RFC 2350 STANDARD

POPIS CSIRT TÝMU SPOLEČNOSTI KBM-INTERNATIONAL S. R. O.

1. O TOMTO DOKUMENTU

Tento dokument obsahuje popis CSIRT týmu společnosti KBM-International s.r.o. podle standardu RFC 2350. Poskytuje základní informace o týmu CSIRT, možnostech jeho kontaktování, jeho odpovědnosti a nabízených službách.

1.1 DATUM POSLEDNÍ AKTUALIZACE

Toto je verze číslo 3 ze dne 16. 11. 2017.

1.2 DISTRIBUČNÍ SEZNAM PRO OZNÁMENÍ

Žádný distribuční seznam pro oznámení neexistuje.

1.3 MÍSTA, KDE MŮŽE BÝT TENTO DOKUMENT NALEZEN

Aktuální verze tohoto popisného dokumentu je dostupná na internetových stránkách KBM CSIRT týmu – ke stažení zde

2. KONTAKTNÍ INFORMACE

2.1 NÁZEV TÝMU

KBM CSIRT: CSIRT tým společnosti KBM-International spol. s.r.o.

2.2 ADRESA

KBM-International s.r.o.
Palackého 1732
35201, Aš
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 351161201, +420 351161207

+420 608281308 (mimo pracovní dobu)

2.5 FAXOVÉ ČÍSLO

Není k dispozici

2.6 OSTATNÍ TELEKOMUNIKACE

Není k dispozici

2.7 ELEKTRONICKÁ ADRESA

Pro hlášení incidentů prosím použijte adresu csirt@e-kbm.cz

Pro ostatní komunikaci prosím použijte adresu helpdesk@e-kbm.cz

2.8 VEŘEJNÉ KLÍČE A ŠIFROVACÍ INFORMACE

Pro hlášení incidentu a související komunikaci prosím použijte tento klíč:
User ID: KBM CSIRT <csirt@e-kbm.cz>UID: 0xd17ea67066f23d81 Key type: RSAKey size: 4096 Expires: neverFingerprint: DC88 4124 F9D6 EECA F731 A823 D17E A670 66F2 3D81
Key fingerprint = BD5F 3D1A 9363 E33C FEEB F160 1207 16F3 A724 8CE4

2.9 ČLENOVÉ TÝMU

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

Řízení a dohled poskytuje Lukáš Karban, vedoucí technického oddělení KBM-International s.r.o..

2.10 DALŠÍ INFORMACE

Obecné informace o bezpečnostním týmu KBM CSIRT lze nalézt na stránce e-kbm.cz/csirt

2.11 KONTAKT S VEŘEJNOSTÍ

Preferovaný způsob kontaktování KBM CSIRT je prostřednictvím e-mailu.

Hlášení incidentů a související otázky by měly být zaslány na adresu csirt@e-kbm.cz. Tím se vytvoří hlášení v našem systému a následně je upozorněn pracovník ve službě.

V případě ostatních dotazů prosím zašlete e-mail na support@e-kbm.cz

Není-li možné (nebo je-li nevhodné z bezpečnostních důvodů) použít e-mail, můžete bezpečnostním tým KBM CSIRT kontaktovat telefonicky na čísle +420 351161201.

Pracovní doba bezpečnostním týmu KBM CSIRT je obecně omezena na běžnou pracovní dobu (08:00-16:30 od pondělí do pátku, s výjimkou svátků).

3. STANOVY

3.1 POSLÁNÍ

KBM CSIRT hraje klíčovou roli při ochraně informační infrastruktury zákazníků KBM-International s.r.o., veřejných institucí a komerčních ISP a institucí v západní části České republiky. 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 zákazníci KBM-International s.r.o. a zároveň instituce veřejného sektoru a ISP na jejich vyžádání. KBM CSIRT řeší úniky informací, narušení itegrity, potlačení služeb a nelegitimní použití u zákazníků KBM-International s.r.o. a s nimi souvisejících institucí a sítí.

3.3 ZAŘAZENÍ

KBM CSIRT je součástí sítě CSIRT týmů České republiky.

3.4 OPRÁVNĚNÍ

KBM CSIRT pracuje v mezích české legislativy.

KBM CSIRT spolupracuje se správci systémů a uživateli v rámci institucí veřejného sektoru a ISP.

4. ZÁSADY

4.1 TYPY INCIDENTŮ A ÚROVEŇ PODPORY

KBM CSIRT je oprávněn řešit všechny typy počítačových bezpečnostních incidentů, které vznikly nebo mohou potenciálně vzniknout u zákazníků KBM-International s.r.o.

Úroveň podpory poskytnuté KBM CSIRT se liší v závislosti na typu a závažnosti incidentu nebo problému, typ původce, velikosti uživatelské komunity a zdrojů KBM CSIRT v okamžiku incidentu, ale v každém případě bude poskytnut nějaký typ reakce během jednoho pracovního dne.

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 KBM CSIRT potřebnou podporu.

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.

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

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

KBM CSIRT 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 CSIRT týmů v případě potřeby
- Komunikace se zúčastněnými stranami.

5.1.3. ŘEŠENÍ INCIDENTU

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

5.2 PROAKTIVNÍ PŘÍSTUP

KBM CSIRT shromažďuje seznamy bezpečnostních kontaktů pro každou instituci svých zákazníků. Tyto seznamy jsou k dispozici v případě potřeby při řešení bezpečnostních incidentů nebo útoků.

KBM CSIRT 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.

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

KBM CSIRT se také snaží zvyšovat povědomí o bezpečnosti u svých zákazníků.

6. FORMULÁŘE PRO HLÁŠENÍ INCIDENTŮ

Formulář je ke stažení zde

7. ZPROŠTĚNÍ ODPOVĚDNOSTI

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