Is Your Healthcare Prepared for Ransomware's Evolving Threats?

Written by
CompliancePro Solutions

Posted on
Dec 6, 2022 10:50:52 AM

A faceless attacker infiltrates a company's computer network ... encrypts its data ... and suddenly ... 'access denied.' No one can retrieve business files until the ransom is paid—*if* the criminal chooses to release it. This is a ransomware attack.

Ransomware attacks can debilitate any organization. But healthcare organizations are particularly vulnerable because their patients are vulnerable. Restricted access to data can ignite a multitude of complications and risks: ambulance diversions, obstructed medication systems, interrupted scheduling, surgeries, and other services, etc.

> Only 2% of healthcare organizations get **ALL** their data back after paying ransom.
>
> *Source: Sophos; The State of Ransomware in Healthcare 2022*

Ransomware—More Than Just Data at Stake

In September 2020, circumstances related to a ransomware attack on a German hospital indirectly caused the death of a patient. The attack crashed a hospital's IT systems, preventing the facility from admitting the woman who needed urgent care and forcing her to go to another hospital. The U.S. also felt its first credible claim of death related to ransomware in 2019. During a ransomware attack at an Alabama hospital, a baby sustained a severe brain injury during its birth and later died due to improper care associated with the attack.

With these cases in mind, it's not hyperbole to claim that ransomware attacks can literally be a matter of life and death for healthcare organizations. However, even with data security prevailing at such critical importance, healthcare systems continue to fall victim to cyberattacks, and the ransomware variety is increasing.

Ransomware Is Ramping Up

One of the first notable ransomware attacks—WannaCry—occurred in 2017 and hit 80 medical facilities within the U.K.'s National Health System. In 2020, a major hospital chain serving more than 400 locations found its computer networks failing. The culprit? Ransomware. This was, so far, one of the biggest attacks on a medical facility in the U.S. Two years later, in October 2022, ransomware assailants hit the fourth-largest U.S. healthcare system and provoked delayed surgeries, doctor appointments, and other patient care.

However, these incents are just the newsworthy attacks, the mammoth organizations. According to Sophos' The State of Ransomware in Healthcare 2022, 66 percent of all healthcare organizations suffered a ransomware attack in 2021—a 94 percent increase from the previous year and the highest volume increase of all sectors at 69 percent. Also concerning is that there was a 67 percent increase in attack complexity and a 59 percent rise in the attack's overall impact. Interestingly, healthcare sits at the bottom with the "lowest average ransom payment"—around $197,000.

Source: Sophos; The State of Ransomware in Healthcare 2022

The report suggested that this surge in ransomware in the healthcare industry may be in part due to the burgeoning ransomware-as-a-service model. Ransomware-as-a-Service (RaaS) works much like Software-as-a-Service (SaaS), offering subscription-based access to ransomware tools instead of productive business software. This threat model amplifies attack potential for organizations because it unleashes attack capabilities for any bad actor with money and inclination—technical mastery or ransomware experience isn't needed any longer.

Fighting the Ransomware "Disease"

Protecting against cybercrime has always been a critical priority for healthcare organizations. But as ransomware threat models evolve and proliferate attack potential, industry leaders must step up their security efforts in response.

Here are a few more stats from Sopho's report to drive home the importance of formidable data security protocols:

- 65% of encrypted data was restored after paying ransom
- Healthcare is the sector most likely to pay ransom—at 61%; other sectors average 46%
- Attack remediation costs for healthcare is US$1.8M—second highest of all sectors

- 94% of healthcare organizations hit by ransomware stated that it hindered their ability to operate
- 44% of healthcare organizations that suffered an attack took a week to recover; 25% took up to a month
- 90% of private sector healthcare organizations said a ransomware attack caused them to lose business or revenue

Reactive Ransomware Response Is Still Pervasive

Far too many health organizations rely on reactive methods for ransomware security: 50 percent admitted they depend on data backups, and 43 percent suggested cyber insurance would keep them safe from an attack. But these reactive remediation efforts won't prevent attack-related disruptions, diminished care, postponed surgeries, etc., that could exacerbate patient illnesses or precipitate death. Data backups and insurance won't repair reputations, make patients feel safe—or bring them back. And cyber insurance can't recover data.

Prevention is where healthcare must focus its effort. Healthcare facilities must work to prevent attacks when lives are literally at risk.

Tips for Healthcare Organizations to Prevent Ransomware Attacks

1. Conduct frequent security assessments
2. Perform vulnerability scans and penetration tests
3. Monitor networks and usage activities
4. Educate employees on cybersecurity best practices and regularly test their knowledge
5. Consult third-party experts for reliable security advise

Of course, no fortress is ever 100 percent impervious. And cybercriminals will never relent in their endeavors to outmaneuver security tactics. But the more effort healthcare organizations make to prevent ransomware attacks, the better their chances are to remain secure and avoid catastrophic disruptions and loss. Organizations should employ all reasonable preventative security measures at their disposal—patient lives depend on it.

If you'd like to learn more about protecting your healthcare organization against ransomware and other cybersecurity threats, contact CompliancePro Solutions' privacy and security experts today.