ARTICLES

Trends in Ransomware

By Rob Rosenzweig

Aug 15, 2018

At some point, any business could be faced with a malicious ransomware attack. As cyber criminals grow more sophisticated, ransomware attacks are becoming more destructive year after year, and the cost to companies in remediation, lost revenues, business interruption and reputation is steadily on the incline.

Some trends have started to emerge in the past year.

Ransomware is on the rise. By far and away, ransomware is the fastest growing attack pattern we're seeing. In fact, 2017 could be called the year of the mega ransomware attack. WannaCry, which essentially crippled the U.K.'s National Health Service computer systems, forcing hospital closures and cancellations of critical appointments and surgeries, was the beginning of the ransomware tidal wave.

A month later, NotPetya became the most destructive global ransomware attack to date, costing over two billion dollars in a single quarter in business interruption to companies across Europe. Originating in the Ukraine, the attackers targeted companies including Maersk Lines, Merck & Co., DHL, FedEx and multinational law firm DLA Piper, to name a few. The shipping line Maersk alone estimated between $200 and $300 million in lost revenues during the attack.

Had the same ransomware hit systems in the U.S., the cost would have been significantly higher. But it's not just large, multinational corporations that are feeling the impact of ransomware attacks. Enterprises across all industries, geographies and sizes are being targeted.

Higher demands. Another trend we're seeing in ransomware is that extortion fees are going up. A couple years ago, ransoms were routinely in the thousands of dollars range. Today, those demands are generally running into the six- and high-seven-figures, to be paid in bitcoin and other digital currencies.

Whether or not a company should pay the extortion fee depends on how good their controls are prior to the attack. If a company has a robust daily back-up to restore their system, and the cost of remediation is less than the ransom demands, then there's no reason to pay.

Additionally, there's no guarantee of honor amongst thieves in cybercrime. In other words, even if you pay the extortion fee, your data will not necessarily be restored uncorrupted. It's important to hire experienced

vendors who investigate ransomware incidents. They will most likely be able to recognize whether it's a legitimate claim, or if paying the ransom only marks you as an easy target for future attacks.

More destructive malware. As cybercriminals fine-tune their skills, the malware they're creating is growing increasingly destructive in nature. Older forms of malware operated by simply locking companies out of their data. If a company didn't pay the ransom, then it risked losing the data forever. Today's malware has taken destruction to a whole new level, infecting not only a company's data, but the hardware on the systems themselves.

For example, when the international law firm DLA Piper was hit in the NotPetya attack, it wasn't just the firm's digital data that was compromised – their hardware was corrupted as well. Piper attorneys all over the world were told to unplug their devices, phones and laptops while the company bought new ones.

Fortunately, another trend has emerged. That is, cyber insurance is becoming more affordable and accessible than ever before. Media attention to cyber events in the last year has helped drive market demand of cyber insurance. Recent laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018, have shined a light on data breaches in which personally identifiable information has been compromised. And while much of the media focus has been on data privacy and consumer protection, state and federal compliance laws that govern the reporting and remediation of data breaches have helped create more transparency.

As a result, the demand for cyber insurance has grown. Today, even if you're a smaller company, cyber insurance is affordable, accessible and covers more damages related to cyberattacks than ever before. Insurance products are available to cover the costs of business interruption, remediation, and even the expense of replacing hardware.

For more information on how to protect your business against cyberattacks, contact rrosenzweig@risk-strategies.com.

TAGS:
Cyber Liability