COMPUTERS & SECURITY 60 (2016) 154–176

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing

Florian Skopik *, *Giuseppe Settanni*, *Roman Fiedler*

Digital Safety and Security Department, Austrian Institute of Technology, Donau-City-Straße 1, 1220 Vienna, Austria

ARTICLE INFO

Article history:
Received 3 December 2014
Received in revised form 15 March 2016
Accepted 7 April 2016
Available online 13 April 2016

Keywords:
Survey
Cyber security
Information sharing
Cyber incident reporting
Organizational aspects
Standardization

ABSTRACT

The Internet threat landscape is fundamentally changing. A major shift away from hobby hacking toward well-organized cyber crime can be observed. These attacks are typically carried out for commercial reasons in a sophisticated and targeted manner, and specifically in a way to circumvent common security measures. Additionally, networks have grown to a scale and complexity, and have reached a degree of interconnectedness, that their protection can often only be guaranteed and financed as shared efforts. Consequently, new paradigms are required for detecting contemporary attacks and mitigating their effects. Today, many attack detection tasks are performed within individual organizations, and there is little cross-organizational information sharing. However, information sharing is a crucial step to acquiring a thorough understanding of large-scale cyber-attack situations, and is therefore seen as one of the key concepts to protect future networks. Discovering covert cyber attacks and new malware, issuing early warnings, advice about how to secure networks, and selectively distribute threat intelligence data are just some of the many use cases. In this survey article we provide a structured overview about the dimensions of cyber security information sharing. First, we motivate the need in more detail and work out the requirements for an information sharing system. Second, we highlight legal aspects and efforts from standardization bodies such as ISO and the National Institute of Standards and Technology (NIST). Third, we survey implementations in terms of both organizational and technological matters. In this regard, we study the structures of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), and evaluate what we could learn from them in terms of applied processes, available protocols and implemented tools. We conclude with a critical review of the state of the art and highlight important considerations when building effective security information sharing platforms for the future.

1. Introduction

The smooth operation of critical infrastructures, such as telecommunications or electricity supply, is essential for our society. In recent years, however, operators of critical infrastructures have increasingly struggled with cyber security problems (Langner, 2011). Through the use of standard Information and Communications Technology (ICT) products and increasing network interdependencies (Rinaldi, 2004), the surfaces and channels of attacks have increased significantly. New approaches are required to tackle this serious security situation.

* *Corresponding author.*
E-mail address: florian.skopik@ait.ac.at (F. Skopik).
http://dx.doi.org/10.1016/j.cose.2016.04.003

One promising approach is the exchange of network monitoring data and status information (Hernandez-Ardieta et al., 2013) of critical services across organizational boundaries with strategic partners and national authorities. The main goal is to create an extensive situational awareness picture about potential threats and ongoing incidents, which is a prerequisite for effective preparation and assistance in large-scale incidents. Collaboration based on threat information sharing is believed to be effective in a multitude of cyber security scenarios including financially driven cyber crimes, cyber war, hacktivism, and terrorism (see Denise and James, 2015 and Dacey, 2003). The attack morphology can be different depending on the scenario, e.g., cyber crime might use stealthy advanced persistent threats (APTs) to steal intellectual property, while cyber war or terrorism uses botnets to run DDoS attacks. However, information sharing enables the victims to run coordinated and effective countermeasures, and provides preventive support to potential future targets on how to effectively protect their ICT infrastructures (see NIST, 2014b).

We argue that since attacks are becoming increasingly sophisticated, customized and coordinated, we also need to employ targeted and coordinated countermeasures. Typical commercial-off-the-shelf (COTS) virus scanner and firewall systems appear incapable of sufficiently protecting against APTs (Tankard, 2011). The rapidly growing complexity of today's networks, emergence of zero day exploit markets (Miller, 2007), and often underestimated vulnerabilities, e.g., due to outdated software or policies, lead to novel forms of attacks appearing daily. Thus, numerous information security platforms and knowledge bases have emerged on the Web. From there, people can retrieve valuable information about identified threats, new malware and spreading viruses, along with information about how to protect their infrastructure (e.g., see national Computer Emergence Response Teams).[1] However, this information is usually quite generic, not shaped to particular industries and often lacks in-depth knowledge.

In order to make such platforms more effective, sector-specific views along with rich information and experience reports are required to provide an added value to professional users. Many standardization bodies, including NIST (2014a), ITU-T (2012) and ISO (2012), have proposed the establishment of centrally coordinated national cyber security centers, which are currently emerging all over the world.

However, effective cyber security centers are hard to establish and often neither governmental bodies nor companies and customer organizations are well prepared to run and use them. The challenges are grounded in the fact that cyber security information sharing requires a great deal of multi-disciplinary research. Although the setup of such systems is often reduced to addressing technical aspects, it is a similarly significant challenge for legal experts, standardization committees and social as well as economic scientists. For example, questions dealing with the sharing process design, i.e., who is allowed to share what and when in a corporate environment, legal dependencies and regulatory compliance, as well as what can we learn from existing implementations of CERTs, are of equal importance.

[1] http://www.cert.org; April 2016.

Moreover, while there are many works that deal with information sharing among CERTs, such as ENISA (2011a) and ENISA (2013a), there is little experience so far with peer-to-peer sharing of such information among companies. This is for numerous reservations (ENISA, 2010), such as low quality information, reputational risks, and poor management. Raising awareness of these issues and providing an overview of potential solutions are two of the goals of this paper.

It is therefore critical to take a closer look into all of these aspects in a structured form – from the economic motivation (and requirements) on information sharing, over legal and regulatory aspects, to structural and technological matters. Therefore, the contributions of this survey article are as follows:

- *Holistic Picture of Cyber Security Information Sharing*. We shed light on the numerous economic, legal, and regulatory aspects that, besides the technical dimensions, are often neglected.
- *Survey on existing Methods, Technologies, Protocols and Tools*. We survey existing approaches and solutions as a prerequisite to identify open gaps.
- *Evaluation of the State-of-the-Art and Key Findings for Future Systems*. We critically evaluate the current situation and emphasize likely future developments regarding standards, norms and technologies.

The remainder of this paper is structured as follows: Section 2 provides an overview of related work. Since this is a survey paper, we mainly refer to other survey papers here, and omit works that is cited in the the other sections. Section 3 is about the various dimensions that need to be considered when it comes to cyber security information sharing. For that purpose, we group all relevant aspects into five distinct categories. After that, relevant regulations, standards, concepts, supporting tools, and protocols that are essential for setting up effective information sharing procedures are discussed. In particular, Section 4 outlines cooperation and coordination aspects and presents some sample sharing scenarios. Section 5 reviews existing regulatory directives and legal recommendations. Subsequently, Section 6 refers to well-recognized standards in this area, while Section 7 covers concrete implementations in terms of organizational structures. Section 8 deals with technologies, tools and applicable protocols. After this survey, we critically review the applicability of existing solutions in a large-scale national security information sharing network (as set up in the context of a number of projects together with national stakeholders) in Section 9. Finally, Section 10 concludes the paper.

2. Related work

Cyber-attacks are becoming increasingly sophisticated, targeted and coordinated, resulting in so-called advanced persistent threats (Farwell and Rohozinski, 2011; Tankard, 2011). Consequently, new paradigms are required for detecting and mitigating these kinds of attack (Virvilis and Gritzalis, 2013), and eventually to establish situational awareness (Jajodia et al., 2010; Sarter and Woods, 1991; Tadda et al., 2006). Many of these tasks are currently performed within individual