Accellion

How to Defend Your Business Against Ransomware

Ransomware is more malicious than ever, but protecting yourself is easier than you think

A lot of businesses think ransomware is a threat they just have to live with and hope the damage can be minimized. They're not wrong. But even companies that are resigned to the possibility of a ransomware attack often neglect to take simple steps to protect themselves. Maybe it's because business leaders aren't aware of how ransomware has evolved.

Originally, ransomware was conceived by hackers as yet another way to monetize security vulnerabilities. But now, ransomware has been weaponized by sophisticated hacking organizations that don't care about money—they are employed by nation-states and saboteurs to bring enterprises to their knees. In the attack against shipping giant Maersk last year, analysts believe the intention was not just to hold the company's data hostage, but to completely wipe it out of existence.

The costs of these types of attacks are significant, to put it lightly. In 2017, Maersk, the global container shipping leader that transports approximately 20% of the world's freight, reported a $264 million loss for their fiscal second quarter; in that same quarter the previous year, the company had reported a profit of $118 million. Estimates on how much ransomware will cost businesses around the globe range from $5 billion (according to industry analysts) and $1.7 billion (according to the FBI).

Why is ransomware so popular with bad actors? Why not hurt a business with a DDoS attack or ruin a competitive advantage by stealing intellectual property? Why go after all the data?

Data is your organization's most prized asset

Data is increasingly becoming an organization's most critical asset. Data is accumulated from computers, mobile endpoints, and IoT devices, and fed into systems that can parse and analyze at scale. Data is the oil that fuels growth and creates competitive advantages. Its loss can destroy a company's viability.

Every organization should assume it will be the target of a ransomware attack at some point. But no organization should assume it's helpless to protect itself from a ransomware attack. Definitive, concrete steps can be taken.

1. Protect your organization

The first defense against ransomware is to secure your network against malware. Most importantly, use a current operating system that includes the latest security features and capabilities. Hackers are very aware of critical security vulnerabilities in older operating systems, software and applications. These vulnerabilities present an open door for hackers to inject ransomware or other forms of malware. Therefore, it's imperative that you install any and all patches available for the software or systems in your organization. Change any default admin passwords, be stingy with write-access permissions, build a culture that takes security awareness training seriously, and use an FSRM to block ransomware changes to file servers.

2. Backup all your data and test your recovery plan

The most important action a company can take to protect itself is to have a good backup and disaster recovery system. While every business does some sort of backup, most aren't sure if they're backing up everything. Poor data recovery contributes to ransomware risk. As a result, it's critical that you back up all of your data on a frequent and recurring basis.

Accellion

3. Deploy a secure enterprise content access layer

When shared network storage attached to an infected machine is encrypted, entire departments can lose content—even losing backup files if they were mapped to the compromised machine. Companies that use a secure enterprise content access layer can safely share files, even if accessed from an infected system. Secure content access layers make recovery after an attack significantly easier and faster.

4. Never pay a ransom—not even a little one

As soon as your organization pays a ransom, the original attacker sees you as an ATM. The payment you send this week practically guarantees you'll experience another attack next week. And the original hacker will bring friends. As soon as the news of your surrender gets out (and it will), all the denizens of the dark web will turn their heads in your direction and start licking their chops.

If you have followed the steps recommended here, namely: installed all neccessary patches, backed up your data, and applied an extra security layer around your content, you will be less susceptable to a ransomware attack and the debate on whether to pay or not to pay a ransom becomes much less of an issue.

Refusing to pay may be a hard case to make to the board of directors. The cost of paying a ransom may be less than the cost of lost data and subsequent repercussions but it pales in comparison to the impact it will have on the business long-term. Why? Because the first attack is just that – the first attack. There will be future attacks and each will be costly, probably increasingly costly. Have a backup and recovery system in place that covers 100 percent of your data, and you will be invulnerable. Refuse to pay and call the FBI.

Share sensitive data securely with Accellion's secure file sharing platform

Accellion is an essential component of a reliable anti-ransomware plan. Accellion's secure file sharing platform integrates with your organization's existing security infrastructure to provide a security layer around all the systems that hold your content. All incoming files are scanned for viruses (AV) and Zero-Day attacks (ATP) so malware doesn't have a chance to infect your organization because it never gets into your network unchecked.

Ransomware may be inevitable, but you can significantly mitigate the risk. Pair kiteworks with a secure backup and recovery plan, and take back control of your data.

Is Your Anti-Malware Ecosystem Complete?
Contact Accellion today

Accellion, Inc. enables enterprise organizations to securely connect all their content to the people and systems that are part of their critical business processes, regardless of the applications that create that content or where it is stored, while maintaining the controls and visibility needed to demonstrate compliance. Accellion's solutions have been used by more than 25 million end users and have been installed at more than 3,000 of the world's leading corporations and government agencies including NYC Health + Hospitals; KPMG; Kaiser Permanente; Latham & Watkins; National Park Service; Umpqua Bank; Cargill; and the National Institute for Standards and Technology (NIST). For more information please visit www.accellion.com or call (650) 485-4300. Follow Accellion on LinkedIn, Twitter, and Accellion's Blog.

Email: sales@accellion.com
Phone: +1 650 485 4300
Accellion, Inc.
1804 Embarcadero Road
Palo Alto, CA 94303