TOLMAN & WIKER
INSURANCE SERVICES, LLC
INNOVATIVE RISK ADVICE SINCE 1923™
BAKERSFIELD | SALINAS | SANTA MARIA | VENTURA

Cyber Crime: “We are Legion”

September, 2013

Property Casualty 360

In a small, one-bedroom flat in the working class city of Kharkiv, in the former Soviet Union, Dmytro Kozel was surfing the Internet for universities and colleges in the U.S. As a young student in the Ukraine, Kozel had more than a passing interest in advanced education but he wasn’t interested in enrolling in online classes; tonight, he wanted to break into the network of a large U.S. state university.

The university was using a Linux Unix machine and Kozel entered the server by establishing a “null session.” Null is a Microsoft utility that allows services to communicate with one another without user passwords or identification. By logging on as null, he was able to capture everything he wanted to exploit: password files, user accounts and network services. None of his actions were logged or tracked by the server.

He began copying down user names and found the name "backup." He tried a guessed password, “123456” (studies have shown that even the most diligent IT professionals use a simple “backdoor” password at some point). Once he had obtained entry, he grabbed the encoded passwords and submitted them to an open-sourced password-cracking tool freely available on the Web.

It took 15 minutes to decipher 70 percent of the passwords, log on as a super user and gain root access. He closed out the session by hiding his tracks behind a readme.txt file to use later. He spent the rest of the evening searching for other vulnerable sites to access in the future.

Kozel waited two weeks to re-enter the university network. When he returned, he found no advanced firewalls or code changes. His previous visit had gone undetected. He searched the website for the financial aid and billing office and then gathered the usernames and passwords from the administrative server. He began downloading the names, addresses, financial information and Social Security numbers of more than 47,000 students. The state university’s IT department and CIO would not be aware of his actions until months later--when parents began calling the college to report strange activity on their credit cards.

Dmytro Kozel will spend 16 to 20 hours a day searching, sifting and analyzing sites to hack in the U.S. and Europe.

According to Advisen, a benchmark and data research firm for cyber liability insurance, the last six months of involving cases like this have caused chief information officers at public, private and government entities around the country to lose sleep and for uninsured businesses which experience data breaches, millions of dollars.

Some recent examples:

- 3.3 million unencrypted bank account numbers and 3.8 million tax returns were stolen in a phishing attack against the South Carolina Department of Revenue
- The California Department of Social Services lost the personally identifiable information (PII) of more than 700,000 residents, including names and Social Security numbers, when a package containing microfiche, sent by the U.S. Postal Service, arrived damaged with most of the data missing
- The health information and PII of more than 780,000 Utah citizens were put at risk when Eastern European hackers broke into a server maintained by the Utah Department of Technology Services this spring.

A Global Perspective

But it’s not just the U.S. governments, large corporations and public institutions that are susceptible to data breaches. According to govtech.com, European government data breaches have increased by more than 1500 percent, with the next largest increases coming from public businesses (1380 percent) and the private sector (1159 percent). Data breaches overall, in all segments of European commerce and industry, have increased 1015 percent in the last 5 years.

The prospects for 2014 are equally daunting, according to FishNet Security: “The majority of business owners, managers and CIOs (97 percent) stated that they believe the number of data breaches will increase.”

Where are they coming from?

Security giant Symantec states that 37 percent of international breaches are caused by “malicious attacks from hackers and hacking groups.” Statistics provided by Deutsche Telecom show that in one month, (June 2013), there were 30,144,538 global “cyber attacks.”

Although malicious attacks account for a large portion of cyber breaches, 35 percent of overall incidents arise from negligence or human error (lost laptops and system devices, inadvertent data dumps, unencrypted servers, employees susceptible to phishing and malware), and 29 percent are from IT system glitches/failures.

Hacker groups have been around since the early 1980s. The most notorious and active groups are scattered around the world in places like China, Germany, the Russian Federation, Taiwan and Hungary.

Most successful hacking groups coalesce not because of their geographic locations, but because of the unique abilities of each team member. **TeaMp0isoN** formed in 2010 in the United Kingdom. This group was responsible for hacking Facebook, NATO and the English Defense League. **Network Crack Program Hacker (NCPH)** was formed in China. This group is known for its frequent attacks on the U.S. Department of Defense. Some of the most publicized breaches, including Fox.com, the CIA and the FBI, have been caused by Dmytro Kozel’s group, **LulzSec**, whose motto is, “Laughing at your security since 2011.” **Anonymous**, which Time magazine in 2012 called one of “the 100 most influential people in the world,” is associated with international hacktivism and targets governments, corporations and associations that they accuse of censorship. Anonymous took credit for the largest data breach ever, Sony Play Station, in April 2011. Members commonly use the tagline, “We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.”

Like any good business team, hacker groups need specialists to build a strong cyber crime network. Dmytro Kozel works independently in the Ukraine, but his expertise in exploiting IT vulnerabilities makes him an important team member to one of the largest cyber crime groups in the world. In addition to hacking specialists, teams use graphic artists to create enticing emails, websites and other social engineering schemes designed to get unsuspecting employees to click on malicious links. Once data has been stolen, salespeople are needed to bring the product (personal information, health information, credit cards, etc.) to the marketplace. The current price for a credit card number is $10. For stolen health information, the price for each record shoots up to $50 on the black market.

How much money is being lost?

According to the May 2013 benchmark report by the Ponemon Institute, the average total cost of a data breach for a U.S. business was $5,403,644.00. The U.S. experienced the highest total average cost followed by Germany at $4.8 million and then Australia and France at $4.1 and $3.8 million respectively.

These numbers take into account the fact that certain industries have higher costs per breach than others. Businesses that are regulated and governed by local, state or national governments like healthcare, financial institutions, non-profits and education have higher breach costs than other industries like retail, transportation and hospitality. According to Ponemon, the average cost for each record breached for the healthcare industry is $233.00.

Overall, cyber attacks “may be draining as much as $140 billion and half a million jobs from the U.S. economy each year,” according to James Lewis, director of technology and public policy programs for the Center for Strategic and International Studies.

Selling the coverage

No business or entity, public or private, feels that it needs to spend more money on insurance, and most small businesses believe that firewalls and passwords will protect them. Agents need to discuss cyber liability insurance needs with their customers throughout the year, not just in a last-minute rush to provide a quote at the renewal date. Provide information on data breaches that will resonate with your clients, such as proximity to their geographic location or breaches in their class of business. You can find this information on sites like www.privacyrights.org. This approach generates more interest than national headlines involving international multi-billion-dollar companies. Explain to your customers that general liability coverage specifically excludes electronic data and that the fines, penalties, attorney fees, notification costs and public relations costs to restore a business’s good name can cost a non-insured business millions of dollars in out-of-pocket expenses

Eventually, cyber security, cyber privacy and identity theft will be seen as a crisis that needs to be addressed with an additional level of focus. Using plastic credit cards, telephones and unencrypted emails is simply too 20th century. Make sure you can explain the need and the coverage and offer a cyber liability quote for every client at renewal.

www.nationalunderwriter.com

Return to Article Index

Forward this article to a colleague

Address To Recipient Name

Subject

Message

Send Reset