Bundesamt
für Sicherheit in der
Informationstechnik

Leistungsbeschreibung
Betrieb und Hosting
des WID-Meldungssystems bestehend aus den beiden Web Auftritten
www.cert-bund.de
und
www.buerger-cert.de

Stand: 14.02.2017

14.02.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: certbund@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Essentieller Bestandteil eines erfolgreichen IT-Sicherheitsmanagements ist es, stets über aktuelle Bedrohungen und Gefährdungen, beispielsweise durch neu bekannt gewordene Schwachstellen in Soft- und/oder Hardwareprodukten, durch aktuelle Angriffsverfahren oder durch spontane Verbreitungswellen von Schadprogrammen informiert zu sein.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betreibt seit der Gründung des Computer Emergency Response Teams für die Bundesverwaltung (CERT-Bund) als wesentliche dienstliche Aufgabe den Warn- und Informationsdienst (WID). Dieser leistet gegenüber der öffentlichen Verwaltung (WID-Advisories) und der Öffentlichkeit (WID-Kurzinformation) die zentrale Bereitstellung deutschsprachiger und objektiv bewerteter Warnmeldungen. Hierbei werden über dezidierte Mailing-Listen sowie unter der Web Adresse https://www.cert-bund.de Meldungen zu neuen Schwachstellen und Sicherheitslücken sowie anlassbezogen spezielle Warnungen verteilt.

Ergänzend zu dem oben genannten WID-Dienst betreibt das BSI mit dem Bürger-CERT einen an die Bedürfnisse der Bürger angepassten Warn- und Informationsdienst. Hierbei werden ebenfalls über dezidierte Mailing-Listen sowie unter der Web Adresse https://www.buerger-cert.de entsprechende Meldungen für den Bürger veröffentlicht.

Derzeit wird das WID-System durch die Firma OTRS AG betrieben. Der Hosting-Vertrag läuft zum zum 14.06.2017 aus.

Gegenstand der Leistungsbeschreibung ist der Weiterbetrieb (Hosting) und die Pflege der Komponenten und Services (Web-Portal, Mailversand und Publikationssystem) des WID-Meldungssystem um weitere 24 Monate.

2 Hintergrundinformation

Das "WID-Meldungssystem" ist ein System, welches Advisories, Infomeldungen und andere Meldungen über verschiedene Kanäle veröffentlicht. Dabei sollen die Anforderungen der verschiedenen Zielgruppen, Meldungstypen usw. berücksichtigt werden.

Das WID-Meldungssystem setzt sich aus drei Komponenten zusammen:

- ein Autorensystem zur Erstellung von Meldungen, welches direkt durch das BSI betrieben wird. Das Autorensystem verfügt daneben über eine Importschnittstelle für die Zulieferung extern erstellter Meldungen. Weiterhin nimmt das Autorensysteme die Aufträge entgegen und sendet diese an das Publikationssystem
- ein Publikationssystem zum Steuern und Regeln der Meldungsveröffentlichungen, insbesondere der Verteilung per E-Mail mittels benutzerspezifischer Profile sowie
- ein WID-Webportal mit Meldungsarchiv.

Durch Synergieeffekte können jeweils die Autorensysteme und das Publikationssysteme der beiden WID-Portale www.cert-bund.de und www.buerger-cert.de auf den gleichen Systemen betreiben werden. Die Webportale www.cert-bund.de und www.buerger-cert.de müssen auf getrennten Systemen betrieben werden.

Die Verteilung an Empfängerlisten wird von einer unabhängigen Systemkomponente auch bei großen Abonnentenzahlen zuverlässig und schnell durchgeführt. Im WID-Webportal sind alle veröffentlichten Meldungen in einem kategorisierten Archiv öffentlich zugänglich. Das Layout des Portals ist dabei nicht an die Inhalte gekoppelt, sodass Änderungen in der Darstellung jederzeit möglich sind. Alle drei Komponenten arbeiten über definierte Schnittstellen zusammen und sind modular aufgebaut.

2.1 Systemarchitektur

Die Abbildung 1 zeigt die Zusammenhänge der einzelnen am System beteiligten Rollen und Komponenten zu einem Gesamtsystem. Sie ist in netzwerktopologische Bereiche aufgeteilt und zeigt gleichzeitig über Farbkodierungen die Zuständigkeiten der Komponenten zu den Funktionsbereichen (Erstellung, Publikation, Präsentation).

Die einzelnen Komponenten sind aufgrund ihrer sicherheitstechnischen Anforderungen und netzspezifischen Gegebenheiten in drei separate Netzbereiche aufgeteilt. Das Autorensystem ist in das in BSI betriebene Vorfallbearbeitungssystem von CERT-Bund integriert. Dieses System wird aufgrund der darin gespeicherten sensitiven Informationen im BSI gehostet. Das Publikationssystem und die administrativen Oberflächen befinden sich in einem öffentlichen aber durch entsprechende Vorkehrungen sicheren Netzbereich. Das Webportal und die Mailserver bilden den dritten Netzbereich. Da über diese Server die Kommunikation mit den Zielgruppen stattfindet und sie somit öffentlich erreichbar sind, stehen diese verstärkt im Fokus von externen Angriffen. Dieser Problematik wird unter anderem dadurch begegnet, dass dort die sicherheitsrelevante Datenmenge auf ein Minimum reduziert ist. Die Kommunikation zwischen den Komponenten wird auf drei verschiedene Arten realisiert:

1. Verschlüsselte und signierte E-Mail

   Diese Lösung wird bei der Kommunikation zwischen Autorensystem und

Publikationssystem verwendet. Auf Grund der Abschottung des BSI-Netzes gegen das Internet, gibt es zu der Kommunikation per E-Mail für Systemschnittstellen, die diese Grenze überschreiten müssen keine praktikable Alternative (Autorensystem innerhalb des BSI Netzes und der Rest des WID-Meldungssystem außerhalb). Als Container für die Datenübertragung wird eine XML-Datei verwendet, welche den Vorgaben des WID-Protokolls entspricht. Dieses Protokoll ist speziell für diesen Zweck definiert worden.

2. SOAP über https

   Die Schnittstellen Portal-API, PortalAdmin-API und Content-Manager-API nutzen dieses Protokoll, da es eine synchrone, schnelle, sichere und ausgereifte Technik für den an diesen Stellen nötigen Datenaustausch darstellt.

3. ssh (bzw. in diesem Zusammenhang scp und rsync)

   Dieser Übertragungskanal kommt bei der Kommunikation zwischen Publikationssystem und dem WID-Webportal bzw. den WID-Webportalen an zwei Stellen zum Einsatz

   - beim initialen Aufsetzen des WID-Webportals
   - beim Übertragen der Content-Manager-Inhalte auf das WID-Webportal.

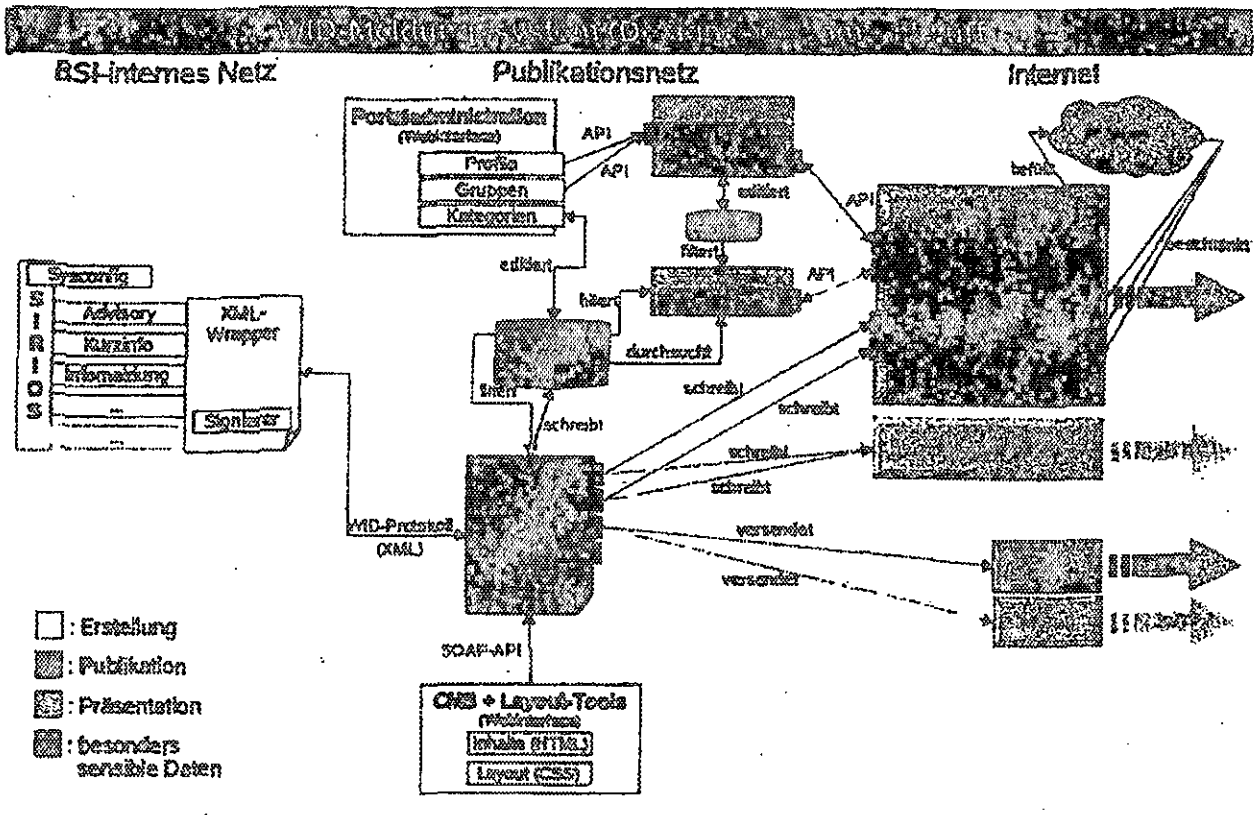

Abbildung 1: Gesamtarchitektur WID-Meldungssystem

3 Leistungsbeschreibung

Von CERT-Bund wird ein Warn- und Informationsdienst (WID) betrieben, über den Meldungen zu neuen Schwachstellen und Sicherheitslücken sowie anlassbezogen spezielle Warnungen an Bundesbehörden, Unternehmen kritischer Infrastrukturen und Industriepartner verteilt werden. Die frühzeitige Verteilung dieser Informationen soll dazu beitragen, Sicherheitsvorfälle im Bereich der Bundesbehörden zu vermeiden oder in ihrer Auswirkung zu beschränken.

Der Anbieter übernimmt den Weiterbetrieb des WID-Meldungssystem www.cert-bund.de und des Bürger-CERT um weitere 24 Monate. Der Anbieter hat folgende Kosten separat auszuweisen:

- gemeinsam genutze Komponenten (von www.cert-bund.de und www.buerger-cert.de) u.a. Publikationssystem, Mailserver, Netzwerkkomponeten, Backup etc.
- sowie die jeweiligen Kosten für die eigentlichen Webserver (www.cert-bund.de bzw. www.buerger-cert.de) - jeweils inklusive des Test- und Vorschausystems).

Derzeit plant das BSI den Webauftritt www.buerger-cert.de in sein Informationsangebot BSI FUER BUERGER überzuführen. Daher behält sich das BSI vor den Leistungsanteil www.buerger-cert.de im einer Frist von einem Monat zu kündigen.

3.1 Allgemeines

3.1.1 Zeitliche Parameter

Die Leistungserbringung erfolgt über eine Laufzeit von 2 Jahren. Es ist eine optionale zweimalige Verlängerung um jeweils 1 Jahr anzubieten.

Der Weiterbetrieb des Hostings der beiden Webauftritte www.cert-bund.de und www.buerger-cert.de erfolgt nahtlos zum 15.06.2017.

3.2 Infrastruktur

3.2.1 Rechenzentrum, Netzwerk und Hardware

Das Rechenzentrum, in dem die WID-Meldungssysteme www.cert-bund.de und www.buerger-cert.de (im Folgenden mit WID-Meldungssystem bezeichnet) gehostet werden, muss über eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz des Rechenzentrums verfügen. Das Zertifikat muss aktuell sein bzw. die Rezertifizierung des Rechenzentrums nach ISO 27001 muss im BSI angemeldet sein.

Netzwerk-Infrastruktur

- Die Netzwerk-Segmente sollen über ein professionelles Rechenzentrums-Firewall-System gesichert werden.
- Vertraglich müssen folgende Bandbreiten zur Verfügung gestellt werden:
  - Internet: 100 MBit/Sek.
  - interne Netze: 1 GBit/Sek.
- Das Backup- und die Administration der Systeme muss über ein separates Netz erfolgen. Dazu benötigen die Systeme über entsprechende Netzwerkschnittstellen.

- Das Rechenzentrum muss über mindestens 3 redundante Netzanbindungen verschiedener, unabhängiger Provider an das Internet verfügen.
- Der Anbieter muss ein dediziertes IP-Subnetz für die Anwendung zur Verfügung stellen.
- Das Testsystem ist in einem eigenen Netzbereich zu betreiben. Für das Produktivsystem ist eine Trennung in Publikationsnetz und „Internetzone", in der sich das Webportal und MTA (Mail Transfer Agent) befinden, vorzunehmen (siehe Abbildung 1 Gesamtarchitektur WID-Meldungssystem).

Der Anbieter hat Hardware- und Infrastrukturkomponenten bereitzustellen. Die Hardwaresysteme sind so zu wählen, dass auf ihnen aktuelle Versionen von

- Betriebssystem Debian
- Webserver Apache
- Datenbanksystem MySQL und
- Mailverteilsystem Postfix

lauffähig sind.

Vom Anbieter sind mindestens fünf professionelle 19"-Serversysteme für den Rechenzentrumsbetrieb, die dem derzeitigem Stand der Technik entsprechen, vorzusehen: eines für die Publikationssysteme, je eines für die beiden WID-Webportale www.cert-bund.de und www.buerger-cert.de (inklusive Vorschausysteme), ein Testsystem und eines für den MTA. Das für das Testsystem eingesetzte Serversystem ist mit mehreren virtuellen Maschinen analog zu dem Produktivsystem, z.B. mittels VMWare, auszustatten.

Es ist von einem E-Mailversand von 3000 Stück pro Minute auszugehen und einer Spitzenabdenkung von 1000 Seiten pro Stunde über das Webportal auszugehen. Für den Fall einer auftretenden höheren Spitzenabdeckung als angenommen, ist das Loadbalancing zu berücksichtigen und als Option anzubieten.

Es wird eine Netzwerk-Verfügbarkeit von 99,95% (Jahresdurchschnitt) und eine Applikations-Verfügbarkeit von 99% (Jahresdurchschnitt) gefordert. (Die „Verfügbarkeit" ist in Kapitel 3.3.3 definiert).

Der Anbieter hat sicherzustellen, dass die Administration des WID-Meldungssystems entweder Vor-Ort im Rechenzentrum oder remote über VPN-Tunnel statt findet. Die VPN-Tunnel müssen die Authentizität der Administratoren und Verschlüsselung gewährleisten.

3.3 Betrieb und Service

3.3.1 SLA und Servicedesk

Der Anbieter hat den Betrieb des gesamten WID-Meldungssystem-Services gegenüber dem BSI zu verantworten. Für die strukturierte Bearbeitung sämtlicher Anfragen (Service Requests), Änderungswünsche (RfC - Request for Change) und Störungsmeldungen (Incidents) soll der Anbieter dem BSI einen Servicedesk zur Verfügung stellen, der als Single-Point-of-Contact sämtliche Vorgänge erfasst, deren Bearbeitung koordiniert und für die schnellstmögliche Wiederherstellung des Service Sorge trägt. Der Anbieter hat mindestens die Meldewege „Telefon" und „E-Mail" anzubieten.

Das BSI wird dem Anbieter melde-berechtigte Mitarbeiter des BSI unter Angabe der Erreichbarkeiten benennen. Für die Erstellung und Abwicklung von Anfragen sind diese BSI-Mitarbeiter, das Lagezentrum, sowie die Fachkraft in Bereitschaft berechtigt. Diese Personen müssen sich über eine feste Rufnummer authentifizieren. Sofern weitere Meldewege eingesetzt werden, sind dafür entsprechende Authentifizierungsmechanismen zu benennen und zwischen BSI und Anbieter abzustimmen.

Bereitstellung des Servicedesk:

Servicezeit (CET): Mo.-So. 0:00 – 24:00 (auch an Feiertagen)

Reaktionszeit: Incidents mit "Critical Impact": 2 Std.

Reaktionszeit: Incidents mit "Medium Impact": 4 Std.

Reaktionszeit: Incidents mit "Low Impact": 24 Std.

Die Impact-Level sind im nachfolgenden Abschnitt exemplarisch definiert.

3.3.2 Support

Gefordert ist ein Support auf 24x7-Basis aller verwendeten Komponenten, d.h. sowohl für die eingesetzte Hard- als auch Software. Die Reaktionszeit beginnt mit der initialen Meldung über eines dieser Meldewege.

Der Anbieter hat das BSI-Lagezentrum unmittelbar bei IT-Sicherheitsvorfällen oder bei Verdacht auf IT-Sicherheitsvorfälle zu informieren. Des Weiteren hat er im Rahmen der vereinbarten Reaktionszeiten bei Incident-Response-Maßnahmen anlassbezogen zu unterstützen.

Der Anbieter ist verpflichtet das BSI initiativ im Fall von Incidents mit „Critical Impact" zu benachrichtigen. Bei sicherheitsrelevanten Vorfällen ist die Fachkraft in Bereitschaft telefonisch im Rahmen der Servicezeit zu benachrichtigen; bei nicht-sicherheitsrelevanten Vorfällen ist das BSI-Lagezentrum (Zeitfenster 09:00 bis 16:00 Uhr) telefonisch zu unterrichten. Der Anbieter verpflichtet sich innerhalb der vertraglich vereinbarten Zeiten auf die Incidents zu reagieren (siehe Kapitel 3.3.1).

Es stehen die folgend aufgeführten Impact-Level zur Verfügung:

3 – Impact Critical	*Mission Critical Incidents (Störungen), welche zum Ausfall des gesamten Systems oder businesskritischer Funktionen führen und eine schnellstmögliche Analyse und Behebung des Incidents erfordern*
	Beispiele: ***Sicherheitsrelevant***
	Beispiel 1: *Das WID-Meldungssystem unterliegt einem DoS-Angriff.*
	Beispiel 2: *Der öffentliche Bereich des WID-Meldungssystem wurde kompromittiert, Inhalte wurden verändert.*
	Beispiel 3: *Es werden Angriffe auf die Profil-Datenbank festgestellt.*
	Nicht-sicherheitsrelevant
	Beispiel 1: *Das WID-Meldungssystem unterliegt einem Hardware-bedingten Ausfall. Der Service steht kurzzeitig nicht zur Verfügung.*
	Beispiel 2: *Die Anmeldedatenbank reagiert nicht, es können sich keine Nutzer am Portal anmelden. Nur der öffentliche Bereich ist erreichbar.*

	Beispiel 3: Der E-Mail-Versand ist temporär (>4 Std.) nicht möglich.
2 – Medium Impact	Incidents (Störungen), welche die Funktionsweise des gesamten Systems oder wichtiger Funktion bei einem oder mehreren Anwendern einschränken und eine schnelle Behebung des Incidents erfordern. ▶ Benachrichtigung über das Monatsreporting *Beispiele:* *Beispiel 1:* Veröffentlichen von Meldungen ist nur beschränkt möglich. *Beispiel 2:* Das WID-Meldungssystem unterliegt Performance Problemen; das Arbeiten ist aber uneingeschränkt möglich. *Beispiel 3:* Ausfall des Publikationssystems; das Veröffentlichen von Meldungen ist nicht möglich.
1 – Low Impact	Incidents (Störungen), welche die Nutzung der Software nicht oder nur unwesentlich einschränken. In diese Kategorie fallen auch Service- und Features Requests (Anfragen) ohne gesonderte Dringlichkeit. ▶ Benachrichtigung über das Monatsreporting *Beispiele:* *Beispiel 1:* Das BSI benötigt Auskunft für nicht im Vorfeld definierte Statistiken/Reports. *Beispiel 2:* Sicherheitskritische Updates der eingesetzten Software-Komponenten. *Beispiel 3:* Erweiterung/Austausch von Hardwarekomponenten ohne Beeinträchtigung der Services.

3.3.3 Reporting

Der Anbieter hat zum jeweils vierten Arbeitstag eines Monats (Mo. - Fr.) über den Vormonat den Status der Incident- und Service-Request-Meldungen sowie die Verfügbarkeit der aufgeführten Komponenten zu berichten. Die Form der Reports und der Kommunikationskanal sind auf dem Kick-Off-Meeting abzustimmen.

Der Anbieter hat folgende Reports anzubieten:

- Report aller monatlichen Vorfälle
- Jahresdurchschnittliche Verfügbarkeit des Netzwerks
- Jahresdurchschnittliche Verfügbarkeit der Applikation
- Auslastung der Systeme (Durchschnitts- und Spitzenwerte von CPU-Last, Speicherauslastung, Plattenplatz)

Die Verfügbarkeiten des Netzwerks und der Applikation ist mit diesen Methoden zu berechnen:

- Zur Messung der Verfügbarkeit des Netzes werden ICMP-Echo-Requests (PINGs) eingesetzt. Die Verfügbarkeit des Netzwerkes gilt als gegeben, wenn in einem betrachteten Zeitraum von allen ICMP-Echo-Requests, die in regelmäßigen Abständen von je einer Sekunde an ein Zielsystem in dem Netzwerk versandt werden, höchstens 5 Prozent nicht innerhalb von einer Sekunde mit einer gültigen ICMP-Echo-Reply-Antwort quittiert werden.
- Zur Messung der Verfügbarkeit des Webportals werden HTTP-GET-Requests eingesetzt. Das Portal gilt als verfügbar, wenn in einem betrachteten Zeitraum von allen HTTP-GET-Requests, die in regelmäßigen Abständen von je einer Minute an den entsprechenden Dienst gestellt werden, höchstens 5 Prozent nicht innerhalb von 10 Sekunden mit einer gültigen und inhaltlich entsprechenden Antwort quittiert werden. Für andere Dienste-Komponenten des WID-Meldungssystems gilt dieses Kriterium entsprechend, sofern nicht anders vereinbart.

3.3.4 Systemwartung und Security-Update-Management

Der Anbieter hat planmäßige wartungsbedingte Ausfälle rechtzeitig anzukündigen und mit dem BSI abzustimmen. Bei Notfall-Wartungen wird eine umgehende Informationspflicht gefordert. Wartungsfenster sind wie folgt definiert:

Planmäßiges Wartungsfenster (Normale Wartungen):

- Der Anbieter muss normale Wartungsfenster 4 Werktage im Vorfeld beim BSI anmelden.
- Wartungsfenster dürfen in diesem Fall max. 4 Std. dauern.
- Es kann max. 1 Wartungsfenster / Monat durchgeführt werden.

Außerplanmäßiges Wartungsfenster (Security Updates):

- Der Anbieter muss außerplanmäßige Wartungsfenster 1 Werktag im Vorfeld beim BSI anmelden.
- Wartungsfenster dürfen in diesem Fall max. 1 Std. dauern.

Emergency-Wartungsfenster (Systemeinbrüche):

- Der Anbieter muss Emergency-Wartungsfenster umgehend beim BSI anmelden.
- Der Meldeweg entspricht dem eines „Critical Impact" Incidents

Der Anbieter muss die Versorgung der Server mit aktuellen Patches sicherstellen. Einzuspielende Security-Updates sind vor der Installation auf einem Testsystem durch den Anbieter zu prüfen und freizugeben, damit weitestgehend sicher gestellt werden kann, dass die Serversysteme durch die Patches nicht in ihrer Funktion und Sicherheit gefährdet sind.

3.3.5 Backup-Service

Der Anbieter ist für das Backup/Recovery zuständig. Die Sicherungen müssen wöchentlich als Full-Backup erfolgen; ansonsten ist täglich ein inkrementelles Backup (immer relativ zum letzten Full-Backup) ausreichend. Es sind die jeweils letzten 10 Backup-Zyklen aufzubewahren.

Zusätzliche Sicherheit im Katastrophenfall und gegen menschliche und technische Fehler sind durch eine Replikation der Sicherung zu einem zweiten System sicherzustellen. Sowohl auf dem lokalen als auch auf dem Offsite-Backup-System ist eine Dateisystemverschlüsselung einzusetzen, sodass die Daten zwar - solange der Rechner online ist - verfügbar sind, aber vor physikalischem Zugriff (Manipulation, Diebstahl etc.) geschützt sind.

Der Transfer der Daten zum Offsite-Backup-System muss über eine verschlüsselte Verbindung geschehen. Weiterhin muss die Identität des Offsite-Backup-Systems überprüft werden. Für das Backup ist ein eigenständiges Netzwerk zur Verfügung zu stellen - das Backup darf auch bei großen Backupvolumen keine Beeinträchtigung der IP-Anbindung ins Internet verursachen.

3.3.6 Monitoring

Dem Monitoring kommt beim Betrieb des WID-Meldungssystems eine wichtige Rolle zu. Man unterscheidet die Überwachung des Zustands und das Protokollieren der Verlaufsdaten. Ersteres ermöglicht jederzeit, den Zustand des Systems abzufragen und die bei Fehlfunktionen automatisch zu bestimmende Aktion auszuführen. Letzteres hilft im Rahmen des Reportings, Ressourcen zu bewerten und Engpässe frühzeitig zu erkennen.

Zur Realisierung der Überwachung sind mindestens die folgenden Methoden zu implementieren:

- Überwachung durch direkte Anfrage des Monitoringhosts an einen Dienst, zum Beispiel ein HTTP-GET-Request auf eine definierte URL, Verbindungstests zu der Datenbank und Abfragen systemnaher Werte über SNMP. In Zusammenarbeit mit dem BSI sind Abfrage-Szenarien zu entwickeln, die die Sicht auf die zu hostende Applikation wiedergeben
- Überwachung durch einen auf dem Host installierten Agenten. Der Agent muss mindestens die systemnahen Werte CPU- und Speicherauslastung, Festplattennutzung, Netzwerkdurchsatz erfassen. Die Daten sind in regelmäßigen Abständen zu erfassen, sodass zeitnah Engpässe erkannt werden und gemäß der in Abschnitt 3.3.2 definierten Impact-Level dem BSI zu berichten.

3.4 Sonstiges

3.4.1 Datenschutz

Der Anbieter muss sich vertraglich auf die Einhaltung datenschutzrechtlicher Bestimmungen verpflichten.

3.4.2 Abnahme

Der Anbieter stellt quartalsweise Rechnungen über den Hardwarebetrieb und das Hosting des WID-Meldungssystems. Zur Abnahme der erbrachten Hostingleistung sind die monatlichen Reports gemäß Kapitel 3.3.3 dem BSI vorzulegen.

3.4.3 Anbieterprofil

Der Anbieter hat ein Unternehmensprofil unter Angabe von Referenzen insbesondere mit der öffentlichen Verwaltung abzugeben.

3.4.4 Reisekosten

Reisen sind nicht erforderlich. Ggf. anfallende Reisekosten hat der Anbieter zu tragen.

4 Anhang

4.1 Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CPU	Computer Processing Unit
HTTP	Hyper Transfer Text Protokoll
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protokoll
MTA	Mail Transfer Agent
RfC	Request for Comment
SIRIOS	System für Incident Response In Operational Security
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
ssh	Secure Shell
URL	Uniform Resource Locator
VPN	Virtuell Privat Network
WID	Warn- und Informationsdienst
XML	Extensible Markup Language

4.2 Glossar

CERT	Ein CERT ist eine Arbeitsgruppe, die sicherheitskritische Vorfälle im Zusammenhang mit IT-Strukturen sammelt, bewertet und ggf. Warnmeldungen veröffentlicht.
CPU	Im allgemeinen Sprachgebrauch wird die CPU oftmals nur als Prozessor bezeichnet und ist die zentrale Verarbeitungseinheit eines Computers. Sie steuert, regelt und kontrolliert Arbeitsprozesse.
HTTP	HTTP ist ein Protokoll zur Übertragung von Daten über ein Netzwerk. Es wird hauptsächlich eingesetzt, um Webseiten aus dem Internet in einen Internetbrowser zu laden.
ICMP	ICMP ist ein Protokoll zur Übertragung von Statusinformationen und Fehlermeldungen von IP-, TCP- und UDP-Protokollen zwischen IP-Netzknoten. Es wird u. a. von

	Protokollen zur dynamischen Ermittlung von Routen verwendet.
IDS	Ein IDS ist ein System zur Erkennung von Angriffen, die an ein Computersystem oder Computernetz gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken erhöhen.
IP	Das Internet-Protokol ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und stellt die Grundlage des Internets dar. Die Aufgabe des Internet-Protokolls besteht darin, Datenpakete von einem Sender über mehrere Netze hinweg zu einem Empfänger zu transportieren. Die Übertragung ist paketorientiert, verbindungslos und nicht garantiert.
Loadbalancing	Unter Loadbalancing werden Verfahren zur Lastverteilung verstanden, um bei der Speicherung, dem Transport und der Verarbeitung von Objekten vorgegebene Kapazitätsgrenzen einzuhalten.
MTA	Als MTA wird ein Programm bezeichnet, das E-Mails innerhalb von Netzwerken (z. B. dem Internet) weiter transportiert.
RfC	RfC sind chronologisch nummerierte Publikationen der IETF (*Internet Engeneerig Task Force*), in denen allgemeingültige Spezifikationen als Bestandteil des "Internet-Standards" definiert sind. Die IETF ist zuständig für die Klärung und Standardisierung von Protokoll- und Architekturbelangen des Internet.
SIRIOS	SIRIOS ist ein Vorfallsbearbeitungssystem für CERT. Es basiert auf dem Trouble-Ticket-System OTRS, mit dem die komplette Korrespondenz (E-Mail, Telefon, usw.) lückenlos zu erfasst werden kann. Die einzelnen Module von SIRIOS ermöglichen eine strukturierte Be- und Verarbeitung von CERT-spezifischen Informationen (z.B. Advisories und Incidents).
SNMP	SNMP ist ein Netzwerkprotokoll, das Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern kann. Das Protokoll regelt die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. SNMP beschreibt den Aufbau der zu versendenden Datenpakete und den Kommunikationsablauf. SNMP ist in der Lage jedes netzwerkfähige Gerät mit in die Überwachung aufzunehmen.
SOAP	SOAP ist ein Kommunikationsprotokoll zum Zugang zu einzelnen Projekten im Internet. Es wird als Anwender-Schnittstelle bei Webservices eingesetzt. SOAP ist ein schlankes Protokoll, mit dem proprietäre Module verpackt und mit allgemein verständlichen Schnittstellen versehen werden können.
ssh	ssh bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit deren Hilfe man auf eine sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem entfernten Computer herstellen kann.
URL	Eine URL gibt eine Adresse im Internet an. Sie besteht aus dem Protokoll (z. B. http://), dem Rechnernamen (z. B. www.bsi.de) und ggf. auch aus der Angabe des Ports (z. B.: 80) und der Pfadangabe.
VPN	Ein VPN dient der Einbindung von Geräten eines benachbarten Netzes an das eigene Netz, ohne dass die Netzwerke zueinander kompatibel sein müssen.
XML	XML ist eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten in Form von Textdaten und wird u. a. für den Austausch von Daten zwischen

Computersystemen eingesetzt, insbesondere über das Internet.