INSIGHTS

Cyber made simple.

one brightly cyber

RANSOMWARE CAN BE FATAL TO SMALL BUSINESS

BY JAY BORDEN

Ransomware is a scourge that affects businesses of all sizes. While larger companies may have the resources to recover in most cases, for small businesses, ransomware can be devastating or even fatal.

The 2023 Data Breach Investigation Report from Verizon reports $26,000 is the median Small Business loss for a ransomware attack. But it can go as high as $2.25 million.

Those amounts only look at the ransom itself and costs of restoring the systems. Don't forget the other impacts on the business. How long can you survive unable to process sales, issue invoices, or deliver product? Recovery can take days or weeks. What if your customers lose faith in you and go to your competitors?

What if employees lose faith in the company and find jobs elsewhere? The loss of the employees and their institutional knowledge can be damaging.

What can you do? Certainly, use good security tools and purchase cyber insurance. However, tools have not blocked all ransomware attacks, or you wouldn't read about them in the news. Cyber insurers are limiting coverage in ransomware attacks.

What else to do? Adapt the least privilege approach. This means that no one has access to any applications or data that isn't specifically needed for their role. Even if they need access to it, they may only need view access and not the ability to write, edit or download anything.

By limiting access attackers and ransomware may also be able to encrypt less. This can increase the ability to restore using backups. With ransomware attackers stealing information first to use as leverage to convince you to pay, limiting access may reduce the amount of information they are able to steal.

onebrightlycyber.com
(888) 773-1920

INSIGHTS

Cyber made simple.

Ransomware Can Be Fatal To Small Business

Continued

Limit who has access to tools and connections. Remote Desktop Protocol, a popular protocol used by Help Desks to help users is often used by cybercriminals to access systems to infect them.

PowerShell is another way attackers compromise systems. Disable PowerShell on end user systems as very few users need it.

Use phishing resistant Multifactor Authentication, MFA. This will help keep attackers out even if they have stolen credentials.

The most important protection method is training. Research shows people are responsible for the vast majority of successful attacks. They click on a bad link, provide credentials in response to what they believe is a legitimate request from an authorized person or more.

Training needs to be frequent and in ways that keep their attention. Create a culture of security. Teach everyone it is far better to report that you fell for something than try to hide it. By reporting it quickly you can help minimize the damage done.

Remember, damage done to a small company affects all the employees as well as the clients and the company itself.

Of course, you need to have an incident response plan and a communications plan created in advance and tested in advance.

Waiting until a breach occurs is too late and significantly reduces your chances of surviving it.

Let One Brightly Cyber help you understand this in more detail and take the necessary actions.

Need help or guidance? Learn how we can help you in so many ways.

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.