DOTmed HealthCareBusiness news

Vulnerable to ransomware? It's not your servers – it's your people

May 24, 2024

Cyber Security

By Ron Zayas

While computers are now essential in every workplace, including healthcare organizations, that doesn't mean that most professionals who use them every day understand how easily they can be weaponized. Healthcare organizations have become a favorite target of thieves and ransomware gangs for a variety of reasons, starting with the critical services they provide. Shutting off access to patient records impacts appointments, surgeries, prescriptions, and even prognoses. When every second counts, the consequences of a comprehensive data or administrative failure can be fatal.

Given these inherent risks, hackers realize that there is a higher likelihood of their ransom demand being met. To pay or not to pay? Either way, the resolution is going to be expensive. Those who opt not to bow to extortion face a significant investment in restoring IT systems, as well as attorney costs and legal liabilities from the class action suits that inevitably follow a breach. Those who pay the ransom are not immune to these consequences either.

The most effective strategy to avoid becoming the next victim is to take preventative action that lowers the risk of a successful breach. While your servers may have been hardened to resist ransomware, hackers have shifted their focus to another vector of attack – your employees. Whether it's the CEO who has run the hospital successfully for a decade, or the new admissions rep hired just a few weeks earlier, each one has the power to prevent an infiltration opportunity.

Such attempted breaches are often successful due to the sheer number of personnel employed in many healthcare organizations. Add to this the growing sophistication of phishing emails, many of which now incorporate artificial intelligence (AI) that can be trained to quickly identify and focus on the most target-rich individuals—those who are more likely to accept a personalized email as authentic.

We're a long way from the old "Nigerian prince" scams; today, thieves leverage personal information from data brokers and people finder services. By combining this data with social media profiles, public records, school records, GPS data, and additional content from other online sources, scammers are armed to

customize a phishing email capable of misleading even the most vigilant recipient.

Few people would be taken in by a notice allegedly from Microsoft or eBay, mentioning an overdue invoice that needs to be paid. Such emails often contain spelling and grammatical errors that make them even more suspicious: “This will be charged immediately unless you tell us invalid is this invoice.”

But what if the email to your work address appears to come from a friend or coworker, and addresses you not by your name but by a nickname only known to those close to you? What if it also mentions your spouse or one of your children by name, and references a recent event in your life, such as a vacation or a new car purchase? The sender’s email address might look different (if it is even noticed at all), but with all these other authentic details, that variable could be attributed to a change in email providers. At this point, an invitation to click on a link to a photo may be accepted – once that happens, the hacker has won – he now has access to your company’s systems.

How did this information get out there in the first place? Usually, because we hand it over willingly. How gladly we’ll complete online requests for a product or service by filling in boxes on websites asking for our email address, our cell phone number, or other personal details that we might hesitate to reveal if someone inquired about them in person. That content is then collected, shared, or sold to anyone who asks for it. Just a few pieces of data can transform a phishing email from one that is highly likely to be deemed suspicious, to one that is very hard to detect.

We know these scams are working because of how many victims have been hit. Last year more than 45 healthcare entities suffered ransomware attacks, causing more than 140 hospitals to experience disruption due to the lack of access to IT systems and patient data. According to the Verizon Cost of a Data Breach Report, the average cost of a healthcare data breach reached $11 million in 2023, an increase of more than 50% in just three years. In 2022, the average ransom payment was $5,000; just one year later, it was approximately $1.5 million. And so far, 2024 is looking to be significantly worse.

How to protect yourself

Since all forms of AI feed on information, one of the most effective solutions is to interrupt this vector of attack by cutting off the pipeline of personal information about your employees online. When hackers have less information to exploit, they will likely look elsewhere for their next target.

Providing employees with a corporate account that monitors and eliminates the types of personal information that fuels attacks can cost just a few dollars per employee per year. These services not only lower the volume of available content, they can replace authentic information (home address, cell phone number) with alternatives that cannot be traced back to their user.

It is also important to educate your employees on the new and more convincing forms of phishing emails, and why it is important to verify any communication before clicking on a link that will infect a work computer.

Finally, stop treating the danger of ransomware as an IT issue. This is now a C-suite issue that should command attention toward enterprise asset protection and risk management.

Every day, publicly available private information is weaponized. One effective strategy to reduce the chances of becoming a phishing victim is to safeguard your employees and vendors by making them aware of the danger. This will help them understand their vulnerability and take action to keep themselves—and your organization—safer.

About the author: Ron Zayas is an online privacy expert, speaker, author, and CEO of IronWall360, an Incogni company. IronWall360 provides online privacy protection to both the public and private sector. For more insight into online privacy laws, proactive strategies, and best online data practices, visit ironwall360.com. Connect with Ron at ron.z@360civic.com or LinkedIn.

THIS ARTICLE ORIGINALLY APPEARED IN *DOTmed HealthCareBusiness news*:
https://www.dotmed.com/news/story/62944?p_begin=0