Cybersecurity Considerations in the Elections

Adrian-Viorel DRAGOMIR,
Anca MITU

Abstract: *Digital technology is changing people's lives, and the digitization strategy that is desired at the governmental level in the European Union aims to make this transformation work for people, public institutions, and companies. Information protection has become a significant challenge for many institutions. They want to make sure that no one can steal or compromise what data and information they have. One of the new pressing problems that must be solved when implementing modern technologies is the protection of information that is not intended for the general public. The complexity of this issue is increasing in the context of the application of personal data protection legislation. In order to respond effectively to the desire to constantly improve the electoral process, Electoral Management Bodies must take measures to improve administrative processes in the sense of simplifying, digitizing and professionalizing staff, which are the new trends in public administration management. The paper examines the most important reforms that electoral management bodies have to make, in line with the new models of the public sector and proposes a new vision on cyber security, to be adopted within them.*

Keywords: *Innovation; Digitalization; Security measures; ICT; Strategy; Information technology.*

Introduction

Since 2018, a number of initiatives have been launched at the level of electoral management institutions in the European Union to secure elections of the European Parliament at national level, following the recommendations of the European Commission for Democracy by Law of the Council of Europe ("the Venice Commission"). Working closely with the Electoral Management Bodies in its 61 Member States and dedicated its annual conference in 2018[1] to cyber security of the information systems that are used in the elections. The recommendations addressed a unified approach to the security of the elections, in particular by focusing attention on remote voting with a view to strengthening citizens' participation in voting, especially in the context of the coronavirus pandemic.

Bearing in mind that electoral processes throughout the country involve the use of IT tools at all stages dedicated to preparing, recording, counting and/or centralizing

results, it is necessary to raise the level of preparedness and security of these events so as not to jeopardize the integrity of the electoral processes as a whole.

The right of voters to participate in elections in a direct, free and secret universal suffrage means that they are not prevented from voting, that their votes are not falsified, the options are not disclosed prematurely, and the electoral process is not cheated by cyber-attacks or other information technology.

Cyber threats, sometimes combined with disinformation as well as other hybrid threats, can become a reality in electoral processes and thus need to be aware of and reflected in planning assumptions and risk management when designing and implementing IT systems that will provide operational support in elections.

As with any new solution, IT&C technology used in the electoral process must be introduced with caution, while ensuring that the digital solutions to be used meet the same legal requirements for elections as the other traditional non-digitized solutions, respectively, free, open elections, correct and based on secret ballot. While respecting these fundamental principles, technology can make a beneficial contribution to elections by complying with the general democratic rules set out in constitutional or electoral law.

CONTENT

Trust in the electoral process is fundamental to ensuring the legitimacy of the results and to ensure compliance with this principle, the electoral management authority must take the following measures[2] [2]:

- public oversight, together with entities responsible for ensuring and maintaining cyber security;
- observation of elections, including training of observers in electoral technology;
- publishing full documentation and allowing controlled access to the technology used in the elections, to demonstrate the truthfulness of results and increase the trust in the process;
- viewing and publishing the voter turnout and the results of the elections in a way that is accessible and understandable to the public;
- open communication of cyber security risks before and during elections;
- educating voters and building public trust in election technologies;
- involvement of key opinion leaders to present the benefits of technology in elections;
- improving relations with media representatives and educating journalists in the field election technologies;
- building trust among cyber security experts, raising awareness and involvement of experts in testing systems that are used in elections.

The occurrence of cyber-security incidents during the elections could

significantly disrupt the democratic process in general and lead to a loss of credibility of the democratic electoral system, of the electoral management bodies and of the parties participating in electoral campaigns. Major incidents or incidents that are most likely to happen may pose the following threats[3]:

- unauthorized access to the IT infrastructure or loss of legitimate access to it;
- manipulation or falsification of the registration process of voters or the members of election commissions for counting votes;
- modification or theft of data, including sensitive data that may change the results of the electoral process. In order to ensure the implementation of the principles set out above, detailed cyber security checks are needed to ensure the integrity of all the software components or devices used in the elections, including:
- check the firmware to be updated;
- management and traceability of changes in technical configuration;
- continuous and adequate monitoring of network traffic to provide a real-time analysis of security alerts generated by network applications and hardware;
- implement a comprehensive security information and event management (SIEM) solution to look for malicious activities using the logs provided by the hardware and software systems and send alarms to their administrators;
- ensuring strong protection against DDoS – denial of service attacks are an important part of all attacks against electoral technology, in terms of protection of platforms used to collect electoral information or publish results. Denial of service is usually achieved by loading the target machine or resource with unnecessary requests in an attempt to prevent certain legitimate demands from being met;
- access control – identification and control of users who have access to data or system and application privileges;
- strong authentication based on the following principles: something that the user knows (passwords), what the user owns (token, mobile applications, smart-cards) or something that the user is (biometrics);
- checking data integrity and securing data transfer – data transfers are potential trade-offs, control amounts and digital signatures being useful tools to ensure data integrity;
- ensuring the segmentation of the network used for computer systems supporting electoral processes, by logical separation (VLAN) or by physical separation, which will ensure that processes that do not have to be accessible to the public, in particular centralization and counting of votes, can take place in an environment physically isolated from other public trials;
- ensuring back-up and recovery tools and procedures of the data from central systems that must be

installed in secure locations where physical access will be verified and restricted;
- ensuring an alternative location that allows data recovery and business continuity in the event of disruptions of any kind, with equipment suitable for this activity pre-reserved and ready for use at any time and complying with the same standards and requirements as the initial system;
- duplication of secured communication channels.

In order to be prepared to prevent cyber security crises, the EMBs should call for the creation, at governmental level, of working groups with expertise in cybersecurity, on the one hand, and in electoral technologies, on the other hand, with the purpose to draw up instructions and methods for preparing and protecting the computer systems to be used in elections and to ensuring interinstitutional cooperation in this field throughout the election period.

This working groups should have a 24/7 format support program during election periods, and the main tasks include coordinating cyber defense and managing crisis events. The working groups should be composed of technical staff with knowledge, certification and duties in technologies and equipment's cybersecurity protection at the level of electoral management bodies, institutions involved in protecting cybersecurity, and the national governmental teams acting as computer security incident response team (CSIRT), at state level[4].

The main roles to be given to the working groups are the testing and auditing of information systems and communication networks supporting electoral processes, which are considered as the cornerstones of cyber security and the only means of ensuring functionality and security. Therefore, testing and auditing should be adopted as comprehensive multi-faceted approaches, with critical systems to be tested for penetration by at least two independent teams and the connections between applications to be deep analyzed.

During election periods, working groups will have to carry out functional tests and loading IT systems tests, which should focus on the system's responses, in the sense of giving the expected and correct response to the data processing.

System security tests must be carried out, which will focus on ensuring that information systems cannot be compromised by changing their parameters that will make them act in undesirable or altered ways. The problem with these functional tests is that there is often an endless list of scenarios and circumstances to test to see if the system is performing in a faulty way, limiting their effectiveness.

Another set of tests that workgroups need to perform are vulnerability scans, which are specific and simplified forms of security testing for known cyber vulnerabilities, which are globally documented by all

companies and entities working in the field of cyber security.

Vulnerability scans are made with software developed specifically for such activities that have in place universally recognized vulnerability libraries that all these companies keep up-to-date. These tests are generally useful for testing the security of communication, processing and data storage infrastructures.

It is impetuous to do penetration tests combined with other types of security tests and audits at the level of the organization. This is one of the final security tests, which are done with experienced testers, allowed to try to attack the information and network systems used in electoral processes, by any means necessary, to demonstrate how safe they are.

In these extensive and creative tests, testers are trying to imitate real attackers using multiple combinations and attack methods. These tests can be very useful to reveal the weaknesses of the system in its entirety, in terms of system organization, system configuration, network connections and ancillary systems, on the one hand, and training of the institution's officials in the field of social engineering and false news, on the other. The tests results depend on the creativity and abilities of the testers, and their final reports can propose solutions to improve the cybersecurity system by reducing the number of vulnerabilities, especially those known.

In setting up the working groups, the following principles shall be taken into account, documented and disseminated to all actors involved in the conduct of the activities, through documents and procedures[5] [5]:

- provide a single point of contact at national level where it is possible to report cyber security incidents and which be able to mitigate, respond and deal with an attack quickly;
- create of a scale of crisis escalation that can detail the type and critic level of an attack;
- creating a clear division of roles and responsibilities;
- creating secure means of communication;
- ensuring full documentation of the systems that are used as support for electoral processes;
- ensuring the flexible allocation of resources, both financial and human;
- an adequate training plan for all members of the groups.

Conclusions

In this complicated geo-political context, security challenges have changed in all direction, now presenting quite different aspects compared to a few years ago. So, cyber security in elections must be addressed with responsibility and caution, and a lot of work needs to be done to keep this area up-to-date and to improve it on a continuous basis.

Thus, in order to better understand and implement this concept and effectively defend against this scourge, long-standing partnerships must be signed with all the states institutions

and private that act as operational centers to respond to cyber security incidents in order to monitor in real time, analyze the impact, respond promptly to cyber security incidents and verify the security level of the products or information systems to be used in elections.

A very important aspect to consider is the training of the staff that is responsible for cybersecurity. Information is necessary to ensure the security of information systems and to be know the last methods of attack, officials should regularly participate in cyber security technology training, product or service presentations, colloquia and cyber-attack and defense simulations. Only in this way the employees that are responsible with security will be informed in this highly dynamic area and will be aware of the real threats posed by cyber terrorism to the electoral field.

Notes

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.151.01.0015.01.ENG&toc=OJ%3AL%3A2019%3A151%3ATOC, website consulted on 11.03.2021.

[2] Whitman, M. E., & Mattord, H. J. (2019), Management of Information Security (6 ed.). Boston, Maryland, United States of America: Cengage Learning, pp. 4-8.

[3] Briony, J.O. (2003), *The potential contribution of ICT`s to political process. Electronic Journal of e-Government, vol. 1*, no. 1, pp. 33-42.

[4] 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, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO, website consulted on 02.03.2021.

[5] European Council conclusions on cyber activities in 2018, https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/ro/pdf, website consulted on 20.02.2021.

Bibliography

WHITMAN, M. E., & MATTORD, H. J. (2019), *Management of Information Security* (6 ed.). Boston, Maryland, United States of America: Cengage Learning, 2019, pp. 4-8.

BRIONY, J.O. (2003), „The potential contribution of ICT`s to political process", *Electronic Journal of e-Government*, vol. 1, no. 1, 2003, pp. 33-42.

Electronic Resources

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA

(the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.151.01.0015.01.ENG&toc=OJ%3AL%3A2019%3A151%3ATOC, website consulted on 11.03.2021.

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, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO, website consulted on 02.03.2021;.

European Council conclusions on cyber activities in 2018, https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/ro/pdf, website consulted on 20.02.2021;