Digital Security
Progress. Protected.

Ransomware: How to protect your company against attacks

Ransomware is one of the most potent threats to modern business, targeting organizations both large and small. To conclude our series exploring the various techniques used by cybercriminals to drop ransomware on corporate networks, we'll explore what organizations can do to ensure they can mitigate the risk.

Education

It is vital to educate staff on the attack vectors cybercriminals use to get ransomware onto the network. There's a reason they continue to use malicious links and infected attachments within emails: because it works.

Share the knowledge and get teams to undertake regular Cybersecurity Awareness Training. Employees who recognize phishing, avoid online scams and understand the techniques cybercriminals use add a vital layer of protection for the business.

Make it clear that staff should report suspicious messages and attachments right away. Early warnings can help an organization tweak its spam and content filters and bolster its firewalls and other defenses.

Make sure you have a plan in place in case a threat is reported, and that you can execute it when necessary.

Segmentation

To maximize its impact, ransomware is designed to spread to as many machines on your network as possible. Therefore, limiting the number of machines that an attacker can reach from a single entry point means you can limit the damage.

There are several approaches to implementing such a strategy, but the most common is network segmentation. This is particularly relevant in the cloud, where low cost and the relative ease with which new servers can be provisioned make it a fertile hunting ground for cybercriminals. **Whether on-premises or in the cloud, make sure every part of the network is properly authorized and securely configured**.

Patching

You need to stay ahead of the bad guys. Timely patching of applications and operating systems closes off potential avenues of attack. Plus, even if a ransomware attack does manage to penetrate your network, **patching can reduce the damage caused**. However, it can be more complicated than it sounds. It is always recommended to thoroughly test patches before they are deployed.

An intelligent, multi-platform patch management solution is highly recommended. It provides businesses with complete visibility over their systems, enables them to fix vulnerabilities before they are actively exploited and lets their teams know what to patch and how.

Back up data

Today, there is more data to be backed up than ever before. The volume of data created, captured, copied and consumed worldwide is expected to reach 181 zettabytes by 2025. A properly managed backup and recovery program provides a safety net for organizations and is crucial for recovery efforts should ransomware strike.

An all-in approach is needed, though. Unless the backup strategy is comprehensive, there is always a chance that the purveyors of ransomware will find that one device that was not backed up. **Backing up data and system state on all endpoints, servers, mailboxes, network drives, mobile devices and virtual machines is crucial**. When backing up data, organizations shouldn't underestimate the usefulness of write-once media. Files stored on media that is not rewritable are immune from the predations of ransomware.

Comprehensive protection

To best protect yourself against the scourge of ransomware, ensuring you have a comprehensive cybersecurity strategy is vital. It is important to implement the latest patches, back up your data, segment your network and educate users. All of this should then be underpinned by implementing a robust, award-winning security solution.