ITU Events

ITU Regional Cybersecurity Forum for Europe and CIS

POLICIES & STRATEGIES

CERTIFICATION FRAMEWORKS

DATA PROTECTION

SECURITY CHALLENGES

5G, eSIM IoT, AI

27 – 28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

Hosted and co-organized by:

REPUBLIC OF BULGARIA
State e-Government Agency

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

REPUBLIC OF NORTH MACEDONIA

National Cyber Security Strategy 2018–2022: RECAP

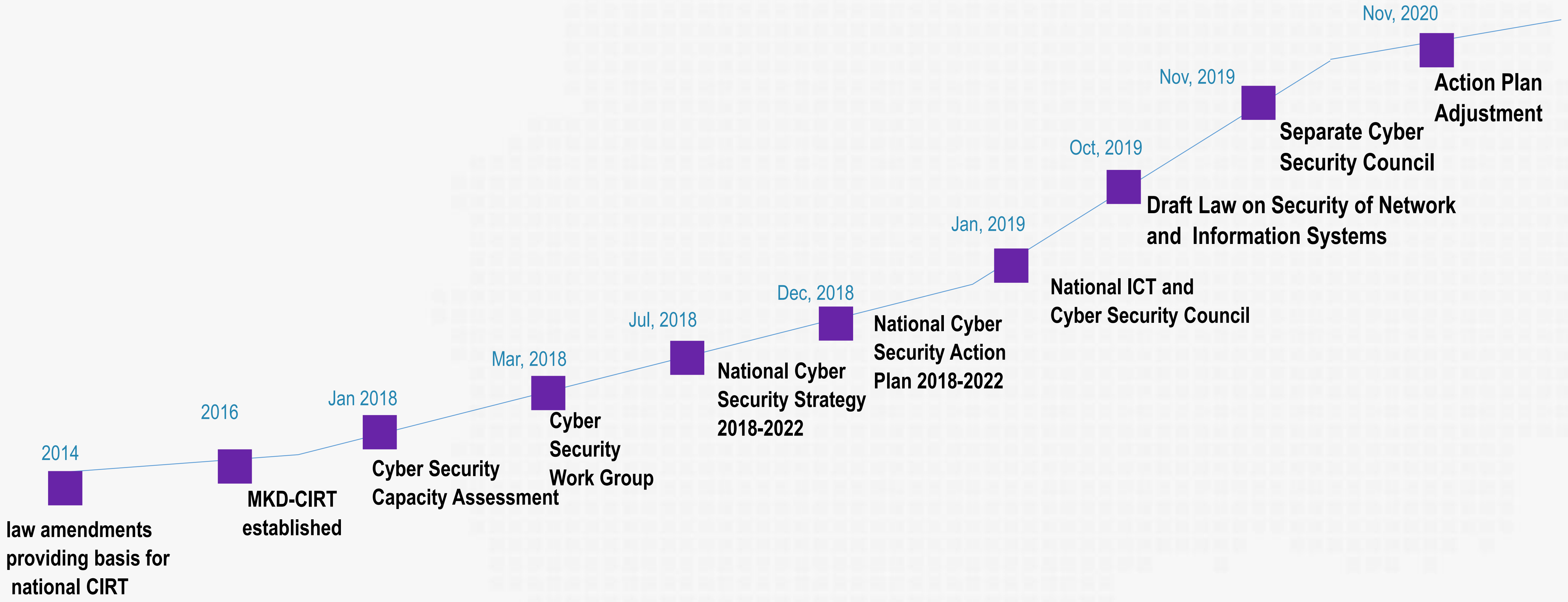
Sofia, February 2020

ABOUT US

North Macedonia

- Population: **2,084,367 million**
- Internet Penetration: **79,3 %**
- Area: **25,713 km^2**
- Currency: **MKD**

CYBER SECURITY ACTIVITIES TIMELINE



2014
law amendments providing basis for national CIRT

2016
MKD-CIRT established

Jan 2018
Cyber Security Capacity Assessment

Mar, 2018
Cyber Security Work Group

Jul, 2018
National Cyber Security Strategy 2018-2022

Dec, 2018
National Cyber Security Action Plan 2018-2022

Jan, 2019
National ICT and Cyber Security Council

Oct, 2019
Draft Law on Security of Network and Information Systems

Nov, 2019
Separate Cyber Security Council

Nov, 2020
Action Plan Adjustment

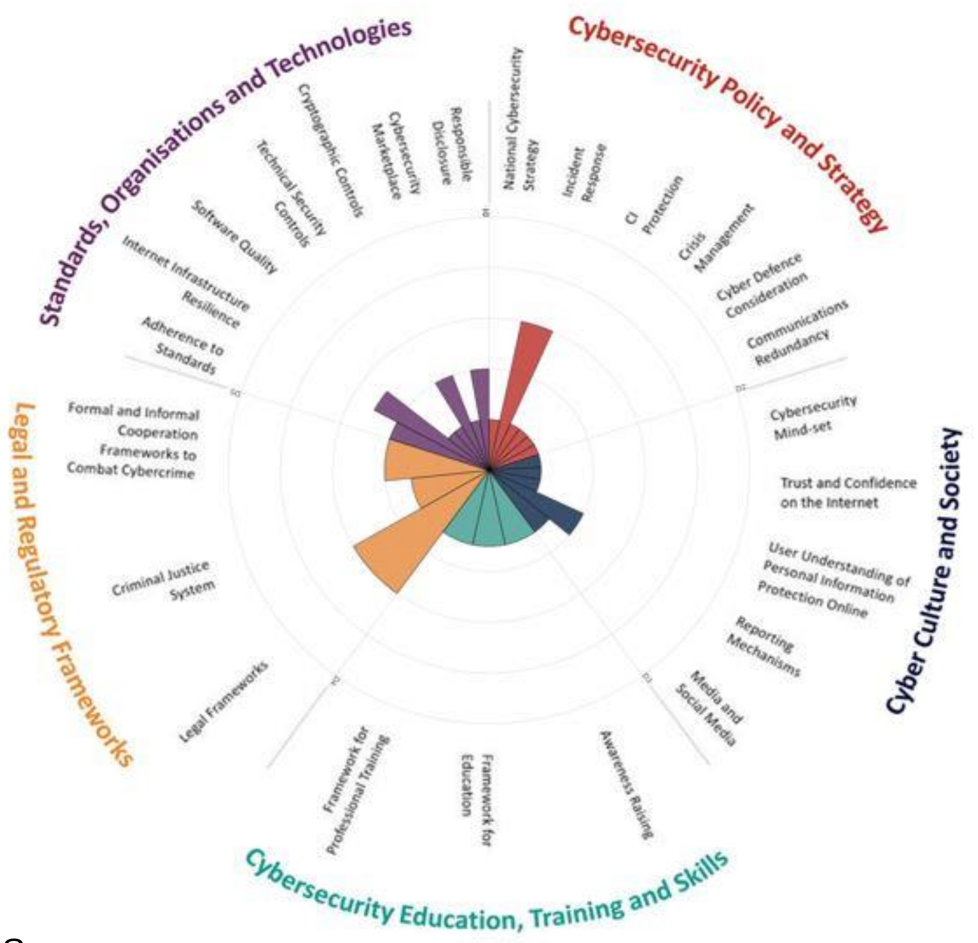
Cyber Security Activities

- **2014** - Amendments to the Law on Electronic Communications providing basis for establishment of national CIRT (no obligation for mandatory incident reporting)
- **2016** - National Computer Incident Response Team MKD-CIRT team established within the Agency for electronic communications

- **Jan-Feb 2018** - Cyber Security Capacity Assessment (GCSCC, University of Oxford)
- **March 2018** - National Cyber Security Working Group established
- **July 2018** –National Cyber Security Strategy 2018-2022 adopted
- **December 2018** - National Cyber Security Action Plan 2018-2022 adopted
- **January 2019** – National ICT and Cyber Security Council established
- **October 2020** - Draft Law on Security of Network and Information Systems - public consultations started
- **November 2019** – Separate National Cyber Security Council established

- **February 2020** – Adjustment to National Cyber Security Action Plan/ Annual operational plan prepared

CYBER SECURITY CAPACITY ASSESSMENT



Jan-Feb 2018 - Cyber Security Capacity Assessment (Global Cyber Security Capacity Centre, University of Oxford – World Bank partnership)

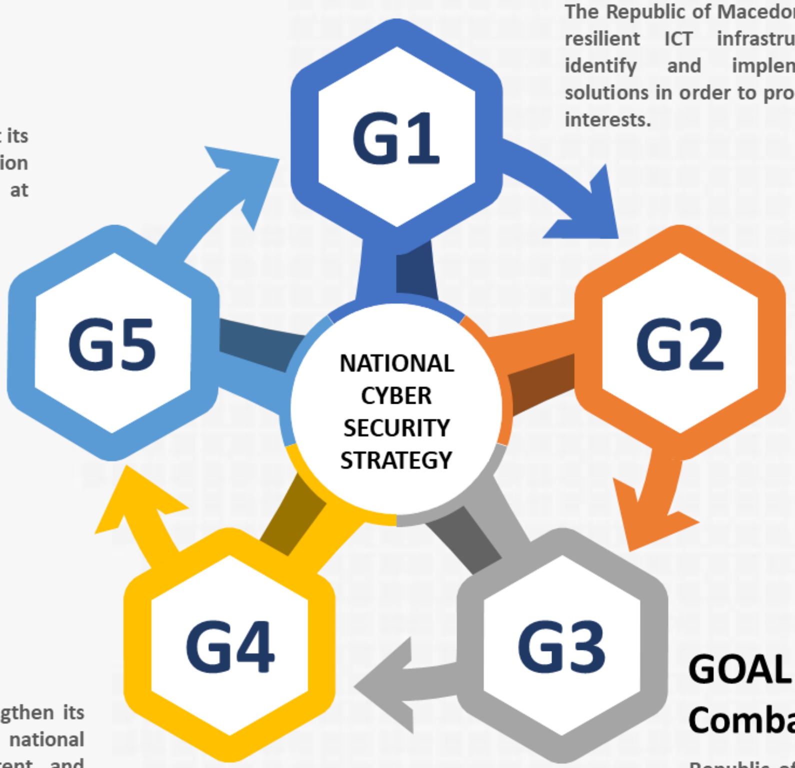
Source:
The Global Cyber Security Capacity Centre | Oxford Martin School: Cybersecurity Capacity Review, Republic of North Macedonia, 2018

STRATEGY PREPARATION PROCESS

Multi-stakeholder engagement – public consultation process

- Public sector entities
- Technology and telecommunications sector
- Finance sector
- Critical Infrastructure owners
- Academia
- Civil societies / NGOs
- International community

NATIONAL CYBER SECURITY STRATEGY 2018-2022



GOAL 1:
Cyber resilience

The Republic of Macedonia to have cyber resilient ICT infrastructure, and to identify and implement adequate solutions in order to protect the national interests.

GOAL 2:
Cyber capacities and cyber culture

The public sector, the private sector and the Macedonian society to have a comprehensive understanding of cyber threats and to have the necessary capacities to protect themselves.

GOAL 3:
Combating cyber crime

Republic of Macedonia to strengthen its capacities for prevention, research and adequate response to cyber crime.

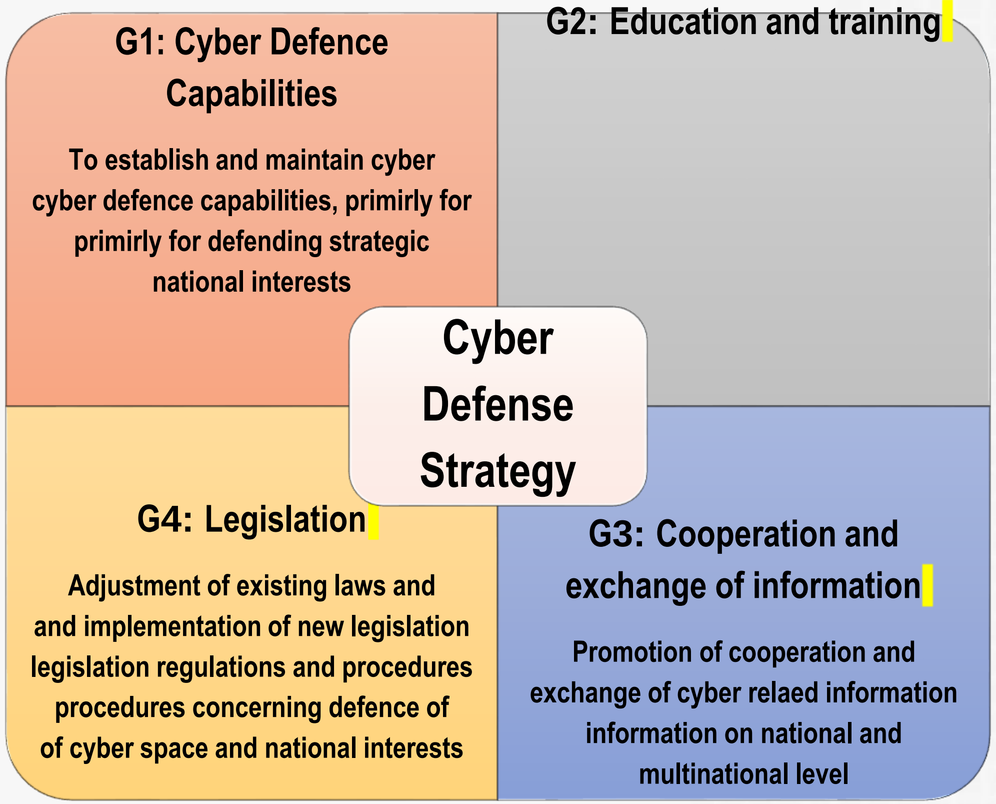
GOAL 4:
Cyber defence

Republic of Macedonia to strengthen its capacities for defence of national interests and to reduce current and future cyber space risks.

GOAL 5:
Cooperation and exchange of information

Republic of Macedonia to protect its cyber space through cooperation and exchange of information at national and international level.

Cyber Defense Strategy



G1: Cyber Defence Capabilities

To establish and maintain cyber cyber defence capabilities, primirly for primirly for defending strategic national interests

G2: Education and training

Cyber Defense Strategy

G4: Legislation

Adjustment of existing laws and and implementation of new legislation legislation regulations and procedures procedures concerning defence of of cyber space and national interests

G3: Cooperation and exchange of information

Promotion of cooperation and exchange of cyber relaed information information on national and multinational level

Goal I

- Building capabilities for protection of national interests
- Capabilities in support of NATO, EU projects and operations
- Capabilities to detect and deter cyber threats
- Management of crisis situation cyber originated

Goal II

- Building cyber awareness concerning cyber defense system
- Develop strategic, operative and tactical level experts
- Establish Institute for Cyber Defense and digital forensics
- Participation in CCDCOE (NATO Cyber Center of Excellence)

Goal III

- Develop system for monitoring and exchange of info concerning CII
- Develop civilian-military cooperation in cyber field
- Defining NSWAN point of contact and secure communication
- Incorporating into NATO's collective defense system

Goal IV

- Unique legislation framework concerning cyber defense
- Methodology for cyber assessment of threats
- Define role of military capacities in defense of CII
- Coordination of military plan with national cyber defense

Combating Cyber Crime

1.Advancing the cyber crime handling and management capacities.
2.Harmonizing the national with international policies related to cyber-crime
3.Development of a single, comprehensive legal framework for cyber crime, taking into consideration the applicable legal framework in the Republic of North Macedonia and EU.
4.Modernizing authorities in charge of cyber crime in order to efficiently combat cyber crime.
5.Establishing efficient procedures to report and research cyber crime.
6.Establishing formal procedures for cooperation and exchange of information in the field of cyber crime among relevant national entities and other security services.
7.Advancing cooperation with regional and international organizations in the fight against cyber crime.

8. Advancing the existing and establishing new mechanisms for cooperation and exchange of information with the private and civil sectors.
9. Securing expert-specialist education and training for individuals working in the field of identification and research of cyber crime.
10. Developing a multidisciplinary academic environment for the advancement of national capacities for cyber crime investigations.
11. Active participation in the creation of international cyber crime regulations and standards, as well as their implementation on national level.
12. Continuous assessment of the adequacy and efficiency of the national cyber crime regulation.
13. Providing continuous education and training for law enforcement entities in the field of cyber security, cyber crime and electronic evidence.

NATIONAL CYBER SECURITY ACTION PLAN 2018-2022

Priority activities

1. Establishing a National Cyber Security Council
2. Establishing a Body with operational cyber security capacities
3. Defining and protection of the Critical Information Infrastructure (CII) and other Important Information Systems (IIS)

* Legal framework – harmonization of the EU NIS Directive, strengthening the authority of the National Centre for Computer Incident Response

NATIONAL CYBER SECURITY COUNCIL

Goal:

- strategic level decision making
- coordination and monitoring of implementation of the Strategy and Action plan
- prioritize cyber security at the top of the political agenda of North Macedonia

Members:

- Minister of Information Society and Administration (chair)
- Minister of Interior
- Minister of Defence

1st session: 02.01.2020

- requested adjustments to the Strategy and Action plan

BODY WITH OPERATIONAL CYBER SECURITY CAPACITIES

- in charge of operational implementation of the Strategy and Action Plan
- competencies defined in the new Draft Law on Security of Network and Information systems (*planned as a part of Digital Agency)
- ongoing project for institutional restructuring (MISA)
- (temporary solution) Inter-ministerial working group established to support the National Cyber Security Council and coordinate the Action Plan on operational level

CRITICAL INFORMATION INFRASTRUCTURE

- methodology for CII identification determined
- sectors determined in line with NIS directive
- CII mandated agencies identified for each sector

next steps:

- capacity building in the CII mandated agencies (expert assistance required)
- determining sector-specific criteria
- establishing list of Critical Services and list of CI Operators
- CII assets and services identification

LEGAL FRAMEWORK

- Draft Law on Security of Network and Information Systems (harmonization with NIS Directive 2016/1148 and in line with ENISA regulation EU 526/2013 and EU 2019/881)
- Extended public consultation process started October 2019
- Legally establishing the Body with operational cyber security capacities as Digital Agency
- Incorporate the National Centre for Computer Incident Response and increase it’s authorities and responsibilities
- Promote strategic collaboration and information sharing, define coordination between CSIRTS
- Adoption planned : end of 2020

CYBER CAPACITIES AND CYBER CULTURE

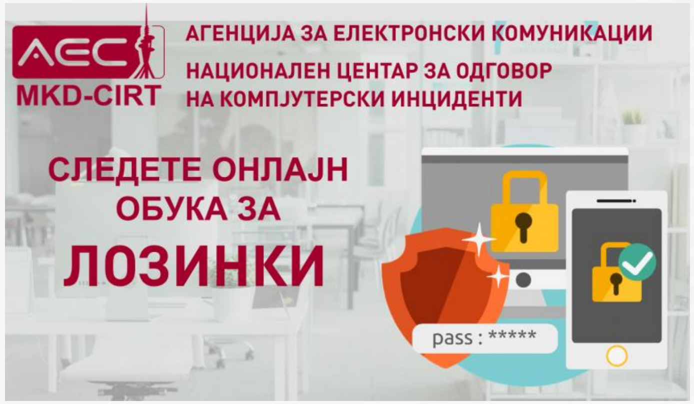
АЕК MKD-CIRT

АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

КЛИКНИ ОВДЕ ЗА ПОЧЕТОК НА ОБУКА

ФИШИНГ НАПАДИ



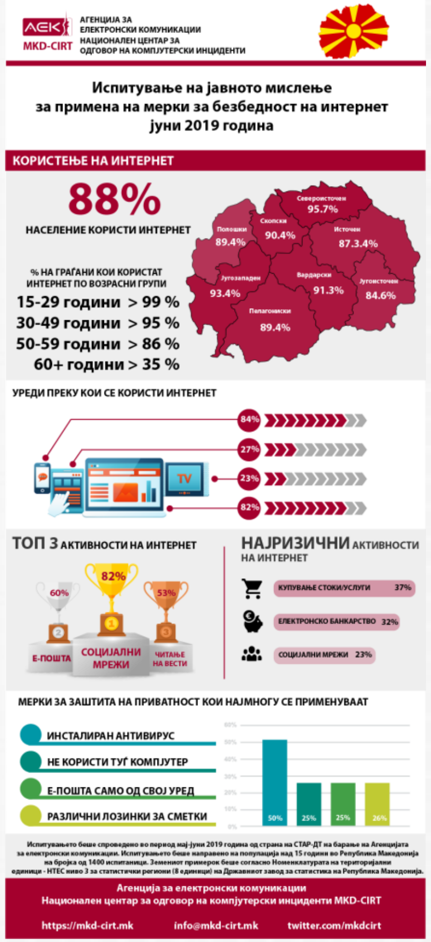
АЕК MKD-CIRT

АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

СЛЕДЕТЕ ОНЛАЈН ОБУКА ЗА

ЛОЗИНКИ



АЕК MKD-CIRT

АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ
НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

Испитување на јавното мислење за примена на мерки за безбедност на интернет јуни 2019 година

КОРИСТЕЊЕ НА ИНТЕРНЕТ

88%

НАСЕЛЕНИЕ КОРИСТИ ИНТЕРНЕТ

% НА ГРАЃАНИ КОИ КОРИСТАТ ИНТЕРНЕТ ПО ВОЗРАСНИ ГРУПИ

15-29 години > 99 %
30-49 години > 95 %
50-59 години > 86 %
60+ години > 35 %

УРЕДИ ПРЕКУ КОИ СЕ КОРИСТИ ИНТЕРНЕТ

ТОП 3 АКТИВНОСТИ НА ИНТЕРНЕТ

НАЈРИЗИЧНИ АКТИВНОСТИ НА ИНТЕРНЕТ

КУПУВАЊЕ СТОКИ/УСЛУГИ	37%
ЕЛЕКТРОНСКО БАНКАРСТВО	32%
СОЦИЈАЛНИ МРЕЖИ	23%

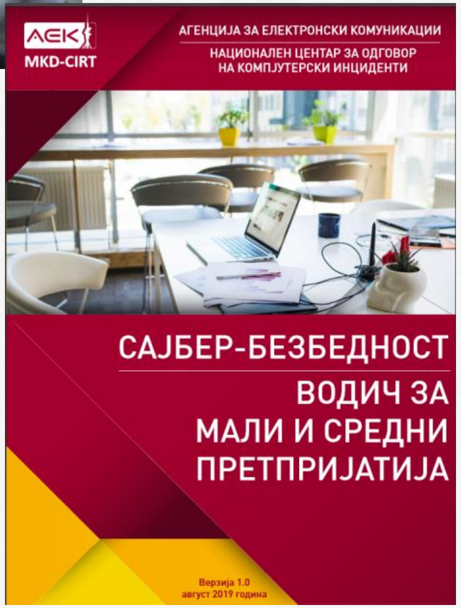
МЕРКИ ЗА ЗАШТИТА НА ПРИВАТНОСТ КОИ НАЈМНОГУ СЕ ПРИМЕНУВААТ

ИНСТАЛИРАН АНТИВИРУС	50%
НЕ КОРИСТИ ТУЃ КОМПЈУТЕР	25%
Е-ПОШТА САМО ОД СВОЈ УРЕД	25%
РАЗЛИЧНИ ЛОЗИНКИ ЗА СМЕТКИ	26%

Испитувањето беше спроведено во период мај-јуни 2019 година од страна на СТАР-ДТ на барање на Агенцијата за електронски комуникации. Испитувањето беше направено на популација над 15 години во Република Македонија на бројка од 1400 испитаници. Земениот примерок беше согласно Номенклатурата на територијални единици - НТЕС ниво 3 за статистички региони (8 единици) на Државниот завод за статистика на Република Македонија.

Агенција за електронски комуникации
Национален центар за одговор на компјутерски инциденти MKD-CIRT

https://mkd-cirt.mk info@mkd-cirt.mk twitter.com/mkdcirt



АЕК MKD-CIRT

АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

САЈБЕР-БЕЗБЕДНОСТ

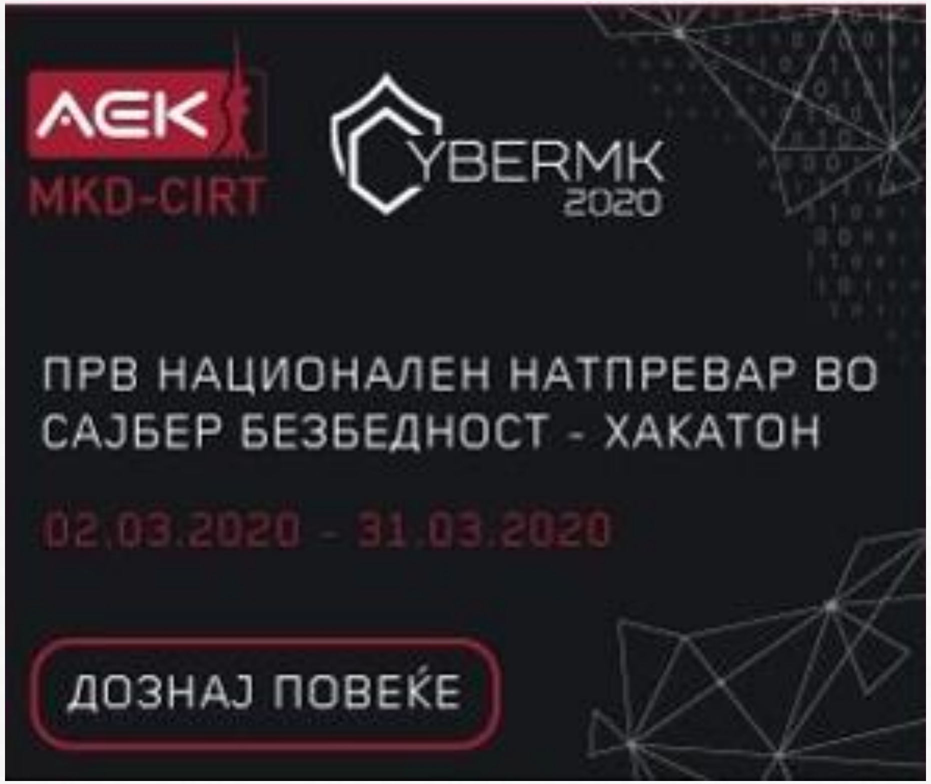
ВОДИЧ ЗА МАЛИ И СРЕДНИ ПРЕТПРИЈАТИЈА

Верзија 1.0
август 2019 година

CYBER CAPACITIES AND CYBER CULTURE

Cyber MK 2020 – First National Cyber Security Hackaton

1st – 15th March	Registration (online)
16th – 20th March	Prequalification (online)
25th March	Semifinals (online)
28th – 29th March	Finals (on site)



ПРВ НАЦИОНАЛЕН НАТПРЕВАР ВО САЈБЕР БЕЗБЕДНОСТ - ХАКАТОН

02.03.2020 - 31.03.2020

CYBER CAPACITIES AND CYBER CULTURE

- ISO 27005 Certified Risk manager courses
- Vulnerability assessment courses
- MKD-CIRT technical capacities for SOC upgraded
- MKD-CIRT classroom with capacity of twenty participants
- MKD-CIRT laboratory for malware analysis and digital forensics equipped
- February – June 2020 - Network security and vulnerability assessment courses (NATO Peace for security program)

COOPERATION AND EXCHANGE OF INFORMATION

- June 2019 – ITU Workshop for Europe on National Cyber Security Strategies
- June 2019 – Cyber Security Conference “CSIRTs and Cyber Resilience”
- July 2019 – UK-North Macedonia National Cyber Security Workshop
- October 2019 – Cyber Security Incident response - Coordination and communication workshop
- November 2019 – Cyber security training for primary school students, teaching staff and parents

- June 2020 - ITU cyber drill

LESSONS LEARNED

- Budgeting
- Keep it lean, especially at the beginning: less people involved, more flexibility, fast action
- Accountability: one institution per activity only
- KPIs
- Realistic timeline
- Monitoring of the implementation
- Periodical revision of the action plan, taking into account current conditions
- Good practice: annual operational plan for effective implementation of activities

INTERNATIONAL PARTNERS

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

British Embassy Skopje

DCAF

DCAF
a centre for security, development and the rule of law

Global Cyber Security Capacity Centre

KWPF
KOREA-WORLD BANK PARTNERSHIP FACILITY

European Commission

ITU

OSCE
Organization for Security and Co-operation in Europe
Mission to Skopje

RegionalCooperationCouncil

THANK YOU!

Natalija Veljanoska

Ministry of Internal Affairs

Natalija_Veljanoska@moi.gov.mk

Government of the Republic of North Macedonia