UPDATE ON PHISHING AND RANSOMWARE—

RESPONDING TO A SURGING THREAT

Jeanne S. Holden

In March 2021, Colorado Retina Associates (CRA) reported that a phishing incident had potentially exposed the protected information of nearly 27,000 patients. Phishing occurs when a fraudulent email or other communication is disguised to look trustworthy to induce individuals to share sensitive information or click on malicious links or attachments. An investigation found that an unauthorized party had accessed two CRA email accounts and may have copied patients' full names, birthdates, Social Security numbers, etc.

Phishing emails are often used to deploy ransomware, malware designed to hold computer files "hostage" until payment is made. In 2020, ransomware attacks on the U.S. healthcare industry surged. Ninety-two individual attacks occurred—a 60% increase from 2019—affecting more than 600 clinics, hospitals, and healthcare organizations and about 18 million patient records.[1] The estimated cost was nearly $21 billion—not to mention the impact on patient care delivery.

Cybercriminals took advantage of vulnerabilities caused by the COVID-19 pandemic and the explosion in work from home, said Erich Falke, chief information security officer/cyber risk practice manager at ePlace Solutions, Inc. (Fresno, Calif.). He explained, "When more employees remotely access a practice's environment, it increases exposure. Unsecure remote access creates more attack vectors, or opportunities, for cybercriminals to exploit."

INTENSIFIED ATTACKS

Early in the pandemic, leading ransomware gangs pledged to avoid hitting healthcare providers. However, their attacks not only increased, but also intensified. "Hackers initially used ransomware to extort money by denying businesses access to their own data," Falke said. "But, over time, up-to-date backups became almost a 'silver bullet,' enabling businesses to avoid paying ransom. Criminals didn't like that." So, they upped the ante.

Falke described the new approach, double-extortion ransomware: "Now, when cybercriminals infiltrate a network, they usually exfiltrate (i.e., steal) a copy of the data before encrypting it. Then, they demand, 'Pay a larger ransom (or two ransoms), first, to regain access to your data and, second, to keep us from making your data and the shutdown public.'" Such publicity could hurt a practice's reputation—or worse, Falke explained. For instance, in 2019, Brookside ENT/Hearing Center (Battle Creek, Mich.) closed permanently following a costly ransomware attack.

A STEPPED-UP RESPONSE

What circumstances compromise cybersecurity and increase the likelihood of cyberattacks? According to Falke, by far the two largest causes of ransomware attacks are unsecure remote internet access and phishing emails. Software vulnerabilities are a third cause, followed by others.[2]

He emphasized that "the gold standard for securing remote access is having employees use multi-factor authentication with either a virtual private network (VPN) or a remote desktop (RD) gateway." Both a VPN and an RD gateway allow remote users to connect to internal resources using an encrypted connection.

Falke detailed five other crucial steps for mitigating the ransomware threat:

1. Use unique and strong **passwords and two-factor**

authentication wherever possible, especially on remote access, email, and privileged accounts. “Criminals scan the public internet looking for low-hanging fruit,” Falke said. “Two-factor authentication adds a second layer of defense.”

2. Prioritize **employee training and awareness.** “Phishing attacks succeed when employees are in a hurry or not paying attention,” Falke said. “Any unexpected email or text with an attachment or link should be verified using ‘out-of-band authentication,’ that is, verification using a different communication channel. Never use the contact information in the suspicious message.” Phishing simulations are particularly effective for determining who needs more training, he said, adding “Compliment those who do well—perhaps give small prizes to the department that does best—but be careful penalizing those who don’t.”
3. Keep **software patched and up to date.** “Using outdated software or software that a manufacturer no longer services (e.g., Windows 7) creates vulnerabilities” that criminals will exploit, Falke warned.
4. Maintain **up-to-date, well-tested backups** for critical systems and data. Consider air-gapped backups. Falke explained, “Backups are air gapped when they are not connected to an operating environment so that they cannot get infected by a ransomware attack.” He continued, “Even cloud storage, which protects data from fire or flood, is vulnerable to ransomware. Attackers steal credentials and delete or encrypt cloud backups. In contrast, physical backup tapes kept offline are air gapped.” To cover all contingencies, practices might supplement cloud backups with physical tapes, Falke suggested.
5. Use **next-generation antivirus protection** throughout the system to the endpoints (desktops, mobile devices, servers, etc.). Falke pointed out that up-to-date antivirus software uses artificial intelligence and cloud-based analytics to detect suspicious activity that traditional antivirus software missed.

All of these steps are in addition to traditional good perimeter defenses like firewalls, Falke added.

SHARED RESPONSIBILITY

Being prepared starts by recognizing that every business, regardless of size, is susceptible to a cyberattack, Falke suggested. Consider: How would your practice be affected if you couldn’t access its systems—even for 10 minutes?

Next, create a strong security culture by making sure all practice doctors and staff feel invested. Falke advised, “Four 15-minute training modules are easier to digest than an hour-long module. Ask for feedback, and tailor training appropriately.” Above all, he said, “Be certain to convey an understanding of why security is important and what damage could be caused by a cyberattack.”

Finally, be prepared to respond if the worst happens. “Have an incident response plan ready and make sure everyone knows what to do,” Falke said, adding “Cyber insurance can play a vital role by getting you quick access to professionals who are experts on limiting the effects of a breach.”

“The earlier you take action with a suspected breach, the less damage there will be to your business and reputation,” Falke said. “Getting immediate help is critical.” ***AE***

> “In 2020, ransomware attacks on the U.S. healthcare industry surged. … The estimated cost was nearly $21 billion—not to mention the impact on patient care delivery.

NOTES

[1] Bischoff, Paul. (2021, March 10). Ransomware Attacks on US Healthcare Organizations Cost $20.8bn in 2020. https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

[2] For data for 2018-2021, see: Coveware. (2021, April 26).Most Common Ransomware Attack Vectors in Q1 2021. https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

Jeanne S. Holden (703-451-5903, jeanneholden@yahoo.com) is a freelance writer-editor based in Springfield, Va.