Security
May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

This post was updated at 2:16 p.m. PDT with comment from an outside database security software vendor.

Hackers broke into the University of California at Berkeley's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced Friday.

At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waggener, UCB's chief technology officer, said in a press conference Friday afternoon.

(Credit: University of California at Berkeley)

The attackers accessed a public Web site and then bypassed additional secured databases stored on the same server. In addition to SSNs, the databases contained health insurance information and non-treatment medical information, such as immunization records and names of doctors patients had seen. No medical records (i.e. patient diagnoses, treatments, and therapies) were taken, as they are stored in a separate system, emphasized Steve Lustig, associate vice chancellor for health and human services.

"Their ID has not been stolen," he added. "Some data has been stolen."

The server breach began on October 9, 2008, and continued through April 9, when a campus computer administrator doing routine maintenance discovered messages left by the attackers. Logs indicate that the hacks originated from overseas, "primarily in the Asian theater," Waggener said, later specifying traces to China.

While campus police and the FBI were immediately notified of the breach, it wasn't until April 21, Waggener said, that officials learned data had been stolen. Since then, the focus of the investigation has been figuring out what was taken and who is at risk. The hackers' specific techniques are still being determined as part of the ongoing criminal investigation, he said.

From the looks of it, however, one outside database security software vendor, Sentrigo CTO Slavik Markovich, suspects an **SQL injection**, in which a small malicious script is inserted into a database that feeds information to the Web site. Markovich also questions whether the university has appropriate monitoring tools in place to have not noticed the hack for six months, and why it hosted data with different levels of sensitivity on the same server.

The university started notifying the 160,000 people at risk via e-mail and snail mail on Friday. Victims include an assortment of current and former Berkeley students--as well as their parents or spouses, if linked to insurance coverage--who had University Health Services health care coverage or received services. Also included are 3,400 students of Mills College in Oakland, Calif., which contracts with the university for health services.

The university has warned those affected to put a fraud alert on their credit reporting accounts. It has also **set up a Web site** and hotline to help the victims.

In 2005, **a PC was stolen** from a Berkeley graduate admission office that held sensitive data on some 98,000 people, stretching back three decades. And the university has dealt with security viruses and the like, Waggener said. But this was the first such server breach.

With this, Waggener said, Berkeley joins a **long list** of **prestigious institutions suffering** from such increasingly sophisticated and malicious attacks. "We're defending against attacks from around the world," he said.

Michelle Meyers is an associate editor who tracks online happenings in media, entertainment, and politics. E-mail Michelle.

Topics: **Vulnerabilities & attacks**

Tags: **hackers**, **data breach**, **ID theft**, **University of California**

Share: Digg Del.icio.us Reddit Yahoo! Buzz Facebook

Related

From CNET

Google fixes severe Chrome security hole

The Cold War moves to cyberspace

F-Secure says stop using Adobe Acrobat Reader

From around the web

Spammers Clog Up the Blogs Wired

Hotels: Hyatt is the latest chain on sal... Budget Travel

More related posts powered by Sphere