



Why do I need a CSIRT?

Przemyslaw Jaroszewski

CERT Polska

Przemyslaw.Jaroszewski@cert.pl

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 1

Why bother with security? (1)

Security threats are real

- Windows server from the box has CodeRed and backdoors within few hours
- 10 minutes online is enough to get scanned
- Slammer has flooded the Internet, infecting all vulnerable hosts in 7 minutes

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 2

Why bother with security? (2)

Ignoring threats costs resources

- DoS - It costs to be offline
- Data theft – Backups don't help much when sensitive information is stolen
- Compromise – How much does your reputation cost?

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 3



What is a CSIRT? (1)

A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental, or educational organization; a region or country; a research network; or a paid client. (CERT/CC)

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 4

What is a CSIRT? (2)

Basic framework for a CSIRT must include:

- mission statement (what to do?)
- constituency (for whom?)
- place in organization (position in structure, risk management)
- relationship with others (who to cooperate with? whom to trust?)

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 5

What is a CSIRT? (3)

- Reactive services (vulnerability handling alerts, incident & artifacts handling)
- Proactive services (announcements, security audits, security tools development, configuration & maintenance, intrusion detection, information dissemination)
- Security Quality (risk analysis, disaster recovery planning, consulting, education, product evaluation)

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 6

Why does it help?

- Prevention is better than cure
- Small things often protect you from great disasters
- Cooperation always pays
- End-user awareness = less headaches

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 7

How do I make money?

- After careful risk assesment you save far more than you spend
- Build your reputation
- You may offer services to your customers as added value or on commercial basis

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 8

How do I start?

- Define the basic framework
- Establish fundamental policies (CoC, information categorization & disclosure, media, etc.)
- Security policy most likely needs an update
- Train your staff
- Launch the incident handling system
- Spread the word in your community
- Establish contacts with other teams

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 9

What other teams?

- TERENA TF-CSIRT –
<http://www.terena.nl/tech/task-forces/tf-csirt/>
- Trusted Introducer –
<http://www.ti.terena.nl/>
- FIRST Community –
<http://www.first.org/>
- Earn reputation & benefit from first-hand information

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 10

Got any leaflets?

- CSIRT FAQ -
http://www.cert.org/csirts/csirt_faq.html
- Handbook for CSIRTs –
<http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- TRANISTS –
<http://www.ist-transits.org/>

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska
Przemyslaw.Jaroszewski@cert.pl

Slide: 11



Thank you for your time

Contact:

Przemyslaw Jaroszewski

CERT Polska / NASK

Przemyslaw.Jaroszewski@cert.pl

<http://www.cert.pl/>

Why do I need a CSIRT?

Przemyslaw Jaroszewski, CERT Polska

Przemyslaw.Jaroszewski@cert.pl

Slide: 12