6 entscheidende Überlegungen für sicheres hybrides Arbeiten

Die neue Normalität sieht so aus, dass Unternehmen ihre Geschäftsprozesse aufrechterhalten und ihren Mitarbeitern nicht nur jetzt sondern auch in Zukunft das hybride Arbeiten ermöglichen müssen. Sicheres hybrides Arbeiten ist nur mit schneller, benutzerfreundlicher Sicherheit und Konnektivität sowie mit ortsunabhängig (sowohl was die Menschen als auch die Daten betrifft) geschützten Transaktionen möglich. Die Benutzer müssen genauso bequem und produktiv arbeiten können wie in einem standardmäßig ausgestatteten Firmenbüro.

Die folgenden sechs Aspekte sind zu berücksichtigen, wenn Sie angemessene Sicherheitsvorkehrungen für Ihre hybriden Arbeitskräfte treffen möchten.

Anwendung der Zero-Trust-Grundsätze

Angriffe finden heutzutage auch in der Cloud statt, denn dort sind die meisten Daten gespeichert. Da hybride Arbeitskräfte über verschiedene Geräte und Netzwerke auf diese Daten zugreifen, ist „stillschweigendes Vertrauen“ keine Option mehr. Bei Zero Trust geht es um den Übergang von Vertrauen plus Überprüfen zu Erst prüfen, dann vertrauen. Er beruht auf dem Konzept einer kontextabhängigen Gewährung der geringstmöglichen Zugriffsrechte und einer kontinuierlichen Neubewertung der Umstände.

Wenn Sie mehr über Zero Trust wissen möchten:

Auslegung der Sicherheit auf maximale Sicht- und Kontrollierbarkeit der Datenumgebung in der Cloud

Der Schutz von Daten, Systemen und Geräten in einer hybriden Arbeitsumgebung erfordert die Transparenz und Kontrollierbarkeit der Cloud- und SaaS-Anwendungen (Statista zufolge verwendet ein durchschnittliches Unternehmen mehr als 110 SaaS-Anwendungen, die überwiegend nicht verwaltet werden, das heißt, es handelt sich um sogenannte „Schatten-IT“). Wenn die Aktivitäten aller Personen im Unternehmen gesehen, gesteuert und kontrolliert werden, verbessern sich Risikobewusstsein und Gefahrenerkennung erheblich.

Unseren Blog lesen

Augenmerk auf Benutzerfreundlichkeit

Die ideale Sicherheitslösung sollte alle genannten Aspekte berücksichtigen, ohne dabei die Benutzerfreundlichkeit bei hybrider Arbeitsweise zu kompromittieren. Vermeiden Sie Sicherheitslösungen, bei denen sich die Latenzzeiten stark erhöhen oder umständliche Datenumleitungen erforderlich werden. Außerdem sollten die Sicherheitskontrollen keine Systemressourcen binden oder zusätzliche Klicks nötig machen.

Lesen Sie weiter: Sicherheit muss die Netzwerkleistung nicht verlangsamen

Übergreifender Datenschutz für Anwendungsfälle jeder Art: Web, Cloud, E-Mail, private Anwendungen, Geräte

Hybrides Arbeiten hat die Vorstellung eines Sicherheitsperimeters überflüssig gemacht und Firmen sind nicht mehr an Grundstücksgrenzen gebunden. Ihre Sicherheitsmaßnahmen müssen den Datenverkehr aus dem Web, aus der Cloud, aus privaten Anwendungen und von Geräten berücksichtigen. CASB, SWG, ZTNA und alle anderen Aspekte von SSE-Architekturen (Security Service Edge) sichern die Datenspeicherung und -übertragung über all diese Vektoren.

Lesen Sie dieses Whitepaper über Datenschutz in der Cloud

Kontextabhängige Sicherheit

Durch hybrides Arbeiten gestalten sich die Interaktionen der Benutzer mit Anwendungen und Daten komplexer denn je. Daher müssen sicherheitsrelevante Entscheidungen über Zugriffsrechte und -richtlinien mehr denn je vom Kontext abhängig gemacht werden. Wenn Zugriffsrechte gewährt wurden, müssen die Sicherheitsteams kontinuierlich den Datenverkehr überwachen, kontextuelle Sitzungsanalysen durchführen, Entscheidungen anhand von externen Risikodaten treffen, Veränderungen in Risikoprofilen erkennen und gefährliche Aktionen neutralisieren.

Erfahren Sie mehr über die Plattform Cloud XD von Netskope.

Effektivere und kostengünstigere Sicherheit durch Konsolidierung der Anbieter

Ein durchschnittliches Unternehmen nutzt 76 Sicherheits-Tools. SSE kann sie nicht alle ersetzen, ermöglicht aber den Verzicht auf eine komplexe und umständlich zusammengestückelte Sicherheitsumgebung mit zahlreichen Anbietern. Eine zentrale Anwendungssuite von einem Anbieter, aber mit vielen Funktionen, ersetzt die alten, schlecht koordinierten Sicherheitslösungen. Die Zusammenführung der Kapazitäten erleichtert die Verwaltung, sorgt für eine einheitliche Richtliniendurchsetzung, optimiert die Verarbeitung des Datenverkehrs und verringert die Gesamtbetriebskosten.

Erfahren Sie mehr darüber, was die intelligente SSE von Netskope für Sie tun kann!

netskope

Netskope, ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert Cloud-, Daten- und Netzwerksicherheit neu, um Unternehmen bei der Anwendung von Zero-Trust-Prinzipien zum Schutz ihrer Daten zu unterstützen. Die Netskope Intelligent Security Service Edge (SSE)-Plattform ist schnell, einfach zu bedienen und sichert Menschen, Geräte und Daten an jedem Ort. Erfahren Sie mehr - www.netskope.com