From: "Ulatowski, Jan" <Jan.Ulatowski@BDR.de>
To: "Rottmann-GroЯner, Heiko -61 BMG" <Heiko.Rottmann-Grossner@bmg.bund.de>
Date: 2/28/2021 7:27:18 PM
Subject: DEA-Meldung: Stцrung 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 Hofschen (CEO), Christian Helfrich (stellv. Vorsitzender)

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		[redacted]
Ehreke	BDr	Jens.ehreke@bdr.de		

Auswahl der Komponenten

Komponenten:

[x] Frontend Reisende
[] Frontend Gesundheitsämter
[] Backend-DB
[] Liste Risikogebiete
[] CDN
[] Infrastrukture
    [] Entwicklungsumgebung
    [] Testumgebung
    [] Produktivumgebung
[] …

Auswahl Servicepriorität:

Priorität

[] 3 – minor
[] 2 – serious
[x] 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:

- Informierung BDr-Eskalationshotline um 16.32 Uhr
- nachfolgend telefonische Informierung BMG-Bereitschaftsdienst
- nachfolgend telefonische Informierung RKI-Bereitschaftsdienst durch PL (nicht erfolgreich, da außerhalb der üblichen Dienstzeiten)
- Informierung 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