10 praxiserprobte Tipps für ein **unterbrechungsfreies Remote-Arbeiten**

Remote-Mitarbeiter nutzen eine Vielzahl an Endgeräten, die mit dem Internet verbunden sind, um ihre Arbeit zu erledigen. Dies stellt eine Bedrohung für die allgemeine Sicherheitslage Ihres Unternehmens dar.

Christopher Sherman, Senior Analyst bei Forrester Research, sagt mit Bezug auf die Situation während der Corona-Krise: „Da ein Großteil der arbeitenden Bevölkerung dazu übergegangen ist, remote zu arbeiten, war die Endpoint-Sicherheit noch nie so kritisch wie heute."

Oder anders ausgedrückt: Wenn Endpoints und Remote-Mitarbeiter nicht sorgfältig verwaltet werden, setzen Sie Ihr Unternehmen einem Risiko aus.

Vor diesem Hintergrund ist jetzt der ideale Zeitpunkt, um Ihre Möglichkeiten für das **Arbeiten im Home Office bzw. außerhalb der Unternehmensräumlichkeiten** zu überprüfen und einige **Best Practices zum Thema „Remote Arbeiten"** umzusetzen. Wir haben die wichtigsten Tipps für Sie zusammengestellt, um Ihren Mitarbeitern sicheres und unterbrechungsfreies Arbeiten von Remote-Standorten aus zu ermöglichen:

1 Passen Sie den Prozess zur Bereitstellung geschäftskritischer Anwendungen an

Stellen Sie sicher, dass die empfohlenen Versionen Ihrer Geschäftsanwendungen auf allen Endgeräten installiert sind. Passen Sie – falls erforderlich – den Deployment-Prozess für Anwendungen an, indem Sie bestimmte Aktivitäten definieren, die vor oder nach der Bereitstellung durchgeführt werden. So können Sie beispielsweise festlegen, dass der zur Verfügung stehende Speicherplatz und die installierten Versionen vor dem Deployment überprüft werden, oder dass nach der Installation eine Verknüpfung erstellt wird.

2 Verbieten Sie die Verwendung von Anwendungen, die auf der schwarzen Liste stehen, und deinstallieren Sie diese automatisch

Erstellen Sie eine Liste mit Anwendungen, die Sie blockieren möchten, weil sie die Produktivität hemmen oder bei der Telearbeit zu Compliance-Problemen führen können. Legen Sie fest, dass solche Anwendungen automatisch deinstalliert werden, sobald sie auf einem Endpoint entdeckt werden und schaffen Sie eine Möglichkeit, wie Ihre Anwender bei Bedarf den Zugriff für bestimmte Anwendungen beantragen können.

3 Überwachen Sie die Administratorenrechte, um Angriffe durch Privilegienerweiterungen zu vermeiden

Bei der Installation von Software ist es teilweise erforderlich, dass Unternehmen ihren Mitarbeitern - je nach Bedarf - Administratorenrechte gewähren. Dabei gibt es keine Beschränkungen, welcher Benutzer welchen Zugriffsgrad benötigt. Behalten Sie deshalb die gewährten Administratorrechte immer im Auge und stellen Sie sicher, dass Sie diese widerrufen, wenn sie nicht mehr benötigt werden.

4 Nicht jede Schwachstelle muss sofort beseitigt werden. Bewerten Sie sie!

Auch wenn Sie das Gefühl haben, dass Sie mit Schwachstellen überhäuft werden: Nicht jede Schwachstelle muss sofort beseitigt werden. Viel wichtiger ist es, dass Sie die Bewertung jeder einzelnen Schwachstelle automatisieren, den Zustand Ihrer Systeme entsprechend konfigurieren und die Patches bereitstellen, die dringend erforderlich sind.

5 Lassen Sie sich von fachkundigen Technikern beraten, um eine schnellere Lösung zu finden

Oft arbeiten mehrere Techniker gleichzeitig an einem Ticket. In diesen Fällen ist es wichtig, dass sie sich untereinander austauschen, um die notwendigen Erkenntnisse gewinnen zu können. Um komplexe Probleme schneller zu lösen, sollten Sie sich von versierten Technikern beraten lassen.

6 Nutzen Sie die integrierten Kommunikationskanäle

Beschleunigen Sie Ihre Fehlerbehebung, indem Sie integrierte Kommunikationskanäle wie textbasierte Chats sowie Sprach- und Videoanrufe nutzen. Dies hilft Ihnen, die notwendigen Informationen von Endanwendern zu erhalten. Darüber hinaus können Sie Ihre User über jede Aktion, die an ihren Endpoints durchgeführt wurde, auf dem Laufenden halten.

7 Fassen Sie elementare Konfigurationen in einer Gruppe zusammen

Erstellen Sie Gruppen mit grundlegenden Konfigurationen, um Browser, USB-Geräte und Firewalls abzusichern, Treiber zuzuordnen oder Dateien, Ordner und Berechtigungen zu verwalten. Die Stromversorgung und standardisierte Bildschirmanzeigen sollten ebenfalls enthalten sein. Stellen Sie sicher, dass jedes neue System, das in Ihre Domäne hinzugefügt wird, über diese Konfigurationen verfügt.

8 Geben Sie Ihren Benutzern die Möglichkeit, Anwendungen selbst zu installieren oder zu deinstallieren

Eine unbeaufsichtigte Installation von Anwendungen kann sich für Mitarbeiter, die remote bzw. im Home Office arbeiten und nur wenig Bandbreite zur Verfügung haben, schnell als Fluch erweisen. Stellen Sie Software stattdessen lieber in einem Self-Service-Portal bereit und geben Sie Ihren Usern die Möglichkeit, Anwendungen je nach Bedarf und der ihnen zur Verfügung stehenden Bandbreite zu installieren.

9 Führen Sie eine Liste mit schädlichen ausführbaren Dateien und blockieren Sie diese vollständig

Trotz eines zuverlässigen Sicherheitssystems finden schädliche EXE-Dateien gelegentlich ihren Weg in ein Netzwerk. Sie sollten daher eine Liste mit schädlichen ausführbaren Dateien führen, die Sie vollständig blockieren, indem Sie den Hash-Wert der ausführbaren Datei angeben.

10 Beobachten Sie Neueinsteiger und greifen Sie bei Bedarf ein

Das Arbeiten an verschiedenen Standorten macht die Einarbeitung neuer Mitarbeiter zu einem mühsamen Prozess. Sie können neuen Technikern eine praxisorientierte Einarbeitungsphase ermöglichen und zu Demonstrationszwecken eingreifen und übernehmen.

Gerade beim Übergang zu neuen Arbeitsmodellen mit Telearbeit aus dem Home Office ist es wichtig, Fehler in mobilen Arbeitsumgebungen auszubügeln. Das erfordert praktikable Lösungen, um Endpoints effektiv verwalten und absichern zu können. Unified-Endpoint-Management-Lösungen wie **Desktop Central** unterstützen Sie dabei, die oben genannten Best Practices in Ihrem Unternehmen zeitnah und mit geringem Aufwand umzusetzen.

Starten Sie jetzt mit einer **kostenlosen 30-Tage-Testversion**