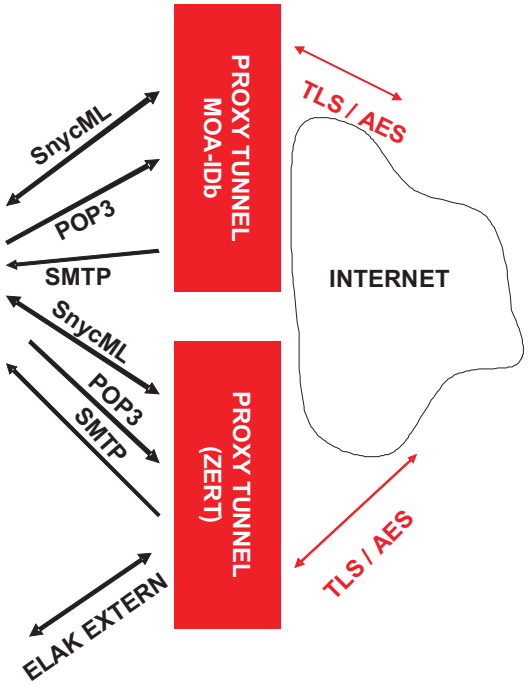
Einheitliches Vorgehensmodell



- Es sollten nur die wirklich notwendigen Zugänge freigeschaltet werden.
- Bei den externen Zugängen sollte ein möglichst einheitliches Sicherheitsmodell verfolgt werden.
- Schlüssel- und Zugangsmanagement sollten aus Effizienz- und Sicherheitsgründen einheitlich sein.

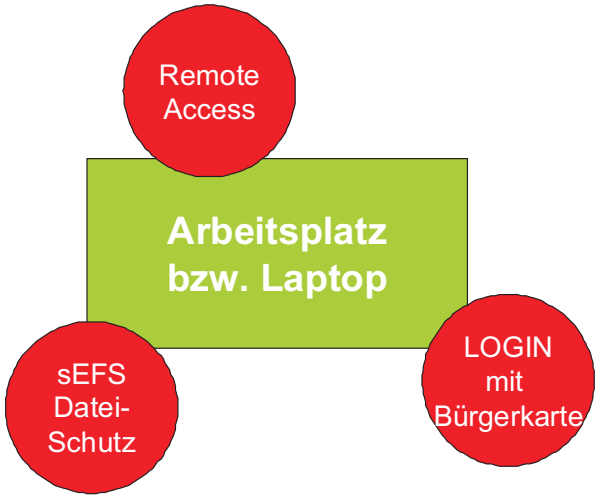
Die Zahl der unterschiedlichen Zugänge beeinflusst die Sicherheit und die Wartbarkeit des Gesamtsystems.

Jeder weitere unterschiedliche Zugang kann die Sicherheit nur verringern und nie erhöhen.

Schützenswerte Zugänge

- Für den normalen Arbeitsablauf werden neben dem frei zugänglichen Internet, Intranet, ELAK, E-Mail, Personenstandsverwaltung und Fachapplikationen notwendig.
- Der Schutzbedarf umfasst:
  - die eindeutige Identifikation
  - die Vertraulichkeit der Daten, die übertragen werden
  - die Vertraulichkeit der nach außen kommunizierten Daten
  - Sicherheit (Freiheit von Viren etc.) der in die Systeme eingehenden Daten

Elemente des Schutzes



- Gerät und Zugang müssen sicherstellen, dass nicht Unbefugte das Gerät benutzbar in die Hände bekommen.
- Firewall und Virenschutz müssen sicherstellen, dass keiner der Kommunikationspartner oder Systeme aus dem Fehlverhalten des Anderen Schaden nimmt.
- Das Dateisystem muss sicherstellen, dass nur Befugte Zugang zu temporär oder permanent verwendeten Daten bekommen.
- Die Verbindung muss die Vertraulichkeit gewährleisten.
- Die Verbindung muss sicherstellen, dass nur die gewünschten Partner an der Kommunikation beteiligt sind.
- Der Zugriff auf Daten der Services und Systeme muss einen Fehlzugriff wirksam verhindern.
- Der Wartungsfall darf nicht zur Weitergabe von Daten an Dritte führen.
- Der Verlust von einzelnen Komponenten darf nicht zum Datenverlust führen.

Werkzeuge zum Schutz

- **Identifikation und Dienstkarte**
  Der Zugang zu den Diensten mit MOA-ID und Dienstkarte bietet hinreichenden Schutz für die Dinge der täglichen Arbeit. Sofern keine Daten vom oder zum lokalen Gerät transportiert werden, kann mit dieser Schutzkomponente das Auslangen gefunden werden.

- **Verschlüsselungsschlüssel ohne drohenden Datenverlust**
  Werden vom bzw. zum lokalen Gerät Daten transferiert, so müssen alle relevanten Bereiche (z.B. Browsercache, passwortgeschützte Zertifikate etc.) verschlüsselt werden. Dazu sind Schlüssel einzusetzen, die den Datenverlust durch Backup verhindern und die für Notfälle Zugänge mit gleicher Verschlüsselungsqualität auch bei Verlust von Tokens erlauben.

- **Schutz von Bereichen des Dateisystems**
  mit dem dienstkartenbasierten „secureEFS" können Bereiche für den normalen Dienstgebrauch hinreichend geschützt werden.

- **Identifizierte und verschlüsselte Verbindungen**
  MOA-ID bietet eine Verschlüsselung mit hinreichender Schlüsselqualität für den normalen Dienstgebrauch. Es ist auch darauf zu achten, dass die Server die geeignete Mindestschutzklasse erfüllen und laufend geprüft werden.

- **Virenschutz und Firewalls**
  Virenschutz ist nach dem Stand der Technik einzurichten. Firewalls müssen sich auf die notwendigen Verbindungen beschränken und es muss das Vorhandensein von weiteren parallelen Verbindungen bei aufrechter Kommunikation wirksam verhindert werden.

- **Sichere Konfiguration**
  Die Sicherheit der Kommunikation der betroffenen Geräte muss dokumentiert sein.

- **Organisatorischer Schutz**
  Einzelne Elemente können auch mit organisatorischen Mitteln geschützt sein, wenn gleiche Wirksamkeit gesichert ist.

Weitere Nutzung

Werden die Geräte auch für andere Umgebungen genutzt (insbesondere E-MAIL und Onlineverbindungen), so sind besondere Sicherheitserfordernisse einzuhalten.

- Es sind andere Benutzeridentifikationen für andere Nutzungen zu verwenden.

- Die Verschlüsselungsbereiche müssen technisch geschlossen sein. Die Verbindungen zu den dienstlichen Angelegenheiten dürfen nicht aufrecht sein.

- Internetverbindungen können auch Teil der dienstlichen gesicherten Kommunikation sein. Vorzugsweise sollte diese über die gesicherte Verbindung und über das Ressort verbunden werden.

Achten Sie laufend auf auffälliges Verhalten.

Über Gefahren und deren Vermeidung wurde ich belehrt und bin in der Lage, die geforderten Sicherheitsmaßnahmen einzuhalten:

....., am .. .. 2005, ...

Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

Zentrum für sichere Informationstechnologie - Austria
A-SIT
Secure Information Technology Center - Austria

Externer Zugang Telearbeit und Laptops

E-Government Flyer Nr.201

DIGITALES ÖSTERREICH

Methoden und Werkzeuge
für den externen Zugang
zu internen Anwendungen

- Einheitliches Vorgehensmodell
- Schützenswerte Zugänge
- Schutzelemente
- Schutzwerkzeuge
- Weitere Nutzung