CIO Platform Nederland

CEG Information Security

Coordinated Vulnerability Disclosure

Model Policy and Procedure

A publication of the CIO Experience Group Information Security

CIO Platform Nederland, February 2016

www.cio-platform.nl/publicaties

Contents

Definitions

A. Coordinated Vulnerability Disclosure is revealing vulnerabilities in a responsible manner in joint consultation between reporter and Organisation, based on a Coordinated Disclosure Policy set by Organisations.
B. A vulnerability is a (presumed) weakness or breach of security of the infrastructure of an ICT system of <<*Organisation*>>.
C. The reporter is the person or body who reports a vulnerability via Coordinated Vulnerability Disclosure.
D. The Organisation, <<*Organisation*>>, is the owner and/or administrator of the system and the recipient of the Coordinated Vulnerability Disclosure report.
E. The Coordinated Vulnerability Disclosure policy is the document containing the rules with which the reporter and the Organisation must comply. See chapter 5.
F. The Coordinated Vulnerability Disclosure procedure is the procedure in which the responsibilities and operations for Coordinated Vulnerability Disclosure are described. See chapter 6.
G. Coordinated Vulnerability Disclosure is also known as Responsible Vulnerability Disclosure.

1 Reason for this initiative

<<*Organisation*>> has a legal obligation to keep our data, specifically personal data, safe. Due to the increasing amount of software in use, it is increasingly difficult to ensure that all this software is indeed as safe as it should be. In order to increase the awareness of any security flaws, it is necessary that organisations are open to reports on vulnerabilities from persons or bodies outside the organisation itself. Therefore it is important for organisations to implement Coordinated Vulnerability Disclosure. This creates clarity, for the organisation and the reporter, regarding the responsibilities of both parties.

<<*Organisation*>> has decided to develop Coordinated Vulnerability Disclosure policy and procedure and to apply these to its own organisation.

2 Legislation

Computer system hacking can be motivated by good and bad intentions. Civil or criminal proceedings could be started in order to determine whether someone has acted in accordance with the law. This chapter describes the Dutch legislation relevant to Coordinated Vulnerability Disclosure.

NB. It is important to note that each country has or may have its own regulations regarding computer hacking and the like. Organisations operating internationally must determine whether Coordinated Vulnerability Disclosure is possible under the current legal systems in all countries in which they operate.

If you don't intend to apply Coordinated Vulnerability Disclosure in the Netherlands, you can skip to paragraph 2.3 below.

2.1 Dutch Criminal Code

The advent of the Computer Crime Act has made hacking punishable under criminal law since 1993. The crime of hacking is described, inter alia, in articles 138ab (computer intrusion) and 161 sexies Sr (damage to systems) of the Dutch Criminal Code. The maximum prison sentences for these offences range, respectively, from one to four years and from one to fifteen years.

The statutory articles 38ab and 161 sexies do not distinguish between malicious hackers and ethical hackers. These statutory provisions therefore make no direct distinction between a malicious hacker who tries break in to a website and an ethical hacker wanting to demonstrate a vulnerability in the context of public interest. The decision as to whether a reporter has acted as an ethical hacker is up to the Public Prosecution Service and the court.

2.2 Prosecution

If, according to the law, computer intrusion has taken place this may have consequences for a vulnerability reporter. The reporter may be prosecuted for this under both civil and criminal law (see frame).

2.2.1 Civil law prosecution

Following a report, the administrator/owner of a system may take civil action. He makes the decision to issue a summons and he decides whether a civil lawsuit should be initiated against the reporter.

The administrator/owner may state in advance in a Coordinated Vulnerability Disclosure policy that prosecution will be waived in certain circumstances or that a civil action will be started. If the reporter complies with these conditions a case should not be opened and prosecution under civil law should not take place.

2.2.2 Criminal prosecution

The Public Prosecution Service may start criminal investigations before proceeding to criminal prosecution. Despite a company having previously stated that it will waive prosecution, the Public Prosecution Service may launch an investigation into the actions of the reporter.

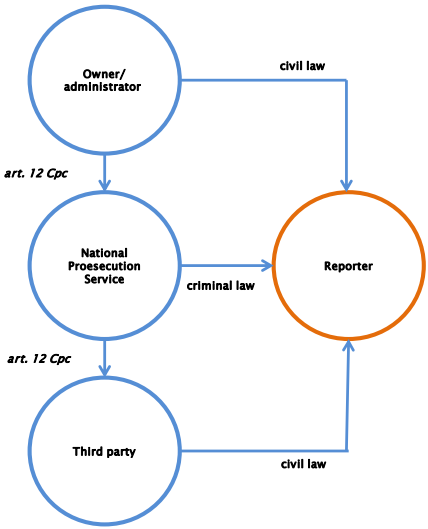
The Public Prosecution Service may abandon prosecution after investigation, according to the so-called principle of expediency[1].

In such case the public prosecutor will then not charge the suspect, on grounds of public interest.

Difference between civil and criminal law:

Criminal law regulates the relationship between the State and the citizen. The Dutch Criminal Code described the laws with which the citizen must comply.

Civil law governs the relationships between citizens and/or companies. In contrast to criminal law, there is no central agency which brings the matter before the court.



[1] Public Prosecution Service (2013), *Glossary: Principle of expediency*. Referenced via https://www.om.nl/onderwerpen/begrippenlijst/opportuniteitsbeginsel

If the Public Prosecution Service decides not to prosecute then a third party with a direct interest - for example the administrator/owner, a client or a patient - may submit a complaint under article 12 of the Dutch Criminal Procedure Code, with the request that the court nevertheless prosecutes. A reporter may therefore be prosecuted both civilly and criminally and both prosecutions may be started separately from each other. The abandonment of a civil prosecution does not therefore directly result in abandonment of a criminal prosecution, nor vice versa.

2.3 Freedom of expression (Article 10 ECHR)

In order to investigate a case of significant social importance, it may be necessary to break the law. Article 10 of the European Convention on Human Rights (ECHR) gives citizens the opportunity to expose abuses. Journalistic value may determine that no punishment is imposed for reasons of public interest, despite the fact an act was in itself illegal. Both professional journalists and citizens can operate as journalists and rely on Article 10.

In such cases it is important, however, that less intrusive methods were not available. If possibilities exist whereby the same information can be revealed, but with fewer consequences, these must be pursued. Article 10 ECHR is binding on all countries that are members of the Council of Europe.

If you're not interested in the Dutch national situation, please continue reading at paragraph 2.4 below.

It can happen that ethical hackers report via a journalist in order to ensure their anonymity. In the Netherlands journalists have the right to keep their source confidential. This protection flows from Article 10 of the ECHR. A ruling of the Dutch Supreme Court[2] stipulates that journalists do not have to reveal their source during a witness hearing, unless revealing the source is necessary for the maintenance of a democratic society. Reasons of 'compelling public interest' will have to be brought and these will have to outweigh the 'extremely compelling public interest' of freedom of the press in order to justify revealing such a source.

The instruction for application of coercion to journalists includes the policy guidelines of the Public Prosecution Service with regard to source protection.

[2] Volkskrant (1996), *Hoge Raad gunt journalist bescherming van bronnen (Supreme Court grants journalist source protection)*. Referenced via http://www.volkskrant.nl/archief/hoge-raad-gunt-journalist-bescherming-van-bronnen~a426812/

In this instruction the national head of the Public Prosecution Service writes: "As the right to source protection is not absolute criminal law enforcement measures may be applied to a journalist, in special circumstances: if this is the only imaginable, effective means to detect and prevent an extremely serious offence. It must concern offences presenting a threat such that the lives, security or health of people can be seriously damaged or endangered."[3]

In addition, source protection for the reporter does not provide indemnity from prosecution nor an absolute guarantee of anonymity. A reporter can also be detected through other channels, as was seen in the case of a report of vulnerability in the system of the Groene Hart Hospital. The suspected hacker was arrested by the national detective unit after an investigation by the THTC (Team High Tech Crime)[4]. This investigation was conducted by the national department of the Public Prosecution Service. In this case publication via a journalist did not prevent arrest of a suspect as the suspected hacker was traced by other means.

2.4 Legislative developments

Developments that could affect the future of Coordinated Vulnerability Disclosure are expected. Examples of this are the European data leak reporting requirements and the national data leak reporting requirements, for instance in the Netherlands (Nederlandse Meldplicht datalekken).

The main effect of these reporting requirements on Coordinated Vulnerability Disclosure relates to the report processing time. The proposals for the reporting requirements indicate that the discovery of a leak must be reported within a certain period of time. This means that proper receipt of a Coordinated Vulnerability Disclosure report may require availability of resources capable of processing the message in time.

[3] Board of attorneys-general (2013), *Aanwijzing toepassing dwangmiddelen tegen journalisten (Instruction on the application of coercion to journalists)*. Referenced via https://zoek.officielebekendmakingen.nl/stcrt-2012-3656.html
[4] National department of the Public Prosecution Service (2013) *Suspect arrested for computer intrusion at Groene Hart Hospital*. Referenced via https://www.om.nl/vaste-onderdelen/zoeken/@30198/verdachte/

3 Standards

Since the advent of the "Guideline for development of Responsible Vulnerability Disclosure practice" by the Dutch National Cyber Security Centre (NCSC), Coordinated Vulnerability Disclosure has been increasingly used by Dutch Organisations. In addition to the NCSC guideline, two international ISO standards have been available since early 2014. This chapter explains both the guideline and the ISO standards.

3.1 Coordinated Vulnerability Disclosure guideline in the Netherlands

Following a motion by the Dutch Member of Parliament Hachchi (D66) during the meeting on Cyber Security and Security of Government Websites on April 10, 2012, Minister Opstelten of Security and Justice has committed to coming up with a framework for Responsible Disclosure, which in this publication is deemed to be the same as Coordinated Vulnerability Disclosure. This framework is set out in the 'Guidelines for developing Responsible Vulnerability Disclosure practice' (Leidraad om te komen tot een praktijk van Responsible Vulnerability Disclosure)". The guideline is aimed at both organisations that are owners/administrators of information systems and at vulnerability reporters. Sources consulted in order to arrive at the guideline include benevolent hackers from the community and examples of best practice.

The NCSC uses the following definition in its guideline for Responsible Disclosure: "Responsible Disclosure in ICT is the revealing of vulnerabilities in a responsible manner in joint consultation between reporter and organisation, based on a Responsible Disclosure Policy set by organisations." [https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html][5]

The definition contains two important elements which characterise the position of the NCSC. First of all, two parties are primarily involved in Coordinated Vulnerability Disclosure: the reporter and the organisation. Secondly the NCSC

[5] NCSC (2013), *Responsible disclosure*. Referenced via https://www.ncsc.nl/binaries/content/documents/ncsc-en/current topics/news/responsible-disclosure-guideline/1/Responsible%2BDisclosure%2BENG.pdf

assumes the Coordinated Vulnerability Disclosure policy is set (in advance) by the organisation.

The NCSC refers to various Coordinated Vulnerability Disclosure policies which can serve as examples. These examples include ones from Floor Terra, Marktplaats.nl, Fox-IT and major Dutch telecom providers.

The guideline explains how a reporter could act in the event that an owner/administrator has no established policy for Coordinated Vulnerability Disclosure. The reporter is, in such a case, advised to directly contact the owner/administrator. If this does not achieve the desired effect a reporter may then decide to engage an intermediary. The guideline identifies the NCSC as an intermediary and it is also stated in the Coordinated Vulnerability Disclosure policy of the NCSC, on their website, that the NCSC can 'act as intermediary' in the event of no or insufficient reaction by a third party.[6]

The guideline has no effect in criminal law contexts. Following the guidelines therefore in no way guarantees the reporter immunity from criminal procedure. A civil law procedure can possibly be prevented by a reporter agreeing with an owner/administrator that no summons will be issued nor other civil law action undertaken.

3.2 ISO standards

The International Organisation for Standardization (ISO) has published several standards regarding security arrangements in organisations. Starting point is standard 27002, which provides best practices and management measures for data security. A responsible disclosure policy must connect with the processes set up on the basis of ISO 27002 or a similar standard.

ISO has also brought out two standards on revealing vulnerabilities and the handling of vulnerability reports. Both standards were applied in the establishment of a Coordinated Vulnerability Disclosure procedure for the model policy.

[6] NCSC (2013), *Responsible disclosure*. Referenced via https://www.ncsc.nl/english/current-topics/responsible-disclosure guideline.html

3.2.1 ISO 29147

ISO 29147 provides guidelines for the disclosure of potential vulnerabilities. The international standard describes methods that an organisation can apply to problems experienced on the public disclosure of a vulnerability. The standard describes four guidelines:

- Receiving reports of possible vulnerabilities
- Distribution of information on vulnerabilities in their products and online services
- Information flows on disclosure of a vulnerability
- Examples of structured information exchange

3.2.2 ISO 30111

ISO 30111 provides guidelines on the way information about vulnerabilities should be processed and how the vulnerability in a product or online service can be remedied. The standard sets out three guidelines:

- A structured process and organisation structure to support the investigation and remedying of vulnerabilities
- The steps involved in verifying a vulnerability
- Vulnerability handling process

4 Coordinated Vulnerability Disclosure objectives

It can of course happen that vulnerability in a product or service is overlooked by the organisation, but is noticed by someone else. The <<*Organisation*>> therefore finds it important to accept reports of vulnerabilities and to work together (possibly with the reporter) to remedy these vulnerabilities. In this way the standard of data security can be raised and damage can be prevented.

Security and the prevention of damage are key considerations. For this reason <<*Organisation*>> wants to remedy vulnerability before it is made known externally. The reporter must therefore allow <<*Organisation*>> sufficient time to stop the leak before the possible publication of the vulnerability.

The lack of clarity regarding prosecution can be partially remedied by drawing up a policy for Coordinated Vulnerability Disclosure. The Coordinated Vulnerability Disclosure policy ensures that there are rules for both reporter and <<*Organisation*>>. In this regard it is important to mention that the Public Prosecution Service and any relevant third party (such as a student or web host) can always undertake independent legal action, regardless of the content of the organisation's policy.

5 Coordinated Vulnerability Disclosure policy

The Coordinated Vulnerability Disclosure policy indicates the rules for the reporter and what can be expected from the organisation. The policy is published on the website in order to create correct expectations on the part of both reporters and the public. The policy is related to the Coordinated Vulnerability Disclosure process. The procedure can be found in Chapter 6.

The policy has been based on the example of the policy developed by Floor Terra.

---------- Policy to be published on website ----------

<<*Organisation*>> regards the security of our systems as extremely important. Despite our concern for the security of our systems, a weak spot may arise.

If you have found a weak spot in one of our systems, we would be pleased to hear from you, so that we can take steps to remedy it as soon as possible. We are keen to cooperate with you in order to better protect our users and our systems.

Our policy for Coordinated Vulnerability Disclosure is not an invitation to actively and intensively scan our company network in order to discover its weaknesses. We monitor our company network. As a result there is a high chance that a scan will be picked up, that our CERT or service provider will investigate and that unnecessary costs may be incurred.

There is a chance that your investigation will include activities punishable under criminal law. If you have complied with the following conditions we will not take legal action against you with regard to the report. The Public Prosecution Service always reserves the right to decide whether to submit you to prosecution under criminal law. The Public Prosecution Service has published a policy letter in this regard, (https://www.om.nl/publish/pages/22742/03_18_13_beleidsbrief_college_responsible_disclosure.pdf).[7]

We request you to:

[7] This applies only in the Netherlands!

- E-mail your findings as soon as possible to <<*provide an e-mail address specifically for reporting security incidents, e.g. security@organisation.org*>>.Encrypt your findings using our PGP key <<*fill in fingerprint*>> to prevent the information falling into the wrong hands.

- Do not abuse the vulnerability by, for example, downloading more data than is necessary to demonstrate the leak, or by changing or deleting data. Exercise extra restraint with regard to personal data.

- Do not share information about the vulnerability with others until it has been solved. Do not use attacks on the physical security or applications of third parties, social engineering, distributed denial-of-service or spam.

- Provide sufficient information to enable reproduction of the vulnerability, so that we can remedy it as soon as possible. Generally the IP address or URL of the affected system and a description of the vulnerability and operations carried out are sufficient, but more might be required in the case of complex vulnerabilities.

What we promise:

- We react within 3 working days to your report - with our appraisal of the report and an expected date of remediation.

- We treat your report confidentially and will not share your personal details with third parties without your authorisation, unless required to do so in order to comply with a legal obligation. We will keep you informed of the progress made in remedying the vulnerability.

- Anonymous or pseudonymous reporting is possible. You should be aware that in such case we cannot contact you concerning, for example, the steps taken, progress in stopping the leak, publication or the possible reward for the report.

- If you wish, we will credit you as the discoverer when reporting on the vulnerability.

We can reward you for your investigation. Although we are not obliged to do so. So you are not automatically entitled to a reward. The form of this reward is not fixed in advance and will be determined by us on a case-by-case basis. Whether we allocate a reward and the form of the reward depend on the accuracy of your investigation, the quality of the report and the severity of the leak.

We strive to resolve all problems as quickly as possible, to keep all involved parties informed and we welcome involvement in any publication about the vulnerability after it has been remedied.

Our policy falls under a Creative Commons Attribution 3.0 license. The policy is based on the example policy of Floor Terra (Responsible Disclosure.nl)

---------- End of policy ----------

6 Coordinated Vulnerability Disclosure procedure

The Coordinated Vulnerability Disclosure policy is related to the Coordinated Vulnerability Disclosure process. The policy can be found in Chapter 5. The flow diagram of this procedure can be found in Appendix A.

6.1 Assumptions

A. <<*Organisation*>> sets out policy and procedure for Coordinated Vulnerability Disclosure and publishes policy and procedure on its website. Policy and procedure are accessible via <<*insert an email address specifically for the communication of security incidents, e.g. security@organisation.org*>>.
B. The organisation has reserve capacity to enable proper reaction to reports. Incident handling and mandating of the person responsible for the process demand particular, extra attention.
C. Data security applied to reports is equal to the standard used for confidential information, unless this is regarded as unnecessary after assessing the notification.
D. Mutual trust forms the basis of Coordinated Vulnerability Disclosure, especially in the case of long-term treatment of the vulnerability. The organisation must keep the reporter and other parties regularly informed of the progress of the process. Major changes in progress should be communicated to the reporter as this can impact publication by the reporter.
E. If the reporter complies with the rules as stated in the Coordinated Vulnerability Disclosure policy, <<*Organisation*> > will not undertake legal action (to prosecute). If it appears that the reporter has not acted in accordance with the rules, legal steps may be undertaken.
F. Coordinated Vulnerability Disclosure and non-compliance with the rules of Coordinated Vulnerability Disclosure can have far-reaching legal implications for the organisation and the reporter. Timely consultation with a company lawyer with regard to civil, criminal and privacy issues is therefore essential.
G. Coordinated Vulnerability Disclosure is primarily a matter between the reporter and the owner/administrator of the system. Reports concerning a third party system cannot be handled by <<*Organisation*>>.
H. If possible, agreements should be made with suppliers of goods and

services to which the Coordinated Vulnerability Disclosure procedure may apply.

6.2 Roles and responsibilities

A. The incident-handling employee or CERT of <<*Organisation*>> is responsible for passing on reports of vulnerabilities to the appropriate Information Security Officer of the operating company. The incident-handling employee or CERT of <<*Organisation*>> can offer advice for remedying the vulnerability and can inform the involved parties concerning a vulnerability.
B. The Information Security Officer of the operating company in which the vulnerability is located is responsible for monitoring the progress of the process and investigating and remedying the vulnerability. In addition, the Information Security Officer maintains contact with the reporter.
C. The communication department can support the Information Security Officer in communicating with the reporter and is involved in publication of a vulnerability.
D. Central switchboard or call center operators and the ICT help desk of the operating company should be aware of the Coordinated Vulnerability Disclosure procedure and must be able to refer a reporter to the incident-handling employee or CERT at <<*Organisation*>> in the event of a report being received by the central switchboard or call center operator or the ICT help desk.
E. The reporter is responsible for his own actions and has to comply with the rules as set out in the Coordinated Vulnerability Disclosure policy of the organisation.

6.3 Receiving the report

A. A report concerning a vulnerability is received via e-mail. E-mail reports are received at <<*insert specific e-mail for reporting security incidents, e.g. security@organisation.org*>> and must be encrypted with the corresponding public PGP key.
B. The report may be delivered anonymously, under a pseudonym or via an intermediary/counsellor. This can mean that no communication is possible with the reporter.
C. The incident-handling employee or CERT of <<*Organisation*>> sends a confirmation of receipt of the report to the reporter. This is not a confirmation of the validity of the leak but confirmation of the start of

the investigation.

D. The incident-handling employee or CERT at <<*Organisation*>> ensures that the report arrives as soon as possible at the department which can best assess and handle the report and the incident-handling employee or CERT of <<*Organisation*>> opens a ticket accordingly.

6.4 Identifying the vulnerability

A. Within three working days the Information Security officer dispatches a digitally signed confirmation of receipt of the vulnerability report. This e-mail contains, at least:
   a) Confirmation of the report
   b) A first assessment of the legitimacy and seriousness of the reported vulnerability
      - The legitimacy and severity of the reported vulnerability must be estimated. This provides a time period within which the vulnerability will be remedied. Standard periods for remedying vulnerabilities are 60 days for configuration and software and 6 months for hardware.
   c) Potential follow-up steps, for the process.
   d) Period in which leak may be remedied.

B. The Information Security Officer tries to verify the suspected vulnerability. If there is a report of a vulnerability in unsupported software, services or websites, it must be established whether this vulnerability also appears in other, supported products or services. In addition, an assessment should be made as to whether the same vulnerability could also arise in other organisations, in or outside the sector and stakeholders should be informed via the appropriate channels.

C. Prioritisation must be determined. This is deduced from two factors: urgency and impact. The prioritisation to be followed is the incident prioritization in for instance the '*Data security incidents scenario'*. In the event of a medium or higher prioritisation category, the Corporate Information Security Officer must be involved in the investigation.

D. A first assessment must be made as to whether the reporter complied with the rules of the policy. If there is a possibility that the rules were breached the Corporate Privacy Officer must be engaged for a legal opinion.

E. When determining prioritization of the report, the information currently available must be taken into account. The following aspects

may be considered:

a) **The reporter's agenda**: The reporter could intend to make the vulnerability public by means of a research report or via a presentation during a conference. The organisation must disclose the vulnerability before or immediately after disclosure by the reporter. The organisation must therefore know the reporter's desired publication date.
b) **General knowledge concerning the vulnerability**: If the vulnerability is widely known it is more likely that it will be exploited.
c) **The nature of possible attacks**: The cost and chance of success of an attack depend on the vulnerability to be exploited. Vulnerabilities with low attack costs and a high chance of success must be remedied rapidly.
d) **Existence and maturity of attack resources**: When effective methods are available to exploit the vulnerability, attack tools can be developed.
e) **The nature of potential damage**: The nature of the product and the potential damage determine the seriousness of the situation for users. An intranet vulnerability, for instance, may have a big impact as a result of leaking personal information.
f) **Evidence of attacks (incidents)**: Incidents where the vulnerability is exploited may indicate an increased risk for users. Depending on the available information, a temporary solution may be developed; this also applies if there is no complete solution available.

6.5 Terminating the investigation

There are several ways in which an investigation can be wound up. The reporter should be informed why the investigation has been stopped.

A. Double reporting: The problem is as previously reported and is already being handled via a Coordinated Vulnerability Disclosure procedure, via some other incident handling procedure, via scheduled maintenance, or is already remedied.
B. Out-of-date product: The vulnerability is only present in a product or service that is no longer supported by the organisation.
C. Non-security vulnerability: The reported vulnerability has no implications for data security or is not capable of abuse using existing techniques.
D. Third party vulnerability: The vulnerability is present in the product or

service of a third party. In consultation with the reporter, contact may be made with the third party.

6.6 Confirming validity

A. Once verification of the vulnerability is completed, the reporter should be informed of the findings and of the next steps in the investigation.
B. It is possible that the organisation cannot reproduce the vulnerability, using the information in the report. The organisation must then ask the reporter for more evidence, to prove that it is actually a data security problem.

6.7 Damage limitation and exposure assessment

A. Start a thorough assessment of the nature and scope of the incident; establish the extent of the damage and secure any evidence.
B. Supplemental: The reporter must be informed of the progress of the investigation. If possible, the reporter should be sent an overall schedule of the remediation and repair work.

6.8 Remediation and repair

A. Take measures to ensure that the cause of the incident is blocked or removed; reduce the impact by preventing further exposure of sensitive data; commence re-starting business processes that were stopped as a result of the incident; ensure that risks associated with this incident are mitigated.

6.9 Publication

A. If an update is available for the relevant vulnerability, in an online environment, install this update.
B. The reporter only publishes the vulnerability once reporter and organisation have agreed to publish it, when all stakeholders are well informed and when the organisation has indicated that the vulnerability has been remedied in accordance with the agreements made.
C. If it is difficult or impossible to remedy a vulnerability, or if high costs are involved, the <<*Organisation*>> may, in consultation with the reporter, agree not to make the vulnerability public.
D. Once the organisation is satisfied with the effectiveness of the update, employees, users and clients must be informed by means of a security advisory (see Appendix C). The solution should be made available on

the website of the organisation.

E. Following publication of a security advice update, further adaptations may be necessary. These adjustments must be clearly tracked.
F. If a ticket has been created by the incident-handling employee or CERT of <<*Organisation*>>, it must be communicated that the matter is closed.

6.10 Informing stakeholders

A. If the vulnerability is possibly also present at other locations, the Information Security Officer may agree with the reporter to inform the broader ICT community or the general public concerning the vulnerability, via the incident-handling employee or CERT of <<*Organisation*>>.

6.11 Rewarding the reporter

A. The organisation ascertains independently and by case whether a reward is granted and what form the reward will take. An allocated reward is awarded as soon as it has been determined with sufficient certainty that the reporter has complied with the conditions of the Coordinated Vulnerability Disclosure policy and the Coordinated Vulnerability Disclosure procedure.

6.12 Publishing

A. The manner of publication is agreed with the reporter. The communication department is involved in decisions about publication.
B. In consultation with the reporter, a joint announcement may be made. This might include a joint presentation at a security conference or publication in a <<*Organisation*>> blog.
C. If the reporter does not want to publish the vulnerability himself, he is informed via e-mail of the conclusion, the (possible) reward and is thanked for his report and efforts.

6.13 Reporting and evaluation

A. Evaluation is carried out as described in the *'Data security incidents scenario'*.
B. Results of the Coordinated Vulnerability Disclosure procedure and the causes of vulnerability are evaluated by the <<*Organisation*>> Core Security Team.

7 Sources

7.1 Policy

Floor Terra (2013), *Responsible Disclosure, example text*. Referenced via www.responsibledisclosure.nl

NCSC (2013), Responsible Disclosure Guideline. Referenced via https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html

Nederland ICT (2013), *Gedragscode Responsible disclosure*. Referenced via (Dutch only) http://www.nederlandict.nl/Files/TER/Gedragscode_responsible_disclosure_2013.pdf

SURFnet (2014), *modelbeleid en procedure responsible disclosure Hoger Onderwijs* (Dutch only)

7.2 Procedure

NEN-ISO/IEC (2014), *NEN-ISO/IEC 29147:2014 Vulnerability disclosure*. Geneva: ISO/IEC

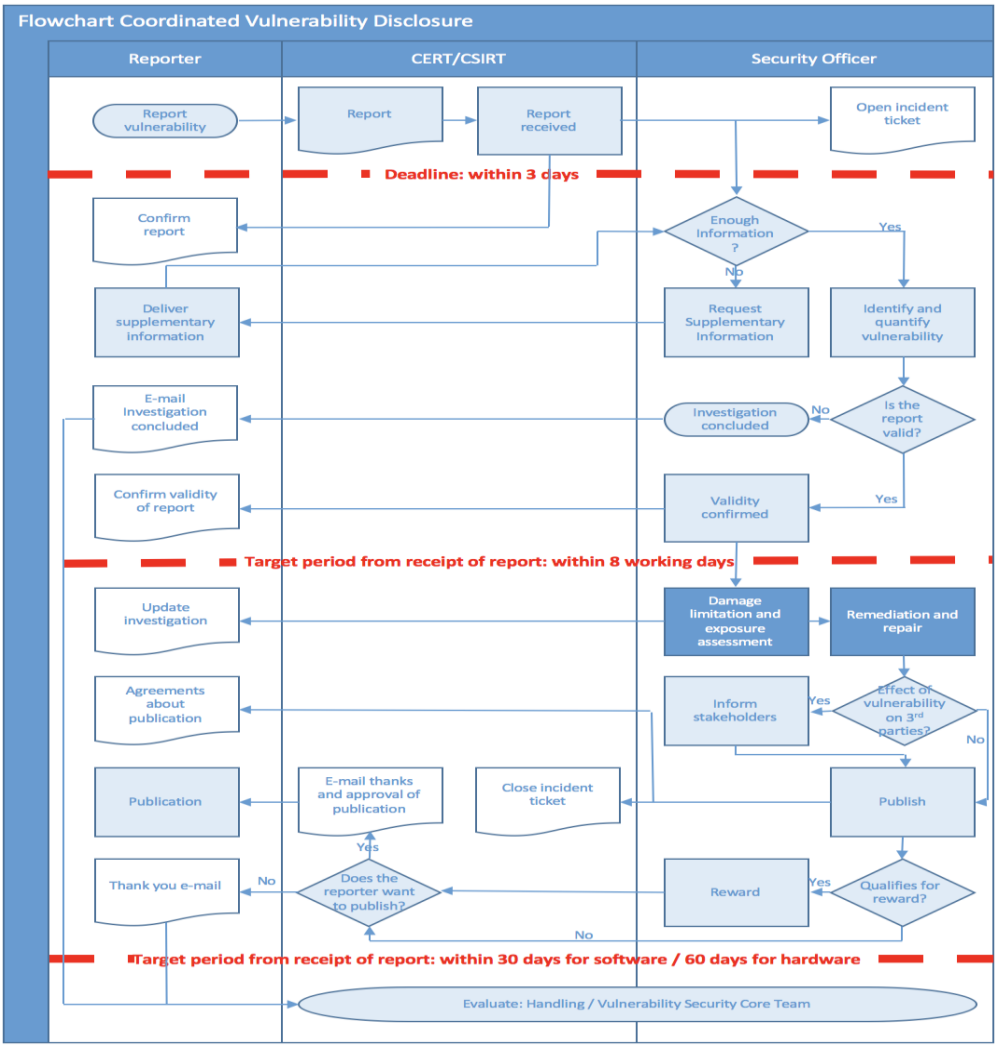
NEN-ISO/IEC (2013), *NEN-ISO/IEC 30111:2013 Vulnerability handling processes*. Geneva: ISO/IEC

7.3 Special thanks

Our special thanks are due to the authors of documents that form the foundation of this publication. We would specifically like to mention Cooperation SURF, the Dutch National Cyber Security Centre and Floor Terra. Their prior work has made it easier for us to offer a helping hand to all Organisations aiming to implement Coordinated Vulnerability Disclosure. By working together we make the digital world safer.

Appendix A: Flowchart, Coordinated Vulnerability Disclosure process

This flowchart shows the sequence of the various stages of Coordinated Vulnerability Disclosure.



Appendix B: Form

Examples of the content of the form for reporting vulnerability may be found in ISO 29147; Annex A or https://forms.cert.org/VulReport/. An example of a form:

This form is only intended for reporting security leaks. Please fill in as completely as possible.

- Name
- E-mail
- Public key
- Telephone no.
- Do you wish to publish with regard to the vulnerability (yes/no)
- Description of vulnerability and actions carried out
- Select file

Appendix C: Security advisory

Examples of security advisories may be found in ISO/IEC 29147:2014; Annex A

The NCSC uses the following layout for security advisories:

- Title
- Advisory-ID
- Version
- Chance
- CVE-ID
- Damage
- Issue date
- Application
- Version(s)
- Platform
- Update
- Summary
- Impact
- Description
- Possible solutions
- Links

"De vereniging van ICT eindverantwoordelijken in grote organisaties van de vraagzijde"

www.cio-platform.nl