REVALSYS
CREATING POSSIBILITIES

TIPS YOU CAN USE
TO PROTECT YOUR BUSINESS FROM RANSOMWARE ATTACKS

Article from Revalsys Technologies

This article explains about the tips to use to protect a business from ransomware attacks

More and more businesses have been establishing an online presence during the pandemic, which has resulted in an unprecedented growth in cyberattacks on businesses. A ransomware attack is the most common type of cyberattack today that takes advantage of loopholes in the security programs of businesses. Ransomware is a kind of malicious software that cybercriminals install in the systems of their victims without them knowing. In this type of attack, the attacker hacks into your entire organization's systems and encrypts or locks its data till you pay him a ransom. The demand for the ransom often comes with a deadline of 24-48 hours, and in the form of bitcoin as it is untraceable.

How You Can Safeguard Your Business From Ransomware Attacks

Don't Pay The Ransom

Businesses are common targets of ransomware attacks. These attacks put sensitive customer data at stake along with a business's reputation, which is why businesses tend to pay the ransom quickly to get access back to their data immediately. Paying your hackers ransom encourages them to continue attacking you in the future. It also results in more cybercriminals launching ransomware attacks on you and on other organizations. There is also no guarantee that you will get access to your data back after paying the ransom.

Update Your Software Regularly

The vulnerabilities in your software and operating system serve as gateways into your systems for hackers. Make sure that you have your systems' antivirus and antimalware set to be updated automatically in frequent intervals and that your operating system is equipped with the latest security patches. Keep checking frequently for new software and OS updates to keep your systems protected from ransomware and other cyberattacks.

Have Multilayered Security

Just using antivirus is not enough to keep your systems secure. Antivirus is not equipped to protect your systems from other kinds of threats. Multilayered security systems are those that use multiple methods to safeguard data on different levels and devices. Some of the types of security you can use for your systems are firewalls, email and data encryption, spam filtering, two-factor and multifactor authentication, etc.

Create Data Backups

You should back up your company data on a regular basis. However, having just one backup copy of the data won’t be enough. You should create multiple copies and store them in online and offline locations. Doing this won’t protect your data from ransomware or other cyberattacks but it can help you to recover your data quickly from backup locations and ensure smooth business continuity in the event of an attack.

Conduct Employee Awareness Training Sessions

Employees are most vulnerable to cyberattacks and are also the first line of defense against these attacks. Most cyberattacks are a result of human error or ignorance. This can be avoided by providing awareness training to employees. Teach them to recognize malicious software, fake ads, and emails containing malicious links, and educate them on the actions to be taken upon receiving such emails.

Enable Spam Email Filters

Ransomware, like other viruses, spreads through phishing emails that contain malicious attachments and links. Senders of these emails gain the trust of their victims by posing as their family, friends, or colleagues, which makes it easy for the victims to fall for them. When you have spam email filters enabled on your company’s email, they scan for and block emails that contain suspicious content or addresses.

Use Multifactor Authentication

Multifactor authentication involves using multiple methods of verifying a user’s identity before allowing them to log into a system. Authentication methods include passwords, biometric authentication, etc. When you use multifactor authentication on your company’s systems, even if your password gets hacked hackers won’t be able to go through the rest of the security measures.

Perform Risk Analyses

Risk analyses can help you to determine if your organization’s systems are secure enough and let you know which are the vulnerable areas in the systems. You should get these analyses done on a regular basis by leading experts in cybersecurity who are aware of the latest cyberattack techniques and cybersecurity threats facing businesses.

REVALSYS
CREATING POSSIBILITIES

CONTACTS

For more information on Revalsys Technologies, visit www.revalsys.com

8-2-293/82/1/83-A, 1st Floor,
Road No 12, Banjara Hills,
MLA Colony,
Hyderabad - 500034
Telangana, India

Phone: +91 7032660301

info@revalsys.com