Sicherheitsdomänen

Jede Einheit (Ressort) ist als getrennte Sicherheitsdomäne auszubilden. Es ist wünschenswert, dass die Gliederung zumindest in größeren Ressorts in Teilbereichen (z.B. pro Sektion) stattfindet. Für jede Sicherheitsdomäne ist ein IT-Sicherheitsverantwortlicher zu benennen.

Die Definitionen der Security Domänen soll durch die CIOs der Ressorts geschehen. In dieser Phase sind auch die IT-Sicherheitsbeauftragten zu benennen. Diese müssen geeignet sein, den Benutzern Auskunft geben zu können und den Einsatz der Zertifikate im Ressort bzw. in der Domäne zu beaufsichtigen

Der Zugang zu den Sicherheitsdomänen ist über verschlüsselte Verbindungen bei einer Schlüssellänge von mindestens 100 Bit und mit Standardprotokollen (SSL, TLS bzw. IPSEC) vorzusehen. Darüber hinaus sind alle anderen Verbindungen mit Firewallmechanismen abzuschotten. Frei zugängliche Services (offenes Internet) sind im Sinne einer DMZ für den Innenbereich unzugänglich zu halten.

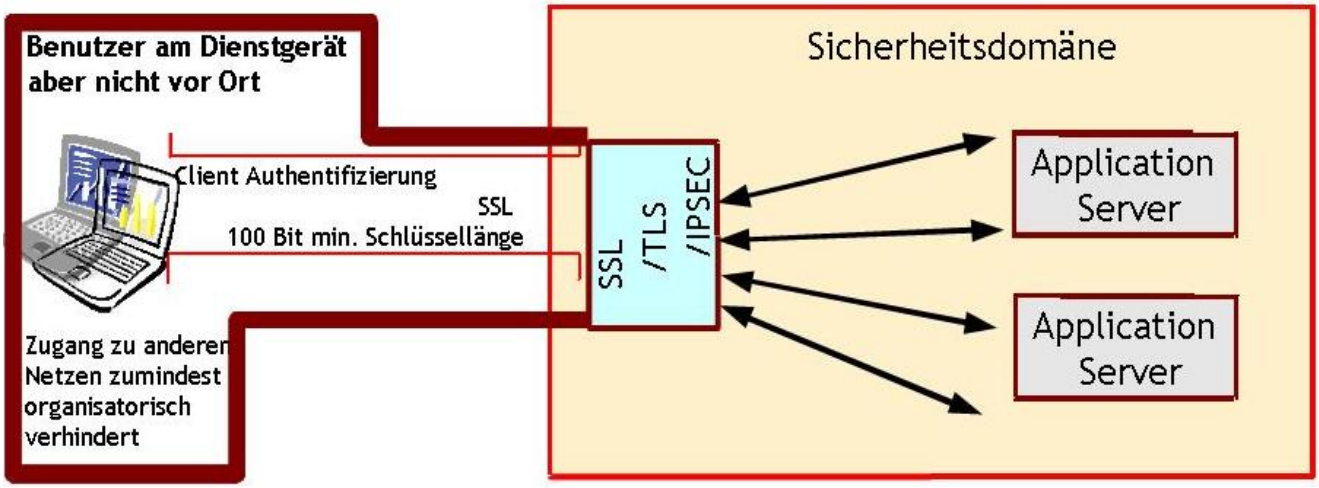

Bild: Zugang zu Sicherheitsdomänen

Erweiterte Sicherheitsdomänen

Neben den internen Sicherheitsdomänen können etwa für den Bereich der Heimarbeit oder für Außendienstarbeiten auch erweiterte Sicherheitsdomänen existieren. In diesen erweiterten Sicherheitsdomänen sind nur Services verfügbar, die beschränkte und lokale Capabilities besitzen. Dies muss jedenfalls für die Veränderung von Daten gesichert sein.

Wireless Zugänge sind ungeachtet Ihres Standortes wie Zugänge aus öffentlichen oder privaten ISPs zu behandeln. Damit gelten funktional die Einschränkungen wie bei Heimarbeitsplätzen. Eine Ausnahme bilden Installationen mit geeigneten Authentifizierungs- und Übertragungssicherungsmechanismen. Darunter zählen z.B. Radius AAA, der Einsatz von Zertifikaten und/oder IPSec, etc.

Zugang

Generell sollte das Intranet nach unterschiedlichen Vertraulichkeitsstufen differenzierbar sein und über eine PKI (*Public Key Infrastructure*) organisiert werden. Es ergibt sich somit eine hierarchische Zertifikatsstruktur für diverse Zugänge.

- offener Internetbereich
- Gruppenzertifikate
- Individualzertifikate

Prinzipiell kann mit einer geeigneten Zertifikatshierachie erreicht werden, dass alle Zugänge sicherheitstechnisch korrekt integriert werden können. Der Zugang zu Services ist somit für Gruppen und auch für einzelne Personen - je nach Bedarf - möglich.