Dr.WEB®
a partir de 1992

SISTEMA ANTIVIRUS
DE PROTECCIÓN
DE LA EMPRESA

Contenido

Amenazas de virus actuales

MITO

Los hackers solitarios crean virus.

Hace mucho, los creadores del software nocivo eran informáticos solitarios. Los programas nocivos modernos no solamente se desarrollan por los creadores de virus profesionales - es un negocio criminal bien organizado en el que participan los desarrolladores de software de sistema y aplicación de alta cualificación.

Elementos de estructura de algunas comunidades criminales

En algunos casos, los roles en comunidades criminales puede distribuirse de forma siguiente:

1. Organizadores - las personas que organizan y controlan el proceso de creación y uso del software nocivo. El software nocivo puede ser usado directamente o vendido a otros delincuentes o grupos criminales.

2. Participantes:

- Desarrolladores de software nocivo
- Testers de software creado
- Investigadores de vulnerabilidades en sistemas operativos y software aplicado para delincuencias
- Expertos en uso de comprimidores de virus y cifrado
- Distribuidores de software nocivo, expertos en ingeniería social
- Administradores de sistemas que aseguran un trabajo seguro distribuido dentro de la comunidad criminal y la administración de botnets
- Hoy día, es muy popular el servicio de desarrollo de programas nocivos, por lo tanto, crece el número de archivos nocivos - para "obtener" un código nocivo ahora no hace falta ser informático.

Vectores principales de ciberdelincuencia comercial

- Compromiso de sistemas informáticos – para unirlos a varias botnets, robar la información del sistema, organizar los ataques (D)DoS.
- Extorsión y/o daño de la información.

- Robos de los medios de autenticación para sistemas de banca en línea y sistemas de pagos en línea - para robar dinero posteriormente.
- Robos de los datos de tarjetas bancarias - para robar el dinero posteriormente.
- Fraude vinculado a marcas - para sacar beneficio o para desacreditar.
- Robos del contenido propietario - para su uso ilegal.

Causas de crecimiento del número de delincuencias realizadas con programas informáticos:

- crecimiento del número de programas nocivos,
- los creadores de virus desarrollolan de las nuevas amenazas que funcionan aún mejor
- los virus usan las vulnerabilidades aún no corregidas por los productores del software,
- las víctimas usan el software sin licencia (así mismo, el antivirus),
- uso incorrecto de los medios de protección (así mismo, del antivirus),
- no se cumplen las reglas de comportamiento seguro en Internet (así mismo, se desactivan
- algunos componentes del antivirus),
- configuración de seguridad incorrecta (así mismo, del antivirus),
- no se cumplen las reglas básicas de seguridad informáticas,
- factor humano - distracción, negligencia etc.

Para atacar los sistemas informáticos de empresas, los ciberdelincuentes usan:

- desventajas de sistemas antivirus de protección de todos los nodos de la red corporativa o ausencia del sistema de protección antivirus (no se trata de uso de antivirus, sino de sistemas de protección antivirus);
- desventajas o ausencia de directivas de seguridad informática en empresas;
- el personal de las empresas no cumple con las directivas de seguridad informática porque no dispone de la información básica sobre la seguridad informática, no se percata del problema, por negligencia;
- medios de la ingeniería social.

¡ATENCIÓN!

El antivirus es una herramienta básica para afrontar ciberdelincuencias.

Antes de lanzar los programas nocivos, los grupos criminales hacen tests de los mismos para asegurarse de que estos programas no pueden ser detectados por todas las soluciones antivirus actuales, lo que permite a los malintencionados implementar los virus esquivando la protección antivirus. Ningún programa antivirus, por muy bueno que sea en cuanto a los tests heurísticos, puede hacer nada en este caso - si el usuario no usa las posibilidades de la Protección preventiva y del Control de oficina.

Así mismo, cada día con mayor frecuencia, los grupos criminales crean las así llamadas amenazas objetivo - los programas nocivos desarrollados para infectar los grupos de usuarios en concreto (por ejemplo, los usuarios de un banco). Suelen ser programas nocivos creados correctamente que no afectan mucho el funcionamiento de los equipos infectados y no pueden

ser detectados por los medios de protección en el momento de infección, lo que permite a estos programas permanecer ocultos durante mucho rato.

Cono la creación de virus hoy día es un negocio criminal, ya no tienen mucho sentido los test de programas antivirus como criterios de selección de los medios de protección antivirus.

Gracias a la buena organización de los grupos criminales que se dedican al desarrollo y difusión de virus, este negocio ya tiene forma industrial. Por lo tanto, el número de programas nocivos creados por los malintencionados aumenta bastante, al igual que el número de entradas de firmas añadidas a las bases de virus a diario.

REALIDAD

Cada 24 horas hasta un millón o más muestras de programas nocivos llegan al laboratorio antivirus Doctor Web.

MITO

Un antivirus debe detectar hasta un 100% de todos los virus.

En otras palabras, un antivirus de calidad debe detectar todas o casi todos los programas nocivos en el momento de su penetración. Un antivirus que omite los programas nocivos no se considera de calidad y debe ser sustituido.

Antecedentes de este mito

EEn el sector antivirus ya hace mucho existen los así llamados test comparativos de detección realizados por los testers "independientes". Para estos tests, se usa una colección de virus y programas autónomos, los antivirus se actualizan y se realizan tests de esta colección. Para ganar, hay que detectar el 100% de los virus de la colección.

Las peculiaridades de estos tests son:

- Ningún tester puede garantizar que solo hay programas nocivos en su colección;
- Estos tests revelan solo una función del antivirus - la detección de amenazas;
- en estos tests, se valora la calidad solo de un componente del antivirus - monitor de archivos o escaner - es decir, se hacen tests para ver cómo el antivirus afronta las amenazas conocidas, no activadas.
- estos tests no revelan el funcionamiento del antivirus en caso de infección del equipo por un virus, si puede desinfectarlo o detectar las amenazas desconocidas.
- Este mito fue creado por causa de realizar estos tests.

La función del antivirus es la eliminación de los archivos malintencionados, pero el mismo puede eliminar solo amenazas conocidas para la base de virus o las amenazas que pueden ser detectadas por mecanismos heurísticos. Antes de recibir actualizaciones, el antivirus no puede detectar ni eliminar una nueva amenaza desconocida.

REALIDAD

Los virus tecnológicamente complicados y los más peligrosos, entre ellos, los rootkits, se crean para sacar beneficio comercial. Los creadores de virus los escanean para ver si pueden ser detectados por todos los antivirus, antes de lanzar un virus de este tipo. Necesitan que el virus funcione durante el periodo máximo posible en el equipo infectado. Desde el punto de vista de creadores de virus, si un virus es fácil de detectar, no es un buen virus. Es por eso que antes de llegar las muestras de programas nocivos al laboratorio antivirus, muchos de ellos no se detectan por el antivirus.

Un virus puede penetrar en un equipo a través de vulnerabilidades del día cero (los así llamados 0day exploits — es una vulnerabilidad que aún solo conoce el creador de virus o para corregir la cual el productor aún no ha lanzado un parche), o bien usando los métodos de la ingeniería social — es decir, se iniciará por el mismo usuario que también puede deshabilitar la protección automática del antivirus.

MITO

Los antivirus capturan los virus por firmas (entradas en las bases de virus).

Si fuera así, el antivirus no podría afrontar las amenazas desconocidas.

Pero un antivirus no dejó de ser el mejor y el único medio eficaz de protección contra todos los tipos de amenazas malintencionadas — y lo que es más importante — tanto conocidos como desconocidos para la base de virus del antivirus.

En los productos Dr.Web para la detección y la desinfección del software malintencionado desconocido se aplican muchas tecnologías eficaces que no son de firmas y cuya combinación permite detectar las amenazas más nuevas (desconocidas) antes de registrar una entrada en la base de virus. Vamos a ver solo algunas de ellas.

- **La tecnología Fly-Code** — asegura el escaneo de calidad de objetos empaquetados ejecutables, descomprime cualquier empaquetador (hasta no estándar) por medio de virtualizar la ejecución del archivo, lo que permite detectar los virus empaquetados hasta por los empaquetadores desconocidos para el software Dr.Web antivirus.
- **La tecnología Origins Tracing** — al escanear un archivo ejecutable, el mismo se ve como una muestra diseñada de una forma determinada, y luego se compara la imagen obtenida con la base de programas malintencionados conocidos. La tecnología permite distinguir los virus aún no añadidos a la base de datos Dr.Web con alto grado de probabilidad.
- **Tecnología del análisis de la entropia estructural** — detecta las amenazas desconocidas por los tipos de ubicación de las partes del código en los objetos escaneados protegidos por los criptoempaquetadores.
- **La tecnología ScriptHeuristic** — previene la ejecución de cualquier script malintencionado en el navegador y en los documentos PDF, sin dañar asimismo la funcionalidad de los scripts legítimos. Protege contra la infección por los virus desconocidos a través del navegador web. Funciona sin distinción del estado de la base de virus Dr.Web junto con cualquier navegador web.
- **La tecnología Dr.Web ShellGuard bloquea el acceso al equipo para los exploits** — los objetos nocivos que intentan usar las vulnerabilidades, así mismo, las desconocidas para todos excepto los creadores de virus (las así llamadas vulnerabilidades del «día cero»), para obtener el control de aplicaciones atacadas o el sistema operativo entero, controlando los procesos iniciados "desde dentro".
- **Analizador heurístico tradicional** — contiene los mecanismos de detección de programas malintencionados conocidos. El funcionamiento del analizador heurístico está basado en el conocimiento (heurísticas) de determinadas peculiaridades (características) de virus - tanto características al código de virus en concreto, como al revés, que raras veces se encuentra en los virus. Cada una de estas características se caracteriza por su "peso" - un número cuyo módulo determina la importancia de la característica en cuestión, y el signo, respectivamente, indica si se confirma o se rechaza la hipótesis sobre la posible existencia del virus desconocido en el código analizado.

MITO

¡Ya hace mucho que no existen los virus!

En realidad, más de 90% de amenazas modernas no pueden llamarse virus, porque no tiene mecanismos de autoreplicación (difusión autónoma sin participación del usuario). La mayoría de las amenazas modernas son programas troyanos. Al igual que los virus, son programas nocivos y pueden dañar bastante el equipo infectado.

Troyanos peligrosos:

1. Son invisibles para usuarios y para algunos programas antivirus.
2. Son capaces de robar la información confidencial, así mismo, las contraseñas, los datos de acceso a sistemas de banca y pagos, dinero de cuentas bancarias.
3. Pueden descargar otros programas nocivos y hasta dañar el sistema operativo.
4. Pueden paralizar completamente el equipo por comando del malintencionado.

En el momento de la creación, estos programas no suelen ser detectados por los antivirus. Además, algunos intentan desinstalar el antivirus.

REALIDAD

Hasta el 70% de los casos de infección de las redes locales de empresas aisladas de Internet se provocan por una infección en dispositivos extraíbles - la gente misma difunde los troyanos a través de unidades extraíbles.

¡ATENCIÓN!

En realidad, en el momento de penetración un antivirus no siempre puede detectar un programa nocivo más nuevo cuyo objetivo es penetración oculta, pero ningún otro software, además del antivirus, es capaz de desinfectar el sistema en caso de un troyano ya penetrado.

MITO

Siempre se nota el funcionamiento de un virus en el equipo. En caso de infección de mi equipo, lo notaré enseguida y tomaré medidas.

REALIDAD

Los programas nocivos modernos muchas veces se diseñan para permanecer mucho rato en el equipo de la víctima. Por lo tanto, no solamente actúan para que el usuario no lo note y no se detectan por muchos programas antivirus en el momento de su creación - existen programas nocivos que afrontan a sus competidores y desinstalan otros programas nocivos. Hasta existen los programas nocivos que corrigen las vulnerabilidades en el equipo.

Por ejemplo, Trojan.Carberp, creado para robar dinero, al iniciarse en el equipo infectado, realiza varias acciones para engañar los medios de control y supervisión. Una vez iniciado correctamente, el troyano se implementa en otras aplicaciones activas y finaliza su propio proceso. De esta forma, todo su funcionamiento posterior se realiza por partes, dentro de terceros procesos.

Por lo tanto, lo que se nota siempre la aparición de cualquier virus es solo un mito.

Recursos de información sobre las amenazas de virus actuales

Laboratorio antivirus Doctor Web:
http://live.drweb.com

Descripción de virus y programas nocivos:
http://vms.drweb.com/search

Informes sobre virus y spam:
http://news.drweb.com/list/?c=10

Línea roja de amenazas:
http://news.drweb.com/list/?c=23

Proyecto de formación «El mundo de antivirus»:
https://www.drweb.ru/pravda

Suscribirse a noticias sobre virus e informes:
https://news.drweb.com/news/subscribe

Enviar un archivo sospechoso para el análisis:
https://vms.drweb.com/sendvirus

Escáner en línea Dr.Web:
http://vms.drweb.com/online

Cómo penetran las amenazas de virus en las redes corporativas

La mayoría de las empresas cometen errores muy graves al crear un sistema de protección antivirus usando la información antigua sobre los modos de penetración de programas malintencionados y las posibilidades de los mismos.

Para organizar un sistema de protección antivirus eficaz de la red local, los expertos en seguridad de información de la empresa deben conocer las vías actuales de penetración de programas nocivos en la red local.

1. Errores de configuración de la protección antivirus

Las estadísticas del servicio de soporte técnico de la empresa Doctor Web confirman que muchas veces la infección se provoca por los virus y troyanos ya conocidos para la protección antivirus - porque los administradores de red desactivan el escaneo antivirus de algunos catálogos y unidades enteras, el escaneo del tráfico del navegador y buzones del correo. Un error frecuente es el rechazo de restricción de acceso a los sitios web fraudulentos y nocivos.

Ningún antivirus puede conocer todos los programas nocivos - en realidad es así, si se trata de un antivirus tradicionales que solo usa las bases de virus. El Antivirus Dr.Web usa la Protección preventiva y el servicio en la nube Dr.Web Cloud, lo que permite prevenir la infección por las amenazas desconocidas para el núcleo antivirus — pero la protección es realmente eficaz solo si el administrador configura las restricciones de acceso a recursos del sistema y de la red Internet usando Dr.Web Process Heuristic y el Firewall Dr.Web.

2. Vulnerabilidades

Una vulnerabilidad es un defecto del software usando el cual se puede dañar la integridad del software o causar errores de funcionamiento del mismo. La vulnerabilidades existen en cada software. No existe software sin vulnerabilidades.

Los creadores de virus modernos usan las vulnerabilidades para penetrar en un equipo local no solo en sistemas operativos, sino también en los programas de aplicación (exploradores, productos de Office, por ejemplo, Adobe Acrobat Reader y complementos para exploradores para visualizar flash).

La administración centralizada de actualizaciones con el Centro de Control Dr.Web permite a la empresa tener un sistema de protección actual - nunca se recomienda rechazar las actualizaciones y el reinicio porque cada actualización es la información sobre centenares y miles de programas nocivos anteriormente desconocidos que pueden atacar su equipo en cualquier momento.

¡ATENCIÓN!
Ningún software contemporáneo, salvo el antivirus, puede limpiar el sistema de software malicioso penetrado a través de las vulnerabilidades.

3. Sitios web

La gente tiene que leer las noticias en Internet para el trabajo y estar al tanto de los eventos. Lo que supone una amenaza es que la mayoría del personal de la oficina:

- conecta a Internet desde su equipo de trabajo en el cual está instalado un software con vulnerabilidades;
- trabaja en Windows con derechos del administrador;
- funciona usando contraseñas fáciles de hackear;
- no realiza las actualizaciones de seguridad de todo el software instalado en el equipo.

Por causa de la navegación no controlada de los sitios web por los empleados es posible que se filtren los datos, se sustituyan o se comprometan los materiales importantes.

¡ATENCIÓN!
Según las estadísticas, más del 80% de los sitios web en Internet vulnerabilidades y pueden ser hackeados. Para la filtración de los datos personales o la infección del sistema a veces basta con solo consultar el sitio web infectado.

Sitios web que con más frecuencia resultan ser fuentes del software malintencionado (en orden descendiente de frecuencia de incidentes).

Sitios web dedicados a tecnologías y telecomunicaciones.

Sitios web comerciales: Medios de información de negocios, portales de noticias de negocios, sitios web y foros de contabilidad, cursos/conferencias en Internet, servicios para mejorar la eficacia del negocio.

Sitios web pornográficos.

4. Dispositivos extraíbles

Hasta en los sistemas informáticos muy protegidos la fuente básica de difusión de los virus hace mucho ya no es correo electrónico, sino los virus en dispositivos extraíbles, con más frecuencia, en unidades flash.

La mayoría de las amenazas modernas son los troyanos. Son programas completamente malintencionados que no tienen un mecanismo de autopropagación y no son capaces de difundirse sin ayuda. La gente misma pasan los troyanos de un equipo a otro en dispositivos flash.

5. Los dispositivos personales del personal, entre ellos, los móviles

Más de 60% del personal tiene acceso remoto a la información corporativa desde sus dispositivos personales, entre ellos, los móviles.

Amenazas

- Los equipos de oficina dejaron de ser objetivo de ataques de cibergrupos de delincuencia ya hace mucho - se atacan también los dispositivos personales del personal, entre ellos, los móviles.
- Casi dos tercios de los empleados (63,3%) tienen acceso remoto a la información corporativa desde dispositivos personales, asimismo, los teléfonos móviles.
- Hasta el 70% de los casos de infección de las redes locales se realizan desde los portátiles personales, netbooks y ultrabooks, los dispositivo móviles del personal, así como las unidades extraíbles (unidades flash), a veces llevadas de casa.
- ¡Un 60% de equipos de hogar no tienen ninguna protección! Quiere decir que fuera de la oficina la gente no está protegida de los ataques de hackers, las aplicaciones que ellos usan pueden tener vulnerabilidades, puede haber virus y troyanos en los equipos. Asimismo, la gente entran en la red local de la empresa con mucha frecuencia.
- Esto crea la posibilidad de filtración, sustitución o compromiso de los datos importantes para la empresa.

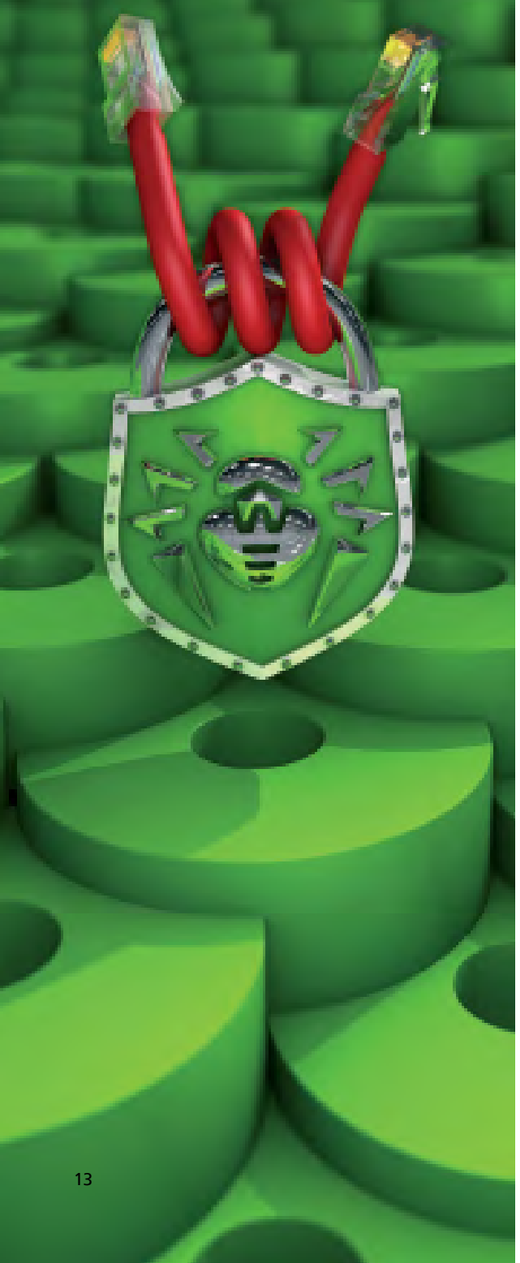
6. Correo electrónico

El tráfico de correo es la fuente principal de difusión de virus y spam. En caso de infección de un equipo, los programas malintencionados pueden obtener acceso a la libreta de direcciones del empleado que pueda contener no solamente las direcciones de sus compañeros de trabajo, sino también de sus clientes y socios - es decir, la infección se difunde no solamente por la red local de su empresa, sino también fuera de esta red. Una de las causas de la epidemia de troyanos cifradores es la posibilidad de recibir programas ejecutables como adjuntos a mensajes de correo electrónico por el personal de la empresa. La negligencia, el descuido y simplemente la ignorancia de los aspectos básicos de la seguridad informática de los empleados de la empresa con mucha frecuencia puede causar que los equipos se conviertan en una parte de botnets y una fuente de spam, lo que daña la imagen de la empresa; además la empresa puede se incluida en listas negras y desconectada de Internet por el envío de spam.

7. Ingeniería social

La mayor parte de malware contemporáneos de la “vida silvestre” no tiene mecanismo de autorreplicación — han sido intencionalmente diseñados para difundirse por los usuarios. Precisamente los usuarios que no conocen los fundamentos de la seguridad informática, cansados o distraídos, violando sin intención o por negligencia las políticas de seguridad, contribuyen a la penetración de virus en la red de la empresa (a través de dispositivos USB, abren de forma automática el correo electrónico de los remitentes desconocidos, navegan sin control en Internet durante las horas de trabajo, etc.). En orden de difundir los troyanos a través de los usuarios, los creadores de virus utilizan técnicas de ingeniería social, trucos ingeniosos que hacen ejecutar el programa malicioso por los mismos usuarios. Hay muchos trucos para usuarios: enlaces de phishing, cartas falsas de los bancos o de la administración de los recursos de red y mucho más. Los diferentes tipos de la ingeniería social se centra siempre en lo mismo: obtener datos personales del usuario, ya sean contraseñas de servicios web o la información confidencial y los datos bancarios.

Requerimientos de la legislación de la federación de rusia sobre la protección antivirus



Requisitos generales

1. El sistema de protección antivirus usado debe:

- qtener un sistema sólido de autoprotección que no permitirá al programa nocivo desconocido dañar el antivirus y posibilitará el funcionamiento del sistema de protección automático hasta recibir la actualización que permita desinfectarlo;
- disponer de un sistema de actualizaciones controlado por el sistema de autoprotección del sistema antivirus que no usa los componentes del sistema operativo que pueden ser comprometidos; el sistema de actualización que permite enseguida, al recibir el comando del sistema de administración centralizado, enviar las actualizaciones al objeto protegido por el antivirus para desinfectar la infección activa;
- disponer de un sistema para recabar la información sobre la nuevas amenazas que permite enviar lo más pronto posible el material para el análisis de virus y las actualizaciones al laboratorio antivirus;
- saber desinfectar no solo de programas nocivos que llegan (no activos), pero también ya iniciados, pero anteriormente desconocidos para la base de virus;
- tener mecanismos adicionales (excepto los de firmas y heurísticos) para detectar los nuevos programas nocivos desconocidos;
- escanear todos los archivos que se reciben a través de la red local hasta el momento de recepción de los mismos por las aplicaciones usadas, lo que evita el uso de vulnerabilidades desconocidas de estas aplicaciones por las aplicaciones nocivas;
- disponer de un sistema para recabar la información de forma centralizada desde las estaciones de trabajo y servidores remotos que permite transmitir lo más rápido posible toda la información necesaria para resolver el problema al laboratorio antivirus;
- tener un servicio de soporte local en ruso.

2. Hay que usar un sistema de administración centralizada de la protección antivirus que debe:

Asegurar la entrega más rápida de las actualizaciones de las bases de virus a todas las estaciones de trabajo y servidores - así mismo, por decisión del administrador, hasta si reduce el rendimiento de la red local protegida. La reducción del periodo de recepción de actualizaciones debe asegurarse por la reducción del tamaño de estas actualizaciones así como por la conexión continua de las estaciones de trabajo protegidas y servidores al servidor de actualizaciones.

Los usuarios no deben tener permisos de desactivar las actualizaciones. La opinión de cualquier empleado sobre la frecuencia de actualizaciones debe ser ignorada.

¡ATENCIÓN!

Ningún software requiere una actualización tan frecuente como un antivirus. Los nuevos virus se crean continuamente, y las bases de virus se actualizan con mucha frecuencia (no menos de 1-2 veces por hora). ¡La actualización automática de antivirus debe estar siempre activada!

Las posibilidades de la administración centralizada del sistema de protección Dr.Web permiten:

- evitar la posibilidad de cancelar las actualizaciones de la estación por empleados;
- desconectar de la red un agente no actualizado, es decir, prevenir la epidemia dentro y fuera de la red local;
- establecer un modo de actualizaciones de componentes Dr.Web necesario en estaciones protegidas, al distribuir la carga en varios periodos temporales;
- supervisar las bases de virus y el estado de las estaciones;
- imposibilitar la desactivación de escaneos periódicos por los usuarios, iniciar los escaneos sin participación del operador de la estación de trabajo, establecer la programación de escaneo con cualquier frecuencia necesaria. La opinión de cualquier empleado sobre la frecuencia de escaneos debe ser ignorada.

¿Por qué es importante escanear el sistema con regularidad?

- El antivirus no conoce el 100% de los virus en cualquier momento.
- Entre la aparición de un nuevo virus y la implementación de su firma a la base de virus pueden pasar días y hasta meses.
- Hasta si la firma de la base de datos es capaz de detectar el virus, no significa que podrá desinfectarlo, el desarrollo de los métodos de desinfección`puede llevar mucho rato.

El Centro de control Dr.Web permite controlar de forma centralizada el cumplimiento con la directiva de seguridad en cuanto a la realización de escaneos periódicos:

- iniciar/detener el escaneo sin intervención del operador de la estación de trabajo;
- establecer las rutas de escaneos;
- establecer la programación de escaneo de grupo e individual con cualquier frecuencia necesaria — es decir, realizar el escaneo a la hora conveniente para el personal.

El Centro de Control Dr.Web Enterprise Security Suite proporciona la administración centralizada de protección de todos los nodos de la red corporativa:

- estaciones de trabajo, clientes de servidores de terminales y clientes de sistemas incorporados en plataformas Windows, Linux y macOS;
- servidores de archivos y servidores de aplicaciones (entre ellos, servidores de terminales) Windows, Novell NetWare, macOS, Unix (Samba) y Novell Storage Services;
- servidores de correo Unix, Microsoft Exchange, IBM Lotus, Kerio;
- puertas de enlace de Internet Unix y Kerio;
- dispositivos móviles bajo la administración de Android y BlackBerry.

Sólo la administración centralizada de la protección con los medios del Centro de control Dr.Web permite realmente ahorrar dinero.

Posibilidad de "ver desde arriba" la red antivirus de la empresa desde la misma estación de trabajo, dondequiera que esté, y los esfuerzos mínimos requeridos para la implementación de la red, así como la administración fácil de Dr.Web Enterprise Security Suite reducen el periodo de servicio de la red al mínimo. La interfaz web web cómoda, la posibilidad de automatizar el trabajo por medio de integración con el sistema Windows NAP y la interfaz para crear procesadores de eventos propios en cualquier lenguaje de script reduce considerablemente la carga de administradores de sistema.

El uso de las funciones del Centro de Control Dr.Web permite:

- realizar la administración, actualización y configuración centralizada de los medios informáticos de la protección antivirus, así mismo, en los equipos no disponibles desde el servidor;
- administrar de forma operativa el sistema de protección de la red local en cualquier momento, desde cualquier parte del mundo, desde un equipo bajo la administración de cualquier sistema operativo simplemente a través del navegador y sin necesidad de instalar el software extra;
- realizar las directivas de seguridad necesarias para una empresa en concreto y los grupos de empleados;
- asignar administradores por separado para varios grupos;
- realizar escaneo antivirus completo o personalizado en busca de amenazas de virus tanto por comando del usuario o administrador, como por programación;
- recabar y analizar la información de varios tipos sobre el estado del sistema de protección de los nodos de la red local, así como crear informes del periodo requerido;

- notificar a los administradores y usuarios sobre el estado del sistema de protección;
- enviar los mensajes informativos a usuarios en modo de tiempo real.

El Centro de Control Dr.Web se licencia de forma gratuita.
Más información: http://products.drweb.com/enterprise_security_suite/control_center

Protección de la red local en caso de usar servicios en la nube

Los riesgos vinculados al uso de servicios en la nube son:

1. Posibilidad de intercepción y modificación de la información transferida. Por lo tanto, se recomienda usar los servidores proxy antivirus tanto en la parte de la nube como en la parte de la empresa. Así mismo, se recomienda usar los canales de protección protegidos, pero tomando en cuenta el riesgo de implementación de programas nocivos en la rotura entre el canal protegido y el programa cliente.
2. Posibilidad de implementar programas nocivos en las máquinas virtuales. Por lo tanto, se recomienda usar los medios antivirus para la protección de todas las máquinas virtuales sin distinción de su ubicación.

Deben usarse las siguientes medidas de protección en caso de usar servicios en la nube:

- gateways de correo en la parte del centro de datos y en la parte de la red local o servidores de correo locales que escanean el correo entrante y recopilan los mensajes de correo si no hay acceso al centro de datos;
- servidores de archivos y servicios que sincronizan el contenido con el contenido de servidores remotos.

Además de usar soluciones antivirus, es necesario:

1. Aislar la intranet de la empresa de la red Internet - dividir la red en la externa e interna.
2. Registrar las acciones del usuario y del administrador.
3. Crear copias de seguridad de la información importante.

Hay que desarrollar los procedimientos siguientes:

1. Control periódico de todas las funciones de seguridad informática realizadas con los medios de hardware y software.
2. Recuperación de todas las funciones de seguridad informática realizadas con los medios de hardware y software.
3. Respuesta a los incidentes de seguridad informática.
4. Notificación al personal y clientes en caso de incidentes de seguridad informática.

Organización de la protección de estaciones de trabajo

Como fue demostrado, las estaciones de trabajo (incluidos los dispositivos móviles) y los servidores son los nodos más vulnerables de la red local. Son fuentes de virus y, con mucha frecuencia, de spam.

Protección de las estaciones de trabajo pertenecientes a la empresa

1. En teoría, cualquier error del software puede ser usado para dañar el sistema completo. Así mismo, puede ser tanto un error temporal como un daño de datos importantes. Para evitarlo, hay que seguir las normas básicas.
   - Descargar e instalar de forma oportuna todas las actualizaciones y nuevas versiones de todo el software instalado en equipos — no solo del sistema operativo. Para realizarlo, todo el software usado debe ser de licencia.
   - Usar un sistema de instalación centralizada de actualizaciones de todos el software instalado en el PC — esto le permitirá al administrador de sistemas, en modo de tiempo real, asegurarse de que no hay vulnerabilidades conocidas en objetos protegidos.

Sólo un administrador de sistemas cualificado puede tomar decisiones sobre la necesidad de actualizar el antivirus, instalar algún programa o reiniciar algún programa instalado en el PC por causa de actualización de seguridad. La opinión de otros usuarios, sobre este asunto sin importar su cargo, debe ser IGNORADA.

2. Hay que proporcionar la administración centralizada de todos los componentes del sistema de protección antivirus de todas las estaciones de trabajo de la red local.
3. Hay que usar la versión actualizada del sistema de protección antivirus.
4. Sin importar su cargo, cualquier usuario debe trabajar solo en una cuenta con permisos restringidos. La cuenta Invitado debe estar deshabilitada.
5. El administrador de sistemas debe conocer el contenido del software instalado en equipos.
6. La instalación autónoma de programas por el usuario debe ser prohibida, esto impedirá que un virus se instale en el equipo esquivando los medios de seguridad.
7. Hay que restringir el acceso de usuarios solo por los recursos de la red local necesarios para el trabajo. Para realizarlo, debe usarse un sistema configurado de control y restricción del acceso.

El Control de oficina Dr.Web bloquea la mayoría de las vías de penetración de virus al prohibir el uso de dispositivos extraíbles (así mismo, las unidades USB) y restringir acceso a dispositivos de red y locales (así mismo, las carpetas del equipo local y los sitios de Internet).

8. La verificación del tráfico de correo debe realizarse antes de que ingresen las cartas en el programa de correo para eliminar la posibilidad de penetración de malware a través de las vulnerabilidades.

¡ATENCIÓN!

Los flujos de correo que pasan a través de la estación de trabajo y el servidor, no coinciden.

- El usuario (o los programas que permitió instalar sin enterarse de sus posibilidades) puede enviar y recibir mensajes:
  - directamente a los servidores de correo de la re Internet (por protocolo SMTP) si en la red está abierto el puerto 25;
  - a los servicios de correo de tipo mail.ru/gmail.com — por protocolos pop3/imap4.
- El usuario (o los programas que permitió instalar sin enterarse de sus posibilidades) puede enviar mensajes por canales privados, y el servidor no podrá analizarlos.
- El servidor (o los programas instalados en el mismo) puede crear los envíos de correo y notificar a los usuarios y remitentes automáticamente sobre varios eventos.

Por lo tanto, es necesario filtrar el tráfico de correo tanto al nivel del servidor de correo como al nivel de estaciones de trabajo.

9. El tráfico de Internet debe ser escaneado antes de llegar a las aplicación cliente. El sistema antivirus debe escanear todos los enlaces que se usarán para descargar algún recurso de la Red, y todo el tráfico antes de llegar el mismo al equipo.

Ya hace mucho para penetrar en un equipo se usan las vulnerabilidades de software (sobre todo Adobe) y no las vulnerabilidades de sistemas operativos. Los componentes Dr.Web SpIDer Gate y SpIDer Mail escanean el tráfico del correo antes de que el mismo llegue al navegador o al cliente de correo. En este caso, los virus no podrán usar las vulnerabilidades de programas instalados en las estaciones de trabajo.

10. El personal debe tener acceso solo a los recursos de Internet necesarios para el trabajo. La opinión del personal, sin importar su cargo, sobre la seguridad de consulta de recursos, debe ser IGNORADA. La posibilidad de acceso del personal a los recursos en Internet no necesarios debe ser prohibida.

El Control de oficina Dr.Web permite:

- restringir acceso a Internet;
- Restringir el acceso a los dispositivos de almacenamiento extraíbles;
- llevar las listas blancas y negras de direcciones para asegurar el acceso del personal a la red Internet, si es necesario para cumplir con las tareas laborales;
- restringir completamente el acceso a la red Internet donde es imprescindible (por ejemplo, en equipos con sistemas de contabilidad);
- prohibir la cancelación de restricciones por el personal en una estación.

ATTENTION !

Este componente también debe ser instalado en los equipos no conectados a la red Internet o aislados de la red local.

11. Un usuario o un programa malintencionado en nombre del mismo no deben tener acceso a ningún recurso local ni de la red, excepto los necesarios para realizar las tareas de trabajo. No tiene sentido convencer a los empleados de que las unidades flash son peligrosas.

Sistema de restricción de acceso de Control de Oficina Dr.Web:

- detecta los archivos y las carpetas en la red local a los cuales un empleado puede tener acceso, y prohíbe los que deben ser inaccesibles para el mismo - es decir, permite asegurar los datos y la información importante contra un daño intencional o deliberado, así como eliminación o robo por los malintencionados o insiders (empleados de la empresa que intentan acceder a la información confidencial);
- restringe o completamente prohíbe el acceso a los recursos de la red Internet y dispositivos extraíbles, y por lo tanto permite evitar la posibilidad de penetración de estos virus a través de estas fuentes.

Un mecanismo adicional de protección contra virus que se difunden a través de dispositivos extraíbles es un modo de prohibir el autonicio en el monitor de archivos SpIDer Guard. Al activar la opción «Bloquear el autoinicio desde dispositivos extraíbles» se puede continuar usando las unidades extraíbles si no se puede rechazar su uso.

MEJOR EXPERIENCIA

La posibilidad de conexión de dispositivos extraíbles a la estación de trabajo debe ser prohibida de forma centralizada.

12. Además, para impedir la penetración de objetos nocivos a la red corporativa, en las estaciones d etrabajo, excepto el antivirus, deben ser usados los siguientes componentes de protección:

- Antispam – para reducir el porcentaje de spam en el tráfico de correo, lo que reducr el riesgo de infección a través de mensajes spam y mejora el rendimiento, porque:
  - Los usuarios no se distraen al consultar el correo entrante,
  - se reduce la posibilidad de omitir o borrar un mensaje importante.
- Firewall – para imposibilitar el escaneo de la red local desde dentro, así como para la protección contra ataques de red.

13. El sistema de protección antivirus debe ser instalado en todas las estaciones de trabajo bajo la administración de cualquier SO, incluidos macOS, Linux y UNIX. En caso de asegurar solo la protección de Windows, los programas malintencionados obtienen un refugio seguro en equipos no protegidos – incluso si no pueden infectar los sistemas operativos y las aplicaciones iniciadas, pueden usarlos como fuente de infección – por ejemplo, a través de los recursos de red en acceso público.

¡ATENCIÓN!

A partir del año 2013, se observa un crecimiento del número de ataques a sistemas operativos Linux y otros sistemas por varias razones no protegidos por un antivirus. Si antes no hubo muchas noticias sobre infecciones de equipos Linux, a partir del año 2013 casi cada semana aparece la información sobre alguna infección masiva o un hackeo.

Protección de los equipos que se usan para trabajar con datos críticos y/o dinero

1. Un equipo que se usa para trabajar con dinero (sistemas de banca en línea) no debe usarse para trabajar con datos críticos, y al revés. Ninguna otra operación debe ser realizada en este equipo dedicado.
2. En el equipo dedicado se debe:

- evitar la posibilidad de iniciar otros programas, sobre todo, cuyo objetivo es desconocido y recibidos de remitentes desconocidos;
- desinstalar los sistemas y servicios de administración remota y bloquear la posibilidad de conexiones remotas de sistemas críticos para el negocio – todos, excepto el recurso al que conecta el sistema de banca en línea;
- bloquear la posibilidad de consultar los recursos de Internet externos por los medios del componente Control de oficina Dr.Web;
- protocolar todos los eventos, así mismo, todas las acciones de administradores y usuarios del equipo;
- bloquear la posibilidad de iniciar programas desde carpetas con documentos y catálogos para archivos temporales, tales como Temp;
- usar solo contraseñas de acceso resistentes al hackeo. La resistencia de contraseñas debe ser controlada por los medios del sistema centralizado que asegura la conformidad de las contraseñas usadas a los requerimientos de seguridad, y su sustitución periódica.

3. Antes de empezar a trabajar con el sistema de banca en línea y/o datos importantes se recomienda actualizar el antivirus y escanear rápido el sistema.
4. Una vez finalizado el trabajo con el sistema de banca en línea y/o los datos importantes, debe finalizar correctamente el trabajo con los datos del sistema (salir del sistema).

Protección de dispositivos informáticos personales desde los cuales el personal de la empresa pueden acceder a la red corporativa

Hoy, día, muchos empleados de oficina usan sus propios dispositivos para acceder a los recursos corporativos y/o trabajan a distancia. Algunos profesionales siempre están en línea: en en trabajo, durante el viaje, en casa. Cualquier empresa está interesada en trabajo seguro de su personal en cualquier lugar y en la protección de los datos corporativos.

Con mayor frecuencia, los equipos de hogar tienen instalado el sistema operativo Windows. Los hackers lo conocen bien porque se usa mucho y para el mismo se crean la mayoría de los programas nocivos. Los modos de protección de este sistema operativo también son conocidos, pero para los equipos de hogar del personal que se usan para acceder a la red corporativa debe cumplirse el requerimiento de restricciones corporativas por una parte y el uso libre del equipo/dispositivo personal, por otra. Por ejemplo, hay que prohibir la consulta de las redes sociales en el trabajo y permitir su uso fuera del horario laboral. Así mismo, hay que tomar en cuenta la posibilidad de trabajo en el equipo para otros miembros de la familia del empleado.

Dos modos de protección son posibles.

- **Primero** – añadir otra cuenta de usuario en el equipo personal (Windows lo permite) y realizar toda la configuración de seguridad necesaria para este usuario. Pero, este modo permite cumplir con los requerimientos de seguridad solo parcialmente. Por ejemplo, en caso de trabajo con la cuenta del usuario "protegido" el virus será bloqueado, pero nada le impedirá penetrar en el equipo en caso de trabajo con otras cuentas y obtener acceso a la información guardada, pero no protegida. Así mismo, con cuentas no protegidas el virus puede cambiar la configuración de seguridad. Por lo tanto, para el usuario protegido deben instalarse también un almacén de archivos y un sistema de control de integridad. Pero el problema más importante es la necesidad de configurar todo esto por el administrador para cada usuario, en la mayoría de los casos, a distancia.
- **La segunda opción (más correcta)** es usar una unidad de arranque o un USB que contiene todos los componentes necesarios para el trabajo protegido. Solo los virus a nivel BIOS podrán esquivar la protección, lo que no pasa a menudo.

¡ATENCIÓN!

Solo al asegurar la protección de todos los dispositivos, entre ellos, los móviles, usados por el personal de la empresa, se puede garantizar que nada nocivo penetrará en la red corporativa desde los equipos personales y dispositivos móviles del personal y los datos y contraseñas usados por el personal para acceder a la red de la empresa no serán robados.

¡IMPORTANTE!

El Centro de control Dr.Web Enterprise Security Suite permite administrar la seguridad tanto de equipos de oficina como de los dispositivos del hogar de los empleados, incluidos los dispositivos móviles que funcionan bajo la administración de Android y Windows Mobile.

1. La opinión del empleado, sin importar su cargo, sobre qué antivirus debe instalarse en su dispositivo personal debe IGNORARSE - mientras este dispositivo forma parte de la red corporativa. En caso contrario, este dispositivo debe declararse "no de confianza" y no debe permitir el acceso del mismo a la red.
2. El cumplimiento de la directiva de seguridad informática de la empresa y en dispositivos personales de los empleados, así mismo, la desactivación imposible de actualizaciones y escaneos periódicos, así como la desinstalación de algunos componentes de protección, debe ser asegurado con los medios centralizados de administración del sistema de protección antivirus.

Por lo demás, para asegurar la protección de equipos personales del personal se requiere un sistema similar al aplicado para la protección de estaciones de trabajo pertenecientes a la empresa.

Las posibilidades del sistema antivirus Dr.Web permiten administrar de forma centralizada la protección tanto de equipos corporativos como personales del personal, incluidos los dispositivos móviles.

Protección de dispositivos móviles desde los cuales se puede acceder a la red corporativa, así mismo, los dispositivos móviles personales de empleados no pertenecientes a la empresa

Los teléfonos y dispositivos móviles por sus posibilidades y el número de vulnerabilidades pueden compararse con estaciones de trabajo. En los dispositivos móviles modernos se usan sistemas operativos y aplicaciones bastante potentes que pueden ser infectados con los mismos métodos que las aplicaciones para estaciones de trabajo. Así mismo, el problema básico de uso de dispositivos móviles personales por los empleados de la empresa es la posibilidad de difusión de programas nocivos desde los mismos e infección de la red local - o la obtención de acceso a sus recursos esquivando la protección.

Los sistemas operativos de dispositivos móviles normalmente se basan en iOS de Apple o Android. Así mismo, los recursos de sistemas normalmente son más débiles que en equipos ordinarios. En estos dispositivos normalmente no se puede usar varias cuentas lo que permitiría restringir los permisos de usuarios y reducir el riesgo de infecciones. Por lo tanto, la protección solo puede ser parcial. Además existe un riesgo importante de extravío o robo del dispositivo, por lo tanto, los terceros pueden acceder a toda la información (incluidas las contraseñas y nombres de acceso a recursos corporativos).

En el dispositivo móvil , para asegurar la protección contra la penetración de archivos nocivos deben ser usados:

1. Antivirus – permitirá prohibir el acceso de archivos malintencionados al dispositivo, entre ellos, los destinados para controlar el desplazamiento del titular del dispositivo, así como sus contactos y conversaciones.
2. Sistema de protección contra la pérdida de dispositivo móvil que permitirá localizar el dispositivo en caso de pérdida del mismo y no permitir que un malintencionado accede a los datos del mismo.
3. Sistema de almacenamiento de la información confidencial en un almacén protegido, lo que impedirá que el malintencionado use los datos del dispositivo móvil.

Protección de dispositivos móviles es necesario si se utilizan estos dispositivos para recibir SMS mensajes, apoyo a las operaciones bancarias es debido a la presencia de software malintencionado que modifica este tipo de mensajes.

Sobre la necesidad de protección de servidores de archivos

Normalmente las empresas protegen solo los equipos de trabajo del personal, dejando sin protección los servidores, dispositivos móviles y equipos del hogar del personal.

Como resultado, un virus que penetre a las estaciones de trabajo empieza a funcionar y penetra fácilmente a los servidores con información muy importante.

¿Por qué es importante proteger a los servidores?

- Un usuario puede infectar el servidor por un virus desconocido en el momento de infección (por medio de llevar el mismo o iniciarlo desde un almacén). El antivirus instalado lo capturará enseguida, basándose en mecanismos heurísticos. Como mínimo, desinfectará el virus durante la próxima actualización.
- Un servidor puede ser hackeado por hackers. El antivirus instalado no lo permitirá: supervisará y borrará los programas malintencionados. Si el servidor se controla por un sistema de administración centralizado, el administrador recibirá instantáneamente una notificación sobre el cambio del estado de la estación (por ejemplo, sobre un intento de parar el sistema de protección).
- El mundo moderno está lleno de tecnologías digitales. Los usuarios pueden trabajar no sólo en la oficina sino también en casa, almacenar los datos en los servidores de archivos de la empresa - y en servidores de la red Internet. Usar sus unidades flash - también los recibidos de amigos y colegas de trabajo. Estos medios pueden contener virus.
- Los teléfonos móviles modernos por sus posibilidades y por el número de vulnerabilidades pueden compararse con equipos — se usan los sistemas operativos y aplicaciones que también pueden ser infectados. Desde los mismos, los virus pueden penetrar en la red corporativa y llegar al servidor.

Los requerimientos a la seguridad de servidores de archivos son distintos para sistemas operativos Windows y Unix. Para los SO Windows el uso del antivirus de archivo supone la protección de servidores de aplicaciones y terminales, y para los SO Unix deben usarse soluciones propias para la protección de cada servicio.

¡ATENCIÓN!

El uso del servidor de las bases de datos en el servidor de archivos protegido no supone desinfección del contenido de las bases de datos para lo cual deben usarse soluciones especiales.

Con mucha frecuencia, el personal de la empresa usa no solo su propio servicio de archivos, sino también los almacenes externos. En caso de usar estos almacenes nadie garantiza que el usuario reciba archivos no infectados por virus - es posible interceptar el canal de conexión a Internet y suplantar la información transferida.

Por lo tanto, además de la protección del servidor de la empresa y todos los recursos de red públicamente disponibles (por ejemplo, las carpetas compartidas por usuarios) en la empresa debe usarse una Gateway antivirus que no permitirá recibir ni enviar un archivo infectado.

Servidores de impresión

Con mucha frecuencia, los servidores de archivos se usan como servidores de impresión - es decir, tiene servicios que permiten recibir y enviar los documentos para impresión por protocolo especial. Estas Gateways también deben ser protegidas porque:

- hay suficientes programas nocivos que infectan los servidores de impresión;
- un malintencionado puede tanto interceptar la información enviada para impresión como enviar para impresión los documentos cuya difusión fuera de la empresa está prohibida.

¡IMPORTANTE!

En caso de usar Linux como plataforma para el servidor, se recomienda proteger no solo las funciones del servicio de archivo de este servidor (servicio Samba), sino el servidor también. Es decir, hay que usar dos software Dr.Web:

- Antivirus Dr.Web para Linux
- Dr.Web para servidores de archivos Unix

Hay que tomar en cuenta no solo el riesgo de infección de servidores de archivos, sino también de impresoras, sobre todo, disponibles desde Internet. Por falta de recursos, en estos dispositivos no pueden ser usados los medios antivirus. Por lo tanto, los medios de restricción de acceso deben usarse como protección.

Protección de servidores terminales

La seguridad de servidores terminales debe proporcionarse con los productos destinados para la protección de sistemas de archivos de equipos porque la única diferencia entre los servidores de archivos y terminales desde el punto de vista de proporción de la seguridad es la necesidad de comprobar las sesiones terminales de clientes, al abrir y cerrar las mismas.

- En caso de entrar en servidores de terminales desde clientes ligeros, no es necesario proteger los clientes ligeros (ningún software antivirus se instala en los clientes ligeros), pero para la protección de las sesiones de terminales debe adquirir el número de licencias Dr.Web Desktop Security Suite Protección integral igual al número de conexiones — además de la licencia de protección del mismo servidor de terminal Dr.Web Server Security Suite.
- En caso de no entrar en servidores terminales desde clientes ligeros, se requiere la protección de clientes que se conectan al servidor terminal (Dr Web Desktop Security Suite Protección integral + Dr.Web Server Security Suite). Así mismo, el sistema de protección de estaciones de trabajo es igual tanto encaso de entrar en el servidor terminal como sin usar esta entrada. En este caso hay que tomar en cuenta que en caso de usar las estaciones de trabajo su número no se toma en consideración en el número de licencias para conectarse al servidor terminal.

El **Centro de Control Dr.Web** permite controlar de forma centralizada el sistema antivirus de protección de cualquier número de servidores de archivos bajo la administración de Windows, macOS, Unix (Samba), Novell NetWare, Novell Storage Services.

Organización del filtrado del correo

El tráfico de correo es la fuente principal de difusión de virus y spam. En caso de infección de la red de la empresa, el correo puede llegar a ser la fuente de virus y la vía de penetración de las mismas en todos los equipos de la red, porque ne un equipo infectado los programas malintencionados tienen acceso a la libreta de direcciones del empleado — puede contener tanto las direcciones de su personal como las de sus clientes.

Bastantes archivos nocivos en el tráfico de correo, así como la «ingenuidad» del personal causa:

- pérdidas y flujos de datos como resultado de la actividad de virus y de utilidades de hackers;
- captura de la red local como resultado de un ataque de virus para convertirla en un elemento de una botnet;
- la empresa forma parte de listas negras y se desconecta de Internet por enviar spam;
- reducción del periodo de respuesta del servidor de correo dedicado a procesamiento del tráfico parásito;
- reducción del rendimiento del servidor o el fallo completo del mismo;
- aumento de la carga de la red interna, reduciendo el rendimiento de recursos de red y el ancho de banda de canales;
- fallo del servidor por causa de recibir "una bomba de correo";
- inactividad del equipo;
- reducir los gastos de almacenamiento del correo, asimismo, del spam;
- más requerimientos a la parte hardware de servidores de correo, y, por lo tanto, la necesidad de actualizar o comprar nuevos equipos.

Así mismo, se registran los siguientes daños de renombre de la empresa:

- errores de la continuidad de procesos de negocios;
- demoras de realización de su trabajo por el personal o imposibilidad de realizar este trabajo (inactividad);
- probabilidad de omitir la información importante;
- pérdida de tiempo laboral para eliminar los incidentes de virus;
- retrasos de cumplimiento de obligaciones para los clientes;
- aumento de tamaño de las cuentas de correo de usuarios y de las copias de seguridad de las mismas, lo que causa problemas de búsqueda de la información importante;
- peor imagen para consumidores y socios;
- creación de la opinión sobre la empresa como tecnológicamente atrasada;
- pérdida de clientes o renuncia de los servicios de la empresa.

1. Es necesario filtrar tanto el correo externo (entrante y saliente), como el correo interno de la empresa — es decir, deben filtrarse todas las vías de recepción y envío del correo.

En caso de infección de la red de la empresa, el correo puede llegar a ser la fuente de virus y la vía de penetración de las mismas en todos los equipos de la red, porque ne un equipo infectado los programas malintencionados tienen acceso a la libreta de direcciones del empleado.

2. El correo debe ser filtrado en el servidor, y luego además en las estaciones de trabajo.

Esta organización de la protección reduce bastante la carga tanto al servidor de correo como a las estaciones de trabajo:

- Al escanear correo, solo un antivirus de correo puede eliminar los programas nocivos que habían penetrado allí anteriormente, - ningún otro antivirus puede hacerlo.
- El filtrado a nivel de servidor de correo permitirá no solo filtrar los mensajes de correo con mayor eficacia, sino también limpiar las bases de correo de virus desconocidos en el momento de penetración, lo que, a su vez, evita su envío accidental al destinatario. Así mismo, las soluciones servidor para filtrar el correo en servidores y Gateways permiten realizar el filtrado por formatos de datos usados, tamaños límite de archivos y otros criterios, lo que no tienen las soluciones para proteger las estaciones de trabajo.
- El tráfico se escanea antes de llegar al cliente de correo. Es decir, los virus no pueden usar las vulnerabilidades de sistemas operativos y programas correspondientes.
- El filtrado de correo a nivel de servidores permite evitar las situaciones cuando el usuario mismo puede desactivar el antivirus o reducir el nivel de protección - los directivos de la empresa y el administrador de sistemas pueden estar seguros de que la red está protegida.
- La protección se hace más actual. A diferencia de una estación de trabajo que puede estar sin actualizar durante mucho tiempo (por ejemplo, si el empleado no está), las bases de virus del servidor siempre están actualizadas.
- Se reduce la posibilidad de conflictos del software antivirus con otro software. Por ejemplo, con un software instalado por el usuario.
- El correo y el spam se filtrará una vez en el servidor, y no varias veces en cada estación, lo que mejorará la velocidad de funcionamiento de las mismas, y el personal se quejará mucho menos de "demoras" en sus equipos de trabajo y le distraerá menos para eliminar las mismas.
- Gracias al filtrado antispam , la carga parásita no productiva del servidor de correo se reducirá (el volumen de spam en el tráfico de correo es de hasta 98%, y el filtrado del mismo mejorará el funcionamiento del servidor de correo). Esto reducirá el número de quejas del personal sobre los retrasos de entrega del correo y los mensajes perdidos.
- Reducirá significativamente el tráfico entre redes por causa de algoritmos de cifrado y compresión aplicados en los productos servidor para el filtrado antivirus del correo — ningún otro productor tiene esta funcionalidad en sus productos para la protección de las estaciones de trabajo.

3. Hay que proporcionar la protección del servidor de correo.

La protección de los servidores de correo (por ejemplo, con los medios Dr.Web Server Security Suite) es una medida de protección obligatoria contra los virus desconocidos para el sistema de protección antivirus en el momento de infección. La penetración de un programa nocivo desconocido en el servidor de correo o/y en el correo convierte el servidor de correo en una fuente continua de programas nocivos.

4. Hay que proteger todas las vías de recepción y envío del correo, no solo el servidor de correo.

El trabajo moderno en una oficina se caracteriza por el uso no solo de servicios internos, sino también de externos, así mismo, de correo, por el personal de la empresa. Muchas veces al personal responsable de la seguridad de la empresa no le informan sobre los casos de uso de estos servicios.

Los flujos de correo posibles de la empresa:

- El usuario (o los programas que permitió instalar sin enterarse de sus posibilidades) puede enviar y recibir mensajes:
  - directamente a los servidores de correo de la re Internet (por protocolo SMTP) si en la red está abierto el puerto 25;
  - a los servicios de correo de tipo mail.ru/gmail.com – por protocolos pop3/imap4.
- El usuario (o los programas que permitió instalar sin enterarse de sus posibilidades) puede enviar mensajes por canales privados, y el servidor no podrá analizarlos.
- El servidor (o los programas instalados en el mismo) puede crear los envíos de correo y notificar a los usuarios y remitentes automáticamente sobre varios eventos.

Por lo tanto, es necesario escanear no solo el tráfico de correo que entra en los servidores de correo de la empresa, sino también el tráfico dirigido a servidores externos no controlados por la empresa, cuyo nivel de protección es desconocido. En la práctica significa:

- filtrar todo el correo corporativo en el servidor de correo (usando Dr.Web Mail Security Suite Antivirus + Antispam) y además procesar los protocolos POP3 y IMAP4 en la Gateway de la red Internet (en función del producto que procesa el tráfico usado en la Gateway – Dr.Web Mail Security Suite Antivirus + Antispam, Dr.Web Mail Security Suite Antivirus + Antispam + SMTP proxy o Dr.Web Gateway Security Suite Antivirus) – además de filtrar el correo en la estación de trabajo;
- filtrar todo el correo externo (protocolos POP3 y IMAP4, SMTP) en la Gateway (usando Dr.Web Mail Security Suite Antivirus + Antispam + SMTP proxy), y en el servidor de correo, solo procesar el correo interno (Dr.Web Mail Security Suite Antivirus + Antispam) – además de escanear el correo en la estación de trabajo.

La segunda opción es más recomendad porque en este caso:

- la carga del servidor de correo se reducirá (el volumen de spam en el tráfico de correo es de hasta 98%, lo que mejorará el funcionamiento del servidor de correo);
- La falta del acceso directo al servidor de correo desde la red Internet no permite a los hackers usar las vulnerabilidades (tanto las conocidas anteriormente como las vulnerabilidades de nivel cero), asimismo, gracias a los mensajes creados a propósito;
- la calidad de filtrado en la Gateway es superior porque la solución para la Gateway no contiene solo la funcionalidad del servidor de correo.

5. El filtrado del correo debe ser integral.

Solo las soluciones integrales para el correo electrónico que combinan el antivirus y el antispam pueden asegurar la protección completa de la misma y reducir los gastos de la empresa. El uso del antivirus sin antispam:

- permite a los malintencionados atacar los servidores de correo de la empresa y los clientes de correo de sus empleados.
- causa el aumento de pago de tráfico;
- causa el aumento de la carga parásita no productiva de servidores de correo;
- baja el rendimiento de todo el personal de la empresa que recibe el correo y está obligado a limpiar sus cuentas de correo de spam.

6. Medidas de protección extra.

- Con mucha frecuencia, los servidores de correo almacenan el correo de usuarios – continuamente (los servidores guardan todo el correo en el servidor de empresas y lo acceden por protocolo IMAP4), o temporalmente (hasta que el empleado empiece a trabajar). Como siempre es probable que un nuevo virus desconocido penetre en el correo antes de ser investigado en un laboratorio antivirus, se recomienda escanear periódicamente el correo de usuarios en busca de los virus no detectados anteriormente, o escanear el correo al enviarlo al empleado.
- Si las instalaciones de la empresa o entidad no están en el mismo sitio y no se usa un canal dedicado para su comunicación, la recepción y la transferencia de mensajes de correo entre estas partes de la empresa deben realizarse a través de la Gateway - hasta si las instalaciones están en el mismo edifico, siempre existe la posibilidad de intercepción o suplantación del tráfico.
- El correo filtrado debe ser movido a cuarentena y/o archivado por si existen quejas sobre filtrado incorrecto (por ejemplo, si el nivel de detección es superior a lo recomendado). La disponibilidad de la cuarentena y de la función del archivado de mensajes en Dr.Web Mail Security Suite permite restaurar los mensajes eliminados por el personal de las cuentas de correo por error, así como llevar a cabo las investigaciones vinculadas con la filtración de la información.

Principios del filtrado de correo en una Gateway de correo

1. Se recomienda filtrar el correo a través de la Gateway de correo (Dr.Web Mail Security Suite Antivirus + (Antispam) + SMTP proxy).

No es seguro ubicar el servidor de correo en Internet o en Intranet de la empresa. Un malintencionado tiene muchas posibilidades de acceder al servidor o suplantar el tráfico, así mismo, usando hardware backdoors. Incluso si las instalaciones están en el mismo edificio, siempre hay probabilidad de intercepción o suplantación del tráfico.

La mejor opción es ubicar el servidor de correo en el borde de la red o en una zona desmilitarizada organizada a propósito (DMZ) de servidores de correo de tránsito (o Frontend). Los servidores reciben el correo y lo redirigen al servidor de correo básico

dentro de la red de la empresa, al mismo tiempo filtrado el tráfico en busca de spam y virus antes de llegar el mismo a la Intranet de la empresa. Estos servidores pueden ser administrados tanto por los expertos de la empresa como por una tercera empresa (por ejemplo, por los expertos del centro de datos).

Siempre se recomienda usar el filtrado del tráfico de correo en la Gateway en casos siguientes:

- empresa — proveedor de Internet;
- el servidor de correo de la empresa está fuera del territorio vigilado de la empresa (por ejemplo, en un centro de datos externo);
- la empresa alquila las direcciones de correo en un servicio especial;
- las instalaciones de la empresa no están en un solo territorio vigilado, sino en varios sitios, y para su comunicación no se usa un canal dedicado (empresa con estructura multisucursal).

¡ATENCIÓN!

Un servidor proxy antivirus usado en los sistemas de filtrado Gateway antivirus permite mejorar bastante la calidad de filtrado del flujo de correo gracias al uso de los mecanismos imposibles en un servidor de correo por causa de limitaciones de interacción con el servidor para las interfaces de programas antivirus. Por ejemplo, la interfaz de interacción con el servidor de correo MS Exchange para sistemas antivirus no permite recibir el mensaje entero, lo que dificulta bastante su análisis en busca de spam.

Ventajas de filtrado de correo en la Gateway

- La falta del acceso directo al servidor de correo desde la red Internet no permite a los malintencionados usar las vulnerabilidades (tanto las conocidas anteriormente como las vulnerabilidades de nivel cero), asimismo, gracias a los mensajes creados a propósito.
- El uso de las soluciones Gateway antivirus (por ejemplo, Dr.Web Mail Security Suite Antivirus + Antispam + SMTP proxy):
  - mejora significativamente la seguridad global de la red;
  - mejora significativamente la calidad de la filtración debido a la ausencia de las restricciones establecidas por los servidores de correo;
  - reduce la carga de los servidores de correo internos y estaciones de trabajo;
  - mejora la estabilidad de funcionamiento del sistema de escaneo de correo en total.
- El procesamiento del correo en la Gateway permite evitar la llegada de spam en el servidor de correo lo que reduce bastante el volumen del tráfico parásito y por lo tanto mejora el rendimiento y la disponibilidad del servidor para usuarios. Como resultado, eso reduce los gastos de la infraestructura IT por causa de:
  - reducción significativa de los gastos del tráfico parásito;

  - falta de necesidad de aumentar el número de servidores o realizar las actualizaciones de hardware;
  - reducir los gastos de almacenamiento del correo, asimismo, del spam.

2. Es necesario garantizar la protección del servidor donde está implementada la Gateway de correo.

Igual que un servidor de correo, una puerta de enlace es un servicio ordinario ubicado en un servidor ordinario. Por lo tanto, si el sistema de archivos usado es Windows, además de la protección de la Gateway debe usarse la protección del servidor, es decir, no un solo producto, sino dos — por ejemplo, Dr.Web Server Security Suite y Dr.Web Mail

Principios de filtrado del tráfico de Internet en Gateways

¡ATENCIÓN!

En caso de usar servicios en la nube, así como si hay sucursales, es obligatorio usar Gateway en la parte de la empresa - solo esta medida garantiza la limpieza del tráfico de Internet recibido.

El uso del filtrado antivirus a base de soluciones Gateway asegura:

- protección contra la infección si hay acceso a los recursos de la empresa por parte del personal que trabaja de manera remota;
- protección contra la penetración de programas nocivos en equipos y dispositivos que no tiene protección antivirus porque es imposible instalar la misma - así mismo, impresoras, equipamiento de red, sistema de administración de procesos tecnológicos.

1. Normalmente, las soluciones antivirus para Gateways Internet no son programas autónomos - son módulos adicionales para programas que deben ser instalados en servidores y aseguran acceso a Internet.
2. Igual que un servidor de correo, una puerta de enlace es un servicio ordinario ubicado en un servidor ordinario. Por eso, en caso de usar el sistema de archivos Windows, además de la protección de la puerta de enlace de la red Internet es necesario asegurar la protección del servidor, es decir, adquirir dos productos antivirus:
   - **Dr.Web Server Security Suite** (software Dr.Web para servidores de archivos Windows).
   - **Dr.Web Gateway Security Suite** (software Dr.Web para puertas de enlace Kerio o Dr.Web para Microsoft ISA Server y Forefront TMG).

¡ATENCIÓN!

Si no hay protección de este tipo, los malintencionados pueden comprometer la red de la empresa.

Peritaje de incidentes informáticos vinculados con virus

Un incidente informático vinculado con virus (en adelante — IIV) — es un incidente informático para el cual se usó un programa nocivo o potencialmente peligroso.

Los incidentes de seguridad informática (SI) predominan los incidentes vinculados con virus. Para realizar un IIV los malintencionados usan software nocivo potencialmente peligroso o las tecnologías estafadoras de ingeniería social que provocan el inicio del software nocivo o potencialmente peligroso por la víctima. Estos incidentes se clasifican por el código penal de Rusia como fraude, lo que permite llamar este segmento del mercado de servicios de SI un segmento de management de incidentes de cibredelincuencia.

Servicio de respuesta a incidentes de SI

En el año 2013, la competencia de la empresa Doctor Web fue ampliada y actualmente la empresa es participante del segmento de servicios de SI y management de incidentes de ciberdelincuencia en particular.

Ahora en la empresa Doctor Web funciona un servicio de respuesta a incidentes de SI. Este servicio cuento con un laboratorio de peritaje informático que investiga los artefactos que tiene que ver con incidentes de SI y un grupo analítico que crea los informes analíticos y realiza la actividad estadística.

Peritaje de IIV

El peritaje del software usado para fraudulencia informática es un acto procesar para investigar ciberdelincuencias, un elemento importante de la base de evidencia.

La empresa Doctor Web realiza peritaje de incidentes informáticos vinculados con confidencialidad, integridad y disponibilidad de los datos informáticos y sistemas, para realizar los cuales se usaron programas nocivos y el software potencialmente peligroso.

Formulario de solicitud para el peritaje:
https://support.drweb.com/expertise

Servicios de peritaje de IIV de Doctor Web

- Valoración previa del incidente, volumen de peritaje y medidas necesarias para corregir las consecuencias.
- Investigaciones de peritaje de artefactos informáticos y otros (unidades de discos duros, materiales de texto, audio, foto y video) que supuestamente tienen que ver con IIV.
- **¡No tiene análogos!** Peritaje psicológico de personas (personal) para detectar los hechos de realizar / ser cómplice / ocultar / estimular las acciones ilegales para el cliente (valoración integral de riesgos), así como los hechos de inactividad o negligencia.
- Recomendaciones para crear un sistema de protección antivirus para evitar IIv o reducir su número en el futuro.

Qué hacer en caso de un incidente informático vinculado con virus

Han sido robados los medios del sistema de banca a distancia

Lamentablemente, las víctimas se enteran de robos ya una vez realizados los mismos. Y en este momento es muy importante dar respuesta correcta al incidente.

¡ATENCIÓN!

– No intente actualizar el antivirus ni iniciar el escaneo – así borrará los rastros de los malintencionados en el sistema.

– No intente reinstalar el sistema operativo.

– No intente borrar algún archivo o programa de la unidad.

– No use el equipo desde el cual supuestamente se filtraron los medios de autenticación del sistema de banca en línea – hasta en caso de extrema necesidad de usarlo.

Sus acciones deben ser rápidos y decididos:

1. Llame enseguida a su banco - a lo mejor aun es posible prevenirlo. Incluso si el pago ya había sido realizado, solicite bloquear todas las transacciones de la cuenta comprometida antes de recibir los nuevos medios de autenticación de acceso (nombre de usuario y contraseña, etoken etc).
2. Redacte una solicitud a su banco (banco remitente del pago) y envíelo por fax. Imprime TRES copias de la solicitud y llévalas al banco. Ponga el número de registro en dos copias - una para Vd. y la otra será adjunta a su denuncia a policía. La solicitud recibida de Vd. debe contener el número de orden del documento entrante recibido por el secretario.
3. Redacte una solicitud para el banco del destinatario del pago de su cuenta, envíelo por fax. Prepare TRES copias, al igual que en los pasos anteriores, y repita el procedimiento de registro.
4. Redacte una denuncia a la policía y adjunte a la misma dos solicitudes a dos bancos (del remitente y destinatario del pago). Para realizarlo, debe acudir a a la sucursal más próxima.

¡ATENCIÓN!

Vd. ha sido víctima de un hecho delictivo.

Para incoar una causa criminal, los cuerpos de seguridad necesitan su solicitud sobre el delito.

En caso de rechazo de recepción de la solicitud, reciba el rechazo por escrito para presentar un recurso al organismo superior de la policía (jefe de policía de su cuidad o región). Un hecho de robo confirmado es suficiente para incoar una causa criminal.

5. Redacte una solicitud para su proveedor solicitando recibir los registros de conexiones a la red durante el periodo de robo.

¡ATENCIÓN!

Los proveedores guardan los logs de conexiones de red no más de dos días - no tiene mucho tiempo.

¡IMPORTANTE!

Imprima todos los formularios de solicitudes para tenerlos siempre a mano y no solo en Internet. De realizarlo todo durante 1-2 días desde el momento de detección del robo.

Archivos cifrados por un troyano Encoder

Los troyanos de la familia Encoder cifran los datos en el equipo de la víctima. Se puede intentar recuperar estos datos. Para realizarlo, contacte con el servicio de soporte técnico de Doctor Web lo más pronto posible.

¡ATENCIÓN!

– No use el equipo infectado antes de recibir instrucciones del servicio de soporte técnico de Doctor Web, incluso en caso de necesidad extrema de usarlo.

– No intente reinstalar el sistema.

– No intente borrar ningún archivo o programa del sistema.

– En caso de haber iniciado el escaneo antivirus, no debe realizar ninguna acción irrecuperable para desinfectar/borrar los objetos nocivos. Antes de hacer algo con los virus/troyanos encontrados, póngase en contacto con un experto de Doctor Web o guarde las copias de todo lo nocivo – esto puede ser necesario para buscar la clave de descifrado de datos.

Siempre recomendamos presentar una denuncia a la policía.

Vd. ha sido víctima de un hecho delictivo.

Doctor Web

125040, Federación de Rusia, Moscú, 3-a calle Yamskogo Polya, ed. 2-12a
Teléfono: + 7 495 789-45-87 (multicanal)
Fax: +7 495 789-45-97
www.drweb.com