ADFA hack a national security failure, expert finds

December 12 2012, by Sunanda Creagh

Hackers have accessed personal details on thousands of Australia's future military leaders. Credit: AAP Image/Alan Porritt

A hacker has accessed personal details on thousands of Australia's future military leaders, a situation one expert has described as a national security failure.

According to media reports, a single hacker from the Anonymous group, calling himself Darwinare, released online the names, birthdays and passwords of 20,000 staff and students from a university database at the Australian Defence Force Academy.

The hacker is reported as saying it took three minutes and that his only motivation was boredom.

The University of New South Wales, which runs the campus, emailed all staff and students after the hack occurred on November 15 to say that identification numbers, birthdays, passwords had been stolen.

"We believe that the impact on you will be minimal," the email said.

"Email alias information may be used for targeted SPAM, phishing and other sort of email attacks on students. You should be especially vigilant in dealing with any suspicious emails."

"Student name and birthday information may be used for attempts at identity theft and again this requires additional vigilance."

A spokesperson for the Department of Defence said UNSW had taken "steps to mitigate the impact of the data breach and reduce the possibility of further data breaches."

"The university also worked with Defence to ensure former military students and staff were made aware of the breach," the spokesperson said in an email.

Mark Gregory, Senior Lecturer in Electrical and Computer Engineering at RMIT University, described the situation as mind-boggling.

"This, in my view, is a national security failure and should be treated as such," he said.

Dr Gregory is a retired army captain and it is his own alma mater that has been hacked.

"What's even more frightening is that they have now have access to private information on the people who are going to be our future military leaders in years to come," he said.

"Defence spends vast sums protecting every aspect of the organisation. Defence contractors also spend considerable sums achieving security clearance. Yet here we have a massive security failure by an organisation that receives considerable Defence funding. For Defence not to be checking that adequate security is in place at ADFA is, in my view, something that people should face the sack for," he said.

Dr Gregory said it was not yet clear how Darwinaire accessed the database but said the hacker may have used a brute force attack, where all possibilities are systematically checked until the right password information is found.

Another possibility is that the hacker broke through the university's firewall to access the administrative system directly or access a computer that can tap into the administrative system.

"The administrative systems should only be able to be accessed on the internal network from secure private subnets and never from the external internet. The administrative systems should be partitioned off so only certain people on certain internal networks have access," said Dr Gregory, adding that the administrative systems should have required two-step authentication—such as the sms passcodes or tokens used by online banks—to verify the security clearance of everyone trying to access the system.

"For most universities and other organisations, it's standard practice that these kinds of administrative systems can't be accessed from outside even through the use of VPNs or remote control of desktops. It slows things down but it's absolutely necessary to ensure security is maintained."

Jason But from the Centre for Advanced Internet Architectures at Swinburne University of Technology said a security system is only as strong as its weakest link.

"No reports have emerged as to how the hacker has accessed the ADFA systems, so we can only speculate as to where the weak link is. It is possible that more secure systems were accessed via less secure systems where the hacker has bypassed the stronger levels of security commonly applied to shield secure systems from generic Internet access," he said.

"While I can understand the political implications, it is disturbing how much this attack is being downplayed. To claim that only historical passwords were stolen is naive in assuming that most people regularly change their passwords in a routine manner. Coupled with the fact that passwords are regularly reused across multiple systems, this list could provide an avenue of attack into unrelated systems where users share common accounts."

The potential for identity theft was also being downplayed, Dr But said.

"The information which has been stolen can now be used to fish for further information, making ADFA users more vulnerable to future attacks. One would expect that organisations such as ADFA would have a higher priority on security of their computer and data systems."

The speed with which the hacker claimed to be able to access the data was also disturbing, he said.

This story is published courtesy of the The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation

Citation: ADFA hack a national security failure, expert finds (2012, December 12) retrieved 25 April 2024 from https://phys.org/news/2012-12-adfa-hack-national-failure-expert.html