AKADEMIE FÜR LEHRERFORTBILDUNG UND PERSONALFÜHRUNG
DILLINGEN

SCHULNETZ

Qualifizierung von Systembetreuerinnen
und Systembetreuern

Datensicherheit
im Unterrichtsbereich
und in der Schulverwaltung

– Szenarien und Problemstellungen –

Haben Sie schon Erfahrungen mit dem Verschlüsselungstrojaner oder mit defekten Festplatten gemacht? Sind Ihnen schon einmal Daten auf wundersame Art abhanden gekommen? Hatten Sie schon mal Bedenken, dass Ihre vertraulichen Daten in falsche Hände geraten könnten?

Nachfolgend sind häufig auftretende Problemstellungen genannt, die zu Datenverlusten oder Vertraulichkeitsverletzungen führen können und mögliche Lösungsansätze skizziert, die diese Probleme verhindern sollen.

In den SCHULNETZ-Lehrgängen „Datensicherheit im Unterrichtsbereich und in der Schulverwaltung“ werden diese Lösungsansätze in praktischen Übungen erprobt.

IMPRESSUM

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen
Autoren:	Georg Schlagbauer, Akademie Dillingen Barbara Maier, Akademie Dillingen
URL:	http://alp.dillingen.de/schulnetz
Mail:	schlagbauer@alp.dillingen.de
Stand:	Oktober 2016

SZENARIEN ZUR DATENSICHERHEIT

Versehentliches Löschen von Daten

Problemstellung:	Die Sekretärin hat versehentlich eine Datei überschrieben. Sie bemerkt dies sofort, benötigt diese Datei jedoch, um weiterarbeiten zu können.
Lösungsansatz:	Es existiert eine Datensicherung des gestrigen Tages. Idealerweise hat die Sekretärin lesenden Zugriff auf diese Datensicherung.
Problemstellung:	Der Schulleiter hat versehentlich Daten gelöscht. Er merkt dies erst nach einigen Monaten.
Lösungsansatz:	Es existiert eine Datensicherung, die einige Monate alt ist.

Defekte Hardware

Problemstellung:	Eine Festplatte im Server oder in einer NAS-Box wird defekt.
Lösungsansatz:	Es existiert eine aktuelle Datensicherung (bei einer defekten NAS-Box oder einer defekten Festplatte in einem Fileserver).
	Es existiert ein aktuelles System-Image (z. B. bei einem defekten Anwendungsserver oder einem defekten virtualisierten Server)

Vorbeugende Maßnahmen:

- Server-Festplatten, die für den Dauerbetrieb geeignet sind
- Erneuerung des Servers nach spätestens 5 Jahren
- Geeigneter Standort des Servers (Temperatur, Staubbelastung)
- Überwachung (Monitoring) des Servers oder der NAS-Box
- Festplatten im RAID-Verbund

Zugriff auf einen nicht mehr lauffähigen PC

Problemstellung:	Das Notebook eines Kollegen bootet nicht mehr bzw. arbeitet nicht mehr korrekt. Es liegen wichtige Daten darauf, die der Kollege benötigt.
mögliche Ursachen:	Bootreihenfolge oder Windows-Einstellungen verändert, Virus auf dem Notebook, Betriebssystem zerschossen, Arbeitsspeicher ist defekt, Festplatte ist defekt.
Lösungsansatz:	Notebook von einem Windows- oder Linux-Live-System booten und überprüfen, ob man noch auf die Daten zugreifen kann. Gegebenenfalls Daten sichern, Notebook auf Viren überprüfen. Die Festplatte als zweite Festplatte in einen anderen Computer einbauen und den Zugriff testen.

Diebstahl einer NAS-Box

Problemstellung:	Eine NAS-Box wird gestohlen. Auf der NAS-Box sind auch vertrauliche Daten, die nicht in falsche Hände geraten sollen.
Lösungsansatz:	Man legt mehrere Datensicherungen auf verschiedenen Systemen an unterschiedlichen Standorten an. Auf das Datenvolume der NAS-Box wird ein Passwort gesetzt und die Verschlüsselung aktiviert. Um das Datenvolume zu entschlüsseln muss nach dem Neustart einer NAS-Box das Passwort eingegeben werden.

Verlorener USB-Stick

Problemstellung:	Ein USB-Stick mit sensiblen Daten geht verloren. Die Daten sollten nicht in falsche Hände geraten.
Lösungsansatz:	Der USB-Stick wird verschlüsselt und mit einem Passwort gesichert. Wird der USB-Stick an einen fremden Computer benutzt, frägt Windows nach dem Passwort. Am eigenen Computer zu Hause muss das Passwort nicht eingegeben werden.
mögliche Programme:	Bitlocker (bei Windows-Systemen)

Verschlüsselungstrojaner

Problemstellung:	Ein Verschlüsselungstrojaner hat Dokumente auf dem lokalen PC und auf dem Dateiserver verschlüsselt.
mögliche Ursache:	Der übliche Verbreitungsweg für Verschlüsselungstrojaner sind E-Mail-Anhänge. Wenn ein solcher Anhang (z. B. ausführbare exe-Datei, Java-Script-Datei, Office-Dokument mit Makros) ausgeführt wird, wird der Trojaner aktiv. Er kann prinzipiell auf alles zugreifen, auf das der jeweilige Benutzer schreibenden Zugriff hat (lokale Dokumente, angeschlossene USB-Laufwerke, Serverlaufwerke, Cloud-Anbindungen).
vorbeugende Maßnahmen:	In Client/Server-Umgebungen kann detailliert geregelt werden, auf welche Bereiche ein Benutzer schreibenden oder nur lesenden Zugriff braucht.
Lösungsansatz:	Man benötigt eine Datensicherung auf die der Benutzer keinen schreibenden Zugriff hat, zumindest nicht in dem Moment, in dem der Trojaner aktiv ist. Es existiert eine Datensicherung auf einer externen Festplatte, die nicht am PC angeschlossen ist. Der Benutzer speichert seine Daten auf einem Server. Die regelmäßige Datensicherung erfolgt automatisiert vom Serversystem aus. Der Benutzer hat keinen schreibenden Zugriff auf die Datensicherung.

Versand von Dokumenten per E-Mail

Problemstellung:	Dokumente mit sensiblen Daten sollen per E-Mail verschickt werden.
Lösungsansatz:	Die Dokumente werden verschlüsselt. Das Passwort zum Entschlüsseln der Dokumente wird telefonisch mitgeteilt.
mögliche Programme:	7-Zip zum Packen und verschlüsseln der Dokumente

Vertrauliche Dokumente

Problemstellung:	Der Schulleiter macht sich persönliche Notizen zur Beurteilung von Lehrkräften. Außer ihm soll niemand diese Notizen lesen können.
Lösungsansatz:	Die vertraulichen Dokumente werden verschlüsselt. Nur der Schulleiter kennt das Passwort zum Entschlüsseln.
mögliche Programme:	integrierte Verschlüsselungsfunktion von Office-Dokumenten, VeraCrypt bei mehreren unterschiedlichen Dokumenten

Datenbanksicherung:

Problemstellung:	Auf einem Server liegen Datenbanken, mit denen regelmäßig gearbeitet wird (z. B. ASV). Die Datenbanken sollen täglich gesichert werden.
Lösungsansatz:	Ein Datenbank-Dump (z. B. mysqldump, pgdump) erstellt eine tägliche Sicherung auf dem lokalen System (mit Sicherungsdatum). Datenbank-Dumps, älter als eine Woche, werden automatisch gelöscht. Die Dumps werden in die automatische Sicherungskette des Server mit einbezogen.

Systemsicherung eines PC oder Notebook

Problemstellung	Durch die Installation von überflüssigen Programmen, durch Viren oder durch fehlerhafte Einstellungen wird ein PC oder Notebook extrem langsam oder läuft nicht mehr richtig.
Lösungsansatz:	Es existiert ein Image der Systempartition, das zurückgespielt werden kann. Bevor dies geschieht, sollte überprüft werden, ob auf der Systempartition Daten liegen, die der Anwender noch braucht.
mögliche Programme:	Alle Imaging-Programme (z. B. Drive Snapshot, Acronis, Partimage, etc.) Die Systeminstallation einzelner PCs oder Notebooks kann mit einem Imaging-Programm relativ gesichert und auch zurückgespielt werden. Der konkrete Aufwand ist vom jeweiligen Programm abhängig.

Systemsicherung eines Servers

Problemstellung	Von einem Anwendungsserver sollen regelmäßig Systemsicherungen angefertigt werden, damit der Server bei Bedarf einfach wiederhergestellt werden kann.
Lösungsansatz:	Am einfachsten ist die Serversicherung bei virtualisierten Servern (ESXi, Hyper-V). Die virtuellen Maschinen können automatisiert gesichert werden (z.B. Ghetto-VCB unter ESXi). Das Virtualisierungssystem selbst muss nicht gesichert werden, da es bei Bedarf sehr schnell wieder eingerichtet ist.

Sicherung von Daten mit Berechtigungen

Problemstellung:	Auf einem Windows-Server liegen Benutzerdaten in den Home-Verzeichnissen der einzelnen Benutzer. Bei der Datensicherung soll die Berechtigungsstruktur mit gesichert werden.
Lösungsansätze:	Die Sicherung erfolgt auf einem gleichartigen System, das die Berechtigungsstruktur kennt. Die Sicherung erfolgt mit einem Programm, das einen Container bildet, indem die Berechtigungen erhalten bleiben (z.B. .tar unter Linux, 7zip oder proprietäres Archiv unter Windows). Systemsicherung mit einem Imaging-Programm das den Zugriff auf einzelne Dateien erlaubt (z.B. Drive Snapshot).

FALLBEISPIELE ZUR DATENSICHERHEIT

Der Lehrerarbeitsplatz zu Hause

Die Unterrichtsvorbereitung liegt lokal auf einem Desktop-Computer oder auf einem Notebook. Für die Unterrichtsvorbereitung soll eine Datensicherung eingerichtet werden. Außerdem möchte die Lehrkraft auch in der Schule auf die Unterrichtsvorbereitung zugreifen können.

Datensicherung auf externe USB-Festplatten

Zur Datensicherung sind mehrere USB-Festplatten verfügbar. Die Datensicherung erfolgt auf die USB-Festplatten, die abwechselnd benutzt werden und nach der Datensicherung vom Computer getrennt werden. Wenn die USB-Festplatten groß genug sind, können auch mehrere Datensicherungs-Versionen gespeichert werden (Datenarchivierung).

Die Datensicherung erfolgt halbautomatisch auf „Knopfdruck“ (USB-Festplatte anstecken – Vorbereitetes Desktop-Icon zum Start der Datensicherung drücken – Nach Beendigung USB-Festplatte entfernen).

Ergänzungen zur Datensicherung:

Die regelmäßige Datensicherung kann vollständig automatisiert auf einer NAS-Box erfolgen, falls der Computer zum festgelegten Zeitpunkt läuft. Alternativ kann die Datensicherung auch halbautomatisch auf „Knopfdruck“ erfolgen (z. B. Icon auf dem Desktop mit „Backup / Shutdown“). Es bietet sich an, dass unterschiedliche Versionen auf der NAS-Box gespeichert werden (Tagessicherung, Monatssicherungen). Wenn die automatisierte Datensicherung mit einem anderen Benutzeraccount oder nicht über das SMB-Protokoll erfolgt, bietet dies eine zusätzliche Sicherheit (z. B. bei einem Verschlüsselungstrojaner).

Zugriff auf die Unterrichtsvorbereitung

Um auch in der Schule auf die Unterrichtsvorbereitung zugreifen zu können, bieten sich mehrere Varianten an:

> Die Unterrichtsvorbereitung wird auf einen USB-Stick synchronisiert. In der Schule wird mit dem USB-Stick gearbeitet. Zu Hause erfolgt wiederum eine Synchronisation. Der USB-Stick ist verschlüsselt, ohne Kenntnis des Passworts können die Daten nicht gelesen werden.

Die Unterrichtsvorbereitung wird mit einem Online-Speicher synchronisiert (Dropbox, Skydrive, Owncloud). In der Schule wird auf den Online-Speicher zugegriffen. Die Daten auf dem Online-Speicher sind verschlüsselt.
Die Unterrichtsvorbereitung zu Hause erfolgt auf einem Notebook, das der Lehrer mit in die Schule nimmt. Der Zugriff auf das Notebook ist mit Kennwörtern gesichert, gegebenenfalls kann zusätzlich die Datenpartition des Notebooks verschlüsselt sein.

Unterrichtsnetz einer kleinen Schule

Als zentraler Ablageort im Unterrichtsnetz dient eine NAS-Box. Auf dieser existieren Vorlagen- und Austauschlaufwerke mit unterschiedlichen Schreib- und Leseberechtigungen für Lehrkräfte und Schüler sowie ggf. persönliche Ablageorte der einzelnen Lehrkräfte. Die größte Datenmenge beanspruchen die Systemimages, die zur Wiederherstellung der Computer im Unterrichtsnetz dienen.

Datensicherung NAS-to-NAS

Als Backupserver dient eine zweite NAS-Box (automatische NAS-to-NAS-Sicherung). Gegebenenfalls können einzelne Sicherungen umbenannt werden (z. B. Backup_20161006), so dass dieser Zustand erhalten bleibt.

Zusätzliche Datensicherung auf USB-Festplatten

Viele NAS-Boxen bieten eine komfortable Sicherungsfunktion, mit der eine Datensicherung per Knopfdruck auf eine angeschlossene USB-Festplatte erfolgt.

Schulverwaltung einer kleineren Schule

Als zentraler Ablageort dient ein Windows-Server (ASV-Server und Datei-Server), auf den die Schulleitung und das Sekretariat Zugriff haben. Alle relevanten Daten befinden sich auf diesem Server, die Schulleitung und das Sekretariat wissen, dass sie alle Daten auf dem Server speichern sollen.

Datensicherung auf eine NAS-Box

Der Datenbereich des Servers wird täglich auf eine NAS gesichert, (Tagessicherung, Monatssicherung). Die Tagessicherung wird täglich überschrieben, gelegentlich wird eine Tagessicherung umbenannt (z. B. Backup_20161006), so dass dieser Zustand erhalten bleibt.

Die NAS-Box befindet sich nicht im selben Raum, wie der Server der Schule. Das Datenvolume der NAS-Box ist verschlüsselt und mit einem Passwort gesichert (Schutz der Daten bei einem Diebstahl der NAS).

Zusätzliche Datensicherung auf USB-Festplatten

Zusätzlich gibt es mehrere USB-Festplatten, die als Ergänzung zur Datensicherung des Servers benutzt werden (manuelle oder halbautomatische Sicherung).

ASV-Backup

Die relevanten Daten der ASV sind in einer Postgres-Datenbank gespeichert. Diese Datenbank wird täglich mit einem Dump (pgdump) gesichert, der Datenbank-Dump wird im Datenbereich des Servers abgelegt, so dass dieser in die normale Sicherungskette integriert ist.

Vertrauliche Daten der Schulleitung

Die Schulleitung speichert vertrauliche Daten in einer verschlüsselten Form auf dem Server ab. Dadurch werden diese Daten gesichert, sind aber nur lesbar, wenn das Passwort bekannt ist.