

From: "Ulatowski, Jan" <Jan.Ulatowski@BDR.de>

To: "Rottmann-Großner, Heiko -61 BMG" <Heiko.Rottmann-Grossner@bmg.bund.de>

Date: 2/28/2021 7:27:18 PM

Subject: DEA-Meldung: Störung Reisenden-Portal

Attachments: 210228\_DEA\_Incident.docx

---

Sehr geehrter Herr Rottmann-Großner,

in der Anlage übersende ich Ihnen die Meldung zur heutigen DEA-Störung, hervorgerufen durch einen Angriff auf die DEA-Systemverfügbarkeit:

- 1. Angriff: 15:46 Uhr bis 16:56 Uhr
- 2. Angriff: 17:38 Uhr bis 18:45 Uhr

Durch die Angriffe gab es Einschränkungen hinsichtlich der Verfügbarkeit des DEA-Dienstes. Die Schutzmechanismen zum Schutz von Vertraulichkeit & Integrität haben funktioniert.

Für etwaige Rückfragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

Jan Ulatowski

CMS (Credential Management Systems)

Abteilungsleitung PSM (Projekt- und Service-Management)

---

Bundesdruckerei GmbH

Kommandantenstr. 18 10969 Berlin

T + 49 (0) 30 – 2598 - 2562

jan.ulatowski@bdr.de

www.bundesdruckerei-gmbh.de

Sitz der Gesellschaft: Berlin

Handelsregister: AG Berlin-Charlottenburg HRB 70764 B. USt-IdNr.: DE 812746617

Geschäftsführer: Dr.-Ing. Stefan Hofschien (CEO), Christian Helfrich (stellv. Vorsitzender)

Die Unternehmen der Bundesdruckerei-Gruppe nehmen den Schutz Ihrer persönlichen Daten sehr ernst und beachten die einschlägigen Regeln der Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes. Daher weisen wir darauf hin, dass im Rahmen unserer elektronisch geführten Kommunikation persönliche Daten erhoben und gegebenenfalls gespeichert werden. Diese Datenverarbeitung erfolgt ausschließlich zu geschäftlichen Zwecken. Sie haben das Recht, Auskunft über Ihre bei uns gespeicherten, persönlichen Daten zu beantragen. Bitte wenden Sie sich dazu an [datenschutz@bdr.de](mailto:datenschutz@bdr.de). Weitere Hinweise zu Ihren Rechten und die Kontaktdaten unseres Datenschutzbeauftragten finden Sie unter: <https://www.bundesdruckerei-gmbh.de/de/datenschutz.html>.

Diese Mitteilung ist ausschließlich zur Kenntnisnahme durch die natürliche oder juristische Person bestimmt, an die sie adressiert ist. Sie kann vertrauliche Informationen enthalten, die nach geltendem Recht nicht weitergegeben werden dürfen. Sollten Sie nicht der beabsichtigte Empfänger der Mitteilung oder der Bevollmächtigte für die Weitergabe an den beabsichtigten Empfänger sein, teilen wir hiermit mit, dass jede Weitergabe, Weiterleitung oder Vervielfältigung dieser Mitteilung strengstens verboten ist. Wenn Sie diese Mitteilung irrtümlicherweise erhalten haben, löschen Sie sie bitte und teilen Sie uns dies umgehend mit.

## DEA - Incident-Meldeformular Datum: 28.02.2021

### Beschreibung / Titel:

Bitte Problembeschreibung in einigen Worten angeben

Einschränkung der Verfügbarkeit DEA Digitale Einreiseanmeldung am 28.02.21 15:46 Uhr bis 18:45 Uhr

### Kundenkontakt

Eingabe der Kundenkontaktdaten, für mögliche Rückfragen zur Incident Beschreibung:

Name	Firma	E-Mail	Telefon	Mobiltelefon
Ulatowski	BDr	Jan.ulatowski@bdr.de		
Ehreke	BDr	Jens.ehreke@bdr.de		

Auswahl der Komponenten

Komponenten:
<input checked="" type="checkbox"/> Frontend Reisende <input type="checkbox"/> Frontend Gesundheitsämter <input type="checkbox"/> Backend-DB <input type="checkbox"/> Liste Risikogebiete <input type="checkbox"/> CDN <input type="checkbox"/> Infrastruktur <input type="checkbox"/> Entwicklungsumgebung <input type="checkbox"/> Testumgebung <input type="checkbox"/> Produktivumgebung <input type="checkbox"/> ...

Auswahl Servicepriorität:

Priorität		
<input type="checkbox"/> 3 – minor <input type="checkbox"/> 2 – serious <input checked="" type="checkbox"/> 1 – critical		
Fehlerklassen	Definition	Beispiel
Priorität 1 (critical) Nur für Produktivsysteme	Der Geschäftsbetrieb und der Service sind unterbrochen.	Der Incident verursacht z.B. den Ausfall des Reisenden-Frontends.
Priorität 2 (serious)	Das System ist ganz oder teilweise verfügbar. Ein wesentlicher Teil des Systems ist ausgefallen oder nicht verfügbar. Der Incident muss so schnell wie möglich behoben werden.	Ein Incident schränkt den Zugriff auf einen Service ein, z.B. Frontend für die Gesundheitsämter. Es gibt wesentliche Einschränkungen für den Betrieb.
Priorität 3 (minor)	Geringer Einfluss oder Unterbrechung: IT Probleme, andere Services oder Funktionen sind eingeschränkt. Wesentliche Komponenten der Anwendung sind verfügbar.	Ein Incident verursacht eine nicht wesentliche Einschränkung der Anwendung, ohne Einfluss auf die Erreichbarkeit, Funktionsweise oder Layout der Anwendung.

## Detaillierte Incident-Beschreibung

*Detaillierte Beschreibung des Problems. Einfügen von Screenshot und zusätzlichen Dokumenten*

### Ablauf:

15:50 Uhr Störung identifiziert: DEA-Dienst nicht verfügbar

15:50 Uhr Störungsmeldung an Entstörungsteam

seit 15:50 Uhr Störungsanalyse

### Ursachenanalyse techn. Störung & Maßnahmen

- Angriff auf Systemverfügbarkeit durch DDoS-Attacke von unbekannter Seite
  - 1. Angriff: 15:46 Uhr bis 16:56 Uhr
  - 2. Angriff: 17:38 Uhr bis 18:45 Uhr
- dadurch Einschränkung der Verfügbarkeit
- Schutzmechanismen haben hinsichtlich Schutz von Vertraulichkeit & Integrität funktioniert
- eingeleitete Maßnahmen:
  - Black-Holing der Einreiseportal-IP-Adresse um 18:03 Uhr
  - Anpassung des Mechanismus zum Schalten der Störungsseite auch bei Angriffen

### Meldekette:

- Information BDr-Eskalationshotline um 16.32 Uhr
- nachfolgend telefonische Information BMG-Bereitschaftsdienst
- nachfolgend telefonische Information RKI-Bereitschaftsdienst durch PL (nicht erfolgreich, da außerhalb der üblichen Dienstzeiten)
- Information BMG/RKI per E-Mail um 17:18 Uhr

### Störungsseite:

- Umschalten auf Störungsseite war nicht möglich, da von Angriff mit betroffen
- Workaround für Schalten der Störungsseite bei erneutem Angriff implementiert:
  - Umstellung Störungsseite auf AWS