Blog for MPA Networks

http://mpa.com/blog/defend-network-advanced-persistent-threats/

Defend Your Network Against Advanced Persistent Threats

Posted July 12, 2016

If you've looked over our previous posts since we've started our blog, you know how serious we are about protecting your company from everyday cyber-threats—mainly phishing, ransomware, and various other malware. Today we'd like to discuss a different form of cyber-threat plaguing businesses over the past decade: what the security community has termed **advanced persistent threats**, or **APT**.

What exactly is "persistent" about APT? Most hacking attacks can be classified as "smash-and-grab robbery": Break into a network and make off with anything of value—user identities, account numbers, cash—and disappear before anyone notices.

An APT attack compromises a network's defenses and **stays as long as possible**—weeks, months, or years—discreetly infiltrating servers, eavesdropping on email, or quietly installing remote bots or trojans which enable deeper espionage.

Their primary goal is *information*—classified material, trade secrets, or intellectual property—that might draw interest on the black market.

Robbery, Inc.: A Worldwide Enterprise

While unsophisticated hackers might lurk in the shadows like criminal gangs, **APTs often emanate from professional environments not unlike a prosperous Bay Area**

tech company—posh high-rise offices, full-time employees with salaries and benefits, and formal product development teams. The difference is they're conducting business in China, Russia, and other cyber sanctuary nations where international cybersecurity is unenforced and intellectual property laws don't exist.

The more extensive an APT infection, the harder it is to isolate and eradicate it—like cockroaches under a kitchen sink. Many enterprise IT managers simply accept APT as a fact of life—conceding that trying to combat these intrusions would actually encourage the culprits to dig deeper into the network.

So if APT makes long-term data theft inevitable, how can you still protect yourself? **Make the stolen data unusable.**

Alphabet Soup? Fight APT with DLP

The second acronym we'll talk about today is **DLP: data leak protection**. DLP encrypts sensitive data so that it can only be accessed by authorized users or workstations with a corresponding decryption key. If that data is intercepted by an APT, it's rendered unreadable—and worthless.

Multiple name-brand security vendors offer a wide range of turnkey DLP solutions. Low-end products will automatically encrypt data which follows specific patterns (Social Security numbers, 16-digit credit cards), while high-end products can be configured to use complex algorithms and language analytics to locate and protect other specific forms of confidential data (such as client files, product designs, or sales figures). When unauthorized access is suspected, files can be temporarily quarantined against a possible data breach before they leave the company network.

Are APTs already lurking within your network? What proprietary data can your business not afford to lose? **How can you evaluate DLP products to find the best solution for you?** Talk to us for help.