· Service Description: Security-related Information Dissemination

Definition

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include:

- reporting guidelines and contact information for the RENU-CERT
- archives of alerts, warnings, and other announcements
- documentation about current best practices
- general computer security guidance
- vendor links
- other information that can improve overall security practices

This information is developed and published by the RENU-CERT, and can include information from external resources such as other CSIRTs, vendors, and security experts. This service includes maintaining a public or private archive or knowledge base of vulnerability, artifact or other incident information and corresponding response strategies.

Objective

To **raise awareness** about various threats that exist and could cause serious damage to the constituency. Not only does this improve their understanding of security issues, but it also helps them perform their day-to-day operations in a more secure manner.

Inputs

There exist **three** main types of information sources that contribute information as input for this service:

- Vulnerability information about (the RENU constituency's) IT systems
- Incident reports and Incident handling reports
- Open-source Cyber-threat intelligence feeds

Other sources will include:

- Mailing lists
- Vendor-specific product vulnerability information
- Websites
- Information on the Internet (Google, etc...)
- Partnerships that provide vulnerability information, such as other CSIRTs

Function Description

The service follows a flow as shown in Figure 1 and the sections below.

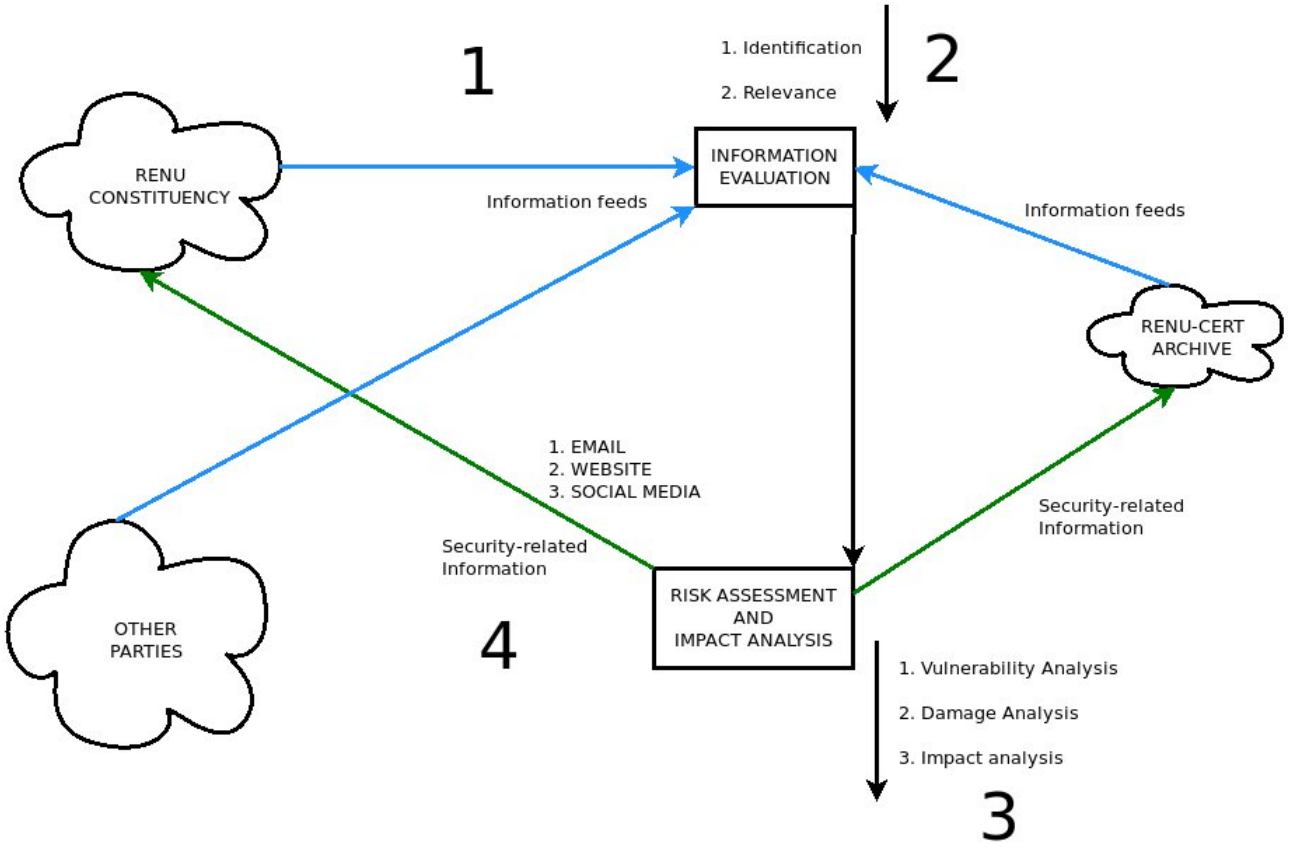

Figure1: Information dissemination flowchart

Information Evaluation

Identification

Incoming information always has to be identified by its **source** and it has to be determined whether the source is **trustworthy** before any information is given to the constituency. Otherwise, people might get falsely alerted, and lead to unnecessary disturbances in business processes.

Relevance

Here, filtering of the incoming vulnerability information on relevance is done, with the goal to find an answer to the questions: "Does the constituency use this piece of software/hardware?"; "Is the information relevant for them?" See Appendix 1.

Risk assessment and Impact analysis

To keep risk analysis simple but effective, the RENU-CERT will use the GOVCERT.NL rating scheme, as explained below.

Vulnerability Analysis

Vulnerability assessment:

RISK	Answer A	Risk Score for A	Answer B	Risk Score for B
Is the vulnerability **widely known**?	No, limited	1	Yes, public	2
Is the vulnerability **widely exploited**?	No	1	Yes	2
Is the vulnerability **easily exploited**?	No, hacker	1	Yes, script kiddie	2
Precondition: **default** configuration?	No, specific	1	Yes, standard	2
Precondition: physical access required?	Yes	1	No	2
Precondition: user account required?	Yes	1	No	2

Vulnerability assessment evaluation:

Total risk score	Risk Level
11,12	HIGH
8,9,10	MEDIUM
6,7	LOW

Damage Analysis

Damage assessment:

RISK	Answer A	Score for A	Answer B	Score for B	Answer C	Score for C
Unauthorised access to data	No	0	Yes, read	2	Yes, read+	4
Denial of Service	No	0	Yes, non-critical	1	Yes, critical	5
Permission	No	0	Yes, user	4	Yes, root / SYSTEM	6

Damage assessment evaluation:

Total risk score	Risk Level
6 – 15	HIGH
2 – 5	MEDIUM
0,1	LOW

Impact Analysis

Impact assessment:

This is a numeric value and can simply be calculated with Equation 1 below:

$$Impact\ Level = Risk\ Level \times Damage\ \ Level$$

Equation1: Impact score

Impact assessment evaluation:

(Risk Level * Damage Level) (commutative)	**Impact Level**	**Action**
HIGH * HIGH HIGH * MEDIUM	HIGH	Immediate action needed
MEDIUM * MEDIUM MEDIUM * LOW	MEDIUM	Action in one week
LOW * LOW	LOW	Include it in general process

Outputs

The information generated from the service will be distributed via various RENU-CERT distribution channels as mentioned in Table 1. A copy of this information will be archived for future use. See for more detail on the format of various disseminated information.

Table1: Content Distribution channels

Channel	**Details**
Email	cert@renu.ac.ug
Website	https://cert.renu.ac.ug (Security Updates section)
Social Media	• Twitter: https://twitter.com/renu_cert

Information types disseminated

This section lists information that will be communicated through **formal** channels i.e. website and email. **Informal** channels like social media **MAY** contain not only references to the same information published/disseminated via the formal channels, but also anything that the RENU-CERT sees as useful to the constituency regarding computer security. This makes social media a more flexible tool to publish/disseminate both formal **and** informal security-related information (for example a Twitter retweet or a picture sent via WhatsApp). Types of information disseminated by the RENU-CERT include:

- **Announcements** – This may include, but is not limited to, intrusion alerts, vulnerability or artifact warnings, and general security advisories. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities,

recently compromised/hacked sites/systems or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited. The RENU-CERT will notify the various parts of the constituency about the vulnerability and will share information about how to fix or mitigate the vulnerability. This service **may** involve communicating with vendors, other CSIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability. Particularly distinct types of announcements include:

- **Advisories** – provide mid-term and long-term information about problems and solutions suitable to raise awareness and help avoid incidents. They typically contain information about new vulnerabilities, but may also contain information about intruder activity. Advisories are typically directed at a technical audience such as system and network administrators, but sometimes contain additional background information for less technical readers.
- **Alerts** – These are short-term notices about critical developments containing time-sensitive information about recent attacks, on-going investigations, successful break-ins, or new vulnerabilities. There may already be complete information regarding the subject of an alert, but something may have changed to require the publication of new information.

Availability

This service is available to the entire RENU constituency; i.e. the RENU member institutions and the team at the RENU Secretariat site.

The service is available **24/7**. Information dissemination through **formal** channels will be done **only** during **working** hours. Information dissemination through **informal** channels may be done at anytime i.e. during working **and** non-working hours.

During the execution of this service, the constituent should **not** expect information to be distributed regularly. It will only be sent in response to newly found information or when the need arises.

Quality assurance

To minimise the verbosity of information distributed to the constituency via email, the RENU-CERT will **only** send, through this channel, information of **HIGH** impact level. The RENU-CERT website will contain information of **all** risk and impact levels, and may be referenced by social media posts.

The rigorousness of the Information Evaluation and Risk Assessment steps will be on a **best-effort** basis for **informal** publications via social media i.e. pictures, videos and/or other social media content.

Interface with other services

During the handling phase of the **Incident Handling service**, the steps necessary to resolve an incident might involve generating alerts to the RENU constituency to minimise its possible spread.

An incident handling report generated at the end to the handling process of the Incident Handling service is archived. The archive of reports also serves as an **input** information source for the this service**,** in that it provides information for generating advisories and announcements. It also provides input into the assessment of the RENU constituency's installation base to better customise the information disseminated by the RENU-CERT to its constituents.

Information disclosure and interaction

No confidential information of any kind and from any party will be disclosed in the distributed information generated by this service.

· APPENDIX

.1 Assess the installation base of the constituency

The first step is to gather an overview of the IT systems installed at your constituency. By this, the RENU-CERT can evaluate the relevance of incoming information and filter it before redistribution, so the constituents will not get overwhelmed with information that is basically useless for them. A simple tool like MS Excel or LibreOffice Calc can be used to generate this list.

Possible information to collect would be:

* - required information

- Category* – e.g. Desktop, Network, Server, Service
- Application* – e.g. Browser, Office suite, Router, Web server
- Software
  - Product Name*
  - Version
- Operating System
  - OS Name*
  - Version
- Constituent

Information Formats

Announcement

- Title
- Reference Number (RENU-CERT:ANNOUNCEMENT:YmdHMSN)

- date +%Y%m%d%H%M%S%N

- Description (details)
- Appendix
  - Reference Links
  - Attachments (if any/necessary) e.g. screenshots

Alert

- Title
- Reference Number (RENU-CERT:ALERT:YmdHMSN) - date +%Y%m%d%H%M%S%N
- Risk Level
- Impact/Damage Level

- Description (details)
- Appendix
  - Reference Links
  - Attachments (if any/necessary) e.g. screenshots

Advisory

- Title
- Reference Number (RENU-CERT:ADVISORY:YmdHMSN) - date +%Y%m%d%H%M%S%N
- Systems affected
- Related OS + version
- Risk Level
- Impact/Damage Level
- External IDs – e.g. CVE numbers
- Overview of the Vulnerability
- Impact
- Solution
- Description (details)
- Appendix
  - Reference Links
  - Attachments (if any/necessary) e.g. screenshots