|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | INCIDENT ACTION PLAN | | | | | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | In order to be ready for potential incidents: Review the incident response plan's guiding security policies; Identify sensitive assets; Do a risk assessment; Determine the important incident categories; Create clear documentation of processes, roles, and obligations; Make a communication strategy. | | | | | | | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | **CONTAINTMENT**  \* Contain the incident to prevent it from escalating.  \* isolate network segments and take any affected systems offline.  \* apply temporary fixes to affected systems and redeploy clean systems. | | |  | **ERADICTION**  \* Identifying the attack's root cause.  \* Removing the threat from systems.  \* Planning to fix any exploitable vulnerabilities. | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **INCIDENT DESCRIPTION** |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | \* An advanced persistent threat gains access to an encrypted list of passwords.  \* Detect abnormal network behaviour and identify if those deviations represent a security incident.  \* Determine incident severity. |  | **RECOVERY**  \* Restore affected systems to service.  \* Choose when to restore, how to check if systems are secure, and the length of time monitoring is necessary. | | |  | **LESSONS LEARNED**  \* Extensively review the incident—ideally within two weeks from incidents conclusion document.  \* This section discusses what measures should be taken to prevent a similar incident in the future, including any recommended changes to systems or procedures. | | |  |  |
|  |  |  |  |  |  |  | [© TemplateLab.com](https://templatelab.com/) | | |  |  |