AUSZUG AUS... IT DIRECTOR AUSGABE 12|2021

Mit Sicherheit keine Kompromisse

Mit der Erweiterung des Netzwerks in das Homeoffice in Verbindung mit Cloud-basierten Anwendungen gestalten Unternehmen ihre Geschäftsprozesse zwar effizienter – doch die Flexibilität hat ihren Preis. Nur wer direkt bei der Infrastruktur und integrierten Services ansetzt, kann hier auch gewinnen.

> Das Bewusstsein für Sicherheit muss auf allen Ebenen vermittelt werden, insbesondere in hybriden Arbeitsumgebungen. Die Arbeit entkoppelt sich zunehmend von stationären Geräten. Mitarbeiter greifen dezentral auf dieselben Daten und Anwendungen in der Cloud zu, teilweise über mehrere Geräte außerhalb des Unternehmensstandorts. Dieser Punkt verdient Aufmerksamkeit, denn laut einer aktuellen, repräsentativen Studie des Digitalverbands Bitkom haben Schäden durch unabsichtlich handelnde Mitarbeiter besonders zugenommen. Unternehmen müssen dieser Realität gerecht werden und sich die Frage stellen, wer Zugriff hat und nicht von wo. Dieser identitätsbasierte Sicherheitsansatz versteht die Netzwerkgrenze also nicht mehr als physische, gerätegebundene Gegebenheit, sondern als personenbezogenes Zugriffsrecht auf Daten und Anwendungen.

Sicherheit fängt beim Provider an

Die lückenlose Überwachung des ein- und ausgehenden Datenverkehrs geht mit einem erheblichen Verarbeitungsaufwand einher, der viel Zeit und Ressourcen bindet. Um das zu bewältigen, gilt: Die Sicherheitsmaßnahmen und Filter müssen so früh wie möglich ansetzen. Bei Netzwerkanbietern wie Colt sind Security Services wie DDoS-Protection z.B. Teil des Backbones. Angriffe können so gestoppt werden, bevor sie Unternehmen erreichen. Eine zentrale Anlaufstelle für Netzwerk und Security schafft somit eine durchgängige Kontrollkette und reduziert Sicherheitslücken und Kosten, die bei der Nutzung mehrerer Anbieter für Security entstehen würden. Da sichere Verbindungen das Kerngeschäft von Netzwerkanbietern ist, legen sie zudem besonders hohen Wert auf die Sicherheit der eigenen Infrastruktur, die regelmäßig von eigenen Teams geprüft wird, um schnell und flexibel auf die sich stets weiterentwickelnden Cyberbedrohungsszenarien zu reagieren.

Die Firewalls, die wie bisher am zentralen Standort eines Unternehmens stehen, können die neue Art der hybriden Zusammenarbeit nicht mehr zuverlässig absichern – und werden ohne kontinuierliches Management gar selbst zum Sicherheitsrisiko. Managed Firewalls in Kombination mit einer permanenten Netzwerküberwachung, die vom Provider vollständig verwaltet werden, schaffen hier Abhilfe.

Mit Zusatzservices wie Content Application Security kann das Monitoring über den Datenverkehr hinausgehen und die potenziellen Schwachstellen wie ungepatchte Sicherheitslücken in älterer Software oder Geräten regelmäßig prüfen. Diese Lücken sind zwar einfach durch die Installation des neusten Patches des Herstellers zu beheben – doch den meisten Unternehmen fehlt es an Zeit und Ressourcen, die Vielzahl der Patches im Netzwerk auf dem neuesten Stand zu halten. Regelmäßige, automatisierte Schwachstellen-Scans geben hierbei einen Anhaltspunkt. Natürlich sollte man sich nicht nur auf einen effizienten Scan und Filter verlassen. Sicherheit muss schon in der Netzwerktopologie mitgedacht werden. Über Netzwerksegmentierung kann potenzieller Schaden qua zugrunde liegender Architektur eingedämmt werden.

> „Über Netzwerksegmentierung kann potenzieller Schaden eingedämmt werden."

Gerade für den Datenstrom in und aus der Cloud verschaffen in die Netzwerkumgebung integrierte und automatisierte Sicherheitsfunktionen einen großen Vorteil, um Geschäfts-

In dezentralen Arbeitsmodellen *ist Sicherheit besonders wichtig.*

prozesse sicher und ohne Performance-Einbußen umzusetzen. Über Secure Network Gateways werden Daten von jedem Standort aus in Public oder Private Clouds anhand vordefinierter Sicherheitsrichtlinien geleitet. Hardware-Applikationen halten in puncto Leistungsfähigkeit und Skalierbarkeit bei Weitem nicht mit und zwingen zu einer Auswahl des zu prüfenden Datenverkehrs, da er in der Gesamtheit manuell schlichtweg nicht zu bewältigen ist. Sicherheit bis zum Netzwerkrand für Unternehmen, die auf SD-WAN setzen, bieten darüber hinaus Services wie Remote Access über SD-WAN. Diese basieren auf Secure Access Service Edge (SASE). SASE beschreibt eine Netzwerkarchitektur, die SD-WAN-Funktionen mit Cloud-nativen Sicherheitsdiensten verbindet und so den Schutz aller Zugriffsarten und Applikationen bis zum Netzwerkrand (Edge) ermöglicht. Dabei können die Zugangsrechte für jeden Anwender über ein intuitives Online-Portal zugewiesen werden.

Turbo gezündet

Die Pandemie hat die Digitale Transformation von Unternehmen enorm beschleunigt. Was Unternehmen in Sachen Flexibilität auf den Weg gebracht haben, gilt es jetzt mit einem detailierten Sicherheitskonzept auf ein stabiles Fundament zu stellen. Ein umfassendes Monitoring des immer weiter zunehmenden Datenverkehrs in weit verzweigten, komplexen Netzwerken ist so nicht mehr zu stemmen. Hier bedarf es Komplettlösungen, die Backbone und leistungsfähige Services aus einer Hand anbieten, um Schaden möglichst früh abzuwenden. <

SVEN MÜLLER