Running a Global Community for Security Teams

Thomas Schreck
FIRST.org

December 16, 2018

Abstract

The Forum of Incident Response and Security Teams (FIRST) is a global community existing of 450 security teams in 90 countries with the aim to connect security teams. Those teams cooperatively handle computer security incidents and promote incident prevention programs. In the last 30 years, we gained a lot of experience in how to run a global community which needed to adapt to the changing environment of Internet threats and how to respond. However, we still face a lot of challenges and this position paper outlines the challenges we see and what we are doing to improve the situation.

1 Our Challenges

While working with different security teams from various regions in the world, we observed that they have similar challenges. In the last years, FIRST tried to describe those challenges and speak about them openly at various events and stakeholder groups. From those challenges, we describe two of them in this section, one is the problem of how the various groups, like Computer Security Incident Response Teams (CSIRT), Product Security Incident Response Teams (PSIRT), security researchers, etc., can find the right contact. The other is the increasing demand that it is necessary that security teams need to learn, to speak the same language.

1.1 Whom to contact?

The problem of identifying the right contact addressing a security issue, like a compromised system or a vulnerability within a product, was always challenging for the different stakeholders. However, with changing environments, like outsourcing or cloud computing, this problem becomes even more problematic. Also, with the new GPDR legislation and the consequential limitation with the WHOIS system, had a impact to most CSIRTs. Researchers [5] have shown that the notification of vulnerabilities are error-prone and in most cases either the security team have not responded or they were not able to identify a contact.

However, in large scale attacks, like with Wannacry [4] or the Mirai botnet attacks[1], it is necessary that security teams can be contacted in an automated way and that the data about it is accurate all the time. Without such information a global successful coordinated response to attacks is complicated when not even impossible.

1.2 Speaking the same language

In their daily business security teams are faced with different communication channels, like management briefings, talking to the technical team within the constituency, or external teams and researchers. When communicating it is keen, that the understanding of the different terms are important. On top of that it must be guaranteed that information is treated according to the rules the source of the information classified it. Therefore it is necessary that security teams agree on a standard how to exchange information and how to classify it.

Lastly with the enormous numbers of incidents a team is confronted on a daily basis, it is necessary that standard tasks are automated. In order to achieve this automation, global standards are required which enables security teams to exchange data, like incidents, abuse, or even intelligence.

2 Our Approaches

The last years, FIRST started various programs to improve the situation, we described above. This section will provide an overview of some of our recent program we are working on: (1) tackling the problem with a database for security teams, we built on top of our public member data an API, (2) we

are working within our Special Interests Groups on various standards, and (3) our education program.

2.1 Building a Global Database of Security Teams

FIRST is maintaining a database about security teams for many years, which includes a public and a private part. The goal is that our members but also others are able to access information to contact a team. Our only interface to this member database was a website, where you are able to search for the team, based on IP addresses, domains, etc. In 2016 we have seen the problem that others wanted to automate parts of their incident communication. Therefore we created an interface based on a REST-API and created a JSON-Scheme to allow the automation. The interface is accessible through `https://api.first.org`.

2.2 Define Global Standards

Another challenge in our community is that we need to use common standards to exchange information. Therefore we are maintaining some standards, including the following:

Common Vulnerability Scoring System provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.

Traffic Light Protocol is set of designations used to ensure that sensitive information is shared with the appropriate audience.

Information Exchange Policy is a standard describing a policy for the exchange of sensitive information.

2.3 Education

Early on we identified the need for capacity building in our area of expertise. Therefore we started a education initiative, which included next to creating training materials, also the creation of a service framework. In this initiative we have created a service framework for CSIRTs [2] and PSIRTs [3] which are adapted by various groups.

We also created various trainings, using experts from the community. The training various from basic courses, to ramp up new teams, to specific topics like, how to use CVSS. Next to delivering the training in person around the world, we also created an online-platform so that we can reach more people.

References

[1] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the mirai botnet. In *Usenix Security*. Usenix, 2017.

[2] FIRST. FIRST CSIRT Framework Version 1.1. `https://first.org/education/csirt_service-framework_v1.1`, 2017.

[3] FIRST. FIRST PSIRT Framework Version 1.0. `https://first.org/education/FIRST_PSIRT_Service_Framework_v1.0`, 2018.

[4] Emi Kalita. *WannaCry Ransomware Attack: Protect Yourself from WannaCry Ransomware Cyber Risk and Cyber War*. Independently published, 2017.

[5] Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes. Hey, you have a problem: On the feasability of large-scale web vulnerability notification. In *25th USENIX Security Symposium*, 2016.