akerman

Blog Post

Cybersecurity Attackers Target Hospitals Amidst COVID-19

April 13, 2020
By Christy S. Hawkins

Among the many obstacles facing businesses as a result of the COVID-19 pandemic are new cyberattacks targeting key infrastructure and industry in the United States. With all the compounding factors making this threat even more dangerous, the spike in cyberattacks was so significant that the International Criminal Police Organization (INTERPOL) has become involved and issued a "purple notice" alert to law enforcement in its member countries. The notice was issued as part of a coordinated effort to combat the attacks, and it alerts the public to information on the modus operandi, objects, devices, and concealment methods used by criminals. Since the World Health Organization's (WHO) declaration of COVID-19 as a pandemic on March 11, 2020, cybercriminals have targeted hospitals, COVID-19 vaccine testing facilities, healthcare workers, and even the WHO itself.

The cyberattacks primarily take the form of malware (including ransomware) phishing, (including email phishing, SMS phishing, phishing for credential theft, and phishing for malware deployment) and exploitation of possible weaknesses in technologies (including from out-of-date patches and security flaws). Employees working in new remote environments and with newly deployed technologies to facilitate working from home to prevent

Related People

Christy S. Hawkins

Related Work

Data Privacy and Security
Healthcare
Hospitals and Health Systems

Related Offices

Dallas

Health Law Rx

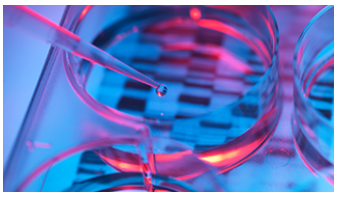
Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

Coronavirus Resource Center

Visit the Resource Center

transmission of COVID-19 are particularly vulnerable to these threats.



Many of the attacks aimed at hospitals have utilized ransomware, which locks away a hospital's critical systems and data, such as electronic medical records or billing systems, until the hospital pays a ransom to the attacker. Cyber criminals are exploiting for financial gain the urgent need to access information during the COVID-19 pandemic. When these attacks lock hospitals out of critical systems, such as electronic medical records, the delay in access could impact patient care, even potentially causing deaths, during a time when resources are already strained and every second counts in treatment response.

Phishing uses social engineering to trick an email recipient into clicking a link, opening a file, or providing their credentials based on a seemingly legitimate email. Phishing takes advantage of a person's natural reaction to urgent communications, such as requests from supervisors or other trusted senders. Phishing has become more successful and more prevalent in recent years, and the COVID-19 pandemic brings with it exactly the type of panic and curiosity that cybersecurity attackers can skillfully exploit. The phishing attacks can target hospital workers, individuals who live in areas significantly impacted by COVID-19 infections, and individuals who have transitioned to remote work environments. Many phishing attacks utilize the proffer of COVID-19 financial incentives, including government payments and rebates, as the lure. Others may include claims of real-time COVID-19 outbreak tracker, or even skillfully titled attachments or emails that masquerade as urgent communications to employees.

More detail about the COVID-19-related cyberattacks and how healthcare organizations and the public at large can combat them can be found at the U.S. Department of Homeland Security's National Cyber Awareness System Alert AA20-099A. To avoid falling

victim to a cyberattack, we urge increased focus on the following:

1. **Pause and assess**. Fear, panic, curiosity, and concern are the natural human reactions that make people fall for social engineering attacks. When a COVID-19 themed communication evokes one of these feelings, remind your team to pause and assess the situation and information before they decide how to handle the information.
2. **Be careful before opening email attachments.** You might be the last line of defense against a cyberattack. When in doubt, make a phone call to the person who sent the attachment, and make sure the call is to a phone number you already have for the person. This is difficult in practice, especially in times like these where quick action and response is of the utmost importance.
3. **Be on the lookout**. Individuals who remember their training and know what to look for are less likely to fall victim to an attack. Look out for common forms of phishing attacks. For example, employees should be warned about SMS phishing, which can be engineered as an urgent text message alert regarding the status of COVID-19 infections, relief payments, or other related information.

Fortunately, organizations can help combat these attacks by training their employees, keeping them updated as threats evolve through the pandemic response, and using the tools they have available to them. Organizations can also ensure that they are taking appropriate technical measures to protect themselves. These measures can include malware defense, regular backup schedules, and even routine patching, among others. Cybersecurity infrastructure in critical sectors will be as important in the coming weeks and months as it has ever been, and organizations will need to be vigilant to protect themselves. Further, organizations must remain flexible in order to adapt to rapidly changing

conditions to protect themselves against these attacks.

This information is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.