IT-SICHERHEIT 2021
Resilienz ist der Schlüsselfaktor

CYBER-ANGRIFFE
Wie können Unternehmen sich schützen?

DATENSCHUTZ
Vertrauensanker für die Digitalisierung

Handelsblatt Journal

Eine Sonderveröffentlichung von Euroforum Deutschland

NOVEMBER 2021 | WWW.HANDELSBLATT-JOURNAL.DE

euroforum

Medienpartner
Handelsblatt
Substanz entscheidet.

Advertorial

IT-Security – Die Zukunft ist Software

Agilität und flexibles Handeln als Erfolgsfaktoren für Business Continuity

von Benjamin Isak

Der schnelle Übergang zum Homeoffice im Jahr 2020 und der weiter anhaltende Wechsel auf hybride Arbeitsmodelle stellen nicht nur Unternehmen branchenübergreifend vor komplexe Herausforderungen bezüglich ihrer IT-Sicherheit. Auch der gesamte öffentliche Sektor wie Behörden und Ministerien, die zu jeder Zeit essenzielle Services für Land und Bevölkerung unterbrechungsfrei erfüllen müssen, stehen unter Zugzwang.

Dabei steigt naturgemäß der Druck auf die IT- und Security-Teams. Die Business Continuity muss zu jeder Zeit gewährleistet sein und gleichzeitig sollen Mitarbeiter im Homeoffice oder unterwegs sicher, flexibel und komfortabel arbeiten können.

Um dies zu erreichen, sollte man in Sachen IT-Sicherheit auf skalierbare Software-Lösungen setzen und dies sowohl im Enterprise-Bereich, als auch bei der Kommunikation von Verschlusssachen (VS-NfD) bei Behörden und geheimschutzbetreuten Unternehmen.

Schnelligkeit gewinnt!

Eine wesentliche Herausforderung stellt die Reaktionsgeschwindigkeit im Handeln dar: Wie zügig und robust kann ein Unternehmen reagieren, wenn von heute auf morgen die Anzahl der Mitarbeiter im Homeoffice stark erhöht werden muss? Was bedeutet dies für eine vorhandene Remote-Access-/Enterprise-VPN-Infrastruktur? Hierbei unterscheidet man, wo und wie die Umgebung konzipiert ist und betrieben wird:

- **OnPremise**
  Das Unternehmen betreibt alle Netzwerk-Lösungen und Anwendungen selbst in den eigenen Räumlichkeiten oder dem eigenen Rechenzentrum.

- **In der Cloud**
  Jegliche Netzwerk-Infrastrukturen und Anwendungen laufen in der Cloud und werden dort gehostet, gegebenenfalls werden sie sogar von Dritt-Anbietern betrieben.

- **Hybrid**
  Hierbei handelt es sich um einen Mischbetrieb aus Cloud und OnPremise.

Arbeiten Sie schon oder warten Sie noch?

Egal welches Betriebsmodell man wählt: Software schafft den entscheidenden Vorteil. Besonders bei Fragen der Skalierbarkeit und Lieferzeiten hat eine Software-Lösung für Enterprise-VPN die Nase vorn. In den aktuell schwierigen Zeiten mit globalem Chipmangel sowie massiv gestörten Lieferketten kann Hardware, wie beispielsweise ein Gateway für Remote-Access, im Zweifel gar nicht oder erst nach Monaten geliefert werden.

Zeit, die gerade dann nicht vorhanden ist, wenn eine Infrastruktur für gestiegenen Homeoffice-Bedarf unvorhergesehen schnell erweitert werden muss. Wie es sich hierbei mit der Aufrechterhaltung der Geschäftskontinuität und der Flexibilität in den Handlungsmöglichkeiten als Unternehmen verhält, liegt auf der Hand.

Betrachtet man den gleichen Fall unter Einsatz einer rein softwarebasierten Enterprise-VPN-Lösung, stellt sich das Szenario völlig anders dar. Und dabei ist es nicht von Belang, wo oder in welchem Betriebsmodell die Lösung läuft.

Zur Erweiterung einer Remote-Access-Infrastruktur ist der Prozess teils aufwendig, wenn Hardware zugekauft und konfiguriert werden muss. Wer hingegen softwarebasiert aufgestellt ist, kann seinen Anbieter direkt kontaktieren und innerhalb von Minuten durch Software- und Lizenzbereitstellung die Infrastruktur erweitern, wenn nicht sogar die Userzahl verdoppeln. Hierdurch kann Mitarbeitern in kürzester Zeit ein sicherer und performanter Zugang zum unterbrechungsfreien Arbeiten von überall ermöglicht werden.

Echte Virtualisierbarkeit und Skalierbarkeit machen den Unterschied

Zentralkomponenten wie Gateways und VPN-Management sind für alle Anwender vollumfänglich virtualisierbar und können hochverfügbar zugeschaltet werden. Die Geschäftstätigkeit ist somit zu jeder Zeit sichergestellt und unternehmerische Flexibilität bleibt bestehen. Eine Software-Lösung stellt also die Voraussetzung für nachhaltiges Handeln und echte Cyber-Resilienz dar!

Benjamin Isak,
Director Sales Public & Defence, NCP engineering GmbH

An dieser Stelle bieten etablierte deutsche Hersteller wie NCP engineering aus Nürnberg als Experten für IT-Security und Secure Communications passende und teils vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bis zur Geheimhaltungsstufe VS-NfD zugelassene Lösungen an. Unternehmen, Behörden und Ministerien sind mit diesen Produkten sicher und zukunftsfähig in Bezug auf digitale Souveränität und Cyber-Resilienz aufgestellt.

www.ncp-e.com