LEGAL
MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

The Rise of Ransomware

By Michael Kemps

For years, the legal profession has practiced self-insulation. Combining a firewall with antivirus software was seen as the magic armor for protection. Keeping technology current by patching, upgrading and maintaining our legal technology investments were avoided and seen as unnecessary, painful costs. Today, the vulnerabilities of that armor have been detected and exploited.

We are experiencing an exponential increase in the number of threats to our technology environments. Our clients are demanding security audits and reviews to ensure their data is secure and compliant with their client's demands. Something has to change.

One of the greatest risks to law firms is ransomware and its attendant loss of productivity and theft of confidential information. Law firms are being exposed to malicious code that instantly encrypts files and data, with a demand for payment to unencrypt and release information. These variants are bringing unprepared firms to their knees by going as far as to render entire systems useless. Generally, the only way to recover is to undergo lengthy data restoration and to reimage local clients.

Information security policies must be developed and additional training provided to ensure users are aware of threats and how to avoid them.

There are a number of things that need to be done in order to control this onslaught.

1. SECURITY TRAINING AND POLICIES

Information security policies must be developed and additional training provided to ensure users are aware of threats and how to avoid them.

While most administrators feel users need more training to better recognize security-compromising events, i.e., email phishing attempts, many end users feel they are already able to spot when they are the victim of a sophisticated phishing attempt. The firm's IT department and management team must be on the same page when it comes to information security and the amount of training required to support the firm's directives and legal and ethical requirements. Update that training on a regular basis.

2. UPGRADE AND REPLACE OUTDATED TECHNOLOGY

All too often, law firms focus on retaining technology as long as possible in order to control or reduce costs. The risk associated with this approach is increased exposure to outdated applications and operating systems that are unsupported and more likely to be attacked by viruses and ransomware. It is best practice to retain servers for a maximum of five years, desktops for up to four years and laptops for three. Stretching the life of hardware and software outside of these timeframes increases support demand and business interruption risk. As we rely more on these tools, the need to keep them current greatly increases.

3. TAKE ADVANTAGE OF HIGHER PERFORMANCE INTERNET

Maintaining systems today requires downloading large software updates. Doing so consumes large amounts of bandwidth. Contact your Internet Service Provider (ISP) and request bandwidth usage reports over a 30-day period. Use fiber connections wherever possible, and ensure that firewall capacity is matched to the bandwidth utilized.

4. MAINTAIN SOFTWARE VERSIONS AND PATCHING

Keeping software, operating systems and applications patched and updated follows industry best practices. It is common for firms to implement system-wide upgrades and follow with leaving them as-is for long periods of time. This was previously done with the idea that stability would potentially be greater by not only achieving standardization but by maintaining a uniform platform. It is possible to achieve standardization while also patching an updating minor version updates firm-wide. Not doing so creates unacceptable vulnerabilities.

5. IMPLEMENT EFFECTIVE ENDPOINT PROTECTION

Simply installing antivirus software from a top-tier vendor is insufficient. Ransomware attacks are becoming commonplace. Antivirus software that depends on previously identified virus signatures is generally ineffective in combating malicious code. Wrappers, variations, packers and specific machine targeting are evasion techniques utilized to avoid and render antivirus software ineffective. Instead, consider implementing true endpoint protection (EPP) software that identifies attacks based on behavior rather than signatures.

6. UTILIZE NEXT GENERATION FIREWALLS AND UNIFIED THREAT MANAGEMENT

Investing in next generation firewalls (NGFW) with redundancy and sufficient processing power to provide unified threat management (UTM) is critical. Devices that simply provide network address translation (NAT) and port blocking are insufficient. Edge devices should prevent threats, including scanning for viruses, refusing denial of service (DoS) attacks and limiting unapproved web content — while simultaneously ensuring simple and consistent access to the services required to run the law firm.

7. LOCKDOWN POLICIES

Focus on services actually required within the law firm and provide options for desired ones. In order to preserve security within the firm, consider blocking services that the firm does not approve. Personal email accounts, social networking platforms, chatting services, media streaming and similar applications all demand bandwidth and increase security risks. Perform risk/benefit analyses. Support desired services with guest wireless access and firm-supplied and managed, mobile devices.

8. AUDIT OPEN PORTS AND SECURITY HOLES

There is no possible way to entirely secure an environment from external and internal threats. The best way to ensure that an environment is appropriately protected is to have it reviewed on a recurring schedule by an authorized third party. Reporting should identify open ports and applications, accounts and password policies, among other threats. Ideally, vulnerabilities would be reviewed quarterly and addressed. At a minimum, this should be done annually.

Security — and the protection and prevention of ransomware attacks in particular — requires a multi-layered approach. Technology environments within law firms are constantly adapting. We must remain steadfast in our efforts to stay current, protect ourselves and

transcend our paradigm by massively improving our vigilance.

ABOUT THE AUTHOR

Michael Kemps is the Founder and Chief Executive Officer at Innovative Computing Systems. He founded the company in 1989 after developing relationships with several law firms that eventually became early clients.

Email
LinkedIn
Twitter
Website

MICHAEL KEMPS
CEO
Innovative Computing Systems