5 biggest cybersecurity concerns facing CIOs, CISOs in 2016

By Clint Boulton

Dated: 19 January 2016
Published by: Thoughts On cloud

Last year began and ended with a series of high-profile cybersecurity attacks, starting with the pilfering of 80 million Social Security records at health insurer Anthem and culminating with infiltrations at Starwood, Hilton and Hyatt hotel chains. Expect digital assaults, — ranging from standard malware to more sophisticated, clandestine entries — to continue on leading corporate brands in 2016, according to Raytheon's Websense business. The cybersecurity software maker, which analyzed threat data from 22,000 customers in 155 countries, says hackers will conjure attacks that target emerging technologies, such as mobile payments and top-level domains.

Companies and consumers can also expect targeted attacks on aging Internet infrastructure, as well as on the Facebook, Twitter and Instagram accounts of presidential election candidates, says Carl Leonard, a Websense principal security analyst and author of the company's 2016 predictions report. CIOs, scrambling to defend their corporate assets, will continue to invest in cyber insurance, though they will find it tough going as insurers conduct more scrupulous vetting of potential clients' cybersecurity postures. Below are the five biggest concerns CIO and CISOs need to focus in the new year, according to Websense.

1. Hacks of mobile payments and other non-traditional payment systems. As smartphones continues to become the preferred source of authentication for many financial transactions, malware authors will increase their efforts to steal funds from consumers' Apple Pay, Google Wallet and other mobile payment systems.

CIOs listen up: once attackers have learned to infiltrate consumer's mobile wallet they may tap into your corporate networks for those smartphone owner's work. "Emails, contacts, authentication measures and apps that access the corporate network from the phone can become a phenomenal source of intellectual property, insider information and other confidential business materials become easily obtainable and can net an attacker sizable treasure," Leonard says.

2. From Heartbleed to heartache. Open source vulnerabilities, including Heartbleed, Shellshock and Poodle, struck fear into the hearts of Akamai and other companies in 2015. Expect more attacks on the creaky Internet infrastructure. Leonard notes that a significant number of the Alexa 1000 top websites are not up-to-date on certificates. "We observed certificate issues related to older hashing schemes such as SHA-1, as well as problems related to the version of ciphers supported. If some of the "big names" on the Internet are struggling to keep up, how can smaller vendors cope?"

Additional problems include old and broken Javascript versions; end-of-life challenges for core software such as Windows XP; and new applications built on recycled code with old vulnerabilities. "It's very difficult for systems to be migrated because you risk losing functionality or introducing new bugs," he says.

3. New top level domains pose phishing pitfalls. Emerging general TLDs, which number more than 800 and may expand another 1,300 in the next few years, will be used in active spam and other malicious campaigns. Leonard says criminals and nation-state attackers will lure, via social media, email and other tools, unsuspecting users toward malware and data theft. For example, criminals could steer unsuspecting consumers towards shop.apple, apple.macintosh or apple.computer to try to steal their information. In a Raytheon Websense sample set of several TLDs, millions of different URLs hosted malicious content. "These TLDs will also make it significantly harder for defenders to protect, as many are unprepared for the new landscape," Leonard says.

4. Presidential elections are prime "hacktivism" time. As the U.S. moves closer to the U.S. Presidential election in November, so-called "hacktivists" will increasingly delight in hijacking the Facebook, Twitter and Instagram accounts of candidates and news outlets and attempt to spread misinformation. Such lures will look like political party or candidate email, advocating an online petition or survey about specific election issues, linking to a supposed news story, or relaying information about voter registration or debates. "They're generally politically motivated hackers that delight in bragging about their achievements afterward," Leonard says. To hedge against such risks, Leonard says he imagines some campaign teams hiring CIOs to protect their media assets.

5. Cyber insurance better aligns with cybersecurity postures. Cyber insurance premiums soared in 2015, as companies race to purchase indemnification coverage. To maintain profitability, insurance carriers will require more threat and protection intelligence and develop baseline requirements for issuing cybersecurity policies. Such policies will take into account a company's

market capitalization, defense and risk profile, attack frequency, as well as the capability to halt attackers and remediate breaches.

Insurers will send auditors to conduct hands-on assessments of cybersecurity systems, reinforcing the need for advanced threat detection, both of the perimeter and at the data level. "That can dictate premiums, or even whether you get a payout to your claims," he says. "We expect to see an increasing sophistication in the way the risks associated with a cyber breach are factored into policy cost, just as a driver's safety record and driving habits are factored into the cost of an automotive policy."

Cause for some optimism

Given the threats outlined, cybersecurity defense appears to be, yet again, an exercise in Sisyphean boulder pushing. But Leonard strikes an optimistic tone, noting that CIOs can shore up their assets by building a team of trusted advisors, including internal and external partners. These teams will share the labor for monitoring technology developments and introducing new technologies, as well as the practices of cyber criminals, and evolving legislation.

Moreover, companies must assign data owners and data custodians to distribute responsibility for safety, and vet suppliers, including third-party companies with which they work. Educating employees', often a company's weakest security link, is paramount. CIOs should also commit to cybersecurity drills that incorporate communication, threat assessment and risk mitigation.

This article was written by Clint Boulton from CIO and was legally licensed through the NewsCred publisher network

http://www.thoughtsoncloud.com/2016/01/5-biggest-cybersecurity-concerns-facing-cios-cisos-in-2016/

submitted by: Ruth Edge – Cardinia Shire Council