The SCDOR Hack: Great Security Theater in Five Stages

Hal Berghel, *University of Nevada, Las Vegas*

The South Carolina governor's response to the SCDOR hack represents a textbook application of Elisabeth Kübler-Ross's "five stages of grief" to cybersecurity.

In fall, 2012, the State of South Carolina Department of Revenue (DOR) computer systems were hacked, allegedly by Eastern European criminals.

According to Governor Nikki Haley, the security breach yielded the digital denizens of delicta 3.9 million taxpayer files, 1.9 million dependent files, 699,900 business records, 3.3 million bank accounts, and 5,000 expired credit cards (www.wyff4.com/news/columbia-statewide-news/Cyberattack-final-tally-released-SCDOR-head-replaced/-/9324106/17489378/-/ax1yul/-/index.html). Some estimates of the amount of stolen data are even higher (http://standrews.patch.com/articles/dems-call-for-independent-investigation-of-hack-creation-of-fund).

In any case, the extent of the breach attracted considerable media scrutiny, which in turn highlighted the weak security measures in place in the state's IT infrastructure. This attention proved embarrassing to Governor Haley, who compounded the embarrassment by issuing a series of misguided press releases culminating in some great security theater.

I offer this story as my candidate for the 2012 security breach of the year.

THE HACK

The State of South Carolina hired Mandiant (mandiant.com), an information security company, to assess the damage. The following analysis of the hack is derived from Mandiant's *Public Incident Response Report*, released 20 November 2012.

Apparently, the incident began with email phish bait containing a link to online malware that was received by at least one unidentified DOR employee on 13 August 2012, who clicked on that link, which compromised the computer. The injected malware subsequently forwarded the harvested userID and password information to the hacker, who reused it for remote login to one or more of the victim's workstations, and sent it from there to a DOR server.

Within a few weeks, the attacker leveraged this access to obtain userIDs and passwords for all Windows account holders and also install a back door on one DOR server. By mid-September, the attacker was able to access and compress sensitive taxpayer data files from the DOR server cluster, transmit them over the Internet, and cover his or her tracks. By 20 October 2012, DOR had implemented a Mandiant remediation plan.

While the nature of the attack is interesting, were it not for the type of data compromised and the governor's response, this would've been a relatively routine incident. The payload was South Carolina taxpayer records—a veritable treasure trove of goodies in identity theft.

According to Mandiant, the compromise extended to 44 computer systems. Malicious software ("backdoor") was installed

0018-9162/13/$31.00 © 2013 IEEE Published by the IEEE Computer Society

on one system, database backups were stolen from three systems, one system was used for egress downloads to the attacker, and the attacker accessed 39 systems to perform activities such as reconnaissance and password hash dumping.

The attack used 33 unique pieces of malware and data management utilities, including

- a backdoor,
- multiple password dumping tools,
- multiple administrative utilities,
- multiple Windows batch scripts to perform scripted actions, and
- multiple generic utilities to execute commands against databases.

The attack reportedly came from at least four undisclosed IP addresses, it used at least four DOR accounts, and compromised 74.7 gigabytes of data from 23 database backup files, representing the millions of taxpayer records. Only some of the data was encrypted when stored on the DOR servers. No explanation was offered about what underlying rationale DOR used to justify encrypting some taxpayer records and not others.

South Carolina's information security policy at the time of the SCDOR hack might become a timeless classic to rival those of the Brothers Grimm and Hans Christian Andersen.

POLITICIANS AND THE FIVE STAGES OF COVERING YOUR ASSETS

The South Carolina governor's response is a textbook application to cybersecurity of Elisabeth Kübler-Ross's "five stages of grief." For want of a better phrase, we'll label this the "politicians' five stages of covering your assets."

Stage 1: Denial and isolation. Apparently DOR didn't even notice the 12 August hack until the US Secret Service informed the state leadership a month and a half later (www.fitsnews.com/2012/11/02/scdor-refused-cyber-security-aid). What's even more unbelievable is that the DOR director may have been informed that malware was being downloaded on DOR computers the day after the hack, but did nothing (www.databreaches.net/?p=26699). This denial is more expansive than its counterpart in Egypt.

Stage 2: Anger. Governor Haley first went on the attack with typical political embroidery: "I want this person slammed against the wall" (www.huffingtonpost.com/2012/10/26/nikki-haley_n_2025317.html). As it turns out, she didn't have to look far to find someone to slam, as one candidate was just down the hall.

Stage 3: Bargaining. This is also known as making a deal with the political base, if not the devil. Following in the long-established tradition of doublespeak, Governor Haley offered the following comment: "The industry standard is that most Social Security numbers are not encrypted. A lot of banks don't encrypt. It's very complicated. It's very cumbersome. There's a lot of numbers involved with it" (http://finance.yahoo.com/news/haley-taxpayer-didnt-encrypted-223600346--finance.html).

Stage 4: Depression and worry. At this stage, the governor stated, "There wasn't anything where anyone in state government could have done anything to avoid it" (29 Oct. 2012; www.fitsnews.com/2012/10/29/nikki-haley-nothing-could-have-stopped-hackers). Obviously, she hasn't attended many SANS conferences over the past few decades. She clearly didn't ask the state's payment card industry and anti-money-laundering specialists to weigh in before this statement was crafted. We speculate that, taken together, stages 3 and 4 circumscribe what may be the Palmetto State equivalent to a force majeure defense.

Stage 5: Acceptance. "International hackers are not going to do this from 9 to 5," Haley observed. Therefore, she indicated that she was going to add four FTEs for 24/7 monitoring of the systems recently put in place to reveal suspicious activities on state computers (www.youtube.com/watch?v=YXk-tngz6f0). After extensive media criticism, Haley suggested that the state should have done more to protect the taxpayer data. There's a news flash for you.

At this point, it appears that South Carolina's taxpayer-victims will pay $20 million for remediation, with another $20 million budgeted for beefing up DOR's cybersecurity defense in 2013. In her press conference on 15 November, Governor Haley announced that her administration would be adding systems to monitor network activity. Her explanation of how this system will work is priceless: www.youtube.com/watch?v=YXk-tngz6f0.

ANALYZING THE BLUNDERS

What makes the South Carolina experience most interesting isn't so much the forensics but the state's reaction. There's a lesson in top-down blundering that could have been easily avoided had professionals with any significant background in digital security been consulted.

At the administrative level, the state's greatest embarrassment is due to the governor's dissemination of misleading and confusing information. The lesson here for

all administrators and executives is that the appropriate response to security breaches isn't convulsive blathering. Any seasoned security professional or enlightened legal counsel would have advised confining press releases, especially during the investigation, to prepared statements vetted by the CISO, CIO, and legal counsels well in advance of the incident. These responses should follow a proscribed template, for example, "The State of xxxxxx Department of xxxxxx respects the privacy of all citizens and taxpayers, and is committed to protecting sensitive data. We will have more to say as the investigation proceeds." Full stop. End of story.

One reason the South Carolina DOR's CISO didn't vet a press release was that the department didn't have a CISO. DOR director Jim Etter speculated that the anticipated $100,000 salary for a CISO was a barrier to successful recruiting (save $100,000 versus spending $40,000,000—this is a classic product of FROI (foolish return on investment) analysis. Security professionals have dealt with this penny-wise, dollar-foolish attitude for many years (www.berghel.net/col-edit/digital_village/apr-05/dv_4-05.php). Incidentally, Etter submitted his resignation 20 November.

Inquiring minds must ask: what information security policy was in place at the time of the SCDOR hack? The mainstream media seems to have missed this issue entirely. That policy should have made explicit such things as the organization's position on data classification and retention, encryption, password policies, incident response policy, and so forth. Best practices have been widely agreed upon and standardized for decades (BSO7799, ISO 17799, ISO 27000, COBIT, FISCAM, and PCI DSS) and have found their way into federal law (HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley).

URL PEARLS

The Mandiant report of the SCDOR incident is online at http://governor.sc.gov/Documents/MANDIANT%20Public%20IR%20Report%20-%20Department%20of%20Revenue%20-%2011%2020%202012.pdf.

Reports on the economics of the SCDOR hack can be found at

- www2.wjbf.com/news/2013/jan/06/south-carolina-legislators-pledge-tackle-cybersecu-ar-5308319;
- www.fitsnews.com/2012/12/11/scdor-running-deficit; and
- www.usatoday.com/story/news/nation/2013/01/06/south-carolina-cyber-security-protections/1566082.

For the story behind the unfilled DOR CISO position, see www.bankinfosecurity.com/blogs/how-much-good-ciso-worth-p-1387 or www.wltx.com/news/article/210418/2/Etter-Revenue-Dept-Without-Cyber-Expert-for-1-Year.

There is some question about whether these best practices made it as far as South Carolina. The state's information security policy at the time of this incident might become a timeless classic to rival those of the Brothers Grimm and Hans Christian Andersen.

Hal Berghel, *Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@computer.org.*