Ransomware Plan

5/1/2022

Daniel Weinert, Eric Michalczyk, Amanuel Adane, Tyler Miller

Preparation:

1. Determine the designated members of the Cybersecurity Incident Response Team (CIRT).
2. Ensure that all software and systems are kept up to date and secured and are updated at a regularly scheduled interval (i.e., Every Saturday at 1:00 AM).
3. Create backups of critical systems and data as needed.
    a. Implement a backup policy with the scheduled backup times being dependent on the severity of the system and the data it holds in it (less important systems are backed-up less often, more important systems that contain protected information are backed-up more often).
    b. Store backups in a secure offline environment, not accessible by the network.
4. Ensure that important and protected data is encrypted securely while it is processing, in transit, and at rest.
5. Have a secure password policy in place and ensure it is implemented on all accounts. Each password would need to consist of a 12 character minimum, and would need to include numbers, upper-case and lower-case letters and symbols as well. Passwords would be required to be changed every 6 months.
    a. Require multi-factor-authentication for all accounts as well.
6. Have security measures in place to detect and alert when ransomware attacks occur.
    a. Have Anti-Virus (AV) and other security software installed on systems.
    b. Have firewalls, IPS, IDS, and SIEM systems installed on all networks.
7. Implement file and registry monitoring on all systems that contain data. This will then detect any file modification operations and alert the system administrator of them.
8. Establish an escalation and contact plan depending on the data and systems comprised.
9. Implement write/read access only as applicable and refuse all non-privileged accounts permission to change drive and folder/file permissions.
10. Establish software download/install restriction policies and restrict the use of macros in Microsoft Office.

Identification:

1. Identify and isolate any systems affected by ransomware.
    a. If several systems appear to be impacted, take the network down at the switch level.
        i. If for various reasons it will not disconnect, unplug the network devices at the physical level.
    b. Do not power off any machines as important forensic artifacts may be lost, rather, isolate all affected machines from all other devices.
        i. In case of the possibility that the network does not shut down and the ransomware cannot be isolated, power down the affected systems in order to stop the spread of ransomware. <u>Do this only if absolutely necessary!</u>
2. Identify the systems that are in immediate danger of becoming infected.

   a. Isolate these machines and close any potential connections they may have to the infected systems and/or networks.
3. Alert the CIRT of the incident and work with them to:
   a. Develop and document an initial understanding of what has occurred.
   b. Formulate a short-term plan of action.
      i. Assign actions among team members and prioritize protecting critical systems.
4. Identify if the ransomware is running under a specific user/account.
   a. If it is, lock down or delete the account (depending on the account's importance).
5. Look for malicious activity in temporary and other easily writeable locations (I.e., Windows *%TEMP%* folder).
6. Examine any file manipulation activity across the network.
7. Locate patient zero and determine the ransomware's initial entry point into the network.
8. Figure out how the ransomware is operating and what it is doing to steal and lock down the data.
9. Look for common identifying traits of ransomware by using hash values and/or IP addresses and further analyze these traits by using threat intelligence platforms that analyze the hash value and IP addresses
10. Contact federal authorities (if needed) for assistance with handling the ransomware.
    a. CISA (regarding guidance and assistance on the incident)
       i. Report@cisa.gov / (888) 282-0870
    b. FBI (regarding assistance on criminal investigations)
       i. https://www.fbi.gov/contact-us/field-offices

Containment:

1. Identify any potential gaps and entry points using the information gathered in the previous steps.
2. Implement any temporary containment solutions to try to keep the ransomware from spreading to other devices and networks/network segments on the network.
3. Enter previously identified ransomware hash values into all security tools (AV, SIEM) so that the tools will detect and prevent additional spreading of the ransomware.
4. Find and change all compromised accounts' passwords.
5. Isolate the affected systems and networks/network segments from all other systems and networks/network segments on the network.

Eradication:

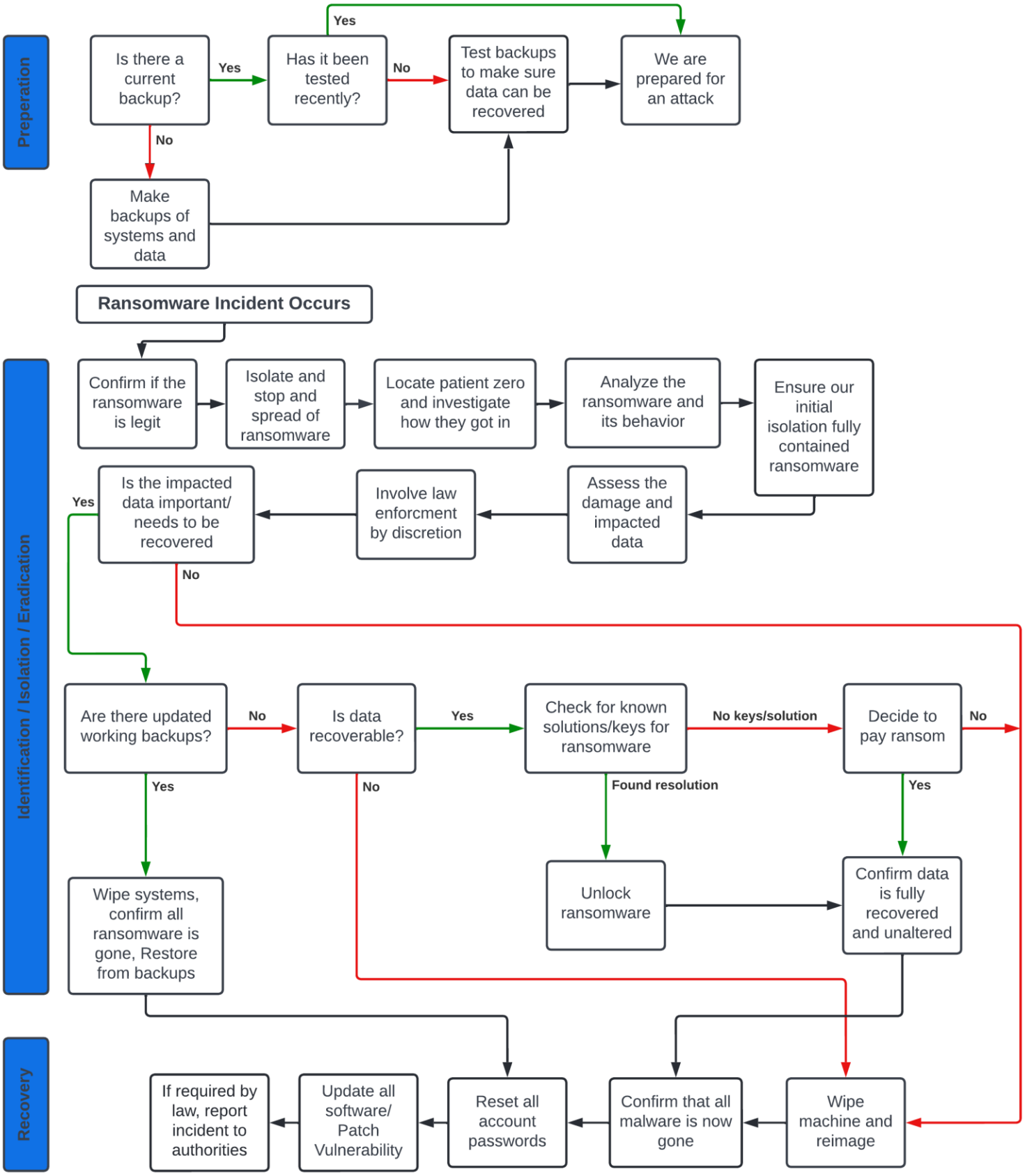
1. Safely create backups of all infected systems (if possible) and preserve any artifacts and relevant information for later forensic analysis.
    a. Prioritize the importance of all volatile data storage.
2. Assess and determine the damage done and then implement a prioritization plan based on that evidence and determine if the stolen information is worth saving or not based on information type:
    a. Personal Health Information (PHI):
        i. If it is determined that electronic protected health information (ePHI) has been encrypted as a result of the ransomware, then a breach has occurred under the Health Insurance Portability and Accountability Act (HIPPA) privacy rule (i.e., unauthorized individuals have taken possession or control of the information).
        ii. Determine the severity of the breach regarding HIPPA rules:
            1. The nature and extent of the PHI involved in the breach
            2. Has an unauthorized party acquired or viewed such PHI?
                a. If so, was the PHI securely encrypted?
            3. To what extent (if any) has the risk to PHI been mitigated?
        iii. Prioritize customers' PHI and recover those systems as soon as possible if such a choice is required.
    b. Personal Identifiable Information (PII):
        i. Determine what type of PII has been impacted:
            1. Determine whose data was impacted (customer's, employee's, vendor's), and those people's physical presence to consult with privacy regulations governing such information on an international, federal, state, and local basis.
                a. Implement steps and actions based on such regulations.
    c. Payment Information:
        i. If the payment system is outsourced to a vendor and, therefore, the organization does not store any financial information, then the data is not governed under the Payment Card Industry Data Security Standards (PCI-DSS).
3. Check for known solutions and keys to the ransomware.
    a. Exercise caution when attempting to use these keys as wrong keys or other methods of circumventing paying the ransom may lead to permanent data loss.
4. Examine if any data has been exfiltrated out of the system(s).
    a. If it has, then cut off the attacker's access to the point(s) where the data is being exfiltrated to.
    b. Prioritize eliminating access to all unencrypted data first.
5. If no other option is possible and the data is essential and needs to be recovered, then (if desired), work with the authorities to prevent total loss, then negotiate/pay the ransom.
    a. Calculate if the requested ransom amount is worth paying or not (regarding potential financial losses with the loss of data and type of data)

Recovery:

1. Evaluate all systems that can be restored from backups:
    a. For all systems that can be, wipe the systems and reimage them.
        i. Thoroughly wipe and overwrite all previous data, then load the backup data via a backup image (such as a snapshot).
2. Ensure all traces of the ransomware are gone:
    a. Ensure there are no back doors present, no malicious files left on the system, no unauthorized connections, etc.
3. Decide if reporting the incident and data breach is necessary and/or desired under breach notification regulations:
    a. Regarding PHI, consult HIPPA breach notification provisions and determine this based on severity of the data breach.
    b. Regarding PII, consult breach notification laws that govern the impacted data.
4. Initiate mandatory password changes for all accounts.

Lessons Learned:

1. Figure out how to best change our policies to better prevent breaches and ransomware attacks in the future.
2. Determine what areas of our organization's cybersecurity we need to strengthen to better implement the previous step.
3. Provide end user training to make all employees more aware of cyber resilience policies and best practices.


Preperation
Is there a current backup?
Yes
Has it been tested recently?
Yes
No
Test backups to make sure data can be recovered
We are prepared for an attack
No
Make backups of systems and data
Ransomware Incident Occurs
Identification / Isolation / Eradication
Confirm if the ransomware is legit
Isolate and stop and spread of ransomware
Locate patient zero and investigate how they got in
Analyze the ransomware and its behavior
Ensure our initial isolation fully contained ransomware
Assess the damage and impacted data
Involve law enforcment by discretion
Is the impacted data important/ needs to be recovered
Yes
No
Are there updated working backups?
No
Is data recoverable?
Yes
Check for known solutions/keys for ransomware
No keys/solution
Decide to pay ransom
No
Yes
No
Found resolution
Yes
Wipe systems, confirm all ransomware is gone, Restore from backups
Unlock ransomware
Confirm data is fully recovered and unaltered
Recovery
If required by law, report incident to authorities
Update all software/ Patch Vulnerability
Reset all account passwords
Confirm that all malware is now gone
Wipe machine and reimage