Dienstbeschreibung DFN.Security

1 Zweck dieser Dienstbeschreibung

Diese Dienstbeschreibung gibt einen grundlegenden Überblick über den Leistungsumfang des Dienstes DFN.Security und stellt Voraussetzungen und Rahmenbedingungen für die Teilnahme an diesem dar. Der Dienst DFN.Security steht mit „Basisleistungen“ allen Teilnehmern im DFN zur Verfügung und kann mittels der „erweiterten Leistungen“ für Teilnehmer mit besonderen Sicherheitsanforderungen bzw. höheren oder sehr hohen Schutzbedarfen ergänzt werden.

Diese Dienstbeschreibung ergänzt inhaltlich die Dienstvereinbarung DFN.Security um organisatorische und technische Details zur Realisierung, zum Betrieb und zu betrieblichen Anforderungen.

Sie wird nach den Erfordernissen und im Interesse seiner Mitglieder und Nutzerschaft des DFN-Vereins und im Hinblick einer zeit-, bedarfs- und kostengerechten Weiterentwicklung des Dienstes zukünftig erweitert und aktualisiert.

2 DFN.Security auf einen Blick

Mit dem Dienst DFN.Security stellt der DFN-Verein seinen Teilnehmern ein Bündel an Leistungsmerkmalen zur Erhöhung der Informationssicherheit von durch den Teilnehmer betriebenen IT-Infrastrukturen bereit.

DFN.Security orientiert sich an den spezifischen Bedarfen der wissenschaftlichen Einrichtungen und wurde konsequent auf die Einsetzbarkeit in heterogenen IT-Landschaften, wie sie in wissenschaftlichen Einrichtungen vornehmlich vorhanden sind, ausgerichtet. Als eines der weltweit leistungsfähigsten Portfolios an Leistungsmerkmalen zur Förderung der Informationssicherheit an Wissenschaftseinrichtungen unterstützt der Dienst DFN.Security damit den sicheren Betrieb von Informationsinfrastrukturen zur Unterstützung exzellenter Forschung in Deutschland. Der Dienst umfasst Merkmale, welche auf die Sicherstellung von Verfügbarkeit, Integrität und Vertraulichkeit von Daten und Systemen ausgerichtet sind.

2.1 Leistungsumfang

Der DFN.Security-Dienst umfasst zwei Dienstkategorien. Die Dienstkategorie „Basisleistungen“ schließt folgende grundlegende Leistungsmerkmale ein, die allen Teilnehmern am Deutschen Forschungsnetz für die Einbindung in die eigenen Informationssicherheitsmanagementprozesse zur Verfügung stehen

- Unterstützung bei dem Security Incident Management im Falle eines Angriffs oder Sicherheitsvorfalls durch das Incident Response Team (IRT) des DFN-CERT.
- Überwachung einer begrenzten Anzahl von Diensten bzw. IT-Systemen auf Kompromittierungen durch Logdaten-Analyse
- Zustellung von Warnmeldungen über mögliche Sicherheitsvorfälle mit Bezug zu IP-Adressen oder Internetdomains des Teilnehmers mit Handlungsempfehlungen[1]
- Zustellung von Schwachstellenmeldungen zu vom Teilnehmer betriebenen Diensten bzw. IT-Systemen
- Überprüfung des Netzes des Teilnehmers auf aus dem DFN-Netz offen erreichbare Dienste bzw. IT-Systeme durch den Netzwerkprüfer[2]
- Überwachung einer begrenzten Anzahl von IT-Systemen auf Kompromittierungen durch aktives Dienstemonitoring mittels der Komponente SOC-Probe
- Schutz vor dem Zugriff auf bösartige Domains mittels DNS-RPZ
- DoS-Basisschutz zur Analyse und Abwehr von DDoS-Angriffen[3]
- Zugriff auf das DFN.Security-Portal (ehemals DFN-CERT Portal) zur Konfiguration der oben genannten Leistungsmerkmale im Self-Service

Die Leistungsmerkmale sind komplementär und ergänzen sich. Der Teilnehmer kann frei entscheiden, welche der o. g. Leistungsmerkmale aktiv in Anspruch genommen werden und welche nicht.

Für Teilnehmer mit erweiterten Sicherheitsanforderungen bzw. höheren oder sehr hohen Schutzbedarfen umfasst der DFN.Security-Dienst zusätzliche Leistungsmerkmale in der Dienstkategorie „erweiterte Leistungen“. Die erweiterten Leistungen werden im Rahmen der Kostenumlage des DFN-Vereins mit einem separaten Entgelt realisiert, welches durch die Mitgliederversammlung des DFN-Vereins beschlossen wurde. Die erweiterten Leistungen umfassen folgende Leistungsmerkmale:

- Alle Merkmale der Basisleistungen
- Bereitstellung eines SOC-Agents, welcher im Netz des Teilnehmers Ereignisdaten (z. B. Logdaten) der dafür ausgewählten Systeme aggregiert und an die Auswertungssysteme beim DFN-CERT weiterleitet, wo sie vollautomatisiert auf Hinweise zu sicherheitsrelevanten Vorfällen untersucht werden. Zusätzlich erfolgt eine manuelle Sichtung und Bewertung erkannter Anomalien durch Experten des DFN-CERTs

[1] Es können nur Warnmeldungen mit IP-Bezug zugestellt werden, wenn die IP-Adressen zu einem direkt an das X-WiN angeschlossenen Adressbereich gehören.

[2] Es können nur Netze des Teilnehmers geprüft werden, die direkt an das X-WiN angeschlossen sind.

[3] Der DoS-Basisschutz kann ausschließlich von Teilnehmern genutzt werden, die gemäß der Entgeltordnung des DFN-Vereins hierzu berechtigt sind.

- Aktive kontinuierliche Suche nach neuen bisher unbekannten Bedrohungsmustern (Indicators of Compromise, IoC) durch Threat Hunter im DFN-CERT
- Überwachung von IT-Systemen auf Kompromittierungen durch aktives Dienstemonitoring mittels der Komponente SOC-Probe
- Begleitende Beratung und Unterstützung bei der Modellierung der Schutzgegenstände des Teilnehmers durch Experten des DFN-CERT
- Regelmäßige Überprüfung der Kontaktdaten der Ansprechpersonen bzw. Eskalationswege
- Aktive Überwachung des X-WiN-Anschlusses des Teilnehmers in Ergänzung des DoS-Basisschutz zur Erkennung, Analyse und Abwehr von DoS-Angriffen[4]

Teilnehmer mit den Basisleistungen des DFN.Security-Dienstes können die erweiterten Leistungen über eine vom DFN-Verein bereitgestellte Ergänzungsvereinbarung zur Dienstvereinbarung des DFN.Security-Dienstes zu den dort definierten Konditionen beauftragen, wenn sie dies wünschen.

2.2 Dienstkategorien

Der Dienst steht in zwei Kategorien „Basisleistungen“ und „erweiterte Leistungen“ zur Verfügung. Die Leistungsmerkmale beider Kategorien sind in Abschnitt 2.1 kurz aufgelistet und werden nunmehr in Kapitel 3 bzw. 4 detaillierter beschrieben.

3 Leistungsmerkmale der Basisleistungen

Grundsätzlich hat ein Teilnehmer die Wahl, welche Merkmale der Basisleistungen er in Anspruch nimmt. Sie können jeweils eigenständig genutzt werden, entfalten aber im Zusammenspiel aller Leistungen die maximale Schutzwirkung.

3.1 Unterstützung bei der Reaktion auf Angriffe und Vorfälle

Das Incident Response-Team (IRT) des DFN-CERT ist auf die schnelle und effiziente Analyse und Reaktion bei Sicherheitsvorfällen ausgerichtet. Es unterstützt bei der Analyse und Beschaffung von Daten, der Vermittlung von Kontakten, der Bekämpfung von Quellen (wie z. B. der Deaktivierung von Phishing-Seiten) und gibt Hilfestellungen und Handlungsempfehlungen für die Vorfallsbearbeitung. Dafür koordiniert das IR-Team seine Aktivität in nationalen und internationalen Kooperationen mit anderen Computer-Notfallteams und unterstützt die Kooperation operativer Sicherheitsteams deutscher Hochschulen, Lehr- und Forschungseinrichtungen aktiv im EDUCV (https://www.educv.de/).

[4] Die aktive Überwachung kann nur an Anschlüssen mit realisiertem DoS-Basisschutz erfolgen.

3.2 Logdaten-Analyse

Für die Logdaten-Analyse werden Schnittstellen zur Übermittlung von Logdaten an das DFN-CERT bereitgestellt. Die Log-Daten werden anschließend anhand der im DFN-CERT vorhandenen Bedrohungsmuster (Indicators of Compromise, IoC) hinsichtlich potenzieller Sicherheitsvorfälle analysiert. Zur Einlieferung der Log-Daten wird dem Teilnehmer ein SOC-Connector sowie Beschreibungen zur Konfiguration und Nutzung dieses Leistungsmerkmals bereitgestellt, um eine weitgehend eigenständige Aktivierung durch den Teilnehmer zu ermöglichen.

Erkannte Auffälligkeiten werden über die etablierten Meldewege entsprechend der im DFN.Security-Portal hinterlegten Kontakte mittels der Automatischen Warnmeldungen den teilnehmenden Einrichtungen gemeldet. Bei gravierenden Sicherheitsproblemen ist eine direkte Kontaktaufnahme durch das SOC des DFN-CERT möglich.

3.3 Zustellung von Warnmeldungen

Die Automatischen Warnmeldungen können von allen DFN-Teilnehmern über das DFN.Security-Portal genutzt werden. Warnmeldungen werden für eine Einrichtung erzeugt, wenn beim DFN-CERT Auffälligkeiten im Zusammenhang mit IP-Adressen oder Domains dieser Einrichtung bekannt geworden sind. Bei den Auffälligkeiten handelt es sich in der Regel um Hinweise zu vermuteten Kompromittierungen. Der Dienst wird allerdings kontinuierlich um präventive Anteile erweitert und umfasst daher auch Informationen zu potenziell problematischen Konfigurationen/Systemen/u. ä. die keinen direkten Hinweis auf eine Kompromittierung darstellen. Dieser Dienst erweitert die etablierte "manuelle" Unterstützung bei Sicherheitsvorfällen, aber ersetzt diese nicht. Wenn das DFN-CERT Hinweise auf gravierende Sicherheitsprobleme in einer Einrichtung erhält, wird über diese wie bisher direkt und so schnell wie möglich informiert. Die vom DFN-CERT verschickten Warnmeldungen haben immer den gleichen Grundaufbau. Sie enthalten eine Zusammenfassung bzgl. der betroffenen IP-Adressen bzw. Domains, den Meldungstyp und einen Zeitstempel.

Zur Erstellung der Warnmeldungen beobachtet und analysiert das DFN-CERT eine Reihe von öffentlichen und teilweise geschlossenen Quellen, um Probleme zu entdecken, die einen Bezug zu Systemen im DFN besitzen. Darüber hinaus werden eigene Sensoren betrieben, um die Informationsbasis auszuweiten. Das DFN-CERT sammelt, korreliert und normiert diese Daten und stellt jedem Teilnehmer den Zugriff auf die Daten seiner Einrichtung zur Verfügung. Dies umfasst die Möglichkeit zur Konfiguration einrichtungsspezifischer Einstellungen.

Meldungen mit Bezug zu IP-Adressen können den jeweiligen Teilnehmern vom DFN-CERT automatisch auf Basis der jeweiligen IP-Dienste des Teilnehmers zugeordnet werden. Von der Einrichtung verwendete Domains müssen vom Teilnehmer im DFN.Security-Portal hinterlegt werden und werden nach einer erfolgten Domainvalidierung für die Verteilung von Informationen verwendet. Domainvalidierungen haben eine begrenzte Gültigkeit, müssen also regelmäßig wiederholt werden. Um einen Verlust von Meldungen aufgrund einer abgelaufenen

Domainvalidierung zu verhindern, wird die erneute Prüfung, soweit möglich, durch automatische Prozesse im DFN.Security-Portal unterstützt.

Die Ereignisse, auf denen die Automatischen Warnmeldungen basieren, können jederzeit unmittelbar über das DFN.Security-Portal eingesehen werden. Zusätzlich kann sich der Teilnehmer per E-Mail über neu aufgetretene Warnmeldungen informieren lassen. Je nach Dringlichkeit der Meldung werden diese E-Mails umgehend versandt oder zu festgelegten Zeiten als Sammelbenachrichtigung zugestellt.

Alternativ können die Meldungen über einen RSS-Feed, der unter einer nicht ratbaren URL ohne Client-Authentifizierung bereitsteht, abgerufen werden. Der Feed erlaubt eine Filterung nach Meldungstyp, Netzsegment oder Domainname.

3.4 Zustellung von Schwachstellenmeldungen

Erfahrungsgemäß ist der Aufwand zur Behebung eines Schadens meist wesentlich größer als der Aufwand zu dessen Verhinderung.

Das DFN-CERT legt daher besonderen Wert auf eine Unterstützung der Teilnehmer mittels präventiver Maßnahmen. Durch vorbeugende Maßnahmen sollen Schwachstellen beseitigt werden, bevor Angreifer diese ausnutzen. Hierfür stellt das DFN-CERT Schwachstellenmeldungen zu einer Vielzahl von Produkten zur Verfügung, eine aktuelle Liste der unterstützten Produkte wird vom DFN-Verein online zur Verfügung gestellt.

Die Schwachstellenmeldungen können von allen Teilnehmern über das DFN.Security-Portal genutzt werden. Sie erhalten dann umgehend eine Benachrichtigung, wenn in einem System neue Schwachstellen bekannt geworden sind und Maßnahmen zu deren Mitigation zur Verfügung stehen. In einer Schwachstellenmeldung enthalten sind daher in der Regel auch Links auf Patches, mit denen die Schwachstellen beseitigt werden können oder Hinweise auf Workarounds oder Mitigationen. Im DFN.Security-Portal kann konfiguriert werden, zu welchen Systemen diese Informationen per E-Mail bezogen werden sollen sowie an welche Empfänger ein Versand erfolgt. Dabei wird die Auswahl bezüglich der zu beziehenden Schwachstellenmeldungen anhand eines Kategorienbaums, der in Plattformen und Software-Kategorien aufgeteilt ist, getroffen. Alternativ kann ein Abonnement auf CPE-Basis (Common Platform Enumeration) hinterlegt werden. Zusätzlich kann für den E-Mail-Versand entschieden werden, ob eine Schwachstellenmeldung einen minimalen Schweregrad besitzen muss und zur Vereinfachung der Filterung kann ein Präfix für die Meldungen definiert werden.

Jede Schwachstellenmeldung besitzt eine Bewertung nach mindestens CVSS (Common Vulnerability Scoring System) Version 3.1 des Base- und Temporal Scores. Zur automatischen Verarbeitung umfasst jede E-Mail einen maschinenlesbaren Anhang, derzeit im JSON-Format, mit dem Meldungstext.

Die oben genannten Kategoriebäume sowie die konkreten Softwareprodukte unterliegen Änderungen bzw. werden in Abhängigkeit von den unterstützten Distributionen und Systemen

kontinuierlich ergänzt. Informationen über diesbezügliche Änderungen können im DFN.Security-Portal gesondert per E-Mail abonniert werden.

3.5 Netzwerkprüfer

Dieser Infrastrukturdienst kann von allen Teilnehmern über das DFN.Security-Portal genutzt werden. Mit dem Netzwerkprüfer kann eine Einrichtung die eigenen (und nur diese!) Adressbereiche von außen selbst prüfen.

Der Netzwerkprüfer scannt maximal ein Class C-Netz, also 256 Adressen, mit einem Standardscan. Über diesen werden aktive Systeme und offene Ports ermittelt, getestet werden die am häufigsten benutzen ca. 19.000 TCP-, UDP- und SCTP-Ports.

Bei einem auf bis zu acht Adressen beschränkten Scan findet ein Tiefenscan statt, der bei offenen Ports zusätzlich eine Diensterkennung (Banner Grabbing) durchführt.

Eine Liste erreichbarer Systeme und offener Ports wird als Scan-Ergebnis angezeigt. Es besteht die Möglichkeit, Scans regelmäßig wiederholen zu lassen sowie Scan-Ergebnisse über die Weboberfläche des Netzwerkprüfers, die Teil des DFN.Security-Portals ist, miteinander zu vergleichen. So werden nicht nur Veränderungen aufgezeigt, sondern es kann auch geprüft werden, ob durchgeführte Änderungen beispielsweise an der Firewall zu den gewünschten Ergebnissen geführt haben.

Bei allen Ergebnissen ist zu beachten, dass diese die Sicht eines externen Scans wiedergeben. Erfolgt ein vergleichbarer Scan aus dem internen Netz, können die Ergebnisse abweichen.

3.6 Aktives Dienstemonitoring

Durch das aktive Dienstemonitoring mittels SOC-Probe werden Teilnehmer beispielsweise über in Kürze ablaufende Zertifikate, unbeabsichtigt öffentlich oder ungeplant nicht verfügbare Serverdienste und andere, ähnlich gelagerte Sicherheitsmängel, informiert. SOC-Probe wird vom DFN-CERT betrieben und durch den Teilnehmer im Self-Service konfiguriert. Das Dienstemonitoring stellt somit eine externe Sicht auf Dienste zur Verfügung.

In Abhängigkeit von dem konkreten Sicherheitsmangel wird der Teilnehmer direkt oder zu festgelegten Zeiten über den Missstand informiert. Die Information erfolgt über den bekannten Kanal der Automatischen Warnmeldungen. In den Basisleistungen kann dieses Leistungsmerkmal nur für eine begrenzte Anzahl von überwachten Systemen angeboten werden.

3.7 Schutz vor dem Zugriff auf bösartige Domains mittels DNS-RPZ

DNS-RPZ (Domain Name System Response Policy Zone) ist ein Verfahren, um bei der Namensauflösung durch rekursive DNS-Resolver mittels eigener Richtlinien einzugreifen und

dadurch letztlich den Zugriff auf bestimmte Domains zu unterbinden. Über den Dienst wird ein Feed (genauer mehrere Response-Policy-Zonen) bereitgestellt, in dem Informationen zu maliziösen Domains gesammelt zur Verfügung stehen. Zur Nutzung dieses Leistungsmerkmals benötigt der Teilnehmer einen RPZ-fähigen DNS-Resolver oder eine entsprechende Appliance.

Wird eine Zone aufgrund neuer Erkenntnisse aktualisiert, wird der DNS des Teilnehmers informiert. Durch den automatischen Abruf der aktualisierten Zone und die Einbindung in das eigene DNS wird direkt auf neu ermittelte Bedrohungen reagiert. Stellen Nutzende eine DNS-Anfrage für eine Seite mit maliziösen Inhalten, die in einer eingebundenen Zone gelistet ist, liefert der DNS-Resolver nicht die IP-Adresse der angefragten Seite, sondern die einer sicheren Landingpage zurück. Die Landingpage informiert die Nutzenden über die erfolgte Umleitung der DNS-Anfrage und stellt einen teilnehmerspezifischen Supportkontakt bereit. Teilnehmer können die über den Dienst verfügbare Landingpage nutzen oder eine eigene Webseite erstellen.

Eine Übersicht über die Blockierungsvorgänge in der eigenen Einrichtung steht mittels der Logdaten-Analyse zur Verfügung. Mit dem Übermitteln der betreffenden DNS-Server-Logs werden die geblockten Zugriffsversuche in Form automatischer Warnmeldungen für Administrierende zusammengefasst.

Das Extrahieren von Daten aus dem DNS-RPZ-Feed und deren Verwendung in anderen Systemen, wie SIEMs, Web Application Firewalls usw., ist untersagt.

3.8 DoS-Basisschutz

Mit dem durch das Network Operations Center (NOC) des DFN bereitgestellten Dienst DFN-DoS-Basisschutz können IT-Ressourcen vor einer Überlastung (Denial-of-Service, DoS) durch zu viele eingehende Datenpakete geschützt werden. Für den Schutz ist es unerheblich, ob die eingehenden Datenpakete von einer oder von vielen Quellen erzeugt werden und ob sich diese Quellen innerhalb oder außerhalb des Wissenschaftsnetzes befinden.

Mit dem Dienst sollen die betroffenen IT-Ressourcen möglichst präzise nur vor unerwünschter Nutzung geschützt werden (Mitigation) und alle andere Nutzung möglichst wenig beeinträchtigt werden, um damit auch während eines DoS-Vorfalls die betroffenen IT-Ressourcen mit bestmöglicher Qualität zur Verfügung stellen zu können.

Der Dienst DFN-DoS-Basisschutz bietet keinen Schutz vor einer Beeinträchtigung der Verfügbarkeit von IT-Ressourcen durch eine Ausnutzung von Sicherheitsschwachstellen oder fehlerhaften Konfigurationen (schwachstellenbasierte DoS-Vorfälle). Dieser Schutz muss weiterhin vom Teilnehmer selbst erbracht werden, z. B. durch regelmäßige Sicherheitsupdates, fachgerechte Konfigurationen und den Einsatz von Firewalls. Diese vom Teilnehmer zu leistenden, notwendigen Schutzmaßnahmen werden durch das in diesem Dokument beschriebene Sicherheitsportfolio des DFN-Vereins unterstützt.

Der DoS-Basisschutz stellt keine aktive Monitoringmaßnahme dar, sondern erfordert eine Kontaktaufnahme durch den Teilnehmer im Fall einer Überlastsituation.

3.9 Self-Service im DFN.Security-Portal

Das DFN.Security-Portal ist die Managementschnittstelle für Nutzer zum Abruf und zur Konfiguration der Basisleistungen des DFN.Security-Dienstes.

Der Zugriff auf das DFN.Security-Portal ist mittels TLS-Client-Authentifizierung abgesichert und setzt das Vorhandensein eines über die DFN-PKI bezogenen Zertifikats voraus. Für die initiale Nutzung ist die Benennung einer Ansprechperson gegenüber dem DFN-Verein erforderlich. Diese Person erhält nach erfolgter Registrierung einen Administrationszugriff auf das DFN.Security-Portal und kann dort u. a. die zugeordneten Netzbereiche strukturieren und mit Kontakten für den Empfang Automatischer Warnmeldungen versehen, Systeme modellieren, für die Schwachstellenmeldungen bezogen werden sollen, Domains der Einrichtung eintragen und verifizieren, sowie Scans für den Netzwerkprüfer anlegen.

Die Ansprechperson ist in der Lage weitere Kontakte im DFN.Security-Portal zu erstellen, die ebenfalls Zugriff auf das System erhalten können.

Das DFN.Security-Portal ist die zentrale Komponente für die durch einen Teilnehmer möglichen Konfigurationen sowie den Abruf der für ihn bestimmten Informationen. Im DFN.Security-Portal sind dementsprechend das Archiv der Schwachstellenmeldungen (seit August 2016), Informationen über neue Produkte und Kategorien, allgemeine Mitteilungen zum DFN.Security-Portal und den Automatischen Warnmeldungen, Automatische Warnmeldungen selbst und Ergebnisse von durch den Netzwerkprüfer durchgeführte Scans abrufbar, auch wenn diese Informationen nicht per E-Mail zugestellt werden und solange die maximale Speicherdauer für bestimmte Daten nicht überschritten wurde.

4 Leistungsmerkmale der erweiterten Leistungen

Für Teilnehmer mit höherem Schutzbedarf bietet der DFN.Security-Dienst erweiterte Leistungen, die die Basisleistungen ergänzen: Sie unterstützen mehr Bedrohungsszenarien und beinhalten eine erweiterte Datenanalyse sowie eine durch die Modellierung der Schutzgegenstände in den SOC-Werkzeugen zielgerichtete Versorgung. Das Plus an Leistungen schlägt sich aber auch auf der Aufwandsseite nieder: Sowohl beim Teilnehmer als auch beim DFN-Verein entstehen signifikant höhere Aufwände und zu erfüllende Voraussetzungen, die für die erfolgreiche Dienstnutzung unabdingbar sind. Die erweiterten Leistungen werden im Rahmen der Kostenumlage des DFN-Vereins mit einem separaten Entgelt realisiert, welches durch die Mitgliederversammlung des DFN-Vereins beschlossen wurde.

Die erweiterten Leistungen des DFN.Security-Dienstes umfassen grundsätzlich alle Leistungsmerkmale der Basisleistungen. Es gibt jedoch teilweise technisch abweichende

Implementierungen, bspw. um die Modellierung der Schutzgegenstände durch Experten des DFN-CERT durchführen zu lassen (statt im Self-Service über das DFN.Security-Portal).

4.1 Logdaten-Analyse nach Übermittlung mit dem SOC-Agent

Für die erweiterten Leistungen unterliegt die Logdatenannahme und -analyse nicht den Mengenbeschränkungen, die für die Erbringung der Basisleistungen angesetzt werden müssen, und kann in Abstimmung mit dem DFN-CERT hinsichtlich der konkreten Formate angepasst werden.

Für die Annahme und Weiterleitung der Logdaten steht dem Teilnehmer die Komponente SOC-Agent zur Verfügung, welche im Netz des Teilnehmers betrieben wird. Der SOC-Agent wird in einer für den Teilnehmer geeigneten Form ausgeliefert (z. B. als Container-Image) und der Teilnehmer wird bei der Inbetriebnahme beraten. Nach der Aggregation erfolgt die Datenweiterleitung hin zum zentralen SOC-System des DFN-CERT, wo die Daten vollautomatisiert durch das System und manuell durch SOC-Analysten auf Hinweise zu sicherheitsrelevanten Vorfällen untersucht werden.

4.2 Erweitertes aktives Dienstemonitoring

Durch das aktive Dienstemonitoring mittels SOC-Probe werden Teilnehmer beispielsweise über in Kürze ablaufende Zertifikate, unbeabsichtigt öffentlich oder ungeplant nicht verfügbare Serverdienste und andere, ähnlich gelagerte Sicherheitsmängel, informiert. SOC-Probe wird vom DFN-CERT betrieben und in den erweiterten Leistungen für den Teilnehmer auch konfiguriert. Das Dienstemonitoring stellt somit eine externe Sicht auf Dienste zur Verfügung. In den erweiterten Leistungen kann in diesem Leistungsmerkmal eine deutlich größere Anzahl von Systemen pro Teilnehmer überwacht werden als in den Basisleistungen.

In Abhängigkeit von dem konkreten Sicherheitsmangel wird der Teilnehmer direkt oder zu festgelegten Zeiten über den Missstand informiert. Die Information erfolgt über den bekannten Kanal der Automatischen Warnmeldungen.

4.3 Suche nach Bedrohungsmustern

Das DFN-CERT sucht aktiv und kontinuierlich nach neuen bisher unbekannten Bedrohungsmustern (Indicators of Compromise, IoC) und wertet Cyber Threat Intelligence (CTI) anderer Sicherheitsteams, CERTs auf nationaler, europäischer und internationaler Ebene durch Experten im DFN-CERT aus. Darüber hinaus werden neue Bedrohungsmuster auch anhand eigener Analysen bzw. den im Rahmen der Vorfallsbearbeitung gewonnenen Erkenntnissen erstellt.

4.4 Beratung und Unterstützung bei der Modellierung der Schutzgegenstände

Regelmäßige, in der Regel jährliche, Beratung und Unterstützung bei der Modellierung der Schutzgegenstände durch Experten des DFN-CERT sind in den erweiterten Leistungen inbegriffen. Dies stellt sicher, dass im DFN-CERT immer eine aktuelle Modellierung vorliegt, sodass die SOC-Analysten bei der manuellen Datenauswertung darauf basierend die Kritikalität einer potenziellen Gefährdungssituation bewerten können und der aktive DoS-Basisdienst auf die relevanten Systeme zielt. Weiterhin wird sichergestellt, dass die vorliegenden Kontaktdaten aktuell und passend sind, damit im Notfall keine Zeit durch die Suche nach korrekten Ansprechpartnern verloren geht. Zusätzlich wird sichergestellt, dass der Teilnehmer über Änderungen und Erweiterungen des Dienstes informiert bleibt.

4.5 Reporting (DFN.Security-Portal, DFN.Security-Dashboard)

Wie für die Basisleistungen stellt das DFN.Security-Portal auch bei den erweiterten Leistungen einen wichtigen Konfigurations- und Informationspunkt dar. Es wird für die erweiterten Leistungen allerdings noch um ein DFN.Security-Dashboard in einem zusätzlichen Webportal ergänzt. Über dieses DFN.Security-Dashboard sind Informationen über die eingelieferten Ereignisdaten des Teilnehmers abrufbar. Auch für die Nutzung dieses DFN.Security-Dashboards ist eine TLS-Client-Authentifizierung erforderlich.

5 Schnittstellen

Der DFN-Verein ist der Ansprechpartner für die Dienstvereinbarungen und anderen vertraglichen Aspekte. Das DFN-CERT ist für die Erbringung des Dienstes verantwortlich und stellt den fachlichen Ansprechpartner dar.

5.1 Organisatorische Schnittstellen

Für Teilnehmer stehen drei organisatorische Schnittstellen zur Verfügung:

- Klärung organisatorischer Fragen, wie Nutzungsbedingungen, Verträge, Auftragsdatenvereinbarungen, Entgelte, etc.

  DFN-Verein: dfn.security@dfn.de, 030/884299-9123

- Klärung technischer Fragen, wie Zugang zum Portal, Fragen zu Automatischen Warnmeldungen, Konfiguration der Dienste, etc.

  DFN-CERT: cert@dfn-cert.de, 040/808077-590

Das DFN-CERT ist werktäglich Montag bis Donnerstag mindestens von 09:00 bis 17:00 Uhr und Freitag von 9:00 bis 16:00 Uhr besetzt. Es gelten die gesetzlichen Feiertage des Bundeslandes Hamburg. An Heiligabend und Silvester ist wie an anderen Feiertagen die Verfügbarkeit eingeschränkt.

- Unterstützung bei DDoS-Angriffen im Leistungsmerkmal DoS-Basisschutz:

DFN-NOC: noc@noc.dfn.de, 0711/63314-112

Das DFN-NOC ist werktäglich von Montag bis Freitag in der Zeit von 8.30 Uhr bis 18.00 besetzt. Es gelten die gesetzlichen sowie tarifvertraglich vereinbarten Feiertage des Bundeslandes Baden-Württemberg.

5.2 Technische Schnittstellen

Die Konfiguration der Leistungsmerkmale der Basisleistungen erfolgt im Self-Service durch den Teilnehmer im DFN.Security-Portal. Die Konfiguration einiger Leistungsmerkmale der erweiterten Leistungen erfolgt zusätzlich durch das DFN-CERT in Kooperation mit dem Teilnehmer.

Für die Bereitstellung einzelner Leistungsmerkmale aus den erweiterten Leistungen wird im Teilnehmernetz ein SOC-Agent in Kooperation mit dem Teilnehmer betrieben.

Meldungen der einzelnen Leistungsmerkmale werden im DFN.Security-Portal angezeigt und, je nach Konfiguration des Teilnehmers, per E-Mail versandt. Zusätzlich können die Meldungen als RSS-Feed abonniert werden.

6 Dienstgüte und Verfügbarkeit

6.1 Wartungsmaßnahmen

Um die Leistungsmerkmale des DFN.Security-Dienstes auf dem aktuellen Stand der Technik zu halten, müssen regelmäßig angekündigte Wartungsarbeiten durchgeführt werden. Durch redundanten Aufbau und weitere Maßnahmen wird eine Wartungsredundanz geschaffen, die es erlaubt, regelmäßig anfallende Wartungsarbeiten durchführen zu können, ohne dass diese notwendigerweise Auswirkungen auf die Diensterbringung haben.

Für nicht regelmäßig anfallende und aufwändige, aber selten auftretende, Wartungsarbeiten ist eine Wartungsredundanz nicht sinnvoll. Sofern derartige Wartungsarbeiten mit Auswirkungen auf die Diensterbringung durchgeführt werden müssen, werden sie mit mindestens drei Werktagen Vorlauf an die vom Teilnehmer benannten Kontaktadressen angekündigt.

Unter Umständen müssen aus anderen Gründen Arbeiten, die Auswirkungen auf die Diensterbringung haben, auch ohne eine vorherige Ankündigung und ohne weiteren Verzug durchgeführt werden (z. B. bei Störungen). Hier erfolgt die Information der Teilnehmer unverzüglich, sobald eine solche Situation erkannt wird.

6.2 Entstörung

Störungen des Dienstes werden durch das DFN-CERT automatisiert bzw. durch Experten erkannt, bewertet und weiter analysiert, um Gegenmaßnahmen einleiten zu können. Zusätzlich werden Meldungen über Störungen durch die Teilnehmer des Dienstes an die angegebenen Kontaktadressen gerne entgegengenommen.

Der Dienst DFN.Security wird in großen Teilen vollautomatisch durch entsprechende IT-Systeme erbracht. Diese stehen 24/7 zur Verfügung und werden durch geeignete Maßnahmen auf minimale Ausfallzeiten ausgerichtet. Im Falle einer technischen Störung wird diese an Werktagen, an Wochenend- und Feiertagen am darauffolgenden Werktag, bearbeitet und schnellstmöglich behoben.

Leistungsmerkmale, welche manuelle Tätigkeiten seitens des DFN-Vereins bzw. des DFN-CERTs betreffen, stehen, soweit nichts Abweichendes vereinbart wurde, 8/5 außer an gesetzlichen Feiertagen in Berlin, Stuttgart bzw. Hamburg sowie Heiligabend und Silvester über die vereinbarten Kommunikationswege (siehe Schnittstellen Abschnitt 5.1) zur Verfügung.

A. Anhang Glossar

CERT	Computer Emergency Response Team
CPE	Common Platform Enumeration
CTI	Cyber Threat Intelligence
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
EDUCV	Edu-CERT-Verbund
IoC	Indicator(s) of Compromise
IRT	Incident Response Team
NOC	Network Operations Center
RSS	Rich Site Summary, später Really Simple Syndication, stellt ein Dateiformat für Web-Feeds dar
SCTP	Stream Control Transmission Protocol
SOC	Security Operations Capabilities im DFN-CERT. Wird

	häufig auch als Security Operations Center bezeichnet.
SOC-Agent	Komponente zur Aggregation und zum Übertragen von Logdaten zur weiteren Auswertung
SOC-Probe	Komponente für ein aktives Monitoring von Diensten aus dem Netz des DFN
Teilnehmer	Einrichtung, die am Dienst DFN.Security teilnimmt
TLS	Transport Layer Security
UDP	User Datagram Protocol

B. Anhang Änderungshistorie

Version	Datum	Änderungen
1	Juli 2023	Initiale Version
2	Februar 2024	Ergänzung Leistungsmerkmal DNS-RPZ Redaktionelle Anpassungen