CISCO
SECURE

5 Tipps für Hybrid-Arbeit mit Sicherheit

Rund um den Globus halten Hybrid-Modelle zunehmend Einzug in die Arbeitskultur. Für Unternehmen und ihre Belegschaften bringt diese flexible Arbeitsweise neue Vorteile mit sich. Zugleich birgt sie aber auch neue Herausforderungen rund um die Frage, wie Teams und Unternehmensressourcen dabei weiterhin geschützt bleiben. Anhand der folgenden fünf Tipps gewährleisten Sie dies mühelos und ohne Kompromisse – im Büro, remote und auch überall dazwischen.

1 Über die Prinzipien sicherer IT-Nutzung aufklären

Wer den Arbeitsort flexibel wählen kann, erwartet, dass die IT ebenso flexibel ist: Sie soll an jeden Ort mitfolgen. Dadurch ist sie (und somit Ihr Unternehmen) jedoch neuen Bedrohungen ausgesetzt. Für Ihre Teams aus IT und Security gilt es daher, der Belegschaft zu vermitteln, wie sie an jedem Endpunkt ihrer hybriden Arbeitsumgebung sicher bleiben und potenziellen Risiken vorbeugen kann.

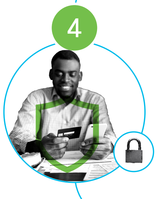
2 Personenidentitäten zweifelsfrei verifizieren

Unternehmen aller Art sollten mittels Multi-Faktor-Authentifizierung (MFA) eine einfache erste Sicherheitsebene für ihre Ressourcen einrichten. Das Prinzip: Der Zugriff auf diese wird nur all jenen gewährt, die zur Verifizierung ihrer Identität und des Status ihres Geräts zusätzlich zum Benutzernamen und Kennwort einen weiteren Nachweis (z. B. über ihr Smartphone) erbringen.

3 Standortunabhängig Zugriffssicherheit gewährleisten

Ein VPN sorgt über einen sicheren Tunnel zu Anwendungen dafür, dass Mitarbeitende sowohl unterwegs als auch im Homeoffice produktiv und vernetzt bleiben. Zugriff erhalten dabei nur autorisierte Benutzer:innen. Damit gewährleisten Sie ein adäquates Maß an Sicherheit, ohne dabei die Benutzerfreundlichkeit zu beeinträchtigen.

4 Bedrohungen an sämtlichen Eintrittspunkten abwehren



Die meisten Bedrohungen nehmen Benutzer:innen am Endpunkt ins Visier. Daher braucht es mehrere Verteidigungslinien: Eine erste, die auf DNS-Ebene greift, und eine letzte für Bedrohungen, die ihren Weg ins System finden konnten. Die erste Ebene blockiert für schädliches Verhalten bekannte Domänen und dämmt bereits durchgedrungene Malware ein, die letzte Ebene dient zum Schutz vor komplexeren Bedrohungen.

5 Sicherheit zentralisieren auf einer unkomplizierten, integrierten Plattform

Ein Flickenteppich aus Punktlösungen mit jeweils eigenen Bedienkonzepten ist kompliziert und der Sicherheit somit wenig zuträglich. Für effektive Sicherheit ist Einfachheit gefragt – so wie sie die SecureX-Plattform bietet, die Ihre Cisco Secure-Produkte nahtlos mit Ihrer Infrastruktur integriert.

Starker Schutz für Ihre Daten, ganz gleich, von wo aus Ihre Teams auf sie zugreifen: Mit Cisco Secure Hybrid Work vereinen Sie Sicherheit am Optimum mit Arbeit ohne Grenzen – unkompliziert, umfassend, jederzeit und überall.

Mehr zur Lösung unter
cisco.com/go/securehybridwork.

cisco The bridge to possible