clés de licence appropriées et donnez-leur des instructions sur l'installation et la configuration recommandée.	
Suggérez aux employés de mettre à jour le firmware de leur routeur à domicile.	
Les paramètres de l'antivirus doivent exclure la possibilité de leur modification (par exemple, par les membres de la famille). Expliquez aux employés comment configurer l'antivirus et vérifiez si la tâche est accomplie.	

Recommandez aux employés d'utiliser leurs ordinateurs via un compte utilisateur et non pas sous un compte administrateur. Expliquez-leur les risques liés à l'utilisation des droits administrateur. Recommandez-leur également d'utiliser un compte séparé pour le traitement des documents d'entreprise.	
Configurez les restrictions du composant Office Control pour les comptes utilisés par les employés afin d'exclure l'accès aux ressources malveillantes.	

Lorsque vous installez une protection antivirus sur les dispositifs du personnel

La protection antivirus des ordinateurs et des périphériques qui sont utilisés pour le télétravail et auxquels des personnes tierces peuvent accéder (membres de la famille etc.) peut être assurée par des versions monoposte des produits antivirus Dr.Web sans la gestion centralisée, ainsi qu'avec le système de gestion centralisée de la protection antivirus.

L'utilisation de la protection gérée de manière centralisée comporte moins de risques pour l'entreprise puisque dans ce cas, l'employé et les personnes ayant un accès à son PC ou son mobile, par défaut, n'ont pas de possibilité de désactiver les outils de protection ou bien de modifier leur configuration. Ceci protège contre le piratage du réseau d'entreprise et contre le vol de données.

- Si pour protéger les employés qui font du télétravail vous utilisez des solutions sans la gestion centralisée :

Action	Statut
Donnez aux employés le nombre de licences ou de fichiers clés nécessaires à leur travail et fournissez-leur un accès aux packages d'installation nécessaires s'ils effectuent eux-mêmes l'installation.	
Avant d'installer la protection antivirus, il est recommandé d'effectuer une analyse antivirus avec la version actuelle de Dr.Web CureIt!	
Vérifiez la disponibilité les droits administrateur pour installer l'antivirus.	
Avant l'installation de la protection antivirus, désinstallez les solutions d'autres éditeurs si elles ont été précédemment installées sur les machines en question.	
Déployez un système de protection.	
En cas de détection d'un logiciel incompatible avec l'agent antivirus de Dr.Web Enterprise Security Suite, ou d'un logiciel potentiellement dangereux, supprimez-le.	
Vérifiez les résultats de déploiement de la protection et les configurations effectuées.	
Faites une analyse antivirus des postes de travail du personnel.	

- Si les dispositifs et les ordinateurs des employés sont inclus dans le système centralisé de protection :

Action	Statut
Vérifiez la disponibilité des droits administrateur pour installer l'antivirus.	
Installez les mises à jour de sécurité sur les appareils et les ordinateurs.	

Avant l'installation de l'agent antivirus Dr.Web Enterprise Security Suite, il est recommandé d'effectuer une analyse antivirus en utilisant la version actuelle de Dr.Web CureIt!	
Avant l'installation de la protection antivirus d'entreprise, désinstallez les solutions d'autres éditeurs si elles ont été précédemment installées sur les machines en question.	
Configurez le serveur antivirus Dr.Web si les employés doivent se connecter au serveur directement ou bien installez un serveur proxy.	
Dans le réseau antivirus du Centre de gestion Dr.Web, créez des groupes séparés pour les postes protégés du personnel.	
Effectuez les étapes nécessaires pour la configuration des groupes crées. Si lors de l'installation, il est nécessaire d'indiquer des paramètres d'accès au serveur antivirus ou au serveur proxy, autorisez les actions appropriées via le Centre de gestion.	
Ajoutez les fichiers clés ou des fichiers assurant la protection d'un nombre nécessaire d'employés au Centre de gestion Dr.Web.	
Créez le nombre requis de nouveaux postes de travail et donnez aux employés des packages d'installation des agents antivirus conformément au schéma de déploiement sélectionné.	
Vérifiez les résultats de déploiement de la protection et les configurations effectuées.	
En cas de détection d'un logiciel incompatible avec l'agent antivirus de Dr.Web Entreprise Security Suite, ou d'un logiciel potentiellement dangereux, supprimez-le.	
Faites une analyse antivirus des postes de travail du personnel.	
Utilisez les fonctionnalités du Centre de gestion Dr.Web pour contrôler la liste des mises à jour installées et des logiciels installés par votre personnel. En cas de détection d'un logiciel potentiellement dangereux, créez des règles interdisant son utilisation à l'aide du module Contrôle des applications Dr.Web.	

Marche à suivre détaillée pour l'organisation de la protection distante des employés faisant du télétravail à l'aide des outils de Dr.Web Enterprise Security Suite

A propos de Doctor Web

Doctor Web - éditeur russe de solutions antivirus Dr.Web. Doctor Web développe les produits Dr.Web depuis 1992. Acteur-clé du marché des logiciels, la société répond à un besoin fondamental des entreprises : la sécurité de l'information.

Doctor Web est la première entreprise à avoir proposé sur le marché russe un modèle novateur d'antivirus en tant que service (Saas). Jusqu'à maintenant, la société reste un leader sur le marché des services internet de sécurité pour les fournisseurs de services informatiques.

Ils font confiance à Dr.Web

L'expertise de Doctor Web sur les diverses problématiques de la sécurité de l'information permet à la société de considérer les particularités et le profil d'entreprises de toute taille et d'offrir à ses clients les meilleurs produits à un coût total minimum.
Doctor Web répond aux besoins de grandes entreprises russes, de sociétés et d'institutions au niveau international, ainsi qu'à ceux d'utilisateurs particuliers dans le monde entier. L'étendue géographique des utilisateurs témoigne de la confiance qu'ils placent dans les logiciels Dr.Web, créés par des programmeurs russes de talent.

Ils ont choisi les produits Dr.Web : https://customers.drweb.com.

Pourquoi Dr.Web ?

Doctor Web est propriétaire des technologies Dr.Web. Doctor Web est l'un des rares fournisseurs de solutions antivirus possédant ses propres technologies de détection et de traitement des programmes malveillants ainsi que son Laboratoire viral, son service global de veille et de recherche sur les menaces et son service de support technique.

Doctor Web – éditeur russe des solutions antivirus Dr.Web. Doctor Web développe les produits Dr.Web depuis 1992.
Doctor Web France – 333b, avenue de Colmar – 67100 Strasbourg
Téléphone: 03 90 40 40 20 / Fax.: 03 90 40 40 21
https://www.drweb.fr | https://free.drweb.fr | https://curenet.drweb.fr