Hackers test, teach computer pros at Cyber Range

7 January 2015, by Rick Barrett, Milwaukee Journal Sentinel

You won't find this town on a map, but it's a very scary place. In Alphaville, a virtual town used for cyber security training, the banks are robbed on a regular basis, the power plant and water system are under constant siege, and wireless networks at coffee shops are crawling with spyware meant to steal your personal information.

The computer system at the town's city hall has been hijacked and the elementary school's system is infected with malware that could have disastrous consequences.

Alphaville is part of the Michigan Cyber Range, which teaches computer network professionals to detect, prevent and mitigate cyber attacks in real-world settings.

Like a test track or a firing range, the cyber range has "live fire" exercises that challenge the skills of participants in a variety of situations.

They operate against "a live, thinking and adapting adversary," said William J. Adams, a retired Army colonel and now vice president of research and cyber security for Merit Network Inc., a nonprofit that runs the Michigan Cyber Range.

Inspired by mock towns used to train soldiers, Alphaville simulates cyber warfare against government, schools and businesses. Such attacks, in the real world, have become increasingly sophisticated and dangerous, which makes training like this more valuable.

Wisconsin state officials have taken classes through the Michigan Cyber Range. This spring, they will engage in exercises where one team launches an attack on a system while another team defends it.

"It's like a war game. You have to think like the enemy to predict where the enemy is going," said Jack Heinemann, director of the Wisconsin Security Research Consortium, a nonprofit organization that seeks science and technology solutions for national Homeland Security requirements.

Michigan has cyber-range "hubs" at universities and Army National Guard bases. By plugging a laptop into a portal at one of the hubs, information technology professionals can enter Alphaville to test their skills against hackers, who are in reality Merit Network staff or volunteers from colleges.

The cyber range also can be accessed from Wisconsin through a private cloud - large groups of remote, networked computers - managed by Merit Network.

In one of the exercises, the hackers attempted to break into Alphaville Power & Electric so they could turn off power to various buildings. In another exercise, students at the U.S. Military Academy at West Point attacked the city while the Army National Guard defended it.

Nothing is safe in this town, which can be configured to suit the needs of the training for government, schools or businesses.

"Alphaville is a place that applies to just about everybody. It's not going to be an exact copy of your enterprise, but it's going to be pretty close," Adams said.

"We have all of the neat toys, and we are always looking to build others," he added.

Increasingly, hackers are going after businesses. It's a new kind of economic warfare, said Tom Still, president of the Wisconsin Technology Council, an advisory group to state government.

Wisconsin has some high-value targets, too, including large companies in the manufacturing, insurance, health care and financial sectors.

"We are probably right there with everybody else, at least, in terms of our vulnerabilities," Still said.

The Merit Network wants to establish three cyber "volunteer fire departments" in Wisconsin that would respond to major attacks and assist police in investigating the attacks.

Volunteers would be solicited from industry, academia, state and local governments.

"We are going to pick from the best people available," Adams said.

Often it's an individual, not software, that gives hackers an entry point into a system.

Adams recalled one incident where a college professor used a special Internet search tool, not realizing it exposed the college's entire web server to a specific type of attack.

People are too trusting, and the more user-friendly technology has become, the more vulnerable it is, said Jon Brown, senior technology leader with Vantage Point Solutions, a Mitchell, S.D., consulting firm that does work for Wisconsin telecom businesses.

"It's easier for somebody who knows what they're doing to take advantage of that," Brown said.

Wireless access points can be established to capture the traffic from users who don't realize they're being monitored. Similarly, hackers can listen in on Bluetooth phone conversations.

Social media also has left individuals and businesses vulnerable.

"Most people don't understand Facebook's ever-evolving security settings. There are all kinds of stalking potential because people put way too much information on social media sites," Brown said.

No one is immune from attack, said Bill Esbeck, executive director of the Wisconsin State Telecommunications Association, which represents broadband providers.

"It's only a question of how well prepared you are. You can't stop the hackers from trying to breach the networks," Esbeck said.

"I recently asked an expert how I could best protect myself from hackers and identity theft," Esbeck said. "He handed me a pen and pad of paper. Unfortunately, he was only half joking."