Mitigating the Risk of Ransomware Attacks with a Disaster Recovery Plan

Liéla Pressley

College of Science, Engineering, and Technology, Grand Canyon University

ITT-307, Cybersecurity Foundations

Ingrid Gaviria

March 20, 2023

Mitigating the Risk of Ransomware Attacks with a Disaster Recovery Plan

Section 1: What is Ransomware?

Ransomware attacks have more than doubled since 2021, many companies are left recovering for months and even years due to the loss of data, time, access to key operating systems, etc. Ransomware is a type of malware designed to prevent you/your company from accessing your computer, data, specific applications, files, etc. These cyber-attacks can steal, delete, or encrypt your data while wanting a form of payment in hopes to restore what has been accessed, modified, damaged, or locked. When these attacks occur, our organization risks important information being accessed with malicious intent, and applications and systems being tampered with causing devastating effects on our operations and ultimately affecting our organization's ability to function optimally.

Section 2: Major Goals of this Plan

Preparing for ransomware attacks is one of the best ways to mitigate the risk of impact from them. The biggest goal our organization hopes to accomplish through this plan is to ensure CIA is upheld even when faced with a ransomware attack.

The major goals of this plan are the following:

- To minimize the amount of data lost in the relevant disaster
- To determine what parts of applications and data is most relied upon for operations
- To minimize the financial impact of the interruption
- To establish the alternative means of operations
- To provide essential tools and policies for when a ransomware attack occurs
- To provide a foundation for smooth and quick service restoration
- Aim to have an RPO of essential operational data/consumer data to be no more than 4 hours worth
- Aim to have RTO of servers/software to be restored within 4 hours

Section 3 : Personnel

Data Processing Personnel

Name	Position	Address	Phone #

Section 4: Risk Assessment

Our organization requires that risk assessments will be performed at least twice a year; one is a risk-control self-assessment made by management and staff and the other being a quantitative assessment provided by a vendor. This will allow us to analyze factors that will reduce the likelihood of being attacked with ransomware as well as limit the damage if hit by such an attack.

Our Cybersecurity and information assurance teams will determine which third-party vendor best fits the needs for that year but our current risk assessment will include the following:

- Interviews with key personnel and management to understand critical data/systems for daily operations
- Review preventive security controls- strong authentication, phishing training/awareness
- Run external port scans to identify exposed login interfaces
- Provided risk assessment reports with recommendations on how to improve

Section 5: Mitigation Strategies

Backups

- Our organization will have a routine, up-to-date backups on all vital data using an offsite backup service. The data will be encrypted so if stolen it can not be easily read/compromised.
- For services that run on cloud platforms we will use cloud vendors such as AWS Solutions with the tool, HashiCorp Terraform, to allow cross-platform usage.

Prevent Malware Spread via Security Controls

- Managerial- Adhere to Security Policies and ensure they are up-to-date
- Operational- Ensure quarterly training/assessments on security hygiene amongst users
- Technical- Ensure filtering/blocking of unnecessary and malicious sites, files, content, and code is set up. Establish access controls following the principles of least privilege, while ensuring OS and apps are updated/patched regularly.

Malware Prevention on Devices

- Depending on the OS and device, the organization will use an MDM in order to permit trusted applications to run on company devices.
- Ensure that Antivirus and antimalware products will be installed if necessary and disable scripting and macro environments.

Section 6: IT Resource Restoration

Our goal is to restore any systems within a maximum time of 4 hours, some of the procedures to aid in this goal include the following:

- Ensuring backups are isolated/offline and updated with automation implemented when possible and safe.
- Ensure backups are enabled to restore computer systems to bare-metal sate

- If possible, see if instant rollback on virtual machines can restore specific data that is deemed as critical.
- Have IT professionals research if decrypting is an option for encrypted files/data- if not reach out to authorities for help- try to avoid paying any ransom unless advised
- Implement mandatory restoration tests and procedures a minimum of twice a year

Section 7: Security Monitoring and Management

Security monitoring tools that will be utilized throughout the company include:

- SolarWinds Security Event Manager
- LifeLock
- AppLock

Our organization will also implement Mobile Device Management (MDM) to all mobile devices using Kandji, unless another tool is deemed necessary.

References

Ciampa, M. (2021). *EBook: CompTIA security+ guide to network security fundamentals*. (pp. 353-377, 389-397)Cengage.

Evangelist, S. M. P. (2022, June 16). *Ransomware Recovery: The Basics and 6 Critical Best Practices*. https://bluexp.netapp.com/blog/rps-blg-ransomware-recovery-the-basics-and-7-critical-best-practices#h_h2

I. (2022, May 31). *How a Disaster Recovery Plan Can Help Prevent Ransomware Attacks*. Innovative Network Solutions. https://www.inscnet.com/blog/how-a-disaster-recovery-plan-can-help-prevent-ransomware-attacks/

LMG Security. (2021, March 8). *Ransomware Risk Assessment*. https://www.lmgsecurity.com/services/advisory-compliance/ransomware-risk-assessment/

Mitigating malware and ransomware attacks. (n.d.). https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#:~:text=Ransomware%20is%20a%20type%20of,be%20stolen%2C%20deleted%20or%20encrypted.