strategy+business

ONLINE MAY 16, 2017

Cybersecurity after WannaCry: How to Resist Future Attacks

A few key habits and attributes can help protect companies from ransomware — now and going forward.

BY DAVID BURG AND SEAN JOYCE

pwc | strategy&

Cybersecurity after WannaCry: How to Resist Future Attacks

A few key habits and attributes can help protect companies from ransomware — now and going forward.

by David Burg and Sean Joyce

The ransomware attack known as WannaCry first struck on Friday, May 12, 2017, and by the following Monday, it had reached more than 200,000 computers in 150 countries. Although we still don't know all the details, it's clear that some organizations were victimized far more severely than others. The news of this episode reinforces a view that we at PwC have promoted for a long time: Effective protection against cyber-attacks has less to do with any particular technological factor, and everything to do with proactive risk management in general.

Like all ransomware, WannaCry damages companies in two ways. First, it costs the organization to recover the documents that the algorithm has encrypted. Second, even if the ransom payment is small — and there's no guarantee that future ransomers will limit theirs, as was the case with the WannaCry fee, to US$300 in bitcoin — the costs of coping can be immense. Research conducted by PwC found that most ransomware incidents resulted in hours of downtime or networks taken offline for up to 10 days. Moreover, the attackers still hold any proprietary data they picked up. They can sell it or release it publicly, even after the targeted company has paid a ransom.

We expect there will be more attacks because the techniques and exploits used to distribute WannaCry were only recently leaked to the world in April 2017 (allegedly from the National Security Agency by an anonymous group called Shadow Brokers). Similar documents (allegedly originally from the Central Intelligence Agency) were published by WikiLeaks in March 2017, and there will probably be more such leaks, not just in the U.S. and Europe, but in countries around the world. Every breach will empower independent actors with tools heretofore held by governments. Ransom, blackmail, surveillance, shutdown, and data manipulation are all more feasible than they were only a few months ago.

All companies and organizations must now ask themselves the same question, whether they were affected by WannaCry or not: How can we protect ourselves from similar attacks in the future? Here are five key factors that separate vulnerable companies from more resilient enterprises.

1. Robust digital hygiene. The WannaCry event highlights the importance of vigilant IT management: staying up to date with technological advances. Microsoft released its patch for WannaCry's Windows vulnerability in March 2017. Companies that promptly installed it were protected, while many of the hardest-hit companies were using outdated operating system software and even pirated software. Robust hygiene also involves rigorous backup practices. For example, don't just back up your company's data. Test the backups regularly. Secure them so they are separate from your

David Burg
david.burg@pwc.com
is a principal in the PwC US advisory practice. He is PwC's global and U.S. cybersecurity leader.

Sean Joyce
sean.joyce@pwc.com
is a principal in the PwC US advisory practice. He leads the firm's cybercrime unit, focusing on cybersecurity, anti-money laundering, fraud, and anti-bribery/anti-corruption. Previously, he was deputy director with the U.S. Federal Bureau of Investigation.

Also contributing to this article were PwC US partner Thomas Archer, PwC UK partner Kris McConkey, and PwC US directors Adam Malone and Mark Ray.

other systems or networks; otherwise, they will be corrupted as well.

2. The ability to detect intrusive behavior. Human error is still the most prevalent means of gaining access to proprietary information. Employees often unwittingly expose data to a cyber threat actor through a fraudulent email or other socially engineered techniques, thereby giving hackers access to passcodes or other means of entry. Organizations with effective risk management practices rarely release sensitive information to outsiders inadvertently. They are particularly protective of administrative accounts and other privileged information; they make it extremely difficult to obtain the kind of data that would allow someone to take over a system. They are also attuned to detection, learning to recognize the keystroke behavior common to intruders and isolate it in real time. The one thing they share openly is the data about the intruders they detect; collaboration among security professionals from a wide range of organizations is one of the best defenses against cybercrime activity.

3. Thoughtful design of IT infrastructure. Every company has its own most valuable information assets: critically important intellectual property, proprietary customer-related data, financial data, and other strategically valuable insights. These must be protected differently from other information assets. Design your systems accordingly. Pay particular attention to your information supply chain: Which vendors, suppliers, and partners have access to your data, and what are they doing to secure it? Rethink your authentication and security controls; for example, introduce two-factor authentication, in which a password must be combined with biometrics, tokens, or some other authentication factor.

4. Advance planning and rehearsal. In the same way that you have developed advance plans for floods, fires, and other emergencies, prepare for cyber-attacks before they occur. The plans should specify how you will respond if there is an attack, and who will be accountable for which aspect. (For example, who will head up the information chain that notifies customers if their credit card information is stolen — the chief risk officer, the chief information security officer, or someone else?) To prepare for ransomware attacks, set up a decision matrix. Who will retrieve the information from a backup? Who will communicate with the data kidnappers? Under what last-resort circumstances — for example, a threat to life — might you be forced to pay the ransom? Think through all of this in advance and rehearse your responses. If a crisis does occur, you will already know what to do.

5. Early adoption of cloud technology. Cloud-based systems are updated easily and automatically in one lo-

cation, accumulate data in real time about attacks and intrusions, and incorporate built-in constraints that separate software layers and block intrusive software from reaching fruition. This gives them an edge over systems that rely on computers on the premises. It may also be relatively difficult for intruders to exploit holes in cloud-based architecture. For example, in late April 2017, Google blocked a spear phishing attack (an attempted use of targeted email to get people to send compromising information); the cloud-based aspects of Gmail software enabled it to rapidly identify and isolate the intruding malware.

Of course, even if you have these five attributes in place, you cannot be complacent. The most effective companies have focused on developing their cybersecurity acumen. New ways of approaching your computer systems will become a way of life: preventing intrusion; preparing for your response (including separating your backups from your network); detaching your backups from the rest of your activity; responding rapidly and effectively to intrusions when they occur; recovering, if necessary, with measures you have put in place ahead of time; and building resiliency. When these activities have become ingrained in your company, then your prowess at managing cyber risks becomes a strategic asset. If you can do that, you can also master many of the other management challenges in our increasingly complex business environment. ✚

strategy+business magazine
is published by certain member firms
of the PwC network.
To subscribe, visit strategy-business.com
or call 1-855-869-4862.

- strategy-business.com
- facebook.com/strategybusiness
- linkedin.com/company/strategy-business
- twitter.com/stratandbiz

strategy&