“CSIRT Services, Information exchange and Cooperation”

International Regulatory Conference
16 May 2018, Ohrid, Republic of Macedonia
Инфо за MKD-CIRT / About us

Закон за електронските комуникации, член 26-а:
(1) Во состав на Агенцијата како посебна организациона единаца се формира национален центар за одговор на компјутерски инциденти (MKD-CIRT) како официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи кој идентификува и обезбедува одговор на безбедносни инциденти и ризици.

Law on electronic communications, article 26-a
• Official national point for contact and coordination in handling security incidents on networks and information systems, that will identify and ensure response to security incidents and risks.

CERT, CIRT, CSIRT ...
All ministries, public administration and the services of the Government of the Republic of Macedonia

Operators of Critical Infrastructure in the Republic of Macedonia, and

Large organizations in the banking, transport, communication, health, energy and other strategic sectors in the country

MKD-CIRT is open for cooperation with all stakeholders. More information on starting the cooperation can be found on the following link: https://mkd-cirt.mk/registracija/
MKD-CIRT constituency (2/2)

Sectors of critical infrastructure
• Water supply
• Transport
• Financial services
• Research and education
• Energy
• Information and communication technologies
• Health
# MKD-CIRT services

<table>
<thead>
<tr>
<th>Reactive</th>
<th>Proactive</th>
<th>Security Quality Management services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts &amp; Warnings</td>
<td>Announcements</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Incident handling</td>
<td>Tech watch</td>
<td>BC &amp; DR planning</td>
</tr>
<tr>
<td>Vulnerability handling</td>
<td>Security audits/Pentests</td>
<td>Security awareness</td>
</tr>
<tr>
<td>Incident coordination and response</td>
<td>Tools development</td>
<td>Training</td>
</tr>
<tr>
<td>Analysis of threats and vulnerabilities</td>
<td>Intrusion detection</td>
<td>Evaluation and certification of products and services</td>
</tr>
</tbody>
</table>
MKD-CIRT services

Alerts and warnings
- for disclosing details of current threats and steps that can be undertaken to protect against these threats

Incident response and handling
- provide technical assistance to address the security incidents when they occur, in order to mitigate the damage and recover from the incident.

Vulnerability response
- Assess the adequate measures necessary to respond to newly discovered vulnerabilities; assess their seriousness and impact, decide whether to issue warnings thereof or verify or further investigate their weight/impact

Coordinate an incident response
- coordination point at national or regional level among the countries affected by the security incident

Basic awareness, education & training
- Implement small-scale programmes for raising public awareness. Conduct basic training on computer incident response and main cybersecurity best practices

Coordinating an incident response
- Raising public awareness
- Conducting basic training
Reporting incidents and response

Citizens: web form for anonymous reporting on incidents:

Reporting on incidents by constituents
https://mkd-cirt.mk/prijava-na-incident/

• Fill in Word form with all the required information
  • Encryption with MKD-CIRT public key
  • Key ID: 0x333C00DB
  • Key Type: RSA 4096
  • Key Fingerprint: 0FB9 3DA3 E008 FA8B FC6A 9C71 0741 17A1 333C 00DB

• Send by e-mail to info@mkd-cirt.mk
The Incident Report should include a description of the incident or event

- Protection level of submitted information (Strictly Confidential, Confidential or Public)
- Contact Information (Name and surname, e-mail address, phone number)
- Details of the incident
  - Date, time / timestamp of detection and time zone
  - Level of impact on the organization (Critical, High, Low, No Impact, or Unknown)
  - Incident category (one of ten categories)
  - Current status of the incident (On-going, Incident is under control (localized), Incident has occurred previously, and Unknown)
  - Number of affected systems (estimate)
  - Features (description) of the incident
- System details
  - Name and address (Host / IP)
  - System function (e.g.: DNS system, Web server, E-mail server, etc.)
  - Tracking the incident report (Initial Report to MKD-CIRT, Continuation of a previous report)
MKD-CIRT, Incident categorisation

1. Compromised information
2. Compromised asset
3. Unauthorized access
4. Malicious code
5. (Distributed) Denial of Service
6. Theft or loss
7. Phishing
8. Unlawful activities
9. Scans / probes / Access attempts
10. Policy violations
Incident response coordination 1/2

• Network for information exchange and coordination
• 49 organization at this time
  • Administrative contacts
  • Technical expertise contacts
  • Public-facing resources (CIDR, domains ...)
• Next steps: Experts registry for mutual assistance
• MISP – malware information exchange platform
Incident response coordination 2/2

• First National exercise on incident response coordination

• Organized together with OSCE mission to Skopje

• 45 participants

• 35 organizations
  • Government
  • Public sector
  • Private operators of critical infrastructure

• Highly positive feedback and requests for further trainings
Notifications on threats and vulnerabilities

• Publishing announcements, advice and guidelines on our web site at https://mkd-cirt.mk
• Announcing information on Twitter https://twitter.com/mkdcirt
• Continuous campaign Stop. Think. Connect.
• Using the MISP Platform for Informing Constituents
International cooperation

• MoUs and agreements:
  • Government CSIRT of Moldova
  • National CERT of Slovenia
  • National CERT from Kosovo
  • National CERT from Albania
  • ICCIN – International Cyber Counter Intelligence Network
  • Stop.Think.Connect – International initiative
  • Trusted Introducer TF-CSIRT – MKD-CIRT, member since 2016
    • Accreditate member of TF-CSIRT since December 2017
  • Frequent communication and information exchange with CSIRTs from other countries: Italy, Spain, Czech Republic, Netherlands, Bulgaria
The following list contains all "Listed" teams. "Accredited" and "Certified" teams are - by definition - also "listed" teams, and are therefore contained in this list for your convenience.

**MKD-CIRT**

- **Macedonia, Former Yugoslav Republic**
- Updated on 11 Apr 2018

### General Information
- **Established**
  - 2016
- **Host Organisation**
  - Agencija za elektronski komunikaci Skopje (Agency for Electronic Communications)
- **Constituency Types**
  - Financial Sector, Government, National

### Contact Details
- **Team Email**
  - info@mkd-cirt.mk
- **Main Phone**
  - +389 2 3091 232
- **Public URLs**
  - https://mkd-cirt.mk
- **Emergency Phone**
  - +389 70 338 155
- **Timezone**
  - GMT+01 / GMT+02
- **Business Hours**
  - 08:30 to 16:30 Monday to Friday
Main objectives of the GCI is to measure the cybersecurity commitment of countries, thus helping them identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide.

ITU Global Cybersecurity Index

MATURING

INITIATING

2014 2017

MKD

LEGAL
Cybercriminal Legislation, Substantive law, Procedural cybercriminal law, Cybersecurity Regulation.

TECHNICAL
National CIRT, Government CIRT, Sectoral CIRT, Standards for organisations, Standardisation body.

ORGANIZATIONAL
Strategy, Responsible agency, Cybersecurity metrics.

CAPACITY BUILDING
Public awareness, Professional training, Educational programmes, R&D programmes, Incentive mechanisms, Home-grown industry.

COOPERATION
Intra-state cooperation, Multilateral agreements, International fora, Public-Private partnerships, Inter-agency partnerships.
Work statistics for MKD-CIRT

Annual work report for 2017, published at https://mkd-cirt.mk/dokumenti/
Public web in Macedonia

Number of registered .mk domains во 2017 TLD (Top Level Domain): 25168

• In 2017 we had 349 public web pages that were hacked, 23 official government web sites, .gov.mk

• Defacement & hacktivism

Number of attacked web sites per month in 2017
Incidents reported to MKD-CIRT

Number of reported incidents to MKD-CIRT in 2017

- Report malware: 50.62%
- Fast-Flux report: 0.18%
- DDoS: 0.36%
- Phishing: 0.18%

Graph showing the number of reported incidents by month:
- January: 30
- February: 75
- March: 52
- April: 57
- May: 9
- June: 135
- July: 50
- August: 27
- September: 27
- October: 33
- November: 19
- December: 48
Situation with malware in Macedonia for 2017 1/2

Number of distinct IP addresses as sources of attacks per day
Situation with malware in Macedonia for 2017 2/2

Reported malicious activities by malware type
Report on the Public survey for attitude towards cyber security, March 2018

Published at https://mkd-cirt.mk/dokumenti/

- Cybersecurity measures used when working on the internet
- Level of usage of online services and e-banking
- How well are citizens informed about protection of personal data on the internet
- Cybersecurity measures used by citizens when accessing social networks
- Types of devices used for accessing internet and online services
Public survey for attitude towards cyber security, March 2018

Types of devices used for internet access and used services:
- 90% of citizens are internet users
- 19% TV
- 84% Social networks
- 31% mobile
- 87% PC
- 3 out of 4 citizens use social networks
- Most frequent activities on internet:
  - Social networks: 84%
  - Buying/selling goods: 65%
  - News reading: 57%

Application of safety measures, use of passwords:
- Password on devices:
  - Не (No): 26%
  - Да (Yes): 74%
- Two-factor authentication:
  - Да (Yes): 76%
  - Не (No): 24%

Backups:
- 48% don’t make backup
- Out of all users practicing data backup:
  - Every day: 19.8%
  - 2-3 times per month: 16.9%
  - Each week: 19.4%
  - Less than: 43.9%
Public survey for attitude towards cyber security, March 2018

81.4% of respondents are concerned about identity theft.

Actions taken by respondents to protect children from online harassment:
- Talk with child on risks associated with using the internet: 33.8%
- Monitor child’s activities on the internet: 30.1%
- Limit child’s time for daily internet usage: 24.7%

Social networks usage and caution measures:

Top 5 social networks:
- Facebook: 77%
- Viber: 64%
- Instagram: 42%
- Skype: 37%
- YouTube: 34%

Most frequently shared personal information on the internet:
- Real name and surname: 7%
- Personal photo: 61%
- Date of birth: 42%
- Address: 40%
- E-mail: 28%

Awareness on the existence of social networks privacy policy:
- No: 49%
- Yes: 51%
MKD-CIRT activities for 2018

Annual work program for 2018 is published at https://mkd-cirt.mk/dokumenti/
MKD-CIRT Activities in 2018

New systems for:
- Threats intelligence
- Vulnerability assessment

Vulnerability assessment of the public web in Macedonia
Publishing guides for safe internet usage
Capacity building trainings for our constituents:
- Using the malware information sharing platform for information exchange
- Web applications Vulnerability assessment
- Pentesting with Kali Linux

Cybersecurity conference, October 2018
Thank you!

You can report incidents to us by:


info@mkd-cirt.mk

02/3091-232