CERT der Bundesagentur für Arbeit

Beschreibung nach RFC 2350

IT-Systemhaus

Änderungs- und Versionsübersicht

Version	Datum	Autor	Änderungsgrund	Kapitel/Seiten
1.0	24.01.2018	CERT der BA	Neuerstellung	Alle
1.1	21.06.2018	CERT der BA	Korrekturen/ Ergänzungen	1.1 / 1.4 / 1.5 / 2.7 / 2.8 / 4.3
1.2	11.09.2018	CERT der BA	Korrekturen	Alle

Inhalt

RFC 2350 CERT der Bundesagentur für Arbeit

1. Vorbemerkung

Dieses Dokument beschreibt öffentliche Informationen zum "CERT der Bundesagentur für Arbeit" nach RFC 2350[1]. Es enthält grundlegende Informationen über das CERT sowie Kontaktmöglichkeiten und beschreibt seine Zuständigkeiten sowie Dienstleistungen.

1.1 Letzte Änderung

11. September 2018 13:37:00 +0200

1.2 Verteilerliste für Änderungen

Änderungen an diesem Dokument werden gegenwärtig nicht über eine Verteilerliste mitgeteilt. Es gilt jeweils die aktuellste auf dem Webserver bereitgestellte Version.

1.3 Veröffentlichung dieses Dokumentes

Die aktuelle Version dieses Dokuments finden Sie immer unter: https://www.arbeitsagentur.de/cert

1.4 Authentizität des Dokuments

Die Authentizität dieses Dokumentes kann entweder per TLS-Zertifikat (https Aussteller D-Trust) oder als digitale Signatur eines PDF-Dokumentes geprüft werden. Entsprechende Zertifikate zur Prüfung der PDF-Signatur finden sich unter https://www.pki.arbeitsagentur.de.

1.5 Identifizierung des Dokuments

Titel: "RFC 2350 CERT der Bundesagentur für Arbeit"
Version: 1.1
Datum: 21.06.2018
Ablauf/Verfall: Dieses Dokument ist gültig bis zum Ersetzen durch eine spätere Version.

[1] https://www.ietf.org/rfc/rfc2350.txt

2. Kontaktinformation

2.1 Name des Teams

CERT der Bundesagentur für Arbeit

2.2 Postalische Adresse

CERT der Bundesagentur für Arbeit
Regensburger Str. 104
90478 Nürnberg
Deutschland

2.3 Zeitzone

Das CERT operiert in der mitteleuropäischen Zeitzone (MEZ) GMT+0100 bzw. GMT +0200/MESZ während der Sommerzeit in Europa (Ende März bis Ende Oktober).

2.4 Telefonnummer

+49 911 179 6500

Bitte beachten Sie, dass die oben genannte Telefonnummer ausschließlich für die Kommunikation im Zusammenhang mit sicherheitskritischen Vorfällen bestimmt ist. Bei Missachtung behalten wir uns eine Sperrung externer Telefonnummern in unserem System vor.

2.5 Faxnummer

Eine Kommunikation per FAX findet nicht statt.

2.6 Andere Kommunikationsmöglichkeiten

Keine.

2.7 E-Mail Adressen

Alle Berichte über Sicherheitsvorfälle, Störungsmeldungen, Warnungen, Ratschläge, Empfehlungen etc. sind an IT-Systemhaus.CERT@arbeitsagentur.de zu senden.
Die Verwendung von Telefon zur Meldung von Zwischenfällen sollte so weit wie möglich vermieden werden.

2.8 Öffentlicher Schlüssel und Verschlüsselungsinformationen

Das CERT der Bundesagentur für Arbeit nutzt zum Schutz der E-Mail Kommunikation mit anderen CERTs oder Partnern das Verschlüsselungsprotokoll S/MIME. Weitere Informationen dazu finden sich unter:
https://www.arbeitsagentur.de/e-mail-verschluesselung

Das aktuelle S/MIME Zertifikat ist zu finden unter:
https://cert-download.arbeitsagentur.de

2.9 Betriebszeiten des CERT-BA

Montag - Donnerstag:	08:00 Uhr bis 16:30 Uhr,
Freitag:	08:00 Uhr bis 13:00 Uhr.

Ausnahmen: 24. und 31. Dezember sowie gesetzliche Feiertage in Bayern

3. Organisatorischer Rahmen

3.1 Ziele und Aufgaben (Mission statement)

Das CERT der Bundesagentur für Arbeit gewährleistet den Schutz der Bundesagentur für Arbeit und ihrer gesamten Organisation vor vorsätzlichen oder böswilligen Angriffen gegen die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen durch den Einsatz und die Weiterentwicklung von Präventions-, Detektions- und Reaktionstechniken. Entsprechende Vorfälle werden zentral erfasst, bearbeitet und gesteuert. Ferner wird zur nachhaltigen Bildung und Erweiterung des Sicherheitsbewusstseins beigetragen.

3.2 Zielgruppe (Constituency)

Die Zielgruppe des CERT der Bundesagentur für Arbeit sind interne Abteilungen und externe Kunden.

3.3 Finanzierung und Förderung

Das CERT der Bundesagentur für Arbeit ist eine interne Einheit des IT-Systemhauses als Dienststelle der Bundesagentur für Arbeit und wird ausschließlich durch diese finanziert und gefördert.

3.4 Autorität

Das CERT der Bundesagentur für Arbeit besitzt den Auftrag zur Koordination und Durchführung von Security Incident Response und Security Incident Handling innerhalb der Bundesagentur für Arbeit und ihrer Kunden. Entsprechende Befugnisse sind beschrieben und im, nach ISO27001 (BSI-Grundschutz) zertifiziertem, ISMS der Organisation hinterlegt.

4. Richtlinien

4.1 Vorfallstypen und Support

Das CERT der Bundesagentur für Arbeit bearbeitet alle Arten von sicherheitsrelevanten Vorkommnissen an IT-Systemen oder Personen, die in seiner Zielgruppe auftreten oder zu geschehen drohen. Dies umfasst auch Vorkommnisse, die das Security Management betreffen. Abgrenzungen zum Fraud-Management und Datenschutz existieren.

Das Ausmaß des Supports richtet sich nach Art und Schwere des Sicherheitsvorfalls, der Anzahl der betroffenen Benutzer und den Auswirkungen auf IT-Systeme und das Personal der betroffenen Institutionen. Ebenso ist die Unterstützung durch die verfügbaren Ressourcen begrenzt.

4.2 Kooperationen, Interaktionen und Weitergabe von Informationen

Das CERT der Bundesagentur für Arbeit legt großen Wert auf die operative Zusammenarbeit und den

Informationsaustausch zwischen Computer Emergency Response Teams (CERTs) und anderen Organisationen, in Bezug auf Erkenntnisse über Angreifer und Angriffsmethoden. Zum Austausch von IoCs werden Threat Intelligence Plattformen (z.B. MISP) genutzt.

4.3 Kommunikation und Authentifizierung

Das CERT der Bundesagentur für Arbeit schützt sensible Informationen gemäß den einschlägigen Vorschriften und Richtlinien in Deutschland und der EU. Es verwendet gängige kryptographische Methoden, um die Vertraulichkeit und Integrität der Kommunikation zwischen anderen CERTs und ihren Partnern zu gewährleisten. Das CERT der Bundesagentur für Arbeit berücksichtigt auch die von den Urheberrechtsinhabern der Informationen vergebenen Sensitivitätskennzeichen. Die Kommunikationssicherheit (Verschlüsselung und Authentifizierung) wird durch S/MIME oder andere zu vereinbarende Methoden erreicht.

5. Dienstleistungen

5.1 Reaktion auf Vorfälle

Das CERT der Bundesagentur für Arbeit besitzt die Fähigkeit sicherheitsrelevante Ereignisse innerhalb der Bundesagentur für Arbeit zu erkennen (SIEM) und die Befugnis diese zu untersuchen und zu behandeln.

5.2 Koordination eines Vorfalls

Die zentrale Koordination der Behandlung und Reaktion liegt beim CERT der Bundesagentur für Arbeit. Es ist in der Lage, einen gemeldeten Vorfall zu bewerten, zu eskalieren und zu bearbeiten.

5.3 Proaktive Aktivitäten/Maßnahmen

Das CERT der Bundesagentur für Arbeit bietet aktuelle Informationen zu Sicherheitslücken und gibt Handlungsempfehlungen zur Behebung (Patching, Workarounds etc.). Das CERT bietet Informationen für interne Security Awareness Kampagnen und Unterstützung bei sicherheitsrelevanten Schulungen für interne Abteilungen.

Darüber hinaus evaluiert und entwickelt das Team kontinuierlich neue Produkte und Tools zur Sicherung der Infrastruktur und zum Aufspüren von Bedrohungen.

6. Vorfall melden

Es gibt keine öffentlichen Formulare zur Meldung von Vorfällen durch Parteien außerhalb der Bundesagentur für Arbeit. Alle Nachrichten sollten an IT-Systemhaus.CERT@arbeitsagentur.de gerichtet werden. Wir empfehlen, jede Kommunikation bzgl. potentieller Sicherheitsvorfälle oder Sicherheitslücken mit S/MIME zu verschlüsseln.

7. Haftungsausschluss (Disclaimer)

Die CERT der Bundesagentur für Arbeit übernimmt keine Haftung für Fehler oder Auslassungen sowie für Schäden, die durch die Nutzung der zur Verfügung gestellten Informationen entstehen.