Dr.WEB®
depuis 1992

Protégez votre univers

Cours DWCERT-070-3
La protection antivirus de l'entreprise

Formation :
La protection antivirus de l'entreprise

Sommaire

09.06.2014

I. 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

Une telle «organisation du travail» a permis aux cybercriminels de tester leurs malwares sur toutes les solutions antivirus actuelles. Le fait que les virus et les Trojans soient testés par les malfaiteurs sur les antivirus actuels permet aux hackers de parfaire leurs techniques et de mieux réussir leurs attaques. 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.

Le passage à l'envergure industrielle du développement des logiciels malveillants a augmenté significativement le nombre de malwares non détectés au moment de leur pénétration dans un système.

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.

- Le Laboratoire de veille et de recherche sur les menaces reçoit des échantillons du monde entier.
- Chaque jour, le laboratoire antivirus Doctor Web analyse au moins 100.000 échantillons de malwares.

Plus d'informations : http://live.drweb.com.

Les analystes ne sont pas des magiciens et ne peuvent pas analyser tous les fichiers suspects reçus. L'un des éléments le plus important de l'antivirus est le système de traitement du trafic entrant. La performance de ce système est aussi importante que la qualité de la protection sur les ordinateurs des utilisateurs.

UNE IDÉE FAUSSE.

L'antivirus doit détecter 100% des virus.

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.

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 supposédes 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).

Les faits.

- La base virale Dr.Web possède un nombre minimum d'entrées. Une seule entrée dans la base de données virales Dr.Web permet d'identifier des dizaines, des centaines voire des milliers de virus similaires. La principale différence entre la base virale Dr.Web et les bases virales des autres éditeurs est que la base de Dr.Web détecte le même nombre (ou plus) de virus et de programmes malveillants avec un petit nombre d'entrées.
- Doctor Web ne cesse de développer des technologies de détection des logiciels malveillants et sort des nouvelles versions de son noyau antivirus périodiquement. Lors de la sortie d'un nouveau noyau antivirus, le code est optimisé et le nombre d'entrées dans la base réduit, ce qui augmente encore la vitesse de fonctionnement de l'antivirus.

La diminution du nombre d'entrées est le résultat de l'application de nouvelles technologies de détection : Dr.Web peut détecter plus de malwares avec un nombre d'entrées plus petit !

- Et même s'il n'y a pas d'entrée du virus dans la base Dr.Web, il sera détecté grâce aux multiples technologies utilisées dans le noyau antivirus.
- L'addition d'une nouvelle entrée ne réduit pas la vitesse du scan !

Quels sont les avantages pour les utilisateurs d'une base virale compacte?

- Une plus grande vitesse de recherche des malwares
- Une réduction des pré-requis système
- Exige moins d'espace libre sur le disque dur
- Une économie du trafic lors de la mise à jour de la base virale
- La capacité de détecter des virus qui apparaîtront dans l'avenir en se basant sur une signature déjà présente dans la base.

ATTENTION !

Des millions de personnes dans le monde utilisent chaque jour un produit unique : Dr.Web CureIt!, conçu pour analyser les ordinateurs et les traiter en cas d'infection, sans désinstaller l'antivirus en place.

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.

UNE IDÉE FAUSSE.

Même si l'ordinateur est infecté, il est moins cher de restaurer Windows depuis une sauvegarde que d'acheter un antivirus.

Menaces.

Un logiciel malveillant peut se dissimuler dans des fichiers stockés d'autres partitions du disque dur et sur des supports amovibles. Dans ce cas, la réinstallation de Windows ne peut pas résoudre le problème : Dès que l'utilisateur accède à ce fichier, le malware est réactivé.

ATTENTION !

Seul un antivirus est capable de lutter contre un Trojan qui a déjà pénétré le système.

Si vous n'avez pas fait de sauvegarde de chaque poste de travail — pas de panique. Si, avant l'installation de Dr.Web, votre système a été infecté, Dr.Web va le traiter et l'ordinateur fonctionnera normalement. Pour le traitement des infections actives, il est suffisant d'effectuer un scan rapide de votre ordinateur, et toutes les menaces trouvées seront neutralisées. Le traitement de plusieurs ordinateurs dans le réseau prendra moins de temps que la restauration de leurs systèmes depuis des sauvegardes. Dans ce cas :

- les fichiers contaminés seront désinfectés ;
- le registre Windows sera automatiquement corrigé ;
- les services malveillants seront automatiquement supprimés ;
- les rootkits et bootkits seront automatiquement supprimés.

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

09.06.2014

II. 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.

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.

Ne désactivez JAMAIS la mise à jour automatique de votre antivirus !

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.

Les Trojan.Carberp pénètrent les ordinateurs lorsque les utilisateurs **naviguent sur des sites piratés**. *Or votre système est 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 aux hommes d'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.

ATTENTION !

Parmi les supports amovibles nous ne trouvons pas seulement les clés USB, mais également tous les périphériques USB ! *Le virus peut être transmis d'un ordinateur à un autre via un appareil photo ou un lecteur MP3.*

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.

Aujourd'hui, nombreux sont les collaborateurs qui ne travaillent pas uniquement au sein de l'entreprise, mais continuent à travailler de chez eux ou lors de leurs déplacements, de même que pendant leur temps libre. Il faut également prendre en compte les collaborateurs travaillant à distance. Tout cela représente un avantage pour l'entreprise, mais également pour les cybercriminels.

A l'époque, les administrateurs système pouvaient garantir le niveau de sécurité demandé, car ils contrôlaient tous les appareils dans l'entreprise. Maintenant, c'est impossible.

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.

Les faits.

- Les employés peuvent être de vrais professionnels dans leur domaine, mais ils ne sont pas forcément des experts de la sécurité antivirus et ils peuvent manquer d'attention vis-à-vis de ces questions.

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.

Lamajorité 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.

III. Les objectifs de l'entreprise. Comment l'activité de l'entreprise est-elle liée à la structure du réseau local ?

En général, les employés de l'entreprise :

- Créent des fichiers texte et image sur les ordinateurs et les appareils mobiles ;
- Envoient/reçoivent des emails à /de la part de contacts appartenant à l'entreprise ou externes.
- Reçoivent/envoient depuis/àl'extérieur des données ;
- Stockent ces données dans le système de l'entreprise ou téléchargent des données depuis le système de sauvegarde.

Il est difficile de trouver une entreprise dont les employés n'ont pas ces pratiques, devenues courantes.

Pour le bon fonctionnement de l'entreprise, son réseau doit comprendre :

- des postes de travail et/ou des terminal clients — sur lesquels les employés ou des visiteurs peuvent travailler ;
- des serveurs de fichiers pour le stockage de données, ainsi que pour l'échange d'informations entre les employés de l'entreprise ;
- des serveurs de bases de données, des serveurs d'applications (par exemple un serveur 1C), des serveurs DNS/DHCP/Active Directory — pour effectuer le travail quotidien et relier les ordinateurs à un réseau.
- des serveurs de messagerie — pour traiter le courrier interne et externe;
- des passerelles Internet — pour assurer la sortie du réseau interne de l'entreprise au réseau externe (pas toujours Internet).

Bien sûr, chaque entreprise ne doit pas obligatoirement posséder ces composants, mais dans la plupart des cas, l'entreprise possède des postes de travail et au minimum un serveur de messagerie et une passerelle Internet.

Il existe peu d'exceptions et surtout dans les cas suivants:

- **Tous les employés ou un groupe d'employés accèdent à Internet via leur canal dédié.** Dans ce cas, il n'y a pas de serveur ni de passerelle Internet. Ce type d'organisation est très rare, car il est le plus cher. Il est utilisé par les petites entreprises ou par les entreprises qui embauchent beaucoup d'employés externes, qui utilisent les services publics pour échanger des données.
- **L'entreprise utilise des serveurs externes.** Dans ce cas, l'entreprise loue les adresses emails ou les domaines emails sur un serveur externe (par exemple sur gmail.com).

Si l'entreprise possède des serveurs. La question est,

- **combien de serveurs il y a dans l'entreprise ;**
- **comment leurs rôles sont-ils répartis ;**
- **où se trouvent-ils (locaux ou distants) ;**
- **leur accessibilité par les utilisateurs (via le réseau local ou via Internet), etc.**

Les réseaux locaux des fournisseurs de services.

Les réseaux de fournisseurs d'accès Internet ont deux réseaux locaux indépendants. Le premier est le réseau interne de l'entreprise avec son serveur de messagerie, passerelle Internet et postes de travail des employés. Et le second réseau fournit le service aux clients. Ainsi, le réseau du fournisseur d'accès Internet comprend les composants suivants.

- Une passerelle pour l'accès des clients à Internet. Les utilisateurs accèdent via cette passerelle aux sites Internet, aux serveurs de messagerie externes, aux postes de travail distants.
- Le serveur de messagerie sur lequel l'entreprise peut créer des boîtes aux lettres ou louer des domaines.
- Le réseau interne du fournisseur dans lequel l'entreprise peut placer ses sites, fichiers, documents. D'habitude, ce trafic de réseau interne est gratuit pour les clients.
- Les serveurs virtuels sur lesquels l'entreprise peut créer ses propres serveurs.
- Les postes de travail et/ou les terminal clients des employés du fournisseur.
- Le serveur de messagerie interne du fournisseur combiné (mais pas obligatoirement) avec le serveur dont les services sont fournis aux clients

Les grands fournisseurs peuvent posséder plusieurs serveurs. Cela se fait soit pour équilibrer la charge aux heures de pointe, soit pour la redondance en cas de panne d'un ou plusieurs serveurs. Le nombre de serveurs dépend de la taille du fournisseur et du nombre de services offerts aux clients.

Les fournisseurs d'accès Internet peuvent assurer la protection des utilisateurs contre les virus et le spam :

- en utilisant les agents antivirus et antispam sur les ordinateurs des clients ;
- en traitant le trafic email et Internet des clients.

Il est recommandé d'utiliser ces deux méthodes, car :

- le traitement du trafic au niveau du fournisseur réduit la charge sur l'ordinateur du client (grâce à l'absence de spam) ;
- la protection antivirus au niveau de l'utilisateur bloque la pénétration de virus depuis les clés USB.

Les systèmes spéciaux.

Un certain nombre d'entreprises et d'institutions nécessitent un système de protection antivirus spécialisé.

Par exemple :

Les systèmes supportant une lourde charge

La particularité de ces systèmes est que les applications installées utilisent toutes ou presque toutes les ressources du système. Par exemples, les ordinateurs utilisés par les designers ou constructeurs.

Il est possible d'installer sur cette machine tous les composants antivirus sauf le moniteur de fichiers.

Comme cette configuration n'assure pas **une protection résidente**, il est recommandé d'autoriser le scan des archives, ainsi que le scan antivirus fréquent (une fois par semaine au minimum).

Le noyau antivirus de Doctor Web utilise peu de ressources système et peut automatiquement diminuer sa priorité en cas de charge élevée.

Les systèmes temps réel.

La particularité des systèmes temps réel est :

1. Le respect du temps d'exécution de chaque opération dans leur séquence - les cyclogrammes. Ce sont des systèmes qui assurent des processus techniques spécifiques (le ravitaillement de la station essence ou le dépôt du carburant), ou les systèmes militaires (le lancement d'un missile).

Comme vous le savez, le scan antivirus d'un fichier n'a pas de temps réglementé, il est modifié après chaque mise à jour.

Donc, il est impossible d'utiliser un système antivirus standard dans les systèmes temps réel.

2. Les systèmes temps réel tournent non seulement sous les modifications des OS standards (Windows NT4, Windows Embedded), mais également sous des systèmes d'exploitation spéciaux, comme Neitrino.

   Les OS spéciaux ne sont pas compatibles avec les systèmes antivirus.

En ce qui concerne les systèmes temps réel basés sur les OS standard, il est possible d'utiliser le scanner antivirus, configuré pour le scan du système lors du démarrage. De plus, il faut utiliser ce système au sein du segment du réseau local dans lequel le trafic réseau est scanné avant son traitement sur la machine protégée.

IV. La structure générale des réseaux locaux.

Selon l'activité de l'entreprise, la structure d'un réseau local peut comporter les variantes suivantes :

- **Les ordinateurs sont séparés sans connexion entre eux et Internet.** Cette organisation est appliquée dans les entreprises qui manipulent des documents classifiés. Dans ce cas, le réseau des ordinateurs individuels ou des serveurs, et le transfert de données entre l'ordinateur et le reste du réseau est assuré par des outils spécialisés.
- **Les ordinateurs séparés sans connexion entre eux, mais avec connexion Internet.** Cette version est utilisée lorsque les employés de l'entreprise travaillent à la maison ou si l'entreprise travaille aveec des free-lance. Chacun de ces employés accède à Internet pour échanger des données.
- **Les ordinateurs reliés en réseau, sans connexion Internet.** Ce type est utilisé dans les réseaux qui exigent un haut niveau de sécurité. Dans ces entreprises, il y a un réseau gérant les ordinateurs avec connexion Internet, et un réseau isolé de l'Internet. Dans ce cas, le transfert de données entre les réseaux externe et interne est assuré par des outils spécialisés.
- **Les ordinateurs reliés en réseau, avec connexion Internet.** C'est le cas le plus fréquent dans la pratique.

En plus de la topologie du réseau, il faut prendre en considération le type d'accès utilisateur à l'ordinateur. Il existe deux types — **mono-utilisateur et multi-utilisateurs**. Dans le premier cas, un seul utilisateur peut travailler sur l'ordinateur, dans le second, plusieurs. En règle générale, à part l'utilisateur, un administrateur système a également accès à un ordinateur, c'est pourquoi tous les réseaux sont multi-utilisateurs par défaut.

Aujourd'hui, les réseaux multi-utilisateurs sont organisés **sur la base de groupes de travail** ou **sur la base de domaines**. Les autres variantes (réseaux ad-hoc basé sur Novell Netware) sont plus rares. La différence entre les groupes de travail et les domaines est que dans ce dernier cas, le réseau dispose d'un serveur de domaine (au moins un ou deux — le principal étant celui de réserve), dans lequel la structure Active Directory conserve l'information sur les utilisateurs et les ordinateurs du réseau, les politiques de groupe du réseau, les mots de passe, etc.

L'information sur l'organisation du réseau est très importante. S'il n'y a pas de structure de domaines, rien ne peut garantir qu'un seul mot de passe pour le compte administrateur est utilisé sur tous les ordinateurs, ce qui rend difficile le déploiement de la protection antivirus, en augmentant le temps de préparation du réseau pour le déploiement.

L'impact de la législation.

La structure du réseau, ainsi que son système de protection antivirus dépend de l'activité de l'entreprise, soumise à des exigences légales. Par exemple, les employés de l'entreprise peuvent travailler avec des documents classés secrets ou bien l'entreprise peut être en contact avec certaines institutions étatiques.

En outre, l'entreprise peut assurer le fonctionnement d'infrastructures importantes (chemins de fer, centrales nucléaires, etc) et doit donc respecter certaines règles légales. En règle générale dans ces entreprise, **le réseau local interne est séparé du réseau externe**, et la plupart des employés n'ont pas d'accès Internet (ou uniquement quelques services).

Le Cloud et les réseaux locaux.

Le passage au Cloud comprend le déplacement des postes de travail et des serveurs dans un centre de données ou l'utilisation de services externes.

Cela optimise le coût de l'infrastructure et augmente la fiabilité des sous-systèmes serveur, mais **apporte plus de risques pour la sécurité de l'information** :

- les malfaiteurs ainsi que les malwares peuvent accéder aux données de l'entreprise sur les serveurs distants (ainsi qu'exploiter des vulnérabilités de machines infectées sans protection adéquate),
- Les données peuvent être interceptées et/ou modifiées lors du transfert sur et depuis le serveur,
- L'infrastructure distante peut être défaillante ou son accès impossible.

Cette utilisation du Cloud peut causer de nouveaux risques pour la sécurité de l'entreprise :

- La hausse des dépenses en matière de sécurité du transfert de données, car il faut avoir un canal sécurisé et utiliser des produits appropriés ainsi qu'obtenir des licences pour travailler avec le cryptage.
- Aucune garantie d'inaccessibilité des données pour les employés du prestataire de service.
- Il existe un problème avec la suppression des données envoyées dans le cloud.

Et ce n'est pas tout.

Les mêmes problèmes touchent les entreprises en cas d'utilisation de services tiers cloud, car les données sont transférées via un canal sécurisé mais évitent les systèmes de sécurité, notamment antivirus, ce qui signifie que l'on peut transmettre ce que l'on veut à l'utilisateur.

En effet, lors du transfert des services de l'entreprise dans le cloud, le contrôle de la sécurité est confié au prestataire de service.

L'une des tendances lors du passage au cloud est l'utilisation d'un antivirus cloud. En général, les centres de données sont basés sur VmWare. Dans ce cas, pour assurer une protection antivirus sur tous les centres de données, il faut créer une machine virtuelle sur chaque serveur, qui va filtrer tout le trafic et analyser toutes les opérations avec les fichiers, effectuées sur toutes les machines virtuelles du centre, mais ces machines ne sont pas dotées d'un antivirus. Ce systèmede sécurité est basé sur l'idée que l'antivirus doit détecter tous les malwares qui tentent de pénétrer le système, mais ne tient compte du fait que l'antivirus doit également détecter les menaces inconnues au moment de leur pénétration.

C'est pourquoi lors de l'utilisation de services cloud, il faut prendre des mesures pour :

- interdire l'accès aux serveurs distants, prévenir le vol et/ou la modification de données, y compris lors du transfert de données entre les serveurs, entre les serveurs et les postes de travail qui font partie du réseau local ;
- prévenir l'infection des serveurs distants lors du transfert de données ;
- réduire le temps d'indisponibilité à cause de la perte d'accès aux serveurs distants.

Pour ce faire il est possible d'utiliser :

- des systèmes de chiffrement ainsi que des canaux VPN ;
- 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.

Comme exemple de l'utilisation de services externes, nous pouvons citer le service « Dr.Web Antivirus » pour les entreprises. L'entreprise utilise le service Internet Dr.Web AV-Desk, déployé par un fournisseur d'accès Internet au lieu d'organiser son propre système de protection antivirus. Il est important que ce service ne requière pas la connexion des postes de travail du client au serveur de la protection antivirus permanente.

L'utilisation de services externes.

Les employés utilisent souvent des services Cloud payants ou gratuits, par exemples des services de messagerie ou de stockage de données (google.docs, google.mail, google.disk et autres), dont l'accès n'est pas contrôlé par les systèmes de protection antivirus de l'entreprise.

L'utilisation de ces services inclut également des risques. Les services externes représentent un outil assez commode pour la pénétration des malwares, car personne ne peut garantir que les documents stockés dans ces services ne seront pas modifiés par quelqu'un. Les fichiers modifiés, reçus de services Cloud, pénètrent le réseau local en évitant les systèmes de protection antivirus de l'entreprise (par exemple les antivirus sur la passerelle Internet), même s'ils sont transmis via un protocole sécurisé, celui-ci n'est pas contrôlé par les moyens de protection mis en œuvre dans l'entreprise.

C'est pourquoi chaque entreprise doit protéger tous les nœuds du réseau que les malwares peuvent exploiter. Cela comprend au moins 1) les postes de travail, 2) les serveurs de messagerie et les passerelles Internet.

V. Les erreurs à éviter lors de l'organisation de la protection du réseau.

Un manque de connaissances sur les menaces actuelles, sur les capacités des systèmes antivirus, sur les exigences de la législation pour la protection des réseaux ainsi que certaines idées fausses peuvent entraîner des erreurs typiques lors du déploiement du système antivirus du réseau.

1. « La protection des postes de travail est suffisante. La protection des serveurs n'est pas nécessaire ».

Dans de nombreuses entreprises, seuls les postes de travail sont protégés par un antivirus. En effet, il est considéré que :

- Les virus peuvent pénétrer le réseau uniquement via les postes de travail, ce pourquoi il n'est pas nécessaire de protéger les serveurs ;
- tous les fichiers entrants transitent via les postes de travail, il est donc suffisant de les protéger eux et seulement eux — l'antivirus installé sur les postes doit détecter et supprimer tous les programmes malveillants ;
- personne ne travaille sur les serveurs, donc personne ne peut les infecter ;
- la protection des serveurs est un luxe coûteux.

Le résultat est qu'une telle protection antivirus **n'assure pas le niveau minimal de protection**.

Pourquoi faut-il protéger les serveurs (de fichiers, terminal server, d'applications (de bases de données)) ? :

- L'utilisateur peut infecter le serveur avec un virus **inconnu** de l'antivirus au moment de sa pénétration, et qui a d'abord contaminé son poste de travail puis s'est propagé dans le réseau. L'antivirus installé sur le serveur peut le détecter en utilisant les technologies heuristiques. Ou dans le cas extrême, l'antivirus traitera ce virus lors de la prochaine mise à jour. Sans l'antivirus, le serveur devient une source d'infection permanente.
- Le serveur peut être piraté. L'antivirus installé sur le serveur va détecter et neutraliser les malwares. 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).
- 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, ainsi que 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.

2. « L'entreprise ne doit protéger que les appareils lui appartenant ».

Aujourd'hui, personne ne peut nier la nécessité de protéger les postes de travail de l'entreprise. L'erreur la plus répandue dans l'organisation de la protection du réseau est de protéger uniquement les ordinateurs de bureau.

A l'époque, les administrateurs système pouvaient garantir le niveau de sécurité demandé, car ils contrôlaient tous les appareils dans l'entreprise.

Aujourd'hui c'est impossible, car tous les ordinateurs n'appartiennent pas à l'entreprise. Ce sont les PCs portables ou les Smartphones des employés.

60% des appareils personnels n'ont aucune protection !

Or, depuis ces ordinateurs, les employés accèdent au réseau local alors qu'ils peuvent contenir des fichiers malveillants et constituer une tête de pont pour les attaques ciblées.

C'est pourquoi l'entreprise peut souhaiter protéger tous les appareils utilisés par les employés, professionnels et personnels.

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.

3. « La fonction antivirus seule est suffisante ».

La plupart des entreprises protègent les postes de travail avec un antivirus seul. On croit que cela est suffisant – même si le virus pénètre le système, l'antivirus le neutralisera et « nous n'avons pas beaucoup de spam «.

Il est pensé à tort qu' un bon antivirus doit connaître tous ou presque tous les logiciels malveillants au moment de leur pénétration. L'utilitaire de désinfection Dr.Web CureIt! vise à neutraliser les menaces déjà présente **(malheureusement dans la plupart des entreprises, cet outil est utilisé illégalement)**, et l'antivirus, qui n'accomplit pas bien ses fonctions sera remplacé, car il est considéré comme étant de mauvaise qualité.

ATTENTION !

L'antivirus de fichiers d'hier n'assure pas le même niveau de sécurité que le système de protection antivirus d'aujourd'hui.

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.

La protection complète permet d'endiguer la 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). Un nouveau virus, qui n'a pas encore été analysé par le Laboratoire, et donc indétectable à l'instant T par les logiciels antivirus, ne pourra pas pénétrer le serveur ou le poste de travail protégés.

Les avantages de la protection complète.

- L'analyse du trafic Internet avant le traitement par le navigateur et l'analyse du trafic email avant qu'il ne soit traité par le client de messagerie. Dans ce cas, les virus ne peuvent pas exploiter les vulnérabilités des logiciels en question. Il y a déjà longtemps que les vulnérabilités des logiciels installés sont exploitées (notamment Adobe) plutôt que celles du système d'exploitation ;
- la réduction du spam dans le trafic email jusqu'à zéro augmente considérablement la productivité parce que :
  - les utilisateurs passent moins de temps à vérifier les messages entrants,
  - la probabilité de manquer ou de supprimer un message important se réduit.

4. « Toutes les menaces proviennent d'Internet. A quoi bon protéger un ordinateur sans connexion Internet ? »

Ces machines non protégées représentent des brèches dans le système de protection de l'entreprise et peuvent provoquer l'infection des réseaux locaux.

Les principaux moyens de pénétration des logiciels malveillants sur ces machines sont les supports amovibles utilisés par les employés, s'il n'y a pas de Dr. Web Office Control, installé sur l'ordinateur, qui peut limiter l'accès.

5. « Il n'y a pas de virus touchant Mac et Linux ».

Une autre idée fausse consiste à dire que vu le nombre relativement réduit de programmes malveillants ciblant les systèmes d'exploitation Mac, Linux et Unix, il faut seulement protéger les postes de travail et les serveurs 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.

6. « Le serveur n'ouvre pas les messages, donc il ne peut pas être contaminé. Notre administrateur système est compétent, il ne va pas infecter notre système ».

Oui, c'est vrai, mais si les messages sont stockés sur le serveur, seul l'antivirus pour les serveurs peut supprimer les logiciels malveillants contenus dans les boîtes aux lettres.

En outre, il ne faut pas oublier que les systèmes de protection antivirus des passerelles et des systèmes de messagerie interceptent les virus lors de la propagation (pénétration) et ne peuvent pas assurer la protection au moment de l'activation des virus (lancement), car cette étape ce passe sur les postes de travail. C'est pourquo **outre la protection** des services, il faut également utiliser un antivirus pour la protection du système de fichiers.

7. « Le Centre de Gestion du système antivirus est conçu pour faciliter le travail de l'administrateur système ».

Ce n'est pas vrai. La gestion centralisée du système de protection antivirus augmente significativement le niveau de la sécurité informatique de l'entreprise. Le Centre de Gestion Dr.Web assure **le respect des politiques de sécurité de l'entreprise** sur chaque objet protégé. Il vous permet de :

- spécifier des paramètres personnalisés d'accès pour des utilisateurs ou pour des groupes d'utilisateurs différents, sans avoir besoin de configurer la protection sur chaque poste de travail ;
- garantir que l'antivirus sur le poste est activé et fonctionne avec les paramètres spécifiés par l'administrateur réseau ;
- assurer les mises à jour de l'antivirus et les sessions de scan régulières sur le poste.

ATTENTION !

** Le Centre de gestion Dr.Web est soumis à licence gratuitement.*

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

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.*

Les faits

- Après sa mise à jour, l'antivirus peut détecter sur votre ordinateur de nombreuses menaces, auparavant inconnues de lui.

Le scanner analyse plus en profondeur le système, c'est pourquoi il peut trouver des virus non détectés par le moniteur de fichiers – **c'est tout-à-fait normal**.

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

Il convient de prêter une attention particulière à la protection du réseau lors de l'utilisation deservices 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.

Les pré-requis supplémentaires.

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.

VII. Les caractéristiques des éléments du réseau et les principes de leur protection

1. Les postes de travail et les appareils mobiles.

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. Mais les virus peuvent pénétrer l'ordinateur en utilisant d'autres moyens, pour en savoir plus, consultez la section « Les possibilités d'intrusion virale ».

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.
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.

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 sensibles 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.
- **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.

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.*

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.

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.

2. Les serveurs.

Le réseau de l'entreprise peut inclure :

- les serveurs de fichiers ;
- les serveurs de messagerie ;
- les passerelles Internet ;
- les serveurs de bases de données, les serveurs d'applications, les serveurs DNS/DHCP/Active Directory...

2.1. La combinaison des rôles de serveurs.

Les fonctions des différents types de serveurs peuvent être soit combinées sur un seul serveur, soit distribuées sur des serveurs distincts.

Dans le premier cas, un serveur peut se servir du serveur de messagerie ou combiner les fonctions du serveur de fichiers et de la passerelle Internet. C'est pourquoi si un serveur combine plusieurs fonctions (s'il ne s'agit pas devirtualisation des serveurs, voir ci-dessous) on parle de rôles du serveur – le rôle du serveur de messagerie, le rôle de la passerelle etc. Il faut connaître la différence entre la combinaison de rôles et le lancement de différents serveurs à l'aide de la virtualisation. Dans ce dernier cas, chaque serveur est lancé sur une machine virtuelle isolée et n'affecte pas le fonctionnement des autres serveurs (si nous ne tenons pas compte de l'utilisation des ressources du serveur de virtualisation).

Les fonctions de différents serveurs peuvent être combinées sur un seul serveur — s'il ne s'agit pas de virtualisation, alors on parle de rôles du serveur.

Il faut connaître la différence entre la combinaison de rôles et le lancement de différents serveurs à l'aide de la virtualisation. Dans ce dernier cas, chaque serveur est lancé sur une machine virtuelle isolée et n'affecte pas le fonctionnement des autres serveurs (si nous ne tenons pas compte de l'utilisation des ressources du serveur de virtualisation).

D'habitude, un serveur exécute les rôles du serveur de messagerie et celui de passerelle Internet. Un serveur de fichiers, en plus de sa fonction principale (le stockage de fichiers), peut être utilisé pour d'autres services. Par exemple :

- le serveur DNS/DHCP, destiné à la distribution aux utilisateurs des adresses de réseau local ;
- le serveur Active Directory, destiné au stockage de données sur les utilisateurs du réseau ;
- le serveur de base de données et le serveur d'applications (par exemple, le serveur 1C) ;
- le terminal server ;
- le serveur de messagerie ;
- la passerelle Internet.

ATTENTION !

- *La combinaison des rôles permet à l'entreprise de réduire le nombre de serveurs, mais réduit également considérablement le niveau de sécurité – le piratage d'un serveur donne accès à tous les service du réseau de l'entreprise.*
- *Du point de vue de la sécurité et de la fiabilité, il ne faut pas avoir sur la passerelle Internet d'autres services que le pare-feu.*
- *Le contrôleur AD est également recommandé sur le serveur dédié.*

Si l'entreprise n'opte pas pour la combinaison des rôles (à cause des exigences de sécurité ou de l'incompatibilité des logiciels), un serveur physique peut comprendre plusieurs serveurs virtuels, dont chacun assure un service réseau : DNS, DHCP, AD, serveur de fichiers, etc. Dans ce cas, lors du déploiement

de la protection antivirus, il faut tenir compte du fait que les machines virtuelles peuvent être contaminées via la machine exécutant le rôle de l'hyperviseur, ainsi que du risque de propagation de logiciels malveillants entre les machines virtuelles.

Les fonctions des différents types de serveurs peuvent être distribuées sur des serveurs distincts. Ces serveurs peuvent être situés soit dans l'entreprise (donc leur sécurité devra être assurée par l'entreprise), ou à distance (y compris les services Cloud).

2.2. La redondance de la charge et sa distribution.

Afin d'augmenter la fiabilité des services fournis par les serveurs, la redondance est utilisée – soit au niveau d'un serveur (utilisation de composants à haute disponibilité, matrice RAID, etc), soit au niveau du service – l'entreprise utilise plus de services que ceux dont elle a besoin, pour en avoir en back-up. Les deux schémas sont souvent utilisés :

- redondance chaude, lorsque tous les serveurs fonctionnent simultanément, et que l'équilibreur de charge distribue la charge entre les serveurs. Si un serveur tombe en panne, il ne sera plus pris en compte par l'équilibreur ;
- redondance froide, lorsqu'un seul serveur fonctionne et que l'autre sert de back-up (en cas de panne du premier).

Le nombre de serveurs fournissant un service particulier, peut être augmenté lorsqu'un seul serveur ne peut supporter la charge induite. Si la puissance d'un serveur n'est pas suffisante, soit on utilise un équilibreur de charge, soit les serveurs sont organisés en cluster. Dans le dernier cas, le serveur représente un nœud du cluster.

2.3. Les serveurs de fichiers (les serveurs de bases de données et les serveurs d'applications)

Les fonctions et les types de serveurs de fichiers.

Le serveur de fichiers est une machine qui stocke les fichiers accessibles aux utilisateurs.

Il faut comprendre la différence entre les serveurs de fichiers créés sous Windows et Unix.

Le serveur de fichiers fonctionne sous Windows, et tous les dossiers (répertoires) peuvent être accessibles (partagés) aux utilisateurs. Le serveur de fichiers constitue un des rôles du serveur, tel que le serveur DNS/DHCP, AD, le serveur de base de données, le serveur terminal, le serveur de messagerie, la passerelle Internet. Mais le serveur de fichiers ne doit pas obligatoirement être le serveur de bases de données ou fournir le service terminal. L'administrateur système choisit les rôles pour le serveur.

ATTENTION !

Dans le système d'exploitation Windows, le moniteur de fichiers de l'antivirus analyse tous les fichiers du système et pas seulement ceux qui sont disponibles pour les utilisateurs.

- La fonction de serveur de fichiers dans le système d'exploitation Unix, est, dans la plupart des cas, assurée via le sous-système Samba, qui imite les services Windows correspondants.

ATTENTION !

Dans le système d'exploitation Unix, le moniteur de fichiers de l'antivirus analyse les fichiers ouverts pour l'utilisateur. Les autres ne sont pas scannés. Cela est dû au fait que le moniteur de fichiers de l'antivirus pour Unix représente un plug-in pour le sous-système Samba.

Le nombre de serveurs de fichiers de l'entreprise.

Nous pouvons supposer que chaque entreprise possède au moins un serveur Active Directory ou DNS/DHCP. Ou même deux : le principal et celui de réserve, car son fonctionnement est très important pour

l'entreprise. Nous ne prenons pas en considération les cas où les adresses sont prescrites manuellement, car c'est pratique seulement pour les très petites entreprises.

Nous pouvons également supposer qu'une assez grande entreprise possède un serveur 1C, car ce logiciel est presque toujours utilisé par les comptables.

Protection des serveurs de fichiers

1. 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.
2. Pour bien organiser la protection du serveur il faut :

- connaître les services supplémentaires qui fonctionnent sur le serveur de fichiers ;
- connaître les conséquences du partage de plusieurs services sur un serveur protégé, ainsi que le niveau de la protection de chaque service.

> ***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.*

3. 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.

2.4. 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 :

1. Dr.Web Antivirus pour Linux
2. 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.

2.5. Les terminal server

Fonction et brève description du fonctionnement

Lorsque l'entreprise possède un terminal server, les employés travaillent directement sur le serveur, comme si le clavier, la souris et l'écran étaient connectés au serveur.

Il existe deux types de connexion au terminal server :

- en utilisant un client léger, sans disque dur, dont la seule fonction est de se connecter au terminal server ;
- en utilisant un logiciel spécial depuis un système d'exploitation standard ;

Les terminaux server peuvent fonctionner soit sous Windows, soit sous Unix.

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.

2.6. Les serveurs virtuels (y compris cloud) et les postes de travail.

Fonction et brève description du fonctionnement.

Avec le perfectionnement des performances des serveurs, la combinaison de plusieurs services au sein d'un serveur semble avantageuse. Cependant, la combinaison de services est souvent impossible ou dangereuse. La solution consiste à utiliser des serveurs virtuels — le serveur dont l'unique fonction est hyperviseur , qui contrôle les systèmes d'exploitation lancés dans l'environnent virtuel. Dans ce cas, les systèmes d'exploitation et les applications fonctionnent sur l'émulation du serveur physique.

3. Les serveurs de messagerie

Le serveur de messagerie est un service qui fonctionne sur un serveur de fichiers standard.

La fonction des serveurs de messagerie.

- le traitement du courrier entrant et sortant,
- l'envoi massif d'e-mails,
- l'échange de données entre les employés,
- la gestion électronique des documents.

Les serveurs de messagerie les plus répandus.

- Microsoft Exchange, Kerio MailServer, Lotus Domino et Communigate Pro sont des solutions commerciales.
- Sendmail, Postfix, Exim (uniquement sous Unix), ne sont généralement utilisés que dans leur version gratuite.

Le nombre de serveurs de messagerie de l'entreprise.

La bonne marche de l'entreprise dépend, entre autres, du bon fonctionnement de la messagerie **ainsi que** de l'absence de virus et de spam. Presque chaque entreprise possède un serveur de messagerie.

Les cas où les entreprises utilisent des serveurs de messagerie externes, qui ne leur appartiennent pas, sont très rares, et même si l'entreprise utilise des services cloud, les serveurs de messagerie sont généralement administrés par des employés de l'entreprise ou (dans le cas d'outsourcing) les employés y ont accès. Cependant, il y a des cas où les entreprises (généralement de petite taille), au lieu de déployer leur serveur de messagerie, peuvent louer des boîtes aux lettres à un service externe (comme gmail).

En fonction de l'organisation de l'entreprise, elle peut posséder plus d'un serveur de messagerie. Dans un réseau multi-branche, chaque branche peut avoir un serveur de messagerie, le serveur de messagerie peut être placé à la périphérie du réseau (dans une zone démilitarisée), etc.

Cloud et serveurs de messagerie.

Le placement du serveur de messagerie dans le centre de données Cloud, d'un côté, accroît la fiabilité du serveur de messagerie, car elle sera égale à celle du centre de données Cloud. Mais de l'autre côté, chaque arrêt de connexion avec le centre de données Cloud (plantage du CDC, ligne coupée) peut arrêter l'activité de l'entreprise. En conséquence, pour assurer une continuité de fonctionnement en cas de panne, il faut utiliser deux canaux vers deux fournisseurs de services, déployer au sein du réseau local de l'entreprise des serveurs de transport pour recevoir les e-mail pendant l'indisponibilité du serveur principal. De plus, l'entreprise peut utiliser des serveurs qui assurent l'intégrité des messages entre l'envoi et la réception.

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.

4. Les passerelles de messagerie

Contrairement au serveur de messagerie, la passerelle de messagerie ne stocke pas de messages – elle les traite en temps réel et les transmet aux destinataires. Les passerelles de messagerie sont utilisées :

- **Par les fournisseurs d'accès** – pour filtrer les messages des clients contre les virus et le spam.
- **Par les entreprises**, à la fois pour réduire la charge sur le serveur de messagerie, et pour l'isoler de l'Internet (sécurité élevée).

Le filtrage des emails contre le spam et les malwares au niveau des passerelles de messagerie est plus efficace que le filtrage au niveau du serveur de messagerie. Tout serveur de messagerie limite les fonctionnalités de l'antivirus. Par exemple, l'analyse antispam est rendue compliquée par le serveur de messagerie MS Exchange qui ne permet pas de recevoir le message en entier. De plus, dans ce cas, les statistiques ne reflètent pas le nombre exact d'emails analysés, car le plug-in API (l'interface de l'interaction du serveur de messagerie avec le module de filtrage antispam et antivirus) affiche le nombre des parties de messages vérifiées.

Les passerelles de messagerie possèdent des modules pour recevoir et envoyer les messages ainsi qu'une connexion Internet. C'est pourquoi elles peuvent effectuer un filtrage et une vérification de l'authenticité des messages.

ATTENTION !

En cas d'utilisation de services de messagerie Cloud, l'entreprise doit posséder les passerelles de messagerie, car c'est le seul moyen de recevoir un trafic email sain.

Les types de passerelles de messagerie.

La plupart du temps, les passerelles de messagerie sont basées sur les systèmes d'exploitation Unix. Pourtant il existe deux variantes : l'utilisation d'un serveur de messagerie standard (souvent gratuit, comme Postfix ou Sendmail) comme serveur de transport ou l'utilisation de solutions antivirus spéciales, qui ont un module de transport des messages.

L'utilisation en tant que passerelle d'un rôle du serveur MS Exchange (Edge) est plus rare. Les rôles de MS Exchange peuvent soit être exécutés sur un serveur soit être distribués entre les serveurs. Un des rôles de MS Exchange est la passerelle de messagerie. Toutefois, en raison des particularités de licencing, la répartition de rôles exige l'achat de licences particulières, c'est pourquoi l'utilisation de **Dr.Web SMTP proxy** au lieu du rôle Edge permet de réaliser des économies.

Les logiciels ainsi que les appliances peuvent être utilisés en tant que passerelle de messagerie assurant le scan complet de tout trafic transistant via tous les protocoles, y compris les services de messagerie externes.

ATTENTION !

Du point de vue de la sécurité et de la fiabilité, il ne faut pas avoir sur la passerelle Internet d'autres services que le pare-feu. Le contrôleur AD est également recommandé sur le serveur dédié.

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 trafic, 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**.

5. Les passerelles Internet.

Fonction et brève description du fonctionnement.

Les passerelles Internet ont pour fonction d'assurer la connexion Internet de les utilisateurs de l'entreprise.

Les solutions antivirus pour les passerelles permettent :

- D'éliminer la possibilité d'exploitation des vulnérabilités par les malwares, y compris les failles inconnues, ce qui va réduire la probabilité de l'infection du réseau local ;
- D'accélérer le fonctionnement des postes de travail grâce au transfert des systèmes de scan antivirus sur la passerelle.

Les solutions antivirus pour les passerelles permettent de limiter l'accès aux ressources web et fichiers conformément à la politique de sécurité de l'entreprise.

Les logiciels ainsi que les appliances peuvent être utilisés en tant que passerelle pour le filtrage du trafic Internet sortant et entrant via tous les protocoles, même si les employés ont un accès Internet non limité.

Toute entreprise dont les employés ont un accès Internet libre a une passerelle Internet. L'entreprise ayant des succursales doit posséder un nombre de passerelles égal au nombre de ses filiales.

Il faut protéger la passerelle de l'entreprise si :

- les serveurs de l'entreprise se trouvent en dehors de ses locaux,
- l'entreprise possède des filiales,
- les départements de l'entreprise se trouvent dans différents lieux.

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 principes de filtrage du trafic web sur la passerelle.

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.

VIII. 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. Avant de suivre nos recommandations, assurez-vous que le vol a été causé par le virus. Pour ce faire, interrogez brièvement les employés qui travaillent avec la banque en ligne. Si vous ou eux n'ont pas effectué l'opération suspecte, dans la plupart des cas c'est un virus ou un attaquant.

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.
   Exemple de demande
3. Ecrivez une demande à la banque bénéficiaire et envoyez-la par fax. Comme au dessus, il faut préparer trois exemplaires et les enregistrer.
   Exemple de demande
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.
   Exemple de demande

   ATTENTION !
   Vous êtes la victime d'une crime.
   Pour ouvrir une enquête, la police doit avoir une plainte.
   Exemple de demande
5. Ecrivez une demande à votre fournisseur d'accès pour obtenir les logs de connexions réseau.
   Exemple de demande

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 via Internet depuis un autre ordinateur !

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.*

Comment établir une demande au support technique de Doctor Web

1. Remplissez le formulaire de requête au support technique.
2. Précisez le maximum d'information sur la menace y compris les exigences des attaquants. Si vous avez des suppositions sur ce qui a provoqué l'infection, ajoutez à votre demande les liens ou fichiers appropriés.
3. Joignez quelques fichiers cryptés (si possible, des fichiers de type et de taille différents (jpg, zip, doc, pdf, etc) et les exigences des attaquants.
4. Si vous avez reçu ce Trojan via email, sauvegardez ce message (si vous ne l'avez pas supprimé) en fichier eml et ajoutez-le à votre commentaire dans la requête.

Soumettre une requête pour le décryptage.

Il est recommandé de déposer une plainte à la police.

Vous êtes la victime d'une crime.
Pour ouvrir une enquête, la police doit avoir une plainte.
Exemple de demande
Votre ordinateur peut être réquisitionné pour examen.

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.

Il est recommandé de déposer une plainte à la police.

Pour ouvrir une enquête, la police doit avoir une plainte.
Exemple de demande

SARL Doctor Web

Doctor Web est un développeur russe de solutions de sécurité informatique. Les produits antiviraux Dr.Web sont élaborés depuis 1992.

Doctor Web France

Adresse: 333b, Avenue de Colmar, 67100 Strasbourg

Tél. : 03 90 40 40 20 **, fax. :** 03 90 40 40 21

www.drweb.fr | www.drweb.com | www.av-desk.com | freedrweb.com | mobi.drweb.com