Cyber Security: A Rising Threat for Dental Offices

Ondrej Krehel, CEO & Founder of LIFARS


Ondrej Krehel

Cyber terrorism targeting smaller healthcare offices is increasing at an alarming rate. While these incidents do not get equal media coverage in comparison to attacks on multinational corporations and governmental agencies, a data breach at a dental office is arguably more disruptive to the victim because the associated costs can potentially bankrupt smaller sized businesses. Victims of cyber-attacks at medical offices are far reaching and often extend to the patients. A decrease in or a complete loss of trust towards their medical provider often occurs when patients learn that their SSN and other personal data are for sale on the darkweb.

Besides impacting the work flow, a patient's trust, and the general disruption of your business, a breach imparts many additional costs. First is the expenditure of money and time to investigate and remedy the problem. This can be an enduring process if your attacker is well entrenched in your environment. Next is the cost of notifying and protecting the individuals who may have lost personal information in the attack. A recent study of the healthcare providers' industry, estimates that each record compromised in a data breach costs nearly $1,000 to remediate. (http://www.cutimes.com/2015/11/04/data-breaches-cost-1000-per-record-study) Finally, there is a chance of litigation against your company. Thus, small businesses, like dental offices, that are faced with these compounding costs have a very difficult time surviving cyber-attacks.

Especially prevalent against medical offices are malware attacks, like ransomware, which takes a computer system hostage by encrypting files and demanding payment in return for unlocking them. Ransomware is one of the most widely used attacks against dental offices. Its popularity stems in part from patient data being valuable to hackers and identity thieves. In addition, a dental office will often have an immediate need to access patient data when serving clients and could easily be pressured to pay hackers for release of this information. Victims of ransomware often pay their attackers in as little as three days. This makes for a very lucrative, albeit illegal, business practice. The FBI, however, opposes paying the ransom because these payments encourage more ransomware attacks.

Ransomware, such as the popular Locky, Cyptowall, and PowerWare, is often spread through electronic messages that trick a user into opening an attachment or a link to a site where malware is downloaded onto the user's computer. Often sent by email, and sometimes social media channels, the messages that spread ransomware can appear to come from employees inside your organization.

Like all cyber-attacks, ransomware is evolving and becoming more sophisticated. Newer types of ransomware are targeting dental offices by breaking into their IT support system. Dental offices using a remote desktop connection for their outsourced IT services are vulnerable to brute force attacks of their remote desktop protocol (RDP) functionality (https://threatpost.com/655000-healthcare-records-being-sold-on-dark-web/118933/). A group from Russia is also reselling the compromised servers to other hackers on the dark forum, xDedic (https://lifars.com/2016/10/xdedic-marketplace-hacked-servers-go-sale/). An analysis of new attacks indicate that ransomware is waiting inside the environment for months, learning what is most valuable to the company and how to best harm the business, before encrypting files.

To protect yourself, dental offices need to take a proactive position to prevent malware from harming their business. The existing security infrastructure should be able to detect and prevent a breach of your system and if necessary, automatically clean any malware before a response is required. In addition, it is important to educate your employees to not open suspicious e-mails. The HIPAA compliance Ransomware Factsheet is useful in helping to inform your staff and business associates on how to prevent malware infections (http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf).

Moreover, it is vital that your organization follows the principles of cybersecurity best practices: "least privileges," "need-to-know," and "cybersecurity is never done." These principles, when executed correctly will mitigate the harm and costs associated with cyber-attacks.

"Least Privileges" and "Need-to-Know" is the practice of limiting rights and permissions to staff members based on what is essential to their job function. It is easy to compromise a network when a single user is granted too many rights. This can include ensuring that standard users do not have local admin privileges. Least Privileges and Need-to-Know prevents a compromise from causing excessive damage.

The third principle, "Cybersecurity is Never Done," addresses the ever-evolving nature of cyber-attacks. Because cybersecurity is an ever-changing landscape it is important to continuously test your system and maintain a good security posture. A system that was secure five years ago may be outdated and at risk today. This principle, Cybersecurity is Never Done, is especially challenging for dental offices and many small businesses. As technology ages, new vulnerabilities are found and usually patches are released, which must be considered for maintaining security. ■

LIFARS helps businesses keep up with proper update management and patch holes, or replace vulnerable systems. LIFARS provides risk analysis, user and staff training, and cyber threat monitoring to help companies to continuously stay current with the changing landscape of cyber-attacks.

For more information please visit www.lifars.com or call 212-222-7061.