Freie Universität Berlin

– –

– Nur für den internen Dienstgebrauch –

Freie Universität Berlin

FU Directory and Identity Service

– FUDIS –

der ZEDAT

Fragenkatalog des Sicherheits-Audit

Fassung: März 2009
Version 1.1

Inhalt

Vorbemerkung

Dieses Dokument beinhaltet alle Prüffragen, die bei der Durchführung des Sicherheits-Audits gestellt werden. Die Fragen sind in zwei Gruppen aufgeteilt. Die erste Gruppe, Kapitel 2 Grundlegende Fragestellungen (Selbstauskunft), soll vom Antragsteller vor Beginn des eigentlichen Audits ausgefüllt und eAS zugesandt werden. Der zweite Teil, Kapitel 3 Audit, beinhaltet alle Fragen, die während des Audit von den Auditoren gestellt werden. Mit Hilfe dieser Fragen wird der Grad der Umsetzung der aufgeführten Maßnahmen überprüft.

Der Antragsteller bekommt den vollständigen Fragenkatalog zugesandt. In Kenntnis des gesamten Prüfumfangs wird er somit in die Lage versetzt, den Umsetzungsgrad der aufgeführten Maßnahmen im Vorfeld zu überprüfen.

1 Systemsteckbrief

Systemname(n)

IP-Adressen

Betriebssystem(e)

Anwendung(en)

Verantwortlichkeit(en)

2 Grundlegende Fragestellungen (Selbstauskunft)

Nr.	Infrastruktur und Technik	System / Dokumentation / Ansprechpartner
1.	**Allgemeine Infrastruktur**	
1.1.	Wo sind die Systeme physikalisch aufgestellt?	
1.2.	Wie ist der Zugang zu den Räumlichkeiten geregelt?	
1.3.	Wie sieht die Netzstruktur der FUDIS nutzenden Systeme aus, existieren dedizierte Netze?	
1.4.	Existiert eine Außenanbindung (Internet)?	
1.5.	Falls eine Außenanbindung existiert, wird Fernwartung genutzt?	
1.6.	Sind lokale oder Netz basierte Firewalls vorhanden?	
1.7.	Sind Intrusion Detection vorhanden?	
1.8.	Sind Intrusion Prevention Systeme vorhanden?	

Nr.	Infrastruktur und Technik	System / Dokumentation / Ansprechpartner
2.	**Hardware und Betriebssystem der Server**	
2.1.	Wie viele FUDIS nutzende Server existieren, welche Betriebssysteme werden eingesetzt?	
2.2.	Wurden an den Servern Härtungen bezüglich des Betriebssystems oder der Applikationen vorgenommen? Wenn ja, auf welcher Basis wurden diese Härtungen durchgeführt?	
2.3.	Wird Zusatzsoftware wie Viren-, Trojanerschutz etc. eingesetzt?	
3.	**Anwendungen**	
3.1.	Werden LDAP-Server-Dienste eingesetzt?	
3.2.	Werden LDAP-Client-Dienste eingesetzt?	
3.3.	Falls LDAP eingesetzt wird, welche LDAP-Versionen werden eingesetzt?	
3.4.	Falls LDAP eingesetzt wird, welche Funktionen haben die LDAP-Instanzen?	
3.5.	Falls LDAP eingesetzt wird, sind mehrere LDAP-Instanzen vorhanden?	
3.6.	Welche Übertragungsprotokolle werden benutzt?	

Nr.	Infrastruktur und Technik	System / Dokumentation / Ansprechpartner
3.7.	Welche Form der Datenschnittstelle wird benutzt?	

Nr.	Infrastruktur und Technik	System / Dokumentation / Ansprechpartner
4.	**Security spezifische Installationen, Konfigurationen oder Richtlinien**	
4.1.	Findet verschlüsselte Kommunikation zwischen allen FUDIS nutzenden Systemen statt, wenn ja wie?	
4.2.	Existieren Frontend- oder Backup-Systeme und wird der Datenverkehr zwischen diesen Systemen durch eine Firewall geschützt?	
4.3.	Werden die FUDIS nutzenden Applikationen mit „Root“ oder administrativen Rechten betrieben?	
4.4.	Benötigt eine der genutzten Applikationen Schreibrechte auf den betreffenden FUDIS-LDAP-Server?	
4.5.	Welche Personendaten (Attribute) werden von FUDIS nutzenden Systemen benötigt?	
5.	**Betrieb, Update und Patch Management**	
5.1.	Existiert ein geregelter Prozess für das Update- und Patchmanagement der FUDIS nutzenden Systeme?	
5.2.	Ist der Update- und Patchprozess technisch für die Systeme umgesetzt?	
5.3.	Ist der Update- und Patchprozess technisch für die Applikationen umgesetzt?	
5.4.	Falls von FUDIS bezogene Daten gespeichert werden, wie werden diese Daten vor unbefugtem Zugriff gesichert?	

Nr.	Infrastruktur und Technik	System / Dokumentation / Ansprechpartner
5.5.	Falls von FUDIS bezogene Daten gespeichert werden, existiert eine Regelung wie diese Daten per Backup gesichert werden?	
6.	**Logging und Monitoring**	
6.1.	Existiert ein Monitoring für die FUDIS nutzenden Systeme?	
6.2.	Falls Logging-Funktionen des Systems oder der Applikationen benutzt werden, wie werden welche Daten wohin geschrieben?	
7.	**Organisatorisches**	
7.1.	Sind die Verantwortlichkeiten bezüglich Systemverantwortung, Applikationsverantwortung, Betrieb, Updateprozess etc. der FUDIS nutzenden Systeme geregelt?	
7.2.	Sind Urlaubs- oder Krankheitsvertretungen für die Wartung und Pflege der FUDIS nutzenden Systeme oder Applikationen geregelt?	
7.3.	Existiert eine verbindliche Regelung welche Anwender FUDIS-Daten abfragen und nutzen dürfen; sind Vertreterregelungen vorhanden?	
7.4.	Fand eine Schulung der verantwortlichen Administratoren vor der Installation der Systeme und Applikationen statt?	
8.	**Dokumentation**	
8.1.	Existiert ein vollständiges Konzept für die Anbindung an FUDIS?	
8.2.	Falls Daten von FUDIS empfangen werden, existiert ein vollständiges Konzept für die Art und Nutzung dieser Daten?	

Nr.	Infrastruktur und Technik	System / Dokumentation / Ansprechpartner
8.3.	Existiert eine vollständige Dokumentation der Installation?	
8.4.	Sind die Konfigurationen dokumentiert? Werden Veränderungen an den Konfigurationen dokumentiert?	

3 Audit

Die in diesem Abschnitt aufgeführten Fragen zum Umsetzungsgrad der Maßnahmen werden von den Auditoren bei der Durchführung des Audits gestellt. Die Fragen sind unterteilt in die drei Gruppen „normal“, „hoch“ und „sehr hoch“, entsprechend den Schutzklassen der FUDIS-Produkte. Bei Wahl eines FUDIS-Produkts der Schutzklasse „normal“ sind lediglich die Fragen der ersten Gruppe relevant. Bei einem FUDIS-Produkt der Schutzklasse „hoch“ müssen zusätzlich die Fragen der zweiten Gruppe beantwortet werden. Die dritte und letzte Fragengruppe betrifft nur FUDIS-Produkte der Schutzklasse „sehr hoch“. Sie müssen dann zusätzlich zu den anderen Fragengruppen bearbeitet werden.

Auditiertes System:	

Audit-Termin(e):

Datum	Beginn	Ende	Ort

Gesprächsteilnehmer:

Name	Bereich	Funktion

3.1 Maßnahmen des Schutzbedarfs „normal“

Nr.	Maßnahme	Umsetzungsgrad Ja Nein Teilweise Entbehrlich	Ansprechpartner
1.	Ist ein räumlicher Zugangsschutz zu den FUDIS nutzenden Serversystemen vorhanden?		
2.	Werden die Daten mobiler Computer bei lokaler Speicherung von FUDIS-Daten gesichert?		
3.	Wird der Softwareeinsatz der FUDIS-Daten verarbeitenden Systeme kontrolliert?		
4.	Ist Virenschutz, Schutz vor Schadsoftware, auf FUDIS-Daten verarbeitenden Servern und Clients vorhanden?		
5.	Ist das Abmelden und Ausschalten bei FUDIS-Clients technisch und organisatorisch umgesetzt?		
6.	Wird die Verarbeitung bzw. Nutzung von FUDIS-Daten auf personenbezogene Benutzerkennungen beschränkt?		
7.	Ist der Gebrauch von Passwörtern gemäß dem IT-Sicherheitsrichtlinie für FUDIS nutzende Zugängen umgesetzt?		
8.	Sind die Zugriffsrechte auf FUDIS nutzenden Transaktionen restriktiv vergeben?		
9.	Ist der Einsatz von Diebstahl-Sicherungen bei FUDIS nutzenden Client-Systemen umgesetzt?		
10.	Sind die Zugänge des Netzes der FUDIS nutzenden Systeme gegen unberechtigte Nutzung geschützt?		

Nr.	Maßnahme	Umsetzungsgrad Ja Nein Teilweise Entbehrlich	Ansprechpartner
11.	Werden die vorhanden Administratorkennungen nur für administrative Tätigkeiten benutzt?		
12.	Werden bei Ausscheiden von Mitarbeitern die dazugehörigen Berechtigungen entzogen?		
13.	Wird die Vergabe von Zugriffsrechten auf FUDIS nutzende Transaktionen / Systeme restriktiv behandelt? (Autorisierung)		
14.	Werden FUDIS nutzende Transaktionen protokolliert?		
15.	Existiert eine generelle Protokollierung auf den Servern?		
16.	Sind die Administratoren über die Sensitivität der FUDIS-Daten informiert?		
17.	Werden die entsprechenden administrativen Transaktionen schriftlich protokolliert?		
18.	Findet im FUDIS-Daten verarbeitenden Netz Netzmonitoring statt?		
19.	Sind im FUDIS-Daten verarbeitenden Netz nicht benötigte Netzwerkzugänge deaktiviert?		
20.	Findet Kommunikation zwischen Systemen mit ausschließlich gleichem Sicherheitsniveau statt?		
21.	Werden Datenträger mit FUDIS-Daten (personenbezogen) sicher entsorgt?		
22.	Ist das Physische Löschen und Entsorgen von Datenträgern geregelt?		

Nr.	Maßnahme	Umsetzungsgrad Ja Nein Teilweise Entbehrlich	Ansprechpartner
23.	Informieren sich die Administratoren regelmäßig über Schwachstellen?		
24.	Werden die Administratoren regelmäßig geschult?		
25.	Finden regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen statt?		
26.	Existiert eine Regelung der Verantwortung für Notfälle?		
27.	Existieren gesonderte Notfall-Pläne für ausgewählte Schadensereignisse?		
28.	Existiert ein Alarmierungsplan?		
29.	Existiert eine Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen?		
30.	Existiert eine geregelte Außerbetriebnahme der Server?		

3.2 Maßnahmen des Schutzbedarfs „hoch“

Nr.	Maßnahme	Umsetzungsgrad Ja Nein Teilweise Entbehrlich	Ansprechpartner
1.	Wird verschlüsselte Kommunikation genutzt?		
2.	Sind Vertraulichkeitserklärungen unterschrieben und vorhanden?		
3.	Existieren Vorgaben zum Management der Schnittstellen?		
4.	Existiert eine geeignete physikalische Segmentierung der Netzwerke?		
5.	Existiert eine geeignete logische Segmentierung der Netzwerke?		
6.	Existiert eine Trennung in Frontend und Backend Systeme?		
7.	Wurde das relevante Betriebssystem „minimal“ installiert?		
8.	Existieren verbindliche Regelungen für die Behandlung von Sicherheitsvorfällen?		

3.3 Maßnahmen des Schutzbedarfs „sehr hoch“

Nr.	Maßnahme	Umsetzungsgrad Ja Nein Teilweise Entbehrlich	Ansprechpartner
1.	Werden verschlüsselte Dateisysteme genutzt?		
2.	Existiert ein Zutrittsschutz zu den Terminals?		
3.	Wurde die Bedienoberfläche der Clientsoftware angepasst?		
4.	Werden Integritätschecks auf den FUDIS nutzenden Systemen durchgeführt?		
5.	Wird auf den relevanten Systemen nur ein Dienst pro Server genutzt?		