WORDPRESS INCIDENT RESPONSE

How planning for the worst protects your site today

MIKEY VEENSTRA

@HEYITSMIKEYV

- Wordfence Threat Analyst
- Security Researcher
- Ethical Hacker
- Locksport Hobbyist
- World’s Greatest Dad*

* Disputed

We don’t need a fire escape plan because:

We don't need a fire escape plan because:

WE DON'T START FIRES

We don’t need a fire escape plan because:

WE’VE GOT SPRINKLERS

We don’t need a fire escape plan because:

WE HAD AN INSPECTION

We ~~don't~~ need a fire escape plan because:

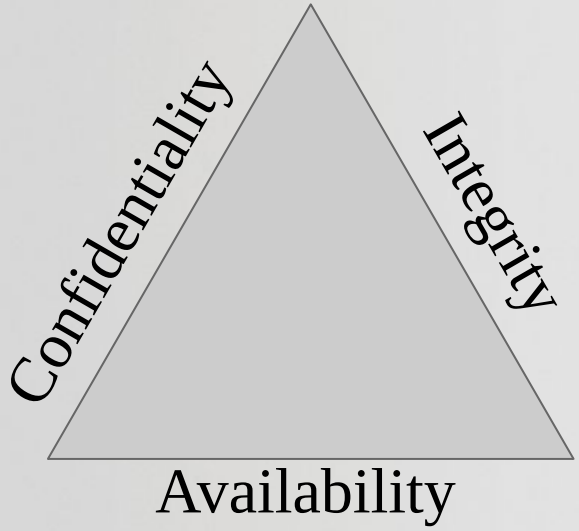
THINGS CAN GO WRONG

NIST Guidelines

The content and recommendations in this talk echo the NIST (National Institute of Standards and Technology) Incident Handling Guide.

You could read the 79 page document instead, if you really wanted to, I guess.

Protecting Our CIA



Events vs. Incidents

An **event** is an observable occurrence in a system or network.

- Web Traffic
- Blocked Attack
- Sent/Received Email

An **incident** is when an event (or events) negatively impact CIA.

- DDoS Crashes Server
- Exploited Vulnerability
- Successful Phish

Preliminary Steps

Before starting your plan:

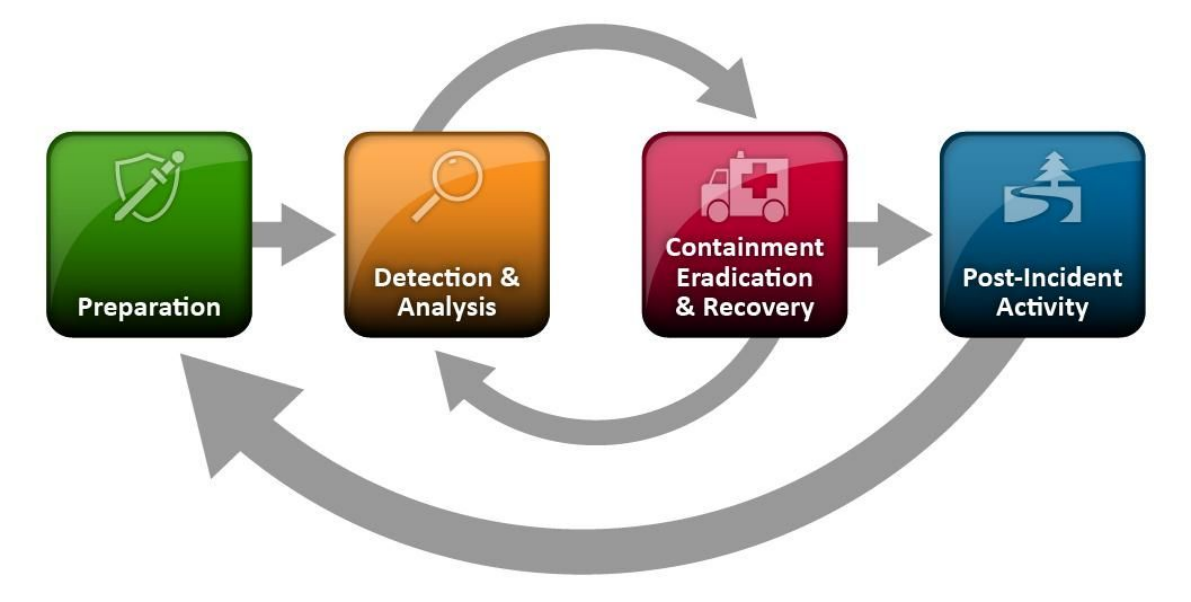
- Identify who leads the response process.
- Ensure they have management support:
  - Authority to assign roles
  - Authority to contact outside parties
  - Authority to test plans and run drills
- Agree on strictness of plan:
  - Rigid policy vs. Looser Guidelines

Communication Is Critical

The key to a successful response is communication. Affected parties need updates early and often.

- Inform your users of anything that affects them.
  - Regulations like GDPR enforce this.
- Share relevant details with other organizations.
- Ensure clear lines of communication with your IR team before an incident occurs.

Incident Response Life Cycle



Step 1: Preparation

Ensure your incident response team has the tools they need to be successful.

- Contact Information
- Reporting Tools
- A “War Room”
- Analysis Tools
- Documentation
- Clean Backups

Step 1: Preparation (cont.)

The easiest incidents to handle are the ones that didn’t happen. Secure your assets to minimize incidents.

- Risk Assessment
- Software Patching
- Access Controls
- Intrusion Detection
- Malware Prevention
- User Training

Step 2: Detection

Minimizing **time-to-detection** (TTD) is a major factor in reducing the impact of a security incident.

Reduce TTD by identifying:

- Attack Vectors
- Attack Precursors
- Indicators of Compromise

Step 2: Detection (cont.)

Attack Vectors are the points in a system or network where threat actors may be attempting breach.

Different vectors require different response.

- Web Services
- Email
- Removable Media
- Impersonation
- Improper Usage
- Many, Many Others

Step 2: Detection (cont.)

Attack Precursors are signs that an incident may occur in the near future. Not all incidents have precursors.

Examples of precursors include:

- Web server logs revealing vulnerability scans
- Wordfence issued vulnerability warning
- Received threats

Step 2: Detection (cont.)

Indicators of Compromise (IOCs) are signs that a security incident may have already taken place.

IOCs vary greatly by vector, but may include:

- Unusual Logins
- Detected Malware
- Resource Overuse
- Changed Files
- User Reports
- Bounced Emails

Step 3: Analysis

Not every precursor or indicator is a definite sign that an incident has occurred. They need to be verified.

Steps to make this easier include:

- Understanding what baseline behavior looks like
- Log retention policies to ensure availability
- Online research

Step 3: Analysis (cont.)

If analysis determines an incident took place, it’s time to prepare for active response.

First determine the following:

- Intrusion Vector
- Impact to CIA
- Recoverability

Then notify relevant parties: Leadership, IR Team, Law Enforcement, Human Resources, Legal, etc.

Side Note: Who You Gonna Call?

Successful **Digital Forensics & Incident Response** (DFIR) engagements rely on specialized skills and tools that your usual IT staff or sysadmins likely don’t use.

Seeking help from outside teams is common even in larger organizations. If something mission critical is on the line, **it may not be the time to try and save a buck** by keeping the process in-house.

Step 4: Containment

Prevent the situation from getting any worse. The decisions made will vary based on attack vector.

- Do we need to shutdown or disconnect anything?
  - How long will it be down?
- What sort of evidence needs to be preserved?
- What can we learn about the attacker’s behavior?

Step 4: Containment (cont.)

If a legal followup is desired, take the time to ensure proper gathering and handling of any evidence.

- Relevant Logs
- Attacker IPs
- Timestamps
- Malware Hashes
- File Changes
- Database Activity

Enforce a **chain of custody**, so all parties handling and transporting evidence are noted and tracked.

Step 5: Eradication

Destroy the invaders.

Depending on scope, this may be bundled with Step 6.

- Delete malware files and scrub injections from otherwise good files.
- Remove malicious database content, like post content injections, rogue users, evil settings, etc.

Step 6: Recovery

Start the climb back towards “Business As Usual”

- Restore from a clean backup if necessary
  - This might count as Eradication if you’re **positive** the backup is not compromised.
- Remediate any vulnerabilities used by attackers.
- Update all secrets, like passwords, keys, and salts.

Step 7: Post-Incident Activity

What can we learn from what happened? Hold a meeting with your team and discuss:

- What happened and when?
- How effectively did we respond?
- What information did we need sooner?
- Were there things we did poorly?
- What tools would have made response easier?
- How do we prevent this from happening again?

Step 7: Post-Incident (cont.)

Make decisions about evidence retention.

Some questions to ask:

- Do we intend to move forward with a legal case?
- How long should we retain the data?
- What will it cost to securely store all relevant data for the duration we've decided?

Recommendations

- Identify your resources **before an incident occurs**.
- Minimize incidents by securing systems properly.
- Automate as much detection as possible.
- Keep reliable backups **and test them**.
- When an incident occurs, don’t destroy evidence.
- Maintain communication with all parties.
- Learn from incidents to prevent future ones.

Thanks For Stopping By!

Questions? Ask away!

Find me on Twitter: @heyitsmikeyv

Check out our blog: wordfence.com/blog