Dr.WEB®
Hecho en Rusia

PROTEGE LO CREADO

Lista de tareas

para la seguridad informática
si los empleados cambian
al trabajo remoto

Documento para el administrador de sistemas

Lista de tareas para la seguridad informática si los empleados cambian al trabajo remoto

Antes de cambiar al trabajo remoto:

Acción	Nota de cumplimiento
Prepare una lista de software recomendado para instalar en los equipos del personal y formalícela en una circular interna. Cada empleado remoto debe consultar la circular.	
Prepare las distribuciones de los productos recomendados para el uso por el personal, y ubíquelas en un sitio disponible para el personal junto a las instrucciones de instalación, configuración recomendada y una lista de plugins. Asegúrese de que todos los programas han sido descargados, instalados y configurados correctamente.	
Recomiende al personal usar contraseñas seguras, en caso necesario, ayude a los empleados a seleccionar y cambiar la contraseña.	
Recomiende al personal instalar las actualizaciones de seguridad del SO usado y aplicaciones, en caso necesario, ayude a los empleados con eso. Controle el cumplimiento de esta tarea.	
Asegúrese de que los servicios de trabajo de la empresa están disponibles desde fuera de la oficina. Valore la capacidad de los canales de Internet y de los canales de comunicación de seguridad para ver si es suficiente para el trabajo remoto de Sus empleados.	
Minimice el número de los servicios de la empresa disponibles desde fuera. Cada uno es un posible objetivo de un ataque. En caso necesario, desactive los procesos de negocios no seguros no imprescindibles temporalmente. Escanee Sus recursos en busca de vulnerabilidades, para estar preparado a los ataques DDoS de los malintencionados.	
Si duda de cumplimiento de las medidas de seguridad por algunos empleados, para minimizar el riesgo asigneles las tareas no vinculados al trabajo con datos importantes.	
Para evitar la recepción y el envío de los mensajes infectados los empleados deben trabajar con el correo a través del servidor de correo de la empresa, asegure esta posibilidad.	
Asegure un escaneo antivirus de los mensajes de correo a nivel de servidor de correo en busca de programas maliciosos y spam.	
Instale los medios de seguridad en los dispositivos de trabajo remoto – un antivirus, un antispam, un Firewall, un medio de restricción de acceso a los recursos no seguros. Si no es posible instalar de forma remota y configurar los medios de protección, prepare para los empleados las distribuciones de los medios de seguridad, las claves de licencia, infórmelos sobre el procedimiento de instalación de las mismas, así como sobre la configuración recomendada.	
Recomiende al personal actualizar el firmware del router de hogar.	

La configuración del antivirus debe excluir la posibilidad de un cambio deliberado de las opciones del funcionamiento del programa (por ejemplo, por los miembros de la familia de los empleados). Informe a los empleados sobre cómo realizar la configuración y controle la realización de esta tarea.	
Recomiende al personal trabajar solo con permisos de usuario y no de administrador. Explíqueles los riesgos de trabajo con permisos de administrador. Recomiende usar otra cuenta de usuario para trabajar con documentos corporativos.	
Configure las restricciones del Control de oficina para la cuenta usada por los empleados para el trabajo para evitar el acceso del personal a los recursos maliciosos.	

Al instalar la protección antivirus en los dispositivos del persona

La protección antivirus de los equipos y dispositivos usados para el trabajo remoto y a los cuales pueden acceder los terceros (miembros de la familia etc.) puede consistir tanto en versiones de productos antivirus Dr.Web para un solo usuario sin administración centralizada, como en un sistema de protección antivirus centralizada de la empresa.

El uso de la protección administrada de forma centralizada supone menos riesgos para la empresa porque tanto un empleado como las personas que pueden acceder a su PC o móvil, de forma predeterminada no pueden desactivar los medios de seguridad ni cambiar su configuración. Eso evitará posibles hackeos de la red de la empresa y robos de datos.

- Si para la protección de los empleados remotos se usan soluciones sin administración centralizada:

Acción	Nota de cumplimiento
Proporcione el número requerido de licencias o archivos de claves a los empleados, proporcione el acceso a las distribuciones requeridas para los mismos si los empleados solos se encargan de la instalación.	
Antes de instalar la protección antivirus, se recomienda realizar un escaneo antivirus con la versión actual de Dr.Web CureIt!	
Compruebe si dispone de permisos de administrador para instalar el antivirus.	
Antes de empezar con la instalación de la protección antivirus corporativa, desinstale las soluciones de otros productores si las hay.	
Implemente el sistema de protección.	
En caso de detectar un software potencialmente peligroso incompatible con el agente antivirus Dr.Web Enterprise Security Suite, elimínelo.	
Controle el resultado de implementación de la protección y la configuración realizada.	
Realice un escaneo antivirus de las estaciones del personal.	

- Si los dispositivos y los equipos del personal forman parte del sistema de administración de seguridad centralizada:

Acción	Nota de cumplimiento
Compruebe si dispone de permisos de administrador para instalar el antivirus.	
Instale todas las actualizaciones de seguridad requeridas en los dispositivos y los equipos.	
Antes de instalar el agente antivirus Dr.Web Enterprise Security Suite, se recomienda realizar un escaneo antivirus con la versión actual de Dr.Web CureIt!	
Antes de empezar con la instalación de la protección antivirus corporativa, desinstale las soluciones de otros productores si las hay.	
Configure el servidor antivirus Dr.Web si el personal se conecta directamente al mismo, o instale un servidor proxy antivirus.	
Cree los grupos separados Dr.Web para las estaciones protegidas del personal en la Red antivirus del Centro de control.	
Cumpla con las acciones requeridas de configuración de los grupos creados. Así, por ejemplo, si durante la instalación se requiere indicar las opciones de acceso al servidor antivirus o al proxy antivirus, permita las acciones correspondientes en el Centro de control.	
Añada al Centro de Control Dr.Web el archivo de claves o los archivos que aseguran la protección del número de empleados requerido.	
Cree el número requerido de las nuevas estaciones y proporcione a los empleados las distribuciones de los agentes antivirus según el esquema de implementación seleccionado.	
Controle el resultado de implementación de la protección y la configuración creada.	
En caso de detectar un software potencialmente peligroso incompatible con el agente antivirus Dr.Web Enterprise Security Suite, elimínelo.	
Realice un escaneo antivirus de las estaciones del personal.	
Use la funcionalidad del Centro de control Dr.Web para controlar la lista de actualizaciones instaladas y el software instalado por el personal. En caso de detectar software potencialmente peligroso, cree las reglas que prohíben su uso con el módulo Control de aplicaciones Dr.Web.	

Instrucciones detalladas sobre la protección remota con los medios de Dr.Web Enterprise Security Suite para personal que trabaja fuera de la oficina

Sobre la empresa Doctor Web

Doctor Web es un productor ruso de los medios antivirus de protección de la información bajo la marca Dr.Web. Los productos Dr. Web. se desarrollan a partir del año 1992. Es una empresa clave en el mercado ruso del software para asegurar la necesidad básica del negocio – la seguridad de información.

Doctor Web fue la primera empresa que ofreció un modelo de innovación de uso de antivirus como servicio en el mercado ruso y hoy día sigue siendo líder del mercado ruso de los servicios Internet de seguridad para proveedores de servicios de IT.

Los clientes confían en Dr.Web

La plantilla de Doctor Web la componen los expertos de varios ámbitos de seguridad informática, lo que permite a la empresa tomar en cuenta lo máximo posible las peculiaridades del funcionamiento de empresas de varios tamaños y perfil de actividad y ofrecer a los clientes los productos de calidad óptimos por precio total mínimo.
Entre los clientes de los productos de la empresa hay usuarios de hogar de todas las regiones del mundo y grandes empresas rusas, pequeñas empresas y corporaciones estratégicas. La geografía de los usuarios Dr.Web confirma la gran confianza en el producto desarrollado por los informáticos rusos de gran talento.

Véase un listado de solo algunos clientes de Dr.Web: https://customers.drweb.com.

¿Por qué Dr.Web?

Todos los derechos de las tecnologías Dr.Web pertenecen a la empresa Doctor Web. La empresa es uno de los pocos vendedores antivirus en el mundo que tiene sus propias tecnologías únicas para detectar y desinfectar los programas malintencionados, cuenta con su propio laboratorio antivirus, el servicio global de supervisión de virus y el servicio de soporte técnico.

125040, Rusia, Moscú, c/3 Yamskogo Polya, 2, edif. 12a
Tel.: +7 495 789–45–87 (multicanal), Fax: +7 495 789-45-977
https://www.drweb.com | https://curenet.drweb.com | https://free.drweb.com