Vereinbarungen zur externen Technischen Administration bei der Musterschule

Wartungs- oder Reparaturarbeiten in der Schule

- Wartungs- und Reparaturarbeiten sind gegenüber den betroffenen Mitarbeitern oder der Schule rechtzeitig anzukündigen.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden. Es gelten die besonderen Bestimmungen der Vertraulichkeits- und Sicherheitsvereinbarung im Anhang.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, Firmenname sowie Name des Wartungstechnikers).
- Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Anlage zu überprüfen. Insbesondere die Rücknahme der für Testzwecke vorgenommenen Eingriffe ist zu kontrollieren.

Externe Wartungs- oder Reparaturarbeiten

- Werden IT-Systeme zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher physikalisch zu löschen. Ist dies nicht möglich, weil aufgrund eines Defekts nicht mehr auf die Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen Informationssicherheitsmaßnahmen zu verpflichten. Es sind vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.
- Bei der Durchführung externer Wartungsarbeiten muss protokolliert werden, welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden, wer dies veranlasst hat, was der Wartungs- bzw. Reparaturauftrag umfasst, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann das Gerät wieder zurückgebracht wurde. Um dies nachhalten zu können, ist eine Kennzeichnung der IT-Systeme oder Komponenten erforderlich, aus der zum einem hervorgeht, welcher Organisation diese gehören, und zum anderen eine eindeutige Zuordnung innerhalb der Organisation möglich ist.
- Beim Versand oder Transport der zu reparierenden Komponenten sollte darauf geachtet werden, dass Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf den IT-Systemen noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z. B. in verschlossenen Behältnissen oder durch Kuriere. Weiterhin müssen Nachweise über den Versand (Reparaturauftrag, Begleitzettel, Versandscheine) und den Eingang beim Empfänger (Empfangsbestätigung) geführt und archiviert werden.
- Bei IT-Systemen, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung, alle oder einige Passwörter

entweder bekannt gegeben oder auf festgelegte Einstellungen wie "REPARATUR" gesetzt werden, damit die Wartungstechniker auf die Geräte zugreifen können.
- Nach der Rückgabe der IT-Systeme oder Komponenten sind diese auf Vollständigkeit zu überprüfen. Alle Passwörter sind zu ändern. PC-Datenträger sind nach der Rückgabe mittels eines aktuellen Viren-Suchprogramms auf Computer-Viren zu überprüfen. Alle Dateien oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

Regelungen zur Fernwartung

Die Fernwartung von IT -Systemen birgt besondere Sicherheitsrisiken. Bei der Fernwartung ist zu unterscheiden, ob internes oder externes Wartungspersonal auf die IT-Systeme zugreift. Damit Administratoren IT-Benutzern schnell helfen können, ohne dass sie sich zum Aufstellungsort der jeweiligen IT-Systeme begeben müssen, werden bei der IT-Betreuung häufig Fernwartungszugänge genutzt. Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzliche Sicherungsmaßnahmen unumgänglich.

Das zu wartende IT-System muss die folgenden Sicherheitsfunktionen realisieren:

- Der Benutzer des IT-Systems muss dem Fernzugriff explizit zustimmen, z. B. über eine entsprechende Bestätigung am System. Er sollte alle Tätigkeiten während des Fernzugriffs beobachten.
- Das externe Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Werden dabei Passwörter unverschlüsselt übertragen, sollten Einmalpasswörter benutzt werden.
- Die Durchführung einer Fernwartung muss protokolliert werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.

Darüber hinaus können am zu wartenden IT-System noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,
- Einschränkung der Rechte des Wartungspersonals: Das Wartungspersonal sollte nicht die vollen Administrator-Rechte besitzen. Es sollte eine abgestufte Rechteverwaltung realisiert werden, bei Unix-Systemen ist außerdem M 2.33 *Aufteilung der Administrationstätigkeiten unter Unix* zu beachten, bei PC -Netzen M 2.38 *Aufteilung der Administrationstätigkeiten*
  (Das Wartungspersonal sollte nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind.)
- auf dem IT-System sollte für das Wartungspersonal eine eigene Benutzer-Kennung existieren, unter der möglichst alle Wartungsarbeiten durchgeführt werden,
- wird die Verbindung zur Fernwartungsstelle auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch einen "Zwangslogout" beendet werden.

Fernwartung über externe Netze oder durch Dritte

Fernwartung über externe Netze oder durch Dritte ist besonders kritisch. Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzlich zu den oben genannten Sicherheitsmaßnahmen folgende Punkte zu beachten:

- Bei einer Fernwartung über externe Kommunikationsverbindungen, müssen die Zugänge und die Verbindungen abgesichert werden. Das Fernwartungspersonal muss sich authentisieren und die übertragenen Daten müssen verschlüsselt werden. Beispielsweise kann die Anbindung per VPN oder exklusiv genutzte Verbindungen realisiert werden.
- Wenn dies technisch möglich ist, sollten alle Tätigkeiten während der Administration von Dritten durch eigene IT-Experten beobachtet werden. Beispielsweise können bei der Fernadministration eines Clients über eine graphische Benutzeroberfläche oft alle Ein- und Ausgaben am zu wartenden IT-System angezeigt und aufgezeichnet werden. Auch wenn Fernwartung durch Dritte genutzt wird, weil intern das Know-How oder die Kapazität nicht verfügbar ist, kann das externe Wartungspersonal nicht unbeaufsichtigt gelassen werden. Bei Unklarheiten über die Vorgänge sollte der lokale IT-Experte sofort nachfragen. Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.
- Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, also z. B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzer-Kennungen erfolgen.
- Alle Remote-Administrationsvorgänge müssen aufgezeichnet werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.

Es sind auch mit externem Wartungspersonal vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.