Stopping Russian and Chinese Hackers

How a Small U.S. County Was Attacked; **No One is Safe**

The United States ranks highest in cyber-crime costs. According to Heritage.org, on average, the minimum cost among 85 companies surveyed in 2015 was USD 1.9 million and maxed out at USD 65 million. Companies fell victim to Trojans, viruses, worms, malware, phishing schemes, and hacker attempts. Even the most secure datacenters were prey to miscreant behavior. In the past year, Chick-Fil-A, Sony Pictures, Go Daddy, Las Vegas Sands Corp, Staples Inc., Morgan Stanley, Anthem Inc., Uber, Forbes.com, Register.com, Penn State University, Beacon Health Care, United Airlines, American Airlines, Trump Hotel Collection, WhatsApp, Experian, and Scottrade all made headlines because of cyber-crime activity. (And these are just a few of the big names who were willing to admit they had been hacked.)

And cyber-crime shows no signs of slowing down. In fact, leading economists agree that cyber-crime is the fastest growing economic crime in the world. For instance, among those businesses surveyed, each experienced 50 intrusion events per week in 2010. In 2015, that figure rose sharply to 160 per week according to the Ponemon Institute’s 2015 analysis of hacker activity, both private and public sector.

Cyber-crime does not stalk just large corporations, however. While large companies with large bankrolls provide large paydays, they are often much more difficult to breach. Many cyber-terrorists target small business, and even home users, to mine data and extort victims. Ransomware attacks, which hold companies hostage for blackmail, have been the biggest headache for cyber-security specialists recently. Time.com reports that in 2014, the CryptoWall virus infected 650,000 computers world-wide and earned hackers USD 250,000 in six months alone. According to the FBI, victims lost more than USD 18 million in 2015 alone from a different version of CryptoWall. It is expected in 2016 that hackers will earn on average USD 70,000 per month from these types of crimes. There are even “exploit kits” that less-than-savvy criminals can buy on the black market from hacker groups, mostly found in China, Russia, Ukraine, and Eastern Europe.

In this era of cyber-crime, NO ONE IS SAFE. We are at war.

The best strategy to protect your assets and intellectual property is to deploy several arsenals in the war. Firewalls, multiple virus scanners, intrusion detection devices, data encryption, password complexity and a host of other defensive mechanisms are not nice-to-haves, but an absolute requirement in today's enterprises.

Recently, a small U.S. county's I.T. department suspected that hacking was occurring in their environment. While virus scanning mechanisms were preventing most malware, county officials were still concerned that sensitive data was being collected by cyber-thieves.

The county tech team engaged Argent Software to determine if there were any previously undetected cyber-attacks occurring. In less than one hour, Argent was deployed and configured to report on any suspicious activity. The result? Argent detected 600+ pages of offshore attempts to hack the county's sensitive data in the past 24-hour period alone. Police records, medical records, utility payment records, marriage licenses, real estate information, and countless other sensitive information were at risk. Argent for Compliance collected, scanned, and consolidated all critical data from across the network and, within minutes, reported the hack attempts. Argent for Compliance identified the IP addresses of the cyber predators and county officials were quickly able to trace the origin of the hacks back to Malaysia and China.

I.T. personnel determined that the criminals were invading a public kiosk computer in the Sheriff's office. This computer was supposed to be used by citizens to access their records only. However, the office staff would, against policy, regularly login to watch YouTube videos (as their desktops did not have speakers). They would inadvertently and innocently leave the computer logged in and their elevated security permissions opened up a backdoor for hackers. It was further determined that the organization's firewall systems were antiquated owing to government spending cutbacks.

The I.T. staff was able to show Argent's built-in CJIS Compliance Reports to the Sheriff's Department. After proving their case to county leaders, the I.T. staff was granted emergency funds to purchase and configure new firewall devices within the week. The county received a substantial return on its investment with Argent Software in less than one week.

Proactive and responsible I.T. personnel do not sit idly by and wait for cyber-crimes to catch them unaware. Conversely, many companies and organizations – especially smaller ones – assume incorrectly that hackers won’t bother assaulting them. Argent for Compliance is a robust and scalable solution that provides a complete audit trail of malicious behavior. It can be installed and configured quickly and easily and will help provide your organization with protection against cyber-crime.

Argent’s award winning solutions work tirelessly defending companies and agencies to keep them safe from cyber terror. If security is a concern for your organization, can you risk having Argent for Compliance missing from your I.T. armory?

Argent Software created this document for informational purposes only. Argent Software makes no warranties, express or implied, in this document. The information in this document is subject to change without notice. Argent Software shall not be liable for any technical or editorial errors, or omissions contained in this document, nor for incidental, indirect or consequential damages resulting from the furnishing, performance, or use of the material contained in this document, or the document itself. All views expressed are the opinions of Argent Software. All trademarks and registered trademarks are the property of their respective owners.