INCIDENT RESPONSE PROCESS

LIELA PRESSLEY
ITT-380 | iNFORMATION ASSURANCE
PROFESSOR CHRISTOPHER MOLSTAD
4/28/24

BUSINESS CONTINUITY

This process document is designed to provide procedural guidelines for our incident response team if and when a malware incidnet occurs. Each step, process and team member responsibility is intentionally mentioned to best launch our company for security, succesful recovery and efficient business continuity as much as possible when facing a malware attack. It is important to note that having a developed step by step process is necessary but is not effective if business continuity management is not well established in these worst-case scenario circumstances.

There are three major success factors in mantaining business contintuity including support from management to allocate necessary resources, establishing efficient reports and accountability, and having the information assurance management team included and involved in the programs.

BUSINESS CONTINUITY- PROCEDURES/STEPS

1. Recongnize the necessity of business continuity programs and establish a geneal understanding of its need
2. Identify all of the relevant business needs in order to be successful and operatable (such as the interdepencies, strategies,operations resources, etc.
3. Develop continuity strategies and alternatives on a operational, processing, and resource recovery level to reduce loss and assess solutions that can be operatable in worst case scenarios such as a malware attack
4. Be ready to develop and implement business continuity responses, in the prepared plan there are going to be niche plans but all need to be specific yet flexible depending on the incident. Malware attacks can come in all shapes and sizes, these plans need to be able to response to them.
5. Have regular backup and restoration procedures prepared and already running on a regular basis.

INCIDENT RECOVERY PLAN

TEAM STRUCTURE

1. Team leaders will vary depending on the specific department, purpose and incidnet but this person will be in charge of ensuring that all guidelines and procedures are being adhered and that all employees understand the necessity of these guidelines and their roles. They will also be part of the disaster recovery plan making process to ensure that it is relevant and parallel to the business' objectives as well as navigating decisions and reports with stakeholders.
2. IT specialists will be covering the different areas of the relevant systems, servers, infrastructures they are working with. They are going to be assessing, reporting, and monitoring the damages and recovery processes and relaying the impact of damages and what needs to be done in order for successful recovery. They will also implement restoration strategies with their technical background and understanding
3. Comms coordinator aka the communication coordinator is in charge of relaying the it or security specialists findings to stakeholders or team leaders while providing why these statstics or reports are impactful to the business and its goals. They will relay these reports in a manner that a non-technical role willbe able to understand clearly and effectively while advocating (in partnership with the team leader) on what resources, procedures and managerial support is recquired. They will also establish a efficient line of communciation such as email, phone or other forms of meetings with relevant vendors, public relations, other departments within the company and other parties to debrief.

TEAM STRUCTURE

team work and clear communication across department and team responsibiliteis s essential to a successful recovery plan. Management is required to provide advocation, resources, redirecting back to the goals at hand. Security professionals are to provid insight, monitor, report and analyze the recovery that needs to be done and how. While communications are to convey these messages and reports to all relevant parties clearly and effectively.

INCIDENT RECOVERY PLAN

REBUILDING

1. After eradicating all signs of the malware and exploits rebuidling begins
2. Evaluate the damages, losses, and systems that need to be restored
3. Reference the alternative ways to achieve the same necessary goals and determine which one is the most effective method
4. Have the incident handling team perform tests with approval from the relevant system owners and administrators.
5. Once the results are in and residual risk is reported, devide whether the systems are able to be used once again or if alternatives still need to be utilized.
6. Accrediation officials will determine step 5
7. Repeat these processes for every system that was compromised and effected.
8. Maintain diligent monitoring for new threats and vulnerabilities
9. Start the review and reporting process to strengthen the company.

REFERENCES

GRAHAM, Y. (2023, JUNE 13). BUILDING A DISASTER RECOVERY TEAM: ROLES, RESPONSIBILITIES, AND BEST PRACTICES. RIGHT PEOPLE. HTTPS://RIGHTPEOPLEGROUP.COM/BUILDING-DISASTER-RECOVERY-TEAM-ROLES-RESPONSIBILITIES-BEST-PRACTICES/

SCHOU, C., HERNANDEZ, S. (2015). INFORMATION ASSURANCE HANDBOOK: EFFECTIVE COMPUTER SECURITY AND RISK MANAGEMENT STRATEGIES. MCGRAW HILL LLC.