New Jersey Law Journal

Universities 'Peculiar Creatures' in Cybersecurity World

David Gialanella, New Jersey Law Journal

May 21, 2015

Cyberattacks targeting Rutgers University and Penn State University have brought the issue of cybersecurity close to home—but also served to re-establish that higher-education institutions are unique targets.

“Universities are kind of peculiar creatures for cybersecurity,” said Vincent Polley, an attorney based near Detroit who co-authored “The ABA Cybersecurity Handbook” and who heads technology consultancy KnowConnect.

In the university structure—“a confederation of schools that are fairly loosely coordinated”—there’s “frequently not a lot of top-down management,” he said.

“Add to that an environment where people are encouraged to experiment,” and it’s a dynamic that’s “probably not replicated or experienced in any other environment, anywhere,” he said.

Scott Christie, a partner in the cybersecurity and data privacy practice at Newark’s McCarter & English, called universities “relatively soft targets” when compared to other entities, such as financial institutions.

“Given the fact that it’s in the university context, it relies upon the level of security that the school network administrators impose, which may or may not be the same as a nonuniversity network,” he said.

What’s frustrating about the Rutgers attack that began in March—as well as another attack at nearby Fairleigh Dickinson University (FDU) around the same time—is that neither appears to have relied specifically on network security weaknesses, attorneys and consultants said.

Both universities, according to reports, experienced what are called distributed denial-of-service attacks (DDoS attacks), which seek to deluge the target’s systems with requests—typically from outside machines, said Polley, former co-chair of the information technology and security law practice group at Detroit-based Dickinson Wright.

DDoS attacks entail an orchestrator gaining control of those machines, sometimes through email “worms,” and prompting them to send undetected information requests. The objective is that the target site or server, flooded with requests, is crippled and goes down.

Gideon Lenkey, president of Milford-based information security firm Ra Security Systems, said, “It’s hard to find because the machines that are attacking are not knowingly attacking.”

But Polley said “a DDoS attack is not taking advantage of system vulnerabilities.”

He called them “trivial attacks” and “nuisance attacks” that harness the “power to be disruptive,” and said how long a network is offline depends on the sophistication of both the target and the orchestrator.

Both Polley and Lenkey said a DDoS attack may be motivated by personal politics or simple anger.

“It makes me think of a nation-state versus some kid in his basement just trying to cause damage,” said Leeza Garber, corporate counsel and director of business development at technology consultancy Capsicum Group in Philadelphia, which got its start as the technology arm of law firm Pepper Hamilton.

“Sometimes it may seem easier to gloss over if there wasn’t personal information taken,” but “all of these varied types of cybercrimes are malicious—with different purposes,” she added.

“While a DDoS attack may not seek direct financial gain, causing a network to fail can cause a host of other issues for a university in particular,” Garber said.

FDU’s attack was resolved fairly quickly, while Rutgers experienced multiple Internet outages—apparently the result of multiple attacks—that ended up affecting final exam schedules, according to reports.

Rutgers spokesman E.J. Miranda said the university—which found no evidence that confidential information was compromised during the incidents—has not retained outside counsel to advise on cybersecurity, but did retain outside vendors.

“Rutgers, like all academic, government and corporate institutions, is increasing the resources dedicated to protecting and improving the security of university data and electronic environments,” Miranda said in a statement.

“We resolved the DDoS issues and have implemented new safeguards and retained new cybersecurity vendors in the wake of the incidents,” he added.

“Rutgers, as any institution with an Internet presence, continuously monitors our Web connections and servers to detect and respond to such issues as viruses, malware, denial of service and phishing. We have also retained a firm to assist in evaluating and developing security practices to govern the management of sensitive data through various types and layers of security.”

An FDU spokeswoman didn’t provide a comment by press time.

A spokesman from the U.S. Attorney’s Office would not comment on whether the office is investigating Rutgers or FDU, though the FBI previously acknowledged its involvement, according to reports.

The nature of the Penn State issue—which was reported more recently, in May—appears to have been different. The university said the College of Engineering’s network sustained two attacks last November, with at least one of those carried out by a hacker located in China.

In a May 15 statement that quoted numerous school officials, Kevin Morooney, Penn State vice provost for information technology, said, “Our information security protocols and practices help us to turn back millions of malicious computer attacks against the university every day.

“However, in this case we are dealing with the highest level of sophistication,” the statement said. “Unfortunately, we now live in an environment where no computer network can ever be completely, 100 percent secure.”

The university addressed the cyberattack privately, in order not to tip off the attackers, according to the statement.

The events at Rutgers, FDU and Penn State—as well as prior issues at other schools, such as the University of Maryland—bear out a common saying among cybersecurity experts: that it’s “not a matter of if, but when,” an attack will occur.

Cybersecurity lawyers interviewed last October warned of universities’ vulnerability. But maintaining defenses at a university or anywhere else is not so much a question of foresight as it is one of the practicality: Email-based attacks often rely on breaching a barrier that Lenkey previously referred to as “the human fire wall”—which is often the last but weakest line of defense, he said.

Christie at McCarter & English noted that universities provide a high number of network access points, for student convenience, and aren’t necessarily on the lookout for actions such as large data file transfers or multiple request for access by a single user name, which would set off alarms for a nonuniversity client.

Another cybersecurity lawyer, Fernando Pinguelo, agreed that universities’ structures make them special cases.

It creates “a unique situation because, when you’re dealing with a company, you’re not integrating the clients into the IT systems,” said Pinguelo, who chairs Scarinci Hollenbeck’s cybersecurity and data protection group out of the firm’s Ocean office.

Universities in many ways are fundamentally different from retailers and other corporations, but, he pointed out, they all have budgets to heed.

“It’s like any organization, for-profit or otherwise,” Pinguelo said. “It can sometimes be the last issue to address. ... When IT isn’t part of your money-making stream, I find that it often isn’t addressed as quickly or completely.

“The fact of the matter is, even if you spent every available resource trying to create this wall, there’s always going to be a way to breach it.”

Contact the reporter at dgialanella@alm.com.
