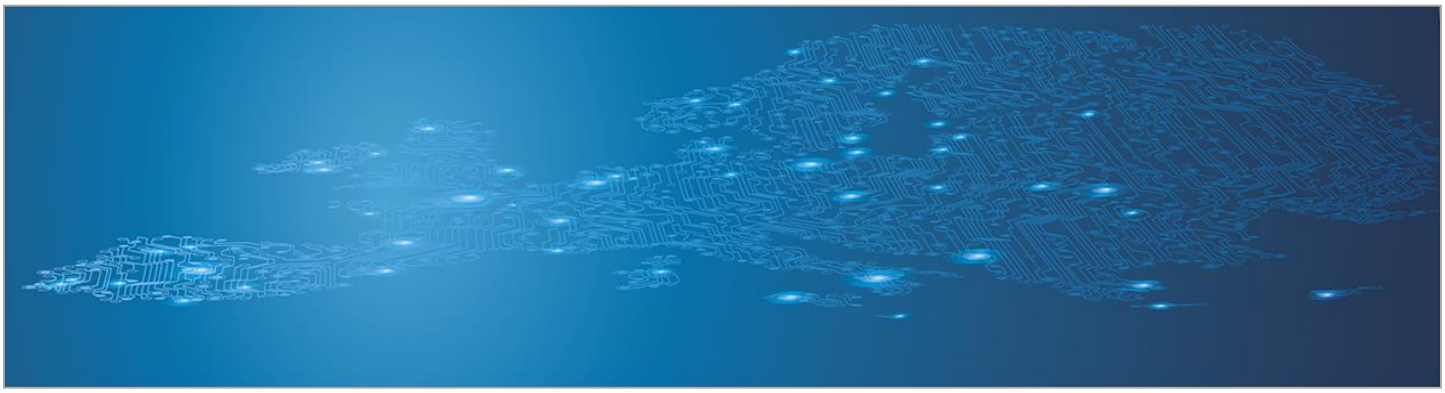

Scalable and Accepted Methods for Trust Building in Operational Communities

Version 1.0

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Lionel Ferette

Contact

For contacting the authors please use cert-relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The author would like to thank the experts who provided the information that fed this report, and the thriving communities that are its subject. The author gratefully acknowledges the continuous support and valuable feedback from Jo De Muynck, Andrea Dufkova, and Marco Thorbruegge (ENISA).

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-113-7, doi 10.2824/320219

Executive summary

One of ENISA's role is that of community builder. In order to properly fulfill this role, ENISA must have a better insight at what makes or breaks a community – trust. This report takes a first informal look at how communities build and maintain trust, by looking at four different operational communities. We highlight commonalities and differences, and give a first set of recommendations to enhance trust in a community.

Table of Contents

Executive summary iii

1 Introduction 1

2 Defining Trust 1

3 A look at operational communities 1

3.1 FIRST 1
3.1.1 Membership Process 1
3.1.2 Activities 2

3.2 TF-CSIRT/Trusted Introducer 2
3.2.1 Membership Process 2
3.2.2 Activities 3

3.3 NSP-Security 3

3.4 EU FI-ISAC 3

4 Discussion 4

4.1 FIRST 4

4.2 TF-CSIRT 4

4.3 NSP-Security 4

4.4 EU FI-ISAC 4

5 Conclusions 5

6 References 5

1 Introduction

As shown in previous ENISA reports [1] [2] [3], trust is a cornerstone for cooperation between CERTs [1] and it is instrumental for valuable information sharing among operational communities in general. As such, participation in trust building activities is one of ENISA's recurrent recommendations [2]. This document takes an informal look at existing operational communities that single out trust building as being one of their goals. Its purpose is to get preliminary insight before going into further details in the scope of a future Work Programme.

The communities we look at are not only CERT-related, as the problem of trust building goes beyond the world of CERTs and can be applied to any community made either of individuals or teams that need to collaborate occasionally.

2 Defining Trust

Trust can be defined in terms of a set of expectations [3]. Previous work by ENISA [4] shows that CERTs that meet the following expectations are more likely to be trusted by other CERTs:

- Technical expertise
- Active membership in CERT initiatives
- Ability to respond quickly and act on security threats
- Stability of the team
- Maturity level of the team

In other words, a trusted CERT is mature team that acts on shared information and shares back.

It should be noted that even with this kind of definition, trust is established gradually: first, people trust people, then people trust teams, and finally teams trust teams.

3 A look at operational communities

3.1 FIRST

The Forum of Incident Response and Security Teams (FIRST[1]) was founded in 1990 as a worldwide network of individual computer security incident response teams that cooperate voluntarily to improve their abilities to deal with and prevent computer security problems. FIRST is a membership organisation that is governed by an operational framework, and each member must designate a primary and alternate representative to FIRST. Participants in FIRST are part of a network of teams that voluntarily work together in order to deal with response to computer security problems and their prevention.

FIRST's approach to trust is twofold:

1. Control the entrance of new members
2. Provide activities that foster trust

3.1.1 Membership Process

FIRST members are mostly teams, though individuals can apply. Teams willing to become members need to provide basic information about how to contact them and their policies. New candidates must also have two existing teams supporting their membership ("sponsors"). Usually, a representative of one of the sponsors performs a site visit to meet the new team and their management, and assess its

[1] http://www.first.org/

level of maturity – funding, security policies and other operational factors. The visiting sponsor then reports to the membership committee that decides on new memberships.

It should be noted that membership is for life. Once a team has been admitted, there is no re-evaluation (this makes the FIRST model different from the TF-CSIRT/TI model for example).

3.1.2 Activities

FIRST provides activities and structure for information sharing:

- Mailing lists for discussion: in principle, these lists can be used to discuss any subject with the whole community. However, given the large number of participants and the uncertainty of who will receive the mails, these lists are seldom used for sensitive information.
- Workshops (Technical Colloquium, Special Interest Groups, Symposium, etc.): these activities gather members in small to medium groups that have similar interests or are geographically close, and are focused on technical issues. One or several team representatives present their projects, or ask for feedback, or train others. It is at this level that most trust is established, as groups are small and closed enough to foster the sharing of information.
- Conference: the annual conference gathers representatives of teams from all over the world, but membership is not a requirement to register. The information shared in sessions is thus seldom of sensitive nature, but the numerous side activities leave room for personal contact.

3.2 TF-CSIRT/Trusted Introducer

TF-CSIRT[2] provides a forum where members of the CSIRT community can exchange experiences and knowledge in a trusted environment in order to improve cooperation and coordination. It maintains a system for registering and accrediting CSIRTs, as well as certifying service standards.

TF-CSIRT's approach to trust is similar to that of FIRST, but goes a bit further:

1. Control the entrance of new members
2. Provide activities that foster trust
3. Provide an additional maturity level

3.2.1 Membership Process

As with FIRST, members are mostly teams. Individuals are only admitted by invitation of the community. The cornerstone of TF-CSIRT membership is the "Trusted Introducer"[3]. This service serves as a neutral and trusted third party that introduces new teams to the community. The first step for a team to join the community is to acquire "Listed" status with Trusted Introducer. This requires two sponsors (already accredited teams) that can testify that the candidate team is a CERT in good standing, and very basic contact information. Full membership additionally requires full contact information, as well as summaries of key policies like the Information Sharing policy. By and large, the information gathered is closely mapped to RFC2350 [5], augmented by statements regarding the team's support for a number of good practices.

Certification is the next level of maturity for member teams. By getting certified, a team demonstrates that it meets certain criteria as evaluated by a neutral third party.

[2] http://www.terena.org/activities/tf-csirt/

[3] http://www.trusted-introducer.org/

The biggest difference with FIRST is that all levels of participation must be regularly confirmed in order to maintain the privileges that are associated with them:

- Listed teams need to confirm their contact information once a year,
- Full Members need to update the whole of their information every four months, and
- Certification is only valid for three years, after which the whole certification process must be renewed.

3.2.2 Activities

The activities are similar to FIRST, so we will focus on the differences that can have an influence on trust:

- Closed meetings. The closed meetings are reserved for full members, and the focus is on sharing information that is not public.
- Use of the Traffic Light Protocol. Use of the TLP is institutionalised during meetings, and teams are encouraged to share Amber and Red level information during the closed meeting.
- Encrypted mailing lists. There are mailing lists that encrypt any message for each recipient individually. This allows to share more sensitive information. They are not often used, though.
- Out of Band Alerting System. Teams can use an alerting system that reaches all other teams through text messages in case of major emergencies.

3.3 NSP-Security

NSP-Security[4] is a low profile community of volunteer incident responders. It revolves around a mailing-list, and individuals willing to participate must satisfy a number of requirements:

1. Work for a corporation that is in position to actively handle incidents (ISP, vendor …), and use a corporate email address.
2. Action is mandatory, contribution is encouraged. All members are encouraged to share information on the mailing list, and acknowledge actions. Those prevented by laws or policies from doing so are required to take action whenever it is in their purview.
3. Reposting information outside the mailing list is forbidden.

It should be noted that the last two requirements can be at odds with each other, as acting on information might require notifying others. Also, the mailing list is not encrypted.

On top of the above requirements, side activities are organised during various security conferences to allow members to meet each other in person.

3.4 EU FI-ISAC

The EU FI-ISAC is the Information Sharing and Analysis Centre for the European Financial Institutions. It gathers together individual representatives from Financial Institutions (banks, central banks …), CERTs, and Law Enforcement. Its purpose is information sharing about incidents, threats, trends, vulnerabilities, etc., in the financial sector.

The approach of the EU FI-ISAC to trust is as follows:

1. Mandatory use of the TLP. Participants are encouraged to share Amber or Red information.

[4] https://puck.nether.net/mailman/listinfo/nsp-security

2. Participants sign an NDA before each meeting.
3. Mandatory contribution. Contribution is taken in the largest sense possible, but systematic silence is not tolerated.
4. Continuity. As much as possible, people in the group should remain the same over time.

4 Discussion

In this section we discuss how each community fares with regard to the criteria listed in Section **Error! eference source not found.**.

4.1 FIRST

FIRST is a CERT initiative, so its very existence is a trust building mechanism for its members. However, its size and the single level of maturity (membership) means that just being a fellow member will not automatically make a team trustworthy to another one. The size of FIRST also makes its mailing list almost devoid of sensitive information, because teams do not know who else is subscribed.

This is where the other activities play an important role: participation in the conference, symposia, and other face-to-face meetings allow teams to meet each other. Those who actually present their experiences or tools during these activities will get extra credit, because they will show expertise and a sharing mind-set. However, speaking slots are limited, and experience shows that the same teams or even the same persons present their results, while the rest passively absorbs the information.

With regards to the ability to act on information, FIRST as an organisation can do little: they have no control on what data a team will receive, and how they will actually act on it.

4.2 TF-CSIRT

Since TF-CSIRT shares a similar organisational form to that of FIRST, it’s no surprise that the trust situation is similar in some aspects. The mailing list is seldom used for sensitive information sharing, and during meetings the same teams and people are presenting, and are thus more easily trusted. Likewise, TF-CSIRT has little control on the way a team treats information it receives.

The difference lies in the tiered membership. It gives a lot more credit to certified teams. The distinction between closed and open meetings, with TLP Amber or Red information being shared only in the closed meeting, allows for a closer-knit community. Also, the number of accredited teams is still small enough that being a fellow member can be enough for a basic trust relationship.

4.3 NSP-Security

Contrary to FIRST and TF-CSIRT, NSP-Security is made up of individuals. The need for vetting new members and the mandatory taking of action makes for a high level of trust between members. The downside of only having individual members is that there is no automatic way for the trust relationship to be transferred to the members’ organisation or company.

4.4 EU FI-ISAC

As for NSP-Security, members are vetted, and participation is mandatory. The biggest difference is that a neutral trusted third party is vetting the participants. The EU FI-ISAC is also organised around regular physical meetings. This provides the framework for a high level of trust between participants – over time. The downside is scalability: speaking slots are limited during face to face meetings, and there is only so many persons one can talk to during an informal social event that usually accompanies the meetings.

5 Conclusions

We considered four operational communities whose goals include fostering trust between their members. All of them are successful in a certain way, though some scale better than others.

An important observation is that all consider human contact important – even the one based solely on a mailing list, NSP-Security. This leads to a first recommendation that organisations need to dedicate time and resources to the participation of face to face meetings.

Sharing and personal contact is one of the most important factors in establishing trust. Formal presentations during meetings are one of the most obvious ways of providing opportunities for sharing. However, as the number of members in a community grows, the number of speaking slots limits scalability. This situation can be improved in several ways:

- Encourage speaker rotation
- Vary the format of meetings by providing space for active discussion
- Propose side activities that allows personal contact

ENISA should keep investigating ways of improving trust building in operational communities in the future, with a more rigorous approach.

6 References

[1] ENISA, “Baseline Capabilities of National/Governmental CERTs - Update Recommendations 2012,” 2012.

[2] ENISA, “Baseline Capabilities of National / Governmental CERTs - Part 2: Policy Recommendations,” 2010.

[3] F. Fukuyama, Trust: The Social Virtues and The Creation of Prosperity, Free Press, 1996.

[4] ENISA, “Deployment of Baseline Capabilities of National/Governmental CERTs - Status Report 2012,” 2012.

[5] N. Brownlee and E. Guttman, “Expectations for Computer Security Incident Response,” June 1998. [Online]. Available: https://www.ietf.org/rfc/rfc2350.txt.

Catalogue Number TP-05-14-117-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN number: 978-92-9204-113-7
doi: 10.2824/320219

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu