Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: INTERNET-DIENSTLEISTER

Sichere Bereitstellung von ISP-Dienstleistungen

Handlungsempfehlungen für Internet-Service-Provider (ISP)

Eine ständige und qualitativ hochwertige Verfügbarkeit des Internets ist heute in fast allen Bereichen der Arbeitswelt sowie des Privatlebens von zentraler Bedeutung. Um diesem Anspruch gerecht zu werden, haben Internet-Service-Provider gemäß §109 TKG geeignete technische Vorkehrungen und sonstige Schutzmaßnahmen zu treffen.

Die Bundesnetzagentur hat im Benehmen mit dem BSI einen *Katalog von Sicherheitsanforderungen*[1] *für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach §109 TKG* (im Folgenden Sicherheitskatalog) erstellt.

Zur Sicherstellung der Erbringung einer bestmöglichen Dienstleistung ist die Umsetzung verschiedener organisatorischer Maßnahmen erforderlich. Kapitel 1 des vorliegenden Dokuments fasst wesentliche Aspekte zusammen.

Das BSI hat zwischenzeitlich in Zusammenarbeit mit Internet-Service-Providern zu verschiedenen Themenfeldern detaillierte Handlungsempfehlungen veröffentlicht, welche die im oben genannten Sicherheitskatalog beschriebenen Maßnahmen konkretisieren und den derzeitigen Stand der Technik („Best Current Practise“) widerspiegeln. Einen Überblick über die aktuell adressierten Themengebiete gibt Kapitel 2. Weitere Empfehlungen zur Verbesserung der Internetsicherheit werden in Kapitel 9 des Sicherheitskatalogs gegeben.

1. Organisatorische Maßnahmen

Zu den wesentlichen organisatorischen Maßnahmen gehören:

1.1 Informationssicherheitsmanagement

Ein angemessenes Sicherheitsniveau kann nur durch geplantes und strukturiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Eine systematische Vorgehensweise ist die grundlegende Voraussetzung für eine erfolgreiche Umsetzung und Kontrolle von Sicherheitsmaßnahmen. Die hierzu notwendigen organisatorischen Standardmaßnahmen zur Erreichung eines Mindestschutzniveaus werden im BSI-Grundschutzbaustein ISMS.1 beschrieben.

1 http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf

1.2 Sorgfältiges Personalmanagement

Sowohl Mitarbeiter als auch externes Personal müssen mit Sicherheitsmaßnahmen vertraut sein und dafür regelmäßig entsprechend geschult und sensibilisiert werden. Die relevanten Aspekte werden im BSI-Grundschutzbaustein ORP.2[2] aufgeführt.

1.3 Notfallmanagement

Zu den wesentlichen organisatorischen Maßnahmen gehört auch die Etablierung eines funktionierenden Notfallmanagements. Einen Überblick hierzu liefern der BSI-Standard 100-4 sowie der BSI-Grundschutzbaustein DER.4[3].

1.4 Datensicherungskonzept

Jeder ISP sollte ein angemessenes und funktionstüchtiges Datensicherungskonzept erstellen, so dass der IT-Betrieb kurzfristig wieder aufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen. Details hierzu finden sich in BSI-Grundschutzbaustein B Con.3[4].

1.5 Datenschutz

Zum Schutz personenbezogener Daten sind von den datenverarbeitenden Stellen technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Einen Überblick hierzu gibt der BSI-Grundschutzbaustein Con.2.

1.6 Behandlung von Sicherheitsvorfällen

Um die Informationssicherheit im laufenden Betrieb zu gewährleisten, ist es notwendig, die Behandlung von Sicherheitsvorfällen im Vorfeld zu konzipieren und einzuüben. Gemäß §109 und §109a TKG besteht eine Mitteilungspflicht gegenüber der BNetzA, sofern sich durch den Sicherheitsvorfall erhebliche Auswirkungen auf den Betrieb oder die Dienstleistungserbringung ergeben. Weitere Informationen hierzu gibt auch der BSI-Grundschutzbaustein DER.2.1[5].

1.7 Patch- und Änderungsmanagement

Bei jedem ISP sollte ein funktionierendes Patch- und Änderungsmanagement etabliert sein. Der BSI-Grundschutzbaustein OPS.1.1.3[6] zeigt auf, wie ein Prozess Patch- und Änderungsmanagement kontrolliert und optimiert werden kann, damit Störungen im Betrieb vermieden sowie Sicherheitslücken minimiert und zeitnah beseitigt werden können.

1.8 Physischer Schutz von technischen Einrichtungen

Jeder ISP sollte die in den Grundschutzbausteinen INF[7] beschriebenen Maßnahmen umsetzen, um die von ihm betriebenen technischen Einrichtungen ausreichend vor Manipulationen zu schützen.

1.9 Technische Absicherung der IT-Systeme

Die Kompromittierung eigener IT-Systeme erschwert oder verhindert die Einhaltung definierter Schutzziele. Jeder ISP sollte geeignete vorbeugende Maßnahmen gegen Schadprogramme zusammenstellen sowie das Vorgehen im Fall einer Infektion mit Schadprogrammen regeln. In BSI-Grundschutzbaustein OPS.1.1.4[8] wird die Vorgehensweise zur Erstellung und Realisierung eines entsprechenden Sicherheitskonzeptes erläutert.

2 https://www.bsi.bund.de/dok/10095918 sowie Umsetzungshinweise: https://www.bsi.bund.de/dok/10137244
3 https://www.bsi.bund.de/dok/10095786
4 https://www.bsi.bund.de/dok/10095836 sowie Umsetzungshinweise: https://www.bsi.bund.de/dok/10095932
5 https://www.bsi.bund.de/dok/10095794
6 https://www.bsi.bund.de/dok/10095818 sowie Umsetzungshinweise: https://www.bsi.bund.de/dok/10095924
7 https://www.bsi.bund.de/dok/10137152 sowie Umsetzungshinweise: https://www.bsi.bund.de/dok/10137226
8 https://www.bsi.bund.de/dok/10095808

Die BSI-Standards zur Internet-Sicherheit (ISi-Reihe)[9] geben ebenfalls weiterführende Empfehlungen.

1.10 ISO 27001-Zertifizierung

Eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz umfasst sowohl eine Prüfung des Informationssicherheitsmanagements als auch der konkreten Sicherheitsmaßnahmen auf Basis von IT-Grundschutz.

2. Technische Maßnahmen

2.1 E-Mail-Sicherheit

Trotz diverser Vorhersagen, dass sich in Zukunft die Internetkommunikation immer stärker auf soziale Netzwerke verlagern wird, bildet E-Mail derzeit noch immer das meistgenutzte Medium für die Übertragung von elektronischen Nachrichten. Hiermit verbunden ist jedoch auch die Tatsache, dass E-Mail nach wie vor einer der meistgenutzten Transportkanäle für die Verbreitung von Malware, wie Viren, Würmern und Trojanern, ist. Ein nicht minder großes Ärgernis ist das enorme Aufkommen an Spam-Nachrichten, welche nach wie vor den weitaus größten Anteil aller versendeten E-Mails umfassen.

Die Handlungsempfehlung „E-Mail-Sicherheit“[10] fasst verschiedene Maßnahmen zur Eindämmung von Malware und Spam sowie zur Absicherung der Postfachzugänge zusammen.

2.2 Malware-Schutz

Schadsoftware auf angeschlossenen Kundensystemen können die Infrastruktur von ISPs beispielsweise durch das Versenden von Spam oder das Durchführen von DDoS-Angriffen schädigen. Die Handlungsempfehlung „Malware-Schutz“[11] gibt eine Zusammenfassung von Maßnahmen zum Schutz vor Schadsoftware, die durch Provider im Privatkundenbereich umgesetzt werden sollten. Die Empfehlungen umfassen die Bereiche Kundenunterstützung (Customer-Support), technische Schutzmaßnahmen sowie providerübergreifende Kooperation.

2.3 Sicheres Webhosting

Ungenügend gesicherte Webseiten und -server im Internet sind als potenzielle Verbreitungswege für Schadprogramme anzusehen und stellen daher eine Bedrohung dar.

Die BSI-Empfehlung „Sicheres Webhosting“[12] richtet sich an Webhoster und behandelt Maßnahmen zur Verbesserung der Sicherheit für Webhostingkunden. Hierfür werden die verschiedenen Phasen des Webhostings sowie grundlegende Maßnahmen betrachtet.

2.4 Sichere Bereitstellung von DNS-Diensten

Das DNS-Protokoll weist prinzipielle Schwächen auf. Daher werden regelmäßig neue Schwachstellen gefunden, die die Manipulation von DNS-Einträgen ermöglichen. Die Handlungsempfehlung „Sichere Bereitstellung von DNS-Diensten“[13] beschreibt wesentliche Aspekte, die für einen sicheren und zuverlässigen Betrieb von DNS-Servern umgesetzt sein sollten.

9 https://www.bsi.bund.de/ISi-Reihe
10 https://www.allianz-fuer-cybersicherheit.de/dok/6621320
11 https://www.allianz-fuer-cybersicherheit.de/dok/6621316
12 https://www.allianz-fuer-cybersicherheit.de/dok/6621318
13 https://www.allianz-fuer-cybersicherheit.de/dok/6621324

2.5 Anti-DDoS-Maßnahmen

Die Handlungsempfehlung „Anti-DDoS-Maßnahmen“[14] beschreibt Maßnahmen, die zum einen durch interne Umsetzung und zum anderen in Zusammenarbeit mit den Kunden dazu beitragen können, DDoS-Angriffen und deren Auswirkungen entgegenzuwirken.

2.6 Maßnahmen gegen Reflection Angriffe

Das BSI beobachtet in 2014 eine deutliche Zunahme an Distributed-Denial-of-Service (DDoS) Angriffen, die sogenannte Reflection-Techniken einsetzen. Dabei wird das Zielsystem nicht direkt angegriffen, sondern offen zur Verfügung stehende Dienste im Internet missbraucht. Das Dokument „Maßnahmen gegen Reflection Angriffe“[15] fasst zahlreiche Möglichkeiten zusammen, mit denen Systeme gegen deren Ausnutzung im Rahmen von Reflection-Angriffen abgesichert werden können.

2.7 IPv6 für Internet-Service-Provider

Die Handlungsempfehlung „IPv6 für Internet-Service-Provider“[16] gibt Hinweise, die bei der Einführung von IPv6 beachtet werden sollten.

2.8 Sichere Bereitstellung von Domaindienstleistungen

Internet-Domains sind ein wesentlicher Bestandteil jeder Internetanbindung, da sämtliche Inhalte von Internet-Diensten üblicherweise über Domainnamen adressiert werden. Der zuverlässigen Registrierung und Verwaltung von Internetdomains im weltweiten Domain-Name-Service (DNS)-Verbund kommt daher eine hohe Bedeutung zu. Die Handlungsempfehlung „Sichere Bereitstellung von Domaindienstleistungen“ zeigt auf, wie eine sichere Bereitstellung von Domaindienstleistungen erfolgen und einer maliziösen Verwendung von Domainnamen begegnet werden kann.

2.9 Inter-Domain-Routing

(Inter-Domain-)Routing bezeichnet Routing über mehrere autonome Systeme hinweg. Diese Form des Routings wird meist vom Internet-Dienstanbieter administriert. Im Internet stellt das sogenannte Border Gateway Protocol (BGP) den de-facto-Standard für Inter-Domain-Routing dar. Der unbedachte oder nicht ausreichend geprüfte Eingriff in das Routing kann dazu führen, dass Teilbereiche des Netzes nicht mehr erreichbar sind oder Kommunikationswege unbemerkt umgeleitet werden können. Die Ergreifung von Maßnahmen zur Verhinderung der Manipulation von BGP-Routen ist somit eine wichtige Aufgabe. Die Handlungsempfehlung „Inter-Domain-Routing“[17] gibt eine Zusammenfassung gängiger Best-Practice-Ansätze sowie Empfehlungen zur Verbesserung der Sicherheit des Internetroutings.

Diese BSI-Empfehlung ist unter Mitwirkung der als Partner der Allianz für Cyber-Sicherheit registrierten Internet-Service-Provider (*1&1 Internet AG, Deutsche Telekom, Kabel Deutschland, Unity Media KabelBW, Vodafone und Strato AG)* entstanden.
Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

14 https://www.allianz-fuer-cybersicherheit.de/dok/6621328
15 https://www.allianz-fuer-cybersicherheit.de/dok/6621326
16 https://www.allianz-fuer-cybersicherheit.de/dok/6621330
17 https://www.allianz-fuer-cybersicherheit.de/dok/6621332