



Security Architekturen mit Firewalltechniken

Abgabe 2

Beschreibung

Sie sind der IT-Leiter eines Unternehmens mit gewachsener IT Infrastruktur, die folgende Komponenten beinhaltet:

- Unternehmenszentrale
 - mit Server Infrastruktur
 - Internet Zugang
 - Webserver für die Unternehmenswebsite
 - Mailserver (Exchange)
 - Veraltete Firewall
- 10 Produktionsstandorte
 - Diese sind über eher langsame MPLS Leitungen an die Zentrale angebunden.
 - Für die Lagerverwaltung werden Barcode Lesegeräte mit WLAN eingesetzt
 - Die benötigten Services werden in der Zentrale bereitgestellt

Die Kosten für die MPLS Leitungen sind ein permanentes Problem bei Ihren Budget Verhandlungen. Außerdem ist derzeit ein Virenschutz nur auf den PCs und Servern vorhanden. In der Vergangenheit gab es Probleme mit Malware welche sich über E-Mail verbreitet hat, da die Virensignaturen der PCs veraltet waren. Die Mitarbeiter beschwerden sich zudem über das zunehmende SPAM Volumen und die schlechte Performance zwischen der Zentrale und den Produktionsstandorten. Vor einigen Wochen waren Sie das Opfer einer gezielten Ransomware Attacke, welche viele Clients und Fileshares verschlüsselt hat. Zum Glück haben Sie letztes Jahr die Backup Lösung erneuern können und die verschlüsselten Daten wiederherstellen können. Die Awareness für Security ist im Management daher hoch. Niemand will hier nochmals einen Stillstand der Produktionsstandorte riskieren.

Aufgabenstellung

Es steht eine Erneuerung der Firewall Infrastruktur für die Zentrale und die Außenstandorte an, mit folgenden groben Anforderungen:

- Der CFO des Unternehmens war mit einem Sales Mitarbeiter der Security Firma Forti-Alto Software Technologies beim Golfen. Von diesem hat er gehört, dass SD-WAN und im speziellen SASE die Zukunft der Standortvernetzung sind und sich damit auch noch Geld sparen lässt. Daher soll die Anbindung der Produktionsstandorte über diese Technologien evaluiert werden.

- Virenschutz für Mail und Web Traffic der Mitarbeiter
- Gezieltes Blocken von Applikationen
- Zugriffsmöglichkeit der Außendienstmitarbeiter auf den zentralen Exchange Server in der Zentrale. Der Leiter Vertrieb hegt allerdings schon lange den Wunsch den Exchange in die Azure Cloud zu verlegen und versucht demnächst zusammen mit Microsoft den CFO beim Golfen davon zu überzeugen. Daher die Lösung sollte Cloud ready sein.

Sie werden verschiedene Anbieter einladen Angebote für dieses Projekt zu legen. Erstellen Sie für die interne Bewertung der Angebote einen Kriterienkatalog („Muss“ und „Soll“ Kriterien). In diesem sollen die groben Anforderungen so detailliert wie möglich dargestellt werden, sodass eine Bewertung der Anbieter möglich ist.

Abgabe

- Deadline: 17.5.2020, 23:59h
- Upload im Moodle, max. 20 Punkte erreichbar
- Einzelübung, daher keine Gruppenarbeit
- Gerne können wieder Annahmen getroffen und kreativ gearbeitet werden