Securing the healthcare industry with Rapid Response Retainer

Use case



The healthcare industry holds some of our most personal information. Its information systems are extraordinarily complex, with workflows that range from fax machines and paper mail to 5G wireless telemetry, remote surgery and the Internet of Things (IoT). The inherent value associated with protected health information (PHI) and the various ways to potentially obtain it have proven irresistible to hackers.

The situation

An IT manager at a large Midwestern hospital group noticed something strange: the behavior of two local administrator accounts looked peculiar. One account in particular was attempting to log into different servers by brute force. After some investigation, the department determined that those admin accounts were not authorized and had not been created through normal channels.

Insider threats account for 48% of all data breaches in the healthcare industry.[1]

The hospital group had recently acquired some companies and administrators knew that security was not all it needed to be while various systems were being merged, but they also couldn't cut off access entirely because that would have crippled operations.

It was time to call in some help, to figure out how the accounts were created, what the owners were up to in the network and what the next steps needed to be.

The healthcare industry has a particularly large attack surface and correspondingly complicated security needs. However, security problems aren't always especially sophisticated. Legacy workflows including fax machines, paper records and postal mail coexist with sophisticated networks, cutting-edge technology, mobile workstations and IoT. Mistakes such as incorrectly performed mail merges, where the wrong letters (with highly sensitive personal information) get stuffed into the wrong envelopes, are not uncommon. Miscellaneous errors like that accounted for 30% of healthcare industry breaches in 2019.[1]

Coupled with a rigorous regulatory environment and thin-to-nonexistent profit margins, these challenges mean security professionals in the healthcare industry have their hands full. Nearly half of all breaches in healthcare – 48% of them – are at the hands of internal bad actors. People make mistakes, unauthorized apps cause accidental data leakage or overly curious staff abuse their access to look up sensitive information about friends, family or celebrities.

The response

Like any good defense, the hospital's security response started long before the attack by engaging Verizon's Rapid Response Retainer. The retainer, as typical, had begun with a network assessment and an onboarding call, where the hospital's CISO and other team members had an in-depth conversation with a Verizon Threat Research and Advisory Center (VTRAC) investigation liaison they would be working with.

When trouble struck, help was only as far away as VTRAC's 24-hour emergency number. A VTRAC response always begins with a scoping call, where an experienced investigator responded quickly and set the wheels in motion.

verizon

The VTRAC investigator started by interviewing staff to understand how the network was typically accessed: through shared workstations or if VPNs or two-factor authentication were required. In this case, the hospital relied heavily on shared workstations. Moreover, there was no VPN; because networks had not been merged after the acquisition, access was through remote desktop protocol (RDP), which does not use two-factor authentication.

After extensive investigation across the hospital's very complex network, it became apparent that the owners of the rogue accounts hadn't actually accessed proprietary information. They seem to have been uninterested in stealing data themselves, but were probably poised to sell access to someone who did want the health, personal and payment data stored on the network.

VTRAC, as part of its response, can walk you through detailed processes for collecting data of evidentiary value. They take memory dumps, collect forensic images and perform targeted collection of specific log data—things that help explain what happened, how it happened, how far the attack spread, and what data was either at risk or compromised. This is uncommon expertise that hospitals don't generally have on staff, making the VTRAC team's knowledge invaluable.

Lessons learned

It's a truism: people are the weakest link in your security chain. It could be a corporate decision to not enforce best security practices. It could be one executive's inattentive click on an email hyperlink that plants malware. It could be a careless envelope stuffer or an overly curious orderly with inappropriately broad privileges. In healthcare, security is complex, expensive and necessary to maintain regulatory compliance and brand protection.

Rapid Response Retainer is a solution that streamlines response in a cost-effective manner. It has customizable SLAs that govern the speed of response, cover flexible annual assessment options and weekly threat intelligence summaries, and offer add-on VTRAC capabilities including network telemetry analysis, endpoint telemetry analysis and dark web hunting. The Rapid Response Retainer can help hospitals survive attacks that could be catastrophic.

VTRAC reviews your response plan to make sure it's up to date and reflects your network's current reality. We also can help perform tabletop exercises to test it. Whichever options you select, the retainer is about preparedness and ultimately making sure that you have good plans in place when something bad happens.

Meanwhile, there are myriad ways customers can use the Rapid Response Retainer: examining web application servers for vulnerabilities, performing source code reviews and proactive threat hunting in the form of security health checks to double-check for undetected activity by threat actors. The goal is to give customers peace of mind that the VTRAC team is there for them around the clock, helping victimized enterprises shore up their defenses and quickly get on the path to remediation.

Stay ready

The time to prepare for an attack is long before anyone even thinks about targeting your organization. You need an experienced team on your side to help make sure there are no surprises lurking in your network, all doors are secured and there's a well-crafted action plan in place should something go wrong. Being ready reduces the very real risk to your reputation and your business.

Learn more:

Contact your Verizon Business Account Manager at 877.297.7816 or visit enterprise.verizon.com/products/security/incidentresponse to learn more.

verizon✓

1 *2020 Data Breach Investigations Report*, Healthcare Industry Report.

Network details & coverage maps at vzw.com. © 2020 Verizon. 000000000