abacode™
Cybersecurity Experts

Ransomware and Employee Training

White Paper

January 23, 2017

Summary

In the past two years, global incidents of ransomware have surged significantly, especially in attacks targeting organizations. Attacks are up to 4,000 per day now, as they quadrupled in 2016. Ransomware is defined as a type of malware that renders the user's device or files inaccessible until a ransom set by the hackers is paid. Certain dangers surround different aspects of ransomware, and they will be discussed within this white paper. As with any area of cybersecurity, employee training is the key to decreasing vulnerabilities within a company or organization. Employees must have a strong understanding of how ransomware works and what can be done to minimize attacks.

Problem

Hackers evolve with technology. As a result, they will most likely stay one step ahead of their victims and remain able to manipulate them with ease. This issue becomes costly, however, when paired with the recent rise in ransomware, the go-to for cybercriminals looking to make quick and easy money. According to the FBI, ransomware costs totaled to $209 million in the first three months of 2016, a significant rise from the previous years. Though ransomware began as malware present in spam emails geared toward individuals, it has become a phenomenon featuring specific attacks aimed at organizations (not to mention doubling in cost for victims from $294 in 2015 to $679 now, according to Symantec's research).

The health care industry still requires the most drastic cybersecurity measures, as it remains the most targeted sector when it comes to cybercrime, especially ransomware. Hospitals are especially affected, as a ransomware incident can shut down operations until ransom money is paid and risk the lives of patients, especially those undergoing surgery. Since ransomware has become such an issue in health care, cybersecurity has become a top priority across the industry. However, as victims create means of protection and prevention, hackers evolve to get past those means, similar to the way superbugs evolve due to antibiotics. Nevertheless, by minimizing human error, organizations find themselves in a much stronger position when preventing cyber attacks. Employee training and knowledge of the ins and outs of cybersecurity is essential in this day and age, and not just for hospitals.

Because the few hundred dollars that the average attacker demands in exchange for encrypted files, many would say that paying the ransom is the easiest way to go. This is simply a mistake, unless there is no way the data can possibly be recovered. Paying a ransom because it is the cheapest option only encourages criminals to strike again, because as long as an enterprise is profitable, there is no reason to stop. Due to this, giving in to ransomware criminals gives them the incentive to hit another individual or firm, and the ransomware trend will only increase. Cybersecurity experts and the FBI encourage victims never to pay ransoms, unless paying is the only possible option and all other solutions have been exhausted.

It must be included in this white paper that a large driving factor behind the rise of ransomware has been the rise of Bitcoin, as this untraceable digital currency attracts hackers hoping to stay anonymous and still receive payment with ease. Both ransomware and Bitcoin experienced a boom in the beginning months of 2016, and though ransomware was possible before Bitcoin, it was more difficult for criminals to stay completely hidden. Bitcoin represents an opportunity for total anonymity that many cyber criminals are capitalizing on. Hackers also heavily utilize Tor and the dark web as methods to further hide their identities.

Attack Breakdown

Ransomware attacks typically occur through phishing, as PhishMe, Inc. recently found that 97% of phishing emails contain some form of ransomware. The ransomware dubbed 'Locky" dominates the field thus far due to how long it has been around. Locky's strategy is similar to that of most ransomwares:

1. An email with a document attached reaches the device, and the document contains complete gibberish.
2. The document advises the user to enable macros.
3. Once macros are enabled, code is run within the document, which in turn saves a certain file to the disc.
4. That file downloads the malware onto the computer or other device.
5. Files are completely encrypted.
6. Device background is changed to a message from the hackers, directing the victim to a website on which they will receive further instructions about payment.[1]

Of course, this attack breakdown is simply a specific example of one of the most common ransomwares. The most basic attack method is to find vulnerabilities in a network and exploit them by injecting malware and then demanding a ransom in exchange for the removal of said malware. Hackers know, however, that human error is the most predictable vulnerability, which is why phishing emails remain the number one ransomware vector in 2017.

---

[1] Information about Locky provided by security software company Sophos, Ltd.

Solution

Ransomware attacks can be avoided with the proper approach, which is one that heavily emphasizes employee training and awareness. This is imperative for preventing any sort of cyber-attacks, but especially ransomware. Because most attackers depend on humans to click on their emails and download their malware, employees must learn what should not be clicked and how to recognize a phishing email. They must learn how easy it is to download files containing malware without realizing it, and they must learn to backup all files frequently and store the backups somewhere untouchable by the network the originals exist on.

Of course, protecting the network is crucial in preventing ransomware, but attackers see employees as a way in. They recognize most laymen have gaps in their knowledge about the finer points of cybersecurity, so while they expect to encounter barriers such as anti-virus or anti-malware programs, they do not count on their victims recognizing attacks and actively counteracting them. Employee training in cybersecurity can save organizations hundreds of thousands of dollars in ransomware costs and discourage the practice of ransomware as it becomes less effective in the face of more educated targets.

A series of simple steps should be undergone in order to prevent ransomware. Employee training, as previously stated, is most important, as learned employees are far less likely to enable macros and fall for social engineering scams, phishing emails, or suspicious links. They are also far more likely to back up files off the network and understand what to do in the face of a cyber attack.

Besides training, having a monitoring system in place throughout the technological environment of a company keeps company executives notified of any changes or possible breaches within that environment. Keeping software and protection up to date can also reduce instances of ransomware, as can creating a multi-layered protection system and ensuring that employee privileges within the company network are monitored. Constructing an organization-wide policy for dealing with ransomware if an incident were to occur greatly minimizes chaos and damages, as well.