Servicio «Antivirus Dr.Web»

para el

Contenido

Introducción

Sistema de protección antivirus Dr.Web

Conclusión

Introducción

Amenazas de virus actuales

Los hackers solitarios elaboran los virus

Anteriormente, los creadores de software maliciosos eran programadores solitarios. Los programas maliciosos actuales son desarrollados por los creadores de virus profesionales, y 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 distribuidas de la siguiente manera:

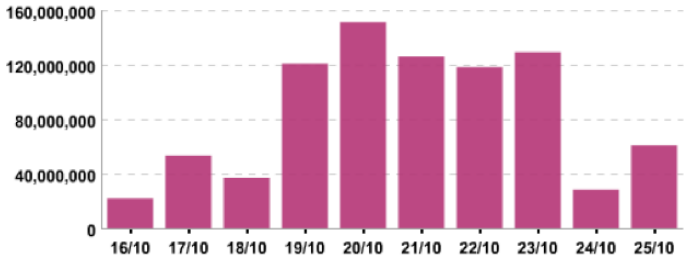
1. Organizadores son personas que organizan y dirigen el proceso de creación y el uso de software malicioso. El uso de malware puede ser tanto directo como a través de su venta a otros delincuentes o asociaciones.
2. Los participantes:

- Desarrolladores de malware
- Personas que realizan la prueba de software creado (se pone a prueba incluso para ser detectado por los software antivirus conocidos)
- 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

Gracias a una buena organización de los grupos criminales involucrados en el desarrollo y propagación de virus, la producción de virus se ha puesto en marcha, que proporcionó el crecimiento explosivo del número de programas maliciosos creados por hackers. Este hecho influyó de inmediato en la cantidad de registros de firmas diarias que se agregan a la base de datos de virus.

Hechos

- El servicio de monitoreo de virus Dr.Web recoge muestras de virus en todo el mundo.
- Todos los días el laboratorio antivirus Doctor Web recibe en promedio al menos 60.000 ejemplares de malware.
- El 28 de noviembre 2012 fue establecido un récord - se ha recibido más de 300.000 ejemplares para el análisis. Esto no es todo de lo malicioso que se crea en 24 horas.



Analistas de virus no son magos, por lo que no pueden procesar al instante miles de archivos sospechosos que entran cada día. Por lo tanto, un elemento esencial de la lucha contra el malware son los programas de procesamiento automatizado de ingreso de archivos sospechosos. La calidad de estos sistemas no es menos importante que la de los productos comerciales que se ejecutan en los ordenadores de los usuarios.

Antivirus debe detectar el 100% de los virus.

Antecedentes de la ilusión

En la industria antivirus existen las llamadas 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 un sólo componente de la pluralidad de componentes antivirus - monitor de archivos o escáner, es decir, se pone a prueba la lucha de antivirus con amenazas **conocidas**;
- estas pruebas no muestran cómo se comporta antivirus en condiciones reales de la infección por virus, cómo es capaz de tratar un virus en particular;
- estas pruebas no muestran si el antivirus es capaz de **detectar amenazas** desconocidas.

Precisamente estas pruebas dieron lugar a esta ilusión peligrosa.

Hechos

- Los virus tecnológicamente sofisticados y altamente peligrosos, incluyendo rootkits, se elaboran 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 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.

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 el tipo de amenazas maliciosas, y lo más importante, tanto **conocidas**, como **desconocidas** para la base de datos de virus.

Los productos Dr.Web con el fin de detectar y neutralizar el 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 las amenazas desconocidas según la ubicación de las secciones de código en los objetos escaneados protegidos por los empaquetadores, según la interrupción de las funciones del sistema y algunos otros parámetros que permiten detectar una parte significativa de las amenazas desconocidas.
- **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 navegadores 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.
- 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 antivirus 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?

- Ahorro de espacio en disco.
- Ahorro de memoria operativa
- Ahorro del tráfico en la actualización de las bases de datos
- Alta velocidad de escaneo de los virus
- 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.

¡Hace mucho que 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!

Ningún otro software, **excepto antivirus**, es capaz de curar el sistema contra el troyano que ya había penetrado.

Ilusión №5

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

Hechos

- Los malware actuales a menudo actúan de forma incógnita para el usuario, sin ser detectados en el momento de su creación por muchos programas antivirus.
- El objetivo de los creadores de virus modernos es la creación de malware que debe permanecer el mayor tiempo posible en el sistema sin ser detectado por el usuario del sistema, ni por los programas especiales (antivirus).
- 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 №6

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.

La fuente principal de infección de virus es el correo electrónico.

Hechos

Las principales fuentes de infección de virus de la red corporativa (en orden descendente de número de infecciones):

- PC personales / PCs de hogar / portátiles / dispositivos móviles de empleados
- portátiles / dispositivos móviles de clientes
- dispositivos extraíbles, ¡no son sólo unidades flash!
- sitios legítimos (necesarios para el desempeño de trabajo y, por lo tanto, no se bloquean) infectados por hackers
- páginas phishing y sitios maliciosos especialmente creados
- correo electrónico
- vulnerabilidades en sistemas operativos y software de aplicación

Es hora de "recoger piedras"

En la historia de la industria antivirus fue un período cuando los programadores en diferentes países por alguna razón decidieron que podían crear programas denominados "antivirus". En 1994, la expansión amplia de virus polimórfico Phantom-1, que no pudo ser detectado por ningún antivirus, excepto Dr.Web, ha puesto todo en su lugar, y ha echado en un vertedero de la industria las artesanías antivirus inútiles.

En julio de 2001, se estalló una epidemia de CodeRed. Resultó que sólo un antivirus en el mundo - el antivirus Dr.Web - fue capaz de detectar el virus en la memoria del ordenador. Incluso en la actualidad, hay pocos programas antivirus capaces de tratar este tipo de amenazas.

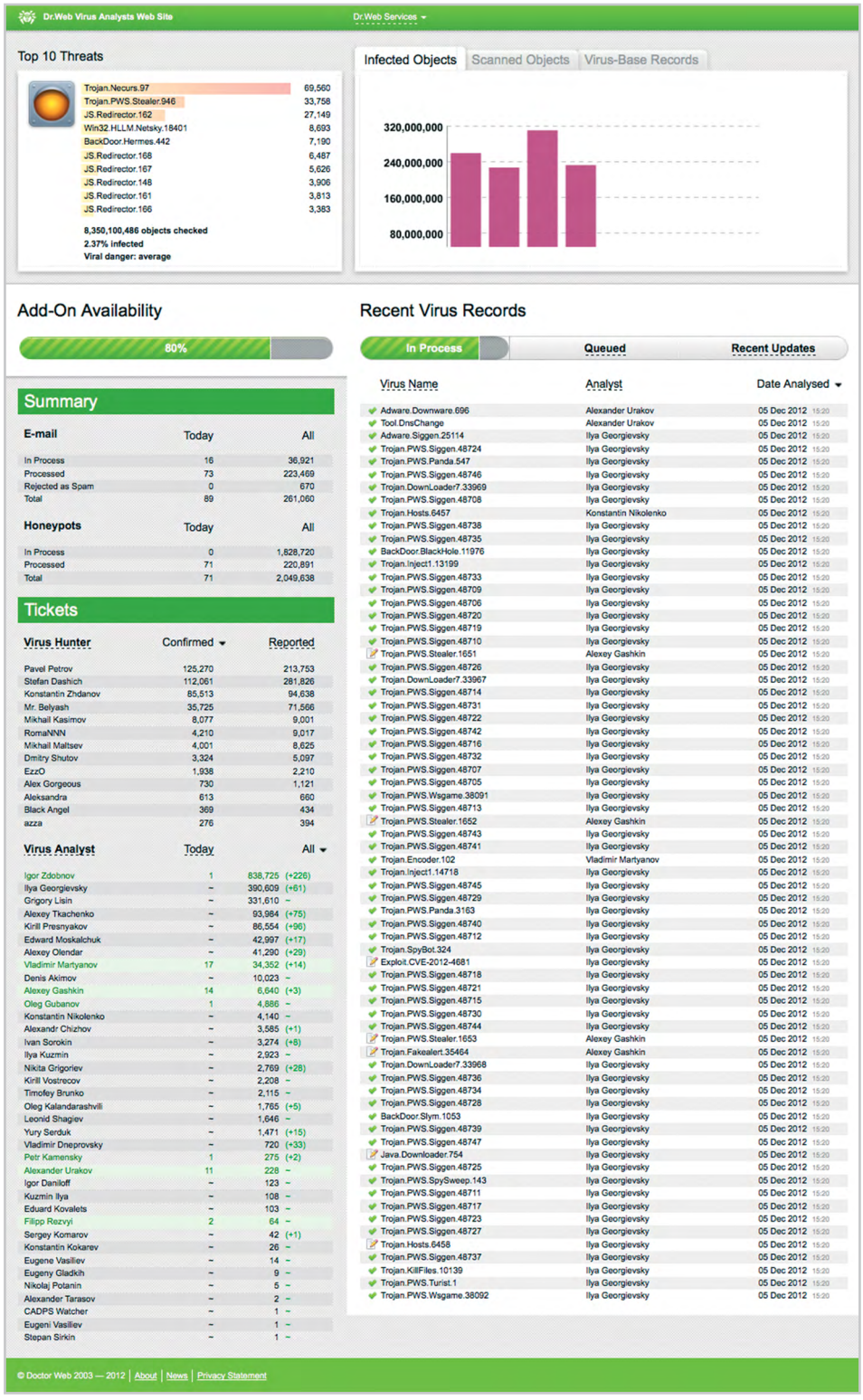
Hoy en día, al parecer, la industria antivirus está lista de nuevo para ser limpiada, lanzar el lastre. En el futuro, en el mercado permanecerán sólo el antivirus que:

- identificará y neutralizarán los virus no sólo basadas en firmas y tecnologías heurísticas, es decir, tendrán una funcionalidad que no permita dejar pasar un objeto malicioso dentro del sistema, incluso si la firma aún no ha sido añadida a la base de datos de virus;
- tendrá un sistema impenetrable de autodefensa - para que un nuevo virus desconocido que ha logrado penetrar en el sistema no pueda poner el sistema fuera del servicio;
- será capaz cualitativamente limpiar el sistema de malware penetrado cuando el programa está activo, resiste, impide la detección y opera en detrimento del usuario, en otras palabras, tratar el sistema en las condiciones reales, restaurar su estado operativo, ya que sólo en las condiciones de una infección real se pone a prueba la calidad de las tecnologías antivirus;
- tendrá disponible un sistema de recogida de información, que permite enviar rápidamente al laboratorio antivirus toda la información necesaria para resolver el problema;
- tendrá una infraestructura poderosa de desarrollo, el propio servicio de monitoreo de virus, el laboratorio antivirus y servicio de atención al cliente;
- será capaz de modelar los nuevos tipos de amenazas antes de que los hagan los creadores de virus y utilizar las tecnologías para luchar con éstos (que definitivamente no serán basadas en firmas).

Todas estas cualidades ya están presentesen el antivirus Dr.Web moderno.

Siempre vivo, siempre abierto

http://live.drweb.com -es un recurso abierto, que muestra el desempeño del laboratorio antivirus "en vivo". Allí podrá ver cómo se procesan las muestras de programas maliciosos que ingresan y qué virus es más común actualmente.



Introducción

Seguridad es un servicio

El software antivirus se utiliza en todas las áreas de la empresa - en el proceso de gestión de la empresa, en la gestión de la contabilidad y de la contabilidad financiera, en la producción. Un antivirus eficaz garantiza la continuidad de los procesos de negocio y es uno de los factores más importantes que influyen en el coste total de propiedad de la infraestructura de TI en su conjunto.

Como muestra la práctica, dentro de toda la gama de productos de las empresas antivirus las empresas pequeñas y medianas en su mayoría utilizan productos de uso personal.

¿Qué antivirus más a menudo se compra para las empresas? ¿El mejor en el mercado? ¿El que más se adapte a las condiciones específicas de la empresa? ¡De ningún modo! Se adquiere aquella licencia para el antivirus, la que sabe administrar el administrador del sistema. Un gran número de funciones de software puede no utilizarse simplemente debido a la ignorancia de su existencia, o por no saber cómo usarlas. Como resultado, la seguridad de la información se convierte en un rehén de la evaluación subjetiva y las calificaciones del administrador.

Un factor grave que impide la implementación de la tarea de un funcionamiento eficaz de la infraestructura de TI en una empresa es la falta de los administradores de sistemas capaces de gestionar de manera competente el sistema de seguridad de la información de la empresa, lo que requiere conocimientos especiales, los cuales la mayoría de los administradores de TI no los tiene. Esto produce una amenaza para la seguridad de la información y como resultado aumenta significativamente el coste total de antivirus, conduce a problemas en el momento de cumplir con los requisitos legales en materia de seguridad de la información.

Es un problema grave para las pequeñas y medianas empresas. Por lo general, los administradores de sistemas prestan servicios en varias empresas a la vez o tienen bajo nivel de cualificación. El descenso de la dependencia de la empresa en estos factores es un problema importante para los gerentes.

Software como un servicio (Software as a service)

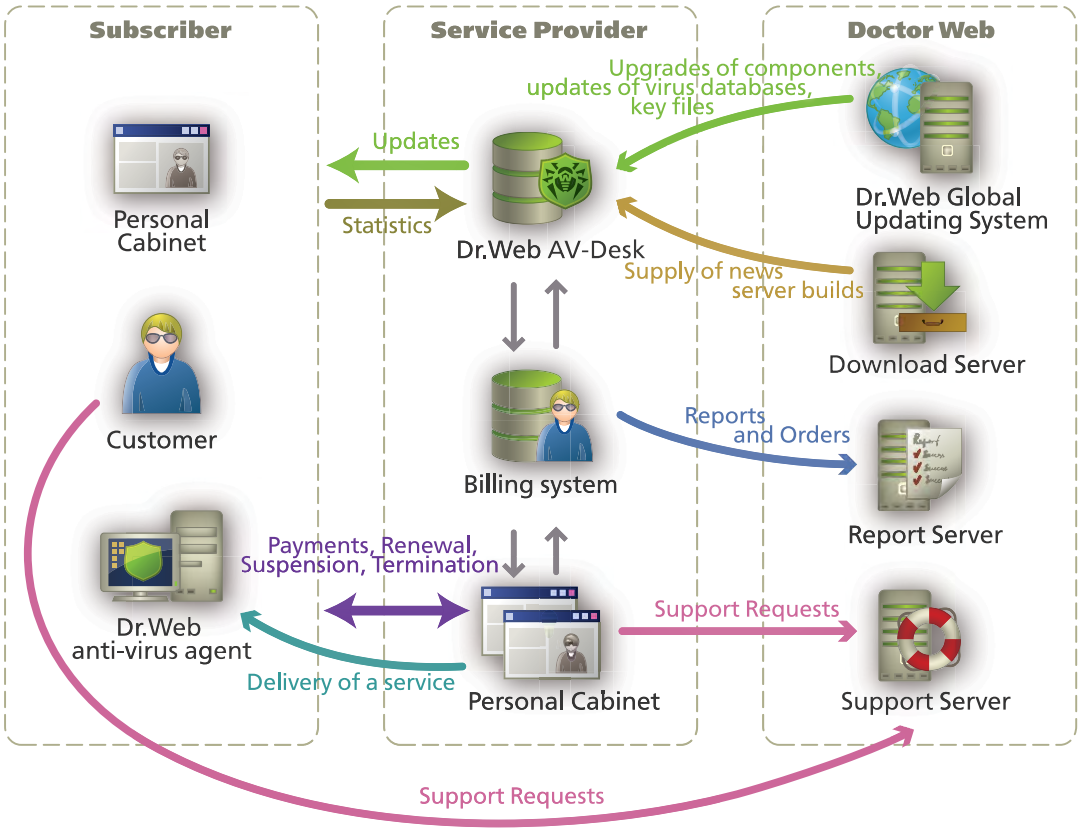
El software as a service (SaaS) es un modelo difundido ampliamente fuera de Rusia para abastecer el software como un servicio.

Hasta el año 2007 su uso en la industria antivirus de Rusia fue obstaculizado por la falta de soluciones nacionales de clase similar. Cuando fue lanzado en mayo de 2007 el servicio de Internet Dr.Web AV-Desk, desarrollado por la compañía rusa Doctor Web, en el mercado de servicios de TI en Rusia, surgió un nuevo segmento - segmento de servicios de la protección antivirus.

Los proveedores de estos servicios son los proveedores de servicios de TI, que han instalado el servicio de Internet Dr.Web AV-Desk, por medio del cual proporcionan los servicios de protección de empresas contra las amenazas de Internet - el servicio Antivirus Dr.Web.

¿Cómo funciona?

1. El proveedor de servicios Antivirus Dr.Web instala el software de servicio de Internet Dr.Web AV-Desk en sus servidores y organiza la suscripción al servicio Antivirus Dr.Web.
2. Los clientes se suscriben, instalan el software Dr.Web, e independientemente administran las configuraciones de la suscripción.
3. Doctor Web proporciona al proveedor de servicios las actualizaciones oportunas de las bases de datos del virus y los módulos de programa Dr.Web, presta apoyo técnico a los proveedores y los suscriptores al servicio.
4. El proveedor cobra a los clientes una cuota por utilizar el servicio, monitoriza el estado de la red antivirus, suministra a los suscriptores las actualizaciones de bases de datos, recopila información estadística sobre las infecciones virus.



Si la empresa no cuenta con un administrador del sistema de plantilla

Para resolver el problema de suministrar la seguridad efectiva en las condiciones de falta de administradores de sistemas calificados se puede mediante el uso de antivirus Dr.Web como un servicio a través del proveedor de servicios de TI.

- Su empresa tendrá administración calificada del proceso de protección de la información.
- Los especialistas del proveedor de servicios son profesionales certificados por Doctor Web que tienen pleno conocimiento del producto gestionado y utilizan estos conocimientos para la gestión de la protección de la información.
- Para hacer cumplir estrictamente las políticas de seguridad en todos los objetos protegidos de la empresa se restringe parcialmente la capacidad del personal para intervenir en los ajustes o se establece una prohibición total de hacer los cambios.
- Gracias a la gestión calificada de servicios, la respuesta competente a las amenazas de virus y acciones profesionales del proveedor para restaurar la operatividad de la red después de un ataque virus, los gastos imprevistos se reducen al mínimo, en particular, debido a la ausencia de gastos en el hardware del servidor y en la contratación de profesionales altamente retribuidos en el área de seguridad de la información.

La administración externa del servicio Antivirus Dr.Web es una garantía de alta fiabilidad de la infraestructura de TI y análisis imparcial del estado virus de la red de la empresa.

Sistema de protección antivirus Dr.Web

Componentes del sistema de protección antivirus

Ilusión №8

La gestión centralizada del sistema de protección antivirus

Si su empresa cuenta con un administrador del sistema de plantilla o a tiempo parcial, el proveedor de servicios puede entregarle funciones de control del sistema de protección antivirus a través del Centro de Control. Esto proveerá a la empresa con más posibilidades de gestión de la protección de información de la red antivirus.

Productos de clase empresarial con el centro de control valen más caro que las versiones monousuarias. Su manejo es extremadamente complicado, que requiere la presencia de un especialista en seguridad de la información.

Hechos

El suministro de productos de servidor Dr.Web de clase empresarial bajo el modelo SaaS ha reducido significativamente el costo de estos productos y los hizo disponible a los consumidores. El centro de control como parte del servicio Antivirus Dr.Web:

1. Está licenciado de forma gratuita.
2. Lo podrá gestionar el especialista de cualquier calificación.
3. Automatiza al máximo el trabajo de protección de la red local con los gastos mínimos en acompañamiento, debido a que los ajustes para todas las estaciones o grupos de estaciones se producen en 2-3 clics y con la misma facilidad se puede cambiarlos, si es necesario.

Las opciones del Centro de control del servicio Antivirus Dr.Web contribuye a un buen funcionamiento de la empresa y como resultado reduce al mínimo el costo de los procedimientos empresariales.

El centro de control como parte del servicio Antivirus Dr.Web le permite gestionar la protección de:

- estaciones de trabajo bajo Windows y OS X,
- servidores de archivos Windows,
- dispositivos móviles Android.

Comodidad y ahorro real

- El centro de control del servicio Antivirus Dr.Web es la capacidad de "ver de arriba" toda la red antivirus de la compañía de cualquier tamaño, desde un solo lugar.
- El Centro de control minimiza el tiempo de mantenimiento del sistema, permite gestionar de forma rápida el sistema de seguridad de la red local en cualquier momento, desde cualquier parte del mundo a partir, desde el ordenador bajo cualquier sistema operativo a través del navegador, sin necesidad de instalar un software adicional.
- La disponibilidad de una interfaz web cómoda le permite instalar de forma centralizada, actualizar y configurar los componentes del sistema de protección antivirus, iniciar los ordenadores en el modo "móvil".
- Al utilizarlo se reduce la carga en las estaciones locales mediante la compresión de tráfico de red y el cifrado de datos - los que comenzarán a funcionar más productivamente, desaparecerán quejas de mal funcionamiento de antivirus.

Garantía de un alto nivel de seguridad de la información

La gestión centralizada del sistema de protección antivirus como parte del servicio Antivirus Dr.Web permite:

- implementar políticas de seguridad necesarias para una compañía determinada - sin tener que configurar la seguridad en cada estación de trabajo;
- garantizar que el personal no tendrá capacidad para desactivar el antivirus o sus componentes individuales, lo que inevitablemente conducirá a un nivel bajo de la protección;
- garantizar el rendimiento de antivirus con las configuraciones que ha establecido el administrador de la red;
- planificar y ejecutar de forma remota escaneos periódicos llevados a cabo por el administrador, o según el horario;
- controlar la regularidad de actualizaciones y la incapacidad de su desactivación;
- recopilar y analizar información sobre el estado del sistema de protección antivirus, así como preparar informes por el período de tiempo requerido;
- notificar a los administradores y usuarios sobre el estado del sistema de protección;
- responder rápidamente a los problemas emergentes de la naturaleza viral, lo que, a su vez, reduce el riesgo de infección de la red y las pérdidas financieras debido a la inactividad de los trabajadores, la pérdida de datos, desconexión de Internet, contaminación de los socios.

¡Atención!

- Incapacidad de capturar el tráfico y sustituirlo proporciona una administración segura de cualquier número de estaciones de trabajo, no importa en qué lugar del mundo se encuentran.

Servidor proxy

El servicio Antivirus Dr.Web puede ser proporcionado incluso en el caso de uso de una topología compleja de red, por ejemplo, si los agentes antivirus no tienen acceso directo al servidor de servicios (servidor Dr.Web AV-Desk), y entre ellos no hay enrutamiento de paquetes (la LAN interna aislada lógicamente de Internet).

Para la organización del acceso directo en este caso se ofrece un componente separado de la red antivirus - el servidor proxy. El servidor proxy también puede utilizarse para reducir el tráfico de red (optimización de tráfico) y reducir el tiempo necesario para obtener actualizaciones, porque soporta caché de actualizaciones y componentes de agentes antivirus.

El uso de tecnología de compresión de tráfico (es una opción en el servidor del servicio) no es un obstáculo para usar el servidor proxy. El procesamiento de la información transferida se realiza independientemente de si el tráfico está comprimido o no.

¡Atención!

La red antivirus puede incluir uno o más servidores proxy.

Instalación en la red (instalación remota)

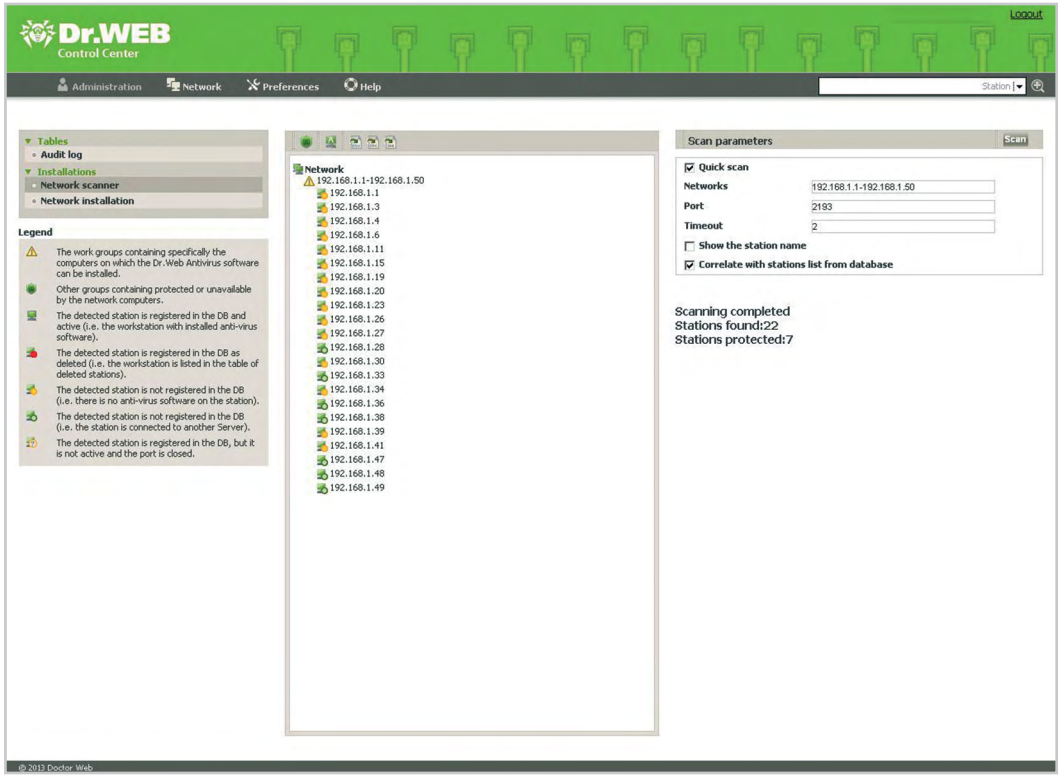
El servicio Antivirus Dr.Web tiene todas las ventajas de productos de clase empresarial con la gestión centralizada del sistema de protección antivirus. Una de estas ventajas es la capacidad de identificar los equipos dentro de la red local, donde no hay protección antivirus, así como la posibilidad de instalar de forma remota Dr.Web en los equipos sin protección.

La instalación remota es posible, tanto si la estación de trabajo entra al dominio bajo una cuenta de administrador, como si la estación remota no entra al dominio o se utiliza una cuenta local.

¡Atención!

Si la estación remota no entra al dominio o se utiliza una cuenta local en el equipo remoto, algunas versiones de los sistemas operativos MS Windows requieren una serie de ajustes. Esto se describe en la Guía del administrador.

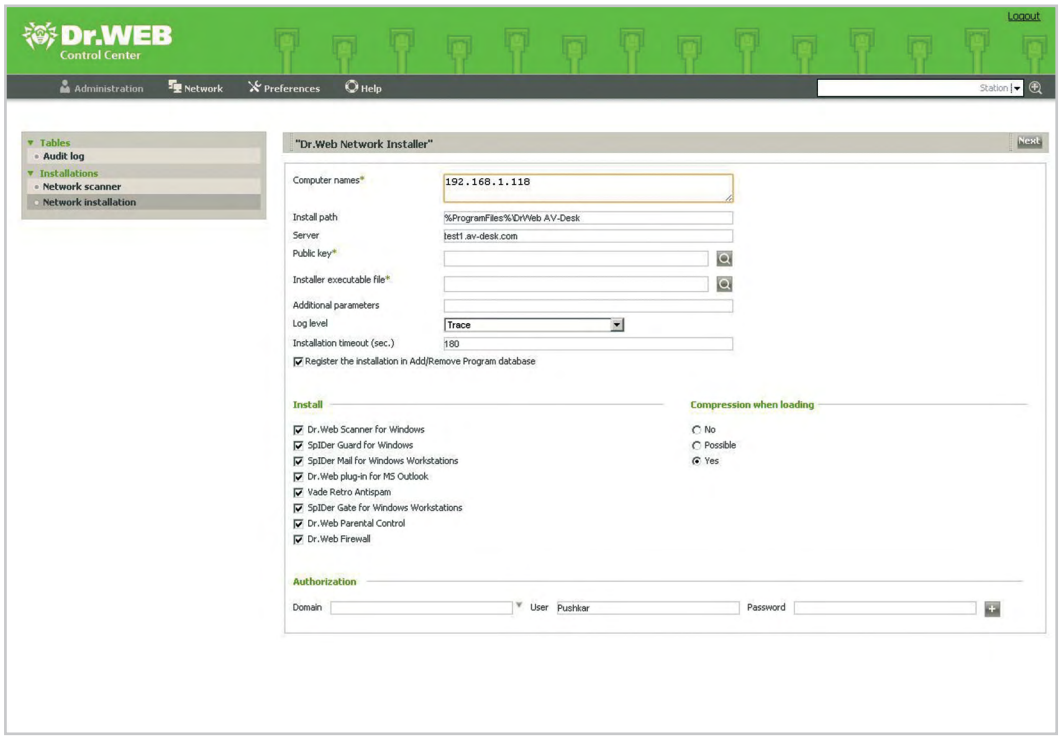
El centro de control del servicio Antivirus Dr.Web incluye escáner de red que busca ordenadores por las direcciones IP en la red local, cuyo resultado es una lista jerárquica de los ordenadores, indicando en cuál de ellos está instalado el software antivirus, y en el cuál no está.



La instalación puede llevarse a cabo en uno o varios equipos sin protección mediante la preparación de una tarea correspondiente en la barra de herramientas.

¡Atención!

La instalación remota puede ser ESTRICTAMENTE en redes enrutadas.



Los administradores de sistema

Si la empresa cuenta con un administrador de sistemas a tiempo completo, o utiliza los servicios de administrador temporero, el administrador puede gestionar el sistema de protección antivirus Dr.Web través del Centro de control cómodo y fácil de utilizar, tomar sus propias decisiones e implementar soluciones en el cumplimiento de políticas de seguridad, responder rápidamente a los incidentes vinculados con virus, es decir, tener toda la influencia en la seguridad de información de la compañía.

Tipos de Administradores

- **Administrador de grupos con plenos permisos** - el empleado tiene acceso al Centro de control y puede manejar la configuración del sistema. Por lo tanto, se recomienda asignar gerente de la empresa (si la empresa es pequeña, no tiene un administrador del sistema y el jefe combina la función del control del sistema de protección antivirus), o administrador del sistema autorizado para administrar el sistema de protección antivirus.

¡Atención!

Si una empresa utiliza los servicios de un administrador temporero, es necesario considerar cuidadosamente si se le puede delegar en este volumen la gestión del sistema de protección antivirus, ya que dicha función proporciona el control total sobre el sistema.

- **Administrador de grupos con plenos permisos (sólo lectura)** - el empleado tiene acceso al Centro de Control, puede obtener estadísticas del sistema, pero no puede cambiar nada en las configuraciones. Esta función se puede asignar al funcionario autorizado para llevar a cabo el análisis estadístico del sistema y llevar a cabo auditorías de sistema de seguridad.
- **Administrador de grupos con derechos restringidos** - el empleado tiene acceso al Centro de control y puede manejar cualquier ajuste dentro de los permisos establecidos por el administrador de grupos con plenos permisos, con excepción de gestión de suscripciones (crear /suspender / renovar /eliminar). Esta función es útil 1) para los clientes de proveedores de servicio Antivirus Dr.Web en el outsourcing y 2) para los administradores de proveedores de acceso a los suscriptores. Si hay varios grupos, a cada grupo se le puede asignar un administrador particular.

¡Atención!

Para asignar un administrador del sistema se debe tener acceso a la funcionalidad apropiada - recurra a su proveedor de servicios.

Grupos Gestión de grupos

En las empresas medianas y grandes para facilitar la gestión de la seguridad se utiliza el mecanismo de agrupación que abastece para el servicio Antivirus Dr.Web una escalabilidad excepcional. Agrupación permite:

- crear grupos, unificar las estaciones protegidas en grupos, añadir/ quitar estaciones del grupo;
- utilizar diferentes políticas de seguridad para los diferentes grupos (suponemos que para el grupo de Contabilidad puede ser asignada la tarea de prohibir la cancelación de actualizaciones, y para el grupo de Administradores pueden no ser asignadas severas restricciones en el uso de Internet);
- especificar con un solo comando las tareas para todas las estaciones protegidas del grupo, así como iniciar la ejecución de las tareas en ellas;
- establecer para los diferentes grupos los horarios individuales de actualizaciones y escaneos, lo que permitirá distribuir la carga en la red;
- elaborar informes sobre los grupos;
- enviar alertas - a las estaciones individuales, grupos separados o todos los grupos.

Si la empresa tiene más de 15 suscripciones para el servicio Antivirus Dr.Web, tiene sentido para crear grupos en el sistema de protección antivirus y aplicar diferentes políticas de seguridad a estos grupos utilizando múltiples configuraciones del Centro de control.

El administrador del sistema tiene la capacidad de ampliar o limitar los permisos de gestión de los agentes - a los usuarios individuales, grupos de usuarios o todos los grupos de usuarios:

- permitir cambiar la configuración;
- restringir parcialmente la capacidad de cambiar la configuración;
- prohibir completamente cambiar la configuración;
- gestionar el conjunto de componentes Dr.Web, instalado en los ordenadores de los usuarios;
- instalar/desinstalar componentes en los PCs de los usuarios;
- ejecutar las tareas en las estaciones protegidas;
- actualizar bajo obligación los agentes que no han sido actualizados;
- ejecutar bajo obligación las sesiones de escaneo en las estaciones protegidas en segundo plano.

Tarifas de servicios y componentes de protección Dr.Web

La suscripción al servicio se realiza en forma de paquetes de tarifas. La composición de cada paquete de suscripción incluye componentes para proteger estaciones de trabajo, servidores de archivos Windows y los dispositivos móviles.

Elija paquetes de tarifas según las necesidades operativas reales, los requisitos para la seguridad de la información y la situación financiera actual de la empresa.

	Dr.Web Classic La protección mínima necesaria contra los virus	Dr.Web Premium Protección completa contra amenazas de Internet
Protección de estaciones de trabajo		
Windows	8/7/Vista/XP/2000 SP4	
OS X	10.4 y superior	
Antivirus, antispyware, antirootkit	✔	✔
Antispam		✔
Web antivirus		✔
Control Paterno		✔
Firewall	✔	✔
Protección de servidores de archivos		
Windows		Windows Server 2003/2008
Todos los componentes de protección Dr.Web Premium	✔	
Protección de dispositivos móviles		
Android		2.0/2.1/2.2/2.3/ 3.0/3.1/3.2/4.0/4.1/4.2
Antivirus	✔	✔
Antirrobo		✔
Antispam		✔
Soporte técnico básico		
Actualizaciones de las bases de datos de virus	✔	✔
Actualizaciones de módulos de software Dr.Web	✔	✔
Número de consultas al soporte técnico	Ilimitado	
Otros servicios		
Cambio gratuito por otro paquete de tarifas	✔	✔
Suspensión de suscripción (por 1, 2 o 3 meses)	✔	✔

¿De qué amenazas protege el servicio Antivirus Dr.Web?

	Dr.Web Classic	Dr.Web Premium
Virus	✔	✔
Troyanos	✔	✔
Keyloggers	✔	✔
Programas - ladrones de contraseñas	✔	✔
Spyware	✔	✔
Rootkits	✔	✔
Software potencialmente peligroso (Riskware)	✔	✔
Los virus polimórficos	✔	✔
Gusanos de correo	✔	✔
Dialers	✔	✔
Bromas	✔	✔
Programas dialers pagados	✔	✔
Utilidades de los hackers	✔	✔
Spam		✔
Phishing		✔
Pharming		✔
Scamming		✔
Spam técnico		✔
Robo de información confidencial		✔
La delincuencia cibernética dirigida contra los niños		✔
Acceso no autorizado a la red	✔	✔

¡Hoy en día sólo antivirus no es la panacea!

¿Porqué sólo antivirus no es suficiente? ¡Pero recientemente no fue así!

¡Atención!

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

El sistema de protección antivirus moderno, entre otras cosas, debe incluir:

- antispam eficaz, debido a que el spam es uno de los principales portadores de malware;
- filtrado de tráfico HTTP para proteger contra la penetración de código malicioso desde las páginas Web;
- sistema para restringir el acceso a medios extraíbles y recursos de la intranet (control de oficina);
- firewall personal.

¡Atención!

Esta funcionalidad sólo está disponible en el paquete Dr.Web Premium.

Cuando se usan correctamente dichos componentes (según las recomendaciones de este folleto) se excluye la necesidad de comprar productos adicionales con capacidades similares. Esto le permite implementar el sistema de protección antivirus contando con un presupuesto limitado.

Mejores prácticas

- Al configurar el acceso de los usuarios a los componentes del Centro de control, guarde los permisos para poner en marcha cada uno de los componentes, y deshabilite la edición de la configuración de los componentes, así como su detención.
- La opinión de los usuarios acerca de que componentes de sistema de protección antivirus deben instalarse en su PC, debe ser IGNORADA.

Usted paga sólo por lo que está usando

"Pagar sólo por lo que se necesita en el momento" es un principio fundamental de la filosofía del servicio de licenciamiento, que es capaz de adaptarse a las necesidades de las empresas a pagar sólo por el volumen necesario de servicios en el momento. **Se abona sólo por el número real de las suscripciones, donde la cantidad puede cambiar de forma flexible tanto hacia arriba como hacia abajo**.

Esto permite la planificación más precisa de los gastos en seguridad de la información en el corto y largo plazos, basándose en las necesidades reales del negocio, elimina los costos crecientes impredecibles y da una comprensión completa de los posibles costes futuros en la protección de la información.

Ventajas del licenciamiento de servicio Antivirus Dr.Web

- Tarificación a partir de 1 mes. Pague sólo por el número real de suscripciones en el ejercicio fiscal.
- La conexión de las nuevas estaciones se produce de inmediato.
- A medida que el número de personal se reduce, se produce la desconexión de las estaciones de servicio no necesarias.

Haga la reducción de los gastos en la seguridad de información cuando no son necesarios, y auméntelos en la medida de una necesidad de negocio real.

Descuentos

Al suscribirse al servicio Antivirus Dr.Web, empiezas a ahorrar en seguridad de la información desde el primer mes de uso.

Suscríbase al servicio y obtenga descuentos ....

por el número de objetos protegidos...

de 10 a 40% - en función del número de objetos protegidos a los que se ha suscrito

Cantidad de PC	Descuento, %
1–25	Precio básico de la tarifa
26–50	10
51–100	20
101–200	25
201–300	30
301–400	35
401–500	40

... y por el período de uso del servicio

del 5 al 15% - un descuento extra especial para los que utilizan el servicio de forma continua*

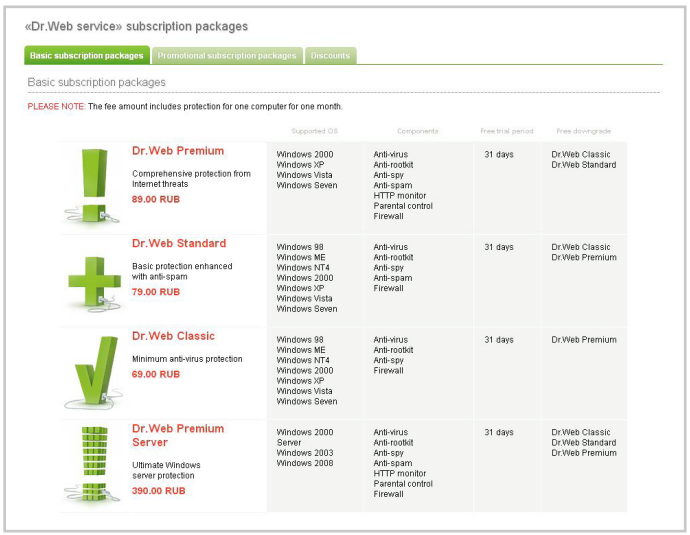
El período de suscripción	Descuento, %
1 año	5
3 años	10
5 años	15

** Sin suspender o cancelar la suscripción. Se establece a partir de 13, 37 y 61 meses, respectivamente.*

Licenciamiento del servicio flexible es la clave para el ahorro de costes en la seguridad de información.

Centro de Control de Suscripciones (CCS)

El proveedor de servicios habilita al cliente el acceso al Centro de control de suscripción. CCS permite al cliente controlar el proceso de suscripción y su extensión, pasar a otros paquetes de tarifas, recibir estadísticas de virus y estadísticas de servicio, recibir noticias de la compañía Doctor Web en tiempo real, ponerse en contacto con el soporte técnico.

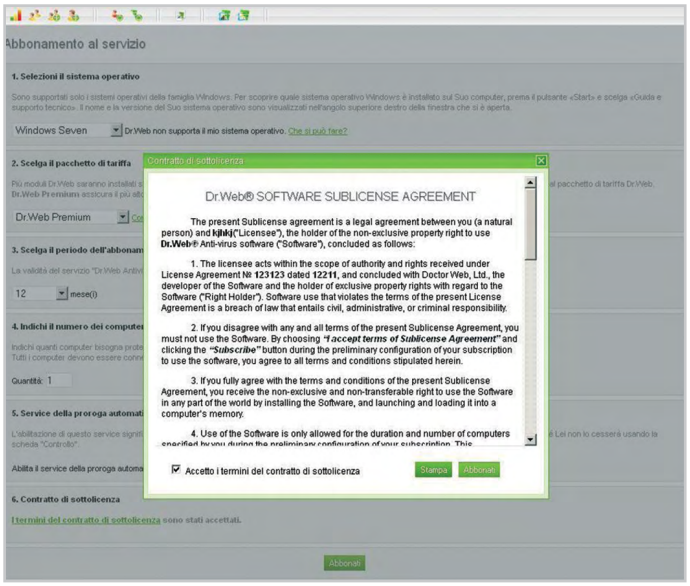


Suscripción

A través del Centro de control de suscripción en cualquier momento se puede conectar al servicio nuevas estaciones (para ampliar la licencia) o desactivar estaciones innecesarias, cuando se presente la necesidad.

Para suscribirse, usted debe:

1. Especificar el sistema operativo.
2. Eligir el paquete de tarifas.
3. Especificar el número de PC.
4. Especificar el periodo de suscripción (un mes mínimo).
5. Aceptar los términos del acuerdo de sublicencia.
6. Hacer clic en el botón Suscribirse.



¡Atención!

Al marcar el icono "Servicio de renovación automática está activado", la suscripción se renovará automáticamente cada mes.

Instalación del software en una estación separada

El enlace al paquete de instalación Dr.Web está disponible en CCS inmediatamente después de suscribirse. Es necesario descargar el paquete de instalación, ejecutarlo y esperar a que se acabe la instalación Dr.Web. Al terminar la instalación en la esquina inferior derecha de la pantalla aparecerá un icono verde con una araña en el escudo, en el cual estará parpadeando un triángulo amarillo con un signo de exclamación. Es necesario reiniciar el ordenador y esperar a que se establezca la conexión con el servidor antivirus - el proceso de conexión con el servicio está completado.

¡Atención!

1. Antes de instalar, es necesario asegurarse de que el PC no tiene otros programas antivirus, ya que los módulos residentes en su composición pueden ocasionar conflictos de incompatibilidad de distinto software.

1. Sistema de protección antivirus Dr.Web comienza a funcionar después de la instalación de software del servicio Antivirus Dr.Web.

Renovación

No se debe preocuparse por el tema de renovación. La renovación de los servicios se realiza de forma automática, si está activada la opción "Servicio de renovación automática está activado".

Suspensión de la suscripción

Si es necesario, en cualquier momento se puede suspender la suscripción - por un plazo hasta 3 meses.

Para dejar de recibir dichos servicios, en la pestaña "Administación" seleccione "Suspender la suscripción".

¡Atención!

En el caso de suspensión de la suscripción, usted pierde el derecho a descuentos que se acumulan por el periodo de uso de los servicios (véase sección **Descuentos**).

Comienzo de la suspensión

- En el caso de la tarificación diaria - desde la fecha de suspensión.
- En el caso de la tarificación mensual - desde el primer día del próximo mes calendario.

Expiración de la suspensión

- Después de expirar el período predeterminado de suspensión. Se activa simultáneamente el servicio de renovación automática, si ha sido activado antes de la suspensión de la suscripción.

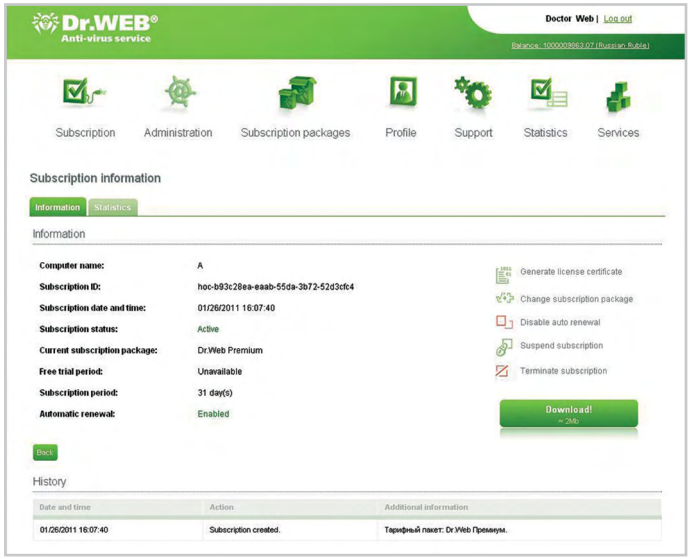
Renovación automática de suscripción después de la suspensión

Se produce en el caso de que el servicio de renovación automática fue activado antes de la fecha de suspender la suscripción. La suscripción se renueva en las mismas condiciones que estaban en vigor antes de la fecha de suspensión.

Suspensión de la suscripción

En cualquier momento, se puede dar de baja del servicio. Al mismo tiempo:

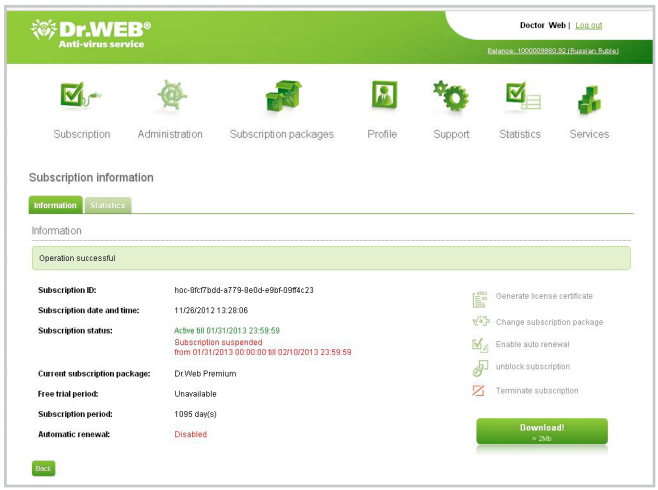
- en el caso de la tarificación diaria, la suscripción se finaliza de inmediato;
- en el caso de la tarificación mensual la suscripción sigue vigente hasta el final del mes en curso. Los recursos pagados por adelantado y no gastados en el momento de la terminación de la suscripción no son reembolsables.



Para detener la suscripción en la pestaña “Administración” seleccione “Darse de baja”.

Reanudación manual de la suscripción después de darse de baja

La suscripción se reanuda después de seleccionar “Reanudar la suscripción”, el enlace para descargar el archivo Dr.Web volverá a estar disponible. De hecho, es una nueva suscripción. Se activa simultáneamente el servicio de renovación automática, si ha sido activado antes de la suspensión de la suscripción.



En la ficha Administrar, seleccione Renovar suscripción.

El certificado licenciado en línea

En el Centro de control de la suscripción se puede obtener el certificado de licencia Dr.Web y confirmar la presencia de licencia para el software Dr.Web.

Estadística

Centro de control de suscripción proporciona una variedad de informes acerca del rendimiento de Dr.Web en estaciones de trabajo protegidas. El funcionamiento de software se hace transparente para el usuario.

La información sobre los parámetros de cada suscripción y grupo de suscripciones está disponible, así como los datos acerca de todas las suscripciones. En cualquier momento (incluso cuando se suspende la suscripción), se puede revisar el estado de la suscripción, la información sobre cada suscripción o todas las suscripciones, la dinámica del uso de las suscripciones (según grupos y tarifas).

Estadísticas de virus

Información sobre cómo el antivirus Dr.Web protege las estaciones de trabajo — estadísticas sobre virus y malware detectados por Dr.Web — se puede encontrar en los cuadros e índices en la pestaña "Estadísticas".

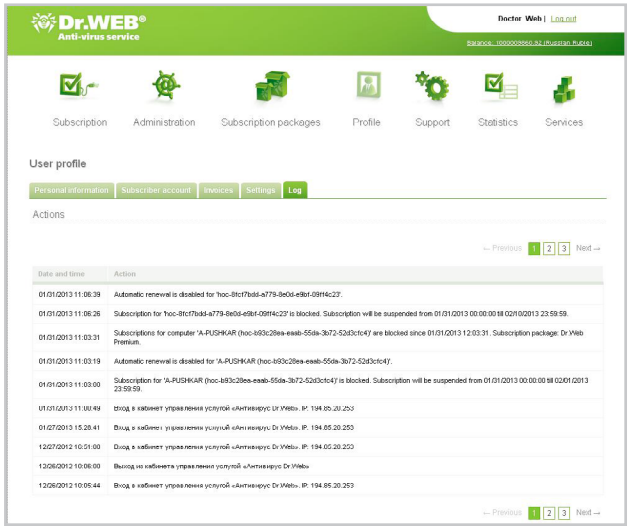
Para cada estación por cualquier período (configurable) se muestran:

- un resumen de objetos maliciosos detectados por el antivirus Dr.Web;
- los diez virus más frecuentemente detectados.

Registro de actividades

El registro contiene la información integral (historial) sobre las actividades del cliente en el Centro de suscripciones:

- actividades en el mes en curso por cada suscripción y por todas las suscripciones (suscripciones, cancelación, suspensión, ingreso en la cuenta, etc.)
- actividades con la cuenta personal del cliente en el mes en curso (recarga, carga, y reembolso).



Sistema de protección antivirus Dr.Web

Política de seguridad de información

Creación de una ecosistemas única de protección

Como muestra la práctica, las estaciones de trabajo 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, los virus pueden penetrar en los equipos de diferentes maneras - desde las tarjetas flash de los usuarios, desde los archivos protegidos por contraseña, que se adjuntan a los mensajes de correo electrónico y, por lo tanto, evitan el escaneo en el servidor, desde los sitios infectados a los que los usuarios han entrado apretando los enlaces en los correos desconocidos.

De acuerdo con las normas existentes el sistema de protección antivirus de cada estación de trabajo debe incluir un antivirus eficaz y un sistema para limitar el acceso a los recursos locales con el fin de evitar los casos de acceso intencional o inadvertida a los datos e intervención en el buen funcionamiento del sistema.

Uno ilusión común es que, debido al número relativamente pequeño de programas maliciosos que se ejecutan bajo sistemas operativos como Linux y Unix, es necesario proteger solamente estaciones de trabajo y servidores que se ejecutan 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 en la red.

¡Atención!

El centro de control del servicio Antivirus Dr.Web permite controlar de forma centralizada el sistema de protección antivirus de cualquier número de estaciones de trabajo bajo Windows y OS X.

Objetivo №2

Protección del servidor de archivos

Amenaza

Normalmente, las organizaciones sólo protegen los ordenadores de los empleados, dejando sin protección los servidores, dispositivos móviles y los ordenadores personales de los empleados. Como resultado un virus penetrado en las estaciones de trabajo aparece fácilmente en los servidores que contienen información importante.

¿Por qué es importante proteger los servidores?

- El usuario puede infectar el servidor con un virus desconocido en el momento de la infección (llevándolo o iniciándolo desde el almacenamiento). El antivirus instalado lo intercepta de inmediato, basándose en mecanismos heurísticos. En el último caso va a tratar el virus durante la próxima actualización.
- El servidor puede ser hackeado. El software antivirus instalado no lo permitirá: va a monitorear y destruir los programas maliciosos. 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).
- El mundo moderno está filtrado por las tecnologías digitales. 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 los servidores de Internet. Utilizar sus unidades de memoria flash y las de amigos y colegas. Estos pueden tener virus.
- Los teléfonos celulares modernos por sus capacidades y vulnerabilidades pueden ser comparados con los ordenadores - allí se utilizan los sistemas operativos y aplicaciones que también pueden estar infectados. Desde los que pueden penetrar los virus a la red corporativa y acceder al servidor.

Mejores prácticas

Si su empresa dispone de un servidor de archivos asignado, el mismo también debe ser protegido.

Solución

Para proteger el servidor de archivos se puede adquirir el paquete de tarifas Dr.Web Premium, que soporta Microsoft Windows 2003/2008.

La protección del servidor en el marco del servicio Antivirus Dr.Web tendrá el mismo precio que la protección de las estaciones, a diferencia de los productos antivirus de servidor comunes costosos. Es una de las numerosas ventajas del servicio.

¡Atención!

El centro de control del servicio Antivirus Dr.Web permite controlar de forma centralizada el sistema de protección antivirus de cualquier número de servidores de archivo bajo Windows.

Protección de los dispositivos personales de los empleados

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. Empleados entusiasmados trabajan no sólo en horario común, y no sólo en la oficina, sino también en el camino y en la casa. A menudo sacrifican horas de descanso, permaneciendo todo el tiempo en contacto. Y el negocio aprovecha estos cambios con agrado. También, muchas empresas emplean con éxito los trabajadores de forma remota - es un ahorro sustancial.

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

- 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.

En los intereses 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.

Para lo cual, las empresas necesitan una herramienta para asegurar:

- la protección de cualquier información en los dispositivos de los usuarios;
- incapacidad para expandir los virus y troyanos desde los dispositivos de usuarios;
- protección para todo tipo de dispositivos, incluyendo móviles - incluso un dispositivo sin protección es una escapatoria para los cibercriminales.

¡Sin embargo, los empleados utilizan los dispositivos para fines personales!

De esta manera, se puede permitir que su hijo trabaje en el ordenador portátil, pasar la noche navegando en la red social infectada con virus, descargar e instalar un archivo de música desde un sitio sospechoso ... ¿Dónde está la seguridad de datos de la empresa?

Utilizando el servicio Antivirus Dr.Web se puede hacer casi lo imposible - proteger cualquier dispositivo de tal modo que sea ventajoso para todos - tanto para la empresa como para sus empleados.

Mejores prácticas

- Se les recomienda obtener la suscripción del servicio Antivirus Dr.Web para los dispositivos personales de sus empleados, entonces todos los equipos que tienen acceso a la red local de su empresa estarán protegidos por un solo productor.
- Mediante el Centro de control del servicio asegúrese del cumplimiento de las políticas de seguridad de la información de su empresa y dispositivos personales de los empleados, incluyendo la imposibilidad de desactivar la actualización, escaneos programados y eliminación de los componentes de protección individuales.
- La opinión del empleado acerca de qué antivirus debe estar instalado en su dispositivo personal debe IGNORARSE - siempre que el dispositivo forme parte de la red corporativa. De lo contrario, dicho dispositivo debe ser anunciado “no confiable”, y no debe tener acceso a la red.

Sólo respetando dichas condiciones se puede garantizar que nada malicioso penetre en la red desde los ordenadores personales de los empleados.

Ventajas para la empresa

- Lealtad de los empleados. ¡El antivirus de regalo es una gran bonificación!
- Abaratamiento de la organización de protección.
- Capacidad de controlar las máquinas protegidas desde un único lugar.
- Capacidad de trabajar en cualquier parte del mundo bajo la misma protección.
- Seguridad de datos garantizada (incluyendo los datos personales) en cualquier momento.
- Reducción del tiempo de inactividad debido a la infección.

Los empleados han ido mucho más allá de los límites de protección y hacer volverlos dentro de sus límites ya no es posible. Tampoco tiene sentido. Lo más lógico es ampliar los límites de la oficina e incluir el espacio privado de cada empleado.

Protección de los dispositivos móviles corporativos y personales de los empleados

Actualmente los dispositivos más comunes están operando bajo el sistema operativo Android.

Amenazas

- La cantidad de amenazas para OS Android crece a un ritmo desastroso junto con el aumento del número de dispositivos que se utilizan.
- Ya existen troyanos bancarios bajo Android.
- Los dispositivos móviles corren gran riesgo de pérdida/robo. La información (incluyendo contraseñas y nombres de usuario a los recursos corporativos) no siempre puede caer en manos amistosas.

Objetivo №3

Solución

El paquete de tarifas Dr.Web Premium incluye una suscripción gratuita para Dr.Web para Android. El sistema incluye los siguientes componentes de protección:

- **Antivirus** no dejará 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.
- **Antirrobo** es el sistema de protección para prevenir la pérdida del dispositivo móvil. Si el dispositivo se pierde o es robado, se puede borrar de forma remota todos los datos.
- **Antispam** – protección contra los mensajes y las llamadas no deseadas, así como de mensajes troyanos devastadores.

¡Atención!

Centro de control del servicio Antivirus Dr.Web le permite gestionar de forma centralizada el sistema de protección antivirus de cualquier número de dispositivos móviles bajo el sistema operativo Android (a partir de la versión 6.2).

Actualizaciones regulares de la base de datos de virus y módulos de programa

Amenaza

Antivirus cuyas actualizaciones pueden ser apagados por los usuarios o realizarse de vez en cuando, no es capaz de proteger de forma fiable.

Hechos

- La base de datos de virus Dr.Web se actualiza varias veces al día.
- Todos los días el laboratorio antivirus Doctor Web agrega a la base de datos de virus unas 200 entradas nuevas, lo que permite detectar la mayoría de las amenazas recibidas para el análisis.
- Actualizaciones "calientes" se emiten inmediatamente después de un nuevo análisis de amenazas de virus.
- Antes de lanzar la actualización, se lleva a cabo la prueba en un gran número de archivos limpios para evitar los falsos positivos.
- Las actualizaciones se envían a los usuarios desde varios servidores ubicados en diferentes partes del mundo.

Mejores prácticas

- Para asegurar la **relevancia** y la **integridad** del sistema de protección antivirus, es necesario **oportunamente** realizar todas las actualizaciones de las bases de datos de virus y módulos de aplicación del antivirus.
- La opinión del usuario acerca de la cancelación de reinicio debido a la actualización del sistema de protección antivirus debe ser IGNORADA.
- La tarea de proporcionar actualizaciones periódicas y el estado actual de protección de los componentes mediante el sistema de protección antivirus sólo puede llevarse a cabo por medio de control **centralizado**.
- El monitoreo de las actualizaciones debe ser DIARIO - es posible que aparezcan los virus capaces de deshabilitar la actualización, o bloquear el acceso al servidor de actualizaciones.

¡Atención!

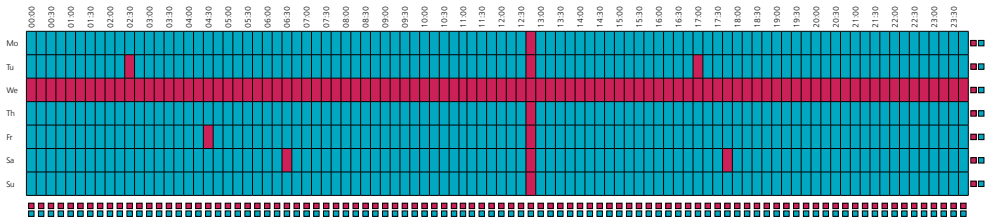
Ningún software requiere una actualización frecuente como antivirus. Los nuevos virus están elaborándose constantemente, y la base de datos de virus se actualiza con una frecuencia muy alta.

¡En cualquier caso, no desactive la actualización automática!

Solución

Al ejecutar ajustes sólo dos o tres veces en el centro de control del servicio Antivirus Dr.Web, le permite excluir la posibilidad de cancelar actualizaciones en las estaciones de trabajo por el empleado, desconectar de la red el agente no actualizado, prevenir epidemias dentro y fuera de la red local, así como:

- 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;
- distribuir la configuración de actualizaciones de una estación a otra, o a todo un grupo o grupos.

Actualización de «agentes móviles»

Amenaza

Solamente un ordenador, aunque tuviera una licencia antivirus, pero el que no se actualiza regularmente, representa un peligro potencial para toda la red local. Inclusive en este ordenador puede estar instalada la banca electrónica ....

Solución

Si el portátil durante mucho tiempo no se encuentra dentro de la red local, seleccione el modo móvil del agente para comunicarse con el servidor para recibir actualizaciones. El modo móvil del agente de servicio Antivirus Dr.Web le permite recibir actualizaciones, incluso fuera de la red de la empresa, lo cual es especialmente oportuno para el personal en comisión de servicios.

Objetivo №5

Escaneos regulares de las estaciones de trabajo

Amenazas

- 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.
- El análisis del escáner se realiza en una profundidad mayor que el análisis de monitor de archivos de fondo - es por eso que a veces ocurre que el escáner detecta virus que no los ve el monitor de archivos

Mejores prácticas

- Los escaneos deben realizarse al menos una vez a la semana.
- Carpeta de cuarentena que recibe objetos sospechosos también debe ser escaneada con regularidad, por lo que puede contener los virus previamente desconocidos, o archivos desplazados como resultado de falsos positivos del antivirus.
- La opinión del personal de la frecuencia con que es necesario realizar los escaneos periódicos, debe ser IGNORADA.

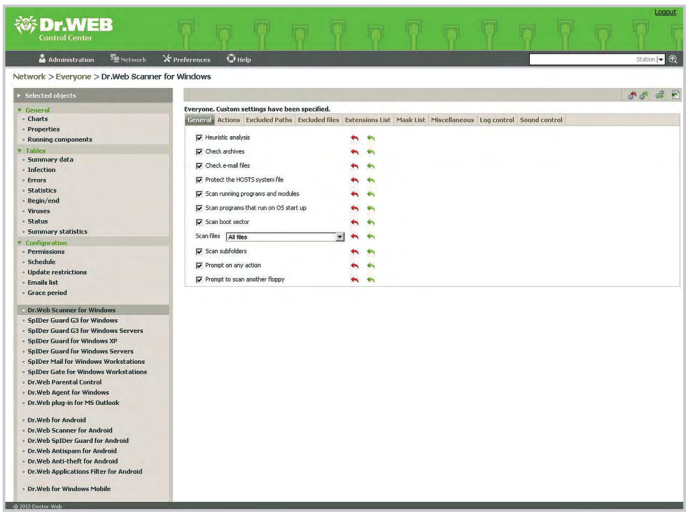
Solución

La configuración de escaneos periódicos en una estación de trabajo separada se produce en el Planificador que le permite:

- iniciar el escaneo sin la intervención del operador de estación de trabajo;
- establecer horarios de escaneos con frecuencia necesaria, es decir, realizar escaneos en el tiempo más conveniente para el personal.
- ejecutar el escaneo obligatorio después del inicio del ordenador;
- especificar las rutas de escaneos (áreas, unidades y directorios que serán escaneados de forma obligatoria) y restricciones;
- especificar la secuencia de acciones automáticas para detectar los objetos maliciosos y sospechosos.

¡Atención!

Las configuraciones del escaneo por defecto instalados por los desarrolladores Dr.Web son los óptimos. A menos que sea necesario, no se deben modificarse.



Control centralizado de los escaneos regulares de las estaciones de trabajo

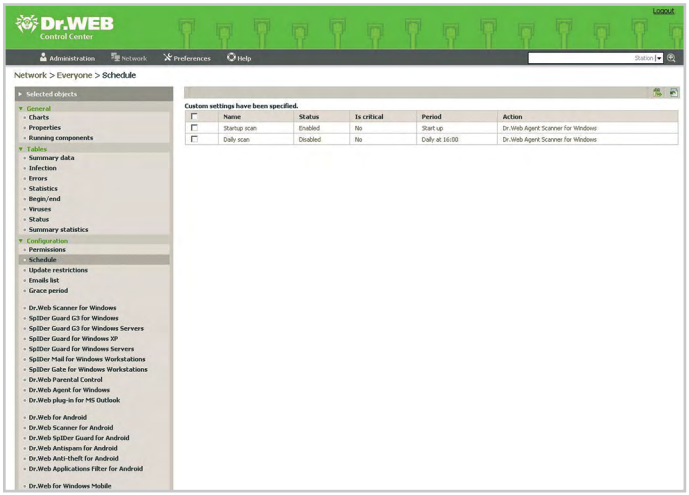
Mejores prácticas

- La única manera de garantizar los escaneos regulares en todas las estaciones de la red local es una **prohibición centralizada** para ejecutar el escaneo.

Solución

Centro de control del servicio Antivirus Dr.Web permite controlar de forma centralizada el cumplimiento de la política de seguridad en cuanto a escaneos periódicos:

- iniciar/detener el escaneo sin la intervención del operador de estación de trabajo;
- especificar las rutas de escaneos;
- establecer horarios de escaneos individuales y grupales con frecuencia necesaria, es decir, realizar escaneos en el tiempo más conveniente para el personal.



Además en el Centro de Control está prevista la oportunidad de iniciar/detener todos los componentes del agente (excepto SpIDer Guard).

Objetivo №7

Acceso restringido a los dispositivos extraíbles

¡Atención!

Esta funcionalidad sólo está disponible en el paquete Dr.Web Premium.

Amenaza

- Todos los días surge una gran cantidad de virus. El antivirus no puede conocerlos a todos - siempre existe el riesgo de infección por un virus desconocido.
- 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.

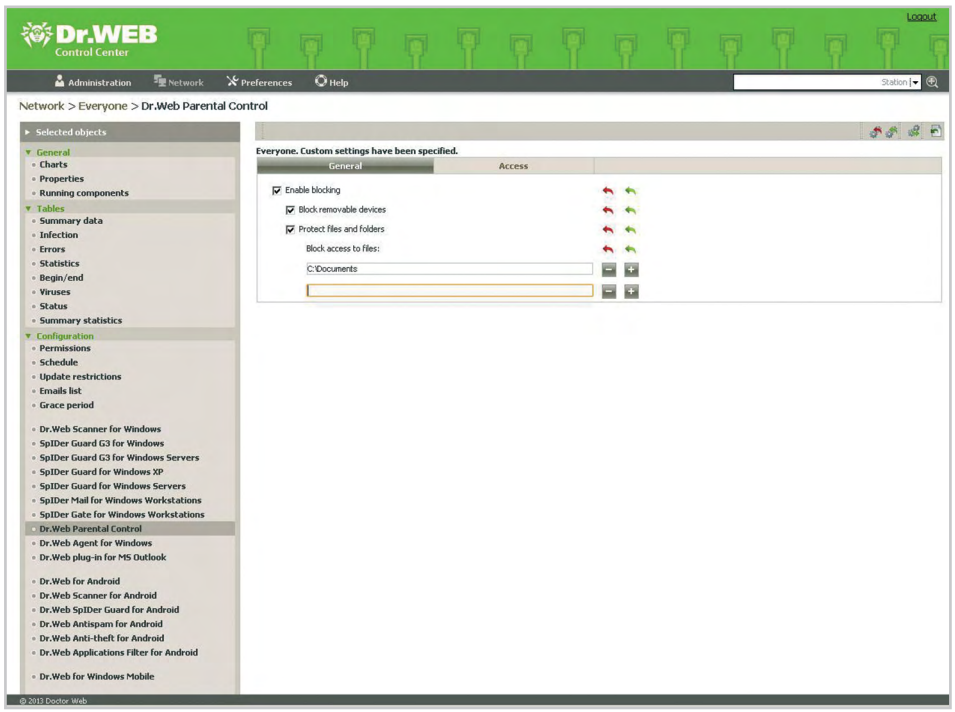
¡Atención!

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 programas maliciosos completamente que no tienen ningún mecanismo de autorreplicación y no son capaces de difundirse por sí mismos. La gente personalmente llevan troyanos de un ordenador a otro en una unidad flash.
- Según varias estimaciones, del 7 al 22% de los casos de pérdida de datos se producen como consecuencia del virus.
- Como resultado del virus podría ser la filtración de información confidencial, desconexión de la compañía de Internet, tiempo de inactividad de los empleados durante la restauración de los ordenadores infectados con virus.
- La constante amenaza de penetración de virus en la red de la compañía distrae a los administradores de realizar otras tareas necesarias para el desarrollo de la empresa.

Solución

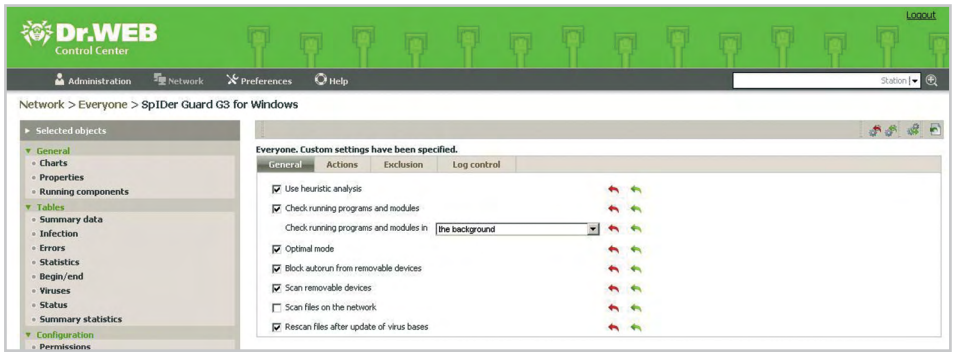
Si es necesario prohibir completamente el uso de medios extraíbles en estaciones de trabajo, active la opción “Bloquear medios extraíbles” en la configuración del componente de control de oficina Dr.Web. El uso de control de oficina cierra uno de los principales canales de virus - a través de los medios extraíbles.



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

- determina 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.



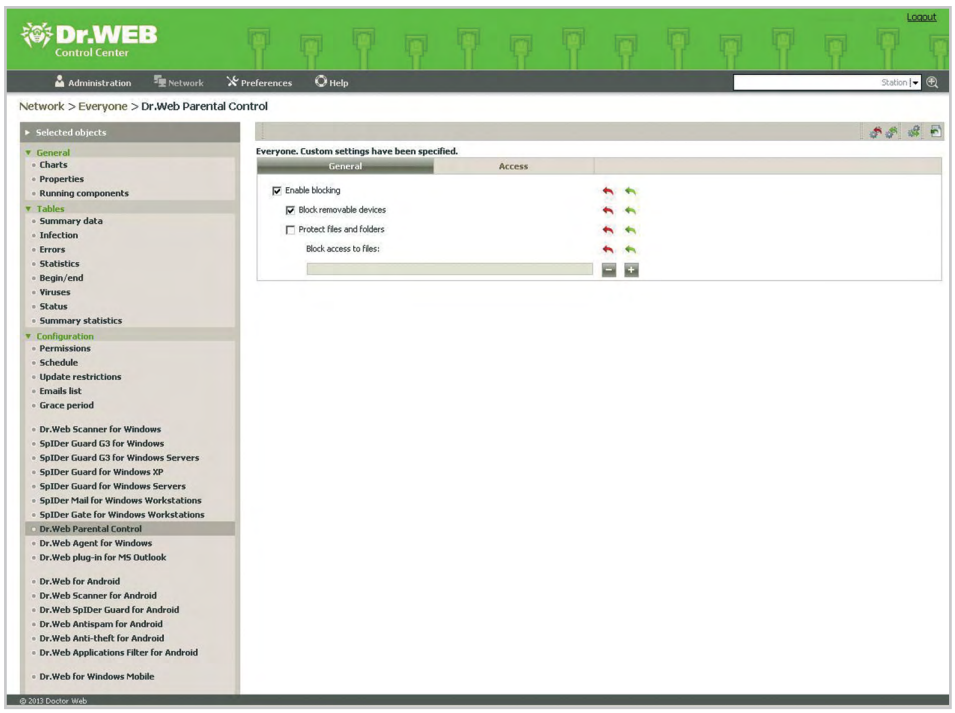
Las medidas mencionadas arriba son eficaces, pero no son suficientes, ya que un empleado puede encontrar y desactivar los ajustes.

Mejores prácticas

El usuario o el malware que actúa en su nombre no deben 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. Es mucho más fácil deshabilitar el acceso **de forma centralizada**.

Solución

Configuración centralizada de restricción de acceso a los medios extraíbles se realiza en el Centro de control del Antivirus Dr.Web.



Objetivo №8

Acceso restringido a sitios de Internet

Objetivo: protección contra las infecciones de malware y protección contra phishing

Amenaza

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 sus ordenadores;
- 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.

¿Qué sitios son las fuentes de los ataques de malware y phishing (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

Mejores prácticas

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.

Solución

Para no contraer la infección cuando se visita un sitio web malicioso es recomendable usar una protección combinada.

¡Atención!

Capacidades del sistema de protección antivirus Dr.Web permiten:

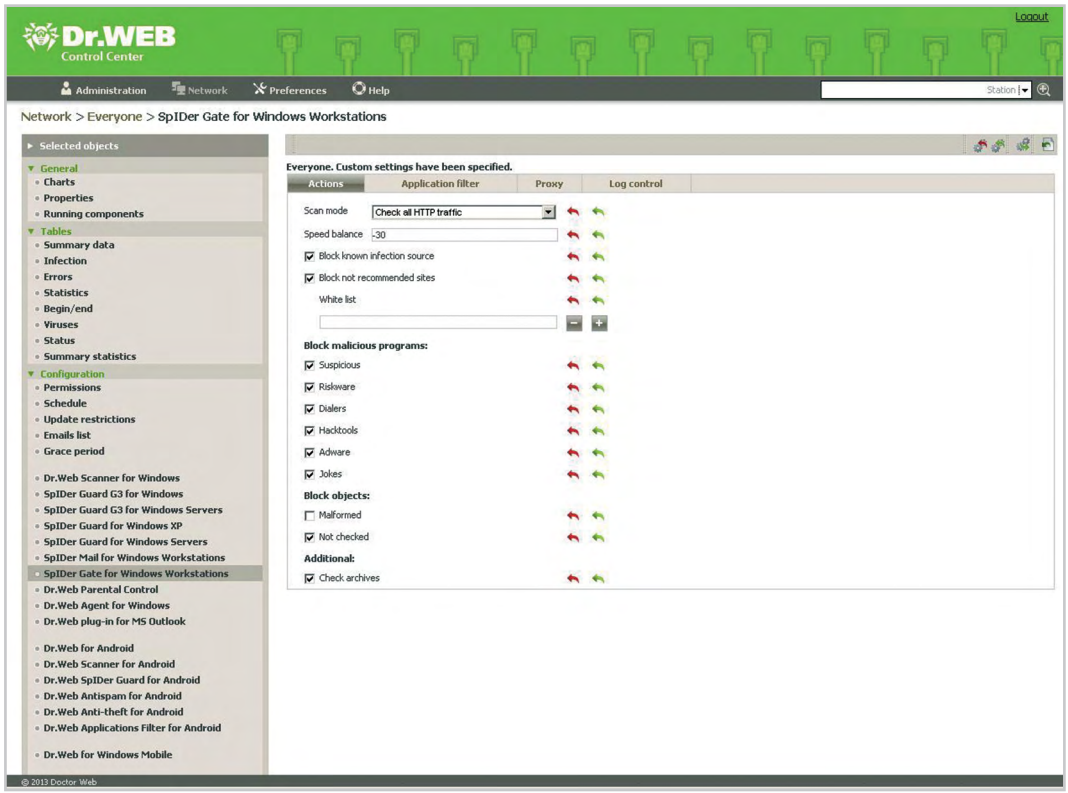
- restringir parcialmente el acceso a Internet;
- llevar listas blancas y negras para garantizar el acceso de empleados a los recursos de Internet que se necesitan para cumplir sus funciones;
- restringir completamente el acceso a Internet, donde sea necesario (por ejemplo, los ordenadores con sistemas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

Protección por medio de motor antivirus Dr.Web

- **Tecnología ScriptHeuristic** – previene la ejecución de cualquier scripts maliciosos en el navegador y documentos PDF, respetando la funcionalidad de los scripts legítimos.
- **La detección de nuevas amenazas usando el análisis heurístico** - para identificar los virus nuevos, anteriormente desconocidos, la información sobre los que no hay en la base antivirus.
- **Tecnología Fly-Code** detecta los virus conocidos ocultos por los empaquetadores desconocidos.
- **El subsistema del escanéo de fondo y neutralización de amenazas activas en Dr.Web Anti-rootkit (Antirootkit API, arkapi)** reside en la memoria y realiza la búsqueda de amenazas activas en las siguientes áreas críticas de Windows: objetos de autoinicio, procesos y módulos ejecutados, heuristicas de objetos del sistema, memoria operativa, discos de MBR/VBR, BIOS del sistema. Al detectar amenazas, el subsistema realiza la desinfección y bloquea los objetos peligrosos.

Protección por medio de los componentes de software a nivel de una estación individual

- **Monitor de archivo SpIDer Guard** es la protección contra las infecciones activas que operan en el sistema.
- **Control de oficina Dr.Web** escanea según la base de datos actualizada los sitios peligrosos e indeseables en 10 categorías (redes sociales, juegos de azar, etc.).
- screenshot
- **Monitor HTTP SpIDer Gate®** escanea basándose en firmas y verifica con los métodos heurísticos — antes de que el tráfico ingrese en el navegador.
- El módulo SpIDer Gate analiza el trafico HTTP entrante en tiempo real, intercepta todas las conexiones HTTP/ HTTPS, realiza la filtración de datos, bloquea las páginas infectadas en cualquier navegador automáticamente, analiza los archivos comprimidos (por ejemplo, descargados con un asistente de descargas, y otras aplicaciones que intercambian datos con servidores web), protege contra recursos de Internet de fishing y otros peligros.
- Es posible desactivar el escaneo del tráfico saliente y entrante, así como compilar una lista de aplicaciones, cuyo tráfico HTTP será comprobado en todo caso y en su totalidad (lista negra). También existe la posibilidad de excluir algunas aplicaciones del escaneo de tráfico (lista blanca).
- El funcionamiento de SpIDer Gate no depende del navegador que se utiliza.
- La filtración prácticamente no influye en el rendimiento del equipo, la velocidad de Internet y la cantidad de datos transmitidos.
- El modo "por defecto" no requiere ninguna configuración: SpIDer Gate comienza a escanear inmediatamente después ser instalado en el sistema.



¡Atención!

Dichos componentes están disponibles solamente en el paquete Dr.Web Premium.

Objetivo №9

Ahorro de gastos en Internet y control sobre las actividades de los empleados

Amenaza

- Si cada empleado de la compañía navega al menos una hora al día en Internet con fines personales, esto constituye unos 12,5% de los gastos de la empresa sobre los salarios.
- En algunos períodos del día (por ejemplo, la hora del almuerzo) los empleados ocupan hasta 80% del ancho de banda en los temas no relacionados con el trabajo.

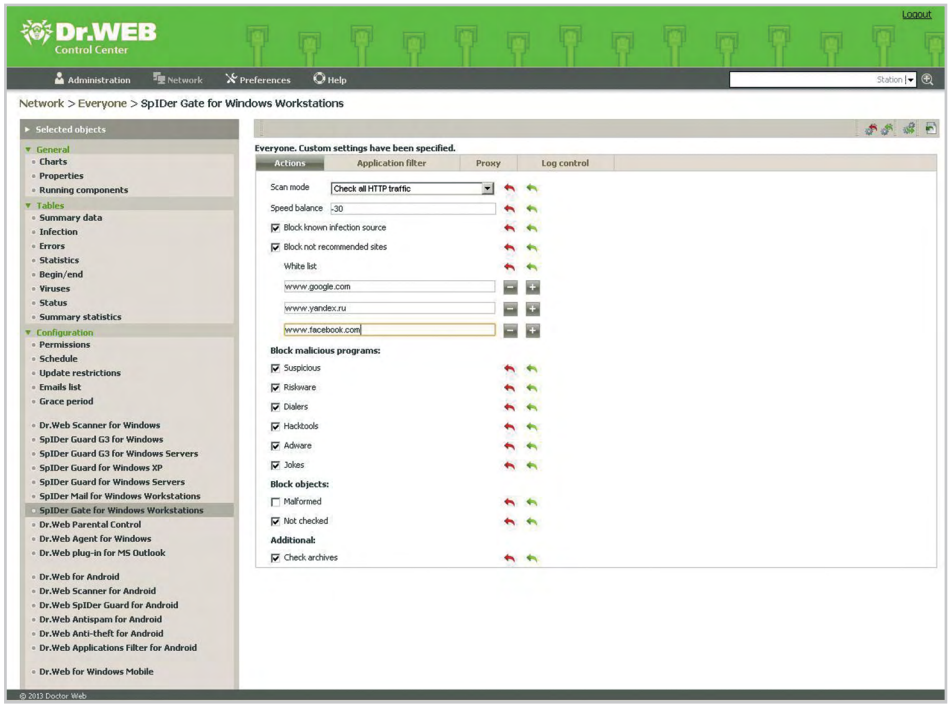
Mejores prácticas

- En las horas de trabajo, el personal sólo debe tener acceso a los recursos de Internet necesarios en términos de trabajo.
- Establezca la restricción **centralizada** de acceso a los recursos innecesarios de Internet.
- La opinión del personal sobre la nocividad de ciertos sitios debe ser IGNORADA.

Solución

La gestión centralizada del servicio Antivirus Dr.Web permite:

- prescribir políticas del acceso a los recursos web para grupos de usuarios o usuarios particulares;
- prevenir los intentos de visitar las páginas no deseadas, por ejemplo, redes sociales, tiendas virtuales, sitios de juegos.



Protección contra el correo no deseado

¡Atención!

Esta funcionalidad sólo está disponible en el paquete Dr.Web Premium.

Reducción del tráfico de spam y eliminación de hasta el 99% de las amenazas que se expanden mediante el spam

Amenazas

1. El tráfico de correo es el **portador** principal 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.
2. 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.

Riesgos en el uso del antivirus sin el antispam

Riesgos vinculados con virus	Riesgos de reputación
▪ La posibilidad de infectar el ordenador y convertirlo en una botnet y el objeto para los ataques de hackers - hasta la denegación en su mantenimiento ▪ La posibilidad de compromiso de la empresa mediante su inclusión en la lista negra y desconexión de la red de Internet a causa de envío de spam en caso de encontrarse en la botnet ▪ El aumento en los costos de infraestructura de TI (el pago de tráfico "parasitario"/almacenamiento de correo, incluyendo spam), aumento de pago por el tráfico	▪ Los socios no recibirán los correos electrónicos a causa de permanencia de la empresa en las listas negras ▪ Empeoramiento de reputación a ojos de clientes y socios; ▪ Se formará opinión acerca de la compañía como atrasada tecnológicamente; ▪ Pérdida de clientes o denegación de los servicios de la empresa.

Ilusión

Antispam requiere una capacitación constante.

Hechos

Sistema inteligente Dr.Web de filtrado de spam no requiere configuración e instrucción, en comparación con los sistemas antispam, cuyo uso requiere el trabajo diario del administrador del sistema.

Mejores prácticas

- La verificación del tráfico de correo debe realizarse antes de que las cartas ingresen en el programa de correo con el fin de excluir la posibilidad de que las vulnerabilidades sean utilizadas por el código malicioso.
- Sólo las soluciones completas para el correo electrónico, que combinan antivirus y **antispam**, pueden proveer una protección integral y reducción de gastos improductivos de la compañía, es decir, pérdidas derivadas de las deficiencias en la organización y gestión de la producción.

Solución

Antispam Dr.Web que forma parte del monitor SpIDer Mail analiza el correo antes de que la carta ingrese en el cliente de correo y no permite que los programas maliciosos - cuyo propagador es el spam - se aprovechen de las vulnerabilidades en el software. Su funcionamiento no tiene prácticamente ningún efecto sobre los recursos de computación del sistema. La efectividad de la selección de spam alcanza el 97-99%.

Objetivo №11

Ventajas de antispam Dr.Web

- **Antispam no requiere capacitación** - a diferencia de los sistemas antispam, cuyo uso requiere el trabajo diario del administrador del sistema, el sistema inteligente Dr.Web de filtrado de spam no requiere configuración y comienza a proceder de forma automática con el primer mensaje.
- **Alta tasa de filtración de correo no deseado** - diversas técnicas de filtrado proporcionan una alta probabilidad de detección de spam, phishing, pharming, scamming y mensajes de rebote.
- **Protección contra botnets** – el proveedor no le quitará el acceso a Internet por envío masivo de spam.
- **El correo no se perderá** - los mensajes filtrados no se eliminan, sino se mueven a una carpeta especial del programa de correo electrónico (siempre que la carpeta esté configurada en la estación local), donde, si es necesario, se pueden ver en la presencia de falsos positivos.
- **Ahorro de tráfico** - el módulo de analizador de spam es completamente autónomo; para su funcionamiento no se requiere la conexión con un servidor externo, o el acceso a una base de datos.
- **Siempre actual** - tecnologías únicas de reconocimiento de correo no deseado en base a varios miles de reglas, permiten llevar a cabo las actualizaciones más de una vez por día.
- **No carga el sistema** - el antispam no tiene carga apreciable sobre el sistema sin aumentar el tiempo al recibir el correo.

Aumentar el rendimiento de los empleados

En tiempos de sobreproducción de la información, la atención humana es un recurso valioso y prácticamente no renovable. Abundancia e incluso una sobreabundancia de información, su accesibilidad fácil debido a la presencia de Internet absorben la atención de la gente. Limpieza de su buzón de correo de spam, cierre de ventanas emergentes y los banners, todos estos factores distraen la atención, reducen el nivel de concentración, provocan el impacto negativo en el estado emocional y mental de una persona. Como resultado, el costo de la atención de un empleado es más caro para las empresas que los costos en los medios de lucha con los factores revulsivos.

Amenazas

1. Un empleado de oficina gasta en promedio unos 6-11 minutos de tiempo laboral por día para revisar y eliminar el correo no deseado.
2. Cuanto más alto sea el cargo del empleado, más se pierde en su remuneración.

Riesgos

El uso de antivirus sin antispam:

- reduce la productividad de todos los empleados que reciben el correo y se ven obligados a limpiar los buzones de spam.
- conduce a una pérdida de tiempo laboral - los retrasos en la ejecución de las funciones del personal y, por lo tanto, los retrasos en en el cumplimiento de las obligaciones con los clientes y socios;
- influye en la disminución de atención y aumento de la fatiga debido a un exceso de factores revulsivos;
- provoca la irritación e insatisfacción de personal debido a la incapacidad de los directivos hacer frente al problema (alto riesgo para la reputación de los directivos).

Solución

Usando antispam como parte de Dr.Web Premium es un medio eficaz de hacer frente a múltiples distracciones que reduce la pérdida de tiempo laboral:

- debido al funcionamiento estable y seguro del ordenador (sin virus y spam en el tráfico de correo);
- debido a la falta de personal en el correo de spam, cuya limpieza puede llevar mucho tiempo.

Configuración del filtrado de spam en una estación individual

El antispam se puede habilitar en el componente de software Dr.Web SpIDer Mail.

Listas blancas y negras

Si es necesario, se puede crear listas de direcciones de confianza y direcciones bloqueadas, cuyo correo será filtrado por defecto.

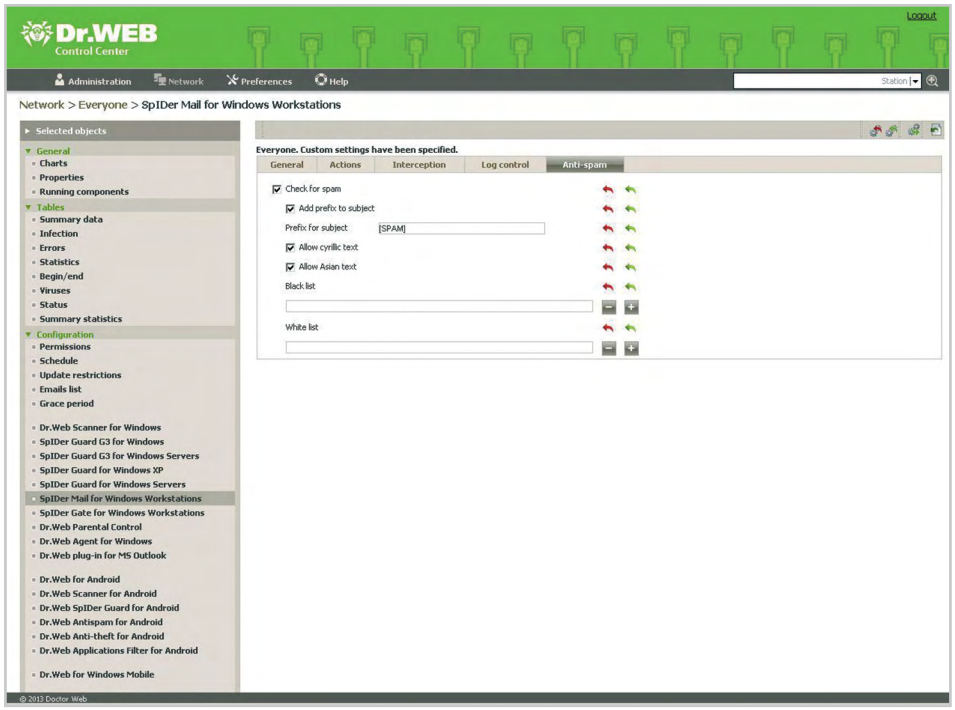
Control centralizado sobre la incapacidad de deshabilitar el antispam

Mejores prácticas

La única medida eficaz para evitar la posibilidad de desactivar el antispam o editar las listas negras y blancas es la **prohibición centralizada** de acceso a las configuraciones de antispam.

Solución

Configuración centralizada de los ajustes de antispam se realiza en el Centro de control de Antivirus Dr.Web.



Objetivo №13

Protección contra los ataques virus en los dispositivos con el sistema de banca electrónica

¡Le recordamos!

1. Amenazas modernos son creados por las bandas criminales bien organizadas, no con el fin de perfeccionar las habilidades de los programadores, sino para robar el dinero de los que saben cómo ganarlos.
2. Las vulnerabilidades existen en cualquier software, incluyendo el sistema de banca electrónica.

Escenarios de ataques actuales destinados a robo de fondos

Para la infiltración / introducción de virus en el sistema de banca electrónica, se utilizan:

- Sitios de phishing
- Creación de páginas web falsas
- Intrusión de los sitios y recursos en Internet con alto nivel de audiencia
- Técnicas de ingeniería social
- La piratería informática

Tipos de ataques dirigidos para robar fondos

- La infección virus del PC a través de una inyección web (a veces redirigiendo a un sitio de phishing)
- Un ataque a los canales de transmisión de datos - se produce la intercepción de peticiones http con el fin de obtener un nombre de usuario / contraseña o los valores de las formas en la pantalla transmitidos
- Los ataques de virus en el servidor - sus objetos pueden ser la búsqueda de vulnerabilidades en el servidor del sistema de banca electrónica u ocultamiento de los hechos de robo de fondos
- Los ataques al ordenador a través de Internet para robar las claves de firmas digitales, contraseñas
- Los ataques al ordenador a través de Internet con el fin de obtener el control remoto de los recursos del ordenador
- Ataque con el objetivo de sustituir el documento cuando se lo llevan para firmar
- Ataque con el objetivo de sustituir una parte o la totalidad de software que se usa
- La introducción de marcadores de software o programas troyanos

Objetos de los ataques

- PCs de oficina;
- dispositivos personales de los empleados;
- dispositivos personales de los clientes de la empresa en cuestión.

Objetivos de los ataques

- el robo y la sustitución de los medios de autenticación de acceso (usuario y contraseña) en el sistema de banca en línea;
- realizar transacciones bancarias mediante el acceso remoto - en una sesión ya existente o paralela;
- penetración en la red de la empresa protegida.

Métodos de robo

- Creación de un pago no autorizado de forma remota directamente desde el equipo del cliente mediante el software malicioso.
- El envío de una orden de pago por los intrusos utilizando el ordenador del cliente cuando el cliente trabaja en el sistema de banca electrónica (con la posibilidad de firmar el documento con una clave guardada en los medios de seguridad, como eToken, iKey, etc.).

Cliente indignado

"Antivirus se ha comprado, el administrador también cobra, los sistemas se actualizan ... ***¡Pero el dinero se ha ido! ¿Quién tiene la culpa?"***

Hechos

1. En la mayoría de las empresas pequeñas y medianas la persona autorizada a firmar las órdenes de pago es el gerente. Ya que dos firmas digitales, la del gerente y del contador, reduce significativamente el riesgo de robos a causa de virus.
2. El acceso a la banca electrónica se realiza no sólo desde el ordenador de la oficina. Sino desde los PCs de hogar y dispositivos móviles (por lo general, bajo Android), que, generalmente, no tienen ningún antivirus, y si tienen, es gratuito y limitado en sus funcionalidades.

En Rusia no hay hechos estadísticos de malversación de fondos a causa de virus a través de la banca en línea. La mayoría de las víctimas ni siquiera se aplican a las autoridades policiales, creyendo que es imposible de recuperar los fondos, y habrá más problemas de recorrer las instituciones. Las víctimas no saben por dónde empezar a actuar en una situación crítica, no conocen el procedimiento para iniciar una investigación para recuperar los fondos perdiendo de este modo el tiempo valioso.

Amenazas

1. Troyanos modernos exitosos tienen el objetivo de robar los fondos de empresas y personas particulares.
2. El más exitoso y peligroso es Trojan.Carberp que se expande mediante un conjunto de exploits Black Hole Exploit Kit, una colección de vulnerabilidades que explotan bugs y características indocumentadas de software moderno, como navegadores y sistemas operativos.
3. El grupo delictivo organizado desarrollan y "promueven" el Trojan.Carberp: los desarrolladores están en un país, los servidores desde los que el troyano se distribuye, en el otro, los organizadores, en el tercer lugar, los "socios" que compran parte de una botnet para su propio uso criminal están en varios países.
4. El troyano tiene la capacidad de descargar plug-ins especiales. Actualmente, hay versiones de los plugins diseñados para la mayoría de los sistemas bancarios famosos. Entre los comandos que realiza Trojan.Carberp hay directivas para ejecutar archivos arbitrarios en el ordenador infectado, iniciar sesiones de escritorio remoto a través de RDP, e incluso eliminar el sistema operativo de la PC infectada. Gracias a un control remoto y los plug-ins se puede organizar un ataque contra una compañía específica bajo la orden desde el exterior. Las acciones del troyano en contra de su empresa depende del "cliente".
5. Los virus de la familia Carberp penetran en los ordenadores de usuarios durante la navegación por los sitios web hackeados, incluidos los de noticias y de contabilidad, los que visitan las victimas potenciales cada día. No es necesario emprender alguna acción con el fin de "obtener el troyano": la infección ocurre automáticamente.
6. El troyano necesita sólo 1-3 minutos para robar contraseñas y el dinero de la cuenta de la víctima.
7. Todos los días en la base de datos de virus Dr.Web se añaden varias entradas de este troyano - el programa está siendo constantemente mejorado por sus creadores. Un ejemplo de nuevos troyanos en un solo día:

```
Trojan.Carberp.14(2) Trojan.Carberp.15(7) Trojan.Carberp.194 Trojan.Carberp.195
Trojan.Carberp.196 Trojan.Carberp.197 Trojan.Carberp.198 Trojan.Carberp.199 Trojan.Carberp.200
Trojan.Carberp.201 Trojan.Carberp.202 Trojan.Carberp.203 Trojan.Carberp.204 Trojan.Carberp.205
Trojan.Carberp.206 Trojan.Carberp.207 Trojan.Carberp.208(14) Trojan.Carberp.209
Trojan.Carberp.210 Trojan.Carberp.211 Trojan.Carberp.212 Trojan.Carberp.214 Trojan.Carberp.215
Trojan.Carberp.216 Trojan.Carberp.217 Trojan.Carberp.218 Trojan.Carberp.219 Trojan.Carberp.220
Trojan.Carberp.221 Trojan.Carberp.222 Trojan.Carberp.224 Trojan.Carberp.225 Trojan.Carberp.226
Trojan.Carberp.227 Trojan.Carberp.228 Trojan.Carberp.229 Trojan.Carberp.230 Trojan.Carberp.231
Trojan.Carberp.232 Trojan.Carberp.233 Trojan.Carberp.234 Trojan.Carberp.235 Trojan.Carberp.236
Trojan.Carberp.237 Trojan.Carberp.238 Trojan.Carberp.239 Trojan.Carberp.240 Trojan.Carberp.241
Trojan.Carberp.242 Trojan.Carberp.243Trojan.Carberp.244 Trojan.Carberp.245 Trojan.Carberp.246
Trojan.Carberp.247 Trojan.Carberp.248 Trojan.Carberp.249 Trojan.Carberp.250 Trojan.Carberp.251
Trojan.Carberp.252 Trojan.Carberp.253 Trojan.Carberp.254 Trojan.Carberp.255 Trojan.Carberp.256
Trojan.Carberp.257 Trojan.Carberp.258 Trojan.Carberp.259 Trojan.Carberp.260 Trojan.Carberp.261
Trojan.Carberp.262 Trojan.Carberp.263 Trojan.Carberp.264 Trojan.Carberp.265 Trojan.Carberp.266
Trojan.Carberp.267 Trojan.Carberp.29(14) Trojan.Carberp.33(10) Trojan.Carberp.45(4)
Trojan.Carberp.5(3) Trojan.Carberp.60(6) Trojan.Carberp.61 Trojan.Carberp.80
```

   Esto es sólo un troyano ...

¿Cómo puede oponerse la compañía que tiene sólo el antivirus de archivos sin medios de protección antivirus completa? - DE NINGUNA MANERA.

Mejores prácticas

1. Solo antivirus para proteger contra este tipo de ataques no es suficiente. Para reducir el riesgo de infección, el sistema de protección antivirus debe incluir:
   - Un sistema de tratamiento de las infecciones activas para cancelar la actividad de programas maliciosos penetrados de algunas manera en el sistema y limpiarlo.
   - El mejor sistema de autodefensa para que funcione correctamente antes de obtener actualizaciones que permiten tratar la infección.

- Control de oficina tiene un mecanismo para restringir el acceso a sitios de Internet (se les recuerda que el troyano se distribuye a través de los sitios).
- El módulo de análisis de los enlaces (HTTP-monitor).
- Centro de control - el sistema no debe permitir a los empleados a cambiar los ajustes con el pretexto de que "todo está muy lento".

2. Como muestra la práctica, los pagos pueden hacerse no sólo desde las máquinas ubicadas en la oficina de contabilidad, sino también desde los ordenadores de hogar y dispositivos móviles. Por lo tanto, es necesario de proteger todas las máquinas y dispositivos móviles que utilizan los empleados de la compañía.
3. El equipo en el que está instalado el sistema de contabilidad o sistemas de banca a distancia debe estar completamente desconectado de la Internet. También debe estar bloqueado de forma CENTRALIZADA el uso de unidades extraíbles.*
4. La opinión del contador sobre las medidas adoptadas para proteger el ordenador debe ser completamente IGNORADO.

** Se produce mediante el componente de control de la oficina como parte del paquete Dr.Web Premium.*

Hechos

Ya existe el primer troyano bancario para la plataforma Android - Android.SpyEye.1.

¿Qué hay que hacer si los recursos han sido robados del sistema de banca electrónica?

Por desgracia, las víctimas se enteran del hecho de robo, cuando todo ya ha sucedido. Y 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.
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.
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.
5. Presente una solicitud a su proveedor para que proporcione registros de conexión de red por el período en que se produjo el robo.

¡Atención!

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

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

Protección contra los ataques de hackers

Tipos de los ataques de hackers

Existe una gran cantidad de tipos de ataques de red. Típicamente, para atacar se usan vulnerabilidades de sistema operativo u otro software instalado, capacidad de procesamiento limitada de la víctima. Dentro de los ataques de red los más comunes son:

- **ataques DoS o DDoS** (ataques que provocan una denegación de servicio), se utilizan para poner temporalmente el sistema atacado fuera de servicio.
- **Ataques de contraseñas.** Su objetivo es identificar las contraseñas usadas - por el método de selección o por medio de la ingeniería social.
- **Spoofing** es la inserción de información falsa o comandos maliciosos en el flujo normal de datos, redirigiendo el tráfico a la dirección IP falsa y/o su sustitución.
- **Sniffing** - intercepción de tráfico (por ejemplo, todos los mensajes de correo electrónico de la víctima) para su posterior análisis.
- **Intercepción de sesiones TCP** (TCP Session Hijacking).
- **Man-in-the-Middle.** El atacante se encuentra como si entre dos hosts de la red y actúa como un servidor proxy, viendo la información que se transmite y siendo capaz de modificarla para sus propios fines. Dichos ataques se llevan a cabo con el fin de robar información, interceptar la sesión actual y obtener acceso a los recursos privados de red, análisis de tráfico, y obtención de información sobre la red y sus usuarios, la realización de ataques de tipo DoS, la distorsión de los datos transmitidos y la introducción no autorizada de la información en la sesión de red.

Eso no es todo. Entre los ataques de red se puede incluir todos los métodos de exploración realizada por la red, abuso de confianza y el acceso no autorizado. Por ejemplo, el escaneo de puertos - una amenaza de este tipo no es un ataque, pero por lo general le precede, ya que es una de las principales formas de obtener información sobre un equipo remoto. La información resultante del escaneo (una "copia" del sistema) da al atacante una idea del tipo de sistema operativo en el ordenador remoto y, entonces, de las vulnerabilidades específicas para este sistema operativo.

Nuevos tipos de ataques surgen constantemente. En particular, el paso de las empresas en la "nube" ha provocado la activación de los ataques a los canales de transición de datos, y la introducción del protocolo IPv6 - la creación de nuevos tipos de ataques, asociados con las vulnerabilidades de este protocolo aún imperfecto en la aplicación.

Consecuencias de los ataques

- El daño o destrucción de los recursos de información, y, por lo tanto, incapacidad para utilizarlos, inactividad de los equipos.
- Las fugas de datos confidenciales, incluyendo contraseñas, el correo y en general, cualquier dato que puede ser robado.
- Riesgos de reputación - retraso o incumplimiento de las obligaciones para con los clientes y socios.

¡Atención!

Ataques en la introducción de programas maliciosos suelen ser desadvertidas por las víctimas cuyos equipos están controlados por los hackers.

Objetivos de los ataques

- Motivos políticos
- Verificar los competidores (incluyendo exploración industrial, venganza)
- Gamberrismo

Solución

El firewall como parte del servicio Antivirus Dr.Web:

- protege contra insiders mediante la prohibición para escanear la red o conectarse a escritorio remoto;
- impide la infiltración de hackers a través de los puertos abiertos;
- protege contra el acceso no autorizado;
- reduce el riesgo de intrusión a través de las vulnerabilidades;
- evita la fuga de datos importantes por la red;
- bloquea las conexiones sospechosas en paquetes y aplicaciones;
- control de conexiones a nivel de aplicaciones permite controlar el acceso de programas y procesos específicos a los recursos de red y registrar la información sobre los intentos de acceso en el registro de aplicaciones.
- la filtración a nivel de paquetes permite controlar el acceso a Internet, independientemente de los programas que inician la conexión. El registro de filtro de paquetes conserva la información acerca de los paquetes transmitidos a través de las interfaces de red.

¡Atención!

Firewall Dr.Web no está instalado de forma predeterminada. Para instalar este componente, es necesario seleccionarlo durante la instalación.

Protección contra la intrusión a través de las vulnerabilidades

Amenaza

- Vulnerabilidad es una falla en el software, con el que se puede poner en peligro la integridad del software o causar incapacidad.
- La 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 plugins para los navegadores para visualizar el flash).

¡Atención!

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

Mejores prácticas

Mantener al día el software instalado en el ordenador no es menos importante que actualizar el sistema operativo. Teóricamente cualquier error en el programa se puede utilizar para dañar el sistema en su totalidad. Será una falla corta o el daño grave de datos, en este caso no importa. Para evitar esto, es importante vigilar el estado del software existente y descargar actualizaciones o nuevas versiones en el momento oportuno.

Solución

El uso del monitor HTTP SpIDer Gate y monitor de correo SpIDer MailD evita la penetración de objetos maliciosos debido a las vulnerabilidades de los programas (tales como los navegadores, Adobe Flash y Adobe Acrobat, los clientes de correo), ya que todo el tráfico, incluyendo encriptado se somete al análisis antes de ingresar en el programa correspondiente.

Protección contra las infecciones usando los métodos de la ingeniería social

El virus más terrible es el usuario.

La sabiduría popular

La mayor parte de malware contemporáneos de la "vida silvestre" no tiene mecanismo de autorreplicación - han sido intencionalmente diseñados para ser difundidos 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.

Mejores prácticas

Para hacer frente a los estafadores que usan este método de ataque, no se requiere mucho. El cumplimiento de las reglas simples contribuye a reducir significativamente la probabilidad de pérdida de datos:

1. Si usted ha recibido una carta exigiendo a informar o confirmar la contraseña a un recurso - bórrelo, no importa las terribles amenazas que puede contener (eliminación de la cuenta, liquidación de la cuenta, etc.). Administración de recursos de red, especialmente los bancos, NUNCA solicitan al usuario cualquier datos.
2. Si usted ha recibido supuestamente de su amigo una carta o mensaje de contenido extraño, además de tener enlaces a algunos recursos - póngase en contacto con él de alguna otra forma (por ejemplo, por teléfono) y averigüe que y por qué se lo ha enviado. Es posible que su cuenta ha sido comprometida y utilizada por los piratas informáticos.
3. Si los recursos extraños ofrecen ir a la página donde tiene que introducir sus datos (por ejemplo, un enlace al sitio vkontakte.ru), introduzca manualmente el texto del enlace en la ventana del navegador , de este modo se excluye totalmente la posibilidad de pasar a un sitio de phishing (hay muchas formas de enmascarar los enlaces verdaderos). Antes de poner el enlace en el navegador, verifique si el nombre de dominio corresponde al nombre de dominio original (para tenderle un lazo, por ejemplo, en lugar de vk.ru, un enlace malicioso puede ser vkontacte.ru).
4. Al leer en Internet sobre el hecho de "frito", por ejemplo, sobre una nueva manera de leer SMS de otras personas, es aconsejable no probarlo en acción. Los hackers nunca anuncian qué vulnerabilidades han podido encontrar. En este caso, juegan en la curiosidad de los usuarios para hacer pasar al recurso infectado.
5. No desactive en el antivirus el monitor HTTP (web antivirus) - eso protegerá todas sus actividades en la red.

¡Importante!

No desactive el monitor de archivo SpIDer Guard. Debe permanecer constantemente en la memoria del ordenador y prevenir la infección mediante el escaneo de los archivos antes de ejecutarlos, así como todos los procesos del sistema y durante cada actualización de antivirus. SpIDer Guard es eficaz contra todas las amenazas conocidas y desconocidas, por lo que utiliza métodos de análisis heurístico. Incluso si el nuevo virus no fuese detectado por SpIDer Guard, igual no podrá realizar acciones maliciosas.

Objetivo №17

Reducción de tiempo de inactividad de virus

Los virus y el spam son las principales amenazas a la seguridad de la información para las empresas de todos los tipos y tamaños. El análisis del estado de la red corporativa, trabajos para prevenir los ataques y acciones para superar los efectos de los incidentes de virus son las tareas que tienen que cumplir los especialistas en TI todos los días. Reducción de tiempos de inactividad causados por objetos maliciosos, es una de las tareas más importantes de los administradores del sistema, de su solución exitosa depende la eficacia de los procesos de negocio de toda la empresa y su imagen como un socio confiable.

Amenaza

- El tiempo de inactividad es un promedio de 2 horas al mes por usuario.
- Cuanto mayor sea el cargo del usuario, mayor será el costo de su tiempo de inactividad.

El tiempo de inactividad se gasta esperando la solución del problema o haciendo intentos independientes para arreglarlo, lo que puede llevar a consecuencias impredecibles, hasta una pérdida completa de los datos.

Solución

En el caso de la utilización del software como servicio:

- mejoras y actualizaciones del software se realizan automáticamente y son administradas e forma centralizada por el proveedor de servicios o administrador del sistema de la empresa;
- el tiempo de inactividad causado por una reacción inexperta de los usuarios a la infección virus que provoca la incapacidad para realizar su trabajo, se descarta por completo, si está deshabilitada la opción de cambiar ajustes en la estación de trabajo protegida.

El servicio Antivirus Dr.Web es una herramienta poderosa para reducir el tiempo de inactividad causado por los virus y malware.

Sistema de protección antivirus Dr.Web

Servicios del Centro de control

Alertas sobre los sucesos del sistema de protección

Está implementado el sistema de alertas al administrador sobre los problemas en la red antivirus, por ejemplo, los informes de ataques de virus, alertas del sistema, notificaciones a los usuarios de los resultados del escaneo. Alertas se llevan a cabo por correo electrónico o utilizando las herramientas de emisión estándar de sistemas operativos Windows. Los textos de mensajes se personalizan.

Servicio de mensajería instantánea

Una interfaz para enviar mensajes a los usuarios del servicio permite al administrador del sistema enviar mensajes informativos a los usuarios individuales o grupos de usuarios. Esta opción puede utilizarse, por ejemplo, para enviar mensajes sobre epidemias y sobre los pasos a seguir en caso de infección por malware, para el envío de mensajes técnicos acerca de los problemas en la red, o felicitando con las fiestas.

Estadísticas e informes

El sistema permite a los administradores obtener información detallada sobre el estado de la red antivirus:

- virus detectados (la lista de los objetos contaminados, virus, acciones del antivirus, etc.)
- información acerca de los virus detectados en las estaciones que se agrupan por tipos de virus;
- información sobre la base de datos de virus instalado: el nombre del archivo que contiene la base de datos específica de virus; versión de la base de datos de virus; el número de entradas en la base de datos de virus; fecha de creación de la base de datos de virus;
- la lista de errores de escaneo en la estación de trabajo seleccionada durante un período determinado;
- la lista de los componentes que se ejecutaban en la estación de trabajo;
- información acerca del estado inusual de estaciones de trabajo y (posiblemente) que requiera intervención por un período determinado;
- lista de tareas asignadas a una estación de trabajo para un período determinado;
- información detallada sobre todos los módulos de antivirus Dr.Web: descripción del módulo - su nombre funcional; archivo que define el módulo separado del producto; versión completa del módulo, etc.;
- la lista de instalaciones de software en la estación de trabajo;
- estadísticas de resumen.

La presentación gráfica de la información sobre el estado de la red protegida permite llevar a cabo la recogida y análisis de la información sobre eventos virus en cada equipo protegido y proporcionar informes estadísticos ilustrativos sobre los resultados del monitoreo.

Registro de auditoría de las acciones

Permite monitorear todas las actividades del administrador del sistema para instalar y configurar el sistema. Si usted tiene preguntas en cuanto a la cronología o justificación de las actividades, el administrador puede proporcionar un informe completo sobre el trabajo realizado - lo que garantiza la máxima transparencia de sus acciones.

¡IMPORTANTE!

Al investigar incidentes informáticos, el registro de auditoría de acciones forma parte esencial de la base de pruebas.

Conclusión

Sobre la compañía Doctor Web

La compañía Doctor Web es el elaborador ruso de medios de protección de información.

Los productos de Dr.Web se están elaborando desde el año 1992 y demuestran constantemente los excelentes resultados de detección de malware.

Todos los derechos sobre las tecnologías Dr.Web son la propiedad de Doctor Web. Doctor Web es uno de los pocos vendedores antivirus en el mundo que tiene sus propias tecnologías únicas para detectar y desinfectar los programas maliciosos. La compañía tiene un núcleo original propio, cuenta con su propio laboratorio antivirus, un servicio global de monitoreo de virus y servicio de soporte técnico.

Hoy en día Doctor Web es una compañía exitosa de crecimiento rápido, que desempeña un papel principal en el mercado de la seguridad informática.

Usuarios Dr.Web

Tasa de crecimiento anual de las ventas de Doctor Web supera los índices promedios del sector. La compañía se está expandiendo gradualmente su posición en el sector público tradicional para las soluciones antivirus Dr.Web, las soluciones de la compañías se utilizan por los ministerios y organismos, los principales bancos, las grandes empresas industriales.

Los consumidores de productos Dr.Web son los usuarios de hogar de diferentes partes del mundo, grandes empresas rusas, las organizaciones pequeñas y grandes corporaciones, a quienes el equipo de Doctor Web está agradecido por el apoyo y confianza en los productos durante muchos años. Los certificados y premios estatales que posee el antivirus Dr.Web, así como la geografía de los usuarios Dr.Web confirman la alta calidad de los productos creados por los programadores talentosos de Rusia.

Capacitación y Certificación

Las causas más comunes de incidentes informáticos de cualquier tipo es la falta de capacitación del personal en el campo de la seguridad informática. Sólo el conocimiento y la comprensión de los conceptos básicos de seguridad informática puede reducir el número de incidentes y garantizar la eficacia del sistema de protección antivirus.

- **Capacitación de los administradores de sistema**

Para un funcionamiento eficiente de los sistemas de seguridad de la información, construidos en base de productos Dr.Web®, han sido desarrollados los programas de capacitación y certificación en el ámbito de seguridad de redes informáticos de la empresa. Los cursos de capacitación se crean con la participación directa de los desarrolladores de la compañía Doctor Web. Durante la capacitación los especialistas efectivamente adquieren las habilidades necesarias para trabajar con los productos Dr.Web, lo que permite realizar una evaluación objetiva del nivel de conocimientos de los profesionales en TI.

- **Capacitación de los usuarios de productos Dr.Web**

El conocimiento de los principios de funcionamiento del antivirus Dr.Web, el que los usuarios pueden comprar durante los estudios, ayudará a afrontar mejor las amenazas informáticas.

Ofrecemos capacitación y certificación para los siguientes cursos:

Código del curso	Título del curso	Calificación	Audiencia objetivo
DWCERT-007	Análisis de infecciones activas y el tratamiento de los sistemas infectados mediante el software antivirus Dr.Web	Especialista certificado en el análisis de infecciones activas y el tratamiento de los sistemas infectados mediante el software antivirus Dr.Web	Los administradores de sistemas
DWCERT-004	Dr.Web AV-Desk v.6	Especialista certificado en administración de Dr.Web AV-Desk v.6	
DWCERT-001	Dr.Web para estaciones de trabajo y servidores de archivos Windows v.7	Especialista certificado en administración de Dr.Web para Windows v.7	
DWCERT-030-5	Dr.Web LiveCD (Dr.Web LiveUSB)	Usuario certificado Dr.Web LiveCD (Dr.Web LiveUSB)	
DWCERT-030-2	Dr.Web para Windows	Usuario certificado Dr.Web para Windows	Usuarios
DWCERT-030-3	Dr.Web para OS X	Usuario certificado Dr.Web para OS X	
DWCERT-030-10	Fundamentos de la protección antivirus. Protección de PC personales / notebook/netbook/ ultrabook y dispositivos móviles	Experto en fundamentos de la protección antivirus	Usuarios

Esto no es una lista completa de los cursos de formación “Doctor Web”.

CONTACTOS

Rusia

Doctor Web, S.L
125124, Moscú, C./ 3ª Yamskogo Polya, edf. 2, entrada 12A
Tel: +7 (495) 789-45-87 (Multicanal),
Fax: +7 (495) 789-45-97
www.drweb.com | www.av-desk.com | www.freedrweb.com | mobi.drweb.com

Alemania

Doctor Web Deutschland GmbH
Rodenbacher Chaussee 6, D-63457 Hanau
Tel: +49 (6181) 9060-1210
Fax: +49 (6181) 9060-1212
www.drweb-av.de

China

Doctor Web Software Company (Tianjin), Ltd.
Área de desarrollo económico y tecnológico de Tianjin, 4ª avenida, nº 80,
天津市经济技术开发区第四大街80号软件大厦北楼112
Tel: +86-022-59823480
Fax: +86-022-59823480
E-mail: D.Liu@drweb.com
www.drweb.cn

Francia

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

Japón

Doctor Web Pacific, Inc.
Edificio NKF Kawasaki 2F1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken 210-0005
Tel: +81 (0) 44-201-7711
www.drweb.co.jp

Kazajstán

Doctor Web – Asia Central, S.L
050009, Almaty, c./ Shevchenko / rincón con c./ Radostovtsa,165b/72g, oficina 910
Tel: +7 (727) 323-62-30, 323-62-31, 323-62-32
www.drweb.kz

Ucrania

Centro de soporte técnico "Doctor Web"
01601, Ucrania, Kiev, c/Pushkinskaya 27, planta 5, oficina 6
Tel./fax: +38 (044) 238-24-35
www.drweb.ua