Handouts: 1992 First Workshop

Policies and Planning Can Prevent Security Incidents

Eugene Spafford
Department of Computer Sciences
1398 Computer Science Building
Purdue University
West Lafayette, IN 47907-1398
spaf@cs.purdue.edu
August 1992

Is This Your Users?

"Why should I worry about this security stuff anyhow? There's nothing on my machine that is worth anything? What do I have to lose?"

– or –

" I didn't know I wasn't supposed to give out my password to the folks at "2600 Magazine."

© 1992 E. H. Spafford

Handouts: 1992 First Workshop

Is This Your staff?

“ He’s had the password “wizard” for the last 5 years now. All his secretaries knew it. But he’s the VP of Engineering and we can’t force him to change it. ”

– or –

“ I didn’t know who to call when the alarm went off. I figured it could wait until morning when you got in, though. ”

3

Is This You?

“ I’m not sure what it is I’m guarding. I’m not even sure what I’m guarding it against. But I can assure you – it’s got the best protection money can buy! ”

4

© 1992 E. H. Spafford

Handouts: 1992 First Workshop

Three Common Failures

- **Organization has no formal policy. Thus,personnel cannot *consistently* make necessary decisions.**
- **Organization has no reasonable response plans for violations, incidents, and disasters.**
- **Plans don't work when needed because they haven't been regularly tested, updated, and rehearsed.**

5

Policy

6

© 1992 E. H. Spafford

Handouts: 1992 First Workshop

Security as Software Engineering

- You need requirements – policy
- You make specifications based on requirements – security guidelines
- You build according to specifications – operational implementation
- You test according to specifications and requirements (verification and validation) – penetration testing, response rehearsals, auditing, etc.
- You debug – incident response

7

Security Policy

- You need to know what you are protecting
- You need to know why it needs protecting
- You need to know its value
- You need a clear statement of responsibility
- You need a clear statement of authority

8

© 1992 E. H. Spafford

Handouts: 1992 First Workshop

Policy

Your policy should be short and easy to understand.

Questions and conflicts should be resolvable by referring to the policy statement.

Responsibilities should be paired with authority.

Policy specifies guards for *people* as well as data – specify rights, too.

Policy guards property, reputation, continuation of business as well as data.

Policy is public…and should be.

9

In Your Policy

Include

- **Statement of purpose**
- **Who labels data & access**
- **Who does audit**
- **Who does response**
- **Who sets guidelines and standards**

Don't Include

- **Names of personnel**
- **Names of products**
- **Names of specific standards or levels**

10

© 1992 E. H. Spafford

Handouts: 1992 First Workshop

In Your Policy

Include

- Who is allowed access
- Who authorizes access
- Disaster planning
- Individual responsibilities
- Role of outsiders
- Appropriate use
- Ownership of data
- Privacy of data
- Penalties
- Priorities
- Unauthorized copies

11

Security Guidelines

Guidelines should be set based on need, economics, circumstances, and threat.

Guidelines should be platform-independent.

Guidelines should evolve slowly and codify successful practice.

Guidelines embody standards of performance and metrics to measure that performance.

Guidelines should include steps for periodic review.

12

© 1992 E. H. Spafford

Guidelines include:

- How backups are done (frequency, storage, etc)
- Audit procedures
- Importation of new software
- Addition of new equipment/repair
- Networking and telecommunications issues (may include encryption)
- Physical security
- Disaster recovery

13

Per-system Guidelines

These are specific to the machine, environment, and software involved.

One person should be accountable for implementing these guidelines.

These may change frequently and be very variable.

14

© 1992 E. H. Spafford

Plans

15

Plan Ahead

Plan what to do in the event of a problem.

Have resources ready and waiting in case you need them.

…the worst time to decide a plan of action is when you need to implement it!

16

© 1992 E. H. Spafford

Handouts: 1992 First Workshop

Planning

Decide what you have on your system, and how important it is to protect.

Do you have adequate resources and personnel involved? Insurance? Hot spares? Contingency sites?

Who needs to be involved? Notified? Warned?

Anticipate threats: level of sophistication, internal/external, duration, severity.

…all your plans should be consistent with a sound risk assessment and with overall policy.

17

Decisions to Make in Advance

- **How important is resumed operation?**
- **How important is formal (legal) action?**
- **How important is information loss?**
- **How important is integrity checking?**
- **Does it matter who hears of the problem?**

18

© 1992 E. H. Spafford

More Planning

For each threat, develop a plan of action to counter it.

For each asset, develop a plan to safeguard it.

Identify key personnel involved.

Identify key tools to be used.

19

Six Parts to Plan

- **Identify and nullify the problem**
- **Identify and fix the source of the problem**
- **Survey the system for other damage**
- **Preserve the evidence**
- **Restore the system.**
- **Cleanup and damage control**

20

© 1992 E. H. Spafford

Things to anticipate

- Break-in
- Virus/worm
- Power loss
- Fire
- Restricted Access
- Mass absence
- Alarm failure
- Vendor failure
- Building loss
- Key person loss
- Communications problems
- Theft
- Audit discrepancy

21

Practice and Refine

22

© 1992 E. H. Spafford

Practice

Actually walk through your plans. Try every step. Involve every alternative within reason.

Involve all external personnel as well as internal personnel.

Have announced and unannounced drills.

Test your backups regularly!

23

Review plans

- **When you change personnel**
- **When you upgrade software**
- **When you upgrade hardware**
- **After any incident response**
- **Periodically**

24

© 1992 E. H. Spafford