Dr.WEB®
Realizzato in Russia

PROTEGGI CIÒ CHE CREI

Lista delle attività

per fornire la sicurezza informatica nel caso di trasferimento dei dipendenti al lavoro da remoto

Inviate questo documento al vostro amministratore di sistema

Lista delle attività per fornire la sicurezza informatica nel caso di trasferimento dei dipendenti al lavoro da remoto

Prima del trasferimento al lavoro da remoto:

Attività	Completata
Preparare una lista dei software consigliati per l'installazione sui computer dei dipendenti e approvarla per disposizione aziendale. Informare ciascun dipendente remoto sulla disposizione.	
Preparare i pacchetti di distribuzione dei prodotti consigliati per l'uso dai dispendenti e collocarli in una posizione accessibile per i dipendenti insieme alle istruzioni per l'installazione, le impostazioni consigliate e la lista dei plugin. Assicurarsi che i programmi siano stati scaricati, installati e configurati nel modo dovuto.	
Consigliare ai dipendenti di utilizzare password forti, se necessario, aiutarli a scegliere e cambiare la password.	
Consigliare ai dipendenti di installare gli aggiornamenti di sicurezza del sistema operativo utilizzato e delle applicazioni, se necessario, aiutarli a farlo. Controllare che l'attività sia stata completata.	
Assicurarsi che i servizi di lavoro aziendali siano accessibili al di fuori dell'ufficio. Determinare la larghezza di banda dei canali Internet e dei canali di comunicazione di riserva per valutare se sarà sufficiente per il lavoro dei dipendenti dall'esterno.	
Ridurre al minimo il numero di servizi aziendali disponibili esternamente. Ognuno di essi è un probabile bersaglio di attacco. Se possibile, disattivare i processi di business non sicuri a cui si può temporaneamente rinunciare. Eseguire un controllo della presenza di vulnerabilità nelle risorse, essere preparati per gli attacchi DDoS dei malintenzionati.	
Se esistono dubbi sull'osservanza delle misure di sicurezza dai singoli dipendenti, per ridurre al minimo il rischio, assegnare loro attività non connesse con l'utilizzo di dati importanti.	
Per evitare di ricevere e inviare messaggi infetti, i dipendenti devono utilizzare l'email attraverso il server di posta dell'azienda — fornire loro tale possibilità.	
Fornire una verifica antivirus dei messaggi a livello di server di posta per rilevare programmi malevoli ed email di spam.	
Installare sui dispositivi da cui verrà eseguito il lavoro remoto strumenti per la sicurezza informatica – antivirus, antispam, firewall, strumento per limitare l'accesso a risorse non sicure. Se gli strumenti di protezione non possono essere installati e configurati in remoto, fornire ai dipendenti i pacchetti di distribuzione dei software di sicurezza, le chiavi di licenza, le istruzioni su come installarli e sulle impostazioni consigliate.	
Consigliare ai dipendenti di aggiornare il firmware del router casalingo.	
Le impostazioni dell'antivirus devono escludere la possibilità di modifiche intenzionali ai parametri di funzionamento del programma (ad esempio, da parte dei membri della famiglia del dipendente). Dare istruzioni ai dipendenti come eseguire l'impostazione e controllare se l'attività è stata completata.	

Consigliare ai dipendenti di lavorare esclusivamente con i permessi di utente – non quelli di amministratore. Spiegare loro i rischi di un lavoro con i permessi di amministratore. Consigliare di utilizzare un account separato per il lavoro con i documenti aziendali.	
Configurare le limitazioni di Office control per l'account utilizzato dal dipendente per il lavoro in modo da prevenire l'accesso del dipendente a risorse malevole.	

Installazione della protezione antivirus sui dispositivi del dipendente

È possibile proteggere i computer e i dispositivi, che vengono utilizzati per il lavoro remoto e a cui possono avere accesso le terze persone (membri della famiglia ecc.), sia tramite le versioni dei prodotti antivirus Dr.Web per utente singolo senza gestione centralizzata e sia tramite il sistema di protezione antivirus centralizzata dell'azienda.

L'uso di una protezione centralmente gestita comporta meno rischi per l'azienda in quanto il dipendente e le persone che hanno accesso al suo PC o dispositivo mobile di default non hanno la possibilità di disattivare gli strumenti di sicurezza e modificarne le impostazioni. Ciò protegge dalla possibilità di violazione della rete aziendale e di furto dei suoi dati.

- Se per proteggere i dipendenti remoti, vengono utilizzate le soluzioni senza gestione centralizzata:

Attività	Completata
Rilasciare ai dipendenti il numero necessario di licenze o file della chiave, fornire loro l'accesso ai pacchetti di distribuzione necessari, se l'installazione verrà eseguita dai dipendenti stessi.	
Prima di iniziare a installare la protezione antivirus, si consiglia di eseguire una scansione antivirus tramite la versione aggiornata di Dr.Web CureIt!	
Controllare la presenza dei permessi di amministratore per l'installazione dell'antivirus.	
Prima di iniziare a installare la protezione antivirus aziendale, rimuovere soluzioni di altri produttori, se erano installate.	
Effettuare il dispiegamento del sistema di protezione.	
Se vengono rilevati software non compatibili con l'agent antivirus Dr.Web Enterprise Security Suite, software potenzialmente pericolosi, rimuoverli.	
Controllare i risultati del dispiegamento della protezione e le impostazioni effettuate.	
Eseguire una scansione antivirus delle postazioni dei dipendenti.	

- Se i dispositivi e i computer dei dipendenti vengono inclusi nel sistema di gestione centralizzata della sicurezza:

Attività	Completata
Controllare la presenza dei permessi di amministratore per l'installazione dell'antivirus.	
Installare gli aggiornamenti di sicurezza necessari sui dispositivi e computer.	
Prima di installare l'agent antivirus Dr.Web Enterprise Security Suite, si consiglia di eseguire una scansione antivirus tramite la versione aggiornata di Dr.Web CureIt!	
Prima di iniziare a installare la protezione antivirus aziendale, rimuovere soluzioni di altri produttori, se erano installate.	
Configurare un server antivirus Dr.Web, se i dipendenti si connetteranno direttamente ad esso, o installare un server proxy antivirus.	
Creare nella Rete antivirus del Pannello di controllo Dr.Web i singoli gruppi per le postazioni protette dei dipendenti.	
Eseguire le attività necessarie per configurare i gruppi creati. Così, se durante l'installazione, sarà necessario indicare le credenziali per l'accesso al server antivirus o al proxy antivirus, consentire le relative azioni nel Pannello di controllo.	
Aggiungere al Pannello di controllo Dr.Web uno o più file della chiave che forniscono la protezione del numero di dipendenti richiesto.	
Creare il numero di nuove postazioni richiesto e distribuire ai dipendenti i pacchetti di distribuzione degli agent antivirus in conformità allo schema di dispiegamento scelto.	
Controllare i risultati del dispiegamento della protezione e le impostazioni create.	
Se vengono rilevati software non compatibili con l'agent antivirus Dr.Web Enterprise Security Suite, software potenzialmente pericolosi, rimuoverli.	
Eseguire una scansione antivirus delle postazioni dei dipendenti.	
Utilizzare le funzionalità del Pannello di controllo Dr.Web per controllare la lista degli aggiornamenti installati e i software che vengono installati dai dipendenti. Se vengono rilevati software potenzialmente pericolosi, creare regole che ne vietano l'utilizzo tramite il modulo Controllo delle applicazioni Dr.Web.	

Istruzioni dettagliate sulla protezione remota dei dipendenti che lavorano al di fuori dell'ufficio tramite Dr.Web Enterprise Security Suite

L'azienda Doctor Web

Doctor Web — fornitore russo di software antivirus di protezione delle informazioni sotto il marchio Dr.Web. I prodotti Dr.Web vengono sviluppati fin dal 1992. L'azienda è un attore chiave nel mercato russo dei software studiati per soddisfare un'esigenza essenziale delle aziende — quella di sicurezza delle informazioni.

Doctor Web è stata la prima azienda ad offrire sul mercato russo il modello innovativo di utilizzo dell'antivirus come servizio e fino ad oggi rimane leader indiscusso del mercato russo dei servizi internet di sicurezza per i fornitori di servizi informatici. .

i fidano di Dr.Web

Grazie alla presenza nell'organico Doctor Web di esperti di varie problematiche di sicurezza delle informazioni, l'azienda può tenere conto, al livello massimo, delle particolarità di lavoro di aziende di varie dimensioni e con diversi profili di attività e offrire ai clienti la migliore scelta di prodotti di qualità con un costo totale minimo.
Tra i consumatori dei prodotti Dr.Web ci sono utenti privati da tutte le regioni del mondo e grandi imprese russe, piccole organizzazioni e aziende della spina dorsale. La geografia degli utenti di Dr.Web testimonia l'alta fiducia nel prodotto creato da programmatori russi di talento.

Ecco solo alcuni clienti di Dr.Web: https://customers.drweb.com.

Perché Dr.Web?

Tutti i diritti sulle tecnologie Dr.Web appartengono all'azienda Doctor Web. L'azienda è uno dei pochi fornitori di antivirus al mondo che possiedono le proprie tecnologie uniche di rilevamento e neutralizzazione di programmi malevoli; ha il proprio laboratorio antivirus, un servizio di monitoraggio dei virus globale e un servizio di supporto tecnico.

125040, Russia, Mosca, la 3° via Yamskogo polya, 2, 12a
Tel.: +7 (495) 789-45-87 (centralino), fax: +7 (495) 789-45-97
https://www.drweb.com | https://curenet.drweb.com | https://free.drweb.com