Carbon Black.

Stopping the Next Ransomware Outbreak

The spike in ransomware outbreaks in the last two years has left security analysts and administrators searching for better protection. But many of the best practices for preventing these notorious attacks come down to standard IT hygene. Here are five simple tips for stopping the next ransomware outbreak and keeping your organization out of the security headlines.

Maintain up-to-date, secure backups

Backups are essential: if you're infected, a clean backup may be the only way to recover your data. Make sure that backups are not connected to the system they are backing up, and verify the integrity of backups and your team's restoration processes by testing on a regular basis.

Configure firewalls and segment your network

This will help prevent the spread of ransomware across your enterprise. Make sure to go through the due diligence of blocking access to known malicious IP addresses and logically segment your network. If every user and server is on the same network, new variants can spread like wildfire.

Develop a regular patching process

This tip alone would have kept your organization safe from the WannaCry and NotPetya outbreaks earlier this year. Patching operating systems, software, and firmware on all devices minimizes the chances of a successful exploit. Consider using centralized patch-management for regular patching, but also ratify an emergency patch process for special incidents.

Create hierarchy for data access

Determine what groups of users need access to different types of data and implement controls to limit unnecessary access. Follow the principle of "least privilege" and only provide administrative access when it is absolutely necessary.

Invest in next-generation platforms

When looking at the technology you have in place for stopping ransomware, it comes down to the fundamental question of whether your current tools provide the visibility necessary to make a prevention or detection decision. Most organizations can't answer that question, which means that it's time to start the conversation and build a criteria for evaluating modern platforms.

Your baseline criteria should include single-agent solutions that use automation and cloud-based intelligence to back up your best practices, can block malware and non-malware attacks, and provide visibility into all activity occurring on your endpoints.

Ready to start evaluating NGAV solutions?

Get started with Cb Defense today!