CSIRT

Pavel Růžička <ruza@ruza.eu>

Brmlab
hackerspace Prague
Lightning talks

June 2016

CSIRT in general

CSIRT in general

Need to define:

CSIRT in general

Need to define:

- Constituency - to whom services are provided

CSIRT in general

Need to define:

- Constituency - to whom services are provided
- Services and teams - what CSIRT offers and who does that

CSIRT in general

Need to define:

- Constituency - to whom services are provided
- Services and teams - what CSIRT offers and who does that
- Contacts - email, ML, GnuPG, etc

CSIRT Service Categories

CSIRT Service Categories

1 Reactive

CSIRT Service Categories

1. Reactive
2. Proactive

CSIRT Service Categories

1. Reactive
2. Proactive
3. Security quality management

CSIRT Service Categories

1. Reactive
   - Reactive services - triggered by an **event or request, such as a report** of a compromised host, widespread malicious code, SW vulnerability, or something identified by an IDS or logging system.
2. Proactive

3. Security quality management

CSIRT Service Categories

1. Reactive
   - Reactive services - triggered by an **event or request, such as a report** of a compromised host, widespread malicious code, SW vulnerability, or something identified by an IDS or logging system.
2. Proactive
   - Proactive services - **assistance and information** to help **prepare, protect, and secure** constituent systems in anticipation of attacks, problems, or events.
3. Security quality management

CSIRT Service Categories

1. Reactive
   - Reactive services - triggered by an **event or request, such as a report** of a compromised host, widespread malicious code, SW vulnerability, or something identified by an IDS or logging system.
2. Proactive
   - Proactive services - **assistance and information** to help **prepare, protect, and secure** constituent systems in anticipation of attacks, problems, or events.
3. Security quality management
   - Security quality services - IT **audit, or training**, identify risks, threats, and system weaknesses

Reactive Services

Reactive Services

- respond to requests for assistance, **reports of incidents from the CSIRT** constituency

Reactive Services

- respond to requests for assistance, **reports of incidents from the CSIRT** constituency
- any **threats or attacks against CSIRT systems**.

Reactive Services

- respond to requests for assistance, **reports of incidents from the CSIRT** constituency
- any **threats or attacks against CSIRT systems**.
- Some services may be initiated by **third-party notification** or by viewing **monitoring or IDS logs** and alerts.

Reactive Services

- Alerts and Warnings

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Reactive Services - Alerts and Warnings

Short-term recommendation for dealing with the resulting problem.

The **alert, warning, or advisory** as a reaction to:

Reactive Services - Alerts and Warnings

Short-term recommendation for dealing with the resulting problem.
The **alert, warning, or advisory** as a reaction to:

- intruder attack
- security vulnerability
- intrusion alert
- computer virus
- hoax

Reactive Services - Incident Handling

? The only CSIRT prerequisite

Providing an incident handling service is the only prerequisite to being considered a CSIRT. That means **responding to requests and reports**, and **analyzing incidents and events**.

Reactive Services - Incident Handling

? The only CSIRT prerequisite

Providing an incident handling service is the only prerequisite to being considered a CSIRT. That means **responding to requests and reports**, and **analyzing incidents and events**.

- **Incident analysis** - info, scope, damage, forensic evidence, tracking source

Reactive Services - Incident Handling

? The only CSIRT prerequisite

Providing an incident handling service is the only prerequisite to being considered a CSIRT. That means **responding to requests and reports**, and **analyzing incidents and events**.

- **Incident analysis** - info, scope, damage, forensic evidence, tracking source
- Incident response on site - N/A

Reactive Services - Incident Handling

? The only CSIRT prerequisite

Providing an incident handling service is the only prerequisite to being considered a CSIRT. That means **responding to requests and reports**, and **analyzing incidents and events**.

- **Incident analysis** - info, scope, damage, forensic evidence, tracking source
- Incident response on site - N/A
- Incident response support - assists and guides the victim(s) of the attack (phone, email, fax, documentation) - DUNNO

Reactive Services - Incident Handling

? The only CSIRT prerequisite

Providing an incident handling service is the only prerequisite to being considered a CSIRT. That means **responding to requests and reports**, and **analyzing incidents and events**.

- **Incident analysis** - info, scope, damage, forensic evidence, tracking source
- Incident response on site - N/A
- Incident response support - assists and guides the victim(s) of the attack (phone, email, fax, documentation) - DUNNO
- Incident response coordination - N/A

brmlab hackerspace prague

Reactive Services - Vulnerability Handling

Receiving information about HW and SW vulnerabilities, **analyzing** vulnerabilities, **developing response** for detecting and repairing the vulnerabilities.

Reactive Services - Vulnerability Handling

Receiving information about HW and SW vulnerabilities, **analyzing** vulnerabilities, **developing response** for detecting and repairing the vulnerabilities.

- Vulnerability analysis - **technical analysis** of HW and SW vulnerabilities. Source **code review, debugging, reproducing** problem on a test system.

Reactive Services - Vulnerability Handling

Receiving information about HW and SW vulnerabilities, **analyzing** vulnerabilities, **developing response** for detecting and repairing the vulnerabilities.

- Vulnerability analysis - **technical analysis** of HW and SW vulnerabilities. Source **code review, debugging, reproducing** problem on a test system.
- Vulnerability response - determining the appropriate **response, patches, fixes, and workarounds**.

Reactive Services - Vulnerability Handling

Receiving information about HW and SW vulnerabilities, **analyzing** vulnerabilities, **developing response** for detecting and repairing the vulnerabilities.

- Vulnerability analysis - **technical analysis** of HW and SW vulnerabilities. Source **code review, debugging, reproducing** problem on a test system.
- Vulnerability response - determining the appropriate **response, patches, fixes, and workarounds**.
- Vulnerability response coordination - N/A

Reactive Services - Artifact Handling

- Artifact analysis - **review** of an objects found on a system involved in probing or attacking systems/networks. i.e **viruses, trojans, worms, exploit scripts and toolkits**.

Reactive Services - Artifact Handling

- Artifact analysis - **review** of an objects found on a system involved in probing or attacking systems/networks. i.e **viruses, trojans, worms, exploit scripts and toolkits**.
- Artifact response - develop **response strategies to detect, remove and defend**

Reactive Services - Artifact Handling

- Artifact analysis - **review** of an objects found on a system involved in probing or attacking systems/networks. i.e **viruses, trojans, worms, exploit scripts and toolkits**.
- Artifact response - develop **response strategies to detect, remove and defend**
- Artifact response coordination - N/A

Proactive services

Proactive Services

- improve the **infrastructure** and **security processes** of the constituency

Proactive Services

- Announcements

Proactive Services

- Announcements
- Technology Watch

Proactive Services

- Announcements
- Technology Watch
- Security Audits or Assessments

Proactive Services

- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and Maintenance of Security Tools, Applications, and Infrastructures

Proactive Services

- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and Maintenance of Security Tools, Applications, and Infrastructures
- Development of Security Tools

Proactive Services

- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and Maintenance of Security Tools, Applications, and Infrastructures
- Development of Security Tools
- Intrusion Detection Services

Proactive Services

- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and Maintenance of Security Tools, Applications, and Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Proactive Services - Announcements

- Intrusion alerts

Proactive Services - Announcements

- Intrusion alerts
- vulnerability warnings

Proactive Services - Announcements

- Intrusion alerts
- vulnerability warnings
- security advisories.

Proactive Services - Announcements

- Intrusion alerts
- vulnerability warnings
- security advisories.

Such announcements inform constituents about new developments with **medium- to long-term** impact, such as newly found vulnerabilities or intruder tools.

Proactive Services - Technology Watch

- This service involves **reading security mailing lists, web sites, news and journal articles** in the fields of science, technology, politics, and government. CSIRT monitors new **technical developments, intruder activities**, and related **trends** to help identify **FUTURE THREATS**.

Proactive Services - Technology Watch

- This service involves **reading security mailing lists, web sites, news and journal articles** in the fields of science, technology, politics, and government. CSIRT monitors new **technical developments, intruder activities**, and related **trends** to help identify **FUTURE THREATS**.
- can be OPTIONALY expanded to include **legal** and **legislative rulings, social** or **political threats**, and **emerging technologies**.

Proactive Services - Technology Watch

- This service involves **reading security mailing lists, web sites, news and journal articles** in the fields of science, technology, politics, and government. CSIRT monitors new **technical developments, intruder activities**, and related **trends** to help identify **FUTURE THREATS**.
- can be OPTIONALY expanded to include **legal** and **legislative rulings, social** or **political threats**, and **emerging technologies**.

- The outcome of this service might be some type of **announcement, guidelines, or recommendations** focused at more medium- to long-term security issues.

brmlab hackerspace prague

Proactive Services - Security Audits or Assessments

Review and analysis of an organization's **security infrastructure**, security practices, based on the requirements defined by the organization or industry standards.

Proactive Services - Security Audits or Assessments

Review and analysis of an organization's **security infrastructure**, security practices, based on the requirements defined by the organization or industry standards.

- Infrastructure review

Proactive Services - Security Audits or Assessments

Review and analysis of an organization's **security infrastructure**, security practices, based on the requirements defined by the organization or industry standards.

- Infrastructure review
- Best practice review

Proactive Services - Security Audits or Assessments

Review and analysis of an organization's **security infrastructure**, security practices, based on the requirements defined by the organization or industry standards.

- Infrastructure review
- Best practice review
- Scanning

Proactive Services - Security Audits or Assessments

Review and analysis of an organization's **security infrastructure**, security practices, based on the requirements defined by the organization or industry standards.

- Infrastructure review
- Best practice review
- Scanning
- Penetration testing

Proactive Services - Configuration and Maintenance of Security Tools, Applications, and Infrastructures

Configuration updates and maintenance of security tools and services.

Proactive Services - Configuration and Maintenance of Security Tools, Applications, and Infrastructures

Configuration updates and maintenance of security tools and services.

- IDS, network scanning or monitoring systems, filters, wrappers, firewalls, VPNs, or authentication mechanisms

Proactive Services - Configuration and Maintenance of Security Tools, Applications, and Infrastructures

Configuration updates and maintenance of security tools and services.

- IDS, network scanning or monitoring systems, filters, wrappers, firewalls, VPNs, or authentication mechanisms
- configure and maintain servers, desktops, laptops, personal digital assistants (PDAs), and other wireless devices according to security guidelines.

Proactive Services - Development of Security Tools

developing security **patches**, secured SW **distributions, tools or scripts** that extend existing security tools, network scanners, scripts, or automated patch distribution mechanisms.

Proactive Services - Intrusion Detection Services

review existing IDS logs, analyze and initiate a response

Proactive Services - Security-Related Information Dissemination

provides comprehensive and **easy-to-find collection of useful information** that aids in improving security.

Security Quality Management Services

Security Quality Management Services

- Risk analysis

Security Quality Management Services

- Risk analysis
- Business Continuity and Disaster Recovery Planning

Security Quality Management Services

- Risk analysis
- Business Continuity and Disaster Recovery Planning
- Security Consulting

Security Quality Management Services

- Risk analysis
- Business Continuity and Disaster Recovery Planning
- Security Consulting
- Awareness Building

Security Quality Management Services

- Risk analysis
- Business Continuity and Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education/Training

Security Quality Management Services

- Risk analysis
- Business Continuity and Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation or Certification

Security Quality Management Services

lessons learned from reactive and proactive services turned into security quality management process can improve the long-term security efforts in an organization.

Security Quality Management Services -Risk analysis

Conduct or assist with **risk analysis** for new systems and business processes.

Security Quality Management Services - Business Continuity and Disaster Recovery Planning

involved in **business continuity** and **disaster recovery planning** for events related to threats and attacks.

Security Quality Management Services - Security Consulting

provide advice and guidance..

Security Quality Management Services - Security Consulting

provide advice and guidance..

- best **security practices** to implement for business operations.

Security Quality Management Services - Security Consulting

provide advice and guidance..

- best **security practices** to implement for business operations.
- developing organizational **security policies**.

Security Quality Management Services - Security Consulting

provide advice and guidance..

- best **security practices** to implement for business operations.
- developing organizational **security policies**.
- **legislative**

Security Quality Management Services - Awareness Building

- developing **articles, posters, newsletters, web**, etc that explain security best practices and provide advice.

Security Quality Management Services - Awareness Building

- developing **articles, posters, newsletters, web**, etc that explain security best practices and provide advice.
- may also include meetings and seminars to keep constituents up to date.

Security Quality Management Services - Education/Training

seminars, workshops, courses, and **tutorials**

Security Quality Management Services - Education/Training

seminars, workshops, courses, and **tutorials** topics:

Security Quality Management Services - Education/Training

seminars, workshops, courses, and **tutorials** topics:

- incident reporting guidelines

Security Quality Management Services - Education/Training

seminars, workshops, courses, and **tutorials** topics:

- incident reporting guidelines
- appropriate response methods

Security Quality Management Services - Education/Training

seminars, workshops, courses, and **tutorials** topics:

- incident reporting guidelines
- appropriate response methods
- incident response tools

Security Quality Management Services - Education/Training

seminars, workshops, courses, and **tutorials** topics:

- incident reporting guidelines
- appropriate response methods
- incident response tools
- incident prevention methods

Security Quality Management Services - Education/Training

seminars, workshops, courses, and **tutorials** topics:

- incident reporting guidelines
- appropriate response methods
- incident response tools
- incident prevention methods
- other info to protect, detect, report, and respond to computer security incidents.

Security Quality Management Services - Product Evaluation or Certification

Product evaluations on tools, applications, or other services to ensure the security of the products

Volunteers?