NABA Recommendations on Ransomware Mitigation

Before a Ransomware Attack

- A serious breach may lead the organization's General Counsel (GC) to invoke legal privilege. Accordingly, it is advisable to develop an action plan for serious incidents in advance to manage communications and external support firms in a manner that will allow the organization to maintain privilege.
- Maintain offline, encrypted backups of data, source code, executables, etc. and test them regularly. Maintaining these offline backups is important as ransomware typically attempts to find and delete any accessible backups. Having such backups greatly mitigates the threat of ransomware.
- Rehearse and maintain up-to-date the enterprise response plan to a ransomware attack, via table-top exercises or equivalent. This plan should detail the restoration process complete with timing, identifying all internal and external parties involved, points of contact, testing the internal and external communications strategy, etc. The priorities for system restoration should be discussed and agreed to in advance so that there is no debates or delays in restoration should a ransomware attack occur.
- Maintain associated backup hardware in fully operational order in order to rebuild systems in the event rebuilding the primary system is not possible.
- Continuously implement phishing countermeasures. Refer to NABA's recommendations on anti-phishing (https://nabanet.com/wp-content/uploads/2020/01/Anti-Phishing-2020-01-07-Final.pdf).
- Ensure all your vendors/suppliers have effective risk management and comprehensive cyber hygiene practices in place. This can be assured during your company's RFI/RFP/RFQ processes and regularly tested. Ransomware threat actors may target vendors/suppliers with the goal of compromising their clients. More specifically, they may use vendor-broadcaster network connections and access to client organizations as a key vector to install ransomware.
- Employ MFA (multi-factor authentication) for all services, particularly for web services, VPN's (virtual private networks), and especially for accounts that access critical systems. Refer to NABA's recommendations for Authentication.
- Through Identity Management, apply least privilege access to all systems and services so that users only have the access to the systems they need to perform their jobs.
- Ensure your organization has a comprehensive asset management strategy. Understand and inventory all your IT assets, both logical (e.g., data, software) and physical (e.g., hardware). Refer to WBU-TC Recommendations for Core Cyber Security Controls (https://worldbroadcastingunions.org/wp-content/uploads/2018/10/WBU-TC-Core-Cyber-Security-Controls-2018-10-03.pdf).
- Retain and adequately secure logs from both network devices and local hosts. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.
- If possible, have comprehensive cybersecurity insurance, providing access to third-party negotiators or directly engage an expert ransomware specialist to negotiate and facilitate payment on your behalf
- Regularly check available on-line resources to counter ransomware, such as is available on the U.S. DHS CISA site: https://www.cisa.gov/stopransomware.

During a Ransomware Attack

- Determine which systems are impacted, and immediately isolate them and if possible, take the associated network down. The system architecture should permit segmentation and isolation as soon as practical once a ransomware threat is detected.
- If taking the network temporarily offline is not possible, locate disconnect affected devices from the network to contain the contagion.
- After an initial attack, ransomware threat actors might monitor your organization's reaction/communications to determine if they've been detected. Use external communication systems (only those whose traffic does not use internal networks) such as mobile phones or other means to avoid tipping off ransomware threat agents.
- Triage impacted systems for restoration and recovery, by: identifying and prioritizing critical systems for restoration; prioritizing restoration and recovery based on a predefined critical asset list.
- Engage your teams and client/stakeholders through your Business Continuity or Disaster Recovery Plans to help you mitigate, respond to, and recover from the incident. Refer to NABA's Recommendation entitled "Cybersecurity Recovery Planning as Part of Disaster Recovery Planning" (https://nabanet.com/wp-content/uploads/2021/09/Cybersecurity-Recovery-Draft-2021-09-01.pdf)

Recommendation

The materiality of cybersecurity incidents, particularly those involving ransomware, is influenced by the following criteria:

- The nature, extent, and potential magnitude of compromised information or the business, with a specific focus on the scope of company operations vulnerable to ransomware attacks.
- The range of harm that ransomware incidents could cause, encompassing potential damage to the company's reputation, financial performance, customer and vendor relationships, and the heightened risk of litigation or regulatory investigations.

The payment of a ransom in the event of such an attack is a strategic business decision by the broadcaster.

A ransomware response and action plan should be developed in advance of an attack by executive management, i.e. CEO, CISO, CTO, Legal, Finance, etc. so that a co-ordinated and comprehensive response is feasible. There are as well expert third-party negotiators available, some as part of the broadcaster's cybersecurity insurance, who can provide expert advise in this regard.

March 2024