Are there undetected threats in your IT system?

According to a 2015 study, a threat can exist inside of your computer systems for more than 200 days before being discovered. Two hundred days is more than half a year… and that study is two years old! This information should alarm every business owner, but especially an attorney. Your client's information is extremely valuable and you have a responsibility to keep it as secure as possible. With unknown threats in your computer system, confidential information may be walking out of the door without you even knowing.

The Advanced Persistent Threat

An Advanced Persistent Threat (APT) is an attack that occurs when an authorized entity accesses a computer system undetected for a significant period of time. While many computer system attacks are done with the intention of damaging the network, an APT is instituted for the sole purpose of stealing information from its victim. These attacks are generally quite sophisticated and they are often carried out by pretty advanced criminal networks.

Further complicating this threat, an APT can take on various forms. Ranging from a mimic administrator account to a more complex trojan horse attack that invades your system through an email attachment. APTs are persistent and diligent in their quest for secure information from your network. The attacker continuously changes its techniques and rewrites codes for the purpose of avoiding detection. Some of these menacing attackers even employ full-time administrators just to keep their APTS up and running.

Addressing the Threat

While APTs are more commonly experienced by government agencies and large organizations, small and medium sized firms should be aware of these threats as they work to develop security systems for their practices. These attackers want "high-value" data and, depending on your area of practice, your practice may have exactly what they are looking to obtain. Strong passwords and common anti-viral software applications may not be enough to keep your data safe from APT attacks, instead you need a layered approach developed by an IT professional who fully understands the threats to your firm.

An article on Security Info Watch discusses ways to detect APT attacks on your network, which should include increased monitoring and detection capabilities. Flagging is one useful method. For example, if your law office generally operates from 8:00 am through 7:00 pm Monday through Friday, the transmittal of data at 3:00 am would be flagged as suspicious for a potential threat.

It's a scary thought, but your law firm and client data is constantly at risk from a variety of attacks, including APTs. Take time to address the dangers or you could be facing some serious consequences.

About Erika Winston:

Erika Winston is a freelance writer with a passion for law. Through her business, The Legal Writing Studio, she helps legal professionals deliver effective written messages. Erika is a regular contributor to TimeSolv and a variety of other publications.