Cybercrime has grown to be a multibillion-dollar black market industry with attackers constantly evolving tactics and selecting new targets. Healthcare organizations around the world, already on tight budgets and short on IT staff, are in a constant struggle to detect and fend off cyberattacks. Healthcare data is the most valuable data on the black market, and as a result Healthcare organizations are vulnerable. In fact, Tom Kellerman, chief executive of Strategic Cyber Ventures, recently stated that “the most exploitable industry in the world is the healthcare sector,” and declared that the industry is chronically being “hobbled by regulation and insufficient investment in computer security.”

For healthcare organizations, this is a dangerous combination of high demand and suboptimal defense, and just one attack can be catastrophic. Defending your data against cyberthreats requires a multilayer defense. This paper addresses five of the most critical cyberthreats of which IT healthcare professionals should be aware: ransomware, malicious URLs, malicious attachments, business email compromise and insider threats.
Five cyberthreats healthcare
IT professionals need to
know about

Ransomware

Ransomware is software delivered most frequently via a malicious URL or attachment. Once it infiltrates a computer in an organization it encrypts files and then moves to other computers and servers, blocking access to critical data until a ransom is paid. When ransomware hits, users can’t access the files unless the ransom is paid or the files are restored from backups.

Ransomware payments for 2016 are expected to hit a billion dollars, according to the FBI. That compares to just $24 million paid in 2015. Most recently, in May of 2017 the WannaCry/Crypt ransomware virus took down hospitals in the U.K.’s National Health Service (NHS), crippling daily operations and even stopping medical procedures.

Malicious URLs

A malicious URL is created with the purpose of downloading malware or harvesting user information. Phishing emails purport to be from a reputable company or person with the aim of compelling individuals to reveal valuable information, such as credit cards or passwords. Emails seem to use legitimate branding such as company icons, colors, and fonts, and obscure where the link is actually going. Malicious URLs can trick users into giving away confidential, sensitive, or valuable information. They can also allow intruders to covertly download protected or valuable information from a computer or the network—often without detection.

Malicious attachments

Malicious attachments are how cybercriminals transmit damaging payloads to a computer or network. Malicious code often lurks in office attachments with macros or in executables masquerading as legitimate documents.

Other attachments will download malware from a command-and-control center rather than be delivered via the attachment, which gives attackers more flexibility. When users open a malicious attachment, the payload can install a virus, a key logger that records keystrokes, or give a cyberthief remote access to a computer, or even the network.

Like URLs, malicious attachments can provide intruders with access to sensitive or valuable information on the infected computer or the network.

---


3 “Eleven of 14 NHS health boards hit by ransomware cyber-attack,” BBC News, May 12, 2017
Business email compromise

Business email compromise, also called whaling, has no malicious payload. Whaling is a form of “spear phishing,” where fraudulent emails appear to come from inside the organization or from a trusted sender.

Ransomware is a carefully crafted scam that targets high-profile employees with access to valuable information or the authority to transfer large sums of money. These attacks are well researched, and are targeted to finance employees who control money, human resources employees who have access to personal information, or a group that has access to patient info.

Attackers identify an employee in the organization, research that individual on social media, including LinkedIn, then use a spoofed domain to send an email that looks like it comes from his or her boss or a C-level executive. After a personalized message and warmup, the attacker looks to incite the action that will funnel the money or information to the attacker. A sense of urgency is often applied to get the target to act immediately.

Internal threat

A malicious insider is an employee who has intentions of stealing data or damaging the organization. Malicious insiders are pretty rare but given their position can cause outsize damage. Examples include:

- Disgruntled employees
- Former employees
- Vendors, contractors or partners with inside information about security organizations or computer systems

A compromised insider is an employee who knowingly or unknowingly gives someone with bad intentions access to valuable and sensitive data, or has the ability to send email that looks like it’s from a legitimate internal user. In the case of a compromised computer or account, the threat actually originates from inside the organization.

A careless insider causes security incidents because that individual doesn’t know, or isn’t paying attention to, security hygiene. Examples include:

- Accidentally sending patient records or sensitive emails to the wrong people, or not encrypting sensitive data sent to the right people
- Accidentally introducing malware to the network by visiting malicious websites or opening malicious email
- Forgetting to log out of a computer, accidentally giving someone else access to busy clinical environments

Cybercrime in the U.S. and U.K.: The threat is clear and present

Cybercrime incidents in the U.S. and U.K. are growing in number and consequence. In the U.S., 90% of healthcare organizations have suffered a data breach, and 50% of those breaches were because of an attack.\(^4\) Attacks frequently target the U.K.’s NHS, which holds large quantities of sensitive patient data and provides online services relied on by the whole country.

In fact, when surveyed, more than one-third of U.K. health trusts admit to being hit by hacking attacks in the past 18 months.\(^5\)

---

4 Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2016

5 “NHS trusts become top target for ransomware campaigns,” ZDNet, Feb. 2, 2017
Costs and consequences of cyberattacks in healthcare

For healthcare organizations already struggling with tight budgets, increasing regulations, performance demands, and not enough staff, cyberattacks can be devastating. Costs and consequences include:

- Data breaches, or unauthorized access to personal, health or financial data that remain exploitable for years
- Hospital shutdowns, including hundreds or thousands of appointments canceled while a cyberattack incident is investigated
- Regulatory fines resulting from violations of the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., the Payment Card Industry Data Security Standard (PCI DSS) in the U.S, the Data Protection Act in the U.K., and the General Data Protection Regulation (GDPR) in the EU.
- Caregivers forced to use pen and paper, rather than computers, to capture patient information and draft patient letters
- Brand damage
- Operational impacts and inability to provide critical patient care, causing serious risk to patient safety
- Irretrievable data loss
- Lawsuits

Cyberdefense best practices

If healthcare organizations are to survive and thrive in the modern threat landscape, a multipronged solution is needed:

1. **Targeted threat protection** to defend against ransomware, spear phishing, whaling and unknown threats across any device, anywhere
2. **Secure messaging** so you can share confidential and sensitive information safely and securely
3. **Content control and data leak prevention** to control the distribution of sensitive information with gateway policies that block, hold or encrypt confidential data
4. **Internal email protection** to stop malicious, compromised and careless employees from damaging the organization
5. **Spam and virus protection** to stop spam and viruses in the cloud before they can impact email

Conclusion

As healthcare organizations struggle to keep up with ever-changing technological developments, one of the most sinister challenges they face is growing cybercrime. Healthcare data is incredibly valuable on the black market, and healthcare organizations have proven to be a frequent target. Defending your data against cyberthreats requires a unified approach with email security at the foundation.

About Mimecast

Mimecast Limited (NASDAQ:MIME) makes business email and data safer for more than 26,400 customers and millions of employees worldwide. Founded in 2003, the company’s next-generation cloud-based security, archiving and continuity services protect email, and deliver comprehensive email risk management in a single, fully-integrated subscription service.