Remote Excellence

Sebastian Lenhard

– Portfolio Unit Manager – IT-Architekturen & IT-Technologien –

Zero Trust - Vertraue nichts und niemandem!

Die IT entwickelt sich ständig weiter. Das Unternehmensnetzwerk hört schon lange nicht mehr an der Unternehmens-Firewall auf. User haben mittlerweile mehr als ein Endgerät, von dem sie auf Unternehmensdaten zugreifen – zu jeder Zeit und von überall. Ein Szenario bei dem die IT-Security und Operation-Teams kaum noch hinterherkommen.

Die bridgingIT GmbH hilft Ihnen dabei diesen Entwicklungsschritt mitzugehen. Es gibt verschiedene Ansätze, die dabei helfen, Support- und Betriebs-Strukturen zu entlasten, mehrere Endgeräte zu verwalten, Ihre User zu "enablen" und somit effizienter zu werden.

„Zero Trust" ist einer dieser Ansätze. Dabei greifen die Clients aus potentiell ungesicherten Netzwerkzonen, wie z.B. dem Internet, auf Unternehmensdaten, Applikationen oder Cloud-Services zu. Dies ermöglicht, dass Zugriffe auf Unternehmensdaten nicht mehr zwingend zentral über die Unternehmensinfrastruktur, Bandbreite und Server laufen. Die Last auf VPN-Services verringert sich und hilft diese zu stabilisieren und für business-kritische Dienste verfügbar zu halten.

Technisch gesehen arbeitet man somit immer remote, egal in welchem Netzwerk man sich befindet.

Zero Trust - Vertraue nichts und niemandem!

Zero Trust-, Modern Management- und Evergreen-Ansätze sind die nächste Evolutionsstufe in der Verwaltung von Endgeräten. Drei zentrale Punkte sollte dabei berücksichtigt werden.

VPN – Nein danke!

Möglichst viele On-Premises Services und Applikationen sollten über das Internet und ohne VPN aufrufbar sein. „Always on"- VPN Konfigurationen gilt es zu vermeiden, um die Bandbreite des Unternehmens zu entlasten und für business-kritische Dienste vorzuhalten.

Security und Standards

Moderne Authentifizierungsmechanismen und Multi-Faktor Anmeldungen (MFA) helfen, die Identität und somit den Zugriff auf Ihre Daten besser zu schützen. Dieser Schutz kann mit Algorithmen kombiniert werden, welche je nach Zugriff entscheiden, ob ein zusätzlicher Faktor notwendig ist.
Der Einsatz von Standards, gerade bei Software, hilft Abhängigkeiten zu vermeiden und somit schnell auf Sicherheitslücken reagieren zu können. Die Hersteller liefern meist sehr schnell Security Patches, welche allerdings – aufgrund von Abhängigkeiten zu Systemen und anderer Software - oft erst mit Verzögerung installiert werden.

Zentrales Management und Monitoring

Zentrales Management und Plattformen helfen, schnell und skalierbar, Endgeräte und Services zu verwalten. Sei es das Installieren von Security Patches oder das Ändern einer relevanten Einstellung.
Zentrales Monitoring hilft in einer Zero Trust Umgebung ebenfalls dabei, „Gesundheitsdaten" der Systeme und Clients zu erhalten und Anomalien festzustellen.

Remote Excellence @bridgingIT

Unsere Leistungen und Kompetenzen

Als mitdenkender Partner adressieren wir die relevanten Gestaltungsebenen in Unternehmen mit einem klaren Umsetzungsfokus. Unser modulares Lösungs- und Leistungsangebot fokussiert Potenziale, Technologien und Transformation immer mit dem Menschen im Mittelpunkt.

Unseren Kunden stellen wir unsere Expertise und Erfahrung natürlich auch REMOTE durch unser Wertvollstes zur Verfügung – leidenschaftliche Berater*innen und erfahrene Profis: Damit ihre REMOTE EXCELLENCE zu einer nachhaltig attraktiven und erlebbaren Erfahrung für alle Beteiligten wird.

Erfahren Sie mehr