Dr.WEB®
depuis 1992

LA PROTECTION ANTIVIRUS DE L'ENTREPRISE

Sommaire

Les menaces virales actuelles

UNE IDÉE FAUSSE

Les hackers qui développent les virus sont isolés.

L'époque où les malwares étaient développés par des hackers isolés est lointaine. Les programmes malveillants modernes sont conçus par des créateurs de virus professionnels et c'est une activité criminelle bien organisée impliquant des développeurs de logiciels qualifiés.

L'organisation des groupes cybercriminels

Dans de nombreux cas, les cybercriminels sont organisés par groupes remplissant chacun une fonction :

1. les organisateurs – personnes qui organisent et gèrent le développement et l'utilisation des logiciels malveillants. Les logiciels malveillants peuvent être utilisés soit directement, soit vendus à d'autres malfaiteurs.

2. Les participants :

- les développeurs des logiciels malveillants
- Les testeurs des logiciels créés
- Les ingénieurs qui recherchent les vulnérabilités des systèmes d'exploitation et des applications à des fins criminelles
- Les «experts» de l'utilisation des packers et du cryptage
- Les experts en ingénierie sociale pour diffuser les malwares
- Les administrateurs système pour assurer le fonctionnement et le contrôle des botnets

Les principaux vecteurs de la cybercriminalité « commerciale » (qui « produit » des virus pour les vendre)

- La compromission des systèmes afin de les enrôler dans des botnets pour surveiller la victime, voler de l'information, et lancer des attaques DDoS.

- Le vol des données d'authentification sur les systèmes de banque en ligne et les systèmes de paiement en ligne pour pirater les comptes.
- Le vol de données de cartes bancaires afin de voler de l'argent.
- La fraude associée à des marques pour gagner de l'argent ou les compromettre.
- La violation de droits d'auteur.

Les raisons de la croissance des vols effectués via des malwares :

- la croissance du nombre de logiciels malveillants,
- la création de nouveaux virus encore plus sophistiqués,
- l'utilisation de vulnérabilités logicielles non corrigées,
- l'utilisation de logiciels illégaux (y compris les antivirus),
- Une mauvaise utilisation des moyens de protection (y compris les antivirus),
- Un comportement risqué sur Internet (y compris la désactivation des composants de l'antivirus),
- Un mauvais paramétrage de la sécurité (y compris l'antivirus),
- Le non-respect des fondements de la sécurité informatique,
- Le facteur humain – la négligence, le manque d'attention, etc.

Pour attaquer les systèmes informatiques de l'entreprise, les attaquant exploitent :

- les manquements dans l'organisation des systèmes de protection antivirus de tous les nœuds du réseau de l'entreprise ou l'absence de tels systèmes ;
- les manquements dans ou l'absence de politiques de sécurité informatique ;
- Le non respect des politiques de sécurité informatique par les employés ;
- les moyens de l'ingénierie sociale.

ATTENTION !
L'antivirus est le principal outil de lutte contre les fraudes Internet.

Avant de répandre des virus, leurs auteurs les testent sur **tous les logiciels antivirus connus** c'est pourquoi il y a toujours une probabilité, que tel ou tel virus ne soit pas détecté pendant quelque temps. Il n'existe pas de programmes antivirus qui puisse faire face aux menaces dans ce cas (quels que soient ses résultats dans des tests heuristiques).

De plus en plus, les attaquants développent des **menaces ciblées** pour attaquer des groupes d'utilisateurs concrets (par exemple les utilisateurs d'une banque). Ce sont des logiciels malveillants qui n'affectent presque pas le fonctionnement de la machine infectée et qui sont indétectables au moment de leur pénétration dans le système, ce qui leur permet de fonctionner assez longtemps à l'insu de l'utilisateur.

Cela a également contribué à dévaluer les tests des logiciels antivirus comme référence lors du choix d'un antivirus.

Les groupes cybercriminels bien organisés développent, diffusent et produisent les virus de manière quasi industrielle. Cela entraîne une croissance explosive du nombre de programmes malveillants en circulation et augmente considérablement le nombre de signatures ajoutées à la base virale.

LES FAITS

Chaque jour, le laboratoire antivirus Doctor Web analyse au moins 250.000 échantillons de malwares.

UNE IDÉE FAUSSE

L'antivirus doit détecter 100% des virus.

Autrement dit qu' un bon antivirus doit connaître tous ou presque tous les logiciels malveillants au moment de leur pénétration. L'antivirus, qui n'accomplit pas bien ses fonctions sera remplacé, car il est considéré comme étant de mauvaise qualité.

Comment est née cette idée ?

Dans l'industrie antivirus il y a longtemps qu'il existe des tests comparatifs, effectués par des testeurs indépendants. Pour effectuer ces comparatifs, les testeurs utilisent une collection de virus, mettent à jour les antivirus et lancent un scan. Pour gagner, l'antivirus doit détecter 100% des virus.

Les particularités de ces tests sont :

- aucun testeur ne peut garantir que sa collection comprend uniquement des virus ;
- ces tests ne montrent que l'**une** des fonctions de l'antivirus – la détection des menaces ;
- ces tests n'estiment que la qualité du moniteur de fichiers ou du scanner, c'est-à-dire la lutte contre les menaces **connues** ;
- ces tests ne montrent pas comment l'antivirus fonctionne dans les conditions réelles, comment il peut traiter les virus, s'il est capable de détecter les menaces inconnues.

Ces tests ont contribué à créer cette fausse idée.

L'antivirus doit neutraliser les fichiers malveillants, mais il ne peut détecter que les virus qui sont **référencés dans sa base virale**. La technologie d'analyse heuristique, permettant de détecter une activité suspecte, complète la détection par signatures. Et sans les mises à jour, l'antivirus ne peut ni détecter, ni neutraliser une **nouvelle** menace.

LES FAITS

Il faut noter que tous les malwares les plus sophistiqués et les plus dangereux, notamment **conçus pour voler de l'argent**, sont testés par leurs créateurs sur tous les antivirus du marché avant leur mise en circulation. Le virus doit rester indétectable le plus longtemps possible ! Si le virus est facile à détecter — c'est un mauvais virus, du point de vue de ses créateurs. C'est pourquoi certains virus ne sont pas détectés par les antivirus avant que leurs échantillons n'entrent dans les bases virales.

Le virus peut pénétrer votre système via une vulnérabilité zéro-day (les exploits Zéro-day sont des vulnérabilités connues des fraudeurs mais qui n'ont pas encore été corrigées par des patchs) ou en utilisant les moyens de l'ingénierie sociale — c'est-à-dire qu'il sera lancé par l'utilisateur lui-même, qui peut, de plus, avoir désactivé l'autoprotection de l'antivirus.

UNE IDÉE FAUSSE

Les antivirus détectent toutes les menaces par des signatures (les entrées dans la base de données virales).

Si c'était le seul moyen de détection, l'antivirus serait incapable de neutraliser les menaces **inconnues**.

Cependant, l'antivirus reste le meilleur et le **seul** moyen efficace de protection contre tous les types de menaces **connues** ou **inconnues**.

Les produits Dr.Web utilisent de nombreuses technologies sans signatures qui permettent de détecter les dernières menaces (inconnues) avant qu'elles soient ajoutées à la base virale. Nous allons parler de certaines d'entre eux.

- **La technologie FLY-CODE** assure le scan des objets empaquetés, décompresse les emballeurs (même les non-standard) au moyen de la virtualisation de l'exécution du fichier, ce qui permet de détecter les virus compressés par des emballeurs inconnus de l'antivirus Dr.Web.
- **La technologie Origins Tracing** — Le moteur d'analyse heuristique Dr.Web détecte les menaces inconnues en fonction de leurs traits caractéristiques s'apparentant à une activité virale et en les comparant aux menaces déjà présentes dans la base. Cette technologie assure un haut niveau de détection des menaces qui ne sont pas encore ajoutées à la base virale de Dr.Web.

- **La technologie d'analyse par entropie structurelle** détecte les menaces inconnues grâce aux particularités de placement du code malveillant dans les objets cryptés par les packers.
- **La technologie ScriptHeuristic** empêche l'exécution de tous les scripts malveillants dans les navigateurs et documents PDF sans compromettre la fonctionnalité des scripts légitimes. Protège contre la contamination par des virus inconnus via le navigateur web. Fonctionne indépendamment de l'état de la base virale Dr.Web avec n'importe quel navigateur web.
- **L'analyseur heuristique traditionnel** comprend des mécanismes de détection des logiciels malveillants inconnus. Son fonctionnement est basé sur les connaissances des attributs et du comportement supposésdes virus – (ce qui est typique d'un code viral, et ce qui ne l'est pas). Chacun de ces éléments est caractérisé par un chiffre, dont la valeur détermine l'importance et le signum montre s'il confirme ou infirme l'hypothèse de la probabilité de la présence d'un virus dans le code analysé.
- **Le module d'imitation d'exécution, quant à lui, est basé sur une** technologie d'imitation de l'exécution du code d'un programme pour détecter les virus polymorphes, lorsque la recherche par la somme de contrôle est impossible ou difficile (à cause de la difficulté de la création de signatures fiables). Cette méthode consiste à imiter l'exécution du code suspecté d'être viral par un émulateur — un simulateur du processeur (et en partie de l'ordinateur et du système d'exploitation).

UNE IDÉE FAUSSE

Les virus n'existent plus !

En effet, plus de 90% des menaces actuelles ne peuvent pas être considérées comme des virus au sens propre, car elles n'ont pas de mécanisme d'auto-réplication. La majorité des menaces aujourd'hui sont des Trojans. Ils appartiennent à la catégorie des programmes malveillants, et peuvent causer des problèmes à l'utilisateur de l'ordinateur infecté.

Les Trojans dangereux :

1. Sont invisibles pour l'utilisateur et certains logiciels antivirus.
2. Sont capables de voler des données confidentielles, y compris les identifiants d'accès aux banques en ligne.
3. Peuvent télécharger d'autres programmes malveillants.
4. Peuvent paralyser l'ordinateur via des commandes à distance envoyées par les cybercriminels.

Ces programmes, au moment de leur lancement, sont souvent indétectables par les antivirus. En outre, certains Trojans essaient de supprimer l'antivirus.

LES FAITS

Dans 70% des cas, les réseaux locaux sans connexion Internet sont infectés **via des supports amovibles** (clés USB ou autres).

ATTENTION !

Il peut arriver que l'antivirus ne détecte pas immédiatement un logiciel malveillant qui s'est introduit de manière clandestine dans le système, mais seul un antivirus est capable de lutter contre un Trojan qui a déjà pénétré le système.

UNE IDÉE FAUSSE

Les actions des virus sont toujours visibles pour l'utilisateur. Si mon ordinateur est infecté, je le comprends tout de suite et je prendrai des mesures.

LES FAITS

Les malwares modernes sont conçus pour rester invisibles le plus longtemps possible dans le système. C'est pourquoi ils se masquent dans le système et sont indétectables par les logiciels antivirus au moment de leur pénétration dans l'ordinateur. Il existe également des malwares capables de lutter avec leurs concurrents et de les supprimer. Il y a même des logiciels malveillants qui exploitent les vulnérabilités de votre ordinateur !

Par exemple, le **Trojan.Carberp**, un trojan bancaire, lancé sur une machine contaminée, entreprend plusieurs actions pour éviter d'être détecté par les outils de contrôle et de surveillance. Après un lancement réussi, le Trojan s'injecte dans les applications en cours et stoppe son processus principal. Ainsi, il fonctionne ensuite au sein des autres processus.

Le mythe des virus dont les actions sont immédiatement et forcément visibles est complètement dépassé.

Les informations sur les menaces virales actuelles sur Internet

Le Laboratoire antivirus de Doctor Web :
http://live.drweb.com

Les descriptions des virus et des malwares :
http://vms.drweb.com/search

Les rapports sur les virus et le spam :
http://news.drweb.com/list/?c=10

Les alertes virales :
http://news.drweb.com/list/?c=23

L'abonnement à la newsletter de Doctor Web :
https://news.drweb.com/news/subscribe

Soumettre un fichier suspect pour analyse :
https://vms.drweb.com/sendvirus

Le scanner Dr.Web en ligne :
http://vms.drweb.com/online

Les possibilités d'intrusion virale dans les réseaux d'entreprise

Il est important que les entreprises s'informent sur les nouveaux moyens de pénétration des malwares ainsi que sur leurs fonctionnalités et sur les « tendances » qui se dégagent de l'observation et de l'étude de l'industrie cybercriminelle.

Donc, les spécialistes doivent connaître les moyens de pénétration **actuels** des logiciels malveillant, afin d'organiser un système de protection antivirus efficace. Les possibilités d'intrusion virale les plus fréquentes aujourd'hui sont :

1. Les vulnérabilités

Une vulnérabilité est une faille dans un logiciel qui, si elle est exploitée à des fins malveillantes, peut compromettre son intégrité ou provoquer une panne. Tout logiciel comporte des vulnérabilités.

Les créateurs de virus exploitent non seulement les vulnérabilités du système d'exploitation, mais également celles des applications (navigateurs, applications Office, par exemple Adobe Acrobat Reader et les plug-ins des navigateurs flash).

Le virus peut pénétrer votre système via une vulnérabilité zéro-day ou en utilisant les moyens de l'ingénierie sociale — c'est-à-dire qu'il sera lancé par l'utilisateur lui-même, qui peut, de plus, avoir désactivé l'autoprotection de l'antivirus.

ATTENTION !
Aucun logiciel, sauf un antivirus, ne peut neutraliser les virus qui ont déjà pénétré le système via une vulnérabilité.

2. Sites Web

L'actualité d'un secteur d'activité est utile aux collaborateurs dans leur activité quotididenne. Le danger est que la majorité des employés de bureau :

- accèdent à Internet depuis un ordinateur personnel sur lequel le logiciel a vulnérabilités ;
- utilisent des ordinateurs sous Windows avec les privilèges administrateur ;
- utilisent des mots de passe faible, qui sont faciles à pirater ;
- n'effectuent pas les mises à jour des logiciels installés sur l'ordinateur.

Surfent sur Internet sans contrôle, ce qui peut permettre aux pirates de voler, remplacer ou compromettre les données importantes de l'entreprise.

ATTENTION !

Les Trojan.Carberp pénètrent les ordinateurs lorsque les utilisateurs **naviguent sur des sites piratés**. Or, votre système peut être contaminé sans votre intervention : **tout se passe automatiquement**.

Les sites qui sont le plus souvent des sources de programmes malveillants (en commençant par les plus « dangereux »)

- Les sites consacrés à la technologie et aux télécommunications
- Les sites destinés au milieu des affaires : les sites d'information liés au monde des affaires, les sites et les forums dédiés au domaine de la finance, les cours et les conférences en ligne, les services d'optimisation de la rentabilité etc.
- Les sites pornographiques

3. Supports amovibles

Même dans les systèmes avec un niveau de protection très élevé, la principale source de propagation des virus n'est pas seulement la messagerie, mais les supports amovibles, surtout les clés USB.

Les programmes malveillants les plus répandus sont les Trojans. Ce sont des logiciels malveillants qui ne possèdent pas de mécanisme d'autoréplication. Ce sont les utilisateurs eux-mêmes qui les lancent sans s'en rendre compte. Ils peuvent être transmis d'un ordinateur à l'autre via les clés USB.

4. Les appareils personnels des employés, y compris les appareils mobiles

Plus de 60% des employés ont un accès distant aux ressources de l'entreprise depuis leurs appareils personnels, y compris les mobiles.

Menaces

- Près de deux tiers des employés ont un accès distant aux ressources de l'entreprise depuis leurs appareils personnels, y compris les mobiles.
- Dans 70% des cas, les réseaux locaux sont infectés via les PC portables, netbooks, ultrabook et les appareils mobiles des employés, ainsi que via les médias amovibles (clés USB).
- 60% des PCs n'ont aucune protection ! Ainsi, en dehors de l'entreprise, les outils ne sont pas protégés contre les attaques, les applications utilisées peuvent comporter des vulnérabilités, les ordinateurs peuvent être infectés par des virus et des Trojans. Cependant, les collaborateurs accèdent régulièrement au réseau de l'entreprise.

- Cela rend possible de voler, remplacer ou compromettre les données importantes de l'entreprise.

5. Messagerie

Or, la messagerie est un des principaux vecteurs de virus et de spam. En cas d'infection, les virus peuvent avoir accès aux contacts des collaborateurs, collègues et clients, ce qui peut entraîner une propagation de l'infection en dehors de votre réseau.

Un manque de vigilance ou de connaissances peut conduire à l'enrôlement des ordinateurs de l'entreprise dans un botnet. Ces ordinateurs envoient ensuite du spam, ce qui peut nuire à la réputation de l'entreprise qui devient black listée, voire à qui l'on coupe l'accès Internet pour envoi de spam.

6. Ingénierie sociale

La majorité des programmes malveillants ne comportent pas de mécanisme d'auto-réplication – ils sont conçus pour être propagés par les utilisateurs.

Les utilisateurs novices en matière de sécurité informatique ou qui ne respectent pas toujours les règles de la politique de sécurité peuvent aider les virus à pénétrer le réseau de la société, notamment en utilisant des clés USB sans les analyser, en ouvrant automatiquement les emails envoyés par des expéditeurs inconnus ou en surfant durant les heures de travail.

Pour diffuser les Trojans, les créateurs utilisent les moyens de l'ingénierie sociale qui incitent les utilisateurs à lancer le fichier d'exécution du programme malveillant. Voici quelques moyens : les liens vers les sites de phishing, les faux messages de banques ou de l'administration des sites Internet, et autres. Ces moyens visent toujours à : obtenir les données personnelles de l'utilisateur, soit les mots de passe, soit des données confidentielles ainsi que les coordonnées bancaires.

Les pré-requis pour l'organisation de la protection du réseau

Les pré-requis généraux

1. Le système de protection antivirus doit :

- **posséder un système d'autoprotection fiable**, qui ne permet pas aux malwares inconnus d'interrompre le fonctionnement de l'antivirus et rend possible son fonctionnement avant la réception des mises à jour, qui permettront de traiter l'infection ;
- **avoir un système de mises à jour**, soumis au système d'auto-protection et qui **n'utilise pas les composants du système d'exploitation**, qui peuvent être compromis ; un système de mises à jour qui peut, après le signal du système de gestion centralisée, immédiatement envoyer les mises à jour pour neutraliser la menace ;
- **disposer d'un système de recueil d'information sur les nouvelles menaces**, qui envoie ces données au laboratoire antivirus pour analyse et pour produire des mises à jour ;
- **être capable de traiter** non seulement les logiciels malveillants inactifs, mais également les malwares déjà lancés, qui étaient inconnus de la base virale avant la mise à jour ;
- disposer de mécanismes supplémentaires (autres que ceux basés sur les signatures et les technologies heuristiques traditionnelles) pour détecter les **nouvelle menaces inconnues** ;
- vérifier tous les fichiers entrants provenant du réseau local **avant qu'ils soient traités par les applications**, ce qui empêche l'exploitation des vulnérabilités de ces dernières ;
- disposer d'un système **centralisé de recueil d'information** depuis les postes de travail et serveurs, qui permet de transmettre rapidement au laboratoire antivirus toutes les données, nécessaires à la résolution d'un éventuel problème ;
- fournir **un service de support technique** en français.

2. Le système de gestion centralisée de la protection antivirus doit :

- **Assurer la livraison la plus rapide possible des mises à jour** des bases virales sur tous les postes de travail et les serveurs – y compris par la décision de l'administrateur système, au détriment des performances du réseau. Minimiser le temps de réception des mises à jour par l'optimisation de leur taille et par la présence d'une connexion permanente des postes de travail et des serveurs au serveur de mises à jour.

- Garantir **l'impossibilité de désactiver les mises à jour**. L'opinion du personnel sur la fréquence des mises à jour doit être IGNORÉE.

ATTENTION !

L'antivirus est un logiciel exigeant du point de vue des mises à jour. De nouveaux virus ne cessent d'apparaître, c'est pourquoi les bases virales requièrent une actualisation très fréquente (1–2 fois par heure). **Ne désactivez JAMAIS la mise à jour automatique de votre antivirus !**

La gestion centralisée du système de protection antivirus Dr.Web vous permet de :

- d'éviter l'annulation des mises à jour sur les postes de travail par l'employé ;
- de désactiver un agent non à jour et, par conséquent, de prévenir la propagation d'épidémies dans le réseau local et en dehors ;
- de spécifier le mode de mises à jour des composants de Dr.Web sur les postes de travail en répartissant la charge par intervalles de temps différents ;
- de contrôler le nombre d'entrées de la base virale et l'état des postes de travail.

- De garantir **l'impossibilité de désactiver les scans** par les utilisateurs, lancer des scans sans la participation de l'utilisateur sur le poste de travail, établir des horaires de scan selon la fréquence souhaitée. L'opinion du personnel sur la fréquence des scans doit être IGNORÉE.

Pourquoi faut-il régulièrement effectuer le scan du système ?

- L'antivirus ne peut pas connaître tous les virus au moment donné.
- Des jours ou même des mois peuvent séparer l'apparition d'un nouveau virus et la sortie de sa signature pour la base virale.
- Même si l'antivirus peut détecter la menace à l'aide de cette signature ajoutée, cela ne veut pas dire qu'il peut déjà la traiter, car il faut du temps pour développer un antidote.

Dr.Web Control Center vous permet de contrôler les scans :

- lancer/arrêter le scan sans l'intervention de l'employé ;
- spécifier le chemin d'analyse ;
- établir des horaires de scan individuels et de groupe selon la fréquence souhaitée – c'est-à dire effectuer des analyses à un moment opportun pour le personnel.

Le Centre de Gestion Dr.Web Enterprise Security Suite fournit la protection de tous les objets du réseau :

- des postes de travail, des clients de serveurs virtuels et terminal server ainsi que des systèmes embarqués sous Windows, Linux et Mac OS X ;
- des serveurs de fichiers et d'applications (y compris terminal server et serveurs virtuels) sous Windows, Novell NetWare, Mac OS X, Unix (Samba) et Novell Storage Services ;
- des serveurs de messagerie Unix, Microsoft Exchange, IBM Lotus, Kerio ;
- des passerelles Internet Unix et Kerio ;
- des appareils mobiles sous Windows Mobile et Android.

L'utilisation du Centre de Gestion Dr.Web permet de réaliser de réelles économies.

La possibilité d'avoir un aperçu global du réseau de l'entreprise, ainsi que la facilité de déploiement et d'administration du réseau de **Dr.Web Enterprise Security Suite** ce qui réduit au minimum le temps de maintenance. L'interface web et la possibilité d'automatiser le fonctionnement grâce à l'intégration avec le système Windows PAN ; Et l'interface pour écrire les gestionnaires des événements en langage de script, ce qui réduit la charge sur les administrateurs système.

Le Centre de gestion Dr.Web permet :

- d'effectuer l'installation, la configuration et la mise à jour des logiciels de protection antivirus, y compris sur les ordinateurs inaccessibles depuis le serveur ;
- de contrôler le système de protection du réseau local depuis un ordinateur, quel que soit son emplacement et l'OS utilisé, via un navigateur, sans nécessité d'installer des logiciels spécifiques ;
- d'appliquer la politique de sécurité souhaitée ;
- d'affecter des administrateurs pour différents groupes ;
- de lancer le scan antivirus complet ou personnalisé d'un nœud du réseau via une commande de l'administrateur système ou de l'utilisateur, ou selon un horaire prédéfini ;
- de recueillir et analyser les données sur l'état du système de protection antivirus, et créer des rapports pour la période de temps requise ;
- d'informer les administrateurs et les utilisateurs sur l'état du système de protection ;
- d'envoyer des notifications aux utilisateurs en temps réel.

Le Centre de gestion Dr.Web est soumis à licence gratuitement.
Plus d'informations : http://products.drweb.com/enterprise_security_suite/control_center

La protection du réseau lors de l'utilisation de services Cloud

Voici les risques que ces services représentent :

1. La possibilité d'interception et de modification des données durant la transmission. A cet égard, il faut utiliser des serveurs proxy sur les deux côtés (Cloud et entreprise). En outre, une bonne pratique est d'utiliser un canal de communication sécurisé, mais il ne faut pas oublier les risques d'intrusion de logiciels malveillants dans l'espace entre le programme client et le canal sécurisé.
2. Il est également possible d'introduire des logiciels malveillants dans une machine virtuelle. C'est pourquoi il faut utiliser une protection antivirus pour toutes les machines virtuelles, quel que soit leur emplacement.

Si l'entreprise utilise des services Cloud ou possède des filiales, elle doit obligatoirement utiliser :

- des passerelles de messagerie du côté du centre de données Cloud et du côtédu réseau local ou des serveurs de messagerie locaux, qui scannent les messages entrants et stockent les messages, si le centre de données Cloud n'est pas disponible ;
- des serveurs de fichiers et des services, qui synchronisent le contenu avec celui des serveurs distants.

L'utilisation de solutions antivirus doit être complétée par :

1. L'isolation du réseau de l'entreprise d'Internet — la division du réseau entre interne et externe.
2. La journalisation des actions de l'utilisateur et de l'administrateur.
3. Les sauvegardes des données importantes.

La mise en place de procédures de sécurité :

1. Le contrôle périodique des exigences en matière de sécurité informatique.
2. La maintenance des outils qui garantissent la sécurité informatique.
3. La réponse aux incidents informatiques.
4. L'information des employés et des clients sur les incidents informatiques.

La protection des postes de travail

En général, les postes de travail (y compris les appareils mobiles) et les serveurs sont les points les plus vulnérables du réseau local. Les malfaiteurs les utilisent pour diffuser les virus et le spam.

La protection des postes de travail appartenant à l'entreprise

1. Il est théoriquement possible d'utiliser n'importe quelle vulnérabilité pour nuire au système. Pour éviter cela,

- il est important, non seulement de mettre à jour l'OS, mais égalementde télécharger les mises à jour ou les nouvelles versions des logiciels installés sur l'ordinateur. Pour ce faire, tous les logiciels doivent être légaux.
- Il faut utiliser un système d'installation centralisée des mises à jour pour tous les logiciels installés sur l'ordinateur. Cela permet à l'administrateur système de contrôler en temps réel l'absence de vulnérabilités connues sur les objets protégés.

Seul un administrateur système qualifié peut prendre la décision de mettre à jour l'antivirus, d'installer un logiciel ou de redémarrer le PC en raison d'une mise à jour de sécurité. L'opinion des collaborateurs, quelle que soit leur fonction, doit être IGNOREE.

2. Il convient de mettre en place une gestion centralisée de tous les composants de la protection antivirus de tous les postes de travail au sein du réseau local.
3. Le système de protection antivirus doit être actualisé.
4. Chaque employé, peu importe son poste, doit travailler sous un compte avec des droits limités. Il faut désactiver le compte Invité.
5. Les logiciels installés doivent être connus de l'administrateur système.
6. La possibilité d'installer d'autres logiciels doit être évitée, ce qui minimise le risque d'infection virale.
7. Les utilisateurs doivent avoir uniquement accès aux ressources du réseau vraiment nécessaires pour effectuer leur travail. Pour ce faire, il faut utiliser un système de contrôle d'accès.

Dr.Web Office Control bloque les moyens de pénétration des virus en interdisant l'utilisation des supports amovibles et en limitant l'accès aux périphériques locaux et réseau (y compris les répertoires sur l'ordinateur local et les sites Internet).

8. Le trafic de la messagerie doit être scanné avant que le courriel n'arrive dans la boîte de réception du client de messagerie pour éviter l'exploitation de ses vulnérabilités.

ATTENTION !
Les flux email transitant via un poste de travail et un serveur ne sont pas les mêmes.

- L'utilisateur (ou un programme dont il a accepté l'installation, sans connaître ses fonctionnalités) peut envoyer et recevoir des emails :
  - directement sur les serveurs de messagerie sur Internet (via SMTP), si le port 25 du réseau est ouvert ;
  - sur les services de messagerie tels que mail.ru/gmail.com – via les protocoles POP3/IMAP4.

- L'utilisateur (ou un programme dont il a accepté l'installation, sans connaître ses fonctionnalités) peut envoyer et recevoir des emails via des canaux sécurisés et les services du serveur ne pourront pas les scanner.
- Le serveur (ou les programmes installés) peut créer ses listes d'envoi et notifier les destinataires et expéditeurs sur les événements.

C'est pourquoi il faut filtrer le trafic au niveau du serveur de messagerie ainsi qu'au niveau du poste de travail.

9. Le trafic Internet doit être scanné avant qu'il n'arrive aux applications clientes. Le système antivirus doit analyser tous les liens qui prévoient le téléchargement de fichiers ainsi que le trafic.

Il y a déjà longtemps que les vulnérabilités des logiciels installés sont exploitées (notamment Adobe) plutôt que celles du système d'exploitation ; **Le moniteur HTTP Dr.Web** analyse le trafic Internet avant le traitement par le navigateur ou par le client de messagerie. Dans ce cas, les virus ne peuvent pas exploiter les vulnérabilités des logiciels sur le poste de travail.

10. Le personnel doit avoir uniquement accès aux ressources Internet nécessaires à leur activité. L'opinion du personnel concernant les sites Web sains doit être IGNORÉE. L'accès du personnel aux ressources inutiles devrait être empêché de façon centralisée.

Dr.Web Office Control vous permet de :

- limiter l'accès à l'Internet ;
- créer des listes black et white pour ne pas complètement interdire l'accès à Internet ;
- interdire l'accès à Internet sur les systèmes où c'est crucial (par exemple, sur les ordinateurs gérant la comptabilité) ;
- rendre impossible la désactivation des restrictions par l'employé.

ATTENTION !

Ce composant doit être installé sur les ordinateurs sans connexion Internet ou réseau.

11. Un utilisateur ne doit avoir accès qu'aux ressources locales du réseau nécessaires pour son travail quotidien (ce qui limite les dégâts en cas d'infection et s'il s'agit d'un programme malveillant agissant en son nom). Il n'est pas toujours facile de convaincre le personnel que les clés USB sont dangereuses.

Le système de contrôle d'accès Dr.Web Office Control :

- spécifie les fichiers et dossiers accessibles et interdits pour le collaborateur, ce qui prévient l'endommagement, la suppression ou le vol de données sen-

sibles par des malfaiteurs ou des insiders (les employés ayant accès aux données sensibles) ;

- limite ou interdit complètement l'accès aux ressources Internet et supports amovibles, ce qui peut empêcher la pénétration de virus via ces sources.

Un mécanisme supplémentaire de protection contre les virus qui se propagent via les supports amovibles est l'interdiction de l'autorun dans le moniteur de fichiers SpIDer Guard. Lorsque l'option « Bloquer l'autorun depuis les supports amovibles » est activée, il reste possible d'utiliser les clés USB, si nécessaire.

LA MEILLEURE PRATIQUE

Il fautinterdire la connexion des dispositifs USB au poste de travail **de manière centralisée**.

12. En outre, pour prévenir la pénétration des objets malveillants à l'intérieur du réseau de l'entreprise, il faut utiliser les composants de la protection antivirus suivants :

- **L'antispam** — pour réduire la quantité du spam dans le trafic email, ce qui réduit le risque d'infection et augmente la productivité, car :
  - les utilisateurs passent moins de temps à vérifier les messages entrants,
  - la probabilité de manquer ou de supprimer un message important se réduit.
- **Le pare-feu** — pour la protection contre les attaques depuis le réseau.

13. Le système de protection antivirus doit être installé sur tous les postes de travail quels que soient leurs systèmes d'exploitation, y compris Mac OS X, Linux et Unix. Si l'entreprise ne protège que les machines sous Windows, cette approche donne la possibilité aux logiciels malveillants de pénétrer les machines non protégées. Et il ne faut pas oublier que même si les virus ne peuvent pas nuire au système d'exploitation ni aux applications installées sur l'ordinateur, ils peuvent l'utiliser comme moyen de se propager via les ressources partagées.

ATTENTION !

La hausse du nombre d'attaques des systèmes d'exploitation Linux est une des tendances de l'année 2013.

La protection des postes de travail sur lesquels les employés travaillent avec des données importantes et/ou financières

1. Il ne faut pas utiliser l'ordinateur sur lequel les employés manipulent des données importantes pour travailler avec des données financières et vice versa. Cet ordinateur doit uniquement exécuter les fonctions qui lui sont attribuées.

2. Sur la machine dédiée il faut :

- éliminer la possibilité d'exécuter d'autres programmes, en particulier à des fins inconnues, et provenant d'expéditeurs inconnus ;
- supprimer les systèmes et les services de gestion à distance et bloquer les autres connexions sauf celle qui assure le fonctionnement de la banque en ligne ;

- bloquer la possibilité de visiter d'autres ressources Web via Dr.Web Office Control ;
- effectuer la journalisation des actions de l'utilisateur ainsi que celles de l'administrateur ;
- désactiver la possibilité d'exécuter des programmes depuis les dossiers contenant des documents et le dossier contenant les fichiers temporaires, tels que Temp ;
- utiliser les mots de passe forts. La persistance des mots de passe doit être contrôlée par un système centralisé qui assure la conformité des mots de passe utilisés aux exigences de sécurité et leur modification régulière.

3. Avant de travailler avec la banque en ligne et/ou des données importantes, il faut mettre à jour l'antivirus et effectuer un scan rapide du système.
4. Après l'utilisation de la banque en ligne et/ou des données importantes, il faut quitter correctement ces systèmes (log out).

La protection des PC personnels des employés utilisés pour l'accès au réseau de l'entreprise

Aujourd'hui, de nombreux employés utilisent leurs appareils personnels pour accéder aux ressources de l'entreprise et/ou travaillent à distance. Il existe un large éventail de professions dont les représentants sont toujours en ligne : au bureau, chez eux ou lors de leurs déplacements. L'entreprise doit assurer à ses employés un environnement de travail sécurisé et ainsi une protection de leurs données.

Le plus souvent, les employés utilisent le système d'exploitation Windows sur leurs PC. Ce système d'exploitation est bien connu des malfaiteurs, la plupart des malwares étant développé spécialement pour Windows. Même s'il existe bien évidemment des moyens de protection pour ce système, l'entreprise doit pouvoir combiner le respect de sa politique de sécurité et une utilisation libre de son appareil personnel par le collaborateur. Or, cela pose souvent des problématiques importantes. Par exemple, il serait nécessaire d'interdire aux employés de visiter les réseaux sociaux durant les heures de travail et laisser cette possibilité durant le temps libre. Mais comment faire lorsqu'il s'agit dun appareil personnel ? De plus, il ne faut pas oublier que les membres de la famille de l'employé doivent également avoir la possibilité d'utiliser cet ordinateur.

Il existe deux variantes de protection.

- **La première** – ajouter un compte utilisateur sur l'ordinateur (c'est possible dans Windows) et lui appliquer tous les paramètres de sécurité nécessaires. Malheureusement, cette variante ne vous permet pas de satisfaire à toutes les exigences de sécurité. En effet, si vous travaillez sous un compte « protégé », la sécurité est garantie, mais si l'utilisateur travail sous un autre compte, rien n'empêche un virus de pénétrer le système et d'avoir un accès aux données stockées sur l'ordinateur. De plus, il pourra éventuellement également modifier les paramètres de sécurité. Il fadura donc ajouter le stockage des fichiers et un système de contrôle de l'intégrité. Mais le problème principal est que l'administrateur système devra configuer ces outils pour chaque utilisateur, et dans la plupart des cas à distance.

- **La seconde variante (la plus efficace)** — un disque d'amorçage ou USB sur lequel tous les composants pour assurer la sécurité sont installés. Les virus pourront éviter la protection au niveau du BIOS, mais peu de malwares peuvent le faire aujourd'hui.

ATTENTION !

Seule la protection de tous les appareils utilisés par les employés, professionnels et personnels, y compris les appareils mobiles, peut **assurer** la protection du réseau contre les malwares pénétrant à partir des appareils mobiles personnels, et la protection des mots de passe utilisés par les employés pour accéder au réseau de l'entreprise contre le vol.

IMPORTANT !

Dr.Web Enterprise Security Suite Control Center vous permet de gérer la protection des ordinateurs de bureau et les PCs des employés, y compris les appareils mobiles tournant sous Android et Windows Mobile.

1. Même si le collaborateur utilise un antivirus sur son appareil personnel, **il est recommandé** d'utiliser le même antivirus que son entreprise, dès lors que cet appareil peut accéder au réseau de l'entreprise. Sinon, ce dispositif doit être déclaré non reconnu et ne peut pas fonctionner dans le réseau.
2. **La gestion centralisée** du système de protection antivirus assure le respect des politiques de sécurité de votre entreprise sur les appareils personnels de vos employés, y compris l'impossibilité de désactiver les mises à jour et les analyses régulières ainsi que de supprimer les composants de protection.

Pour le reste, l'idéal serait d'utiliser le même système de protection antivirus sur les ordinateurs de l'entreprise et sur les PC personnels des employés.

L'antivirus Dr.Web vous permet de : gérer la protection des ordinateurs de bureau et des PC des employés, y compris les appareils mobiles.

La protection des appareils mobiles des employés

Aujourd'hui, les Smartphones ont les mêmes fonctionnalités et les mêmes vulnérabilités que les ordinateurs, car ils tournent sous des systèmes d'exploitation et utilisent des applications qui peuvent être contaminées. Dans ce cas, le problème principal de l'utilisation des appareils mobiles des employés est qu'ils peuvent distribuer des logiciels malveillants dans le réseau de l'entreprise, car ils peuvent accéder aux ressources en évitant la protection.

Les appareils mobiles tournent dans la plupart des cas sous iOS ou Android. Ces systèmes d'exploitation sont plus faibles que ceux utilisés sur les PC. Par exemple, ils n'offrent pas la possibilité de créer plusieurs comptes afin de limiter les droits utilisateurs. Par conséquent, la protection ne peut être que partielle. De plus, il ne faut pas oublier qu'un employé peut perdre son appareil avec les logins et mots de passe.

Pour assurer la protection de l'appareil mobile il faut utiliser :

1. un antivirus — Il neutralisera tous les fichiers malveillants y compris ceux conçus pour visualiser les déplacements du propriétaire de l'appareil, ses contacts et ses appels ;
2. un système de protection contre la perte de l'appareil mobile, ce qui permettra de trouver l'appareil et/ou de bloquer l'accès aux données sensibles ;
3. un système de stockage sécurisé des données sensibles, ce qui empêchera l'attaquant d'utiliser les données traitées par l'appareil mobile.

La protection des appareils mobiles est fortement recommandée si ces dispositifs sont utilisés dasn un cadre professionnel pour recevoir des SMS confirmant les opérations bancaires, car il existe des malwares qui peuvent modifier ces messages.

Protection des serveurs de fichiers

Il est primordial de protéger tous les objets du réseau, notamment les postes de travail, les serveurs et les appareils mobiles. Car un virus qui a, par exemple, pénétré le poste de travail, peut également contaminer les serveurs contenant des données sensibles.

Pourquoi faut-il protéger les serveurs ?

- L'utilisateur peut infecter le serveur avec un virus inconnu de l'antivirus au moment de la pénétration L'antivirus installé peut l'attraper immédiatement en utilisant les mécanismes heuristiques. Ou dans le cas extrême, l'antivirus traitera ce virus lors de la prochaine mise à jour.
- Le serveur peut être piraté. L'antivirus installé l'empêchera : il retrouvera et neutralisera tous les programmes malveillants. Si le serveur est sous le contrôle d'un système de gestion centralisée, l'administrateur système reçoit une notification sur le changement de statut de la station (par exemple, une tentative d'arrêter le système de protection).
- Le monde moderne est imprégné par la technologie numérique. Les utilisateurs peuvent travailler non seulement au bureau, mais aussi à la maison, stocker les données sur les serveurs de fichiers de l'entreprise — et sur des serveurs Internet. Ils peuvent également utiliser des clés USB (même celles reçues de leurs amis et collègues). Ces supports peuvent transporter des virus.
- Aujourd'hui, les Smartphones ont les mêmes fonctionnalités et les mêmes vulnérabilités que les ordinateurs, car ils tournent sous des systèmes d'exploitation et utilisent des applications qui peuvent être contaminées. Les virus peuvent les utiliser pour avoir accès aux serveurs de l'entreprise.

Les pré-requis pour la protection des serveurs de fichiers sous Windows et Unix sont différents. Dans les systèmes d'exploitation Windows, le moniteur de fichiers protège les serveurs d'applications et les terminal server ; dans

les systèmes d'exploitation Unix, chaque service demande l'utilisation d'une solution appropriée.

ATTENTION !

Si vous utilisez le serveur de bases de données sur le serveur de fichiers, vous devez utiliser des solutions spéciales pour traiter le contenu des bases de données.

Les employés utilisent très souvent non seulement le serveur de fichiers de l'entreprise, mais également des outil de stockage externes. Ces outils peuvent véhiculer des fichiers infectés, car il existe toujours une possibilité d'intercepter le flux Internet et de remplacer ou d'endommager les données transmises. À cet égard, il faut protéger le serveur de fichiers et les ressources partagées ainsi qu'une passerelle antivirus pour éviter de recevoir ou d'envoyer des fichiers infectés.

Les serveurs d'impression

Les serveurs de fichiers sont souvent utilisés comme serveurs d'impression, c'est-à-dire qu'ils ont des services qui permettent d'envoyer et de recevoir via un protocole spécial les documents à imprimer. Ces serveurs requièrent une protection, car

- il y a beaucoup de programmes malveillants qui infectent les serveurs d'impression ;
- l'attaquant peut intercepter les documents envoyés à l'impression ou envoyer à imprimer des documents dont la diffusion en dehors de l'entreprise est interdite.

IMPORTANT !

Si votre serveur est basé sur Linux, il est recommandé de protéger non seulement les fonctions du serveur de fichiers (service Samba), mais le serveur lui-même. Cela signifie que vous avez besoin de deux produits Dr.Web :

- Dr.Web Antivirus pour Linux
- Dr.Web pour serveurs de fichiers Unix

Il faut tenir compte de la possibilité d'infection des imprimantes qui sont accessibles depuis Internet. En raison du manque de ressources sur ces dispositifs, il est impossible d'installer des logiciels antivirus. C'est pourquoi il faut limiter l'accès à ces appareils comme moyen de protection.

Protection des terminal server

La protection des terminal server est assurée par les produits conçus pour la protection des systèmes de fichiers, car du point de vue de la protection antivirus, il n'y a qu'une différence entre les deux, c'est la nécessité de vérifier les sessions de terminaleclients(ouverture et fermeture).

- Si l'accès aux terminal server est effectué depuis des clients légers, **ils ne requièrent pas de protection** (aucun malware ne peut pas être installé), mais pour protéger les sessions, il convient d'acquérir le nombre de licences **Dr.Web Desktop Security Suite protection complète** égal au nombre de connexions – en plus de la licence pour la protection du terminal server **Dr.Web Server Security Suite**.

- Si l'accès aux terminal server n'est pas effectué depuis des clients légers, **il faut assurer** la protection des clients qui se connectent au terminal server (**Dr.Web Desktop Security Suite Protection complète + Dr.Web Server Security Suite**). Pourtant, dans un cas comme dans l'autre, le même système de protection antivirus est utilisé sur les postes de travail. La seule chose à considérer dans ce cas : le nombre de postes de travail est ignoré dans le nombre de licences accédant à un terminal server.

Le Centre de gestion Dr.Web vous permet de contrôler d'une manière centralisée la protection antivirus des serveurs de fichiers sous Windows, Mac OS X, Unix (Samba), Novell NetWare, Novell Storage Services, peu importe leur nombre.

Le filtrage de la messagerie

La messagerie est un des principaux vecteurs de virus et de spam. En cas d'infection, les virus peuvent pénétrer tous les ordinateurs du réseau, car sur la machine contaminée, les malwares ont accès aux contacts des collaborateurs qui comprennent les adresses de leurs collègues, ainsi que celles de leurs clients.

La présence de fichiers malveillants dans le trafic email, ainsi que certaines actions ou démarches des employés conduisent à :

- la perte et la fuite de données, objectif de l'activité des virus et des outils de piratage ;
- l'infection des postes de travail pour les enrôler dans un botnet ;
- le risque que l'entreprise soit black listée, voire que son accès Internet soit coupé pour envoi de spam ;
- la baisse du temps de réponse du serveur de messagerie qui doit traiter le pourriel ;
- la réduction des performances voire une panne du serveur de messagerie ;
- l'augmentation de la charge sur le réseau local, ce qui réduit les performances des ressources du réseau et de la bande passante ;
- la défaillance d'un serveur suite à une « bombe email » ;
- un temps d'indisponibilité ;
- l'augmentation des dépenses liées au stockage des messages ;
- l'augmentation du besoin de performances des serveurs de messagerie, c'est-à dire la mise à niveau des machines existantes ou l'achat de nouvelles machines.

De plus, l'entreprise subit les risques suivants :

- perturbation des activités quotidiennes de l'entreprise ;
- indisponibilité des postes de travail ;
- la probabilité de manquer l'information importante ;
- ralentissement de l'activité lié à l'élimination des incidents viraux ;
- retards dans l'accomplissement des obligations de la société envers ses clients ;

- augmentation de la taille des boîtes aux lettres et des sauvegardes, ce qui rend la recherche de l'information requise plus compliquée ;
- un manque à gagner en terme de réputation auprès des clients et des partenaires ;
- l'image de l'entreprise comme une société technologiquement arriérée ;
- un risque de perte de clients.

1. Il faut protéger la messagerie externe (entrant et sortant) ainsi que la messagerie interne de l'entreprise, c'est-à dire qu'il faut protéger toutes les voies de réception et d'envoi des messages

La messagerie peut devenir une source d'infection pour tous les ordinateurs du réseau, notamment si le virus qui a infecté une machine a obtenu l'accès à tous ses contacts email.

2. Il faut filtrer les e-mails sur le serveur puis sur les postes de travail

Cette organisation de la protection réduit significativement la charge sur le serveur de messagerie, ainsi que sur les postes de travail :

- Seul l'antivirus pour les serveurs de messagerie peut supprimer les logiciels malveillants contenus dans les boîtes aux lettres, détectés lors des scans périodiques.
- La protection antivirus au niveau du serveur de messagerie vous permet de filtrer les messages d'une manière plus efficace, ainsi que de nettoyer les bases de données emails des virus. En outre, les solutions pour la protection des serveurs de messagerie et des passerelles peuvent filtrer les messages selon les formats de données, les tailles de fichiers maximales etc., ce qui est impossible dans les solutions pour les postes de travail.
- Le trafic Internet doit être analysé avant le traitement par le client de messagerie. Dans ce cas, les virus ne peuvent pas exploiter les vulnérabilités des logiciels en question.
- Le filtrage des emails au niveau du serveur de messagerie vous permet d'éviter la désactivation ou la réduction du niveau de protection par l'utilisateur et d'être sûr que le réseau est protégé.
- L'augmentation de la fiabilité de la protection. Contrairement à un poste de travail qui peut ne pas recevoir durant une certaine période les mises à jour (si l'employé est en congé), les bases virales des serveurs sont toujours actualisées.
- La probabilité des conflits de l'antivirus avec les autres logiciels diminue.
- Les messages, y compris le spam, seront filtrés une fois sur le serveur et non plusieurs fois sur chaque poste de travail. Cette mesure améliore leurs performances.
- Le filtrage antispam réduit la charge sur le serveur de messagerie (la quantité de spam atteint jusqu'à 98% de la totalité du courrier reçu et son absence améliorera les performances du serveur). Cela réduit les désagréments des employés, causés par la perte d'emails ou un délai de réception trop long.
- Le trafic du réseau local sera considérablement réduit grâce à l'utilisation d'algorithmes de cryptage et de compression intégrés aux produits Dr.Web pour les serveurs. Peu d'antivirus possèdent cette fonctionnalité.

3. Il faut assurer la protection du serveur de messagerie lui-même

La protection des serveurs de messagerie eux-mêmes (par exemple, avec **Dr.Web Server Security Suite**) est une mesure fortement recommandée contre les virus inconnus. La pénétration de logiciels malveillants inconnus sur le serveur de messagerie et/ou dans les boîtes aux lettres peut transformer le serveur en une source permanente de malwares.

4. Il convient donc de protéger toutes les voies de réception et d'envoi des messages

La particularité des bureax modernes est l'utilisation de services externes et internes y compris des services de messagerie. Souvent, les employés responsables de la sécurité de l'entreprise n'informent pas les collaborateurs sur l'utilisation de services externes.

Les flux emails possibles de l'entreprise

- L'utilisateur (ou un programme dont il a accepté l'installation, sans connaître ses fonctionnalités) peut envoyer et recevoir des emails :
  - directement sur les serveurs de messagerie sur Internet (via SMTP), si le port 25 du réseau est ouvert;
  - sur les services de messagerie tels que mail.ru/gmail.com – via les protocoles POP3/IMAP4.
- L'utilisateur (ou un programme dont il a accepté l'installation, sans connaître ses fonctionnalités) peut envoyer et recevoir des emails via des canaux sécurisés et les services du serveur ne pourront pas les scanner.
- Le serveur (ou les programmes installés) peut créer ses listes d'envoi et notifier les destinataires et expéditeurs sur les événements.

A cet égard, il faut filtrer le trafic email entrant non seulement sur les serveurs de l'entreprise, mais également sur les serveurs externes qui n'appartiennent pas à l'entreprise, et dont le niveau de protection est inconnu. En pratique, cela signifie :

- filtrer tous les emails de l'entreprise sur le serveur de messagerie (à l'aide de **Dr.Web Mail Security Suite Antivirus + Antispam**) et traiter les protocoles POP3 et IMAP4 sur la passerelle Internet (**en fonction du produit utilisé sur la passerelle qui traite le trafic — Dr.Web Mail Security Suite Antivirus + Antispam, Dr.Web Mail Security Suite Antivirus + Antispam + SMTP proxy** ou **Dr.Web Gateway Security Suite Antivirus**) – en plus de vérifier les messages sur les postes de travail ;
- filtrer tous les emails externes (protocoles POP3 et IMAP4, SMTP) au niveau de la passerelle (en utilisant **Dr.Web Mail Security Suite Antivirus + Antispam + SMTP proxy**) et assurer le traitement des emails internes sur le serveur de messagerie (**Dr. Web Mail Security Suite Antivirus + Antispam**) – en plus de vérifier les messages sur le poste de travail.

La deuxième structure est préférable parce que :

- elle réduit la charge sur le serveur de messagerie (le spam représente jusqu'à 98% du trafic email) ;

- l'absence d'accès direct au serveur de messagerie depuis Internet empêche les attaquants d'utiliser les vulnérabilités (déjà connues et les vulnérabilités zéro-day), notamment via un message spécialement conçu ;
- la qualité du filtrage des messages au niveau de la passerelle de messagerie est plus haute, car les fonctionnalités de l'antivirus ne sont pas limitées par le serveur de messagerie.

5. Le filtrage des emails doit être complet

Seules les solutions complètes pour la messagerie, comprenant un antivirus et un antispam, peuvent assurer sa protection et réduire les dépenses de l'entreprise. L'utilisation de l'antivirus sans l'antispam :

- permet aux hackers de lancer des attaques sur les serveurs de messagerie de l'entreprise et sur les clients de messagerie ;
- augmente des frais de bande passante ;
- augmente la quantité de pourriels sur les serveurs de messagerie ;
- réduit la productivité et augmente la pénibilité pour les collaborateurs qui doivent nettoyer leurs messagerie constamment.

6. Les mesures de protection additionnelles

- Les serveurs de messagerie stockent les emails des utilisateurs – soit de manière permanente (les utilisateurs stockent tous les messages sur le serveur de l'entreprise et y accèdent via IMAP4), ou d'une manière temporaire (jusqu'au moment où l'employé commencer à travailler). Comme il y a toujours la possibilité pour **le virus** de pénétrer la messagerie avant qu'il soit analysé dans le laboratoire antivirus, il est recommandé soit d'effectuer le scan périodique des boîtes à lettres avec un antivirus, soit analyser les messages avant de les envoyer aux employés.
- Si les locaux de l'entreprise ne sont pas concentrés dans un périmètre protégé, se trouvent dans plusieurs endroits et ne sont pas connectés via un canal attribué pour recevoir et envoyer des messages, il faut utiliser une passerelle pour éviter l'interception ou le spoofing du trafic.
- Les emails malveillants ou suspects seront placés en quarantaine et/ou archivés. La quarantaine et l'archivage des messages inclus dans Dr.Web Mail Security Suite permettent de récupérer les messages supprimés accidentellement et d'analyser le trafic en cas de fuite d'informations.

Les principes de filtrage des emails au niveau de la passerelle de messagerie

1. Il est souhaitable d'effectuer le filtrage du courrier sur la passerelle de messagerie de l'entreprise(Dr.Web Mail Security Suite Antivirus + (Antispam) + SMTP proxy)

Il est **dangereux** de placer le serveur de messagerie accessible depuis Internet dans le réseau local. L'attaquant a les possibilités d'accéder au serveur ou de substituer le tra-

fic, notamment en utilisant une porte dérobée. Même si les locaux sont situés dans le même bâtiment, il y a toujours une probabilité d'interception ou de spoofing de trafic.

La meilleur solution est de placer le serveur de messagerie à la périphérie du réseau ou dans une zone démilitarisée (DMZ) pour des serveurs de messagerie de transit (ou Frontend). Les serveurs reçoivent, filtrent et redirigent les messages vers le serveur principal du réseau de l'entreprise avant que le trafic n'entre dans le réseau interne. Ces serveurs peuvent être gérés en interne ou par une autre entreprise (par exemple, un centre de données).

Il est fortement recommandé d'utiliser le filtrage du trafic de courriel au niveau de la passerelle dans les cas suivants :

- entreprise — fournisseur d'accès Internet ;
- le serveur de messagerie de l'entreprise se trouve en dehors de ses locaux (par exemple, dans un centre de données externe) ;
- l'entreprise loue les adresses email sur un service spécial ;
- les locaux de l'entreprise ne sont pas concentrés dans un périmètre protégé, se trouvent dans plusieurs endroits et ne sont pas connectés via un canal dédié.

ATTENTION !

Le serveur antivirus proxy utilisé dans les systèmes de filtrage du trafic email basé sur une passerelle permet d'améliorer significativement la qualité du filtrage notamment **grâce** à la **non limitation** des interactions entre le serveur et le logiciel antivirus. Par exemple, le serveur de messagerie MS Exchange ne permet pas de recevoir le message entier, ce qui rend compliqué son analyse antispam.

Les avantages du filtrage de la messagerie au niveau de la passerelle

- L'absence d'accès direct au serveur de messagerie depuis Internet empêche les attaquants d'utiliser les vulnérabilités (déjà connues et les vulnérabilités zéro-day), notamment via un message spécialement conçu.
- L'utilisation des solutions antivirus passerelle (par exemple, **Dr.Web Mail Security Suite Antivirus + Antispam + SMTP proxy**) :
  - améliore considérablement la sécurité du réseau ;
  - améliore significativement la qualité de filtrage grâce à l'absence de restrictions appliquées par les serveurs de messagerie ;
  - réduit la charge sur les serveurs de messagerie locaux et les postes de travail ;
  - améliore la stabilité globale du système de filtrage.
- Le traitement des messages au niveau de la passerelle empêche le spam de pénétrer sur le serveur de messagerie ce qui réduit significativement la quantité de spam et le rend plus performant et accessible aux utilisateurs. Cela réduit les dépenses IT grâce :
  - à la réduction considérable du coût du trafic ;

- au fait qu'il n'est pas nécessaire d'augmenter le nombre de serveurs ou de mettre à niveau le matériel ;
- à la réduction des dépenses liées au stockage des messages.

2. Il faut assurer la protection du serveur sur lequel la passerelle de messagerie est déployée

Comme le serveur de messagerie, la passerelle est un service qui fonctionne sur un serveur de fichiers standard. Ainsi, **si votre système d'exploitation est Windows** outre la protection de la passerelle, vous devez également protéger le serveur, c'est à dire utiliser deux produits, par exemple **Dr.Web Server Security Suite** et **Dr.Web Mail Security Suite**.

Les principes de filtrage du trafic web sur la passerelle

ATTENTION !
Si l'entreprise utilise des services Cloud ou possède des filiales, elle doit obligatoirement utiliser la passerelle de son côté, car c'est la seule mesure qui peut assurer la « propreté » du trafic web reçu.

Les solutions antivirus pour les passerelles assurent la protection contre la pénétration des logiciels malveillants sur les ordinateurs qui ne possèdent pas de protection antivirus, dans le cas où son installation n'est pas possible.

1. Les solutions antivirus pour les passerelles Internet ne représentent pas des logiciels indépendants – ce sont des modules additionnel pour les logiciels qui doivent être installés sur les serveurs et qui assurent la connexion Internet.
2. Comme le serveur de messagerie, la passerelle est un service qui fonctionne sur un serveur de fichiers standard. Ainsi, si votre système d'exploitation est Windows, outre la protection de la passerelle, vous devez également protéger le serveur, c'est à dire utiliser deux produits :
   - **Dr.Web Server Security Suite** (logiciel Dr.Web pour les serveurs de fichiers Windows) ;
   - **Dr.Web Gateway Security Suite** (logiciel Dr.Web pour les passerelles Internet Kerio ou Dr.Web pour Microsoft ISA Server et Forefront TMG).

ATTENTION !
L'absence d'une telle protection permet aux attaquants de compromettre le réseau de l'entreprise.

L'examen des incidents informatiques

L'incident informatique viral (IIV) est un incident sur l'ordinateur, causé par un logiciel malveillant ou un programme potentiellement dangereux.

Le nombre des IIV est souvent majoritaire parmi tous les incidents informatiques. Pour effectuer un IIVN, les attaquants utilisent les malwares, les programmes potentiellement dangereux la fraude ou l'ingénierie sociale, afin de provoquer le lancement, par l'utilisateur lui-même, des malwares ou d'autres programmes potentiellement malveillants.

Le service pour répondre aux incidents

En 2013, Doctor Web a commencé à proposer des services de réponse aux incidents informatiques.

Aujourd'hui Doctor Web possède d'un service de réponse aux incidents informatiques. Ce service analyse les données relatives à l'incident informatique,rédige des rapports et fournit des statistiques.

L'examen des incidents informatiques

Doctor Web effectue un examen des incidents informatiques qui ont touché la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques, **qui ont été perpétrés par des malwares**.

Le formulaire de demande d'examen :
https://support.drweb.com/expertise

Le service propose :

- Une évaluation préliminaire de l'incident, de l'importance de l'examen à effectuer et des mesures nécessaires pour remédier à ses conséquences.
- L'analyse des données relatives à l'incident informatique (disques durs, textes, sons, photos, vidéos).
- **Unique !** Un examen psycho morphologique de personnes (personnel) pour étudier l'implication / aide / dissimulation / promotion d'actes illégaux contre le client, le manque d'action ou la négligence.
- Les recommandations relatives à l'organisation du système de protection antivirus afin de prévenir les IIV ou de les réduire dans l'avenir.

Comment agir lors de l'incident informatique

Les vols d'argent sur des banques en ligne

En règle générale, les victimes remarquent le vol une fois qu'il a eu lieu. Votre réaction à cet incident peut être très utile.

ATTENTION !

– Si vous êtes piraté, ne mettez pas à jour votre antivirus et ne lancez pas le scan antivirus : vous pouvez effacer les traces des actions des pirates dans votre système !

– N'essayez pas de réinstaller le système d'exploitation !

– Ne supprimez pas des fichiers ou des programmes de votre disque dur !

– N'utilisez jamais un ordinateur qui a été piraté.

Vos actions doivent être rapides et décisives :

1. Contactez immédiatement votre banque – peut-être il est encore possible d'annuler le paiement. Même si le paiement est déjà effectué, demandez de bloquer toutes les opérations sur le compte compromis avant que vous ne receviez les nouveaux éléments d'authentification (nom d'utilisateur et mot de passe, etoken, etc.).
2. Ecrivez une demande à votre banque (honorant le paiement) et envoyez-la par fax. Imprimez la demande en trois exemplaires, et déposez les à la banque. Demander de mettre le numéro d'enregistrement sur les deux exemplaires – l'un pour vous, l'autre pour votre plainte à la police.
3. Ecrivez une demande à la banque bénéficiaire et envoyez-la par fax. Comme au dessus, il faut préparer trois exemplaires et les enregistrer.
4. Déposez une plainte à la police avec les demandes effectuées aux deux banques (expéditeur et bénéficiaire). Pour le faire, visitez la succursale la plus proche.

ATTENTION !

Vous êtes la victime d'une crime. Pour ouvrir une enquête, la police doit avoir une plainte.

5. Ecrivez une demande à votre fournisseur d'accès pour obtenir les logs de connexions réseau.

ATTENTION !

Les FAI gardent les logs 48 heures seulement !

IMPORTANT !

Imprimez toutes les demandes pour les avoir toujours disponibles. **Il faut tout faire dans les 24–48 heures à partir de la date du vol !**

Les fichiers cryptés par les Trojans Encoder

Les Trojans encoders cryptent les fichiers de l'ordinateur infecté. Il est possible de les restaurer. Contactez rapidement le support technique de Doctor Web !

ATTENTION !

- N'utilisez pas l'ordinateur infecté avant de recevoir les instructions du support technique.
- N'essayez pas de réinstaller le système d'exploitation !
- Ne supprimez pas des fichiers ou des programmes de votre disque dur !
- Si vous avez lancé le scan antivirus, ne traitez/supprimez pas les logiciels malveillants. Avant d'engager une action vis-à-vis des menaces trouvées, consultez les spécialistes de Doctor Web ou sauvegardez les menaces, car cela peut être utile pour le décryptage.

Il est recommandé de déposer une plainte à la police.

Le Trojan a bloqué Windows

ATTENTION !

Ne payez pas la rançon demandée par les attaquants, car vous ne recevrez jamais le code de déverrouillage !

Profitez du service gratuit de décryptage de Doctor Web.
https://www.drweb.com/xperf/unlocker

Il est recommandé de déposer une plainte à la police.

Doctor Web France

333 b Avenue de Colmar, 67100 Strasbourg
Teléfono: +33 (0) 3-90-40-40-20
Fax: +33 (0) 3-90-40-40-21
www.drweb.fr