How to Build a Ransomware Defense Plan for Your Agency

THORNBERRY LTD
Interoperability at our core.

Contents

72 percent

of all ransomware attacks are directed toward healthcare agencies.

Introduction

The 2017 Verizon Data Breach report found that 72 percent of all ransomware attacks are directed toward healthcare agencies.[1] With the high stakes and increasing prevalence of ransomware attacks, it's time for home health and hospice agencies to step up their data protection strategies.

Healthcare at High Risk

In ransomware attacks, cybercriminals encrypt or block access to an institution's files and demand payment for their return. This method of cybercrime is surging. In 2015, there were 3.8 million attacks attempted. But in 2016, that number jumped to 638 million.[2]

Healthcare is most at risk. If a provider can't access its EMR, patient files and additional records, the health and well-being of patients is put at risk.

As proofpoint's Ransomware Survival Guide noted, "Cyber criminals are increasingly turning their sights to organizations with sensitive data, thinly stretched IT departments and a high incentive to quickly settle the matter."[3]

Healthcare checks all these boxes, making it one of the most vulnerable industries to ransomware.

One recent attack that grabbed headlines was at the Hollywood Presbyterian Medical Center: A hospital employee downloaded a ransomware-embedded attachment, believing it was a legitimate email. Access to the hospitals files was lost, and the hospital paid a $17,000 ransom to retrieve the files.[4]

However, even paying the ransom doesn't guarantee a provider access to its data. For example, at Kansas Heart Hospital, which also suffered a ransomware attack, the ransom was paid but the attacker released only some of the files. A further payment was not made, leading to the loss of that data.[5]

“Ransomware can exploit weak spots in networks or outdated software and then take control of files from the inside of the system.

How Ransomware Works

Ransomware encrypts or blocks access to an organization’s computer networks and/or files. Users attempting to access such files see an error or lock screen instead, alerting them that they are unable to access the data and that they will need to pay a certain ransom in order to get the files back and renew the use of their systems.

A common way that ransomware attacks take place is through phishing emails. In this scenario, an employee downloads an email attachment embedded with ransomware software. The email generally is made to seem like it was sent from a legitimate source, for example, a boss or client. The attachment is often disguised as an invoice or other seemingly real document. Malicious ads or websites can also be contain ransomware.

In addition, ransomware can exploit weak spots in networks or outdated software and then take control of files from the inside of the system.

Typically, ransom is demanded in bitcoin, a virtual currency that enables anonymous money-trading for both sender and receiver, as the Ransomware Survival Guide noted.

Preventative Measures

It is vital that every home health and hospice agency has a ransomware defense plan in place. Here are the top seven best practices for preventing ransomware attacks:

Backup offline

In the event that an agency has access to its files blocked, it can avoid paying a ransom and restore access by reverting to backed-up files. However, there are some caveats to this approach.

First, files should always be backed up onto a separate system that is not connected to the organization’s main network. This is because the backup data will also be wiped out in the event of an attack.[6]

98 percent of Office-targeted threats use macros.

Second, the back-up system should normally be disconnected from the internet. It should only be connected when files are being backed-up.

Third, test restore methods.[7] If an organization can not actually restore its data, then no amount of backup will make a difference.

Be on top of updates and patches

Healthcare providers that use outdated software are especially vulnerable to ransomware attacks. This was the case with a wave of attacks in May 2017 that affected more than 40 National Health Service hospitals in the U.K. The ransomware WannaCry exploited security weaknesses in outdated software, with organizations using Windows XP being hit. Be sure to also regularly update to the most recently released patches for the systems you use and keep your software systems updated at all times.

Be cautious with email

Be careful when downloading email assets. Do not click links or download attachments in emails from senders you do not know. It is also possible for ransomware agents to use the email addresses, names and personal information of people you do know to make the email seem real, so vigilance is key. Be wary of emails that have spelling or grammar mistakes, or that have a tone that is unusual for the sender. If the email appears to be sent by a colleague but you are not sure if it is legitimate, reach out to the colleague in person to confirm the email.

Be selective with macros

Ransomware embedded in email attachments is typically set off by enabling macros. The email server will ask users if they would like to enable macros to download the attachment and the user then clicks yes, thinking the attachment is a normal business document. As such, one preventative method can be blocking emails that require macros to be enabled. For instance, Microsoft has found that 98 percent of Office-targeted threats use macros.

"Office macros are usually not required for the majority of PCs used in healthcare environments," Palo Alto Networks advised. "Enable macros for exceptions or certain departments only."[8]

Focus on employee awareness

Employee education is key in fighting ransomware – as many cybersecurity experts have noted, it is designed to specifically exploit human nature. Your staff need to be as knowledgeable as possible about the threat of ransomware, especially how it can be enabled through email. Share case studies of ransomware attacks with staff, instruct them to report any suspicious emails and conduct regular trainings on ransomware prevention best practices.

Pen-test

"Penetration testing" is when an organization gives permission to a cybersecurity firm to conduct simulated attacks on its network. This method of testing can assess a home health and hospice agency's security practices as well as employee knowledge and training. As proofpoint's Ransomware Survival Guide noted, it may be very beneficial for agencies to hire "pen-testers" to help them strengthen their prevention tactics.

Secure all devices

The detection of Android ransomware increased by more than 50 percent in 2016, marking the highest number of attempted attacks on the devices in history, according to IT security firm ESET.[9] The same preventative measures you use on your computer devices on-site should be used on mobile devices as well. You should also identify and prevent against the vulnerabilities unique to smartphones and tablets. For example, ransomware is frequently enabled on smartphones via third-party apps hiding malicious bugs.

Conclusion

Ransomware is a major cybersecurity threat against which healthcare providers of all sizes and types should be defending themselves. Home health agencies and hospices are particularly vulnerable due to typically lower investments in information technology. A ransomware attack can mean that patient health and well-being is on the line as agencies lose access to vital data, sometimes permanently. They should follow best practices for preventing attacks to strengthen their security – the most important of which is thoroughly educating employees about the dangers of ransomware attacks. To learn more about other preventative measures that can be taken to protect your agency, call Thornberry Ltd. at 717-283-0980 or visit www.thornberryltd.com.

THORNBERRY LTD
Interoperability at our core.

Sources: 1 www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034 | **2** www.forbes.com/sites/leemathews/2017/02/07/2016-saw-an-insane-rise-in-the-number-of-ransomware-attacks/#1674a9ad58dc | **3** www.proofpoint.com/us/resources/white-papers/ransomware-survival-guide | **4** www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html | **5** www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom | **6** healthitsecurity.com/resources/white-papers/four-countermeasures-to-protect-against-ransomware | **7** www.proofpoint.com/us/resources/white-papers/ransomware-survival-guide | **8** researchcenter.paloaltonetworks.com/2016/05/tips-to-prevent-ransomware-in-healthcare-environments/ | **9** https://www.eset.com/us/about/newsroom/press-releases/android-ransomware-up-by-more-than-50-percent-eset-research-finds/