JULY 2, 2019

Legaltech news

ONLINE

An ALM Publication

Nervous System: The Day the NSA Took Down the Military

In this month's look at the history of cybersecurity, David Kalat looks back at the '90s, when the NSA reminded the U.S. government just how vulnerable to intrusion its systems could be.

BY DAVID KALAT, BRG

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have actually been with us longer than we remember. ***Nervous System*** *is a monthly blog that approaches issues of data privacy and cybersecurity from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.*

National Security Agency campus in Fort Meade, Md. Credit: AP/Patrick Semansky.

The world of cybersecurity has two enduring clichés. One is that the National Security Agency (NSA) is the ultimate Big Brother, a secretive and all-powerful eavesdropper that can invade any computer system at will. The other is that teenage hackers in their bedrooms are unstoppable forces of cyber intrusion. The general public has come to believe that no privacy protection can effectively keep either of them out.

The roots of these stereotypes are deep and complex, but in the late 1990s both clichés coincided to cement their hold on the public imagination. The one–two punch of "Eligible Receiver" in the summer of 1997 and the "Solar Sunrise" attack in early 1998 dealt humiliating blows to national security. Journalists like Fred Kaplan have written about how these two events influenced the defense establishment to improve cybersecurity policy. Alongside that positive response, however, was a less productive one.

Lt. General Kenneth Minihan became director of the NSA in early 1996. It was a period of calm after the Cold War and before the War on Terror. Minihan, though, knew an awful secret: The country's growing reliance on networked computer systems came at a terrible price—those systems were vulnerable to intrusion. Minihan felt frustrated that the mainstream defense establishment had dismissed his warnings as "Chicken Little" paranoia.

The problem was people. Users locked their computers with easily guessable passwords like "password" or "1234." System administrators allowed known vulnerabilities to go unpatched. Businesses expected the government to attend to security concerns, while the government left businesses to protect themselves. Given the choice between taking proactive steps toward securing

computer networks versus passing the buck and hoping for the best, people almost invariably opted for the cheapest, least demanding path.

Minihan decided the best way to get through to a complacent establishment was to shock it.

In the summer of 1997, Minihan deployed a classified wargame called "Eligible Receiver." The first phase of the game was a tabletop simulation in which a "Red Team" of NSA agents played the roles of Iranian, North Korean, and Cuban cyber-attackers. A "Blue Team" of defenders from the CIA, Defense Intelligence Agency, FBI, Department of State, Department of Justice, Defense Information Systems Agency, and National Reconnaissance Office failed to prevent the Red Team from inflicting major—although simulated—damage on systems like 911 centers and power grids.

In the second phase, NSA agents set up operations in a remote warehouse with the express mission of actually disrupting the communications of the U.S. military's command and control systems. During Minihan's quest to get approval for the exercise, he had been informed that the NSA was bound by law not to use its specialized tools domestically. This meant the Red Team had to rely exclusively on "off-the-shelf" hacker tools found on the Internet. This limitation made what happened next that much scarier.

Minihan set aside two weeks for the exercise, but the Red Team penetrated the entire defense establishment network within *four days*. Had this been a real war, orders from the President of the United States would have been transmitted through a command center that the hackers breached on the first day.

In a third phase, the Red Team took actual hostages in Guam and Hawaii, and hijacked a marine vessel at sea. These real-world (albeit fake) crises were unfolding when the defense establishment was unable to send or receive messages with any reliability.

John Hamre, the newly appointed deputy secretary of defense, and the rest of the defense establishment had to admit that a handful of smart people armed with nothing more than an Internet connection had demonstrated the ability to cause havoc. It was a sobering realization; but it would have shaken the generals even more to have learned one fact Minihan kept to himself—during the exercise, his Red Team hackers had run across what appeared to be actual foreign spies rummaging around in the defense networks.

While the government sized up how to react, in early 1998 another round of attacks that came to be known as "Solar Sunrise" hit almost two dozen computer systems across the military. The common assumption was that Saddam Hussein was behind the attack. Iraq had just expelled the UN inspectors responsible for confirming he had not restarted his weapons programs; President Clinton had started preparing troops for possible deployment to the Persian Gulf; and then Solar Sunrise happened. It was easy to draw lines of connection between the events.

One of the NSA Red Team hackers, however, disagreed. Having planned a similar attack himself for a possible follow-up to Eligible Receiver, he knew what would have been possible. To him, the actual Solar Sunrise breach seemed meandering, disjointed, and almost pointless. If this was an actual Iraqi attack, it was a poor one.

In fact, the real culprits were teenage boys. Israeli forces arrested 19-year-old Ehud Tenenbaum, the alleged ringleader of the group. An FBI raid picked up two American accomplices, who were so young they would only be publicly identified by their hacker pseudonyms "Stimpy" and "Mac." Tenenbaum pled guilty, but claimed he was only motivated to demonstrate that the systems were insecure and needed to be reinforced.

This was the sad truth of Eligible Receiver and Solar Sunrise. The hackers got as far as they did because the users had made it so easy. The NSA Red Team broke into the Joint Chiefs of Staff's intelligence directorate by simply calling the office, claiming to be from IT, and asking for passwords—not especially high-level espionage requiring extraordinary tools or skillsets. Tenenbaum's teenage hackers got into military computers because of a flaw in the Sun Microsystems Solaris operating system—that Minihan had urged be fixed, but no one had taken any steps to patch.

Modest steps on the part of computer users could have hindered or thwarted either attack. That lesson, though, perhaps cut too close to home. It was more comforting to indulge the illusion that our computers were threatened by unbeatable adversaries and hacking prodigies. The myth of the all-seeing NSA and teen geniuses absolved the victims of their role in the incidents.

David Kalat *is Director, Global Investigations + Strategic Intelligence at Berkeley Research Group. David is a computer forensic investigator and e-discovery project manager. Disclaimer for commentary: The views and opinions expressed in this article are those of the author and do not necessarily reflect the opinions, position, or policy of Berkeley Research Group, LLC or its other employees and affiliates.*