Unternehmen müssen die Cybersecurity für Remote-Arbeiter jetzt erst recht vorantreiben

Die Pandemie hat Remote-Arbeit zur Pflicht gemacht und die digitale Transformation in den Unternehmen vorangetrieben. Dabei haben Unternehmen die Vorteile der Arbeit von zu Hause für sich und ihre Mitarbeiter erkannt. Deshalb werden die Netzwerkinfrastruktur und Zero Trust Access in Zukunft ein wichtiges Thema für ein nachhaltiges Homeoffice sein.

Auch wenn es auf den ersten Blick vielleicht wie eine Mammutaufgabe erschien, war die Implementierung von stabilen und sicheren Massnahmen für die Remote-Work zumindest technisch nicht so schwierig, wie viele Unternehmen es zunächst vermutet haben. Mit sorgfältiger Planung und den richtigen Technologiepartnern konnten sie diese Herausforderung schnell überwinden und ihre Strategie zur Remote-Work umsetzen oder erweitern. Unternehmen haben erkannt, dass es viele Gründe dafür gibt, das Arbeiten von zu Hause zu ermöglichen oder diese Möglichkeit sogar auszubauen. Remote-Work wird für viele Unternehmen Normalität und zu einem Grundpfeiler für zukünftige Unternehmensprozesse werden.

Franz Kaiser, Country Manager Switzerland bei Fortinet (Bild: Fortinet)

Dezentrale Arbeit und dynamische Infrastrukturen fordern volle Aufmerksamkeit

Damit Remote-Work nachhaltig bleibt, müssen Unternehmen ihr Netzwerk in den Mittelpunkt stellen, damit sie weiter expandieren können. Das bedeutet, dass ihre Netzwerkinfrastruktur dynamische Veränderungen und die Integration neuer Technologien ermöglicht sowie über integrierte und automatisierte Sicherheitsfunktionen verfügt. Das ist die Voraussetzung dafür, die Komplexität des Netzwerks langfristig zu reduzieren und die Effizienz des Unternehmens zu steigern.

> **“ Remote-Work wird für viele Unternehmen Normalität werden.**

Neben der Flexibilität des Netzwerkes ist Zero-Trust-Access ein zweiter Pfeiler, auf den Organisationen ihre Remote-Work-Strategie aufbauen sollten, um langfristig erfolgreich zu sein. Das liegt zum einen daran, dass Unternehmen mittlerweile erkannt haben, dass ihre VPN-Tunnel alle Nutzer erkennen und verifizieren müssen. Zum anderen gibt es eine Vielzahl an Nutzern, die über viele verschiedene Geräte Zugang zum Unternehmensnetzwerk haben. Die Fähigkeit, alles in diesem Netzwerk zu verstehen und zu erkennen, ist deshalb zu einem entscheidenden Faktor geworden, den Ansprüchen der Remote-Work gerecht zu werden.

Das Recht auf eine Verbindung mit dem Unternehmensnetzwerk kann einem Benutzer, einem Prozess oder einem Gerät nicht standardmässig erteilt werden. Vielmehr sollte bei jeder Appplikationsverbindung eine sichere Authentifizierung durchgeführt werden. Während eines solchen Vorgangs wird genau geprüft, ob eine Anfrage legitim ist, welchen Zweck sie verfolgt und wie sich die Verbindung verhält. Wenn eine Sicherheitslücke oder eine ungewöhnliche Aktivität entdeckt wird, muss das Gerät isoliert und die potenzielle Bedrohung in Sekundenbruchteilen bewertet werden.

Die Remote-Arbeit etabliert sich als Normalität. Deshalb sind dynamische Netzwerkinfrastrukturen und Zero-Trust-Access-Richtlinien ein kritischer Erfolgsfaktor für den langfristigen Erfolg.

Weitere Informationen:
www.fortinet.com