Dokumentation Sicherheitsarchitektur

**01\_Technischer Basisschutz von IT-NT-Systemen**

Systemhärtung:

Req1: Nicht benötigte Dienste und Protokolle müssen deaktiviert werden.  
Req2: Die Erreichbarkeit von Diensten muss eingeschränkt werden.  
Req3: Nicht benötigte Software darf nicht installiert oder muss deinstalliert werden.  
Req4: Nicht benötigte Funktionen der eingesetzten Software und Hardware müssen deaktiviert  
 werden.

Systemaktualisierung

Req5: Software- und Hardware-Komponenten, für die es keine Wartung oder Pflege durch den   
 Lieferanten, Hersteller oder Entwickler gibt, dürfen nicht verwendet werden.  
Req6: Bekannt gewordene Schwachstellen in der Software oder Hardware des Systems müssen  
 behoben oder abgesichert werden.

Schutz von Daten und Informationen

Req7: Schutzbedürftige Daten müssen bei der Übertragung sowie Speicherung gegen unberechtigte  
 Einsichtnahme und Veränderung geschützt werden.  
Req8: Schutzbedürftige Informationen dürfen nicht in Dateien, Ausgaben und Meldungen enthalten  
 sein, die unautorisierten Benutzern zugänglich sind.

Schutz der Verfügbarkeit und Integrität

Req9: Das System muss sich gegen Überlastsituationen schützen.  
Req10: Falls eine Überlastsituation nicht verhindert werden kann muss sich das System berechenbar  
 verhalten  
Req11: Das System muss robust gegen unerwartete Eingaben sein.

Authentifizierung und Autorisierung

Req12: Die Nutzung und der Zugriff auf schutzbedürftige Funktionen und Informationen, dürfen  
 nicht ohne erfolgreiche Authentifizierung und Autorisierung möglich sein.  
Req13: Es müssen Konten verwendet werden, die die eindeutige Identifizierung des Benutzers  
 ermöglichen.   
Req14: Konten müssen gegen unautorisierte Nutzung durch Verwendung mindestens eines  
 Authentisierungsmerkmals geschützt werden.  
Req15: Konten mit weitereichenden Berechtigungen müssen mit zwei Authentisierungsmerkmalen   
 geschützt werden  
Req16: Vordefinierte Konten müssen gelöscht oder deaktiviert werden.  
Req17: Vordefinierte Authentisierungsmerkmale müssen geändert werden.  
Req18: Die Berechtigungen von Konten und Anwendungen müssen auf ein für deren Aufgaben  
 notwendiges Minimum reduziert werden.  
Req19: Das System muss für die Benutzerverwaltung an ein zentrales System angebunden werden.

Schutz von Sitzungen

Req20: Sitzungen müssen gegen eine unautorisierte Übernahme geschützt werden.  
Req21: Das System muss Benutzern ermöglichen sich von ihrer Sitzung abzumelden.  
Req22: Sitzungen müssen nach einer, dem Verwendungszweck angepassten Zeit der Inaktivität,  
 beendet werden.

Authentisierungsmerkmal Passwort

Req23: Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese mindestens 8  
 Zeichen lang sein und drei folgenden Zeichentypen beinhalten: Kleinbuchstaben,  
 Großbuchstaben, Ziffern und Sonderzeichen.  
Req24: Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des  
 eigenen Passwortes jederzeit durch den Benutzer möglich sein.  
Req25: Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss ein Schutz gegen  
 Wörterbuch- und Brute-Force-Angriffe vorhanden sein, der das Erraten von Passwörtern  
 stark erschwert.  
Req26: Falls Passwörter als Authentisierungsmerkmal genutzt werden, darf deren Darstellung nicht  
 im Klartext erfolgen.

Protokollierung

Req27: Sicherheitsrelevante Ereignisse müssen abhängig vom Verwendungszweck des Systems mit  
 genauem Zeitstempel und einer eindeutigen Systembezeichnung protokolliert werden.  
Req28: Sicherheitsrelevante Protokollierungsdaten müssen umgehend nach deren Erzeugung an ein  
 separates System weitergeleitet werden.

**02\_Werb Services**

Allgemeine Vorgaben

Req1: Grundlegende Sicherheitsfunktionen für extern zugänglich Webservices müssen in der DMZ  
 implementiert werden und je nach Kritikalität mit einem Web Service Security Gateway  
 geschützt werden.  
Req2: Werden bei einem Webservice hochvertrauliche Daten im Sinne des Kreditkarten Payment  
 Standards PCI DSS (z.B. Kreditkartendaten, Kundendaten und Kundenpasswörter) verarbeitet,  
 so müssen diese Daten durch Einsatz von durchgängigen Mechanismen auf der  
 Anwendungsebene (End-to-End), wie z.B. XML-Verschlüsselung, individuell geschützt  
 werden.  
Req3: Ein Webservice-Requests muss vor Manipulation / Replay Attacken geschützt werden, wenn  
 dieser über öffentliche, ungesicherte Transportwege übertragen wird.

Authentifizierung

Req4: Der Absender eines Webservice-Requests muss angemessen authentifiziert werden, wenn  
 vertraulichen Inhalte / Informationen übertragen werden.  
Req5: Der Mechanismus zur Authentifizierung eines Absenders muss auf starken kryptografischen  
 Algorithmen / Frameworks basieren.  
Req6: Der Empfänger eines Webservice-Requests muss vom Absender dieses Request  
 authentifiziert werden.  
Req7: Wird ein Webservice-Request mit XML-Signaturen geschützt, dürfen die Signaturdaten NICHT  
 von einem Intermediate Processor aus dem Request entfernt werden.

SOAP und XML

Req8: Wenn ein SOAP-Request bzw. eine SOAP-Antwort nicht sofort abgewickelt wird und in der  
 DMZ zwischengespeichert werden muss, muss die Vertraulichkeit und Integrität der  
 zwischengespeicherten Nachricht sichergestellt werden.   
Req9: Ein neu entwickelter Webservice muss für die Inhalts-Formatvalidierung zwingend   
 XML-Schemata verwenden

WSDL

Req10: Jeder in einem Webservice vermittelte Element- und Attributwert muss mit dem erwarteten  
 Datentyp, der erwarteten Länge und/oder dem erwarteten Bereich beschrieben werden  
 sowie ggf. mit einer formellen Spezifikation zur Beschreibung der akzeptablen Daten.  
Req11: Alle Webservice-Requests MÜSSEN am Webservice-Endpunkt gegenüber der detaillierten  
 WSDL-Spezifikation validiert werden, die diesen Request beschreibt.  
Req12: Enthält der Webservice keine formelle Spezifikation der Eingabedaten, MUSS mittels Black-  
 /Whitelistings verhindert werden, dass illegale Zeichen an den Webserver weitergeleitet  
 werden.  
Req13: Der Öffentlichkeit darf nur die kleinstmögliche Anzahl an APIs / Funktionen über Webservices  
 zugänglich gemacht werden.

03\_Webserver

Plattformanforderungen

Req1: Der Webserver muss der einzige extern zugreifbare Service eines Systems sein, soweit der  
 Webserver nicht ausschließlich für eine Administrations-Schnittstelle genutzt wird.

Installationsanforderungen

Req2: Verschiedene Instanzen des Webservers müssen in getrennten Umgebungen laufen.  
Req3: Alle Webserverprozesse dürfen nicht mit Systemprivilegien laufen.

Konfigurationsanforderungen

Req4: Nicht benötigte http-Methoden müssen deaktiviert werden.  
Req5: Komponenten des Webservers, die für den Betrieb oder die Funktion nicht benötigt werden,  
 müssen deinstalliert werden.  
Req6: Falls CGI verwendet wird, müssen CGI-Wrapper für die erste Parameterüberprüfung/  
 -validierung und Einrichtung der korrekten Runtime- Umgebung für CGI-Programme  
 verwendet werden.  
Req7: Falls CGI verwendet wird darf das CGI-Verzeichnis keine Compiler oder Interpreter (bspw.  
 PERL-Interpreter, PHP-Interpreter/Compiler, TcI-Interpreter/Compiler oder Betriebssystem  
 Shells) enthalten.  
Req8: Falls CGI verwendet wird, darf das CGI-Verzeichnis nicht für Uploads genutzt werden.  
Req9: Falls Server Side Includes (SSI) aktiv sind, muss die Ausführung von Systembefehlen  
 deaktiviert werden.  
Req10: Falls WebDAV für das Schreiben von Dateien verwendet wird, darf Zugriff nicht ohne  
 erfolgreiche Authentifizierung gewährt werden.  
Req11: Falls WebDAV verwendet wird, müssen Zugriffsrechte restriktiv konfiguriert werden.  
Req12: Zugriffsrechte für Webserver-Konfigurationsdateien dürfen nur dem Eigentümer des  
 Webserver-Prozesses oder einem Benutzer mit Systemprivilegien gewährt werden.  
Req13: Default-Inhalte müssen entfernt werden.  
Req14: Schreibzugriff auf ausführbare Dateien, die mit Systemprivilegien ausgeführt werden, muss  
 auf Benutzer mit Systemprivilegien beschränkt werden.  
Req15: Die Erstellung von Verzeichnislisten (Indizierung) muss deaktiviert werden.  
Req16: Informationen über den Webserver in http-Headern müssen auf ein Mindestmaß beschränkt  
 werden.  
Req17: Informationen über den Webserver in Fehlerseiten, die durch den Webserver ausgeliefert  
 werden, müssen entfernt werden.  
Req18: Nicht benötigte Dateitypzuordnungen müssen entfernt werden.  
Req19: Das unautorisierte Überschreiben der Webserver-Konfiguration muss verhindert werden.  
Req20: Der Webserver darf nur Dateien ausliefern, die für die Auslieferung bestimmt sind.

HTTPS-Anforderungen

Req21: Für die Verschlüsselung mit HTTPS muss das TLS-Protokoll verwendet werden.  
Req22: Der Webserver muss so konfiguriert werden, dass die Nutzung der aktuellen Version des TLS  
 Protokolls möglich ist.  
Req23: Die TLS-Konfiguration darf keine unsicheren Cipher-Suites verwenden.  
Req24: Die TLS-Konfiguration muss vorsehen, dass beim Verbindungsaufbau die als am sichersten  
 einzustufenden Cipher-Suites mit oberster Priorität ausgewählt werden.

Protokollierung

Req25: Der Zugriff auf den Webserver muss protokolliert werden.

04\_Secure Shell

Sicherheitsanforderungen: Grundlegendes

Req1: Es muss ausschließlich die Protokollversion SSH-2 eingesetzt werden.