REPUBLIC OF MACEDONIA

AGENCY FOR ELECTRONIC COMMUNICATIONS

NATIONAL CENTRE FOR COMPUTER INCIDENT RESPONSE

MKD-CIRT | REPUBLIC OF MACEDONIA
AGENCY FOR ELECTRONIC COMMUNICATIONS
NATIONAL CENTRE FOR
COMPUTER INCIDENT RESPONSE

2016 ANNUAL PROGRAMME OF THE NATIONAL CENTRE FOR COMPUTER INCIDENT RESPONSE

Contents

ABBREVIATIONS

Cyberspace	Information systems and services directly or indirectly connected to the Internet, telecommunications and computer networks, electronic communications networks
CIRT	Computer (Cyber) Incident Response Team Other abbreviations with similar meaning: CSIRT - Computer Security Incident Response Team CSRC - Computer Security Response Centre CIRC - Computer Incident Response Centre CERT - Computer Emergency Response Team IHT - Incident Handling Team IRC - Incident Response Centre IRT - Incident Response Team
AEC	Agency for Electronic Communications http://www.aec.mk
MARnet	Macedonian Academic Research Network http://marnet.mk
ITU	International Telecommunication Union http://www.itu.int/en/Pages/default.aspx
National/ Governmental CIRT	is a team that serves the Government by helping to protect the key/critical information infrastructures in the country. The National/Governmental CIRT plays a key role in coordinating the handling of incidents among the stakeholders at a national level. The National/Governmental CIRT is an official national contact point for information exchange and cooperation with the National/Governmental CIRTs of other countries (as defined by ENISA).
ENISA	European Union Agency for Network and Information Security https://www.enisa.europa.eu/
IMPACT	International Multilateral Partnership Against Cyber Threats, key partner of ITU

	http://www.impact-alliance.org/index.html
GCA	Global Cybersecurity Agenda. http://www.impact-alliance.org/aboutus/ITU-IMPACT.html
FIRST	Forum for Incident Response and Security Teams https://www.first.org/
TF-CSIRT	Trusted Introducer https://www.trusted-introducer.org/
CERT-EU	Computer Emergency Response Team for EU institutions https://cert.europa.eu/cert/plainedition/en/cert_about.html

LEGAL BASIS FOR ADOPTING THE ANNUAL PROGRAMME

Pursuant to Article 26a, paragraphs 2 and 3, of the Law on Electronic Communications ("Official Gazette of the Republic of Macedonia" No: 39/2014, 188/2014, 44/2015 and 193/2015), the Director of the Agency for Electronic Communications in cooperation with the Minister competent in the field of electronic communications hereby adopts the Annual Programme for the operation of the National Centre for Computer Incident Response established as a separate organisational unit within the Agency for Electronic Communications and submits it for adoption to the Government of Republic of Macedonia.

Accordingly, the Agency for Electronic Communications has received a positive opinion from the Ministry of Information Society and Administration.

INTRODUCTION

While the rapid technological development provides for huge new opportunities and potential sources of efficiency for the organisations of all sizes, these new technologies also bring unprecedented threats. Cybersecurity is a critical issue for all businesses and with the proliferation of new devices connected to the Internet its importance accordingly increases.

Reliable and secure cyberspace, that is to say, reliable and secure information systems and networks from cyber attacks and incidents provide political and social inclusion; reducing barriers between countries, communities and citizens; facilitating interaction and exchange of ideas and information; ensuring freedom of expression and freedom of the media; exercising the fundamental rights, and ensuring that citizens develop a more democratic society.

Studies have shown that a large number of citizens (EU currently represents one-third of the population) do not have confidence in the use of Internet services for electronic commerce and banking due to their concern of data security, i.e. the possibility of abuse thereof.

The cyberspace is not fully regulated, thus allowing cybercrime to be simple and inexpensive.

Crime-motivated computer/cyber attacks on the information systems and networks are becoming ever-growing global threat.

As per the amendments to the Law on Electronic Communications ("Official Gazette of the Republic of Macedonia" No. 188/2014), and pursuant to Article 26a, separate organisational unit - National Centre for Computer Incident Response has been set up within the Agency for Electronic Communications, which will be the official national point of contact and coordination in dealing with security incidents on networks and information systems, and will identify and respond to security incidents and risks.

MISSION

The National Centre for Computer Incident Response has the following mission:

a) coordinate and help/assist the authorities and public sector institutions in the implementation of proactive services for reducing the risk of computer security incidents, as well as in dealing with incidents when they occur,

b) conduct activities for educating and raising awareness among the citizens on the negative effects of cyber threats and cybercrime, and

c) provides timely advice for all its constituents.

CONSTITUENTS

Public sector constituents and critical infrastructure representatives in the Republic of Macedonia with whom MKD-CIRT will cooperate while implementing the 2016 Work Programme are as follows:

General Secretariat of the Government of the Republic of Macedonia

Office of the Prime Minister of the Republic of Macedonia

Ministry of Information Society and Administration

Ministry of Defence

Ministry of Interior

Ministry of Finance

Intelligence Agency

Personal Data Protection Directorate

Directorate for Security of Classified Information

Macedonian Academic and Research Network (MARnet)

Crisis Management Centre

MEPSO

EVN

National Bank of the Republic of Macedonia
Stopanska Banka
Komercijalna Bank
Makedonski Telekom

OBJECTIVES AND TASKS

The main objectives and tasks of the National Centre for Computer Incident Response are as follows:

O1. Play a key role in coordinating the handling of incidents among the stakeholders at a national level.

O2. Respond to computer incidents by providing the necessary services to its constituent/user, allowing it to efficiently deal with the incidents.

O3. Continuously monitor the risks, receive information about computer threats and incidents (automatically or via third parties) and continuously have at its disposal the indicators of incoming or outgoing malicious traffic in the country.

O4. Is an official national point of contact and exchange of information (incidents, vulnerability reports, etc.) within the country and abroad with the National/Governmental CIRTs of the countries in the region and beyond.

O5. Timely inform and notify its constituents. Provide for its constituents security advice, information for early warning and act as a focal point for issues related to cybersecurity.

O6. Fully cooperate and exchange information with the state institutions in charge of law enforcement, particularly those in the field of cybercrime, and adequately address the legal issues that may arise during the incident.

O7. Continuously exchange information, know-how and experience with the constituents, establish best security practices/guidelines and publish them accordingly, as well as continuously provide education and training for the constituents and for the employees of the Centre.

O8. Provide assistance when establishing internal centres for computer incident response of large organisations that manage key/critical information infrastructures (public and private) in the Republic of Macedonia.

O9. Continuously raise the awareness among the citizens on the negative effects of cyber threats and cybercrime.

(O1) PLAY A KEY ROLE IN COORDINATING THE HANDLING OF INCIDENTS AMONG THE STAKEHOLDERS AT A NATIONAL LEVEL.

Upon reporting or identifying a computer incident, the National Centre for Computer Incident Response will play a key role in coordinating the activities required to deal with the cyber incident. The coordination refers to inclusion and notifying the stakeholders at national level resolve and overcome the reported incident.

In order to accomplish this, the following activities will be undertaken:

- provide registry of contacts for crisis management
- provide various security communication channels with the relevant entities at national level
- provide appropriate rulebooks on overcoming the standard and familiar computer incidents

(O2) RESPOND TO COMPUTER INCIDENTS BY PROVIDING THE NECESSARY SERVICES TO ITS CONSTITUENT/USER, ALLOWING IT TO EFFICIENTLY DEAL WITH THE INCIDENTS.

In 2016 it is planned to be provided the following reactive and proactive services as per the recommendation in the ITU-IMPACT Report:

	Service	Description
1	Notifications and alerts	Disclose the details of current threats and steps that can be undertaken to protect against these threats. It includes notification or warning of newfound information on cyber threats and vulnerabilities to the constituents with a recommended course of action and guidance on how to protect the system. The notifications may be preventive, warning, advisory, and guiding.
2	Remote incident response	Provide technical assistance to address the security incidents when they occur, in order to mitigate the damage and recover from the incident. Advice and technical assistance is usually provided by telephone or e-mail.
3	On-site incident response	Provide on-site technical assistance and advice to address the security incidents when they occur, in order to mitigate the damage and recover from the incident. This service is usually related or implemented for critical level incidents.

4	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. Overall, this approach applies to information on vulnerabilities that are publicly known.
5	Basic awareness, education and training	Implement small-scale programmes for raising public awareness. Conduct basic training on computer incident response and main cybersecurity best practices.

And implement the preparatory activities for providing and ensuring the conditions for the following services.

	Service	Description
1	Coordinate an incident response	Acting as a coordination point at national or regional level among the countries affected by the security incident. In order to provide this service, MKD-CIRT must establish confidential communication with various parties and agencies at national, regional and global level.
2	Advanced awareness, education and training	Implement large-scale programmes for raising public awareness, such as conferences at national or regional level. Conduct advanced training on computer incident response and advanced cybersecurity best practices.

3	Coordinate a vulnerability response	Coordinate the responsible disclosure of information about a software/hardware vulnerability in due time. The timing of disclosure is determined so as to minimize the negative impact of early disclosure, by providing sufficient time for the vendor to develop and publish a patch and coincide it with the notification.
4	Analysis of threats and vulnerabilities	The analysis of computer and network threats and vulnerabilities for the purpose of determining their possible/potential impact and how to best mitigate them; Identify the new trends or changes in the modus operandi of the attacker; or advising on the general cybersecurity trends.

These services will ensure that the constituent/user will efficiently handle the cyber incident.

(O3) CONTINUOUSLY MONITOR THE RISKS, RECEIVE INFORMATION ABOUT COMPUTER THREATS AND INCIDENTS (AUTOMATICALLY OR VIA THIRD PARTIES) AND CONTINUOUSLY HAVE AT ITS DISPOSAL THE INDICATORS OF INCOMING OR OUTGOING MALICIOUS TRAFFIC IN THE COUNTRY.

Continuous monitoring of computer threats and incidents will be accomplished by:

- using appropriate software for their records
- monitoring the content presented on the internet in the field of cybersecurity and malicious traffic
- monitoring and participating in for a on the internet by having membership in international organisations
- enabling local alerts and information on identified computer threat or incident.

(O4) IS AN OFFICIAL NATIONAL POINT OF CONTACT AND EXCHANGE OF INFORMATION (INCIDENTS, VULNERABILITY REPORTS, ETC.) WITHIN THE COUNTRY AND ABROAD WITH THE NATIONAL/GOVERNMENTAL CIRTs OF THE COUNTRIES IN THE REGION AND BEYOND.

The function of an official national point of contact and information exchange with the institutions in the country, as well as abroad with the national/governmental CIRTs from countries in the region will be realised by initiating a membership or accession of the Republic of Macedonia and MKD-CIRT in international organisations.

- Initiating accession of the Republic of Macedonia and MKD-CIRT, as the official national point, to the Global Cyberesecurity Agenda Initiative of the ITU/IMPACT coalition comprised of 152 countries. With the accession, MKD-CIRT will gain access to the basic service package offered via GCA by the ITU/IMPACT, including:

  - Access to the reporting and alerting system

  - Option to include local cybersecurity experts in the IMPACT community

  - Option to escalate the detected incidents to IMPACT for the purpose of analysis and coordination when handling said incidents

  - Option to send detected malicious code to IMPACT for analysis

  - Receive periodic notifications and news on information security

  - Cooperation in preparing and conducting cybersecurity exercises that will help strengthen the capacities of MKD-CIRT and its constituents, and simultaneously allow increased international recognition of MKD-CIRT

- Inform ENISA on the establishment of MKD-CIRT as a national point for information exchange for the Republic of Macedonia. The European Network and Information Security Agency together with CERT-EU are the focal point for coordination and exchange of information between the national CIRTs in the Member States of the European Union.

  - Inform the national CIRTs in the Member States of the European Union on the establishment of MKD-CIRT as the official national point for information exchange and coordination of international activities with the Republic of Macedonia.

  - Initiate readiness to cooperate in preparing and conducting cybersecurity exercises that will help strengthen the capacities of MKD-CIRT and its constituents, and simultaneously allow increased international recognition of MKD-CIRT

  - Initiate a request for access to the resources provided by ENISA to other international CIRTs, such as notifications, best practices and working groups.

- Initiate the process for accession to FIRST and gaining the status Affiliated Member. FIRST, as a forum CIRTs, offers assistance in the communication among the individual CIRTs by introducing them to each other, or by using the established infrastructure and systems for information sharing and collaboration. This cooperation has the primary objective to accelerate the process of handling security incidents.

- Initiate the process of enrolment and accreditation of MKD-CIRT in TF-CSIRT Trusted Introducer, as an international organization providing services to CIRTs. The membership of MKD-CIRT will achieve the following:

- MKD-CIRT will be entered in the records and the list of CIRTs, as the official national point in the Republic of Macedonia, and the CIRTs that are members of TF-CSIRT will be informed about the establishment of MKD-CIRT

- Access to resources and infrastructure and systems of TF-CSIRT

- Option for accreditation of MKD-CIRT as a CIRT team with established best practices and implemented operating policies of Trusted Introducer, thus affording MKD-CIRT higher level of trust in communicating with the other members.

- Initiating cooperation with the national and governmental CIRTs in the countries of the region. The aim is to initiate cooperation with teams from other countries with an option to formalize them by signing memoranda of understanding with the following activities:

  - Exchange of information on secure and confidential communication

  - Exchange of information, reporting and alerting on security vulnerabilities and incidents

  - Cooperation and mutual assistance when dealing with international security incidents

  - Participation of local experts from MKD-CIRT and the constituents on regional cybersecurity workshops and exercises

- Informing the public in the Republic of Macedonia on the establishment of MKD-CIRT as the official national point for coordination and exchange of information by sending press releases and continuously informing the public on the security threats and how to protect against them.

- Informing the constituents and organisations in the public and private sector on the MKD-CIRT and its services by sending press releases and information on the manner of providing the services and establishing the cooperation.

(O5) PROVIDE FOR ITS CONSTITUENTS SECURITY ADVICE, INFORMATION FOR EARLY WARNING AND ACT AS A FOCAL POINT FOR ISSUES RELATED TO CYBERSECURITY.

The constituents will be informed in a timely manner by communication via security channels, including:

• introducing several different platforms/communication capabilities (phone, e-mail, fax, hardcopy, web, etc.).

- web-sites intended for advice and early warning, as well as on general information in the field of cybersecurity

- PGP-encrypted e-mail communication

• beside the traditional communication channels, dissemination of less critical or less sensitive (mainly public) information to its constituents and the public through new platforms (Facebook, Twitter, mailing lists, RSS feeds), in order to raise the public awareness on cybersecurity

(O6) FULLY COOPERATES AND EXCHANGES INFORMATION WITH THE STATE INSTITUTIONS IN CHARGE OF LAW ENFORCEMENT, PARTICULARLY THOSE IN THE FIELD OF CYBERCRIME

The National Computer Incident Response Centre will be fully committed to the cooperation and exchange of information with other state institutions responsible for implementing the legal framework of the Republic of Macedonia on the technical and organisational measures ensuring confidentiality and protection of data processing, network security, and personal data protection and in the field of cybercrime.

During this period, the Centre will propose draft amendments to the Law on Electronic Communications, as well as Rulebook on providing security and integrity of public electronic communication networks and services and the activities to be undertaken by operators in case of personal data security breach for the purpose of more efficient coordination of activities for dealing with computer security incidents and to ensure the flow of information on security and integrity of all communications networks.

In the same period, a draft text will be prepared to amend the rulebooks on the technical and organisational measures for ensuring confidentiality and protection of data processing in order to improve the same.

(O7) CONTINUOUSLY EXCHANGE INFORMATION, KNOW-HOW AND EXPERIENCES WITH ITS CONSTITUENTS, ESTABLISH BEST SECURITY PRACTICES/GUIDELINES

An important component in the functioning of the Centre is to provide staff that is technically capable to address all challenges when responding to computer incidents.

We are witnessing the extensive and rapid development of information technology, and particularly the development and distribution of malware. In order to catch-up with this trend of rapid development of new computer threats are their increasingly complex structure, the education and advancement of the Centre's employees are of very high importance. The education and development of the employees will be through self-education by using educational materials available online, by attending specialized courses for CIRTs organized by international organizations (e.g. TRANSIT I, TRANSIT II ...), but also by exchange of experiences with the local, regional and international centres for computer incident response during workshops and seminars.

It will continuously exchange information, know-how and experience with the constituents, define best security practices/guidelines and publish them accordingly. In this regard, MKD-CIRT will continuously provide education and training. Staff education aimed at gaining know-how and skills in the field of information security, information security management, management of computer security incidents, penetration testing, vulnerability detection and analysis, and forensics. The acquired know-how will be verified through certification of the employees in accordance with international certifications recognised by ENISA, ITU and EU, in the field of:

- Information security management and management of security incident response, such as ISC2 CISSP (Certified Information Security Professional), ISACA CISM (Certified Information Security Manager), EC Council CCSO (Certified Chief Information Security Officer), EC Council CIH (Certified Incident Handler)
- Forensics, penetration testing and encryption, such as the EC Council CES/CEH/CHFI (Certified Encryption Specialist/Certified Ethical Hacker/Computer Hacking Forensics Investigator)
- Risk analysis and management, such as ISACA CRISC (Certified in Risk and Information System Control)

(O8) PROVIDE ASSISTANCE WHEN ESTABLISHING INTERNAL CENTRES FOR COMPUTER INCIDENT RESPONSE OF LARGE ORGANIZATIONS THAT MANAGE KEY/CRITICAL INFORMATION INFRASTRUCTURES (PUBLIC AND PRIVATE) IN THE REPUBLIC OF MACEDONIA.

One of the more important activities of the National Centre for Computer Incident Response is to initiate the establishment of internal centres for computer incident response, particularly for organizations managing key/critical information infrastructures, upon request of the constituents, and to participate and assist in the process of establishing the internal centres for computer incident response, particularly for organizations managing key/critical information infrastructures.

This is important for several reasons:

- Increasing the number of trained technical staff in charge of responding to computer incidents
- Improving the maintenance and preventive actions at institutional level for ensuring protection against computer incidents
- Ensuring rapid and effective response in crisis situations
- Raising the awareness level on cybersecurity among the individual institutions

(O9) CONTINUOUSLY RAISE THE AWARENESS AMONG THE CITIZENS ON THE NEGATIVE EFFECTS OF CYBERTHREATS AND CYBERCRIME.

The most important preventive measure for combating computer incidents and cybercrime is raising the awareness of the citizens about cybersecurity.

This objective is accomplished by providing education and training services.

In 2016, following activities are envisaged to meet these objectives:

- Publication of basic educational content on cybersecurity on the official website of the Centre
- Preparation of interactive content for cybersecurity as a continuous activity in the upcoming years
- Preparation of content for different age groups of citizens to be presented via all media channels.
- Continuous public campaigns on internet security for the purpose of raising the awareness of citizens on the protection against cyber attacks

ACTION PLAN

The 2016 Action Plan of the National Centre for Computer Incident Response is presented in Table 1.

Table 1

Ser.	Activity	Timeframe (Q-Quarter)
1	Installation of the hardware and software solutions to support the monitoring and recording of information on cyber threats and incidents.	Q1
2	Setting up a system for service quality management for monitoring the effectiveness of the Centre for Computer Incident Response and for ensuring a continuous improvement process.	
3	Providing a secure way of reporting incidents through various communication channels: telephone/mobile, e-mail with PGP encryption, fax, hardcopy, and web-forms.	Q1

4	Creating official website with the following features ° General information on the Centre ° Enable reporting incidents and illegal content ° Notifications on current information about security incidents ° Access to documents (annual reports, ...) ° List of services and their initiation ° Events ° Useful links ° Legislation ° Contacts ° Public part for release of information, notifications and advice aimed at raising the public awareness on cybersecurity and cyber threats ° Restricted part for secure communication with the constituents	Q1-Q4
5	Preparation of rulebooks and procedures ° Processing of reported incidents by ° external centres ° constituents ° citizens ° Services for the constituents ° Code of conduct and flow of information ° Classification of computer security incidents º Processing and handling of classified incidents	Q1-Q4

6	Informing the public of Republic of Macedonia and publication of basic educational content on cybersecurity on the official website of the Centre	Q1-Q4
7	Preparation of content for different age groups of citizens to be presented via media channels.	Q3-Q4
8	Informing the constituents and collecting data on their infrastructure, authorized contacts and public PGP keys for secure communication and information exchange.	Q1
9	Obtaining personnel security clearance	Q1-Q4
10	Joining international organizations as an official national point of contact for computer incident response.	Q2

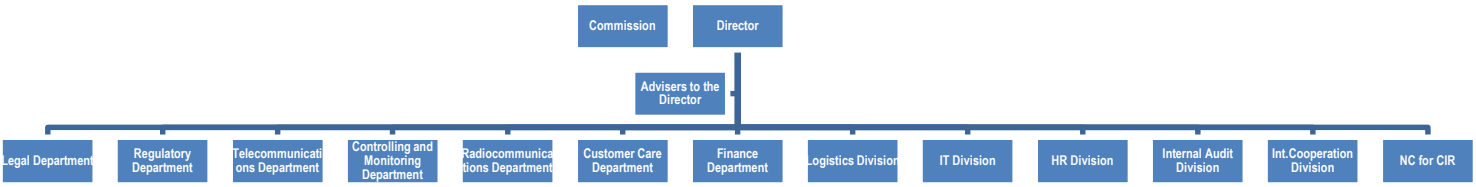
ORGANISATION

ORGANISATION AND AVAILABLE RESOURCES

The National Centre for Computer Incident Response has been established as a separate organizational unit within the Agency for Electronic Communications.

An excerpt from the organogram of the AEC's internal organisation is presented in Figure 1.

Figure 1



HUMAN RESOURCES

5 positions are envisaged fro the National Centre for Computer Incident Response, as per the structure presented in Table 2.

Table 2

Position within the systematization	Qualification	Position code				
Head of Department - National Centre for Computer Incident Response	VSS (B.Sc.)	AEC	01	01	B02	1
Adviser for computer incident response	VSS	AEC	01	01	C01	1
Adviser for computer incident response	VSS	AEC	01	01	C01	1
Adviser for computer incident response	VSS	AEC	01	01	C01	1
Adviser for computer incident response	VSS	AEC	01	01	C01	1

The personnel of MKD-CIRT must have security clearance for access to classified information issued by the Directorate for Security of Classified Information pursuant to Article 38 of the Law on classified information and in accordance with the international recommendations (ITU, ENISA and EU). The personnel of MKD-CIRT must have an authorisation for personal data processing issued by the Agency for Electronic Communications.

MKD-CIRT job applicants must have a certificate related to information and communication security, and priority will be given to applicants with internationally recognized certificates issued by ENISA, ITU and EU, such as ISC2 CISSP, ISACA CISM, CRISC, CCSO, CIH, CES, CEH, CHFI.

FINANCIAL PLAN

The planned funding for operations of the Centre for Computer Incident Response is set out in the 2016 Annual Financial Plan of the Agency for Electronic Communications, which is an integral part of the Annual Work Programme of the Agency for Electronic Communications adopted on 01.12.2015, and published on the website of the Agency for Electronic Communications.

Listed below are extracts from the Annual Financial Plan concerning the operations of the Centre for Computer Incident Response:

Table 3

Account item	**Description**	**Amount**
417710	Training and professional development - CIRT	1.200.000
417741	Seminars and conferences (fees)	350.000
416xxx	Membership fees - CIRT	180.000

Expenditure item 417 - intellectual and other services

Planned expenditures of 1.550.000 denars for intellectual and other services in 2016 comprise of the following:

o Seminars and conferences (fees)

o Training for professional development

Expenditure item 416 - membership fees

The estimated amount of this expenditure category is 180.000 denars, which includes the cost for settlement of regular annual liabilities for: o Membership fees in international institutions (CIRT);

CONCLUSION

During 2016, the Centre for Computer Incident Response will intensively work to fulfil the mission and set objectives by implementing all envisaged activities.

One of the main challenges this year will be staffing the computer incident response team, providing support to all constituents, and educating them to perform their tasks.

Providing basic information on raising awareness among the citizens on cybersecurity and cybercrime in this period will be the basis for further enhancements and continuous enrichment with new content.

This year, the communication with other centres for computer incident response in the region and beyond will be officially open.

ENTRY INTO FORCE

The Annual Programme on the operations of the National Centre for Computer Incident Response shall enter into force on the day of publication of the Decision on its adoption by the Government of Republic of Macedonia in the Official Gazette of the Republic of Macedonia.

Acting Director of the

Agency for Electronic Communications

Vladimir Ristevski

[signature-illegible] [stamp]