SPRING 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics and cybersecurity needs. With the proliferation of data breaches, we chose to focus this E-Newsletter on the topic of encrypted email and transient messaging technologies and the impact on organizations.

SHOULD EMAIL ENCRYPTION KEEP YOU AWAKE AT NIGHT?

According to The Radicati Group's Email Statistics Report 2015-2019, the average office worker sent and received an average of 122 emails per day in 2015. For the average executive, he or she may be receiving 250 to 350 emails per day. Many of these emails contain sensitive or proprietary information requiring protection from prying eyes. Email encryption is the popular choice for secure email transactions, and the encryption technology continues to advance. As this advancement continues and threats abound, many companies ask, should we lose sleep over email encryption?

Sweet Market Dreams

The global email encryption market is expected to grow from $1.5 billion in 2015 to $4.2 billion in 2020, per forecasts from Research and Markets. Although this trend is positive for email security providers, and is a fantastic countermeasure to hackers snooping packets (i.e. sophisticated technologists intercepting your email and reading it in clear text), there are hundreds of email encryption software packages available making email security a potentially dizzying undertaking. The ecosystem is comprised of email encryption solution providers such as HP Enterprise, McAfee, Symantec, and TrendMicro, as well as open source providers such as ProtonMail, Open-Xchange and Tutanota. There are also many vertical solution providers that create custom solutions based on the unique business requirements and security needs of each customer.

Preventing a Nightmare

Many of us receive hundreds of emails per day of which several may reflect phishing attempts to obtain personal or corporate data. Some emails may transmit attachments designed to launch malware within your environment. Global hackers continually up their game and create more adept email ruses. As the volume of email traffic grows quickly, discerning legitimate email from potential threats is increasingly challenging. A sophisticated user can analyze Internet header information for Internet Protocol (IP) address routing, which is similar to tracing a letter for the location

movement from the sender to the recipient, however, an IP address can be spoofed and replaced with a fake address (e.g., the sender may be in China, but the email origin appears as if it's Atlanta). In addition, many health care, financial, and other organizations with sensitive data maintain facilities overseas; so, an IP address lookup may verify correctly that a sender is overseas and the communication could be legitimate.

Encryption software packages typically require recipients outside of the sender's organization to register through a special software package in order to decrypt locally in the recipient's environment, or to be able to read a message on the software provider's server. The software provider's email address may replace the email address of the actual party with whom the recipient was originally communicating, thus convoluting the identification of harmful email. A busy employee could foreseeably disregard, albeit unintentionally, a valid email as a phishing attempt or containing malware. If the employee is in a critical role, they may have 20 external vendors, all using different email encryption programs, with decryption keys that have to be maintained for future use. Passwords may have to be changed every 90 days, complicating the authentication process for employees tasked with managing external vendors. Some applications may not allow a password reset, resulting in permanent lock out from an important message in the event of a mismanaged password.

Discovery Dream Team

The complexity of processing encrypted email becomes exponentially arduous and opens up important issues for e-discovery and computer forensics professionals. If the email resides locally, case teams face difficult judgement calls regarding whether the encrypted email needs to be decrypted and converted to PDFs or are deemed inaccessible. If the email has an expiration period such as 30, 60 or 90 days in the ordinary course of business, is this considered spoliation if the organization did not archive the emails as part of the litigation hold process? For technologies that point to an email within a secure messaging platform hosted by a third party provider, does the organization have a duty to access these sites and print to PDF or some other export option as part of its discovery effort? Case law in this area is reactive in accordance with the pace at which relevant issues are heard by the courts. Until proactive guidance from judges, legislatures, and regulating bodies is promulgated, we can only look to what precedent has been established already. With more innovative secure messaging technologies on the rise, the discovery realm will be burdened with more challenges until further standardization happens.

When in doubt about the safety of an incoming email, contact the sender to validate the email is authentic prior to opening attachments or Web links. Until then, click with caution and try not to stay awake at night. You'll probably sleep better and be able to tackle the 200 emails waiting for you in the morning.

UPCOMING INDUSTRY EVENTS

June 2016
LegalTech West Coast, San Francisco: June 13-14

July 2016
The Masters Conference, Managing the E-Discovery and Social Media Minefield,
New York: July 19

August 2016
HTCIA 2016 International Conference & Training Expo,
Las Vegas: August 28-31

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: