CENTRE FOR CYBER SECURITY BELGIUM (CCB)

PRESENTATION
PITS - PUBLIC IT SECURITY BERLIN 2017

Valéry VANDER GEETEN
Legal Officer
Security Officer - DPO
01
MISSIONS & STRATEGIC OBJECTIVES
MISSIONS

Guidelines and security standards for public authorities

Cyber Crisis Management with Crisis Center and police (CCU)

Coordination - between public authorities; - between public and private sector;

Coordination representation in international cybersecurity forums

Technical assistance (service CERT.be) - for public authorities - for OES/CI

Awareness - publications; - national campaign; - safeonweb.be

National authority / EU POC NIS directive

Coordination security evaluation and certification of information and communication systems
STRATEGIC OBJECTIVES

• Accurate and integrated capabilities
• Cyber security governance for public sector and vital sectors, prevention, investigation & response
• Prevent Cyber Crime

@home  @work

Vital Sectors
Operators of essential services, public authorities ...
STRATEGIC OBJECTIVES

@home

• Population
  • Awareness (public campaigns)
  • Botnet Eradication
  • Support Information (dedicated website)

@work

• Companies
  • Directives & guidelines
  • Partnerships
  • Reliable technologies
ACTIONS @ work

- Partnership with the private sector and academics (Cyber Security Coalition)
- Guidelines (publications)
- National Cyber Security Awareness Campaign
- Safeonweb
- Anti-phishing
- Coordinated vulnerability disclosure policies
MEMBERS OF THE CYBER SECURITY COALITION

**Private**
- Proximus
- KBC
- BNP Paribas Fortis
- Delta Lloyd Life
- AG Insurance
- Baloise Group
- ING
- Carrefour
- Allianz
- Ifs.dworx
- H
- Isabel
- Beyond Banking
- SWIFT
- AXA
- SNCB
- Ethias
- Deloitte
- MIVB
- Colruyt Group
- STIB
- NBB

**Federations**
- Vlaams netwerk van ondernemingen
- VBO
- FEB
- AGORIA
- Assuralia
- UWE
- Union wallonne des entreprises

**Universities**
- UCL
- KU Leuven
- Howest
- LDE
- ICHEC
- ULB
- Université de Namur
- Solvay Brussels School Economics & Management

**Public**
- @wt.be
- BIPT
- Vlaamse overheid
- Economist
- Vlaamse overheid
SAFEONWEB

- 1. Antivirus
- 2. Updating your programs
- 3. Making back-ups
- 4. Using strong passwords
- 5. Phishing
- 6. Scan your device

Together we can reduce this number. Take the test on safeonweb.be
Don’t use ‘football’ as password...

...but use ‘WeWillBeTheChampionIn2016!’ as passphrase.

The longer your password the safer it is. A passphrase is long and easier to remember.

More tips? www.safeonweb.be
The Cyber Security KIT: for SMEs and organizations raise awareness about cyber security among their employees.

Help SMEs and organizations raise awareness about cyber security among their employees.

The Cyber Security KIT deals with three topics:

• How do you make **passwords stronger**?
• How can you recognize **phishing e-mails**?
• How can you protect yourself against **social engineering**?

The goal is to provide SMEs with an overview of basic and more advanced cyber security measures.

Where all SMEs should implement cyber security according to the result of their own risk assessments, this guide provides a quick list of security controls that might or should be implemented.

This guide should enable SMEs to improve their cyber security levels, reduce cyber security risks, mitigate vulnerabilities and improve their resilience.

Cyber Security Incident Management guide provides a full and pragmatic approach on how to deal with cyber incidents in an organisation. This guide is not only a brochure, but also provides a practical frame of reference, as it is written by experts in incident management to raise awareness among all organisations on how to prepare for possible problems.
RANSOMWARE

https://www.cert.be/docs/ransomware-how-protect-and-respond.html
03

ETHICAL HACKING
AND COORDINATED VULNERABILITY
DISCLOSURE POLICY (CVDP)
Is « ethical hacking » legal in Belgium?

The answer depends on the context:

(A) knowingly accessing a computer system *without* authorization even without malicious intentions for example: to verify the existence of computer security breaches = it does constitute a criminal offense (external hacking art. 550 bis, § 1 of the Belgian Criminal Code).

(B) knowingly accessing a computer system of a *responsible* organization that has adopted a coordinated vulnerability disclosure policy (CVDP), without malicious intentions and subject to compliance with the conditions of the CVDP for example: to identify security breaches and show the vulnerability + respect other legal provisions (for example: the secrecy of electronic communications) = it does not constitute a criminal offense.

(C) exceeding its powers of access to a computer system *without* malicious intentions (fraudulent or for the purpose of harming) = it does not constitute a criminal offense (internal hacking art, 550 bis, § 2 of the Criminal Code).
❖ **A security hacker**

Someone who seeks to breach defenses and exploit weaknesses in a computer system or network. Hackers may be motivated by a multitude of reasons, such as profit, protest, information gathering, challenge, recreation, or to evaluate system weaknesses to assist in formulating defenses against potential hackers.

❖ **Different type of hackers**

**Black hat**: hacker who accesses without authorization a computer system for malicious reasons or for personal gain.

**White hat (also called ethical hacker)**: hacker who accesses with authorization a computer system for non-malicious reasons, either to test security system, perform penetration tests or vulnerability assessments.

**Grey hat**: hacker who accesses without authorization a computer system for the sole purpose of notifying the administrator system of potential security threats.
Coordinated vulnerability disclosure policies in information and communication technologies

A coordinated disclosure policy of information and communication technologies vulnerabilities is a set of rules previously determined by an organization responsible for a information or communication technology to enable collaboration between it and a security researcher in information and communication technologies or the general public, who wants to search or has discovered a potential security vulnerability in its systems, services or products.

These rules should allow for an eventual disclosure of this security vulnerability in a responsible, coordinated and prepared manner between the security researcher (or the general public) and the responsible organization.
The coordinator.

Coordinator is a natural or legal person who can act as an intermediary between the security researcher in information and communication technologies or the general public and the responsible organization in charge of the system by providing technical, legal or other assistance in order to promote the effectiveness of the collaboration process between these two parties.

In Belgium, this role could be played by default (if no coordinator is specified in the coordinated vulnerability policy) by CERT.be (Federal Computer Emergency Response Team).
Objectives

a) Provide a legal framework for external collaboration, efficient and at low cost

+ Clarify the situation of security researcher in information and communication technologies or general public who wants to search or has found a security vulnerability.

b) Increase the security of information and communication technologies

c) Insure the trust of users information and communication technologies

d) Insure confidentiality or avoid uncoordinated disclosure of a vulnerability

e) Ensure compliance of the responsible organizations with legal obligations of security
PROJECT OF PUBLISHING A GUIDE (to be finalized)

Adoption of a Coordinated Vulnerability Disclosure Policy (published on the website).

Voluntary process

Must be regarded as an prior authorization to access the system under the conditions of the policy

Access with conditions

Exclude the existence of an external hacking offense
CONTENT OF A COORDINATED VULNERABILITY DISCLOSURE POLICY

- Publicity
- Point of contact
- Security of communications
- Description of reciprocal obligations
- Continuous communication
- Coordinated disclosure
1. DISCOVERY
Verification of discovery by the security researcher
Possible drafting of a summary report with technical information and contact details

2. NOTIFICATION
Use of the contact point of the responsible organization and secure means of communication
Sending an acknowledgment of receipt (within 7 calendar days)
Possible participation of a coordinator

3. INVESTIGATION
Communication for further information
Confirmation
Regular feedback to the alert launcher on status and search results

4. POSSIBLE DEVELOPMENT OF A SOLUTION OR AT LEAST INFORMATION TO ESSENTIAL SERVICES USERS
(if possible within 60 calendar days or 6 months for complex cases)
Conduct positive tests to verify that the solution is working properly
Conduct negative tests to ensure that the solution does not disrupt other existing features
Prioritize the solution for essential services operators (within 30 calendar days)

5. COORDINATED DISCLOSURE
Dissemination of information to sellers and users
Deploying the solution
Possibly the coordinated decision not to disclose vulnerability
Example of coordinated vulnerability disclosure policies in Belgium

**Policy:**
http://www.proximus.com/en/group/governance/regulatory-information#title-4

**Webform:**

**E-mail:**
csirt@proximus.com

**Policy:**

**Webform:**

**Policy:**

**E-mail:**
disclosure@b-rail.be
### Example of a bug bounty platform in Belgium

**INTIGRITI**

**ETHICAL HACKER PLATFORM**

<table>
<thead>
<tr>
<th>Company</th>
<th>Projects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UZ Leuven</td>
<td>1</td>
<td>1 ongoing project. Universitaire ziekenhuizen Leuven, often shortened to UZ Leuven, is an academic...</td>
</tr>
<tr>
<td>bpost</td>
<td>2</td>
<td>2 ongoing projects. bpost is Belgium’s leading postal operator and the universal service provider, which me...</td>
</tr>
<tr>
<td>Telenet</td>
<td></td>
<td>2 ongoing projects. Our purpose is to help and inspire our customers to make the most of life and...</td>
</tr>
<tr>
<td>Intigriti</td>
<td>1</td>
<td>1 ongoing project. Intigriti is an ethical hacker platform where users can report security vulnerabilities in...</td>
</tr>
<tr>
<td>Mobile Vikings</td>
<td></td>
<td>1 ongoing project. Mobile Vikings is an mobile operator that focuses on mobile data. Mobile Vikings ...</td>
</tr>
<tr>
<td>Kinepolis</td>
<td></td>
<td>3 ongoing projects. Kinepolis Group was formed in 1997 as a result of the merger of two family-run cinema ...</td>
</tr>
<tr>
<td>ALDE</td>
<td>1</td>
<td>1 ongoing project. Mariette Schaake has been serving as a Member of the European Parliament for...</td>
</tr>
<tr>
<td>Brussels Airlines</td>
<td></td>
<td>1 ongoing project. Brussels Airlines is the flag carrier and largest airline of Belgium based and headquarter...</td>
</tr>
</tbody>
</table>
Thank you for your attention ! Danke für Ihre Aufmerksamkeit !

Mr. Valéry Vander Geeten
Legal Officer
Security Officer - DPO

CENTER FOR CYBER SECURITY BELGIUM
Rue de la Loi 16 - 1000 Brussels

valery.vandergeeten@ccb.belgium.be

www.ccb.belgium.be
www.cert.be
www.safeonweb.be