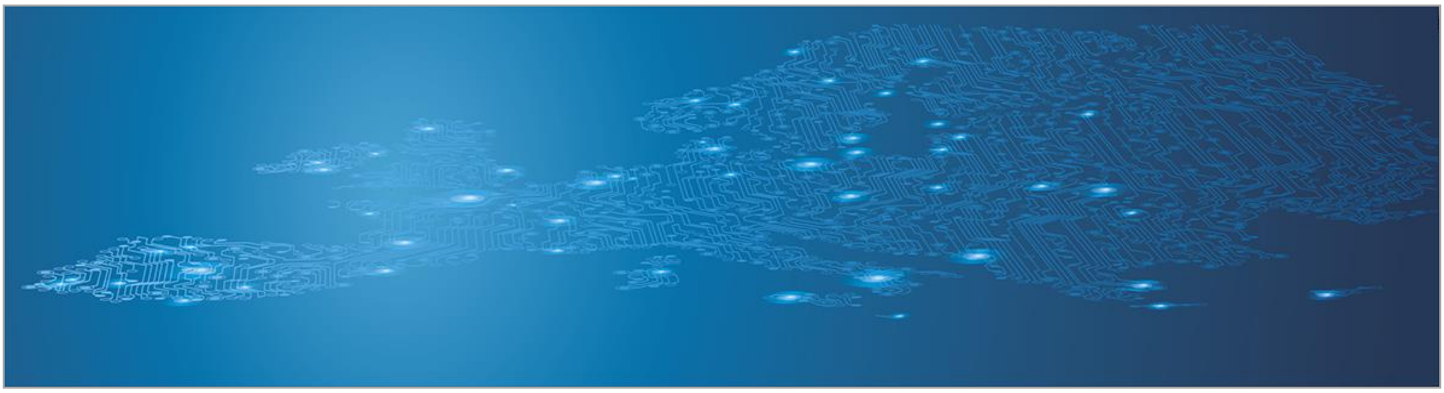

Assesing and testing communication channels between CERTs and all their stakeholders

Toolset, Document for students

September 2014

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.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

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

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

Table of Contents

1 What Will You Learn

In this exercise, participants will discuss all fundamental concepts of the communication channels between CERTs and their constituents, other CERTs, law enforcement, management, public relations (PR), legal counsel, and all other stakeholders. Special attention is given to communications while under attack, and to the testing of communication channels as a means of safeguarding and improving them.

Right from the very start of the CERT community[1] in 1988-9 **communication** between stakeholders was essential for the success of incident response. In fact, the three traditional information security aspects were essential right from the start: *confidentiality, integrity,* and *availability*. Plus another very important one for CERTs: knowing the source of a message and being sure it is from that source – we will refer to that here as *authenticity*.

However, before we come to those, it must be stated that one aspect even comes *before* the four just mentioned: and that is the actual existence of sufficient and trustworthy contact data. After all – without good contacts, CERTs' work would be based on quicksand! These contact points of course need to have been well established in advance, and comprise such parties as (but not limited to):

- Constituents, both at the operational level through security contacts, as at a higher level (for escalations);
- Management, both line management and the top of the organisation (e.g. through a CISO);
- Press contacts / press office;
- Legal counsel;
- Vendors and/or vendor-representatives for the most critical information products used in the constituency;
- The CERT community, either through an upstream CERT with good contacts, or by being part of the web of trust yourself;
- National and/or government CERT;
- National security agencies;
- Law enforcement;
- Other relevant government agencies or contacts;
- Relevant support/consultancy parties, e.g. to do scans, or forensics on demand.
- Next come the four security aspects, in order of priority for CERTs:

[1] http://www.cert.org/encyc_article/tocencyc.html#History

- *Availability*: when communication fails due to saturated, hacked or otherwise sabotaged or failed[2] connections, and if no back-up mechanism is in place, then a CERT cannot gain information about source, character and scope of the attacks; nor can they inform other CERTs or law enforcement about their own findings; and in the case of a spread out constituency, they may find it hard to reach their own constituents.

- *Confidentiality*: when the heat is on due to critical incidents and the stakes are high, communication must be readable only by the intended target, like a colleague CERT, a constituent or the police. When hacking is going on, one should assume that no connection is secure, and that therefore a communication stream could be tapped or intercepted. Only proper encryption can then safeguard confidentiality. This will only work if the CERT has the public encryption keys of their communication partners.

- *Integrity & Authenticity*: a confidential piece of communication is fine, but the receiver also needs to be sure that the information is untampered with, that is, identical to how it was sent by the originator (*integrity*). And he needs to be sure that if the communication claims that it comes from party XY, that indeed it does come from party XY and not from some imposter (*authenticity*). Although these two aspects are not identical, they are usually combined in secure communication (by means of cryptography), and therefore we combine them here too.

Availability is becoming an increasing challenge this decade, because of the fact that TCP/IP is rapidly becoming the protocol of choice for almost all connections[3]. This means that where it used to be so that if the net failed, the phone would still work, this is no longer guaranteed. VOIP is not only used at a local scale, but also backbone providers increasingly integrate all traffic in IP streams. That means that also GSM/UMTS voice traffic is not independent from the Internet anymore, and therefore both landlines and cellular traffic could fail in the case of major outages or attacks. When that happens, most CERTs could right now be essentially isolated. Only very few teams have the possibility to use special protected (usually military) networks, bypassing the commercial net. Alternatives have not been seriously discussed or tested yet in the European CERT community – but this will evidently need to happen in the years ahead. Be reminded that in 2004 when the disastrous tsunami happened in the Thailand/Indonesia/India region, the only communication that worked right after the disaster, was old fashioned radio[4] – with radio amateurs and professionals establishing and improvising communication paths. Analogue radio as well as packet radio may well be serious options – messenger doves seem less suited.

Confidentiality, *Integrity & Authenticity* pose challenges as well – the increase in challenge is here more a matter of scale and organisation than of a technical nature. After all, the techniques have not really changed in the last few decades, they have merely been improved. Basically, all 3 aspects are covered by the use of cryptographic techniques based on asymmetrical key-pairs[5]. For secure web

[2] failed also due to natural disasters or occurrences like storms, earthquakes, volcano eruptions, landslides etc.

[3] http://techcaliber.com/blog/?p=1100 ; also private communication of the author in 2011/2012 with CTOs of various European backbone providers make clear that, basically, TCP/IP over lightpaths, is currently the technology of choice. This means that PSTN traffic but also cellphone traffic is all integrated in huge IP streams routed through fiber networks

[4] http://en.wikipedia.org/wiki/Amateur_radio_emergency_communications and http://www.voanews.com/content/a-13-2005-01-05-voa24-66363817/546509.html

[5] http://en.wikipedia.org/wiki/Public-key_cryptography

traffic TLS/SSL[6] is used, which is based on the use of so called X.509 client and server certificates: the same are the basis for many sorts of secure tunnels, like the remote login tool SSH[7] and various VPN products. Also, X.509 can be used for secure e-mail based on S/MIME[8], which is built into all major e-mail products. Some CERTs actually use S/MIME inside their own organisation or community, however for use between CERTs nationally and internationally the use of PGP/GPG[9] is pre-dominant, and has been since the early nineties. PGP/GPG is not based on X.509 certificates but instead on PGP key-pairs (same principle, different standard). The main difference between the two is that with X.509 the generation of certificates follows a hierarchical method, whereas with PGP the model is that of a maze: everyone can make their own keys, and trust is only based on the mutual signing of keys, which is the result of a conscious act of both parties involved. This “trust-exchange” model suits the organisation of the CERT community, as this is more like an organised maze, and not a hierarchical structure. The challenges are mostly organisational, as said above – with the growing number of teams and team members, it is not easy to scale the PGP keymodel – and alternatively it would be at least as challenging to create a certificate infrastructure for the European, let alone the worldwide CERT community. Additionally, there are some technical challenges too – this is mostly a result of the fact that PGP/GPG is not supported by the main e-mail clients by default. Additional products need to be installed, which sometimes clashes with corporate e-mail policies.

2 Exercise Course

2.1 Task 1: The 1st bit of the incident scenario

Bit 1:

Shortly after reports of unusually large amounts of DNS query traffic from Canada, backbone network latencies start to climb. ISP Network Operations managers reach out to CERTs for help in finding the source of the surging traffic on random ports. CERTs of various sorts contact one another, also including national and governments CERTs. As the latencies become so high on some places that the SLAs with ISP clients are being violated, ISPs and CERTs contact management and legal counsel to inform them. The first questions from the press come in at the PR/communication departments of ISPs and national CERTs – also some CERTs are contacted directly by the press.

And the first Assignment:

Assignment 1:

Discuss, using the incident scenario as thread, the following items:

1. *Shortly establish the CERTs represented in your group and use those as leading examples in the whole Exercise, together with the incident scenario.*
2. *What kind of contacts should your CERT have, like with your constituency of course (two levels, preferably: operational and for escalations), your management (what levels of hierarchy?), etcetera. Make a list together in the group, not leaving any important party out (so not just the common denominators).*

[6] http://en.wikipedia.org/wiki/Transport_Layer_Security

[7] http://en.wikipedia.org/wiki/Secure_Shell

[8] http://en.wikipedia.org/wiki/S/MIME

[9] PGP (http://en.wikipedia.org/wiki/Pretty_Good_Privacy) is the original tool, now provided by a commercial company – GPG (or GnuPG, see http://en.wikipedia.org/wiki/GNU_Privacy_Guard) the open source version. Both adhere to the OpenPGP standard (http://tools.ietf.org/html/rfc4880).

3. *Discuss if your CERTs actually have those contacts available or if they are really easy to reach.*
4. *Discuss if your CERTs are in touch with your contacts, know them, have worked with them – and if and how that could be important.*
5. *Discuss what are the contacts which need to be available for escalations, which also might mean on Sunday morning or when most colleagues are on holiday – and can you actually reach those contacts when really needed?*

The assignment is done in groups of 3-4 – these groups remain so until the end of the exercise.

2.2 Task 2: The 2nd bit of the incident scenario

Bit 2:

Then a number of Root Name Servers and gTLD/country-TLD servers appear to be taken down by unknown causes[10]*. Also some major Neutral Internet Exchanges become compromised. Communications, also between CERTs, are seriously hampered – but do still exist, also thanks to a lot of improvisation, and using trusted parties to relay to others. Given the gravity of the ongoing attacks, secure communications are however essential, and prove to be a further challenge in this situation with a seriously damaged communication mesh.*

And the second Assignment:

Assignment 2:

Discuss, using the incident scenario as thread, the following items:

1. *Confidentiality : when the heat is on, due to critical incidents, and the stakes are high, communication must reach only the intended target, like a colleague CERT, a constituent or the police. When hacking is going on, one should assume that no connection is secure. Discuss in your group how your CERTs have solved this issue in regard communication to their points-of-contact (the ones you discussed before!), and how there may still be blind spots in this regard. Also bear in mind a situation like in the incident, where some of your usual communication partners may not be reachable anymore and therefore you will need to relay through others – how do you do that securely?*
2. *Integrity & Authenticity : an exclusive piece of communication is fine, but the receiver also needs to be sure that the information is* **whole***, that is, identical to how it was sent by the originator (integrity). And he needs to be sure that if the communication claims that it comes from party XY, that indeed it does come from party XY and not from some*

[10] See http://en.wikipedia.org/wiki/Distributed_denial_of_service_attacks_on_root_nameservers#October_21.2C_2002 , http://erratasec.blogspot.nl/2012/02/no-anonymous-cant-ddos-root-dns-servers.html (especially the footnotes), and http://www.cymru.com/monitoring/dnssumm/ : while the set-up of the Root Name Servers is extremely robust, an attack by exploiting vulnerabilities is always feasible – additionally, the gTLD and country TLD servers are probably easier targets.

imposter (Authenticity). Discuss among yourselves, following on the discussion of Confidentiality, how you have solved (or not solved) this issue for your points-of-contact.

3. *DNS failure: this is an issue of availability of communication. DNS failure is unlikely to easily happen, but not unthinkable. When it happens, the Net still functions, but name resolution stops working. You will need to rely on IP numbers then instead. Discuss in your group how your CERTs are prepared for such an event – and what should be done to be prepared.*

2.3 Task 3: The 3rd bit of the incident scenario

Bit 3:

Despite the work of many, the on-going attacks which come from so many sources all over the world, are increasingly damaging. Some networks chose to isolate themselves. The remaining traffic worldwide becomes virtually uncontrollable and saturates the Net. As many backbone links become unusable, most of the phone traffic (including cellphones) dies out too.

And the third Assignment:

Assignment 3 :

Discuss, using the incident scenario as thread, the following items:

1. *Availability : when communication fails due to saturated, hacked or otherwise sabotaged connections, and if no back-up mechanism is in place, then a CERT cannot gain information about source, character and scope of the attacks; nor can they inform other CERTs or law enforcement about their own findings; and in the case of a spread out constituency, they may find it hard to reach their own constituents. Discuss in your group how your CERTs have taken this possibility into account, how they plan for it, what they do when it happens, in these two situations:*
   - *Most of the phonesystem (landlines and cellphones) still works.*
   - *Most or all of the phonesystem (including cellphones) is down too.*

   Be aware that the latter is not unlikely at all these days, with the advent of Voice-over-IP not just on local loops and inside organisations, but also on the backbone level, where providers are more and more tunneling ***all*** *traffic through IP. Usually only military teams (but possible also national and/or government teams) can use special, protected networks which would hopefully still work in cases of emergency. What other means are there?*
2. *Testing communications? Discuss, bearing all you learnt in this Exercise in mind, the case for the testing of communications. Regular testing of things like:*
   - *Points-of-contact*
   - *Cryptography used*
   - *Fallback mechanisms when DNS fails*
   - *Fallback mechanisms when the Net fails*
   - *Fallback mechanisms when the Net and phones fail*

   How do you test it? What to bear in mind? Could this be implemented as a regular test? Or part of regular fire drills?

2.4 Discussion

In each group, notes have been taken, to facilitate this discussion. All trainees are asked to contribute. Special attention is asked for the aspects of **availability** and **testing** in the discussions.

3 Conclusion

The trainees will have dealt with or come across most of the following issues in the course of this exercise:

- The necessity of an extensive and accurate list of points-of-contact (see Introduction for a non-exhaustive list) which will also work under duresse (e.g. escalations outside office hours)
- Safeguarding of the availability of communication to the points-of-contact at least, also when DNS fails, when the Net fails, and when also the phones fail.
- Safeguarding of the security of communication to the points-of-contact at least. Security including here: Confidentiality, integrity, authenticity (availability already treated in previous bullet item).
- Knowledge of applicable communication cryptography like GnuPG/PGP, PGP/MIME, S/MIME (based on X.509 instead of PGP).
- Understanding of infrastructural threats to communication like the non-availability of DNS, the increasing reliance on IP for both VoIP and cellphone traffic.
- Availability of main sources of CERT contact information, like the TI database, FIRST website, ENISA CERT info, IRT and abuse contact info from the RIPE database (and ARIN etcetera)

It is strongly recommended to all trainees to actively **use** the results of this exercise in their teams, to enhance awareness and invite them to plan more proactively on points-of-contact, availability and security of communication, and how to regularly test all facets of the CERT’s communication channels. The below references will prove to be helpful in that regard.

4 References

European CERTs contact info:

1) TI database: https://www.trusted-introducer.org/teams/
2) ENISA CERT inventory: http://www.enisa.europa.eu/activities/cert/background/inv
3) IRT objects in RIPE IP-number database: http://www.ripe.net/data-tools/db/faq/irt-faqs and as example try this query: https://apps.db.ripe.net/search/query.html?searchtext=192.87.106.101&flags=B&sources=RIPE_NCC&grssources=&inverse=&types=#resultsAnchor and click on to the “mnt-irt: irt-SURFcert” which yields https://apps.db.ripe.net/whois/lookup/ripe/irt/irt-SURFcert.html (all contact info for the team called SURFcert)

Teams outside Europe:

4) FIRST worldwide membership info: http://www.first.org/members/map
5) Asia-Pacific teams cooperating in APCERT: http://www.apcert.org/about/structure/members.html

6) North-American IP number registry: http://whois.arin.net/ui and as examply query for 128.103.200.35 and find http://whois.arin.net/rest/net/NET-128-103-0-0-1/pft and subsequently click on to the Abuse info for Harvard University http://whois.arin.net/rest/poc/ABUSE3331-ARIN.html
7) For Latin America use http://lacnic.net/cgi-bin/lacnic/whois and search for abuse-c fields
8) For Africa use http://www.afrinic.net/en/services/whois-query similarly to Latin America
9) For Asia-Pacific use http://www.apnic.net/apnic-info/whois_search/about similarly to Latin America

ENISA *Good Practice Guide for Incident Management*
http://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management
(e.g. p. 18-19, 22. 36, 52, 67, 68)

Handbook for Computer Security Incident Response Teams (CSIRTs)
http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm
(e.g. p. 102-106)

General ENISA information for CERTs : http://www.enisa.europa.eu/activities/cert

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

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