OPINION

Protecting against ransomware requires up-to-date operating systems

By James Savage

Feb. 29, 2016

Hollywood Presbyterian Medical Center recently went public with news of a so-called ransomware attack that had paralyzed its computer systems for 10 days. The episode affected patient care, including some emergency patients being sent to other hospitals.

Ransomware is a form of malware in which rogue software code effectively holds a user's computer hostage until a "ransom" fee is paid.

"It's no different from if they took all the patients and held them in one room at gunpoint," said California state Sen. Robert Hertzberg, who has introduced legislation to make a ransomware attack equivalent to extortion and punishable by up to four years in prison.

What's unusual here is not the event, but rather that the hospital went public. Usually, organizations try to cover over such attacks. In this case, the hospital paid $17,000 to the hackers in order to get their systems up and running again.

What are the most common vulnerabilities that enable hackers to pull of nursing homes and clinics protect their systems — and patients?

A little-recognized fact of information technology security is the significant role that operating system software plays in keeping attackers at bay. Modern operating systems incorporate sophisticated identity and access management (IAM) technologies that — when properly implemented — greatly reduce the threat of unwanted access.

Without modern IAM tools in place at the operating system level, organizations must cobble together access restrictions for each individual software application. That approach almost universally leaves security holes. If you were to ask a skilled information technology consultant how long it would take him or her to break into a computer system running an outdated operating system and create a new, unauthorized network administrator account, you'd probably hear "less than a week."

Unfortunately, this is the normal state of affairs. Health care organizations in particular have had to focus heavily on patient records and updated coding, often at the expense of the basic "blocking and tackling" needed for effective technology management. They are not alone. The dirty little secret in the information technology world: Organizations leave themselves open to threats — and potentially to extreme peril, as in the case of Hollywood Presbyterian — by delaying updates to their operating systems.

It's odd that such a basic need is so often ignored, but not especially surprising. Since the dot.com crash in the early 2000s, there's been a general malaise among IT departments concerning their perception of the significance of operating system maintenance. We estimate that a typical organization is two to three major operating system iterations behind.

One reason for this is reluctance to upgrade from a system with familiar features and interfaces. Another reason is software used in the organization's various lines of business may be incompatible with modern operating systems. IT managers often lament they can't envision updating an operating system for as many as five years from present because it's so difficult to update or replace old, legacy applications.

But in health care, especially, there is almost nothing more important than security. Recent news reports indicate that a person's credit card record might be worth about $20 on the black market, whereas his or her health record is worth $60. Security matters to patients during episodes of care as well as away from the hospital if records are compromised.

Events at Hollywood Presbyterian should serve as a wake-up call to business leaders to heed their IT departments' calls to ensure system software and configurations stay up to date. While it's also essential to train staff to recognize abnormal activity and threats, the single greatest impact on an organization's security is an ongoing commitment to keep operating systems current and properly configured.

James Savage is founder and president of Brookfield-based Concurrency, Inc.

0 Share Tweet Email Print

PART OF THE USA TODAY NETWORK

News Watchdog Opinion Sports Business Entertainment Lifestyle Green Sheet

Connect With Us

Facebook
Twitter
Instagram
YouTube
RSS
Mobile apps
Newsletter
Today's paper
Subscribe
Archives
Historical archives

Contact Us

Phone numbers
Manage account
Paid death notices
Back copies
Digital access FAQ
Classifieds
Display ads

About Us

JOURNAL SENTINEL

Partners

MyCommunity NOW
LIVING LAKE COUNTRY
metroparent
wisconsin trails
JSHomes
JSAutos CarSoup.com
JSJobs