DCAF Geneva Centre for Security Sector Governance
20TH ANNIVERSARY

CYBER THREATS DURING THE COVID-19 OUTBREAK AND ACTIVITIES OF NATIONAL CERTS IN THE WESTERN BALKANS

Nele Achten

CYBER THREATS DURING THE COVID-19 OUTBREAK AND ACTITIVITIES OF NATIONAL CERTS IN THE WESTERN BALKANS

Author

Nele Achten

Table of Contents

1. INTRODUCTION

The objective of this report is to outline the cyber incidents and response of national Computer Emergency Response Teams (CERTs) in Western Balkan economies in Spring 2020, during the first months of COVID-19. The report analyses challenges related to the work of national CERTs and provides insights on how transnational and private sector cooperation could improve cyber incident response in the region. This analysis might also be helpful for other regions in the world where national CERTs have been established more recently.

2. CATEGORISATION OF CYBER THREATS DURING THE COVID-19 OUTBREAK

The outbreak of COVID-19 has changed our life and work environment. Almost from one day to another, most people started to work from home, schools and almost all higher education facilities moved to an online format. Our lives moved online: Sometimes this included an appointment with the doctor through a video call or the delivery of groceries ordered online. This new reality has increased our vulnerability to cyber threats. The following section categorises some of the known cyber threats present during the outbreak of COVID-19 and describes the activities of Western Balkan national CERTs in this context.

In a COVID-19 world, where many services have moved online at accelerated speed, there are naturally more cyber threats to not only individuals and businesses, but also educational institutions, healthcare facilities, critical infrastructure and state organs. In the Western Balkan region, the largest vector of cyber threats during the early months of COVID-19 came from traditional phishing campaigns. In a small survey conducted as part of this report, all Western Balkan national CERTs have reported an increase of phishing attacks. These phishing attacks not only targeted individuals and the health care sector, but also e-commerce and e-businesses.

International policy debates, however, focused largely on cyber threats to the health care sector. Australia and the United States of America, for example, expressed concerns and called out cyber attacks on hospitals as intolerable.[1] In May 2020, more than 40 international leaders called on “the world’s governments to take immediate and decisive action to prevent and stop cyberattacks that target hospitals, healthcare, research organisations, and international authorities providing critical care and guidance in the midst of the ongoing global pandemic.”[2] For a structured debate at the national level, it might be useful to categorise cyber threats in the healthcare sector as follows:

[1] ‘The United States Concerned by Threat of Cyber Attack Against the Czech Republic’s Healthcare Sector’ (April 17, 2020), United States Department of State; ‘Australia and US call out cyber attacks on hospitals during COVID-19 pandemic’ (April 27, 2020) ZDNet, https://www.zdnet.com/article/australia-and-us-call-out-cyber-attacks-on-hospitals-during-covid-19-pandemic/.

[2] For the text of this international call, see for example ‘World Leaders Call on Governments to Stop Cyberattacks Plaguing Healthcare Systems’ (May 26, 2020) CyberPeace Institute, https://cyberpeaceinstitute.org/blog/2020-05-26-world-leaders-call-on-governments-to-stop-cyberattacks-plaguing-healthcare-systems

(1) threats to governmental healthcare agencies

(2) threats to hospitals and healthcare facilities

(3) threats to research- and development facilities

(4) threats related to the use of new apps developed in the context of COVID-19

The survey conducted for this report revealed that most cyber incidents which occurred in Western Balkan economies belong to the first category. However, even without reported incidents, hospitals and COVID-19 related research facilities have become targets. In particular, several significant cyber incidents targeting hospitals have gained international attention after major incidents in two European countries.[3] Both incidents led to an interruption of medical services, risking patients` lives.

In addition to increased cyber threats and policy debates regarding the healthcare sector, an increase in research and public debate on security risks in the sector of education and in the context of digital infrastructuresis taking place.

3. ACTIVITIES AND CHALLENGES OF NATIONAL CERTS IN THE WESTERN BALKANS

National CERTs, or Computer Security Incident Response Teams (CSIRTs), have been created or re-organised in many countries during the last few years. Most mandates of national CERTS are broad and the exact scope of work still needs to be defined. This is not different in the economies from the Western Balkans.

The following analysis is based on a survey and information gathered during an online meeting with representatives of all national CERTs in the Western Balkans.[4] The activities of national CERTs in the Western Balkans during the outbreak of COVID-19 can be divided into two categories: (1) awareness raising and public warnings; (2) trainings and educational activities. Finally, this section addresses co-operation of CERTs with essential service providers.

3.1 Awareness Raising and Public Warnings

During the early months of COVID-19, some national CERTs in the Western Balkans raised public awareness regarding cyber threats related to working and teaching online. Both the Albanian and Serbian CERTs reported public educational campaigns on emerging cyber threats related to the COVID-19 pandemic. The Albanian national CERT, for example, produced

[3] One in Brno (Czech Republic) and the other in Dusseldorf (Germany).

[4] This meeting was organised and supported by the Geneva Center for Security Sector Governance (DCAF), July 2020.

informational materials on secure remote work and advised educational institutions on better security for online examination procedures.

Serbia recently published two public warnings regarding nationwide phishing campaigns. One warning was related to phishing attacks against clients of several banks in Serbia while the other warned about a phishing campaign that targeted an institute of public health by advertising the free distribution of "anti-COVID" protective gear.[5] The Serbian national CERT was made aware of the latter phishing campaign due to information shared by the Slovenian national CERT.

The Slovenian national CERT had previously become aware of several e-mails faking to come from governmental health authority representatives, and aiming to mislead the reader to register for free protective gear. A registration link in the emails contained malware that would damage the victims`computer and networks. After conducting an analysis of the technical information, the Slovenian CERT determined that not only Slovenia but also Serbia, Macedonia and Croatia had been affected by the same phishing attack. The analysis revealed an organised, regional cyberoperation. Following this determination, the Slovenian national CERT notified the national CERTs of all affected countries and shared information regarding the source and consequence of this phishing campaign.

The Slovenian and Serbian national CERTs cooperated particularly closely regarding adequate public warnings and information sharing in response to this phishing campaign. Members of both CERTs have called for similar co-operation across the region. Such cross-border cooperation gives hope that CERTs in the region would also communicate similarly in response to more serious cyber incidents in the future. The cooperation among national CERTs in the Western Balkan economies is, however, still at the very beginning stages, hence a more formalised platform for exchange is thus necessary. Further recommendations on this point will be provided in section 4.

3.2 Trainings and Educational Activities

Many of the national CERTs reported on training and educational activities being carried out in response to emerging COVID-related cyber threats. These trainings consisted mainly of: education aimed at young professionals in order to increase expertise in the region, and technical capacity-building training of CERT staff. Most of these activities were focused on the domestic context. At a meeting held in preparation for the drafting of this report, the Serbian CERT also described some of their continued international collaborations with academic institutions and cyber incident simulations with foreign military forces. Some of the educational activities were adapted to the particular context of this pandemic. The

[5] See notification 'Phishing campaign against clients of several banks in Serbia' (May 19, 2020) and 'Abuse of Institute of Public Health in phishing campaign' (June 1, 2020)
https://www.cert.rs/en/obavestenja.html#3.

Serbian national CERT, for example, offered a webinar on cyber security regulations for national healthcare providers.[6]

3.3 Co-operation and Information Sharing with Essential Service Providers

In a small survey conducted for the drafting of this report, national CERTs in the Western Balkans indicated that they largely did not increase co-operation or exchange of information with the healthcare sector since the outbreak of COVID-19. This might have had different reasons. Essential healthcare providers might not yet have been identified at national level. Where they have been identified, working relationships may not have been established with relevant healthcare related entities.

The establishment of strong working relations with essential service providers is important, but does not always come naturally. CERTs are required to actively reach out to essential health care providers and, over time, demonstrate the benefit to co-operate on cybersecurity capacity issues. Such efforts may need to be accompanied by legal reforms, including the adaptation of a framework similar to the European Union format of co-operation with essential service providers as set out in the Directive on Security of Network and Information Systems (the NIS Directive) of 2016.[7]

For one, the EU NIS Directive lists healthcare providers as operators of essential services. Essential service providers need to comply with specific security requirements and have obligations to report on cyber incidents. The concrete co-operation between CERTs and essential service providers is different in each EU member state and depends on the implementation of the Directive into national legislation. The legal framework might, however, help to clarify the responsibilities of national CERTs in response to cyber incidents. The Czech national CERT, for example, was mandated to conduct the investigation and forensics after a major cyber attack targeted a hospital, because the hospital had been identified as an essential service provider. This highlights the importance and need to immediately identify essential healthcare providers in the Western Balkan region

4. STRENGTHENING INTERNATIONAL COOPERATION

This report has provided background on the activities of national CERTs in the Western Balkans during the early months of COVID-19. The mandates of CERTs in the Western

[6] The Serbian Law on Information Security contains specific provisions for the healthcare sector and only came into force last year (November 2019); 'Webinar "From the Law on Information Security to standards"' Serbian National CERT (August 27, 2020) https://www.cert.rs/en/vest/544-Odr%C5%BEan+vebinar+%E2%80%9EOd+Zakona+o+informacionoj+bezbednosti+do+standarda%E2%80%9C.html.

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Balkans are frequently broadly defined and in order to fulfill their mandates effectively, national CERTs are required to co-operate at regional and international levels. The need and interest for more regional and international co-operation in the Western Balkan region was confirmed by several national CERTs during a regional meeting held in preparation for the drafting of this report. The following sections outline recommendations for potential measures and activities to improve such co-operation.

4.1 Creation of a Regional Governmental CERT Network

Based on the expressed desire of national CERTs in the region to strengthen their co-operation, it is recommended to create a platform for increased regional cooperation of governmental CERTs. Such a platform could support national CERTs in:

- sharing technical information;
- sharing experience and developing best practices for best response;
- conducting practically oriented research on how to improve cooperation with the private sector;
- supporting each other in more effectively co-operating, both internationally with other national CERTs and with cybersecurity researchers

The creation of a regional platform should not be a substantial financial burden however. The objective of such an institutionalised network would rather be to avoid the duplication of work carried out by individual CERTs in the region, by sharing critical information and helping regional cybersecurity grow stronger. Pooled information and efforts could for example be directed at regional awareness raising and public warnings against particular cyber threats.

4.2 Sharing Information and Increasing Capacity through Global Networks

There are several international networks and initiatives available to support the work and co-operation of national CERTs globally. Below are some examples of cybersecurity- and healthcare-sector specific networks that national CERTs and essential health care providers in the region could join:

FIRST – global Forum of Incident Response and Security Teams: FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. It frequently provides expert technical capacity building for member CERTs.

COVID-19 Cyber Coalition: A platform to share pandemic related cyber threat intelligence.

GFCE – Global Forum on Cyber Expertise: The GFCE strengthens international cooperation on cyber capacity building by connecting needs, resources and expertise and by making practical knowledge available to the global community.

Cyber 4 Healthcare: Initiative of the Cyber Peace Institute supporting targeted services for healthcare organisations fighting COVID-19 to find in one click trusted, free cybersecurity assistance by qualified and reputable companies.

Informal cyber drills and technical capacity building exercises, such as:

- FIRST Capture the Flag event
- ENISA's eHealth Security Conference 2020 Online Series
- Further collaborative training and capacity-building exercises with regional and

5. ADDITIONAL INFORMATION AND RESOURCES

Finally, the following collection of information might be useful for national CERTs and policymakers working on strengthening the capacities of national CERTs in the Western Balkans.

Information on Public-Private Co-operation

'Information Sharing and Analysis Centres (ISACs) – Cooperative models' (February 14, 2018) European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.

'Public Private Partnerships (PPP) - Cooperative models' (February 14, 2018) European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models.

'Procurement Guidelines for Cybersecurity in Hospitals – Good Practices for the Security of Healthcare services' (February 2020), European Agency for Cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

International Networks and Initiatives

FIRST Membership Application, https://www.first.org/members/application/.

CSIRTs Network – supported by the EU Agency for Cybersecurity (ENISA), https://csirtsnetwork.eu/.

Trusted Introducer Directory, https://www.trusted-introducer.org/directory/index.html

DCAF Geneva Centre for Security Sector Governance
20TH ANNIVERSARY

www.dcaf.ch

DCAF - Geneva Centre for Security
Sector Governance

Chemin Eugène-Rigot 2E
P.O. Box 1360
CH-1211 Geneva 1

@DCAF_Geneva