Top 9 Things to Keep in Mind to Avoid Ransomware Attacks

Ransomware attacks are getting bolder and more widespread than ever. Company size and industry no longer matter as criminals search for an easy entry point into the network. Here are 9 tips on how to increase your chances at battling against ransomware attacks.

Email gateway security and sandboxing

A secured email gateway protects against email-borne threats. Sandboxing enhances protection by filtering unknown sources before it reaches you.

Web application security/ firewall technology

Secure your web applications with a web application firewall (WAF) through web filtering and traffic monitoring to reduce your attack surfaces.

Threat Intelligence sharing

Leverage on threat intelligence from a reputable security services provider which gives real-time actionable insights to help fight against unknown threats through information sharing.

Protecting endpoint devices

As threats are constantly evolving, traditional antivirus is no longer enough. A next-gen endpoint detection and response (EDR) is imperative to deliver advanced, real-time results to detect and defuse potential threats.

Data backups and incident response

Performing and testing data backups regularly is key to ensure swift data recovery in times of need. A robust incident response plan is essential in ensuring your business is prepared should an attack strike.

Zero trust implementation

Practice zero trust, a security model that is based on the belief that no one (internal and external parties included) should be trusted unless their identification has been thoroughly checked and authenticated.

Firewall and network segmentation

Partition your network according to business need and grant access according to role and current trust status. Every network request is inspected according to the requestor's current trust status. This is to prevent lateral movement of threats within the network.

User training and good cyber hygience are key

Humans are often the weakest link. Hence, it is key for employees to undergo ample training as well as training refreshers so that they know what to look out for. Likewise, businesses are to ensure all systems are patched and updated.

Deception technology

Be aware of deception technology, where it tricks attackers into believing that they have accessed the company's assets when in reality they haven't. This buys time for threat discovery and mitigation.

Source: How to Prevent Ransomware Attacks: Top Nine Things to Keep in Mind, Fortinet