**(Externe) Firewall**

Beschreibung:

Eine Firewall, ob extern als Hardware oder als Software, kontrolliert die Datenübertragungen zwischen Computersystemen und Netzwerken. Externe Firewalls sind spezielle Hardware, auf denen die Software läuft. Die Hardware empfängt und sendet die Pakete, während die Software den Datenverkehr überprüft und regelt. (1)

Schnittstellen:

* LAN
* WLAN
* USB

Risiken:

Systemausfall 🡪 Bei einem Systemausfall kann der Datenverkehr zwischen Computer und Netz nicht mehr kontrolliert werden. Somit können unerwünschte Verbindungen aus dem Netz ungehindert stattfinden.

Datenmanipulation 🡪 In einem Firewall könnten Regeln für die Verbindung so umgeschrieben werden, sodass unerwünschte Verbindungen stattfinden.

Maßnahmen:

* Regelmäßig die Regeln überprüfen.
* Ersatz-Firewall aufstellen um auf Systemausfälle zu reagieren.

Quellen:

1. https://kompendium.infotip.de/netzwerkkomponenten-firewalls-und-dmz.html

**Netzwerkspeicher (NAS)**

Beschreibung:

In einem sogenannten NAS – Network-Attached-Storage werden Dateien gespeichert, die dann in einem Netzwerk zur Verfügung stehen. Somit können mehrere Teilnehmer des Netzwerkes gleichzeitig auf eine Datei zugreifen. (1.)

Schnittstellen:

* LAN
* WLAN
* USB

Risiken:

Datenverlust/Datenmanipulation 🡪 Bei Datenverlust/Datenmanipulation können mehrere Teilnehmer betroffen sein.

Datendiebstahl/Hacking 🡪 Dadurch, dass mehrere Teilnehmer auf dieselben Dateien Zugriff haben, oder durch Hacking, kann es zu Datendiebstahl kommen.

Virenbefall 🡪 Sobald Daten mit Viren auf dem NAS befinden, können sie sich sehr schnell und unkompliziert verbreiten.

Systemausfall 🡪 Bei einem Systemausfall ist kein Zugriff auf Daten mehr möglich.

Maßnahme:

* In regelmäßigen Abständen den Gesundheitszustand der Festplatte testen.
* Mit individuellen Passwörtern sichern um Änderungen vorzunehmen.
* Daten verschlüsseln.
* Dateien mit Cloud-Virenscanner überprüfen.
* IP-Blockade einrichten. (2.)
* VPN statt Port-Freigabe. (2.)
* Automatische Online-Backups.
* Firmware aktualisieren.

Quellen:

1. <http://www.searchstorage.de/definition/Network-Attached-Storage-So-funktioniert-ein-NAS>
2. https://www.sicherdigital.de/infos-fuer-eltern/server-im-heimnetz-absichern-und-konfigurieren-erwachsene

**Server**

Beschreibung:

Ein Server ist ein Programm oder ein Computer, der Programme, Daten oder andere Ressourcen bereitstellt, damit andere Clienten (Programme, Computer..) darauf zugreifen können. Dies erfolgt meistens über ein Netzwerk. (1.)

Schnittstellen:

* LAN
* WLAN
* UI

Risiken:

Datenverlust/Systemausfall 🡪 Bei einem Systemausfall des Servers, können wichtige Daten verloren gehen.

Datendiebstahl/Hacking 🡪 Datendiebstahl kann durch Hacking, oder auch durch eigene Mitarbeiter geschehen, welches ein großes Risiko für das Unternehmen darstellt.

Maßnahmen:

* Server immer aktuell halten. (2.)
* Zugriff nur von einem bestimmten Standort bzw. einer bestimmten IP-Adresse zulassen. (2.)
* Sichere, komplexe Kennwörter verwenden. (2.)
* Webapplikationen immer aktuell halten. (2.)
* Sperren von unsicheren php Funktionen. (2.)
* Standard-SSH-Port ändern.
* Root-Login verhindern.
* Verdächtige IP-Adressen blockieren.

Quellen:

1. <https://de.wikipedia.org/wiki/Server>
2. https://www.united-hoster.de/blog/2016/07/25/5-tipps-server-gegen-hacking-attacken-schuetzen/