Ransomware: Data Held Hostage

Given the increasing frequency of ransomware attacks, organizations need to have appropriate policies and procedures in place before an attack occurs to limit data exposure and data loss and minimize the organization's downtime in the event of a ransomware attack.

By James Vezeris | November 23, 2022

It's 3 a.m. when your phone begins vibrating on the nightstand. Half asleep, you answer the call. Your chief technology officer is on the line, clearly distressed and speaking so fast you can only make out a few words—"data," "locked out," "$1,000,000," and "crypto." Piecing it together, you realize that your organization's systems have been hacked. Once you get the CTO to take a breath, you finally get the full story—your organization has been targeted in a ransomware attack. A hacker has infiltrated your organization's systems and encrypted all of the data, including highly sensitive personal information of your clients and confidential corporate documents. Your employees cannot access the programs they need to do their work, and your customers cannot access your organization's website. For every hour your organization's systems are down, thousands of dollars of revenue are lost. The hacker sent an email to the CTO demanding $1,000,000 in cryptocurrency in exchange for the decryption of the data. How could this happen? What do you do now?

What Is Ransomware?

Ransomware is a term used to describe malicious software (malware) that encrypts an organization's data, denying the organization access to its data. A hacker, whether an individual or a group, who has access to the organization's systems uses ransomware to encrypt the organization's data. The hacker will then demand money from the organization in exchange for a key to decrypt the data. Sometimes, hackers copy or take the data and threaten to release the stolen data if payment is not made. Hackers often request payments be made using cryptocurrency, such as Bitcoin, Ethereum, or Monero, to limit the ability of authorities to trace the payments back to the hacker.

Ransomware attacks can disrupt, if not halt, the operation of an entire organization. There have been several high-profile ransomware attacks that have targeted New Jersey-based companies. For example, Hackensack Meridian Health suffered a ransomware attack in 2019 that interrupted several hospital systems, including its billing and radiology systems. In another example, a hacker requested payment from University Hospital in Newark in exchange for not publishing patient information. Outside the health care sector, a ransomware attack on the Tenafly Public School District crippled the district's computer systems. Somerset County's computer systems were also the target of a ransomware attack this past summer. Personal email and online data storage accounts are also often the focus of ransomware attacks that subject victims to losses in the hundreds or thousands of dollars to have access to their accounts restored.

According to the FBI's Internet Crime Complaint Center, over 3,500 complaints of ransomware attacks were lodged in 2021, with nearly $50 million in adjusted losses. *Internet Crime Report 2021*. These attacks represent a more than 50% increase in attacks compared to 2020, and preliminary numbers indicate that this upward trajectory has continued in 2022. These numbers represent just attacks reported to the FBI's Internet Crime Complaint Center (IC3). According to the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN), the total value of suspicious activity reported in ransomware-related Bank Secrecy Act filings during 2021 approached $1.2 billion!

To Pay, or Not To Pay, That Is the Question

In the cases of Hackensack Meridian Health and University Hospital, the hospitals met the hacker's demands and paid to recover their data. While the amount paid by Hackensack Meridian Health, through its insurer, has not been disclosed, University Hospital reportedly paid $670,000. In each case, the hacker kept their promise, and the data was successfully recovered. However, paying a hacker does not guarantee the successful recovery of the data. Indeed, the FBI recommends that organizations not pay hackers. In addition to having no guarantee that hackers will keep their promises, meeting hackers' demands may encourage them to attack others. Paying a ransom may also make the organization a target for other hackers by showing the organization's willingness to pay to recover data.

Each ransomware attack involves different circumstances that must be considered before deciding whether to meet the hacker's demands. For instance, did the ransomware attack affect all the organization's data or a small subset? Are there backups of the data that can be used to recover the data without paying the hacker? How sensitive is the stolen data? Are there legal ramifications to paying the hacker (e.g., Does insurance allow for payments? Can the payment be made legally?) Depending on the answers to these questions and other considerations, an educated decision can be made about whether to pay.

Regardless of whether payment is the appropriate course of action, bringing the attack to the attention of the authorities should be a top priority. Law enforcement has access to sophisticated tools that can be used to track and, in some instances, capture the hackers behind the attacks. Moreover, the authorities can advise on how best to deal with the hacker.

Preparation Is the Key

Preventative steps can be taken to limit the damage a ransomware attack can cause an organization. While there is no failproof way to secure an organization's data, having data protection policies in place before an attack can limit the scope of the ransomware attack, especially as hackers often provide little time, sometimes only hours, to react to their demands. Additionally, strong data protection policies may limit the organization's liability for a data breach.

Over three-quarters of data breaches, such as ransomware attacks, are due to employees taking actions they should not have, like opening an email attachment from an unknown sender or sharing a password. While mistakes happen, training employees to be aware of risky behaviors and actions will limit the possibility of an employee unknowingly enabling a data breach.

One of the most effective ways to prevent a ransomware attack is to continually provide IT training for employees so they can readily identify (and not fall for) questionable activity, such as spoofing (i.e., impersonating another company or individual), phishing (i.e., requesting the release of sensitive information), social engineering, and other nefarious activities hackers leverage to gain access to secure systems. A properly trained workforce will make it difficult for a hacker to gain access to such systems and, in some instances, force the hacker to give up entirely.

While data is essential to the operation of most organizations, with nearly all organizations collecting data to better serve their clients, not all data needs to be stored. Accordingly, a data policy may limit the amount of data collected and stored by an organization. For instance, a company that sells products may collect data such as customer purchase histories, credit card information, phone numbers, and home addresses. While the company may have a legitimate use for this information, in the wrong hands, this data can be used for fraud and theft. Furthermore, in the context of ransomware attacks, hackers could threaten to disclose this information on the dark web unless their demands are met. To limit the amount of sensitive data that can be accessed in an attack, the company may have a policy against storing sensitive data, such as credit card information. Instead, the company may delete such data after it is used or outsource payments to a third-party system so the organization never handles such sensitive data.

However, in instances where an organization does store sensitive information, the organization should have adequate data protection policies and procedures in place for the collection, storage (including data backup policies), and maintenance of data to ensure sensitive data is secured. For instance, the data policy may call for personally identifiable information, payment information, and other such sensitive information to be anonymized to limit the risk of a customer's exposure if the data is released. The data policy may require the encryption of sensitive information, such as payment information and passwords, so even if such data is accessed, the data is unreadable without a decryption key—beating the hacker at their own game! The data protection policy may also require data to be backed up regularly so that relatively current data can be restored quickly to limit downtime.

Organizations should also consider having third-party audits performed at regular intervals. A third-party audit tests an organization's infrastructure and practices to see if they can withstand external and internal threats. Regular audits can identify infrastructure weaknesses and mitigate damages in a breach while demonstrating to customers and potential acquirers the organization's commitment to data security.

Finally, having a data breach response policy in place will enable a rapid and comprehensive response in case of a ransomware attack or other data breach. Such policies outline how the organization will respond to a ransomware attack or other data breach, including what actions should be undertaken and by whom. The goal is to have a plan that enables a fast response to limit the scope of the breach and to restore systems to normal operation as quickly and efficiently as possible.

Conclusion

Given the increasing frequency of ransomware attacks, organizations need to have appropriate policies and procedures in place before an attack occurs to limit data exposure and data loss and minimize the organization's downtime in the event of a ransomware attack. The expense of such preparation will likely be orders of magnitude less than the damages that may otherwise be incurred by an unprepared organization in the event of a ransomware attack.

James Vezeris *is a partner at Lerner David.*

Reprinted with permission from the November 28, 2022, issue of the New Jersey Law Journal. Further duplication without permission is prohibited. All rights reserved. © 2021 ALM Media Properties, LLC