Cybercriminals Target Healthcare Industry During The Pandemic

Insights
11.16.20

Several federal agencies have teamed up to warn healthcare employers of the increased threat they face as a result of malicious cybercriminals aiming to take advantage of the pandemic to wreak havoc on their operations. The Cybersecurity and Infrastructure Agency, the Federal Bureau of Investigation, and the Department of Health and Human Services recently issued a joint advisory based on "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers." The October 28 Advisory warns that malicious cyberactors are targeting this sector with malware, which can lead to ransomware attacks, data theft, and a disruption of healthcare services. What do healthcare employers need to know about this danger and what can be done to prevent such an attack?

Phishing Emails Are Most Common Threat
The Advisory warns that cybercriminals are executing their attacks by sending phishing emails to healthcare employees. These phishing emails appear to be routine, work-related messages but actually contain links that, if clicked by an unsuspecting employee, could expose the system to cybercriminals. For example, in November 2020, employees at multiple Boston hospitals received phishing emails that appeared to be the Department of Health and Human Services requesting COVID-19 statistics but were actually attempts to illegally access their systems.

Not only have the recent phishing attacks prompted the issuance of the Advisory, but they have also caused many healthcare organizations to restructure their cybersecurity focus. Netwrix's 2020 Cyber Threats Report analyzed cybersecurity concerns for healthcare organizations and how they have changed since the pandemic began. The report found that phishing attacks had been the sixth greatest cybersecurity concern before the pandemic but are now the single-greatest cybersecurity concern.

Consequences Of A Cyberattack In The Healthcare Industry
The Advisory comes just weeks after a German patient died during a cyberattack on the Duesseldorf University Clinic. Due to the attack, the clinic was unable to accept emergency patients, forcing this patient to travel to another facility. While authorities are investigating whether the delayed treatment led to this particular patient's death, this situation demonstrates the potential consequences of a cyberattack on hospitals and healthcare providers.

Not only could such an attack lead to disruption in patient care, but it could also compromise sensitive patient information. Since April 2020, hospitals in Georgia, Michigan, and Missouri have reported phishing attacks that resulted in the aggregate exposure of over 220,000 patients' personal and health information.

Playbook For Employers

Given the frequency of these attacks, healthcare employers may wish to consider requiring employees to complete additional training to ensure that employees can identify phishing emails. As part of this training, you may want to reinforce the devastating impact that a cyberattack could have on your organization and patients to ensure that your employees are taking the matter seriously.

Your organization can also perform phishing drills, where you send test emails to employees requesting that they click on a link. Based on the number of employees who click on the link, you can better determine how susceptible you would be to an actual phishing attack and make determinations regarding the need for additional employee training.

As part of your training, you may also consider educating employees on psychological and emotional factors that can contribute to a cyberattack. In a September 2020 report on data breaches caused by outbound emails (such as responding to a phishing email), Arlington Research found that 37% of the studied outbound email breaches resulted from employee stress and fatigue. The healthcare industry has front-line workers who are experiencing unprecedented pandemic-related stress at work with patients and at home with their families. On top of this, your remote workers may not have adequate separation between their work lives and their home lives, and may have additional personal responsibilities during the workday. An employee who is stressed, fatigued, or distracted may be less likely to discern a phishing email from a legitimate work email. By educating employees on how these factors can contribute to a cyberattack, your organization may reduce the likelihood of one occurring.

You may also want to consider your self-reporting policies, and related discipline, for employees who have fallen victim to a phishing attack. In its September 2020 report, Arlington Research found that 46% of employees who caused the breach were disciplined and, in 27% of the breach cases, the responsible employee was terminated. Given the associated risks, employees may be hesitant to self-report. This is especially true in the present time, with employees already having heightened concerns about job security in light of the pandemic. However, delayed reporting can materially impact the extent of the breach and the response time in addressing it, which can ultimately impact your organization's ability to resume full operations.

If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for addressing those threats, please consult your Fisher Phillips attorney.

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159
Email

Service Focus

Privacy and Cyber