Tips for Preventing and Responding to a Ransomware Attack

Save to myBoK

By Mary Butler

As predicted, 2016 is proving to be the year of ransomware, with multiple reported incidents making news as we approach April. As they become startlingly more common, it's important that HIM professionals be aware of how preventable they are, says Tom Walsh, CISSP, founder and managing partner of tw-Security. Just as with other types of data breaches, ransomware attacks are the result of human intervention—that's also where they end.

How Ransomware 'Gets In'

Ransomware infects healthcare data and information systems the same way that more common malware and viruses do—via e-mails with embedded links or attachments that once clicked on infects all the files on a given machine. But ransomware programmers are more known for using a technique called "spear phishing," which sends very targeted phishing e-mails.

Hackers who use this method will pick a hospital or health system, and then gather as much information about the hospital as they can: looking up the executive team on the hospital's website, looking at those executives' LinkedIn profiles, and then they'll start sending e-mails to people inside that organization. These emails can squeak through the hospital's e-mail client by being sent through a registered domain. Hackers can purchase a domain for $12 and be registered for three days, which is long enough to pass through most e-mail spam filters (e-mails sent from domains less than 72 hours old will often be flagged as spam).

Recipients of spear phishing e-mails open the e-mail because the name of the sender is usually a familiar one if the programmer did their job right. To appear more authentic, the e-mail might carry a "sent from my iPhone" signature at the bottom. Walsh says this trick tipped off one executive to the fact that he was looking at a phishing e-mail, because the "real" sender was a loyal Samsung user.

"The sophistication is very high, which means we must get our users, employees, workers, anyone who works in a hospital, well aware of these things, so they understand and exercise a little more discernment before clicking on links," Walsh says.

Who Deploys Ransomware?

People need to stop thinking about hackers as if they're angry teenagers hiding behind their computer. Walsh says ransomware programmers have frequently been traced to the Russian mafia, whose members recruit programmers from third world countries. In some cases recruiters will threaten to harm the families of potential programmers if they refuse to do a job, and offer wages and benefits that are better than any legitimate job they could find.

Because the stakes are so high for these programmers, they do their job well and in another sense, are very trustworthy, says Walsh. That is, trustworthy in the sense that if targets pay the ransom, their "hostage"—or data—will be released as promised when an attack is launched.

This is why the FBI always urges ransomware targets to pay up. The most recent high-profile ransomware attack in California is a perfect example. The hackers set the ransom at $17,000—a price most providers can afford, since the price of the data being held and the potential for bad press is far higher. The FBI's argument for paying the ransom is that it allows them to follow the criminal's "paper trail," but the catch is that hackers demand payment in Bitcoin, a web-based currency that's very difficult to trace.

Preventing an Attack

Since tactics such as spear phishing are well known to security professionals, training the workforce to avoid and report incidents should be straightforward.

“To me, it’s an easy fix, but a huge culture change,” says Walsh.

One of those seemingly “easy” fixes includes banning employees from using corporate machines for checking their personal e-mail. An organization’s internal e-mail client is likely to have more sophisticated spam filters than web-based providers such as Gmail and Hotmail. But getting hospital staff to refrain from doing it anyway is easier said than done.

Walsh says that in one instance, a ransomware attack originated from a computer in a hospital’s cardiac catheterization lab.

“What happened was, the ransomware encrypted all of the data stored on that local machine—the cath lab has separate computers for doing hard test analysis and that’s what happened. On this computer they run studies. The results get transferred into the health record, and then the raw data from the study stays on the local machine. The ransomware encrypted all that data, and then the ransom note appeared two days later and the hospital lost two weeks worth of study,” Walsh explained.

He says a doctor might come into the lab to check the results of a test, then decide to check their e-mail, unknowingly spreading malware in the process. While they might seem minor, it can be hard to get people to break these habits. But in an era where nearly everyone has a smartphone, there’s no reason a person should be checking personal e-mail on a work machine, Walsh says. And if smartphones are allowed, employees should be required to sign on to a guest wireless network.

Another measure that can help limit the scope of a ransomware attack is to make sure data backups are done as frequently as is feasible. If a facility only backs up their data every two weeks, then two weeks of data is at risk.

“Now, if you’re talking about doing more data backups, you’ve gotta have the hardware in your data center or server room to support that. Memory’s not cheap. You’ve got to go invest capital dollars and getting more data backup methods in place,” Walsh says.

Mary Butler is the associate editor at The Journal of AHIMA.

Original source:
Butler, Mary. "Tips for Preventing and Responding to a Ransomware Attack" (Journal of AHIMA website), April 01, 2016.
