Aufgabe 4.1: Worauf noch zu achten wäre!

Bisher haben wir bereits SSH als sicheren Zugang zu quasi allen Rechnern genutzt. Je nach dem, wie Sie bisher vorgingen, konnte der Zugang auch tatsächlich von jedem Rechner zu jedem Rechner erfolgen. Dies ist oft nicht zugelassen und gerade Auditoren wollen einen sogenannten „Jump-Host“ in der Architektur erkennen können, zu dem sich die Administratoren erst einmal verbinden müssen, bevor Sie sich im Netzwerk weiter bewegen können.

Damit Sie sich bei dieser Aufgabe nicht ganz zuletzt noch aussperren, bleibt diese Aufgabe eine Trocken-Übung, also nicht an der Firewall umsetzen!

Überlegen Sie und begründen Sie Ihre Entscheidung:

- Wenn für Administratoren aus dem Internet ein SSH-Zugriff möglich sein soll, aber nur ein einziges Ziel erreicht werden darf, auf welches System (den sogenannten Jump-Host) würden Sie diesen gewähren?
- Welches Zugangsverfahren (Public Key oder Passwort) würden Sie fordern?
- Welche Systeme dürfen (gemäß Ihrer Entscheidung) die Administratoren ausgehend von dem ausgewählten System dann erreichen?
- Wenn Sie nicht den Zugriff auf alle System von dem Jump-Host aus zulassen, wie stellen Sie dann deren Administration sicher?

Aufgabe 4.2: Kryptographische Tunnel mit SSH

Anwendungsprotokolle unterstützen mehr und mehr kryptographische Verfahren. Außerdem kommen immer mehr VPNs zum Einsatz. Dennoch reichen in vielen Fällen für die alltägliche Nutzung bereits die kryptographischen Tunnel, die mit SSH aufgebaut werden können.

Konfigurieren Sie SSH und Firewalls so, dass folgendes erreicht werden kann:

- Bauen Sie eine SSH-Verbindung aus der „World“ zu einem Rechner in der DMZ (dem Netz zwischen den beiden Netzwerk-Firewalls) auf.
- Konfigurieren Sie vorher einen SSH-Tunnel ausgehend von Port 12345/tcp auf dem von Ihnen verwendeten Rechner in der „World“ zu einem **zweiten** Rechner in der DMZ auf Port 12345/tcp.
- Starten Sie dann auf diesem **zweiten** Rechner in der DMZ mit NETCAT einen Dienst, der auf 12345/tcp läuft und ganz normal Daten annimmt bzw. sendet.
- Starten Sie dann auf dem von Ihnen verwendeten Rechner NETCAT und verbinden Sie sich mit „localhost“ auf Port 12345/tcp.

Testen Sie die Verbindung! Machen Sie sich klar, auf welchen Netzwerk-Segmenten die Daten verschlüsselt (und authentisiert) übertragen werden, auf welchen die Daten im Klartext vorlegen und gefälscht werden können.