Dr.WEB®
desde 1992

Protege lo creado

Curso DWCERT-070-3 Sistema antivirus de protección de la empresa

Especialidad:
Especialista certificado en el sistema antivirus de protección de la empresa

Plan

I. Amenazas de virus actuales.

ILUSIÓN

Los hackers solitarios elaboran los virus.

Ya ha pasado el tiempo cuando los creadores de software maliciosos eran los programadores solitarios. Los programas maliciosos actuales son desarrollados no sólo por los creadores de virus profesionales, sino es un negocio criminal bien organizado que incorpora en sus actividades criminales a los desarrolladores de software de sistema y de aplicaciones altamente cualificados.

Los elementos estructurales de algunos grupos criminales

En algunos casos, los papeles de intrusos dentro de las organizaciones criminales pueden ser distribuidos de la siguiente manera:

1. **Organizadores** — personas que organizan y dirigen el proceso de creación y el uso de software malicioso. El uso de malware puede ser tanto directo como a través de su venta a otros delincuentes o asociaciones.
2. **Los participantes:**
   - Desarrolladores de malware
   - Probadores de software creado
   - Investigadores de las vulnerabilidades en sistemas operativos y software de aplicación con intenciones delictivos
   - «Expertos» en el uso de empaquetadores virus y cifrado
   - Distribuidores de malware, especialistas en ingeniería social
   - Los administradores de sistemas que proveen un funcionamiento seguro distribuido dentro de la comunidad criminal y gestión de las redes de bots

Dicha «organización laboral» ha permitido que los grupos criminales organizaran pruebas de malware desarrollado para que todas las soluciones antivirus actuales no los detectaran. Pruebas de software malicioso creado en las versiones actuales de software antivirus permiten a los hackers introducir virus y troyanos esquivando la protección antivirus. Ningún software antivirus, por muy bueno que sea en las pruebas en la heurística, no puede hacer nada en este caso.

También las bandas criminales cada vez más crean llamadas amenazas avanzadas permanentes — programas maliciosos diseñados para infectar los grupos específicos de usuarios (por ejemplo, los usuarios de un banco). Típicamente, son programas maliciosos de alta calidad que no tienen ningún efecto significativo en las máquinas infectadas y en el momento de la infección no son detectables por medios de protección, lo que les permite permanecer sin ser detectados durante un largo tiempo.

Como resultado de transición a los métodos «industriales» de edición del software malicioso en «la vida silvestre», se emiten solamente los programas maliciosos que no pueden ser detectados (antes de obtener actualizaciones) por los antivirus — incluso utilizando mecanismos heurísticos. Lo cual llevó a un fuerte crecimiento en la cantidad de malware no detectables en el momento de penetración.

La aparición de los virus en las manos de los criminales desvaloró pruebas antivirus como criterios para la selección de la protección antivirus.

Gracias a una buena organización de los grupos criminales involucrados en el desarrollo y propagación del virus, la producción de virus se ha puesto en marcha. Esto provocó un crecimiento explosivo del número de malware creado por los intrusos y que sin duda afectará la cantidad de registros de firmas diarios que se agregan a la base de datos de virus.

Hechos

- Servicio de monitoreo de virus Dr.Web recoge muestras de virus de todo el mundo.
- Todos los días el laboratorio antivirus Doctor Web recibe un promedio de más de 100.000 ejemplares de malware.

Para más información visite: http://live.drweb.com.

Analistas de virus no son magos, y no pueden procesar al instante miles de archivos sospechosos entrantes diariamente. El elemento más importante de la lucha contra el malware son sistemas automatizados de procesamiento de flujo entrante de archivos sospechosos que poseen las compañías antivirus. La calidad de estos sistemas no es menos importante que la de los productos comerciales que se ejecutan en los ordenadores de los usuarios.

ILUSIÓN

Antivirus debe detectar el 100% de los virus.

Antecedentes de la ilusión

En la industria antivirus existen pruebas comparativas de detección que llevan a cabo testers «independientes». Para estas pruebas se toma una colección de virus y malware, los antivirus se actualizan y se ejecutan en la colección. Para ganar la prueba, es necesario detectar el **100%** de virus de la colección.

Las características de estas pruebas son:

- ningún probador puede garantizar que su colección contiene sólo malware;
- estas pruebas muestran **sólo una** de las funciones de antivirus - detección de amenazas;
- en este tipo de pruebas se está evaluando la calidad de **sólo uno** componente de la pluralidad de componentes antivirus — monitor de archivos o escáner, es decir, se prueba la lucha de antivirus con amenazas **conocidas** que se encuentran en una forma **inactiva**;
- estas pruebas no muestran cómo se comportaría antivirus en condiciones reales de la infección por virus del ordenador, cómo puede tratar virus, si puede detectar amenazas **desconocidas**.

Precisamente estas pruebas dieron lugar a esta ilusión peligrosa.

Hechos

- Los virus tecnológicamente sofisticados y altamente peligrosos, incluyendo rootkits, son creados con fines de lucro. Los creadores de virus los comprueban si son detectados por cualquier antivirus antes de lanzar tal virus en la «naturaleza viva». Es que, el virus tiene que actuar en la máquina infectada el mayor tiempo posible. Si se detecta fácilmente el virus, entonces es un virus malo, desde el punto de vista de sus creadores. Es por eso que antes de ingresar las muestras de malware en el laboratorio antivirus, muchos de ellos no son detectados por el antivirus.
- El virus puede penetrar en un ordenador a través de vulnerabilidades de día cero (llamados 0day exploits que son las vulnerabilidades conocidas solamente para el creador de virus, o el fabricante de software aún no ha lanzado un «parche» para corregirlas), o mediante las técnicas de ingeniería social, es decir, lo pondrá en marcha el mismo usuario, quien también podrá deshabilitar la autodefensa.

ILUSIÓN

Antivirus atrapan los virus por las firmas (los registros de la base de datos de virus).

Si fuera así, el antivirus sería incapaz frente a las amenazas **desconocidas**.

Sin embargo, el antivirus no ha dejado de ser la mejor defensa eficaz y **única** contra todo tipo de amenazas maliciosas – y lo más importante – tanto **conocidas**, como **desconocidas** para la base de datos de antivirus.

Los productos Dr.Web para la detección y neutralización de **malware desconocido** utilizan muchas **tecnologías no basadas en firmas**, cuya combinación hace posible detectar las últimas amenazas (desconocidas) antes de su incorporación en la base de datos de virus. Veremos algunas de ellas.

- **Tecnología FLY-CODE** provee un escaneo de alta calidad de los objetos ejecutables empaquetados, descomprime cualquier (incluso no estándar) empaquetador mediante la virtualización de ejecución del archivo, lo que permite detectar los virus comprimidos por empaquetadores aún desconocidos para el software antivirus Dr.Web.
- **Tecnología Origins Tracing** – durante el escaneo el archivo ejecutable está considerado como un espécimen, construido de una manera particular, y luego el espécimen resultante se compara con la base de datos de programas maliciosos conocidos. La tecnología permite reconocer con un alto grado de probabilidad los virus que aún no han sido añadidos a la base de datos de virus Dr.Web.
- **Tecnología de análisis de la entropía estructural** – detecta amenazas desconocidas sobre las particularidades de ubicación de las áreas del código en los objetos escaneados protegidos por los empaquetadores.
- **Tecnología ScriptHeuristic** – previene la ejecución de cualquier scripts maliciosos en el navegador y documentos PDF, respetando la funcionalidad de los scripts legítimos. Protege de la infección de malware desconocido a través del navegador web. Funciona independientemente del estado de la base de datos de virus Dr.Web junto con cualquier navegador web.
- **Analizador heurístico tradicional** – contiene mecanismos para detectar malware desconocido. El funcionamiento del analizador heurístico está basado en el conocimiento (heurística) de ciertos rasgos (características) de los virus, como típicos para el código del virus, y viceversa, que rara vez se encuentran en los virus. Cada uno de estos atributos se caracteriza por su «peso» que es el número cuyo módulo determina la importancia y la gravedad de este rasgo, y el signo, respectivamente, indica si confirma o rechaza la hipótesis de la posible existencia de un virus desconocido en el código analizado.
- **El módulo de emulación de ejecución** – la tecnología de emulación para ejecutar el código se necesita para detectar virus polimórficos y de cifrado complicado, cuando la aplicación directa de búsqueda por la suma de comprobación sea imposible o muy difícil (debido a la imposibilidad de construir unas firmas confiables). El método consiste en imitar el rendimiento del código analizado por el emulador. un modelo de software del procesador (y, parcialmente, de ordenador y sistema operativo).

Hechos

- Antivirus Dr.Web tiene un número bajo de entradas de virus en la base de datos, por lo que una sola entrada en la base de datos de virus Dr.Web detecta decenas, cientos e incluso miles de virus similares. La diferencia principal de la base de virus Dr.Web de las bases de virus de otros programas consiste en que aunque disponga del número inferior de entradas, permite detectar el mismo número (e incluso superior) de virus y programas maliciosas.
- La compañía Doctor Web está en constante desarrollo de la tecnología de detección de malware y produce nuevas versiones del motor antivirus. Pero la producción de motor antivirus no son sólo nuevas tecnologías, es una optimización de código y la reducción de cantidad de entradas de virus, que también afecta positivamente a la velocidad de funcionamiento

  Disminución de la tasa de crecimiento en el número de registros es el resultado de la introducción de nuevas tecnologías de detección: ¡Dr.Web puede detectar una gran cantidad de malware utilizando la cantidad mínima de registros!
- Incluso si no hay registro del virus en la base de datos de virus Dr.Web, lo más probable es que va a ser detectado mediante el uso de múltiples tecnologías implementadas en el núcleo antivirus.
- ¡La base de datos de virus Dr.Web está diseñada de tal manera que, al añadir nuevas entradas, la velocidad de escaneo no se disminuye!

¿Qué le da al usuario el pequeño tamaño de la base Dr.Web y el número de entradas inferior que el de competidores?

- Alta velocidad de búsqueda de malware
- Reducción de los requisitos del sistema
- Ahorro de espacio en disco.
- Ahorro del tráfico en la actualización de las bases de datos
- La capacidad de definir los virus que aparecerán en el futuro mediante la modificación de las versiones existentes

¡ATENCIÓN!

Millones de personas de todo el mundo utilizan cada día el producto único Dr.Web CureIt!, creado específicamente para el tratamiento de los ordenadores infectados por virus que ya tienen instalados otros productos antivirus.

ILUSIÓN

¡Ya no hay virus!

De hecho, más del 90% de las amenazas de virus corrientes en el sentido estricto del término no se pueden denominar, ya que no cuentan con mecanismos de autorreplicación (autorreplicación sin intervención del usuario). La gran mayoría de amenazas actuales son programas troyanos. Pertenecen a la categoría de programas maliciosos y pueden causar serios daños al dueño del ordenador infectado.

Troyanos peligrosos:

1. No los ven usuarios, tampoco ciertos software antivirus.
2. Son capaces de robar información confidencial, incluyendo contraseñas, acceso a los sistemas de banca y de pago, dinero de las cuentas bancarias.
3. Pueden descargar otros programas maliciosos e incluso poner el sistema operativo fuera de servicio.
4. Pueden paralizar por completo el ordenador bajo la orden de los atacantes.

Este tipo de programas en el momento de crearse a menudo no son detectados por antivirus. Es más, algunos de ellos están tratando de eliminar el antivirus.

Hechos

- Hasta 70% de los casos de infecciones de las redes locales de las empresas que están aislados de Internet, se deben a las infecciones que se encuentran en medios extraíbles — la gente **personalmente** distribuye troyanos en unidades flash.

¡ATENCIÓN!

El antivirus no siempre puede detectar el programa malicioso más reciente diseñada para ser penetrada de forma oculta, pero ningún otro software, excepto antivirus, es incapaz de curar el sistema de troyano ya penetrado.

ILUSIÓN

La actividad de virus en un ordenador es siempre perceptible. Si el ordenador está infectado, inmediatamente lo sabré y tomaré medidas.

Hechos

- Malware actuales a menudo están diseñados para estar presente en el ordenador de la víctima a largo plazo. Por lo tanto, no sólo actúan de forma incógnita para el usuario sin ser detectados en el momento de su creación por muchos programas antivirus, sino existen programas maliciosos que luchan con los competidores y eliminan otros tipos de malware. ¡Incluso hay malware que cierran las vulnerabilidades en el ordenador!
- Por ejemplo, **Trojan.Carberp**, creado para robar el dinero, al ejecutarse en una máquina infectada, toma una serie de medidas con el fin de engañar los medios de control y vigilancia. Después de un inicio exitoso el troyano se incorpora en otras aplicaciones en ejecución, y su principal proceso se acaba. Por lo tanto, el resto de su trabajo se desarrolla por partes en el interior de otros procesos.

El mito de que la aparición de cualquier virus puede ser perceptible, finalmente ha dejado de existir.

ILUSIÓN

Incluso si el equipo esté infectado, será más barato restaurar Windows desde la copia de seguridad que comprar antivirus.

Amenaza

El malware puede ocultarse en archivos almacenados en otras secciones del disco duro y medios extraíbles. En este caso, la reinstalación de Windows no va a ser útil: cuando se accede a este archivo el malware vuelve a activarse.

¡ATENCIÓN!

*Antivirus es una herramienta de software **única** que puede curar su ordenador de virus penetrado.*

Incluso si usted no tiene copia de seguridad de cada estación de trabajo - no hay problema. Si antes de instalar Dr.Web el sistema estaba infectado, Dr.Web lo curará, y el equipo va a funcionar de nuevo en modo normal. Para tratar la infección activa es suficiente iniciar un escaneo rápido del ordenador, y todas

las amenazas encontradas serán neutralizadas. ¡El tratamiento incluso de varios equipos de la red tomará menos tiempo que la restauración del sistema desde una copia de seguridad! Al mismo tiempo se ejecuta:

- desinfección de archivos infectados;
- arreglo automático de registro de Windows;
- eliminación automática de los servicios maliciosos;
- eliminación automática de rootkits y bootkits.

Recursos de información sobre las amenazas de virus actuales

- Laboratorio antivirus Doctor Web: http://live.drweb.com
- Descripción de virus y programas maliciosos: http://vms.drweb.com/search
- Reseña de los virus y el spam: http://news.drweb.com/list/?c=10
- Amenazas corrientes: http://news.drweb.com/list/?c=23
- Suscripción al boletín de noticias sobre los virus y reseñas: https://news.drweb.com/news/subscribe
- El envío de archivos sospechosos para el análisis: https://vms.drweb.com/sendvirus
- Escáner Dr.Web en línea: http://vms.drweb.com/online

II. Modos de penetración de amenazas de virus en redes corporativas

La mayoría de las empresas cometen grandes errores en la construcción de la protección antivirus, guiándose por la información obsoleta sobre las formas de penetración de programas maliciosos y sus capacidades.

Para organizar un sistema antivirus eficaz de protección de red local los especialistas de seguridad de información deben saber las rutas **actuales** de penetración de programas maliciosos en la red local. Las formas más comunes a la fecha son:

1. Vulnerabilidades

Vulnerabilidad es una falla en el software, con el que se puede poner en peligro la integridad del software o causar incapacidad. Las vulnerabilidades existen en cada software. No hay ningún software donde no habría vulnerabilidades.

Los creadores de virus modernos explotan vulnerabilidades para poder penetrar en el ordenador local no sólo en los sistemas operativos, sino también en las aplicaciones (navegadores, productos de oficina, tales como Adobe Acrobat Reader y plugin para los navegadores para visualizar el flash).

El virus puede penetrar en un ordenador a través de vulnerabilidades de día cero, o mediante las técnicas de ingeniería social, es decir, lo pondrá en marcha el mismo usuario, quien también podrá deshabilitar la autodefensa.

¡ATENCIÓN!

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

¡ATENCIÓN!

Ningún software requiere una actualización frecuente como antivirus. Los nuevos virus están elaborándose constantemente, y la base de datos de virus se actualiza con una frecuencia muy alta.

¡La actualización automática de antivirus debe estar siempre activada!

2. Páginas web:

La gente tiene que leer noticias en Internet y estar al tanto de las novedades. El peligro es que la mayoría de los empleados de la oficina:

- accede a Internet desde un ordenador personal en el que el software tiene vulnerabilidades;
- trabaja bajo Windows como administrador;
- trabaja usando contraseñas simples, que pueden ser hackeados sin dificultad;
- no actualiza la seguridad de todo el software instalado en el PC.

Visitas incontrolables a los sitios web crea la posibilidad de fuga de datos, sustitución o intrusión de los materiales importantes.

*Los troyanos Carberp penetran en los ordenadores de los usuarios **durante la visita de los sitios hackeados**. No es necesario emprender ninguna acción con el fin de «conseguir el troyano»: **la infección ocurre automáticamente.***

Los sitios que puedan ser fuentes de malware (en orden descendente de frecuencia de incidentes)

- Sitios dedicados a la tecnología y telecomunicaciones
- Páginas web comerciales: los medios de comunicación de negocios, portales de noticias de negocios, sitios y foros de contabilidad, cursos/ lecciones en Internet, servicios para mejorar el rendimiento de empresa
- Sitios pornográficos

3. Dispositivos extraíbles

Incluso en los sistemas de información bien protegidos la fuente principal de la distribución de virus ya no es el correo electrónico, sino los virus en los medios extraíbles, más a menudo unidades flash USB.

¡ATENCIÓN!

Los medios extraíbles no son sólo una tarjeta de memoria flash, sino ***cualquier dispositivo que utiliza puerto USB para conectarse a un PC****. Un virus puede ser transmitido de un ordenador a otro, incluso a través de una cámara o un reproductor de MP3.*

La mayoría de las amenazas modernas son los troyanos. Son los programas maliciosos por completo que no tienen ningún mecanismo de autorreplicación y no pueden difundirse por sí mismo. La gente personalmente lleva troyanos de un ordenador a otro en una unidad flash.

4. Dispositivos personales, inclusive móviles de los empleados

Hoy en día, más del 60% de los empleados tienen acceso remoto a la información corporativa desde los dispositivos personales tales como teléfonos.

Empleados entusiasmados trabajan no sólo en horario común, y no sólo en la oficina, sino también en el camino y en el hogar. A menudo sacrifican horas de descanso, permaneciendo todo el tiempo en contacto. Y el negocio aprovecha estos cambios con agrado. También, muchas empresas toman empleados remotos.

Pero cada ventaja tiene una desventaja, en otras palabras, hay que pagar por todo. Bajo el método de organización antiguo que se va al pasado la empresa podía en cualquier momento garantizar el cumplimiento de un determinado nivel de seguridad, porque los administradores de sistemas controlaban todos los dispositivos en la compañía. Ahora es imposible.

Amenazas

- Los objetivos de los ataques de cibercriminales hace tiempo que dejaron de ser sólo PC de la oficina — se someten a los ataques los dispositivos personales, incluyendo dispositivos móviles.
- Casi dos tercios de los empleados (63,3%) tienen acceso remoto a la información corporativa desde los dispositivos personales tales como teléfonos.
- Hasta el 70% de las infecciones de LAN se producen desde los ordenadores portátiles personales, netbooks y ultrabooks, dispositivos móviles, así como los medios extraíbles (unidades de flash), incluyendo los de hogar.
- ¡Un 60% de los ordenadores de hogar están sin protección! Lo que significa que los usuarios fuera de la oficina no están protegidos contra los piratas informáticos, las aplicaciones que utilizan pueden tener vulnerabilidades, los ordenadores pueden ser infectados por virus y troyanos. Sin embargo, esas personas ingresan regularmente en red local de la empresa.
- Esto crea la posibilidad de fuga, sustitución o intrusión de datos importantes de la empresa.

Hechos

- Siendo excelentes expertos en su campo, los empleados no son expertos en el campo de la protección antivirus, a menudo son prisioneros de mitos.

5. Correo electrónico

El tráfico de correo es el principal **portador** de virus y spam. En caso de infección del ordenador los malware pueden acceder a la libreta de direcciones del empleado, donde puede haber no sólo domicilios de colegas, sino también los de clientes y socios, es decir, la difusión de la infección comenzará no sólo en la red local de la empresa, sino también más allá de esta.

El descuido, la negligencia y simple ignorancia de los fundamentos de seguridad informática de los empleados de la empresa son a menudo las razones por las cuales los ordenadores se convierten en parte de botnets y fuente de correo no deseado que perjudica la imagen de la empresa, lo que podría llevar a que la compañía aparezca en las listas negras y se desconecte de Internet a causa de envío de spam.

6. 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.

III. Objetivos de la empresa. La relación de objetivos con la estructura de la red local

Por lo general, los empleados de la compañía en el transcurso del día:

- crean archivos de texto y de imagen en los ordenadores y dispositivos móviles;
- envían y reciben mensajes de correo electrónico, tanto dentro de la empresa como a los destinatarios externos;
- reciben, envían, hacen posible recibir ciertos datos externos, por lo general, en forma de archivos;
- colocan la información en el almacenamiento de archivos o descargan de allí, incluso en forma de archivos.

Es difícil encontrar empresas y organizaciones donde no se ejecutan dichas tareas. Por lo tanto, en la mayoría de los casos, al tomar la decisión sobre la organización del sistema de protección antivirus, la cuestión no es si se llevan a cabo estas tareas o no, sino cuál es el número de empleados que realiza tareas.

Para llevar a cabo las tareas de la empresa, la red local debe incluir:

- estaciones de trabajo y/o clientes de terminal - puestos donde trabajan los empleados o visitantes;
- servidores de archivos - para almacenar la información, incluyendo los archivos y documentos, y el intercambio de información entre los empleados;
- servidores de bases de datos, servidores de aplicaciones (por ejemplo, el servidor 1C), servidores DNS/DHCP/Active Directory - para llevar a cabo el trabajo diario, los procesos de negocio, la organización de conexión de los ordenadores en una red, etc.;
- servidores de correo electrónico - para procesar el correo interno y externo;
- pasarelas de Internet - para organizar la salida de la red interna de la compañía a la red externa (generalmente, pero no siempre a la red de Internet).

Naturalmente, no todos estos componentes existen siempre — aparte de los componentes arriba mencionados, también hay otros componentes en la red local, pero en la mayoría de los casos en cualquier organización existen estaciones de trabajo y como mínimo un servidor de correo y un gateway de Internet (puede ser un ordenador que tiene el cable del proveedor de servicios de Internet).

Hay muy pocas excepciones:

- **Todos o una parte de los empleados acceden a Internet por medio de su canal de comunicación.** En este caso, no hay servidor y gateway de Internet. Esta opción es bastante costosa para la empresa y, por lo tanto, es inusual. Puede ocurrir en empresas muy pequeñas (por ejemplo, oficinas notariales) o cuando se emplea un gran número de trabajadores de forma remota. Dicho personal usa servicios públicos para el intercambio de información.
- **La compañía utiliza servidores externos.** Generalmente, se alquilan direcciones de correo electrónico o dominios de correo en el servidor externo (por ejemplo, gmail.com).

Por lo tanto, la pregunta si hay servidores en la empresa casi nunca surge. La pregunta consiste en

- **el número de servidores en la empresa - incluyendo aquellos cuya protección no está prevista por el cliente en la actualidad;**
- **cómo se combinan sus papeles;**

- donde están ubicados (de forma local o remota);
- cómo acceder a ellos (en la red local o de forma remota a través de Internet), etc.

Redes locales de proveedores de servicios

La particularidad de las redes de proveedores de servicios, y en primer lugar, los proveedores de servicios de Internet, es que estas empresas tienen dos LANs independientes. La primera es una red interna de la empresa con su servidor de correo, puerta de enlace de Internet y estaciones de trabajo de los empleados de la empresa. Y la segunda que mantiene los clientes en la empresa. Por lo tanto, la red común del proveedor de la red de Internet puede contener lo siguiente.

- Puerta de enlace de los clientes para acceder a la red de Internet. A través de la puerta de enlace los usuarios tienen acceso a los sitios de Internet, servidores de correo externos, lugares de trabajo remotos, etc.
- El servidor de correo, donde los clientes pueden crear sus buzones o alquilar dominios.
- La red interna del proveedor, donde los clientes pueden publicar sus propios sitios, archivos, documentos, etc. Por lo general, el tráfico de la red interna es gratuito para los clientes.
- Los servidores virtuales donde los clientes pueden crear sus servidores.
- Las estaciones de trabajo y/o los clientes de terminal de los empleados ISP.
- Un servidor de correo interno del proveedor, probablemente (pero no necesariamente), combinado con un servidor cuyos servicios se ofrecen a los clientes

Los grandes proveedores pueden tener un número significativo de servidores. Esto se hace tanto para la distribución (equilibrio) de la carga en horas punta, como para reserva en caso de fallo de uno o más servidores. La presencia o ausencia de algunos componentes, la cantidad de servidores depende del tamaño del proveedor y la lista de servicios disponibles para los clientes.

Los proveedores de Internet pueden proteger a los usuarios contra los virus y el spam:

- por medio de instalación de los agentes antivirus y protección antispam en los equipos de los clientes;
- por medio de verificación de tráfico de correo electrónico e Internet de los clientes.

Se recomienda el uso combinado de estos dos métodos, ya que este enfoque tiene más ventajas que el uso de un solo método. Debido a lo cual

- comprobando el tráfico en el ISP se reduce la carga en el ordenador del usuario, sin necesidad de procesar grandes cantidades de correo no deseado;
- uso de protección antivirus por el usuario permite bloquear la entrada de virus a través del dispositivo de flash.

Sistemas especiales

Hay una serie de empresas y organizaciones que utilizan el sistema, cuya protección antivirus debe llevarse a cabo de una manera especial.

Tales sistemas son:

Sistema de carga alta

La particularidad de sistemas de alta carga es el uso total o casi total de programas que se ejecutan en estos equipos, los recursos del sistema. Ejemplos de tales sistemas en una oficina común son las máquinas, en las que se hacen los cálculos de diseño o de ingeniería.

En una máquina de este tipo, se puede instalar todos los componentes del antivirus, salvo el monitor de archivos.

Debido a que esta configuración no proporciona **protección permanente**, se recomienda habilitar el análisis de los archivos durante la recepción y realizar un escaneo antivirus frecuente (al menos una vez a

la semana, por ejemplo, los días no laborables).

El motor antivirus que se emplea en las soluciones de Doctor Web consume muy pocos recursos y puede reducir automáticamente su prioridad en el caso de carga alta.

Sistemas en tiempo real

La particularidad de sistemas en tiempo real es:

1. Se requiere tiempo garantizado de ejecución de cada operación en el transcurso de su secuencia - diagrama secuencial. Estos sistemas incluyen aquellos que mantienen procesos tecnológicos (llenado de combustible en la gasolinera o en el depósito de aceite), sistemas militares (procedimiento de lanzamiento de cohetes).

   Como se sabe, el funcionamiento de antivirus no implica un tiempo garantizado para escanear archivos - que puede cambiarse como mínimo después de cada actualización.

   Por lo tanto, la instalación del sistema antivirus completo en los sistemas en tiempo real es imposible.

2. Para sistemas en tiempo real se utilizan no sólo modificaciones de sistemas operativos comunes - Windows NT4, Windows Embedded, sino también sistemas operativos especiales, como Neitrino.

   OS especializados no son compatibles con sistemas antivirus.

Para proteger los sistemas en tiempo real basadosen los sistemas operativos comunes, sólo se puede instalar el escáner antivirus configurado para analizar todo el sistema al iniciar. Además, el sistema operativo en tiempo real debe ser utilizado como parte del segmento de red local, que proporciona la verificación de tráfico de la red antes de que ingrese en la máquina protegida.

IV. La estructura general de la red local

Dependiendo de los objetivos de la empresa las opciones de la estructura de la red local pueden ser de la siguiente manera:

- **Ordenadores independientes que no están conectados entre sí y que no tienen acceso a Internet.** Por lo general, esta opción ocurre cuando, entre otras cosas, la organización debe realizar tareas de alta privacidad. En este caso, en la red se separan los ordenadores o servidores individuales, y la transferencia de datos entre ordenadores y el resto de la red se lleva a cabo en los medios especiales (a menudo registrados). En particular, la separación de los ordenadores puede estar justificado en el caso de la necesidad de reducir el grado de protección, y por lo tanto, el nivel de los gastos para su mantenimiento de acuerdo con la Ley Federal № 152-FZ.
- **Ordenadores independientes que no están conectados entre sí y que tienen acceso a Internet.** Es un caso de poca frecuencia. La versión más común es el trabajo de los empleados desde casa o subcontratistas. Cada uno de estos empleados se conecta de forma independiente a la red de Internet donde ocurre el intercambio de datos.
- **Los ordenadores conectados a la LAN sin acceso a Internet.** Dicha forma se utiliza normalmente en las redes que requieren alto nivel de seguridad. En tales organizaciones existe una red común o los ordenadores conectados a Internet, y una red interna aislada de Internet. La transferencia de datos entre redes internas y externas se hace en los medios especiales (a menudo registrados).
- **Los ordenadores conectados a la LAN con acceso a Internet.** El caso más común que sucede en la práctica, no requiere comentarios.

En el caso de acceso a la red de Internet la información puede estar en las estaciones de trabajo, servidores ubicados localmente y servidores remotos, incluyendo ubicados en el centro de datos (servicios en la nube).

Al elegir los medios de protección, salvo la topología de la red, se debe considerar el tipo de acceso de los usuarios a los ordenadores. Hay dos tipos — **monousuarios y multiusuarios**. En el primer caso, en el equipo puede trabajar un solo usuario, en el segundo, más de uno. Por lo regular, aparte del usuario el administrador de la red también tiene acceso al ordenador, por lo que todas las redes pueden ser consideradas como multiusuarios por defecto.

Actualmente las redes multiusuarios están construidas **en base de los grupos de trabajo,** o **basándose en el dominio**. Otras opciones (redes punto a punto, redes basadas en Novell Netware) son muy raras. La diferencia entre los grupos de trabajo y dominios se encuentra en el hecho de que en este último caso, la red dispone de un servidor de dominio (por lo menos, uno o dos - uno primario y uno de reserva), en el que la estructura de Active Directory almacena información sobre todos los usuarios y los equipos de la red, políticas de grupo de la red, contraseñas, etc.

La información acerca de la base sobre la que se construye la red, es muy importante: en caso de ausencia de la estructura de dominio no hay garantía de que todos los equipos tengan la misma contraseña del administrador, lo que complica considerablemente el procedimiento de implementación de la protección antivirus, aumentando el tiempo de preparación para el despliegue de la red.

Influencia de la legislación

El tipo de actividad de la empresa ejerce una gran influencia en la organización de la red de área local, y, por lo tanto, en el sistema de protección antivirus, en relación con lo cual puede estar sujeto a ciertas exigencias de la legislación. De este modo, la organización puede utilizar los documentos secretos, y colaborar con ciertas instituciones (el caso más frecuente son las instituciones e institutos de investigación, en colaboración con el Ministerio de Defensa de la Federación de Rusia).

Además, la organización puede mantener infraestructuras importantes (ferrocarriles, centrales nucleares, etc.), y, por lo tanto, se someten a los requisitos de las leyes relativas a la protección de las infraestructuras muy importantes. Por lo general, en las redes locales de este tipo de empresas **una LAN interna está separada de la externa** y la mayoría de los empleados de la empresa no debe tener acceso a Internet o solamente tiene acceso a ciertos servicios.

Nubes y redes locales

Por lo general, la transición en la nube significa la transferencia de las estaciones de trabajo y servidores en un centro de datos (DC) o el uso de los servicios externos en lugar de los propios.

Esto le permite optimizar el coste de la infraestructura y aumentar la tolerancia a fallos de los subsistemas de servidor, pero al mismo tiemp **aumenta los riesgos asociados con la seguridad de la información**:

- el acceso de los intrusos y programas maliciosos a los datos corporativos en servidores remotos (por parte del contratista, incluyendo penetrados a través de máquinas virtuales que no tienen una protección adecuada),
- intercepción y modificación de la información durante la transmisión hacia y desde los servidores remotos,
- posibilidad de fallas en la infraestructura remota o la pérdida de acceso a ésta.

La transición a los servicios externos significa la aparición de nuevos riesgos de seguridad para la empresa:

- Se incrementan los gastos para proveer una transmisión segura - se requiere una organización de canal de datos protegido, lo que significa el aumento de los requisitos de la anchura del canal, y el dinero para la compra de productos respectivos, así como la necesidad de obtener licencias para trabajar con los medios de cifrado.
- No hay garantías de inaccesibilidad de los datos para los empleados del proveedor de servicios.
- Surge un problema con la eliminación de los datos enviados a la nube.

Y esto no es una lista completa.

Problemas similares surgen cuando los empleados utilizan otros servicios en la nube, ya que los datos de la nube se transfieren por un canal seguro evitando los sistemas de seguridad, entonces pasan al usuario cualquier cosa.

De hecho, al transferir los servicios de la empresa en la nube, la empresa pasa de una situación de control de seguridad a una situación de confianza en seguridad de proveedor de servicios.

Una tendencia de moda en la transición a la nube es el uso de los llamados antivirus en la nube. Por lo general, los centros de datos se construyen sobre la base de los productos de VmWare. En este caso, para proveer una protección antivirus en cada servidor de centro de datos se instala una máquina virtual especial, a través de la cual pasa todo el tráfico y en la que se verifican todas las operaciones de archivo que se llevan a cabo en las máquinas virtuales del centro de datos - todas las demás máquinas virtuales no tienen antivirus. Este sistema de gestión de la seguridad está basada en la falsa suposición de que el antivirus debe detectar todos los malware que tratan de penetrarse y no toma en cuenta la capacidad activa de antivirus para contrarrestar la detección de los programas maliciosos desconocidos anteriormente. Por otra parte, este esquema de protección contradice al estándar que se prepara en el área de la seguridad — estandarte nacional (GOST) «Seguridad de la información. Requisitos para la protección de información procesada mediante el uso de la tecnología de virtualización». En particular, de acuerdo con el documento se requiere:

- escanear en busca de malware la zona de descarga de los medios de información conectados a la IP;
- escanear en busca de malware el firmware, el hardware físico y virtual;
- escanear RAM y sistema de archivos del hipervisor y (o) máquinas virtuales en busca de malware;
- escanear en busca de malware los archivos de imagen de software virtualizado y máquinas virtuales, así como archivos de imagen que se utilizan para mantener el sistema de archivos virtual;

- escanear en busca de malware los archivos de configuración del hipervisor y (o) máquinas virtuales;
- filtrado de tráfico de red en las redes virtuales del hipervisor;
- filtrado de tráfico de la red para cada máquina virtual;
- filtrado de tráfico de la red entre los componentes de infraestructura virtual, entre los nodos de red internos y externos del sistema operativo en un host (hipervisor), así como la organización de intercambio de red con las redes de uso de Internet;
- la búsqueda de malware en el entorno operativo del hypervisor del sistema de almacenamiento de datos.

Todo esto puede llevarse a cabo sólo cuando se instala la protección antivirus, incluyendo para cada máquina virtual protegida.

En relación con todo lo anterior, cuando se usan los servicios de nube es necesario estipular medidas para contrarrestar:

- acceso a los datos de los servidores remotos, robo y/o modificación de datos, incluso durante la transmisión de datos entre los servidores remotos y los servidores y estaciones de trabajo ubicados en la red local de la empresa;
- introducción de software malicioso en los servidores remotos, así como durante la transferencia de datos;
- el tiempo de inactividad durante la ausencia de acceso a servidores remotos.

En concepto de estas medidas se pueden usar:

- sistemas de cifrado, así como la creación de canales de VPN;
- gateways de correo en el lado del centro de datos y en el lado LAN o servidores de correo locales que verifican el correo entrante y mensajes de correo electrónico acumulados cuando no hay acceso al centro de datos;
- servidores de archivos y servicios que sincronizan el contenido con el contenido de servidores remotos.

Como ejemplo de los servicios externos puede ser mencionado el uso de servicio «Antivirus Dr.Web» para negocio. La empresa en lugar de organizar su propia infraestructura antivirus aprovecha las oportunidades del proveedor de servicios, que ofrece el servicio de Internet Dr.Web AV-Desk. Es importante que este servicio ha sido diseñado de tal modo para que sus clientes no requieran tener un acceso continuo al servidor de protección antivirus – la protección antivirus funciona de forma fiable incluso en tales condiciones.

Uso de servicios externos

Los empleados de las empresas y organizaciones a menudo utilizan servicios de nube tanto gratuitos como pagados — email, servicios de almacenamiento de documentos, etc. (google.docs, google.mail, google.disk y otros), cuyo acceso no está controlado por los sistemas de seguridad de la empresa.

El uso de estos servicios también lleva ciertos riesgos. Servicios externos son una ruta cómoda de penetración, ya que su uso no garantiza que los documentos almacenados se mantendrán sin cambios. A su vez, los archivos modificados obtenidos desde los servicios en la nube llegan dentro de la red local esquivando las medidas de seguridad de la empresa (por ejemplo, antivirus de gateway de Internet), por lo que se transmiten a través de un canal seguro que está fuera de control de los medios de protección.

En este sentido, todas las empresas deben proteger los nodos de la red, en los que de un modo o de otro puedan aparecer archivos maliciosos - o por los cuales se transmiten. Esto incluye al menos 1) estaciones de trabajo, 2) servidores de correo electrónico y gateways de Internet.

V. Los errores en la construcción del sistema de protección antivirus de la red local

El desconocimiento de las rutas actuales de penetración de amenazas de virus a la red corporativa, las capacidades de los programas antivirus modernos, los requisitos de la legislación para la protección de las redes locales y los conocimientos erróneos que prevalecen entre los profesionales de IT llevan a los siguientes errores típicos en la construcción del sistema antivirus de protección de LAN.

1. «Es suficiente la protección sólo para estaciones de trabajo. Protección para servidores no es necesaria.»

La situación típica para la mayoría de las empresas es cuando las funciones del sistema de protección contra el malware las cumplen sólo los antivirus instalados en las estaciones de trabajo. Se cree que:

- los virus pueden entrar sólo a través de las estaciones de trabajo, por eso no tiene sentido proteger los servidores;
- todos los archivos entrantes pasan a través de las estaciones de trabajo y será suficiente proteger sólo éstos, el antivirus instalado en las estaciones de trabajo debe proporcionar detección y eliminación de todos malware que penetran de una manera u otra;
- nadie trabaja en los servidores, por lo tanto, nadie los puede infectar;
- protección de servidores es cara.

Finalmente el sistema de protección antivirus implementado de tal manera **no proporciona ni siquiera un nivel mínimo de seguridad**.

Las razones por las que es necesario proteger los servidores (de archivo, de terminales, servidores de aplicaciones (bases de datos)):

- El servidor puede estar infectado por un virus desconocido en el momento de contraer el virus, que penetró en el equipo, y luego se difundió en la red. El antivirus instalado en el servidor lo intercepta de inmediato, basándose en mecanismos heurísticos. En el último caso va a tratar el virus durante la próxima actualización. La ausencia de antivirus lo convertirá el servidor en una fuente constante de infección.
- El servidor puede ser hackeado. El antivirus instalado en el servidor va a monitorear y destruir los malware. Si el servidor está bajo el control de un sistema centralizado de gestión, el administrador recibirá inmediatamente la notificación de cambio de estado de la estación (por ejemplo, sobre el intento de detener el sistema de seguridad).
- Los usuarios pueden trabajar no sólo en la oficina sino también en casa, guardar los datos en los servidores de archivos de la empresa y en servidores de Internet; utilizar sus unidades de memoria flash o las de amigos y colegas. Estos medios pueden contener virus. Los teléfonos celulares modernos por sus capacidades y vulnerabilidades pueden ser comparados con los ordenadores – ya que utilizan los sistemas operativos y aplicaciones, que también pueden estar infectados. Los virus pueden llegar a la red corporativa y acceder al servidor.

2. «La empresa tiene la obligación de proteger sólo los dispositivos que le pertenecen».

Hoy en día, nadie puede negar la necesidad absoluta de proteger las estaciones de trabajo de la empresa. Pero el error más común en la construcción de la seguridad de la red local es la decisión de organizar la protección sólo de los equipos de oficina.

Bajo el método de organización antiguo que se va al pasado la empresa podía en cualquier momento garantizar el cumplimiento de un determinado nivel de seguridad, porque los administradores de sistemas controlaban todos los dispositivos en la compañía.

Ahora es imposible, porque hoy en día la mayoría de los equipos que se encuentran dentro de los locales de la empresa, no le pertenecen, son la propiedad de los empleados, sus ordenadores portátiles y teléfonos inteligentes.

Hasta un 60% de los dispositivos y los ordenadores personales de los empleados no tienen protección antivirus.

Desde estos equipos entran a la red local, siendo fuentes de archivos maliciosos y un gran trampolín para que los hackers penetren a una LAN esquivando la protección del perímetro.

En interés de la empresa es necesario garantizar la seguridad de todos los dispositivos que utilizan sus empleados — donde sea que trabajen, y a quien sea que pertenezcan.

¡IMPORTANTE!

El centro de control Dr.Web Enterprise Security Suite le permite gestionar la protección de los ordenadores tanto de oficina, como de hogar, incluyendo los dispositivos móviles bajo Android y Windows Mobile.

3. «Bastará un solo antivirus. Protección completa es un exceso».

La mayoría de las empresas compra sólo antivirus para proteger las estaciones de trabajo y no una protección completa. Se cree que será suficiente, incluso si el virus entra en la máquina, el antivirus lo destruirá, también «tenemos un poco de spam».

Al mismo tiempo erróneamente se cree que la única tarea de antivirus es evitar que un malware penetre en la red de área local, en otras palabras, el antivirus de calidad debe reconocer en el momento de la penetración todos o casi todos los malware. La utilidad Dr.Web CureIt! se encarga de eliminar los malware ya infiltrados y activos **(por desgracia, en la mayoría de las empresas, esta licencia se utiliza ilegalmente de forma gratuita)** y el antivirus que deja pasar malware se considera deficiente y debe ser reemplazado.

¡ATENCIÓN!

El sistema de protección antivirus de hoy no es igual al antivirus de archivos de ayer.

La función del antivirus es detectar y destruir archivos dañinos, pero sólo puede eliminar amenazas **conocidas** a las bases de datos de virus o amenazas que pueden ser detectadas por los mecanismos heurísticos. Antes de recibir actualizaciones el antivirus no puede ni detectar ni destruir una amenaza **nueva desconocida**.

Protección completa bloquea la mayoría de las rutas de ingreso de virus debido a la posibilidad de prohibir el uso de medios extraíbles y restringir el acceso a los dispositivos locales y de red (incluyendo los directorios en el equipo local y sitios de Internet) - un virus nuevo, aún no captado para el análisis en el laboratorio antivirus y por lo tanto no detectado por antivirus, simplemente no podría llegar a un servidor protegido o estación de trabajo.

Ventajas de la protección completa

- Analiza el tráfico de Internet antes de que ingrese en el navegador y escanea el tráfico de correo electrónico antes de que ingrese en el cliente de correo. Es decir, los virus no serán capaces de aprovecharse de las vulnerabilidades de los programas pertinentes - ya hace tiempo en orden de

penetrar en un ordenador se utilizan más vulnerabilidades de software (en primer lugar, Adobe), y no las vulnerabilidades en los sistemas operativos;

- disminución en el porcentaje de spam en el tráfico de correo electrónico hasta un mínimo, lo que aumenta significativamente la productividad, ya que:
  - los usuarios se distraen mucho menos de su trabajo principal para revisar el correo entrante,
  - se disminuye la probabilidad de que se omita o se elimine un mensaje importante.

4. «Todas las amenazas provienen sólo de Internet. Entonces, ¿por qué proteger un ordenador que no tiene conexión a Internet?»

La opinión generalizada es que si el equipo no está conectado a Internet o aislado de la red, no necesita la protección antivirus. Dichas máquinas sin protección son fallos en el sistema de seguridad y causas de infección de la LAN.

Las principales formas de penetración de malware en las máquinas y luego en una red local o en los equipos de los clientes de la empresa son los dispositivos extraíbles que se utilizan sin control por los empleados en caso de ausencia de control de oficina en el ordenador que tiene medios de limitación de acceso.

5. «No hay virus bajo Mac y Linux».

Otra ilusión es que debido al número relativamente pequeño de programas maliciosos para sistemas operativos como Mac, Linux y Unix, sólo es necesario proteger las estaciones de trabajo y servidores bajo sistemas operativos como Windows. Como resultado de este enfoque los malware obtienen un refugio seguro en las máquinas vulnerables — incluso si no pueden infectar los sistemas operativos y las aplicaciones en ejecución, pueden utilizarlos como fuente de infección, por ejemplo, a través de los recursos compartidos de red.

¡ATENCIÓN!

La tendencia del año 2013 fue un fuerte aumento en el número de ataques a los sistemas operativos Linux. Si anteriormente las noticias acerca de la infección de máquinas bajo Linux eran muy inusuales, a mediados de 2013 casi todas las semanas aparecía información sobre nueva infección masiva o la piratería.

6. «Cartas en el servidor no se pueden abrir, por lo que el servidor no podrá infectarse. Tenemos un administrador sensato — no dejará pasar los virus».

Sí, es cierto, pero en el caso de almacenamiento de correo en el servidor SOLO el antivirus para servidores de correo es capaz de eliminar malware de los buzones.

Además, hay que recordar: aunque los sistemas antivirus de protección de gateways y sistemas de correo realizan la tarea de intercepción de virus en la fase de propagación (penetración) y no participan en la protección contra el malware durante su activación (inicio) — lo cual sucede en las estaciones de trabajo — a excepción de la protección instalada de los servicios que se ejecutan en el servidor (incluyendo los de correo), es indispensable **utilizar de forma complementaria** el antivirus para proteger el sistema de archivos.

7. «El centro de control del sistema de protección antivirus sirve sólo para la comodidad del administrador del sistema.»

Es una opinión fundamentalmente equivocada. La presencia de la gestión centralizada del sistema de protección antivirus influye de manera significativa en el nivel de seguridad de la información de la empresa. El centro de control es un **garante de la política de seguridad de la información** para cada objeto protegido. Le permite:

- crear diferentes configuraciones para diferentes grupos de usuarios sin la necesidad de configurar la seguridad para cada estación de trabajo individual;
- asegurar de que el antivirus en cada estación de trabajo no está desactivado y funciona de acuerdo con los ajustes que estableció el administrador de la red;
- realizar actualizaciones regulares del sistema y escaneos de ordenadores.

¡ATENCIÓN!

El Centro de Control Dr.Web está licenciado de forma gratuita.

VI. Requisitos generales para organizar el sistema de protección antivirus de la red local

1. Sistema de protección antivirus que se utiliza debe:

- **tener un sistema estable de autodefensa** que no permitirá a un malware desconocido interrumpir el funcionamiento antivirus normal y hará posible el funcionamiento del sistema de protección antivirus antes de recibir actualización que permita tratar la infección;
- **tener un sistema de actualizaciones** que se encuentra bajo el control del sistema de autodefensa del sistema antivirus y **no utiliza los componentes del sistema operativo** que pueden ser comprometidos; el sistema de actualización que permite bajo la señal del sistema de control centralizado hacer llegar las actualizaciones en el objeto protegido para tratar la infección activa;
- **tener un sistema de recopilación de información sobre las nuevas amenazas**, que permite transferir rápidamente el material en el laboratorio antivirus para el análisis del virus y emitir actualizaciones;
- **tener capacidad de tratar** no sólo los malware entrante (inactivos), sino que ya se están ejecutando y son desconocidos a la base de datos de virus;
- contar con mecanismos adicionales (excepto de firma y heurística) para detectar malware **nuevos desconocidos**;
- escanear todos los archivos entrantes desde la red local **antes de que los reciban las aplicaciones utilizadas**, lo que impide a los malware aprovecharse de las vulnerabilidades desconocidas de dichas aplicaciones;
- tener un sistema de **recopilación centralizada de información** desde estaciones de trabajo y servidores remotos, lo que permite pasar rápidamente al laboratorio antivirus toda la información necesaria para resolver el problema;
- tener **el servicio de soporte local** en ruso.

2. Es necesario usar el **sistema de gestión centralizada** de protección antivirus, que debe:

- **Asegurar la entrega rápida de actualizaciones** de bases de datos de virus de todas las estaciones de trabajo y servidores protegidos — por decisión del administrador perjudicando el rendimiento total de la red local protegida. La minimización de tiempo para obtener actualización debe ser proporcionada por la minimización del tamaño de las actualizaciones, así como por una conexión permanente de las estaciones de trabajo y servidores protegidos con el servidor de actualizaciones.
- Proporcionar **la incapacidad para desactivar las actualizaciones por los usuarios**. La opinión de los empleados de cualquier cargo sobre la frecuencia de las actualizaciones debe **IGNORARSE**.

> ***¡ATENCIÓN!***
> *Ningún software requiere una actualización frecuente como antivirus. Los nuevos virus se están elaborándose constantemente, y las bases de datos de virus se actualizan con la frecuencia muy alta (al menos 1-2 veces por hora).* ***¡La actualización automática de antivirus debe estar siempre activada!***

Administración centralizada del sistema de protección antivirus Dr.Web permite:

- excluir la posibilidad de cancelar actualizaciones de la estación de trabajo por el empleado;
- desactivar de la red el agente no actualizado, y así evitar la propagación de epidemias dentro y fuera de la red local;
- establecer el modo necesario de actualización de componentes Dr.Web en las estaciones protegidas, distribuyendo la carga en diferentes intervalos de tiempo;
- monitorear las bases de virus y el estado de estaciones.

- Proporcionar la **imposibilidad de desactivar los escaneos regulares** por los usuarios, iniciar el escaneo sin intervención de operador de la estación, definir gráficos de escaneos a cualquier frecuencia deseada. La opinión de los empleados de cualquier cargo sobre la frecuencia de los escaneos debe **IGNORARSE**.

¿Por qué es importante escanear regularmente el sistema?

- *El antivirus no reconoce el 100% de los virus en cualquier momento.*
- *El período entre la aparición de un nuevo virus e incorporación de firmas en la base de datos de virus pueden ser días o incluso meses.*
- *Incluso si la firma incorporada en la base puede detectar el virus, no significa que será capaz de tratar este virus - la invención de tratamiento puede llevar mucho tiempo.*

Hechos

- Después de realizar una actualización en resultado de escaneo en el equipo puede ser revelado un número considerable de amenazas previamente desconocidas.

La verificación de escáner es más profunda que el escaneo realizado por el monitor de archivos de fondo — es por eso que a veces ocurre que el escáner detecta virus que no lo ve el monitor de archivo — **es un hecho normal**.

Protección de la red local utilizando servicios en la nube

Debe prestarse una atención especial a la protección de la red local, al usar servicios en la nube. Los riesgos asociados con el uso de servicios en la nube son:

1. Posibilidad de interceptación y modificación de la información durante la transmisión. En este sentido, se recomienda usar servidores proxy antivirus tanto en la nube, como en la empresa. También una buena práctica es utilizar el canal seguro de comunicación, sin embargo, es necesario tener en cuenta el riesgo de penetración de malware en el espacio entre el canal protegido y el programa de cliente.
2. La posibilidad de introducir programas maliciosos en equipos virtuales. En este sentido, se recomienda utilizar medios antivirus para proteger todas las máquinas virtuales, independientemente de su ubicación.

Requisitos adicionales:

El uso de soluciones antivirus deben complementarse:

1. Con el aislamiento de la red interna de la empresa y la red de Internet - la división externa e interna de la red.
2. Registro de acciones de usuario y administrador.
3. Copia de seguridad de la información importante.

Deben ser desarrollados los siguientes procedimientos:

1. El monitoreo periódico de todas las funciones de seguridad de información implementadas por las herramientas de hardware y software.
2. Recuperación de todas las funciones de seguridad de información implementadas por las herramientas de hardware y software.
3. Respuestas a los incidentes de seguridad de información.
4. Informar a los empleados y clientes en caso de incidentes de seguridad de la información.

VII. Características de los componentes de la red y los principios de su protección

1. Estaciones de trabajo y dispositivos móviles

Como muestra la práctica, las estaciones de trabajo (incluyendo dispositivos móviles) y los servidores son los nodos más vulnerables dentro de la red local. Desde estos nodos se distribuyen los virus y, a menudo el spam. Al mismo tiempo, en los ordenadores los virus pueden penetrar de diferentes maneras, para más detalles, consulte «Modos de penetración de malware.»

Protección de las estaciones de trabajo pertenecientes a la compañía

1. Teóricamente cualquier error (vulnerabilidad) en el programa se puede utilizar para dañar el sistema en su totalidad. Puede ser tanto un fallo corto, como el daño grave de datos. Para evitar esto, es necesario seguir unas reglas simples.
   - Descargar e instalar oportunamente todas las actualizaciones y nuevas versiones del software instalado en el ordenador — no sólo del sistema operativo. Entonces, todo el software utilizado debe tener licencia.
   - Usar **el sistema de instalación centralizada de actualizaciones** de todo el software instalado en el PC — esto permitirá que el administrador del sistema controle en tiempo real la ausencia de vulnerabilidades conocidas en los objetos protegidos.

   Sólo el administrador de sistemas cualificado puede tomar decisiones sobre la necesidad de actualizar antivirus, la instalación de un programa o reiniciar el sistema debido a una actualización de seguridad de cualquier programa instalado en el PC. La opinión de otros empleados, independientemente de sus cargos, debe IGNORARSE.
2. Hay que garantizar el control centralizado de todos los componentes de la protección antivirus en todas las estaciones de trabajo dentro de la red local.
3. Es necesario utilizar la última versión del sistema de protección antivirus.
4. Independientemente de la posición, cualquier usuario debe trabajar sólo bajo la cuenta con permisos limitados. La cuenta Invitado debe estar deshabilitada.
5. El administrador del sistema debe conocer la composición de software instalado en los equipos.
6. Debe estar prohibida la instalación de los programas por parte del usuario - lo cual no permitirá al virus penetrar en el ordenador evitando los medios de seguridad.
7. El acceso del usuario deberá limitarse con los recursos necesarios de la red local. Esto requiere el uso del sistema de control configurado y acceso limitado.

   Control de oficina Dr.Web bloquea la mayoría de las rutas de virus debido a la posibilidad de prohibir el uso de medios extraíbles (incluyendo tarjetas de memoria flash) y el acceso restringido a los dispositivos locales y de red (incluyendo los directorios en el equipo local y 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.

9. La verificación del tráfico de Internet debe llevarse a cabo antes de que alcance las aplicaciones de cliente. El sistema antivirus debe analizar todos los enlaces que ofrecen la descarga de cualquier recurso de la web, y todo el tráfico antes de que llegue en el equipo.

   El monitor HTTP Dr.Web verifica el tráfico antes de que entre en el navegador o cliente de correo. En este caso, los virus no serán capaces de aprovecharse de las vulnerabilidades de los programas instalados en la estación de trabajo.

10. El personal sólo debe tener acceso a los recursos de Internet necesarios. La opinión de los empleados, independientemente de sus cargos, acerca de qué recurso web es seguro, y se puede visitar, debe **IGNORARSE**. La posibilidad de acceder a los recursos innecesarios de Internet debe estar prohibida **de forma centralizada**.

    Control de Oficina Dr.Web permite:
    - restringir el acceso a Internet;
    - llevar listas blancas y negras para garantizar el acceso de empleados a los recursos de Internet que se necesitan para cumplir sus funciones;
    - prohibir completamente el acceso a Internet, donde sea necesario (por ejemplo, los ordenadores con sistemas de contabilidad);
    - hacer imposible la cancelación de las restricciones por el usuario en la estación.

    ¡ATENCIÓN!

    Este componente debe instalarse en los equipos que no están conectados a Internet o aislados de la red local.

11. El usuario (por lo tanto, el malware que actúa en su nombre) no debe tener acceso a ningunos recursos locales y de red, excepto de las tareas necesarias para realizar el trabajo. Es inútil convencer al personal de que las unidades flash son peligrosas.

    Sistema de restricción de acceso de Control de Oficina Dr.Web:
    - permite determinar archivos y carpetas en la red local a los que el empleado puede tener acceso, prohibiendo aquellas que deben ser inaccesibles para él, es decir, proteger los datos y la información importante contra el daño premeditado o intencional, eliminación o robo por hackers o insiders (empleados de las empresas que buscan tener acceso a la información confidencial);
    - restringe o prohíbe totalmente el acceso a los recursos de Internet y dispositivos extraíbles y elimina la posibilidad de penetración de virus a través de estas fuentes.

    Un mecanismo adicional de protección contra los virus que se propagan a través de medios extraíbles es el modo de prohibición de auto inicio en el monitor de archivo SpIDer Guard. Cuando se activa la opción «Bloquear Autorun desde medios extraíbles» se puede continuar usando Flash drives en casos cuando es difícil abstenerse de su uso.

    Mejores prácticas

    La posibilidad de conectar dispositivos extraíbles a la estación de trabajo debe estar prohibida **de forma centralizada**.

12. Además, para evitar que los objetos maliciosos penetren en las la red corporativa, las estaciones de trabajo deben utilizar, aparte de la protección antivirus, los siguientes componentes:

- **Antispam** – para reducir el porcentaje de spam en el correo, lo que reduce el riesgo de infección a través de los mensajes de spam y aumenta la productividad.
- **Firewall** – para asegurar la imposibilidad de escaneo de la red local desde el exterior, así como para proteger contra ataques de intranet.

13. El sistema de protección antivirus debe ser instalado en todas las estaciones de trabajo bajo cualquier sistema operativo, incluyendo Mac OS X, Linux y UNIX.

Protección de los equipos donde se lleva a cabo el trabajo con los datos importantes y/o manejo de dinero

Para estos equipos, además de lo anterior, existe una serie de requisitos.

1. El ordenador que se usa para trabajar con los recursos monetarios (sistema de banca electrónica) no debe ser utilizado para trabajar con los datos muy importantes, y viceversa. Ninguna otra operación debe llevarse a cabo en este tipo de ordenador.
2. En un ordenador separado se requiere:

- excluir la posibilidad de ejecutar otros programas, especialmente con destino desconocido y recibidos de remitentes desconocidos;
- eliminar sistemas y servicios de control remoto y bloquear la posibilidad de las conexiones remotas durante el funcionamiento de los sistemas críticos de negocio, excepto el recurso el que se conecta con el sistema de banca electrónica;
- bloquear la posibilidad de visitar los recursos externos de internet mediante los componentes de Control de oficina Dr.Web;
- registrar todos los eventos, incluyendo todas las actividades de administradores y los usuarios de ordenadores;
- deshabilitar la capacidad de ejecutar programas desde carpetas con documentos y directorios de los archivos temporales, tales como Temp;
- utilizar sólo las contraseñas seguras. La resistencia de contraseñas debe ser controlada por medio de un sistema centralizado que proporciona el cumplimiento de los requisitos de seguridad de las contraseñas utilizadas y su sustitución periódica.

3. Antes de utilizar el sistema de banca electrónica y/o los datos importantes se requiere realizar una actualización de antivirus y un escaneo rápido del sistema.
4. Después de finalizar el uso del sistema de banca electrónica y/o datos importantes es necesario cerrar el sistema con los datos correctamente (salir del sistema).

Protección de los dispositivos personales, desde los que los empleados de la compañía tienen el acceso abierto a la red corporativa

Hoy en día, muchos funcionarios de oficina utilizan sus propios dispositivos para acceder a los recursos corporativos y/o trabajan de forma remota. Hay una amplia gama de profesiones cuyos representantes siempre están en contacto: en el trabajo, en el camino, en casa. La empresa debe estar interesada en hacer que el trabajo en cualquier lugar sea seguro, y los datos corporativos estén protegidos.

Muy a menudo los sistemas operativos de hogar operan bajo Windows. Por ser difundido y bien conocido por los piratas informáticos, precisamente para este sistema se crea la mayor parte del malware. Formas de proteger el sistema operativo son bien conocidos, pero para los ordenadores de hogar de los empleados de los que acceden en la red de la empresa, es necesario combinar la obligación de cumplir las restricciones corporativas, por un lado, y por otro lado, el uso libre de un ordenador personal/dispositivo. Por ejemplo, es necesario combinar la prohibición de visitar sitios de redes sociales durante las horas de trabajo y la necesidad de dicha comunicación en el tiempo libre. También es necesario tener en cuenta la oportunidad de trabajar en el equipo, no sólo del empleado, sino de su familia.

Hay dos variantes de la protección.

- **Primero** – agregar la cuenta de otro usuario en su ordenador personal (Windows lo permite hacer) e implementar todos los parámetros de seguridad necesarios para este usuario. Desafortunadamente, este método le permite cumplir los requisitos de seguridad sólo parcialmente. Por lo tanto, si usted trabaja bajo la cuenta del usuario «protegido» el virus no ingresará, nada va a impedir que penetre en el ordenador durante el trabajo bajo otras cuentas y obtenga el acceso a la información guardada sin protección. Asimismo, nada va a impedirle cambiar la configuración de seguridad estando en una cuenta insegura. Así que para un usuario protegido es necesario instalar el almacenamiento de archivos adicional y el sistema de supervisión de la integridad. Pero el problema principal es que todo eso debe ser configurado por el administrador para cada usuario, en la mayoría de los casos de forma remota.
- **El segundo variante (más correcto)** es utilizar un disco de inicio o USB, que tienen todos los componentes necesarios para un funcionamiento seguro. Eludir la protección sólo pueden los virus al nivel de BIOS, pero aun así es inusual todavía.

¡ATENCIÓN!

*Sólo garantizando la protección de todos los dispositivos, incluyendo móviles que usan empleados, se puede **garantizar** que desde los ordenadores personales y dispositivos móviles de los empleados no penetrará nada malicioso en la red corporativa, tampoco serán robados los datos y las contraseñas que utilizan los empleados para acceder a la red de la empresa.*

1. La opinión del empleado, independientemente de su cargo, acerca de qué antivirus debe estar instalado en su dispositivo personal debe **IGNORARSE** – siempre que el dispositivo forma parte de la red corporativa. De lo contrario, dicho dispositivo debe ser anunciado «no confiable», y no debe tener acceso a la red.
2. El cumplimiento de las políticas de seguridad de información de la empresa y en los dispositivos personales de los empleados, incluyendo la imposibilidad de cancelar los escaneos y actualizaciones periódicas, así como eliminar los componentes de protección individuales, debe ser proporcionado por **las herramientas de gestión centralizada** del sistema de protección antivirus.

En lo demás para proteger los ordenadores personales de los empleados se requiere un sistema similar a los utilizados para proteger las estaciones de trabajo que pertenecen a la empresa.

Capacidades del sistema antivirus Dr.Web permiten

Administrar de forma centralizada la protección tanto de los ordenadores corporativos como personales de los empleados, incluyendo los dispositivos móviles.

La protección de los dispositivos móviles que tienen el acceso abierto a la red corporativa, incluyendo los que no pertenecen la compañía.

Los teléfonos celulares y dispositivos móviles según sus capacidades y vulnerabilidades pueden ser comparados con las estaciones de trabajo. Los dispositivos móviles de hoy en día utilizan sistemas operativos muy potentes y aplicaciones que pueden estar infectados, a través de mismo modo que las aplicaciones de estaciones de trabajo. Al mismo tiempo, el problema principal de uso de dispositivos móviles privados es la posibilidad de expandir malware e infectar LAN - o el acceso a sus recursos evitando la protección.

Los sistemas operativos de dispositivos móviles están desarrollados, por lo general, bajo iOS de Apple o variantes de Android. Estos sistemas son por lo general tienen recursos mucho más débiles que los ordenadores comunes. En estos dispositivos, por lo general, no se puede utilizar varias cuentas, lo que limitaría los derechos de los usuarios y reduciría el riesgo de infecciones. Por lo tanto, la protección sólo puede ser parcial. Además, hay un gran riesgo de pérdida o robo del dispositivo, así como toda la

información (incluyendo nombres y contraseñas para acceder a los recursos corporativos) puede caer en manos de terceros.

Con el fin de proteger el dispositivo móvil se debe utilizar:

1. el antivirus que evitará la penetración de los archivos maliciosos en el dispositivo, incluyendo los diseñados para controlar el desplazamiento del dueño del dispositivo, así como sus contactos y negociaciones;
2. el sistema de protección contra la pérdida del dispositivo móvil lo que permitirá encontrar el dispositivo en caso de su pérdida y no dará a un atacante acceder a los datos almacenados;
3. el sistema de almacenamiento de información confidencial en un repositorio seguro, lo que no va a permitir que el atacante utilice los datos que están en el dispositivo móvil.

Protección para dispositivos móviles es obligatoria, si estos dispositivos se utilizan para recibir los mensajes SMS que confirman las operaciones bancarias, — debido a que el software malicioso modifica ese tipo de mensajes.

2. Servidores

Como ya se ha mencionado, la composición de la red que realiza tareas típicas de «oficina» con un alto grado de probabilidad puede incluir:

- servidores de archivos;
- servidores de correo;
- gateways de Internet;
- servidores de bases de datos, servidores de aplicaciones, servidores DNS/DHCP/Active Directory ...

2.1. Combinación de las funciones de servidores

Funciones de los servidores pueden ser combinados en un servidor, y estar distribuidos en servidores independientes (en este caso, los servidores pueden estar colocados ya sea en el territorio de la empresa (y por lo tanto las divisiones de la misma empresa responden por su seguridad), o de forma remota (incluyendo en el centro de datos).

En el primer caso, el mismo servidor puede funcionar tanto como un servidor de correo como el gateway de Internet y el servidor de archivos. Por lo tanto, en el caso de combinación de funciones de varios servidores en uno solo (si no se trata de la virtualización de servidores - de lo cual se hablará más adelante) se habla acerca de las funciones de servidor, servidor de correo, gateway, etc. Es necesario hacer distinción entre el caso de la combinación de las funciones de servidor y ejecución de diferentes servidores usando los sistemas de virtualización. En este último caso, cada servidor se ejecuta en una máquina virtual, independiente y aislada de otras y no afecta a los otros servidores (si no tomar en cuenta el uso de los recursos del servidor de virtualización).

Funciones de los diferentes tipos de servidores pueden unirse en un solo servidor — y si no estamos hablando acerca de la virtualización de servidores, se trata de las funciones de servidor.

Es necesario hacer distinción entre el caso de la combinación de las funciones de servidor y ejecución de diferentes servidores mediante los sistemas de virtualización. En este último caso, cada servidor se ejecuta en una máquina virtual, independiente y aislada de otras y no afecta a los otros servidores (si no tomar en cuenta el uso de los recursos del servidor de virtualización).

Muy a menudo un servidor combina funciones de gateway de Internet y servidor de correo. El servidor de archivos, además de su función principal (permitir el acceso a los archivos que almacena), puede utilizarse para organizar otros servicios que mantienen la red. Por ejemplo:

- servidores DNS/DHCP, que distribuyen entre los usuarios las direcciones de la red local;
- servidor Active Directory, destinado para el almacenamiento de datos sobre los usuarios de la red;
- servidor de base de datos y el servidor de aplicaciones (por ejemplo, servidor 1C);
- servidor de terminales;
- servidor de correo;
- gateway de Internet.

¡ATENCIÓN!

- *La combinación de funciones permite a la empresa a reducir el número de servidores (ahorrar en la compra de hardware de servidor), pero también reduce significativamente el nivel general de seguridad – la intrusión en un servidor habilita el acceso a todos los servicios de red de la empresa.*
- *Desde el punto de vista de seguridad y fiabilidad de la red, no se recomienda habilitar otros servicios, excepto firewall, en gateway de Internet.*
- *Se recomienda instalar Controller AD en un servidor separado.*

Si no es deseable combinar los papeles (debido a los requisitos de seguridad, la incompatibilidad de los programas, etc.) en un único servidor físico pueden ser desplegados varios servidores virtuales, cada uno de los cuales ofrece un servicio de red: DNS, DHCP, AD, servidor de archivos, etc. En este caso, al diseñar el sistema de protección se debe tener en cuenta el riesgo de contagiar una máquina virtual desde la máquina que cumple la función del hipervisor, así como el riesgo de difusión de programas maliciosos entre máquinas virtuales.

Funciones de diferentes tipos de servidores pueden estar distribuidos en servidores independientes. Tales servidores territorialmente pueden ser colocados en el territorio de la empresa (y por lo tanto los departamentos de la empresa están responsables por su seguridad), o de forma remota (incluyendo el centro de datos).

2.2. Reserva de carga y su distribución

Para aumentar la fiabilidad general de los servicios en los servidores se utilizan los fondos de reserva - tanto al nivel de un servidor (el uso de componentes tolerantes a fallos, raid-arrays, etc.), como al nivel del mismo servicio – se utilizan más servidores de lo necesario para garantizar el buen funcionamiento de la empresa y el fallo de un servidor no conduce a fallo de todo el servicio. A menudo se realizan dos esquemas:

- **reserva en caliente** – la carga (por ejemplo, el correo entrante) se distribuye uniformemente usando un equilibrador software o hardware entre todos los servidores. En caso de fallo de uno de los servidores, la carga simplemente deja de ingresar;
- **reserva en frío** – funciona sólo una parte de los servidores, el resto están en espera. En caso de fallo del servidor la carga se transfiere al servidor ejecutado automáticamente.

El número de servidores responsables de un servicio particular puede ser más de uno, cuando un servidor, obviamente, no puede hacer frente a una carga dada. Muy a menudo en el caso de capacidad insuficiente de un servidor se utiliza distribución de la carga a través del equilibrador o unión de servidores en un solo grupo. En el último caso, el servidor es uno de los nodos del clúster.

2.3. Los servidores de archivos (son los servidores de bases de datos y servidores de aplicaciones)

Objetivos y tipos de servidores de archivos

Un servidor de archivos es un ordenador que aloja/almacena ciertos archivos disponibles para los usuarios.

Es importante distinguir los servidores de archivos creados bajo Windows y Unix.

La función del servidor de archivos está integrada en el sistema operativo de Windows y los usuarios pueden tener acceso (compartir) a cualquier carpeta (directorio). Servidor de archivos es una de las funciones de servidor, así como servidor y DNS/DHCP, AD, servidor de base de datos, servicio de terminal, servidor de correo, gateway de Internet, etc. Sin embargo, el servidor de archivos no debe ser un servidor de base de datos u ofrecer un servicio de terminal — ninguna función puede ser primaria o secundaria para las demás. El administrador selecciona las funciones del servidor.

¡ATENCIÓN!
En Windows el antivirus de archivos analiza los archivos de todo el sistema, y no sólo los que están disponibles para los usuarios.

- Las funciones del servidor de archivos para sistemas operativos Unix, en la mayoría de casos, se implementan a través del subsistema instalado Samba, emulando los servicios apropiados de Windows.

¡ATENCIÓN!
En el sistema operativo Unix el antivirus de archivo escanea sólo las áreas abiertas para los usuarios, todos los demás archivos no se analizan. Esto se debe al hecho de que el antivirus de archivos para sistemas operativos Unix es un plugin (un módulo opcional) del subsistema Samba.

Número de servidores de archivos de la compañía

Podemos suponer que cada empresa tiene al menos un servidor Active Directory o DNS/DHCP. Probablemente dos, uno primario y de reserva, ya que el rendimiento de este servicio es fundamental para la empresa. Casos en los que las direcciones se escriben de forma manual, pueden ser ignorados - es cómodo sólo para las empresas muy pequeñas.

También se puede asumir que cada empresa más o menos grande tiene un servidor 1C, los casos cuando se utiliza otro programa de contabilidad o cuando se utiliza la versión no-servidor son relativamente raros.

Protección de servidores de archivos

1. Los requisitos de seguridad de servidores de archivos se difieren para Windows y Unix. Para los sistemas operativos Windows el uso de archivos de protección antivirus significa la protección de servidores de aplicaciones y servidores de terminales, para los sistemas operativos Unix para la protección de cada servicio es necesario utilizar sus propias soluciones.
2. Para solucionar el tema de organización de protección del servidor, es importante:

- saber cuáles son los servicios adicionales que están funcionando en un servidor de archivos;
- darse cuenta de lo que va a suceder si se usan varios servicios en común en un servicio protegido y qué tan confiable será protegido uno u otro servicio.

¡ATENCIÓN!
SEl uso de un servidor de base de datos en un servidor de archivos protegido no implica el tratamiento de contenido de datos — es necesario utilizar soluciones especiales.

3. Muy a menudo, los empleados utilizan no sólo su propio servicio de archivo, sino también el almacenamiento externo. Al utilizar este almacenamiento no se puede garantizar que el usuario recibirá los archivos no infectados por virus - es posible interceptar un canal de comunicación con Internet y la sustitución de la información transmitida. En este sentido, junto con la protección de un servidor de archivos y todos los recursos de la red de acceso compartido (por ejemplo, carpetas compartidas) en la empresa se debe utilizar gateway antivirus que no permitirá recibir o transmitir el archivo infectado.

2.4. Servidores de impresión

Muy a menudo, los servidores de archivos se utilizan como servidor de impresión, es decir, disponen de servicios que permiten recibir y enviar a imprimir documentos mediante un protocolo especial. Estos servidores también requieren protección debido a que:

- hay un número suficiente de programas maliciosos que infectan los servidores de impresión;
- el atacante puede interceptar tanto información enviada para impresión, como enviar a imprimir documentos que están prohibidas a propagarse fuera de la empresa.

¡IMPORTANTE!

Si como una plataforma para el servidor se utiliza Linux, se recomienda proteger no sólo las funciones del servicio de archivos del servidor (servicio de Samba), sino el mismo servidor. Es decir, es necesario utilizar dos software Dr.Web:

1. Antivirus Dr.Web para Linux
2. Dr.Web para servidores de archivos Unix

Es necesario tener en cuenta el riesgo de infección no sólo de servidores de archivos, sino también las impresoras, sobre todo, accesibles desde Internet. Debido a la falta de recursos en dispositivos las herramientas antivirus no pueden ser utilizados. Por lo tanto, como medida de protección se debe utilizar los medios para limitar el acceso.

2.5. Servidores de terminales

Objetivo y breve descripción del funcionamiento

Si hay un servidor de terminales, los usuarios no trabajan en las estaciones de trabajo, sino en el servidor - como si fuera que el teclado, el ratón y el monitor estén conectados al mismo servidor.

Hay dos formas de conexión con el servidor de terminales:

- con un dispositivo especial - un cliente liviano que no tiene disco duro cuya única función es conectarse con el cliente de terminal;
- con un programa especial desde el sistema operativo habitual.

Servidores de terminales pueden ser creados en base al sistema operativo tanto Windows, como Unix.

Protección de servidores de terminales

La seguridad de servidores de terminales se abastece por los productos diseñados para proteger los sistemas de archivos del equipo, ya que la única diferencia entre los servidores de archivo y de terminales en términos de protección — es la necesidad de verificar las sesiones terminales de clientes — la apertura y el cierre.

- Si la entrada en los servidores de terminales se realiza desde un cliente liviano, la protección de clientes livianos **no se requiere** (no se instala ningún software antivirus en los clientes livianos), pero en orden de proteger las sesiones de terminal es necesario adquirir licencias **Dr.Web Desktop Security Suite Protección** completa igual a la cantidad de conexiones, además de la licencia para la protección del servidor de terminales **Dr.Web Server Security Suite**.
- Si la entrada en los servidores de terminales no se realiza desde los clientes livianos, **se requiere** la protección de los clientes que se conectan al servidor de terminales **(Dr.Web Desktop Security Suite Protección completa + Dr.Web Server Security Suite**). El sistema de protección de las estaciones de trabajo utilizando o no la entrada en el servidor de terminales no se difiere. Lo único es necesario tener en cuenta en este caso, al usar las estaciones de trabajo su cantidad no está considerada en la cantidad de licencias para conectarse al servidor de terminales.

2.6. Servidores y estaciones de trabajo virtuales (incluyendo en las nubes)

Objetivo y breve descripción del funcionamiento

Debido a un aumento de la capacidad de servidores, parecería ventajoso utilizar el mismo servidor para la organización del trabajo de varios servicios. Sin embargo, la combinación de los servicios es a menudo imposible o peligroso. La salida es el uso de servidores virtuales — servidores cuyo único servicio es el llamado hipervisor — el servicio que mantiene los sistemas operativos ejecutados en un entorno virtual. Al mismo tiempo, los sistemas operativos y aplicaciones que se ejecutan en ellos, no funcionan en un servidor físico, sino en su emulación.

3. Servidores de correo

Servidor de correo es un simple servicio, alojado en un servidor de archivos común.

Objetivos de los servidores de correo

- procesar el correo entrante y saliente,
- envío masivo de mensajes de correo electrónico,
- intercambio de datos entre los empleados,
- la base para la construcción de sistemas de flujo de trabajo.

Los servidores de correo electrónico más comunes

- Microsoft Exchange, Kerio MailServer, Lotus Domino y Communigate Pro son unas soluciones comerciales.
- Sendmail, Postfix, Exim (sólo bajo Unix), se utilizan generalmente sólo en modo gratuito de aplicación. Si la empresa es pequeña, es más difícil de persuadir al cliente para utilizar la protección antivirus de pago.

Cantidad de servidores de correo en la empresa

Todos los procesos de negocio dependen de un buen funcionamiento del correo de la compañía, así como su «pureza» de los virus y el spam. Prácticamente todas las empresas tienen un servidor de correo.

Los casos en que las empresas utilizan servidores de correo externos que no les pertenecen son muy raros, incluso si la empresa está utilizando los servicios en la nube, los servidores de correo se administran normalmente por los empleados de la empresa o (en el caso de transmitir los servicios al outsourcing) los empleados tienen acceso a éstos. Sin embargo, hay casos en que las empresas (por lo general, pequeñas) en lugar de desplegar su propio servidor de correo alquilan buzones en un servicio externo (por ejemplo, gmail).

Dependiendo de la organización de la compañía, puede haber más de un servidor de correo. Por ejemplo, en una red con múltiples sucursales en cada división puede haber un servidor de correo. El servidor de correo puede ser colocado fuera de la intranet de la empresa (zona desmilitarizada), etc.

Nubes y servidores de correo

El traslado del servidor de correo al centro de datos, por un lado, aumenta la fiabilidad de funcionamiento del servidor de correo, en este momento es igual a la fiabilidad del centro de datos. Sin embargo, por otro lado, cualquier interrupción con el centro de datos (caída del centro de datos, corte de línea) conduce a la suspensión de trabajo de toda la compañía. Como resultado, para garantizar un rechazo se deben utilizar al menos dos canales para dos proveedores de servicios para introducir dentro de la red local los servidores de tránsito que pueden recibir correo en el tiempo de inactividad del servidor principal. No estarán de más los servidores que garantizan la constancia de correo desde el momento de su envío y recepción.

Filtrado de correo

El tráfico de correo es el principal portador de virus y spam. En caso de infección de la red, precisamente el correo puede ser una fuente de virus y la ruta de penetración a todas las máquinas de la red, ya que en la máquina infectada el malware tiene el acceso a la lista de direcciones del empleado - puede contener tanto las direcciones de sus empleados, como las de sus clientes.

La presencia de una proporción significativa de los archivos maliciosos en el tráfico de correo electrónico, así como la «ingenuidad» de los empleados llevan a:

- las pérdidas y la fuga de datos como resultado de virus y herramientas de hacking;
- captura de la red local como resultado de ataque de virus y su conversión en un elemento de botnet;
- la aparición de la empresa en la lista negra y desconexión de la red de Internet a causa de envío de spam;
- reducción de tiempo de respuesta del servidor de correo que está ocupado procesando tráfico no deseado;
- bajo rendimiento del servidor de correo o su falla completa;
- aumento de la carga en la red interna, reduciendo el rendimiento de recursos de red y ancho de banda;
- fallas en el servidor, como resultado de las «cartas bomba»;
- tiempo muerto del equipo;
- aumento del costo de almacenamiento de correo, incluyendo el spam;
- aumento de los requisitos de hardware de servidores de correo, y por lo tanto la necesidad de actualizar o comprar máquinas nuevas.

La empresa sufre los siguientes **daños de reputación**:

- violación de la seguridad de los procesos de negocio;
- retrasos en las funciones del personal o la incapacidad para llevar a cabo deberes (tiempo de inactividad);
- probabilidad de perder información importante;
- pérdida de tiempo laboral para eliminar los incidentes de virus;
- retrasos en el cumplimiento de las obligaciones de la empresa para los clientes;
- aumento del tamaño de los buzones de usuarios y sus copias de seguridad, que a su vez conducen a problemas para encontrar la información deseada;
- empeoramiento de reputación según los clientes y socios;
- se forma una opinión acerca de la compañía como atrasada tecnológicamente;
- pérdida de clientes o denegación de los servicios de la empresa.

1. ***Es necesario filtrar el correo electrónico externo (entrante y saliente) e interno, es decir, se deben filtrar todas las formas de envío y recepción del correo.***

   En caso de infección de la red, precisamente el correo puede ser una fuente de virus y la ruta de penetración a todas las máquinas de la red, ya que en la máquina infectada el malware tiene el acceso a la lista de direcciones del empleado.

2. ***El correo se debe filtrar en el servidor, y luego en las estaciones de trabajo.***

   Este tipo de protección conduce a **una reducción significativa en la carga** en el servidor de correo y estaciones de trabajo:

- Sólo antivirus para correo puede eliminar durante los escaneos periódicos de los buzones los malware penetrados anteriormente — ningún otro antivirus lo puede hacer.
- El filtrado en el servidor de correo permitirá no sólo filtrar de manera más eficaz el correo, sino desinfectar las bases de correo de virus desconocidos en el momento de aparición, que a su vez evitaría su envío casual al destinatario. Asimismo, las soluciones de servidor para el filtrado de correo en los servidores y gateways permiten implementar el filtrado en formatos de datos, tamaño límite de archivos y otros criterios, que no está en las soluciones para la protección de estaciones de trabajo.

- Escaneo de tráfico se realiza antes de entrar en el cliente de correo electrónico. Es decir, los virus no serán capaces de aprovecharse de las vulnerabilidades de los sistemas operativos y el software respectivo.
- El filtrado de correo a nivel de servidor excluye situaciones cuando el usuario puede desactivar el antivirus o reducir el nivel de protección – los dirigentes de la empresa y el administrador del sistema puede tener confianza en la seguridad de la red.
- Aumenta la importancia de protección. A diferencia de la estación de trabajo, que puede permanecer sin actualización mucho tiempo (por ejemplo, durante la ausencia del empleado), las bases de datos de virus del servidor se mantienen siempre al día.
- Disminuye la probabilidad de un conflicto de software antivirus con otro software. Por ejemplo, con el software instalado por los mismos usuarios.
- El correo, incluyendo spam, será filtrado una vez en el servidor, en lugar de varias veces en cada estación, lo que mejorará su rendimiento, y los empleados van a quejarse menos del «freno» en su PC de trabajo pidiéndote eliminarlos.
- Gracias al filtrado antispam, la carga improductiva parasitaria en el servidor de correo electrónico se reduce (la cantidad de spam en el tráfico postal es de hasta 98%, y su filtrado producirá un efecto positivo en el servidor de correo). Esto reducirá el número de reclamaciones del personal sobre los retrasos en la entrega de correo y correos perdidos.
- Se disminuirá significativamente el tráfico interno debido a los algoritmos de cifrado y compresión utilizados en los productos de servidor para el filtrado antivirus de correo, esta funcionalidad no está presente en los productos de protección de estaciones de trabajo de otros fabricantes.

3. Debe estar prevista la protección del servidor de correo

Protección de servidores de correo (por ejemplo, con las herramientas de **Dr.Web Server Security Suite**) es una medida de protección obligatoria contra virus, desconocidos por el sistema de protección antivirus en el momento de la infección. La penetración de malware desconocido en el servidor de correo y/o en los buzones de correo electrónico convierte el servidor de correo en una fuente permanente de malware.

4. Deben ser protegidas todas las rutas para enviar y recibir el correo, no solamente el servidor de correo.

La particularidad de la oficina moderna es el uso de no sólo los servicios internos, sino también externos, inclusive el correo electrónico. A menudo, los empleados responsables de seguridad de la empresa, no se les informa de los casos de uso de tales servicios.

Los posibles flujos de correo de la empresa

- Un usuario (o programas que va a instalar sin conocer sus capacidades) puede enviar y recibir mensajes:
  - directamente a los servidores de correo de Internet (vía SMTP), si en la red está abierto el puerto 25;
  - a los servicios de correo como mail.ru/gmail.com - por protocolos pop3/imap4.
- Un usuario (o programas que va a instalar sin conocer sus capacidades) puede enviar cartas por los canales cerrados, y el servidor no los puede verificar.
- Servidor (o programas instalados) pueden crear sus propias listas de correo y notificar a los remitentes y destinatarios de varios eventos.

Con respecto, se debe **verificar el tráfico de correo que no sólo va a los servidores de correo de la empresa, sino también a servidores externos no controlados por la empresa**, cuyo nivel de protección se desconoce. En la práctica eso significa:

- filtrar todo el correo electrónico corporativo en el servidor de correo (usando **Dr.Web Mail Security Suite Antivirus + Antispam**) y procesar adicionalmente los protocolos POP3 e IMAP4 en el gateway de Internet (dependiendo del producto utilizado que procesa el tráfico en el gateway – **Dr.Web**

Mail Security Suite Antivirus + Antispam, Dr.Web Mail Security Suite Antivirus + Antispam + SMTP Proxy o **Dr.Web Gateway Security Suite Antivirus**) — junto con el escaneo del correo en la estación de trabajo;

- filtrar todo el correo externo (protocolos POP3 y IMAP4, SMTP) en el gateway (utilizando **Dr.Web Mail Security Suite Antivirus + Antispam + SMTP proxy**), y centrar en el servidor de correo sólo el procesamiento de correo interno (**Dr.Web Mail Security Suite Antivirus + Antispam**) — junto con el escaneo del correo en la estación de trabajo.

La segunda opción es preferible, ya que en este caso:

- la carga en el servidor de correo electrónico se reduce considerablemente (la cantidad de spam en el tráfico postal es de hasta 98%, y su ausencia produce un efecto positivo en el servidor de correo);
- la falta de acceso directo al servidor de correo desde la red de Internet no permitirá que los atacantes se aprovechen de las vulnerabilidades (tanto conocidas previamente, como ataques de día cero), incluso a través de mensajes especialmente diseñados.
- la calidad de filtrado en el gateway de correo es mucho mayor debido al hecho de que la solución para el gateway de correo no se limita con servidor de correo según la funcionalidad.

5. Filtrado de correo debe ser completo.

Sólo las soluciones completas para el correo electrónico, que combinan **antivirus y antispam**, pueden proveer una protección integral y reducción de gastos de la compañía. El uso de antivirus sin antispam:

- permite a los intrusos atacar los servidores de correo del a empresa y clientes de correo de sus empleados;
- conduce a un aumento de las tasas de tráfico;
- conduce a un aumento en la carga parasitaria improductiva en los servidores de correo;
- reduce la productividad de todos los empleados que reciben el correo y se ven obligados a limpiar los buzones de spam.

6. Medidas adicionales de seguridad

- A menudo, los servidores de correo almacenan el correo de los usuarios, ya sea de forma permanente (los usuarios guardan todo el correo en el servidor de la empresa y acceden a través de IMAP4) o temporalmente (hasta que el empleado salga a trabajar). Debido al hecho de que siempre hay posibilidad de que un virus **nuevo desconocido** penetre en el correo antes de llegar al laboratorio antivirus, se recomienda verificar periódicamente los buzones de usuario en busca de virus no detectados previamente, o escanear el correo electrónico cuando se lo envía al empleado.
- Si los locales de una empresa u organización no se centran dentro de un perímetro protegido y están ubicados en varios lugares y la conexión entre ellos no tiene un canal separado, la recepción y el envío de mensajes de correo entre estos locales deben llevarse a cabo a través de gateway — incluso si los locales están ubicados en el mismo edificio, siempre existe la posibilidad de interceptar o suplantar el tráfico.
- El correo filtrado debe ser colocado en una cuarentena y/o archivarse en el caso de reclamaciones sobre el filtrado incorrecto (por ejemplo, en el caso de que el exceso de nivel de detección fue mayor que el recomendado). La presencia de la cuarentena y la función del archivo de los mensajes **Dr.Web Mail Security Suite** permite recuperar mensajes borrados accidentalmente de los buzones de correo personal, así como llevar a cabo investigaciones relacionadas con la fuga de información.

4. Gateways de correo

Gateway de correo - a diferencia de servidor de correo — no almacena el correo — lo procesa «en el vuelo» y lo transmite al destinatario. Gateways de correo se utilizan por:

- **Proveedores de servicios de acceso** — para filtrar el correo de clientes de virus y spam.

- **Empresas** – tanto para reducir la carga en el servidor de correo de la empresa, como para aislarlo del Internet (mayor nivel de seguridad).

La aplicación de gateways de correo se debe a una eficiencia mayor de filtración de malware y de spam, lo que no está disponible en el filtrado en los servidores de correo. La causa son las restricciones impuestas por los servidores de correo en el funcionamiento de software antivirus. Por ejemplo, en el caso de filtrado de correo para Microsoft Exchange las restricciones API (la interfaz de software de interacción del servidor de correo con el módulo de filtrado antispam) permiten verificar sólo algunas partes de las cartas (no en su totalidad) para detectar la presencia de malware y spam. En particular, esto conduce al hecho de que las estadísticas no reflejan el número correcto de mensajes analizados, ya que un plugin solo conoce el número de partes de cartas verificadas, pero no la cantidad de cartas.

Disponiendo de sus propios módulos para enviar, recibir el correo y para acceder a Internet, los gateways de correo pueden implementar mecanismos de filtrado y la autenticación, no disponibles en otros casos.

¡ATENCIÓN!

En el caso de uso de los servicios de correo en la nube, el uso de gateway de correo por parte de la empresa es obligatorio - sólo esta medida garantiza la pureza del tráfico de correo recibido.

Tipos de gateways de correo

En general, los gateways de correo se basan en sistemas operativos Unix. Se puede encontrar dos opciones: el uso de servidor de correo común (a menudo gratuito, como Postfix o Sendmail) en calidad del servidor de tránsito o el uso de soluciones especiales antivirus, que tienen un módulo de transmisión de mensajes de correo.

Mucho menos se utiliza como gateway una de las funciones del servidor MS Exchange (Edge). La conclusión es que las tareas (funciones) realizadas por MS Exchange, pueden funcionar tanto en un servidor como ser distribuidas en varios servidores. Una de las funciones del MS Exchange es el gateway de correo. Sin embargo, debido a las particularidades de licenciamiento la distribución de funciones requiere la compra de licencias especiales, por lo que el uso de **Dr.Web SMTP proxy** en lugar de Edge conduce a un ahorro de gastos.

Como gateway de correo se puede utilizar soluciones de software y sistemas de hardware y software que filtran automáticamente el tráfico de Internet entrante y saliente en todos los protocolos principales - que cumplen la tarea de filtrado de mensajes de correo electrónico en el caso de uso de los servicios de correo externos.

¡ATENCIÓN!

En cuanto a la seguridad y fiabilidad de la red, no se recomienda activar en el gateway de Internet otros servicios, salvo el firewall. Asimismo, se recomienda instalar Controller AD en un servidor separado.

Principios de filtrado de correos en el gateway de correo

1. ***El filtrado de correo es recomendable realizar a través de gateway de correo (Dr.Web Mail Security Suite Antivirus + (Antispam) + proxy SMTP).***

   No es seguro exponer el servidor de correo en Internet o Intranet de la empresa. El atacante tiene grandes oportunidades para acceder al servidor o reemplazar el tráfico, inclusive usando las pestañas de hardware. Incluso si los locales están situados en el mismo edificio, siempre existe la probabilidad de intercepción o reemplazo de tráfico.

   La mejor opción es instalar el servidor de correo en la red perimetral o en una zona desmilitarizada (DMZ) de servidores de correo de tránsito (o Frontend). Servidores reciben el correo y se lo envían al servidor principal de correo dentro de la red corporativa, al mismo tiempo filtrando el tráfico en busca de virus y spam antes de que llegue a la red interna de la empresa. Los servidores pueden ser controlados por los especialistas de la empresa y de la empresa externa (por ejemplo, especialistas de centros de datos).

Se recomienda encarecidamente utilizar el filtrado de tráfico de correo electrónico en el gateway en los siguientes casos:

- la empresa es el proveedor de servicios de Internet;
- el servidor de correo de la compañía está fuera de la zona protegida de la compañía (por ejemplo, en un centro de datos externo);
- la compañía arrienda direcciones postales en un servicio especial;
- los locales de la empresa no se concentran en un perímetro vigilado, sino están colocados en varios lugares, y la conexión entre ellos no tiene un canal separado (una empresa con múltiples divisiones).

¡ATENCIÓN!

*El servidor proxy antivirus utilizado en los sistemas antivirus de pasarela para el filtrado de tráfico de correo, puede aumentar significativamente la calidad de filtrado del flujo de correo a través de los mecanismos aplicados **imposibles** en el servidor de correo debido a las **restricciones** de las interfaces para interacción con el servidor previstas para los software antivirus. Por ejemplo, la interfaz proporcionada a los sistemas antivirus para el servidor de correo MS Exchange no permite obtener la carta en su totalidad, lo cual dificulta su escaneo en busca de spam.*

Ventajas de filtrado de correo en el Gateway

- La falta de acceso directo al servidor de correo desde la red de Internet no permitirá que los atacantes se aprovechen de las vulnerabilidades (tanto conocidas previamente, como ataques de día cero), incluso a través de mensajes especialmente diseñados.
- El uso de soluciones antivirus de gateway (por ejemplo, **Dr.Web Mail Security Suite Antivirus + Antispam + SMTP proxy**)
  - aumenta significativamente la seguridad global de la red;
  - mejora significativamente la calidad de la filtración debido a la ausencia de las restricciones impuestas por los servidores de correo;
  - reduce la carga en los servidores de correo internos y estaciones de trabajo;
  - mejora la estabilidad del sistema de escaneo de correo en general.
- El procesamiento de correo en el gateway ayuda a prevenir la aparición del spam en el servidor de correo, lo que reduce drásticamente el tráfico parásito, y por lo tanto mejora su rendimiento y la accesibilidad para los usuarios. Esto reduce los gastos en la infraestructura de IT mediante:
  - reducción sustancial de los gastos en el tráfico no deseado;
  - ausencia de la necesidad de aumentar el número de servidores o llevar a cabo actualizaciones de hardware;
  - disminución del costo de almacenamiento de correo, incluyendo el spam;

2. Es necesario garantizar la protección del servidor en el que se ha instalado el gateway de correo

Como un servidor de correo, un gateway es un simple servicio, alojado en un servidor común. Por lo tanto, **si el sistema de archivos es Windows**, además de la protección de gateway se debe usar la protección para el servidor, es decir, no uno, sino dos productos — por ejemplo, **Dr.Web Server Security Suite** y **Dr.Web Mail Security Suite**.

5. Gateways de Internet

Objetivo y breve descripción del funcionamiento

Debido a que hay muchos usuarios de Internet y un solo cable que conduce afuera, entonces, se necesita el servidor que habilita el acceso para los usuarios.

El uso de soluciones antivirus de gateway permite:

- excluir la posibilidad de que los malware se aprovechen de las vulnerabilidades, incluyendo aún desconocidas — y como consecuencia, reducir las posibilidades de infectar la red local y/o ponerla fuera de servicio;
- acelerar el rendimiento de las estaciones de trabajo transfiriendo el sistema de escaneo antivirus en el gateway.

Por lo general, las soluciones de gateway antivirus permiten realizar en el marco de la política corporativa la regulación de acceso a los recursos de la web, así como las políticas de acceso a determinados tipos de archivos.

Como gateway se puede utilizar soluciones de software y sistemas de hardware y software que filtran automáticamente el tráfico de Internet entrante y saliente en todos los protocolos principales - incluyendo en el caso de libre acceso de los empleados a los recursos externos de Internet.

Hay gateway de Internet en cada empresa que tiene acceso a Internet. La cantidad de gateways en las compañías con muchos sucursales no es menor que la cantidad de sucursales/divisiones.

Es necesario tener la protección de gateway, si:

- los servidores de la compañía se encuentran fuera del área protegida,
- la empresa cuenta con sucursales,
- los sucursales de la compañía están localizados en varias direcciones o locales separados.

¡ATENCIÓN! En el caso de uso de los servicios en la nube, así como si hubiere sucursales, el uso de pasarelas **por parte de la empresa es obligatorio** — sólo esta medida garantiza el tráfico web limpio recibido.

Principios de filtrado del tráfico de Internet en gateways

1. Por lo general, las soluciones antivirus para gateways de Internet no constituyen programas independientes — estos son módulos opcionales para los programas que deben ser instalados en los servidores y que proporcionan acceso a Internet.
2. Como un servidor de correo, un gateway es un simple servicio, alojado en un servidor común. Por lo tanto, si el sistema de archivos es Windows, además de proteger un gateway de Internet se requiere proveer la protección para el propio servidor, o sea adquirir dos productos:
   - **Dr.Web Server Security Suite** (el software Dr.Web para servidores de archivos Windows);
   - **Dr.Web Gateway Security Suite** (el software Dr.Web para gateways de Internet Kerio o Dr.Web para Microsoft ISA Server y Forefront TMG).

¡ATENCIÓN! La ausencia de dicha protección permite a los atacantes comprometer la red de la empresa.

VIII. Pautas de comportamiento en el incidente cuando tuvo lugar la infección de virus

Han sido robados los medios del sistema de banca a distancia

Por desgracia, las víctimas se enteran del hecho de robo, cuando todo ya ha sucedido. En este momento es muy importante reaccionar correctamente delante del incidente. Antes de seguir nuestras recomendaciones, asegúrese de que el robo se produjo como consecuencia del virus. Para lo cual es suficiente encuestar a los empleados que tienen acceso al sistema de banca electrónica. Si usted u otros no realizaron ninguna operación sospechosa desde su punto de vista, es muy probable que haya actuado un virus o un atacante.

¡ATENCIÓN!

- *No intente actualizar antivirus o iniciar un escaneo – de este modo, ¡usted destruirá las huellas de los intrusos en el sistema!*
- *¡No intente reinstalar el sistema operativo!*
- *¡No trate de eliminar ciertos archivos del disco o programas!*
- *¡No utilice el equipo desde el que se hayan filtrado supuestamente los medios de autenticación del sistema de banca electrónica – aunque haya una grave necesidad (laboral)!*

Sus acciones deben ser rápidas y decididas:

1. Inmediatamente póngase en contacto con su banco, tal vez, la transferencia pueda ser detenida. Incluso si el pago ya se ha ido, solicite bloquear todas las operaciones en la cuenta comprometida antes de emitir nuevos medios de autenticación de acceso (nombre de usuario y contraseña, etoken, etc.)
2. Presente una solicitud a su banco (banco del remitente de pago) y envíelo por fax. Imprima solicitud en tres ejemplares y llévelos al banco. Pida que le pongan el número de registro en dos ejemplares- uno quedará con usted, el otro se adjuntará a su declaración a la policía. La solicitud debe contener la fecha y el número de serie del documento entrante recibido por la secretaria.
   Ejemplo de solicitud
3. Presente una solicitud al banco del beneficiario de su cuenta, envíelo por fax. De forma similar como en el párrafo anterior debe hacer tres copias y repita el procedimiento de registro.
   Ejemplo de solicitud
4. Presente una declaración a la policía y adjunte solicitudes a los dos bancos (del destinatario y remitente del pago). Para eso, acuda a una comisaría más cercana.
   Ejemplo de solicitud

¡ATENCIÓN!

El requerimiento de apertura de causa contra los intrusos para las autoridades policiales es el pretexto procesal, que es su denuncia sobre el delito.
Ejemplo de solicitud
Si se le niegan a aceptar la solicitud, pida la denegación por escrito y presente la queja a los órganos superiores de la policía (al jefe de la policía en su ciudad o región). El hecho establecido de robo es un motivo suficiente para iniciar un proceso penal.

5. Presente una solicitud a su proveedor para que proporcione registros de conexión de red por el período en que se produjo el robo.
   Ejemplo de solicitud

¡ATENCIÓN!

¡ISPs mantienen registros de las conexiones de red no más de dos días – hay poco tiempo!

¡IMPORTANTE!

Imprima todos los modelos de solicitudes para tener a la mano en los momentos necesarios y no en Internet, al que puede ser que no tenga acceso.

¡Todo esto debe hacerse dentro de 1–2 días a partir de la fecha de detectar el robo!

Archivos han sido cifrados por el troyano Encoder

Los troyanos Encoder han sido «famosos» por el hecho de cifrar los datos en el ordenador de la víctima. Estos datos pueden ser recuperados. Para realizarlo, póngase en contacto lo más pronto posible con el soporte técnico Doctor Web por teléfono o desde otro ordenador.

¡ATENCIÓN!

- *No utilice el ordenador infectado antes de recibir las instrucciones del soporte técnico Doctor Web – ¡incluso si haya una necesidad fuerte (laboral)!*
- *¡No intente reinstalar el sistema!*
- *¡No trate de eliminar ciertos archivos del disco o programas!*
- *Si ha sido ejecutado un escaneo antivirus, no se puede tomar ninguna acción irreversible para el tratamiento/eliminación de malware. Antes de hacer algo con los virus/troyanos detectados, usted debe consultar con un especialista de Doctor Web o por lo menos, guardar copias de todos los programas maliciosos encontrados - lo cual puede ser necesario para determinar la clave para descifrar los datos.*

Cómo presentar una solicitud para el soporte técnico de Doctor Web

1. Rellene el formulario de solicitud.
2. Comunique la mayor cantidad posible de información acerca de cómo se produjo la infección, incluyendo requisitos de los intrusos. Si hay alguna sospecha de qué ha sido la causa de aparición de troyano, adjunte los archivos o enlaces respectivos a la solicitud.
3. Adjunte en el comentario de solicitud varios archivos cifrados (preferentemente, de diferentes tipos y tamaños: jpg, zip, doc, pdf, etc.) y los requisitos de los intrusos para transferir dinero.
4. Si el troyano ingresó por correo electrónico (a menudo las cartas con estos troyanos simulan cartas del banco que notifican sobre cualquier problema) y no ha eliminado la carta - guárdela en un archivo eml y adjúntelo al comentario en la solicitud.

Enviar una solicitud para descifrar.

Le recomendamos que dirija una solicitud a la policía.

El requerimiento de apertura de causa contra los intrusos para las autoridades policiales es el pretexto procesal, que es su denuncia sobre el delito.
Ejemplo de solicitud
Prepárese a que su ordenador puede ser retirado en cualquier momento para el examen de peritos.

El troyano bloqueador ha bloqueado Windows

¡ATENCIÓN!

¡En todo caso, no se debe pagar el rescate - usted nunca obtendrá el código de desbloqueo!

Utilice el servicio gratuito de la compañía Doctor Web para desbloquear Windows atacado por el troyano.

Le recomendamos que dirija una solicitud a la policía.

Para iniciar la investigación, la policía requiere un pretexto procesal, la denuncia sobre el delito.
Ejemplo de solicitud

Doctor Web S.R.L.

La compañía Doctor Web es el famoso elaborador ruso de medios de protección de información. Los productos de Dr.Web se están elaborando desde el año 1992.

Doctor Web

125124, Federación de Rusia, Moscú, 3-a calle Yamskogo Polya, ed. 2-12a

Telf: + 7 (495) 789–45–87 (multicanal), **fax:** +7 (495) 789–45–97.

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