Categorized | **News**

UMass announces major breach in data security

By: Matt Rocheleau
Published: September 07, 2009

A University of Massachusetts computer server containing thousands of alumni names, Social Security numbers and "very limited amounts" of credit card information was hacked into last September, University officials announced on August 5; however, there is no evidence, and the University believes it is unlikely that, the personal information was stolen.

The server – which is used by the Career Services department and contains data from students attending UMass between 1982 and 2002, and a few others who attended before 1982 – was illegally accessed through a malware program installed by an unknown individual, or individuals, over a 42-day period from September 15 through October 27, 2008. According a University statement, the system was most vulnerable during the intrusion's first two days.

A sole police report of the incident was filed May 7 with the UMass Police Department by two University employees who suspected Chinese nationals were responsible for the intrusion.

MORE ON THIS STORY

- Read the police report from May, 2009.
- **Read the report submitted to Consumer Affairs.**

The police report states that Jeffrey Silver, director of Career Services, and Duane Stinchfield, the department's assistant director and systems administrator, "were sent to the police department by their supervisor to report the matter … They added that the report of the computer hacking was old, and that they suspected Chinese nationals of conducting the attack."

Both Silver and Stinchfield directed questions to the University's media relations office.

"That was a really early theory and, to some degree, speculation," said campus spokesman Ed Blaguszewski. "No one really knows [who was responsible for the intrusion]. We may never know."

The officer who filed the report was not able to be reached for comment in time for publication, and UMPD Deputy Chief Patrick Archbald said he did not know enough about the incident to expand on UMass' suspicion that Chinese nationals may have been responsible.

The University did not announce the intrusion had occurred until last month when state law required the school to do so; however, the Office of Information Technology (OIT) had learned of it last fall and reviewed the case until May, before turning over a more detailed analysis to Stroz Friedberg, LLC, an independent computer forensics company.

Campus spokesman Patrick Callahan said the illegal intrusion was not made public at any point in the 10 months prior to August 5 because of security concerns. Also, officials had not confirmed whether or not the server contained any sensitive data required to send a legal notification until the forensics company's analysis, which cost UMass around $49,000, was complete in mid-July.

"It takes a while to understand the breadth of the something like this," Blaguszewski said. "I think the people involved in reviewing the case realized the seriousness of the matter in a progressive fashion."

OIT had found the intrusion to be "potentially broad in scope" when its evaluation was complete, which caused the University to hire the computer forensics company.

Between mid-July and the recent announcement, the University was in contact with the state Attorney General Martha Coakley's office to determine how to appropriately broadcast the incident.

"All of this is done in compliance with the law, [Massachusetts General Law, Chapter 93H]," Callahan said. "There has been back and forth [with the attorney general's office] on the appropriate and legal way to inform the public."

Callahan said the breach affected both undergraduate and graduate student data, but both spokesmen declined to disclose the number of students whose data might have been compromised. Between 1982 and 2002 Callahan said it was a "large number" of students whose name and social security numbers were on the server, and prior to 1982, a "small number."

were on the server, and prior to 1982, a "small number."

However, a copy of a more-detailed legal notice sent from UMass to the state director of Consumer Affairs and Business Regulations said "thousands" of students are believed to have been at risk, but UMass was unable to determine "with any certainty" the exact number affected.

Though University officials declined to disclose which department used the breached server and how many computers were connected to the server, the more-detailed notice forwarded by state consumer affairs spokesman Alex Faust specified the server belonged to the Career Services office. Career Services is located in 511 Goodell Hall; however, that location was not specified in the notice.

Blaguszewski declined to confirm or comment on the notification sent from UMass to the state consumer affairs office. He said under state law the University is restricted in disclosing or commenting on certain information about such a security breach.

Archbald said UMass police are, "not doing anything further to investigate," the incident because such an investigation would require computer forensics staff and resources that are not available to UMPD.

Based on their analysis, the computer forensics company, "concluded that the intruders' attack was not specifically designed to look for personally identifiable information," said OIT's chief information officer John F. Dubach, in a University statement announcing the intrusion.

"Records do not show large amounts of data being extracted from the server, but that the potential for a loss of data did exist for a short period of time," continued the statement.

When contacted for further details on the incident, Dubach referred questions to the University's media relations office.

Stroz Friedberg's spokesman John Genova said he could not comment on the matter because the company's policy states that client information is confidential.

Amie Breton, a spokeswoman from Martha Coakley's office, said the attorney general had received notification of the University's compliance with state law, but said the office had no further comment and declined to answer additional questions. Breton declined to give a reason why the office would to speak further on the matter.

According to Massachusetts law, the State Treasurer's office is also notified of such an electronic intrusion since credit card data was involved. Media relations contacts there were reached but declined to commented on the incident at UMass.

According to the statements on the intrusion, the computer forensics company's recommended improvements include better security training for system administrators, automated software to detect malicious activity, increasing efforts to identify all computers that contain personal information, reconfiguring the University's firewall and retaining network data for longer periods to better assess incidents.

A number of these steps have already been taken, said Callahan, though he did not know which ones or how many.

"Obviously all of them will be taken at some point," he said.

Blaguszewski added that the University is "drawing lessons" from the hacking.

The most recent police report was not the first time the University has informed UMPD of a computer intrusion, said Archbald; however, he did not know of any such reports filed with UMass police since the one submitted in May.

In April 2008, University Health Services' (UHS) computers were also hacked causing the campus to shut down the 120 of the department's 150 computers. About 40 workstations across campus were affected in the viral attack, which OIT said may have been caused by a hacker or hackers wanting to use the computers to illegally download movies or music.

"This sort of thing is an ongoing battle between the hackers and the IT people," said Callahan.

However, there is no belief that the intrusions in April and September 2008 were related, he said, and the motivation of the attacks in last fall is unknown.

"Protecting the privacy of our students, alumni and all members of the campus community is one of our fundamental responsibilities," said Dubach. "We regret that this incident occurred, and we are taking steps to reduce the University's vulnerability to future attacks."

As required by law, a copy of a legal ad was placed in newspapers in Springfield, Worcester and Boston to announce the intrusion.

The University also set up a Web page, www.umass.edu/computerintrusion, for anyone with further questions about the matter, as well as setting up a special telephone help line, (413) 545-8376 which can be called from 8 a.m. to 5 p.m. Questions can also be e-mailed to computerintrusion@umass.edu.

Matt Rocheleau can be reached at mrochele@dailycollegian.com.

VIRTUAL EDITION

COLLEGIAN PARTNERS

Boston Criminal Defense Attorney

Boston Personal Injury Lawyer

Certificate of Deposit

Get Free Credit Report

Personalized Water Bottles

MEDIA AFFLILIATES

The Amherst Wire A Web-based news magazine and Collegian media partner.

UVC-TV 19 UMass' student-run TV station and Collegian media partnet

INFORMATION

WooThemes

Designed by Adii

Register

Log in

Powered by Wordpress

Entries RSS

Comments RSS

This article was written by:
Matt Rocheleau - who has written 1 posts on The Daily Collegian.

Contact the author

« **UMass football falls short of upset at K-State** **Video: An Interview with Matisyahu** »

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

© 2009 The Massachusetts Daily Collegian | About Us | Advertise with The Collegian | Comments Policy | Questions, Comments and Concerns