Dr.WEB®
seit 1992

DEFEND WHAT YOU CREATE

Checkliste

zur Gewährleistung einer sicheren digitalen Umgebung bei der Gestaltung von Remote-Arbeitsplätzen

Übermitteln Sie diese Checkliste Ihrem Systemadministrator.

Checkliste zur Gewährleistung einer sicheren digitalen Umgebung bei der Gestaltung von Remote-Arbeitsplätzen

Vorbereitung auf den Umstieg auf Homeoffice:

Aufgabe	Erledigt
Erstellen Sie eine Liste von empfohlenen Softwareprodukten, die auf private Computer der Mitarbeiter installiert werden sollen, und legen Sie sie in einer Richtlinie fest. Bringen Sie die Richtlinie den Mitarbeitern zur Kenntnis.	
Laden Sie die Installationsdateien aller empfohlenen Produkte zusammen mit Installations- und Konfigurationsanweisungen und einer Plugin-Liste auf eine für die Mitarbeiter zugänglichen Ressource hoch. Prüfen Sie, ob die Software ordnungsgemäß heruntergeladen, installiert und konfiguriert wurde.	
Machen Sie Ihre Mitarbeiter darauf aufmerksam, dass sie sichere Passwörter verwenden sollen. Helfen Sie ihnen bei Bedarf, ein Passwort zu wählen oder zu ändern.	
Empfehlen Sie Ihren Mitarbeitern, ihr Betriebssystem und verwendete Anwendungen zu aktualisieren. Helfen Sie ihnen dabei bei Bedarf. Stellen Sie sicher, dass die Aufgabe erledigt ist.	
Stellen Sie sicher, dass alle notwendigen Unternehmensdienste bei der Heimarbeit verfügbar sind. Stellen Sie sicher, dass die Bandbreite Ihrer Internetkanäle und redundanten Kommunikationskanäle dafür ausreicht, dass Ihre Mitarbeiter von zu Hause aus arbeiten.	
Reduzieren Sie die Anzahl der aus der Ferne verfügbaren Unternehmensdienste auf ein Minimum. Jedes davon kann doch zum Ziel eines Cyberangriffs werden. Deaktivieren Sie unsichere Geschäftsprozesse, die Sie vorübergehend einstellen könnten, soweit möglich. Scannen Sie Ihre Ressourcen auf Sicherheitslücken. Stellen Sie sicher, dass sie vor DDoS-Angriffe durch Cyberkriminelle geschützt sind.	
Wenn Sie Zweifel haben, dass bestimmte Mitarbeiter Sicherheitsmaßnahmen einhalten werden, sehen Sie davon ab, ihnen Aufgaben zu stellen, die mit der Verarbeitung wichtiger Informationen verbunden sind.	
Damit infizierte E-Mails weder entsandt noch empfangen werden, stellen Sie sicher, dass der E-Mail-Verkehr über den Unternehmens-Mailserver erfolgt.	
Stellen Sie sicher, dass alle E-Mails auf Malware und Spam auf der Mailserverebene gescannt werden.	
Installieren Sie Schutzkomponenten (Antivirus, Antispam, Firewall, Tools zur Verhinderung des Zugriffs auf unzuverlässige Ressourcen etc.) auf Geräten, die Ihre Mitarbeiter bei der Heimarbeit nutzen werden. Falls eine Remote-Installation und -Konfiguration von Sicherheitslösungen unmöglich ist, stellen Sie den Mitarbeitern jeweilige Installationsdateien und Lizenzschlüssel sowie Installations- und Konfigurationsanweisungen zur Verfügung.	
Empfehlen Sie den Mitarbeitern, die Firmware ihres privaten Routers zu aktualisieren.	
Die Antiviruskonfiguration sollte jegliche unbefugte Änderungen der Softwareeinstellungen (z. B. durch Familienmitglieder der Mitarbeiter) ausschließen. Instruieren Sie Ihre Mitarbeiter über die Parametereinstellung und überprüfen Sie, ob die Software richtig konfiguriert wurde.	

Empfehlen Sie den Mitarbeitern, als Benutzer (nicht als Administrator) am Computer zu arbeiten. Erläutern Sie ihnen, welche Risiken bei der Arbeit mit Administratorrechten bestehen. Empfehlen Sie den Mitarbeitern, ein separates Benutzerkonto bei der Arbeit mit Unternehmensinformationen zu nutzen.	
Konfigurieren Sie die Komponente Office Control für das Benutzerkonto, das der Mitarbeiter bei der Heimarbeit nutzt, um Zugriff auf bösartige Ressourcen zu sperren.	

Installation der Virenschutzsoftware auf Geräte der Mitarbeiter

Sie können sowohl Dr.Web Einzellizenzen ohne zentrale Verwaltung als auch ein zentral verwaltetes Virenschutzsystem für private Computer und Geräte Ihrer Mitarbeiter einsetzen, auf die Dritte (z. B. Familienmitglieder) Zugriff haben können.

Die Verwendung des zentral verwalteten Schutzes birgt weniger Risiken für das Unternehmen, weil eine Deaktivierung oder Neukonfiguration der Virenschutzsoftware durch einen Mitarbeiter oder dritte Personen, die Zugriff auf seinen PC oder sein Smartphone haben, in diesem Fall unmöglich ist. Dies ermöglicht es, Ihr Unternehmensnetzwerk vor Hackerangriffen und Datendiebstahl zu schützen.

- Falls Sie Sicherheitslösungen ohne zentrale Verwaltung zum Schutz von privaten PCs und Geräten Ihrer Mitarbeiter einsetzen:

Aufgabe	Erledigt
Stellen Sie Ihren Mitarbeitern die notwendige Anzahl von Lizenzen oder Schlüsseldateien zur Verfügung. Geben Sie den Mitarbeitern Zugang zu Installationsdateien, falls sie die Software selbständig installieren sollen.	
Wir empfehlen, Geräte und PCs vor der Installation anderer Virenschutzprodukte mithilfe der aktuellen Version von Dr.Web CureIt! zu scannen.	
Stellen Sie sicher, dass Sie über Administratorrechte verfügen, um ein Virenschutzprogramm zu installieren.	
Wenn Antivirenlösungen anderer Hersteller auf einem Gerät installiert sind, löschen Sie sie, bevor Sie ein Unternehmens-Virenschutzprogramm installieren.	
Installieren Sie die Virenschutzsoftware und konfigurieren Sie das Sicherheitssystem.	
Falls potenziell gefährliche oder mit Dr.Web Enterprise Security Suite inkompatible Anwendungen erkannt wurden, löschen Sie diese.	
Stellen Sie sicher, dass die Software ordnungsgemäß installiert und konfiguriert ist.	
Scannen Sie Workstations der Mitarbeiter auf Viren.	

- Falls Sie zentral verwaltete Sicherheitslösungen zum Schutz von privaten PCs und Geräten Ihrer Mitarbeiter einsetzen:

Aufgabe	Erledigt
Stellen Sie sicher, dass Sie über Administratorrechte verfügen, um ein Virenschutzprogramm zu installieren.	
Installieren Sie notwendige Updates auf PCs und Geräte der Mitarbeiter.	

Wir empfehlen, Geräte und PCs vor der Installation von Dr.Web Enterprise Security Suite mithilfe der aktuellen Version von Dr.Web CureIt! zu scannen.	
Wenn Antivirenlösungen anderer Hersteller auf einem Gerät installiert sind, löschen Sie sie, bevor Sie ein Unternehmens-Virenschutzprogramm installieren.	
Konfigurieren Sie einen Dr.Web Antivirenserver, falls Geräte der Mitarbeiter direkt an diesen Server angeschlossen werden sollen, oder installieren Sie einen Proxyserver.	
Legen Sie einzelne Gruppen der zu schützenden Workstations der Mitarbeiter im Antivirus-Netzwerk des Dr.Web Verwaltungscenters an.	
Stellen Sie Parameter für die angelegten Gruppen ein. Wenn Zugriffsparameter für den Antivirenserver oder Antiviren-Proxy bei der Installation angegeben werden müssen, lassen Sie die entsprechenden Aktionen im Verwaltungscenter zu.	
Laden Sie die notwendige Anzahl von Schlüsseldateien in das Verwaltungscenter hoch, um Geräte aller Mitarbeiter zu schützen.	
Legen Sie die erforderliche Anzahl neuer Workstations an und stellen Sie Ihren Mitarbeitern Installationsdateien mit dem Antivirus-Agenten gemäß dem gewählten Implementierungsplan zur Verfügung.	
Stellen Sie sicher, dass die Software ordnungsgemäß installiert und konfiguriert ist.	
Falls potenziell gefährliche oder mit Dr.Web Enterprise Security Suite inkompatible Anwendungen erkannt wurden, löschen Sie diese.	
Scannen Sie Workstations der Mitarbeiter auf Viren.	
Im Dr.Web Verwaltungscenter können Sie die Liste aller von Mitarbeitern installierten Updates und Softwareprodukte einsehen. Falls eine potenziell gefährliche Anwendung erkannt wurde, erstellen Sie Regeln mithilfe des Moduls Dr.Web Application Control, um die Ausführung der Anwendung zu sperren.	

Weitere Informationen zum Schutz von Remote-Arbeitsplätzen mithilfe von Dr.Web Enterprise Security Suite

Über Doctor Web

Doctor Web Ltd. ist ein führender, weltweit agierender Hersteller von Antivirus- und Antispam-Lösungen. Das Doctor Web Team entwickelt seit 1992 Anti-Malware-Lösungen und beschäftigt weltweit 400 Mitarbeiter, davon 200 im Research & Development. Doctor Web ist nicht nur Pionier, sondern auch einer der wenigen Anbieter, die ihre Lösungen vollständig innerbetrieblich entwickeln.

Über 120 Mio. Nutzer vertrauen Dr.Web

Die umfangreiche Produktpalette von Doctor Web umfasst effiziente Lösungen zur Absicherung von einzelnen Arbeitsplätzen bis hin zu komplexen Netzwerken. Im deutschsprachigen Raum werden die Produkte von der Doctor Web Deutschland GmbH in Baden-Baden vertrieben. Zu den weltweit über 120 Mio. Nutzern von Dr.Web gehören Privatanwender, namhafte und international agierende, börsennotierte Großunternehmen, Banken und öffentliche Einrichtungen. Zahlreiche Zertifikate und Auszeichnungen zeugen von einem hohen Maß an Vertrauen in Dr.Web Antivirensoftware.

Hier finden Sie einige Kunden von Doctor Web: https://customers.drweb-av.de

Warum Dr.Web?

Alle Rechte an Dr.Web Technologien gehören Doctor Web Ltd. Das Unternehmen ist nicht nur Pionier, sondern auch einer der wenigen Anbieter, die ihre Lösungen vollständig innerbetrieblich entwickeln. Doctor Web Ltd. verfügt über hauseigene innovative Technologien und unterhält ein Virenlabor, einen globalen Virenüberwachungsdienst und Support-Dienst.

Quettigstraße 12
76530 Baden-Baden
Telefon: +49 (0) 170 488 40 28
https://www.drweb-av.de