Incident handling for small sec teams

...

Dino

Why bother

1. Its useful
2. You should
3. You have to
4. **Ignore small events and incidents, and you'll have to deal with major ones**

Defining the goal

1. Call attention to a problem
2. Maintain SLAs
3. Formalize re-assigning of resources for urgent tasks
4. Document unplanned work
5. Record anything that affects CIA(A)

Kinds of events and incidents

1. Technical issues with the infrastructure/codebase
2. Phishing
3. Malware on devices
4. Physical safety issues
5. Security breaches
6. Unlocked PC
7. ...

Event vs incident

Anything suspicious and out of ordinary is an **event**. Employees “report” events to draw attention to something.

Expert Review & Decision

Somebody with expertise has a look at the event and decides if an incident has to be called.

Incident implies immediate reallocation of resources for fixing.

Incident Reporting culture

BUILDING A REPORTING CULTURE

1. Clearly communicate what is expected of employees
2. Everyone should be able to report
3. Rules must ensure no-consequence for self-reporting

THE RISK OF SILENCE

Things you don’t know are things you can’t respond to

You know what will never make an incident worse?

Knowing about it!!!

If employees are afraid to report they will hide problems until it's too late

Responding to incidents

1. Manual or automatic routing system for incidents
2. On-call and standby employees
3. Clear rules for prioritization based on triage and type of incident
4. Special authorization for incident responders to act b4 higher ups can be reached
5. Incident Commander - the person trough which all communication regarding an incident flows within the organization.

Learning from incidents

1. Incident log and statistics
2. Post-mortems
3. Case Studies based on the above
4. Onboarding “challenges” for new team members

Reporting to Sicert

1. Nis2/Zinf-1 important entity obligation
2. Anyone can report it to them
3. https://www.cert.si/prijava-incidenta/

Presentation materials

buzzwrd.me/bsides2026

Scan for slides & extra resources