Popis

ELAT CSIRT

Obsah

1. O TOMTO DOKUMENTU

Tento dokument obsahuje popis ELAT CSIRT týmu podle standardu RFC 2350. Poskytuje základní informace o CSIRT týmu, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1 DATUM POSLEDNÍ AKTUALIZACE

Toto je verze číslo 1 ze dne 15.3.2018.

1.2 DISTRIBUČNÍ SEZNAM PRO OZNÁMENÍ

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

1.3 MÍSTA, KDE MŮŽE BÝT TENTO DOKUMENT NALEZEN

Aktuální verze tohoto popisného dokumentu je dostupná na internetových stránkách https://www.elat.cz/csirt

2. KONTAKTNÍ INFORMACE

2.1 NÁZEV TÝMU

ELAT CSIRT tým

2.2 ADRESA

ELAT s.r.o. - CSIRT
Československého exilu 1888/4
14300, Praha 12 - Modřany
Česká republika

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)

2.4 TELEFONNÍ ČÍSLO

+420 541225561
+420 725858296

2.5 FAXOVÉ ČÍSLO

Není k dispozici

2.6 OSTATNÍ TELEKOMUNIKACE

Není k dispozici

2.7 ELEKTRONICKÁ ADRESA

Pro hlášení incidentů použijte adresu csirt@elat.cz

2.8 VEŘEJNÉ KLÍČE A ŠIFROVACÍ INFORMACE

Pro hlášení incidentu a související komunikaci prosím použijte tento klíč:

Team key ID: E5245F9C

<csirt@elat.cz>

Key fingerprint = 11EC 5F6E 9AC3 E2E0 1185 BC41 44AE 2800 E524 5F9C

2.9 ČLENOVÉ TÝMU

Lukáš Vondráček – vedoucí týmu
lukas.vondracek@elat.cz
PGP key ID: 0xAC6D3E23

Jiří Richter – zastupující vedoucí týmu
jiri.richter@elat.cz
PGP key ID: 0x5DB192F4

Kompletní přehled členů týmu ELAT CSIRT není veřejně k dispozici. Členové týmu se v rámci oficiální komunikace při řešení incidentu identifikují druhé straně plným jménem.

Řízení a dohled jsou zajišťovány vedoucím týmu.

2.10 DALŠÍ INFORMACE

Obecné informace o ELAT CSIRT týmu lze nalézt na stránce
https://www.elat.cz/csirt .

2.11 KONTAKT S VEŘEJNOSTÍ

Preferovaný způsob kontaktování ELAT CSIRT týmu je prostřednictvím e-mailu.
Hlášení incidentů a související otázky by měly být zaslány na adresu
csirt@elat.cz . Tím se vytvoří hlášení v našem systému.

Není-li možné použít mail, můžete ELAT CSIRT tým kontaktovat telefonicky.

Pracovní doba ELAT CSIRT týmu je obecně omezena na běžnou pracovní dobu (09:00-17:00 od pondělí do pátku, s výjimkou svátků).

3. STANOVY

3.1 POSLÁNÍ

ELAT CSIRT tým si klade za cíl pomáhat při ochraně informační infrastruktury svých klientů a partnerů. Naším cílem je pomoci jim účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.

3.2 CÍLOVÁ SKUPINA

Naší cílovou skupinou jsou především naši klienti. Zaměřujeme se na komerční, příspěvkové, ale i státem zřizované subjekty v České republice.

3.3 ZAŘAZENÍ

ELAT CSIRT tým je součástí firmy ELAT s.r.o., která je jeho provozovatelem.

3.4 OPRÁVNĚNÍ

ELAT CSIRT tým pracuje v soukromém sektoru v mezích české a evropské legislativy.

ELAT CSIRT tým plánuje spolupráci se správci systémů a uživateli v rámci institucí soukromého i veřejného sektoru.

4. ZÁSADY

4.1 TYPY INCIDENTŮ A ÚROVEŇ PODPORY

ELAT CSIRT tým je oprávněn řešit všechny typy počítačových bezpečnostních incidentů, které vznikly nebo mohou potenciálně vzniknout, v rámci jeho působnosti.

Úroveň podpory poskytnuté ELAT CSIRT týmem se liší v závislosti na typu a závažnosti incidentu nebo problému, typ původce, velikosti uživatelské komunity a zdrojů ELAT CSIRT týmu v okamžiku incidentu, ale v každém případě bude poskytnut nějaký typ reakce během jednoho pracovního dne. Zvláštní pozornost bude věnována incidentům, týkajícím se kritické informační infrastruktury.

Žádná přímá podpora nebude poskytována koncovým uživatelům; od nich se očekává spolupráce s jejich správcem systému, správcem sítě nebo provozovatelem internetových služeb. Právě těm poskytne ELAT CSIRT tým potřebnou podporu.

ELAT CSIRT tým se zavazuje informovat o potenciálních zranitelnostech, a tam, kde je to možné, informovat výše zmíněnou cílovou skupinu o takových zranitelnostech ještě před jejich zneužitím.

4.2 SPOLUPRÁCE, INTERAKCE A ZPŘÍSTUPŇOVÁNÍ INFORMACÍ

S veškerými příchozími informacemi je nakládáno bezpečně, bez ohledu na jejich závažnost. Informace, které jsou viditelně velmi citlivé povahy, budou zpracovávány a ukládány bezpečně, v případě nutnosti jsou využívány šifrovací technologie.

ELAT CSIRT tým bude využívat informace, které mu budou poskytnuty k řešení bezpečnostních incidentů.

Informace budou dále distribuovány ostatním týmům a členům pouze na základě principu need – to - know, a když to bude možné vždy anonymně. ELAT CSIRT tým operuje v mezích české a evropské legislativy.

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.

5. SLUŽBY

5.1 REAKCE NA INCIDENTY

ELAT CSIRT tým si klade za cíl pomáhat místním správcům při řešení technických a organizačních aspektů incidentů. Zejména plánuje poskytovat pomoc nebo rady s ohledem na následující aspekty krizového řízení:

5.1.1. TŘÍDĚNÍ INCIDENTŮ

- Posouzení, zda je incident věrohodný
- Určení rozsahu incidentu a jeho priority

5.1.2. KOORDINACE PŘI ŘEŠENÍ INCIDENTU

- Kontaktování zúčastněných stran incidentu k prošetření incidentu a následné 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 a médii

5.1.3. ŘEŠENÍ INCIDENTU

- Poskytování poradenství o vhodných postupech lokálním bezpečnostním týmům
- Sledování pokroku lokálních bezpečnostních týmů
- Poskytování pomoci při shromažďování důkazů a interpretaci dat

Kromě toho si klade ELAT CSIRT tým za cíl shromažďování statistických údajů o událostech, které se dějí v rámci jeho pole působnosti, včasné informování o možných útocích a napomáhání při ochraně proti známým útokům.

5.2 PROAKTIVNÍ PŘÍSTUP

ELAT CSIRT tým shromažďuje seznamy bezpečnostních kontaktů pro každou instituci v rámci svého pole působnosti. Tyto seznamy jsou k dispozici v případě potřeby při řešení bezpečnostních incidentů nebo útoků.

ELAT CSIRT tým publikuje oznámení o závažných bezpečnostních hrozbách, aby se v nejvyšší možné míře zabraňovalo incidentům v oblasti informačních a komunikačních technologií a snížil se tak co nejvíce jejich dopad.

ELAT CSIRT tým zpracovává IoC z dostupných zdrojů a v případě pozitivního nálezu zajišťuje předání relevantní informace kontaktu zodpovědnému za postižený systém.

ELAT CSIRT tým se také snaží zvyšovat povědomí o bezpečnosti v rámci svého pole působnosti.

6. FORMULÁŘE PRO HLÁŠENÍ INCIDENTŮ

Není k dispozici

7. ZPROŠTĚNÍ ODPOVĚDNOSTI

Navzdory všem opatřením, která budou přijata v přípravě oznámení informací, upozornění a varování, nepřebírá ELAT CSIRT tým žádnou odpovědnost za chyby, opomenutí, či škody, vyplývající z využití v nich obsažených informací.