itbusiness.ca

RECENT NEWS

Hacker unveils the basics at SecTor

Ethical hacker tells audience that lethal threats can be avoided easily with some common sense

11/21/2007 11:33:00 AM

by Paolo Del Nibletto

Toronto – SecTor's main keynote speaker told a packed audience yesterday that the hacking community is killing businesses and other organizations on a daily basis, while they protect themselves from a big massive attack that may never come.

Ira Winkler, has been dubbed the modern day James Bond, but he believes that Bond, if he existed, would be the second worst spy of all time.

The reason is that he gets caught and breaks the spy code, which is never to get caught, said the former undercover security analyst for the U.S. National Security Agency (NSA).

During his time as a super secret security analyst he stole billions of dollars from major corporations and banks. He even broke into a nuclear reactor and stole its designs in less than four hours.

Winkler was at the SecTor conference to offer his pearls of wisdom and surprisingly he said that hacking and protection from hackers is pretty basic.

He said that a lot of hackers believe they are artists and Winkler dispelled that notion by saying that hacking is very technical.

“I look at it as a science, while others believe it is an art. I used little tricks while others believe there is a feel to breaking into computers. I looked for repeatable tasks instead,” Winkler said.

He added that there is a natural ability and computer aptitude that can make a hacker really good. Special abilities such as visualization where a person can manipulate objects in their mind can be useful. However, they are not a substitute for repeatable tasks.

“A stereotypical hacker breaks into systems without a repeatable process. When I worked at the NSA I first determined the vulnerabilities,” he said.

According to Winkler, the NSA trained him for three years and it is similar to what the Central Intelligence Agency (CIA) does or special-forces such as the Navy Seals do and even the Russian-

based GRU (the GRU in English means Main Intelligence Directorate and is Russia's largest intelligence agency since the KGB was split up back in 1991 after a failed coup attempt against Mikhail Gorbachev).

The training is based on aptitude tests where the can find hidden abilities. The training helps interns, as Winkler calls them, to rapidly recognize vulnerabilities and exploit them.

“I broke into banks and a nuclear reactor without getting caught because I had a (repeatable) process. It is not about being lucky,” he said.

Another area of concern for security solution providers and CIOs is the perception that security is complicated, expensive and that there is a lack of qualified people that can implement it.

“This is a wrong perception,” Winkler said.

He cites the example of TJ Maxx, a U.S department store that was hit recently. Winkler said that TJ Maxx believed they were secure. Visa sent them a note telling them to improve or they would be fined and TJ Maxx ignored it because they did not believe it had a problem.

“Customers believe that if they do not have a problem then they are ok,” Winkler said.

Winkler added that most of the information that can take down a company or organization is already public. Robert Morris's worm was built with public information and it took down a third of the Internet back in 1991. The AT&T server crash was due to a three line programming error. Well know attacks can break into the Pentagon, U.S. Naval ships and 911 systems, he believes.

“There are no secrets,” Winkler said.

Winkler unveiled at SecTor his basics for computer hacking and essentially there are only two ways:

The first is by taking advantage of a problem built into the software.

The second is by taking advantage of the way a computer administrator has set up the system.

“All software has bugs and some will create leakages which lead to security vulnerabilities,” he said.

A glitch in Windows 95 revealed the password in the registry file in clear text. Microsoft, at the time, said that it was a password recovery feature and not a vulnerability, Winkler said.

As for exploiting the way someone created a computer system, that can be avoid with simply common sense.

Winkler gave an example using one of his trainees at the NSA. “I trained this woman who had the last name of Kirk. After she log on to the database I typed in the password CAPTAIN and she said: ‘how did you know my password?’”

According to Winkler, 75 per cent of the largest companies in the world have administrators who use the password ADMINISTRATOR.

Winkler said that these stories are funny because they defy common sense.

He believes that 99.8 per cent of all computer hacks can be prevented. The problem as he sees it is that businesses and organizations do not provide the common knowledge to staff so that they can have this common sense. “It is the company's fault. The NSA failed the Kirk woman and allowed her

to have an easily guessable password."

Security is inefficient inside organizations because they can't explain what they are doing to manage risk.

Winkler said that risk can be broken up into three components: value, threat and vulnerability.

The value is determined by the worth of the information that the computer can provide. Threats can be a hurricane, a flood, human stupidity, hackers and foreign agencies.

As for vulnerabilities, Winkler said that businesses and organizations provide them from something complex inside a computer operation or something as simpl as an unlocked door.

"You have to implement the countermeasures. You can't stop a flood or someone doing something stupid or foreign counter intelligence, but you can stop vulnerabilities such as CAPTAIN Kirk."

Winkler's advice is to look at the base vulnerabilities and eliminate them. He added that hackers who are really good never get caught so concentrate on what you can prevent.

For the record, Winkler believes the worst spy of all time is Sydney Bristow of the TV show Alias.

Close Window