Richtlinie

Einsatz von Fernwartungssoftware an der Frankfurt University of Applied Sciences

Fernwartung von IT-Systemen birgt ein erhöhtes Sicherheitsrisiko für die IT-Landschaft und das Ausspähen sicherheitsrelevanter Daten. Dies gilt vor allem bei externem Zugriff oder bei der Nutzung von Fernwartung durch Dritte, nicht der Hochschule angehörendem Personal. Dieses Dokument stellt eine verbindliche Richtlinie für den Fall auf, dass auf den Einsatz von Fernwartungssoftware nicht verzichtet werden kann.

1. Der Einsatz von Software oder Techniken, die geeignet sind oder ausschließlich dem Zweck dienen, Schutzmechanismen der IT-Infrastruktur zu umgehen, sind generell verboten. Hierzu zählen insbesondere, aber nicht ausschließlich Remote-Administrationstools wie TeamViewer, VNC-Software oder Tunneling-Techniken.
2. Ausgenommen davon sind Verbindungen von Angehörigen der Hochschule über den zentralen VPN-Dienst oder administrative Zugriffe über Terminal-Server, die für diese Arbeiten freigegeben sind.
3. Ausgenommen sind zudem Zugriffe von Administratoren in lokalen Netzen als Ersatz von Vor-Ort-Support, soweit technisch sichergestellt ist, dass die Benutzer der Fernwartung explizit im Einzelfall zustimmen und die Möglichkeit der Fernwartung nur jeweils zeitlich befristet genutzt wird.
4. Weitere Ausnahmen sind genehmigungspflichtig. Der Antrag muss eine Begründung enthalten, warum auf die Fernwartung nicht verzichtet werden kann und aufzeigen, auf welchem Wege sowie durch wen die Fernwartung erfolgt. Der Antrag muss weiter darlegen, wie die einschlägigen Anforderungen aus dem Modul *„M 5.33 Absicherung von Fernwartung“* des BSI-Grundschutzkatalogs umgesetzt werden.
5. Findet ein Zugriff auf ein System statt, auf welchem personenbezogene Daten gespeichert oder verarbeitet werden, ist vor Genehmigung die Einhaltung der datenschutzrechtlichen Bestimmungen des HDSG, insbesondere des *§4 Verabeitung personenbezogener Daten im Auftrag* durch Vorlage bei der bDSB der Hochschule sicherzustellen.
6. Über die Genehmigung des Einsatzes der Fernwartungssoftware entscheidet der IT-Sicherheitsbeauftragte im Einvernehmen mit der Abteilung CIT und im Konfliktfall die Hochschulleitung auf Basis eines technisch-organisatorischen Konzepts.
7. Die Zuwiderhandlung gegen die Bestimmungen dieser Richtlinie stellt einen Sicherheitsverstoß dar und kann zum zeitweisen oder dauerhaften Ausschluss des betroffenen Systems von der IP-Kommunikation führen. Über diese Maßnahme ist der IT-Sicherheitsbeauftragte zu informieren.