RFC 2350 STANDARD

DESCRIPTION FOR THE KBM-INTERNATIONAL S.R.O. CSIRT TEAM

1. ABOUT THIS DOCUMENT

This document contains a description for the KBM-International s. r. o. according to RFC 2350. It provides basic information about the CSIRT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 DATE OF LAST UPDATE

This is version 3 of 2017/11/16.

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications.

1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this KBM CSIRT description document is available from the KBM-International website - download here.

2. CONTACT INFORMATION

2.1 NAME OF THE TEAM

KBM CSIRT: CSIRT KBM-International spol. s.r.o. team

2.2 ADDRESS

KBM-International s.r.o.
Palackého 1732
35201, As
Czech Republic

2.3 TIME ZONE

CET, Central European Time (UTC+1, from the last Sunday in October to the last Saturday in March)

CEST, Central European Summer Time (UTC+2, from the last Sunday in March to the last Saturday in October)

2.4 TELEPHONE NUMBER

+420 351161201, +420 351161207

+420 608281308 ((outside of working hours)

2.5 FACSIMILE NUMBER

not available

2.6 OTHER TELECOMMUNICATION

Not available

2.7 ELECTRONIC MAIL ADDRESS

For the incident reports, please use the address csirt@e-kbm.cz

For the non-incident related messages, please use the helpdesk@e-kbm.cz

2.8 PUBLIC KEYS AND ENCRYPTION INFORMATION

For the incident related communication, you can use this key:
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 TEAM MEMBERS

The KBM CSIRT team leader is Miroslav Kalcic. A full list of KBM CSIRT team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

Management, liaison and supervision are provided by Lukas Karban, Head of Technical department.

2.10 OTHER INFORMATION

General information about the KBM CSIRT can be found at e-kbm.cz/csirt

2.11 POINTS OF CUSTOMER CONTACT

The preferred method for contacting KBM CSIRT is via e-mail.

Incident reports and related issues should be sent to the address csirt@e-kbm.cz. This will create a ticket in our tracking system.

For general questions please send an e-mail to support@e-kbm.cz.

If it is not possible (or not advisable for security reasons) to use e-mail, the KBM CSIRT can be reached by telephone +420 351161201.

The KBM CSIRT's hours of operation are generally restricted to regular business hours (08:00-16:30 Monday to Friday, except holidays).

3. CHARTER

3.1 MISSION STATEMENT

The KBM CSIRT plays a key role in safeguarding the information infrastructure of KBM-International customers, public institutions and commercial ISP and institutions in west part of Czech Republic. Our goal is to help them to effectively face security challenges, react on the incidents, coordinate actions to solve them and effectively prevent them.

3.2 CONSTITUENCY

Our constituency are KBM-International customers, public sector institutions and ISP on their request.

3.3 SPONSORSHIP AND/OR AFFILIATION

KBM CSIRT is part of the CSIRT teams network in Czech Republic.

3.4 AUTHORITY

The KBM CSIRT operates within the bounds of the Czech legislation.

The KBM CSIRT expects to work cooperatively with system administrators and users at public sector institutions and ISP's.

4. POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

The KBM CSIRT is authorized to address all types of computer security incidents which occur, or threaten to occur, in KBM International customers.

The level of support given by KBM CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and KBM CSIRT's resources at the time, though in all cases some response will be made within one working day.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator or their ISP for assistance. KBM CSIRT will support the latter people.

4.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

All incoming information is handled confidentially by KBM CSIRT, regardless of its priority. Information that is evidently very sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.

KBM CSIRT will use the information you provide to help solve security incidents.

4.3 COMMUNICATION AND AUTHENTICATION

E-mails and telephones are considered sufficiently secure to be used even unencrypted for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. TI, FIRST) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. SERVICES

5.1 INCIDENT RESPONSE

KBM CSIRT will assist local administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. INCIDENT TRIAGE

- Determining whether an incident is authentic.
- Determining the extent of the incident, and its priority.

5.1.2. INCIDENT COORDINATION

- Contact the involved parties to investigate the incident and take the appropriate steps.
- Facilitate contact to other parties which can help resolve the incident.
- Making reports to other CSIRT teams if needed.
- Communicate with stakeholders.

5.1.3. INCIDENT RESOLUTION

- Providing advice to the local security teams on appropriate actions.
- Follow up on the progress of the concerned local security teams.
- Provide assistance in evidence collection and data interpretation.

In addition, KBM CSIRT will collect statistics concerning incidents which occur within or involve its constituency, and will notify the community as necessary to assist it in protecting against known attacks.

5.2 PROACTIVE ACTIVITIES

KBM CSIRT maintains the list of security contacts for every institution in its constituency. Those are available when necessary for solving security incidents or attacks.

KBM CSIRT publishes announcements concerning serious security threats to prevent ICT related incidents or to prepare for such incidents and reduce the impact.

KBM CSIRT is also processing IoCs[1] from available sources and in case of a positive finding ensures propagation of relevant information to the contact responsible for the affected system.

KBM CSIRT also tries to raise security awareness in its constituency.

6. INCIDENT REPORTING FORMS

The form is available here.

7. DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, KBM CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.