APP.2: Verzeichnisdienste

APP.2.1: Allgemeiner Verzeichnisdienst

1 Beschreibung

1.1 Einleitung

Ein Verzeichnisdienst stellt in einem Datennetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. In einem Objekt können zugehörige Attribute gespeichert werden, zum Beispiel können zu einer Benutzerkennung der Name und Vorname des Benutzers, die Personalnummer und der Name des IT-Systems abgelegt werden. Diese Daten können dann gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten werden in der Regel von zentraler Stelle aus verwaltet.

Einige typische Anwendungsgebiete von Verzeichnisdiensten sind:

- Verwaltung von Adressbüchern, z. B. für Telefonnummern, E-Mail-Adressen und Zertifikate für elektronische Signaturen
- Ressourcen-Verwaltung, z. B. für IT-Systeme, Drucker, Scanner und andere Peripherie-Geräte
- Benutzerverwaltung, z. B. zur Verwaltung von Benutzerkonten und Benutzerberechtigungen
- Authentisierung, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen

Verzeichnisdienste sind auf Lesezugriffe hin optimiert, da Daten aus dem Verzeichnisdienst typischerweise abgerufen werden. Schreibzugriffe, bei denen Einträge erstellt, geändert oder gelöscht werden, sind seltener notwendig.

Der Einsatz eines solchen Verzeichnisdienstes bietet sich vor allem dort an, wo z. B. die Anzahl der im Netz eingesetzten Clients eine dezentrale Verwaltung erschwert. Ohne einen Verzeichnisdienst könnte nicht mehr gewährleistet werden, dass lokal vorzunehmende Einstellungen, wie z. B. die Vorgaben aus Sicherheitsrichtlinien, aufgrund des hohen Aufwandes zuverlässig erledigt werden. Verwaltungsaufgaben innerhalb des Netzes wie z. B. Passwortänderungen, Kontenerstellung und Zugriffsrechte können effizienter durchgeführt werden, wenn ein Verzeichnisdienst eingesetzt wird.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, allgemeine Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen angemessen zu schützen.

1.3 Abgrenzung und Modellierung

Der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* ist für alle verwendeten Verzeichnisdienste anzuwenden.

Dieser Baustein betrachtet allgemeine Sicherheitsaspekte von Verzeichnisdiensten unabhängig vom eingesetzten Produkt. Für produktspezifische Sicherheitsaspekte gibt es im IT-Grundschutz-Kompendium weitere Bausteine, die zusätzlich auf den jeweiligen Verzeichnisdienst anzuwenden sind. Bausteine zu Server-Betriebssystemen, auf denen Verzeichnisdienste üblicherweise betrieben werden, sind in der Schicht SYS.1 *Server* des IT-Grundschutz-Kompendiums aufgeführt.

Verzeichnisdienste sollten grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mit berücksichtigt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* von besonderer Bedeutung.

2.1 Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten

Die Sicherheit von Verzeichnisdiensten stützt sich stark auf die Sicherheit des Basisbetriebssystems und dabei vor allem auf die Dateisystemsicherheit. Verzeichnisdienste lassen sich auf vielen Betriebssystemen installieren und betreiben, wodurch sich eine große Vielfalt der vorzunehmenden Sicherheitseinstellungen ergeben kann. Diese Vielfalt erhöht die Anforderungen an die Planung und setzt entsprechende Kenntnisse über das jeweilige Betriebssystem voraus. Sollte die entstehende Gesamtlösung sehr heterogen oder komplex sein, kann ein nicht ausreichend geplanter Einsatz des Verzeichnisdienstes im Wirkbetrieb zu Sicherheitslücken führen. Bei Verzeichnisdiensten ist außerdem eine rollenbasierte Administration der Verzeichnisdatenbank üblich. Zudem können einzelne Administrationsaufgaben delegiert werden. Deshalb besteht bei fehlerhafter Planung der Administrationsaufgaben die Gefahr, dass das System unsicher oder unzulänglich administriert wird.

2.2 Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst

Bei der Partitionierung werden die Verzeichnisdaten eines Verzeichnisdienstes in einzelne Teilbereiche (Partitionen) aufgeteilt. Um für eine bessere Lastverteilung zu sorgen, werden Partitionen des Verzeichnisdienstes in der Regel repliziert. Außerdem wird durch die redundante Datenhaltung die Ausfallsicherheit verbessert und somit die Verfügbarkeit erhöht. Von entscheidender Bedeutung ist deshalb auch hier eine geeignete Planung, da Partitions- und Replikationseinstellungen zwar nachträglich geändert werden können, dies aber Probleme verursachen kann. Wird die Partitionierung und die Replizierung des Verzeichnisdienstes fehlerhaft oder unzureichend geplant, kann sich dies negativ auswirken. Es kann etwa zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, zu einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und zu einer insgesamt schlechten Systemperformance bis hin zu Ausfällen führen.

2.3 Fehlerhafte oder unzureichende Planung des Zugriffs auf den Verzeichnisdienst

Zugangs- und Zugriffsrechte im Kontext eines Verzeichnisdienstes zu verwalten, ist eine äußerst arbeitsintensive Aufgabe. Im Extremfall sind dazu viele manuelle Arbeitsschritte erforderlich, die zu Fehlern führen und es erschweren können, den Überblick zu behalten. Eine unzureichende Planung, ob und welche Daten im Klartext übertragen werden dürfen, kann zudem Inkonsistenzen oder Widersprüche zu organisationsinternen Sicherheitsrichtlinien hervorrufen. Auch kann eine fehlerhafte Planung der Sicherheitsmaßnahmen und -techniken zum Schutz vertraulicher Daten innerhalb des

Verzeichnisdienstes zu Inkompatibilitäten bis hin zum Ausfall der Verschlüsselung führen. Dies kann sich unmittelbar auf die Vertraulichkeit und die Integrität auswirken.

2.4 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die durchzuführenden Aufgaben erforderlich sind. Dies gilt auch für die Berechtigungen, die über einen Verzeichnisdienst verwaltete Benutzer und Gruppen erhalten. Werden diese Rechte fehlerhaft administriert, kann einerseits der Betrieb gestört werden, falls erforderliche Rechte nicht zugewiesen wurden. Andererseits können Sicherheitslücken entstehen, falls über die notwendigen Rechte hinaus weitere Rechte vergeben werden. Wenn die Zugriffsrechte im Verzeichnisdienst falsch oder inkonsistent vergeben werden, ist dadurch die Sicherheit des Gesamtsystems erheblich gefährdet. Ein besonders kritischer Punkt sind auch die Administrationsrechte. Werden diese Rechte falsch vergeben, kann das gesamte Administrationskonzept in Frage gestellt oder unter Umständen sogar die Administration des Verzeichnissystems selbst blockiert werden.

2.5 Fehlerhafte Konfiguration des Zugriffs auf Verzeichnisdienste

In vielen Fällen müssen weitere Applikationen wie Internet- oder Intranet-Anwendungen auf den Verzeichnisdienst zugreifen. Eine Fehlkonfiguration kann dazu führen, dass Zugriffsrechte falsch vergeben werden. Es kann auch passieren, dass unautorisiert auf den Verzeichnisdienst zugegriffen werden kann oder dass Daten zur Authentisierung im Klartext übermittelt werden. In diesem Fall können unverschlüsselte Informationen ausgespäht werden.

2.6 Ausfall von Verzeichnisdiensten

Durch technisches Versagen aufgrund von Hardware- oder Software-Problemen können Verzeichnisdienste oder Teile davon ausfallen. Als Folge sind die Daten im Verzeichnis temporär nicht mehr zugänglich. Im Extremfall können auch Daten verloren gehen. Dadurch können Geschäftsprozesse und interne Arbeitsabläufe behindert werden. Sind funktionsfähige Kopien der ausgefallenen Systemteile vorhanden, so ist der Zugriff zwar weiterhin möglich, jedoch je nach gewählter Netztopologie nur mit eingeschränkter Leistungsfähigkeit.

2.7 Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff

Wenn es einem Angreifer gelungen ist, eine notwendige Authentisierung gegenüber dem Verzeichnisdienst erfolgreich zu umgehen, kann er danach unbefugt auf eine Vielzahl von Daten zugreifen. Somit kann der gesamte Verzeichnisdienst kompromittiert werden. Außerdem könnten Unbefugte durch erweiterte Berechtigungen auf Netzressourcen oder Dienste zugreifen. Dies kann dazu führen, dass ein Angreifer alle Verteidigungsmaßnahmen des Verzeichnisdienstes umgeht. Dadurch könnte das betroffene System beeinträchtigt oder gar zerstört werden.

Die Sicherheit eines Verzeichnisdienstes kann ebenfalls gefährdet werden, wenn anonyme Benutzer zugelassen werden. Dadurch, dass deren Identität nicht überprüft wird, können anonyme Benutzer zunächst beliebige Abfragen an den Verzeichnisdienst richten, durch die sie zumindest Teilinformationen über dessen Struktur und Inhalt erlangen. Wenn anonyme Zugriffe zugelassen werden, sind außerdem DoS-Attacken auf den Verzeichnisdienst leichter durchzuführen, da Angreifer mehr Zugriffsmöglichkeiten haben, die nur schlecht kontrollierbar sind.

2.8 Fehlerhafte Konfiguration von Verzeichnisdiensten

Verzeichnisdienste verfügen über zahlreiche Funktionen, sodass der Verzeichnisdienst von Anwendern mit sehr unterschiedlichen Bedürfnissen genutzt werden kann. Eine Fehlkonfiguration dieser zahlreichen Funktionen kann dazu führen, dass unautorisiert auf den Verzeichnisdienst zugegriffen werden kann. Wenn beispielsweise die Standardkonfiguration nicht ausreichend geprüft und angepasst wird, können die Informationen zur Authentisierung im Klartext übermittelt werden. Werden diese

und weitere Informationen unverschlüsselt übertragen, könnten sie ausgespäht und für weitere Angriffe missbraucht werden.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.1 *Allgemeiner Verzeichnisdienst* aufgeführt. Grundsätzlich ist IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Datenschutzbeauftragter

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* vorrangig erfüllt werden:

APP.2.1.A1 Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste (B)

Es MUSS eine Sicherheitsrichtlinie für den Verzeichnisdienst erstellt werden. Diese SOLLTE mit dem übergreifenden Sicherheitskonzept der gesamten Institution abgestimmt sein.

APP.2.1.A2 Planung des Einsatzes von Verzeichnisdiensten [Datenschutzbeauftragter, Fachverantwortliche] (B)

Der Einsatz von Verzeichnisdiensten MUSS sorgfältig geplant werden. Die konkrete Nutzung des Verzeichnisdienstes MUSS festgelegt werden. Es MUSS sichergestellt sein, dass der Verzeichnisdienst und alle ihn verwendenden Anwendungen kompatibel sind. Zudem MUSS ein Modell aus Objektklassen und Attributtypen entwickelt werden, das den Ansprüchen der vorgesehenen Nutzungsarten genügt. Bei der Planung des Verzeichnisdienstes MÜSSEN Personalvertretung und Datenschutzbeauftragter beteiligt werden. Es MUSS ein bedarfsgerechtes Berechtigungskonzept zum Verzeichnisdienst entworfen werden. Generell SOLLTE die geplante Verzeichnisdienststruktur vollständig dokumentiert werden. Maßnahmen SOLLTEN geplant werden, die es unterbinden, aus dem Verzeichnisdienst unbefugt Daten sammeln zu können.

APP.2.1.A3 Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste [Fachverantwortliche] (B)

Die administrativen Aufgaben für die Administration des Verzeichnisdienstes selbst sowie für die eigentliche Verwaltung der Daten MÜSSEN strikt getrennt werden. Die administrativen Tätigkeiten SOLLTEN so delegiert werden, dass sie sich möglichst nicht überschneiden. Alle administrativen Aufgabenbereiche und Berechtigungen SOLLTEN ausreichend dokumentiert werden.

Die Zugriffsrechte der Benutzer- und Administratorengruppen MÜSSEN anhand der erstellten Sicherheitsrichtlinie konfiguriert und umgesetzt werden. Bei einer eventuellen Zusammenführung mehrerer Verzeichnisdienstbäume MÜSSEN die daraus resultierenden effektiven Rechte kontrolliert werden.

APP.2.1.A4 Sichere Installation von Verzeichnisdiensten (B)

Es MUSS ein Konzept für die Installation erstellt werden, nach dem Administrations- und Zugriffsberechtigungen bereits bei der Installation des Verzeichnisdienstes konfiguriert werden.

APP.2.1.A5 Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten (B)

Der Verzeichnisdienst MUSS sicher konfiguriert werden. Für die sichere Konfiguration einer Verzeichnisdienste-Infrastruktur MÜSSEN neben dem Server auch die Clients (IT-Systeme und Programme) einbezogen werden.

Wird die Konfiguration der vernetzten IT-Systeme geändert, SOLLTEN die Benutzer rechtzeitig über Wartungsarbeiten informiert werden. Vor den Konfigurationsänderungen SOLLTEN von allen betroffenen Dateien und Verzeichnissen Datensicherungen angefertigt werden.

APP.2.1.A6 Sicherer Betrieb von Verzeichnisdiensten (B)

Die Sicherheit des Verzeichnisdienstes MUSS im Betrieb permanent aufrechterhalten werden. Alle den Betrieb eines Verzeichnisdienst-Systems betreffenden Richtlinien, Regelungen und Prozesse SOLLTEN dokumentiert werden. Die Arbeitsplätze von Verzeichnisdienstadministratoren MÜSSEN ausreichend gesichert sein. Der Zugriff auf alle Administrationswerkzeuge MUSS für normale Benutzer unterbunden werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst*. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.2.1.A7 Erstellung eines Sicherheitskonzepts für den Einsatz von Verzeichnisdiensten (S)

Durch das Sicherheitskonzept für Verzeichnisdienste SOLLTEN sämtliche sicherheitsbezogenen Themenbereiche eines Verzeichnisdienstes geregelt werden. Die daraus entwickelten Sicherheitsrichtlinien SOLLTEN schriftlich festgehalten und den Benutzern des Verzeichnisdienstes mitgeteilt werden.

APP.2.1.A8 Planung einer Partitionierung und Replikation im Verzeichnisdienst (S)

Bei einer Partitionierung SOLLTE auf die Verfügbarkeit und den Schutzbedarf des Verzeichnisdienstes geachtet werden. Die Partitionierung des Verzeichnisdienstes SOLLTE schriftlich so dokumentiert werden, dass sie manuell wieder rekonstruiert werden kann. Um die Replikationen zeitgerecht ausführen zu können, SOLLTE eine ausreichende Bandbreite sichergestellt werden.

APP.2.1.A9 Geeignete Auswahl von Komponenten für Verzeichnisdienste [Fachverantwortliche] (S)

Für den Einsatz eines Verzeichnisdienstes SOLLTEN geeignete Komponenten identifiziert werden. Es SOLLTE ein Kriterienkatalog erstellt werden, nach dem die Komponenten für den Verzeichnisdienst ausgewählt und beschafft werden. Im Rahmen der Planung und Konzeption des Verzeichnisdienstes SOLLTEN passend zum Einsatzzweck Anforderungen an dessen Sicherheit formuliert werden.

APP.2.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.1.A11 Einrichtung des Zugriffs auf Verzeichnisdienste (S)

Der Zugriff auf den Verzeichnisdienst SOLLTE entsprechend der Sicherheitsrichtlinie konfiguriert werden. Wird der Verzeichnisdienst als Server im Internet eingesetzt, SOLLTE er entsprechend durch ein Sicherheitsgateway geschützt werden. Sollen anonymen Benutzern auf einzelne Teilbereiche des Verzeichnisbaums weitergehende Zugriffe eingeräumt werden, so SOLLTE ein gesondertes Benutzerkonto, ein sogenannter Proxy-User, für den anonymen Zugriff eingerichtet werden. Die Zugriffsrechte für diesen Proxy-User SOLLTEN hinreichend restriktiv vergeben werden. Sie SOLLTEN zudem wieder komplett entzogen werden, wenn der Account nicht mehr gebraucht wird. Damit nicht versehentlich schutzbedürftige Informationen herausgegeben werden, SOLLTE die Suchfunktion des Verzeichnisdienstes dem Einsatzzweck angemessen eingeschränkt werden.

APP.2.1.A12 Überwachung von Verzeichnisdiensten (S)

Verzeichnisdienste SOLLTEN gemeinsam mit dem Server beobachtet und protokolliert werden, auf dem sie betrieben werden.

APP.2.1.A13 Absicherung der Kommunikation mit Verzeichnisdiensten (S)

Die gesamte Kommunikation mit dem Verzeichnisdienst SOLLTE über SSL/TLS verschlüsselt werden. Der Kommunikationsendpunkt des Verzeichnisdienst-Servers SOLLTE aus dem Internet nicht erreichbar sein.

Der Datenaustausch zwischen Client und Verzeichnisdienst-Server SOLLTE abgesichert werden. Es SOLLTE definiert werden, auf welche Daten zugegriffen werden darf. Im Falle einer serviceorientierten Architektur (SOA) SOLLTEN zum Schutz von Service-Einträgen in einer Service-Registry sämtliche Anfragen an die Registratur daraufhin überprüft werden, ob der Benutzer gültig ist.

APP.2.1.A14 Geregelte Außerbetriebnahme eines Verzeichnisdienstes [Fachverantwortliche] (S)

Bei einer Außerbetriebnahme des Verzeichnisdienstes SOLLTE sichergestellt sein, dass weiterhin benötigte Rechte bzw. Informationen in ausreichendem Umfang zur Verfügung stehen. Alle anderen Rechte und Informationen SOLLTEN gelöscht werden. Zudem SOLLTEN die Benutzer darüber informiert werden, wenn ein Verzeichnisdienst außer Betrieb genommen wird. Bei der Außerbetriebnahme einzelner Partitionen eines Verzeichnisdienstes SOLLTE darauf geachtet werden, dass dadurch andere Partitionen nicht beeinträchtigt werden.

APP.2.1.A15 Migration von Verzeichnisdiensten (S)

Bei einer geplanten Migration von Verzeichnisdiensten SOLLTE vorab ein Migrationskonzept erstellt werden. Die Schema-Änderungen, die am Verzeichnisdienst vorgenommen wurden, SOLLTEN dokumentiert werden. Weitreichende Berechtigungen, die dazu verwendet wurden, die Migration des Verzeichnisdienstes durchzuführen, SOLLTEN wieder zurückgesetzt werden. Die Zugriffsrechte für Verzeichnisdienst-Objekte bei Systemen, die von Vorgängerversionen aktualisiert bzw. von anderen Verzeichnissystemen übernommen wurden, SOLLTEN aktualisiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

APP.2.1.A16 Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes (H)

Im Rahmen der Notfallvorsorge SOLLTE es eine bedarfsgerechte Notfallplanung für Verzeichnisdienste geben. Für den Ausfall wichtiger Verzeichnisdienst-Systeme SOLLTEN Notfallpläne vorliegen. Alle Notfall-Prozeduren für die gesamte Systemkonfiguration der Verzeichnisdienst-Komponenten SOLLTEN dokumentiert werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* sind keine weiterführenden Informationen vorhanden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den

Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen