RFC 2350

popis CDC CSIRT společnosti Aricoma Enterprise Cybersecurity a.s.

1. Popis služeb CDC CSIRT týmu

Služby CDC CSIRT týmu jsou definovány v návaznosti na mandát, konstituci, autoritu a odpovědnosti. Jednotlivé služby následně vymezují dílčí oblasti bezpečnosti, do kterých CSIRT tým je zapojen, či jinak přispívá. Celkové služby CDC CSIRT týmu jsou tedy úzce propojeny s aktivitami CDC (SOC as a Service) jako takového.

1.1 O tomto dokumentu

Následující popis CDC CSIRT týmu je zpracován podle standardu RFC 2350. Poskytuje základní informace o CDC CSIRT týmu, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1.1 Datum poslední aktualizace

Toto je verze číslo 1 ze dne: 19.6.2024

1.1.2 Distribuční seznam pro oznámení

Žádný distribuční seznam pro oznámení neexistuje. Veškeré specifické dotazy nebo připomínky prosím zasílejte na adresu CDC CSIRT týmu.

1.1.3 Možnost stáhnout tento dokument

Aktuální verze dokumentu je umístěna zde.

1.2 Kontaktní informace

1.2.1 Název týmu

CDC CSIRT

1.2.2 Adresa

CDC CSIRT
Voctářova 2500/20a
180 00, Praha
Česká republika

1.2.3 Časové pásmo

SEČ, Středoevropský čas (UTC +1, od poslední neděle v říjnu do poslední neděle v březnu)
SELČ, Středoevropský letní čas (UTC +2, od poslední neděle v březnu do poslední neděle v říjnu)

1.2.4 Telefonní číslo

+420 731 652 038 (v pracovní době)
+420 771 501 154 (mimo pracovní dobu)

1.2.5 Faxové číslo

Není k dispozici

1.2.6 Ostatní telekomunikace

Není k dispozici

1.2.7 Elektronická adresa

Pro veškerou komunikaci s CDC CSIRT prosím použijte adresu: cdc-team@aricoma.com

1.2.8 Veřejné klíče a šifrovací informace

```
Type:   RSA/4096   Expires: never
Fpr:    4C29 DC26 A94A F5DF D124 0038 3771 9A81 7FFB A05E
Sub:    RSA/4096  Usage: Encrypt
UID:    AEC CDC (AEC, a.s. Cyber Defense Center) <cdc@aec.cz>
```

1.2.9 Členové týmu

Vedoucím týmu CDC CSIRT je Lubomír Almer (lubomir.almer@aricoma.com).
Kompletní přehled členů týmu CDC CSIRT není veřejně k dispozici.
Členové týmu se při oficiální komunikaci ohledně incidentu představí protistraně plným jménem.

1.2.10 Další informace

Preferovaný způsob kontaktování CDC CSIRT je prostřednictvím e-mailu.
Není-li možné (nebo není-li to z bezpečnostního hlediska vhodné) použít e-mail, můžete CDC CSIRT kontaktovat telefonicky na výše uvedených číslech.
Pracovní doba CDC CSIRT je obecně omezena na běžnou pracovní dobu (09:00 – 17:00 od pondělí do pátku, s výjimkou státních svátků). Mimo pracovní dobu je zajištěna pohotovost.

1.3 Stanovy

1.3.1 Poslání

CDC CSIRT řeší bezpečnostní incident z oblasti kybernetické bezpečnosti pro zákazníky Aricoma Enterprise Cybersecurity a.s., se kterými je uzavřena smlouva o poskytování služeb. Naším cílem je pomoci jim účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.

1.3.2 Cílová skupina

Naší cílovou skupinou jsou zákazníci společnosti Aricoma Enterprise Cybersecurity a.s. a se kterými je uzavřena smlouva o poskytování CDC služeb.

1.3.3 Zařazení

CDC CSIRT je součástí divize Cyber Defense Center společnosti Aricoma Enterprise Cybersecurity a.s.

1.3.4 Oprávnění

CDC CSIRT má mandát od vedení společnosti Aricoma Enterprise Cybersecurity a.s. k řízení životního cyklu bezpečnostních incidentů.
CDC CSIRT může v rámci svých aktivit spolupracovat s národními a mezinárodními organizacemi, a to dle konkrétní povahy a potřeby incidentu.

1.4 Zásady

1.4.1 Typy incidentů a úroveň podpory

CDC CSIRT je oprávněn řešit všechny typy bezpečnostních incidentů, které vznikly nebo mohou vzniknout v rámci jeho působnosti.
Úroveň podpory poskytnuté CDC CSIRT týmem se liší v závislosti na typu a závaznosti incidentu nebo problému, typu původce a dalších skutečnostech v okamžiku vzniku incidentu, ale v každém případě bude poskytnut nějaký typ reakce.
Žádná přímá podpora nebude poskytována koncovým uživatelům. Podpora je poskytována odpovědným pracovníkům za zákaznickou stranu.
CDC CSIRT tým se zavazuje informovat o potenciálních zranitelnostech, a to v případech, kdy vyhodnotí, že takovéto informování je nezbytně nutné.

1.4.2 Spolupráce, interakce a zpřístupňování informací

CDC CSIRT tým je připraven spolupracovat s ostatními důvěryhodnými bezpečnostními týmy na lokální i mezinárodní úrovni.
S informacemi získanými v rámci své činnosti CDC CSIRT nakládá v souladu s legislativou a smluvními závazky. CDC CSIRT bude využívat informace, které jsou mu poskytnuty k řešení bezpečnostních incidentů. Tyto informace budou dále distribuovány jednotlivým členům týmu na základě principu need-to-know.

1.4.3 Komunikace a autentizace

E-maily a telefony jsou považovány za dostatečně bezpečný způsob, použitelný nešifrovaně, při přenosu málo citlivých dat. Je-li nutné zaslat vysoce citlivé údaje prostřednictvím e-mailu, bude využito šifrování PGP.
Je-li nutné prověřit osobu před zahájením komunikace, může tak být provedeno buď prostřednictvím existující sítě důvěry (např. TI, FIRST) nebo jinými metodami, jako je například zpětné volání, zpětný mail nebo, v případě potřeby, osobní setkání.

1.5 Služby

1.5.1 Reakce na incidenty

CDC CSIRT tým si klade za cíl poskytovat podporu a pomáhat se zvládáním bezpečnostních incidentů zákazníkům Aricoma Enterprise Cybersecurity a.s. CDC CSIRT tým si klade za cíl poskytovat odbornou pomoc a součinnost s následujícími typy činností:

1.5.1.1 Třídění incidentů

V rámci třídění incidentů bude realizováno zejména:

- Posouzení věrohodnosti incidentu
- Určení rozsahu a priority incidentu

1.5.1.2 Koordinace při řešení incidentu

V rámci koordinace při řešení incidentu bude realizováno zejména:

- Kontaktování zúčastněných stran incidentu k prošetření incidentu a následně přijetí příslušných opatření.
- Usnadnění kontaktu s dalšími subjekty, které mohou pomoci s řešením incidentu.
- Informování ostatních CERT a CSIRT týmů v případě potřeby.
- Komunikace se zúčastněnými stranami.

1.5.1.3 Řešení incidentu

V rámci řešení incidentu bude realizováno zejména:

- Poskytnutí odborné pomoci a součinnosti o vhodných postupech zapojeným bezpečnostním týmům jednotlivých zákazníků.
- Dohled nad postupem řešení incidentu zapojených bezpečnostních týmů jednotlivých zákazníků.
- Definice opatření/aktivit k ochraně systémů a dalších IT/OT prostředků zákazníků před dopadem incidentu
- Definice nápravných opatření k odstranění identifikovaných zranitelností a dozorování realizace těchto opatření.

1.5.2 Proaktivní přístup

CDC CSIRT se podílí na řadě proaktivních činností vedoucích ke zvyšování bezpečnostního povědomí u zákazníků společnosti Aricoma Enterprise Cybersecurity a.s.

1.6 Zproštění odpovědnosti

Navzdory všem opatřením, kterǻ budou přijata v přípravě oznámení informací, upozornění a varování, nepřebírá CDC CSIRT žádnou odpovědnost za chyby, opomenutí, či škody, vyplývajícΐ z využití v nich obsažených informací.