Managing Internet Related Security Risks

Q-CERT

ict قطر QATAR

Steve Huth
18 January 2006

Overview of Today's Talk

A look at the security problem(s)

What are the benefits of having a Computer Security Incident Response Team (CSIRT) in your organization?

How can organizations like Q-CERT help?

Security isn't what it used to be…

1988

- exploiting passwords
- exploiting known vulnerabilities

Today

- exploiting passwords
- exploiting known vulnerabilities
- exploiting protocol flaws
- zero-day exploits
- examining source files for new security flaws
- probing systems for known types of flaws
- abusing web servers, email
- DNS attacks
- installing sniffer programs
- IP source address spoofing
- distributed denial of service attacks
- widespread, automated scanning of the Internet
- low and slow attacks
- phishing and other forms of social engineering
- redirecting traffic to fraudulent sites
- and more…

Growing Threats, Vulnerabilities and Risks

Threats

- Disgruntled Employees
- Hackers
- Organized Crime
- Competitors
- Cyber Terrorists
- Governments

Vulnerabilities

- OS
- Network
- Applications
- Databases
- PCs, PDA, Phones
- Middleware
- eCommunities (eGovernment, eCommerce, etc)

Risks

- Disclosure of Customer Records
- Sabotage of Operations/Service
- Extortion
- Theft of Trade Secrets
- EFT Fraud
- Loss of Client Confidence
- Legal Liability

Common Responses to Security Problems

Ad-hoc

Heroic individuals

“We had a problem… but we fixed it.”

And my personal favorite…

“There’s no problem here!”

Solving These Problems Requires Trusted Partners

It’s not just technology.

It requires awareness and action at all levels of an organization.

It requires a thoughtful approach to where we spend our time and money.

It’s not your problem or my problem,
it’s our problem.

What can you do to help manage risk in your organization?

Provide appropriate protection for your information assets

Consider an organizational Computer Security Incident Response Team (CSIRT)

- Handling security incidents and reporting observations
- Managing vulnerabilities in your infrastructure
- Training and awareness
- Organizational perspective

CSIRT Benefits

Predictable response to incidents

- Staff know who to call
- Management know how they will respond

Faster and more reliable response

Fewer issues missed

Appropriate protection for your most important information assets

Partnership with your staff and management

- Trust
- Open communication
- Confidentiality

Process improvements

Create partnerships with other organizations

Organizations with a broader perspective

- RIPE
- Q-CERT
- FIRST

RIPE NCC Focus Points[1]

Reliable and Stable Technical Co-ordination of Internet Number Resources

High Quality Services for Operators and the Internet Community

- As a neutral, credible and authoritative source of network and Internet-related information, the RIPE NCC will continue to supply timely, accurate and tailored services to operators and the Internet community.

Security of Internal IT Infrastructure and Services

- The RIPE NCC will focus on IT security activities to further secure its internal IT infrastructure and services.

[1] RIPE NCC Activity Plan 2006

RIPE NCC Focus Points[1]

Reliable and Stable Technical Co-ordination of Internet Number Resources

High Quality Services for Operators and the Internet Community

- As a neutral, credible and authoritative source of network and Internet-related information, the RIPE NCC will continue to supply timely, accurate and tailored services to operators and the Internet community.

Security of Internal IT Infrastructure and Services

- The RIPE NCC will focus on IT security activities to further secure its internal IT infrastructure and services.

[1] RIPE NCC Activity Plan 2006

Q-CERT

Established by ictQATAR and Carnegie Mellon University

Q-CERT will build cyber security capability and capacity in government and private sector organizations in Qatar and the Gulf region by:

- Providing accurate and timely information on current and emerging cyber threats and vulnerabilities
- Responding to significant threats and vulnerabilities in critical infrastructures by conducting and coordinating activities needed to resolve the threats
- Serving as a central, trusted partner in security incident reporting and analysis
- Promoting and facilitating the adoption of standards, processes, methods, and tools that are most effective at mitigating the evolving risks
- Providing unbiased information and training to build the management and technical skills needed for organizations to effectively manage their cyber risks

Q-CERT Benefits

Objective information on current and emerging cyber threats and vulnerabilities

Help raise security awareness among senior management

Local training on security

Regional perspective

Connection to CERT and the FIRST community

Assistance with large-scale attacks

A forum for discussing security issues important to you

A trusted partner in improving security

Summary

To improve organizational security we must work together.

Provide appropriate protection for your information assets.

A CSIRT for your organization can help you manage your risk.

Q-CERT will help build capability and capacity in your organization, the nation, and the region.

Contact Information

Thank you!

For more information about Q-CERT:

q-cert@cert.org

or

Steve Huth
shuth@cert.org

Thank you!

Background Slides

The Role of FIRST

Forum for Incident Response and Security Teams (FIRST)

Members develop and share technical information, tools, methodologies, processes, & best practices

Promotes the creation of incident response teams

See www.first.org

System Operators

Establish comprehensive risk management programs that:

are focused on the survivability of the organization’s missions/business objectives

examine threats and risks to critical assets

produce practice-based risk mitigation and protection strategies

have an enterprise-wide focus – including supply chains and collaborators/partners

adapt to changing threats and vulnerabilities over time