CSIRT
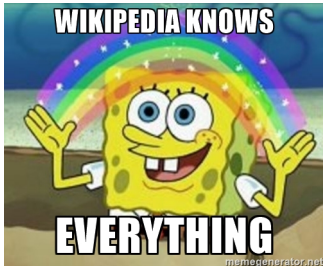
Pavel Růžička <ruza@ruza.eu>

Brmlab
hackerspace Prague
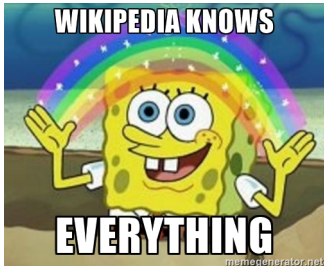Lightning talks

November 2016

CSIRT in general

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   Security Quality Management Services
●○○   ○   ○○○○○○   ○○○○○○○   ○○○○○○○○○○

CSIRT in general

WTF is an CSIRT?

WTF is an CSIRT?

Computer Security

CSIRT in general	CSIRT Service Categories	Reactive Services	Proactive services	Security Quality Management Services
●○○	○	○○○○○○	○○○○○○○	○○○○○○○○○○

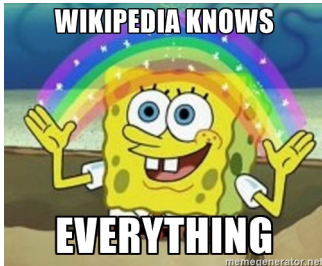CSIRT in general
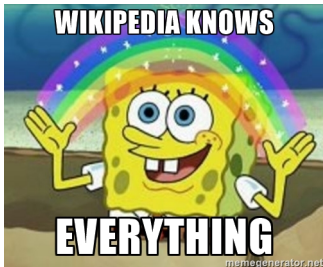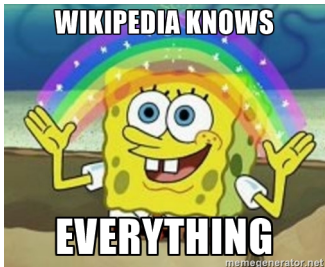
WTF is an CSIRT?

Computer Security Incident Response

WTF is an CSIRT?

Computer Security Incident Response Team (CSIRT)

CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services
●○○ | ○ | ○○○○○○ | ○○○○○○○ | ○○○○○○○○○○

CSIRT in general

WTF is an CSIRT?

Computer Security Incident Response Team (CSIRT)
Computer Emergency

CSIRT in general	CSIRT Service Categories	Reactive Services	Proactive services	Security Quality Management Services
●○○	○	○○○○○○	○○○○○○○	○○○○○○○○○○

CSIRT in general

WTF is an CSIRT?

Computer Security Incident Response Team (CSIRT)
Computer Emergency Response

CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services

CSIRT in general

WTF is an CSIRT?

Computer Security Incident Response Team (CSIRT)
Computer Emergency Response Team (CERT)

CSIRT in general	CSIRT Service Categories	Reactive Services	Proactive services	Security Quality Management Services
●○○	○	○○○○○○	○○○○○○○	○○○○○○○○○○

CSIRT in general

WTF is an CSIRT?

Computer Security Incident Response Team (CSIRT)
Computer Emergency Response Team (CERT)
Hackerspaces and CSIRTs are both organizations that are focused on
computer security, so they can benefit from each others.

| CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services |
| ○●○ | ○ | ○○○○○○ | ○○○○○○○ | ○○○○○○○○○○ |

CSIRT in general

CSIRT types

- listed(136)
- accredited (121)
- certified (17)

The Trusted Introducer maintains the European database of CSIRTs.

`www.trusted-introducer.org/directory/teams.html`

@brmlab
hackerspace prague

Constituency types (Nov 2016)

- Research and Education (68)
- Government (60)
- Commercial Organisation (58)
- Service Provider Customer Base (40)
- ISP Customer Base (37)
- Financial Sector (33)
- National (32)
- Military (13)
- CIIP (13)
- Vendor Customer Base (11)
- Non-Commercial Organisation (9)
- Law Enforcement (3)

CSIRT Service Categories

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   Security Quality Management Services
000   ●   000000   0000000   0000000000

Categories

CSIRT Service Categories

- **Reactive** services

- **Proactive** services

- **Security quality management** services

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   Security Quality Management Services
○○○   ●   ○○○○○○   ○○○○○○○   ○○○○○○○○○○

Categories

CSIRT Service Categories

- **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.

- **Proactive** services

- **Security quality management** services

CSIRT in general	CSIRT Service Categories	Reactive Services	Proactive services	Security Quality Management Services
○○○	●	○○○○○○	○○○○○○○	○○○○○○○○○○

Categories

CSIRT Service Categories

- **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.

- **Proactive** services

    assistance and information to help **prepare, protect, and
    secure** constituent systems in anticipation of attacks, problems, or
    events.

- **Security quality management** services

| CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services |
| 000 | ● | 000000 | 0000000 | 0000000000 |

Categories

CSIRT Service Categories

- **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.

- **Proactive** services

    assistance and information to help **prepare, protect, and secure** constituent systems in anticipation of attacks, problems, or events.

- **Security quality management** services

    IT **audit, or training**, identify risks, threats, and system weaknesses

brmlab
hackerspace prague

Pavel Růžička <ruza@ruza.eu>   CSIRT

Reactive Services

| CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services |
| 000 | o | ●00000 | 0000000 | 0000000000 |

Reactive Services

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.

CSIRT in general	CSIRT Service Categories	**Reactive Services**	Proactive services	Security Quality Management Services
000	0	0●0000	0000000	0000000000

Reactive Services

Reactive Services

3 Vulnerability Handling

1 Alerts and Warnings

2 Incident Handling

4 Artifact Handling

| CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services |
| 000 | 0 | 0●0000 | 0000000 | 0000000000 |

Reactive Services

Reactive Services

1 Alerts and Warnings

2 Incident Handling
   - Incident analysis
   - Incident response on site
   - Incident response support
   - Incident response coordination

3 Vulnerability Handling
   - Vulnerability analysis
   - Vulnerability response
   - Vulnerability response coordination

4 Artifact Handling
   - Artifact analysis
   - Artifact response
   - Artifact response coordination

brmlab
hackerspace prague

CSIRT in general CSIRT Service Categories **Reactive Services** Proactive services Security Quality Management Services
○○○   ○   ○○●○○○   ○○○○○○○   ○○○○○○○○○○

Reactive Services

Reactive.1 - 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

| CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services |
| 000 | 0 | 000●00 | 0000000 | 0000000000 |

Reactive Services

Reactive.2 - 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
- Incident response support - assists and guides the victim(s) of the attack (phone, email, fax, documentation)
- Incident response coordination

| CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services |
| 000 | o | 0000●0 | 0000000 | 0000000000 |

Reactive Services

Reactive.3 - Vulnerability Handling

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

Reactive.3 - 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

| CSIRT in general | CSIRT Service Categories | **Reactive Services** | Proactive services | Security Quality Management Services |
| 000 | 0 | 00000● | 0000000 | 0000000000 |

Reactive Services

Reactive.4 - 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

Proactive services

Proactive Services

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

Proactive Services

1 Announcements

2 Technology Watch

3 Security Audits or Assessments

4 Configuration and Maintenance of Security Tools, Applications, and Infrastructures

5 Development of Security Tools

6 Intrusion Detection Services

7 Security-Related Information Dissemination

Proactive.1 - 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.

| CSIRT in general | CSIRT Service Categories | Reactive Services | **Proactive services** | Security Quality Management Services |
| 000 | 0 | 000000 | 0●00000 | 0000000000 |

Proactive services

Proactive.2 - 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 OPTIONALLY 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.

Proactive.3 - 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.4 - 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.

brmlab
hackerspace prague

CSIRT in general | CSIRT Service Categories | Reactive Services | **Proactive services** | Security Quality Management Services
○○○ | ○ | ○○○○○○ | ○○○○●○○ | ○○○○○○○○○○

Proactive services

Proactive.5 - 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.

CSIRT in general | CSIRT Service Categories | Reactive Services | **Proactive services** | Security Quality Management Services
○○○ | ○ | ○○○○○○ | ○○○○○●○ | ○○○○○○○○○○

Proactive services

Proactive.6 - Intrusion Detection Services

review existing IDS logs, analyze and initiate a response

CSIRT in general CSIRT Service Categories Reactive Services **Proactive services** Security Quality Management Services
000   0   000000   000000●   0000000000

Proactive services

Proactive.7 - Security-Related Information Dissemination

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

Security Quality Management Services

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   Security Quality Management Services
000   0   000000   0000000   ●000000000

Security Quality Management Services

Security Quality Management Services

lessons learned

CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | Security Quality Management Services
000 | 0 | 000000 | 0000000 | ●00000000

Security Quality Management Services

Security Quality Management Services

lessons learned

from **reactive and proactive services**

CSIRT in general CSIRT Service Categories Reactive Services Proactive services Security Quality Management Services
○○○   ○   ○○○○○○   ○○○○○○○   ●○○○○○○○○○

Security Quality Management Services

Security Quality Management Services

lessons learned

from **reactive and proactive services**

turned into **security quality management process**

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   Security Quality Management Services
000   0   000000   0000000   ●000000000

Security Quality Management Services

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 organizations.

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   Security Quality Management Services
000   0   000000   0000000   0●00000000

Security Quality Management Services

Security Quality Management Services

1 Risk analysis

2 Business Continuity and Disaster Recovery Planning

3 Security Consulting

4 Awareness Building

5 Education/Training

6 Product Evaluation or Certification

brmlab
hackerspace prague

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   **Security Quality Management Services**
000   0   000000   0000000   00●0000000

Security Quality Management Services

Security Quality Management Services.1 -Risk analysis

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

CSIRT in general CSIRT Service Categories Reactive Services Proactive services Security Quality Management Services
000   0   000000   0000000   0000●000000

Security Quality Management Services

Security Quality Management Services.2 - Business Continuity and Disaster Recovery Planning

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

CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | **Security Quality Management Services**
○○○ | ○ | ○○○○○○ | ○○○○○○○ | ○○○○●○○○○○

Security Quality Management Services

Security Quality Management Services.3 - Security Consulting

provide advice and guidance..

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

Security Quality Management Services.4 - 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.

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   **Security Quality Management Services**
000   0   000000   0000000   0000000●000

Security Quality Management Services

Security Quality Management Services.5 - Education/Training

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

CSIRT in general | CSIRT Service Categories | Reactive Services | Proactive services | **Security Quality Management Services**
000 | 0 | 000000 | 0000000 | 0000000●000

Security Quality Management Services

Security Quality Management Services.5 - Education/Training

seminars, workshops, courses, and **tutorials** on 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.

CSIRT in general   CSIRT Service Categories   Reactive Services   Proactive services   Security Quality Management Services
000   0   000000   0000000   0000000●00

Security Quality Management Services

Security Quality Management Services.6 - Product Evaluation or Certification

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

HowTo create an CSIRT

Need to define:

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

Register

CSIRT in general
○○○

CSIRT Service Categories
○

Reactive Services
○○○○○○

Proactive services
○○○○○○○

Security Quality Management Services
○○○○○○○○○○●

Volunteers?

Volunteers?