ОБМЕН НА ИНФОРМАЦИЯ ЗА КИБЕРИГУРНОСТТА ЧРЕЗ ПУБЛИЧНО-ЧАСТНО ПАРТНЬОРСТВО

EXCHANGING THE CYBERSECURITY INFORMATION THROUGH PUBLIC AND PRIVATE PARTNERSHIP

Todor Todorov[1, 2]
[1]*Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, Veliko Tarnovo, Bulgaria*
[2]*Institute of Mathematics and Informatics, BAS, Sofia, Bulgaria*
t.todorov@ts.uni-vt.bg

Shpend Lutfiu[1]
[1]*Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, Veliko Tarnovo, Bulgaria*
shpendlutfiu@gmail.com

Abstract

Cyber security threats nowadays pose a challenge to the overall national security of many states. As cybersecurity is considered a shared responsibility between government, network and essential service operators, businesses and end users, coordinating and regulating the sharing of responsibilities and sharing of information will have a positive impact on cyberspace conservation and mitigation of risk. In this paper will be issued considerations related to models, methods and mechanisms of coordination and exchange of information. Such considerations can then serve as a guide in drafting formal frameworks applicable especially to developing countries where the definition of management and sharing of responsibilities related to cyber security issues has already begun.

Keywords: cyber security, information sharing, threats prevention, partnership

INTRODUCTION

Building an information society requires strengthening trust in information and communication technologies (ICT), requires that personal data and privacy be protected and promotes a global culture of cyber security in a context where societies around the world are increasingly dependent by information and communication technologies and as a result may be the target of cybercrime [7], [8].

Governments within a state cannot secure cyberspace alone because they do not own and operate public electronic communications infrastructure. Public networks and services located within the national cyber domain are in most cases not under the control of Governments and this highlights the need for public-private cooperation in the exchange of information and early detection of cyber threats.

National Cyber Security Strategies developed by Governments should involve and consult the private sector in the development, implementation of regulations, initiatives and policies in the field of cyber security [4].

Close and proper public-private cooperation is vital as it:

- Facilitates the exchange of information on the development of legislation and new regulation between stakeholders;
- Provide collaborative work and exchange of training courses that can help alleviate the pronounced shortage of skilled cybersecurity professionals;
- Enable real-time exchange of information about threats and vulnerabilities online. The communication channel is valuable to CERT Nacional as the exchange complements the extended national sources of threat detection and warning;

Coordination of public-private partnerships is essential for the protection of critical infrastructure because it enhances the exchange of information and cooperation in identifying online threats, responding to incidents and taking measures to remedy the situation.

By exchanging information between organizations, an understanding of technical methods and attack methods can be achieved. The Exchange of Tactics, Techniques and Procedures (TTP) allows organizations to force attackers to work harder on each target.

COOPERATION AND EXCHANGE OF INFORMATION

The failure of the cooperation of the public sector and the private sector in the exchange of cyber security information will be formulated according to the following hypotheses [1]:

- Participation in public-private cooperation does not occur if the parties are reluctant to share information about cyber threats in a proper and accurate manner;
- The private sector based on the obligation to meet the required security standards, is reluctant to invest in security standards if initially there is no financial incentive from the Government;
- The private sector in general lacks the necessary resources to participate in public-private cooperation in the exchange of information;

To create sustainable cooperation policies in the exchange of information we must focus on the following objectives:

- To participate in public-private cooperation, the participating parties must first be identified which have the capacity to deal with cyber security threats and incidents;
- Promote and increase trust between the parties;
- Models of cooperation and exchange between the parties regulated by relevant procedures;
- Define the types of information to be exchanged based on a well-defined taxonomy for the classification of incidents, threats and vulnerabilities including the purpose and handling of information by the parties;
- Technical mechanisms of exchange through platforms for exchange of information;

Parties and their role

The parties involved in public-private partnerships as well as in the exchange of information regarding cyber security threats and incidents as well as other information, have different

interests and needs and should each be addressed from their own perspective when regulating this cooperation. Technical capabilities, types of cyber incidents and threats may also vary. Understanding the value of each party as well as increasing trust by identifying the criteria for participation between the parties is crucial. The following figure presents the parties and their role in public-private cooperation:

Types of information

There are in general seven types of information that can be shared within cybersecurity communities. Each type of information has different uses. Some of this information assists government and the private sector in assessing cyber security risk at the national level or at the level of other parties involved in public-private partnerships including critical infrastructure risk.

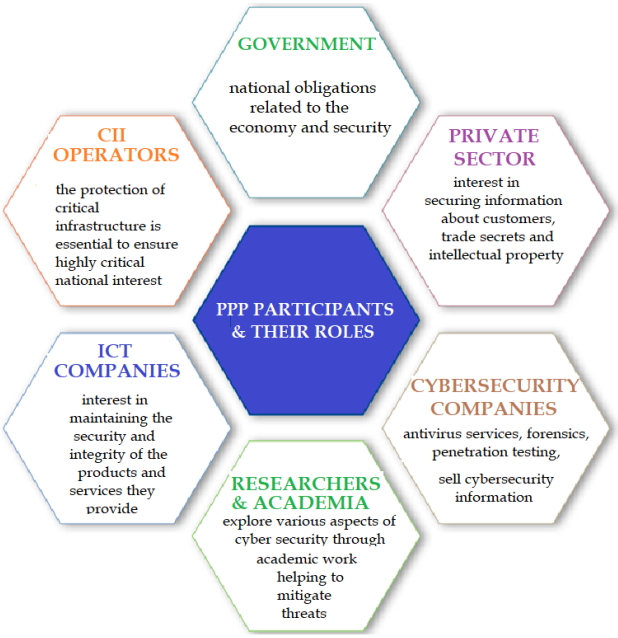

Fig. 1. Parties and their role in public-private cooperation

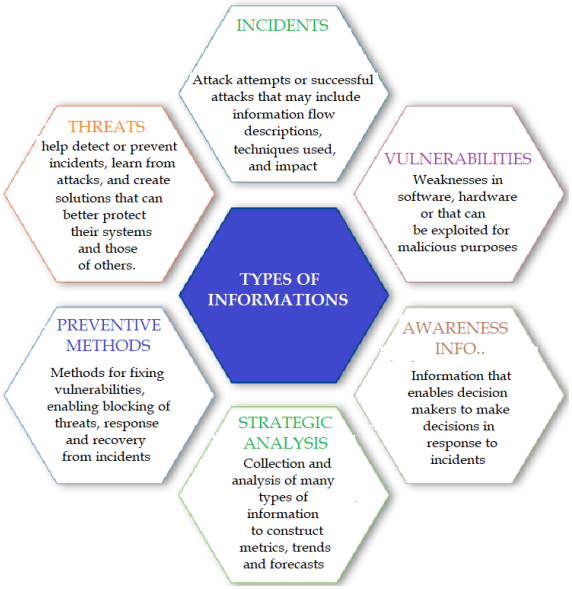

Fig. 2. Types of information for exchange between the parties

MODELS OF COOPERATION

The different approaches of the models for the exchange of information are mainly based on the trust between the parties, the legal framework according to which the different actors operate and the cooperative relations between the parties. These models range from sporadically ad-hoc information exchange to long-term exchange regulated through legally binding formal agreements. Each of the models has its advantages and disadvantages, but choosing the right model is vital in ensuring success in preventing risks and taking appropriate action in responding to cyber security incidents [2], [3], [5].

Voluntary exchange of information

Voluntary exchange of information is probably the most valuable exchange that exists in the cyber security space. By voluntarily sharing information, the parties identify a need or a reason to exchange information, whereby they share and use that information that is valuable and meaningful for taking appropriate action. Governments and companies often decide with whom to share information based on the type of information and the objectives of the parties.

Governments need for national security gives it a clear mandate to share important information with industry, especially information related to threats and vulnerabilities.

Similarly, voluntary efforts in the private sector may be bilateral or may involve a group of entities. Private sector entities often share information on incidents, threats, vulnerabilities, and mitigation among other things:

- Contribute to a national collective defense or response
- Protect customers, their brand and products
- Inform the authorities of serious situations
- Report criminal activity

In some cases, a private sector company will voluntarily share information with both industry and government.

The most effective scenarios for information exchange appear to be private company-to-company exchanges, in addition to collective responses to major incidents or threats.

Thus, as governments they seek to develop more effective information-sharing regimes or incident reporting obligations should consider how to deepen trust, provide a collective benefit by minimizing reputational risk, and respond to a clearly articulated national incident .

Finally, it is also worth noting that some information on cyber security is exchanged through trade sales by security companies and researchers. Due to an increase in information about threats, incidents and vulnerabilities, a significant market has emerged to meet the demand for better security. Private incident and forensic response firms have recently become important as responders to their breaches and as network monitors, acting from the owner information they collect and from information shared by third parties. However, certain information purchased may be used outside of its intended purpose (for example, to exploit the systems), so it is important that any such information be protected.

Forced exchange and disclosure of information

Governments are increasingly demanding the exchange of information on security events based on public-private partnerships between parties with responsibilities in the field of cyber security. Although disclosure regulations are currently limited in most countries, there is an ongoing push that requires incident reporting, especially when the incident affects critical infrastructure.

Based on the NIS Directive adopted by the European Commission, an additional requirement has been defined for market operators to report incidents that have a serious impact on state authorities.

There is a concern that a mandatory approach to incident reporting will divert attention from the most important focus on information sharing or incident response. It is crucial that governments do not combine incident reporting or their need to raise awareness of the situation with the exchange of information between trusted parties.

Moreover, suggestions about the transition from voluntary sharing of information to required sharing information have generally been reluctantly received by the private sector. Mandatory incident reporting is essentially a manager and does not in itself improve operational safety or its response. Often, the focus is on the reporting itself and not on how the information collected will be used, calling calls into question the basic purposes of mandatory reporting. It is critical that mandatory incident reporting be clearly focused and closely aligned to ensure that reported data is used to improve security and that privacy is protected.

INFORMATION EXCHANGE PROTOCOL - TRAFFIC LIGHT PROTOCOL (TLP)

Traffic Light Protocol (TLP) was created to promote the best exchange of sensitive (but unclassified) information in the field of cyber security [6]. The sender of this information should indicate where the information may flow beyond the immediate recipient and this should consult with the original sender when the information is to be disseminated to third parties.

A four-color code is used, the meaning of which can be found in the following table:

TLP categories	
TLP-RED	"For your eyes only". Only to be used by you and not to be spread to other people, even within your own organisation.
TLP-AMBER	To be used and shared with co-workers within your organisation on a need-to-know basis and with clients or customers who need to know this information to protect themselves or prevent further damage.
TLP-GREEN	Used for information that is not very sensitive and can be shared with partners and peers, but not via publicly accessible channels (e.g. websites).
TLP-WHITE	Public information that can be shared freely, taking into account standard copyright rules.

The author should check the information with the right color to indicate the purpose TLP is disseminating such information, usually including the text "TLP: COLOR" at the top and bottom of the document, using the colors in the table above.

If the recipient is to distribute that information to third parties beyond the scope of the specified TLP, it must refer to the source of the information.

TLP is a simple and intuitive scheme to show when and how sensitive cyber security information will be shared, and facilitates collaboration with other entities or organizations at the national and international levels.

The definition of TLP is not a category or subcategory of these standards and should only be used operationally.

TLP is used by public and private organizations in the field of cyber security in most of the countries.

For more information about the TLP standard, please visit www.first.org/tlp

CONCLUSIONS

Reducing cyber security risk increasingly depends on information exchange and cooperation between the parties, utilizing many different models, methods and mechanisms. Establishing effective mechanisms and procedures for information sharing is a complex and difficult process that requires commitment, trust and close cooperation between the parties involved in the public-private partnership.

The experiencees, technology and procedures of the parties involved in the public-private partnership differ based on the activities and responsibilities they have, hence the threats they face may be different, so such cooperation will enable the sharing of practices and experiences with good especially with the public sector where in most cases this sector faces a lack of professional resources.

REFERENCES

[1] Johnson, T., Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, Routledge, 2015.
[2] MISP-User Guide Threat Sharing Platform, https://www.circl.lu/doc/misp/book.pdf
[3] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, CreateSpace Independent Publishing Platform. 2014.
[4] NIS DIRECTIVE, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=GA
[5] Public Private Partnership – Cooperative Models, https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport
[6] Traffic light protocol (TLP), https://www.first.org/tlp/
[7] https://www.securitysales.com/emerging-tech/cybersecurity-tech/cybersecurity-approach-proactive/
[8] https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#712004755218