The Center for Internet Security Boosts Government Cybersecurity (VIDEO)

Steve Towns | October 9, 2012

In 2010, police investigating what appeared to be a relatively minor case of financial fraud made a startling discovery: The case they were working on — which involved $30,000 stolen from a local college — was linked to a worldwide crime ring that was using malware to harvest personal data from infected computers and then sending it across the globe.

The larger implications of the case came to light after forensic images from college servers were examined by the Center for Internet Security (CIS), a New York-based nonprofit that acts as a hub for sharing cyberthreat information and security best practices among state, local and tribal governments. CIS analysts discovered that the servers were infected by a nasty piece of computer code called Qakbot, which opens a back door into compromised computers, allowing cybercrooks to steal confidential information.

By examining file transfer records from the college, the analysts determined that 17 states were victims of the crime ring, and they tracked down an IP address in Russia that was downloading the stolen information. With the permission of police investigators, the CIS quickly contacted states that were impacted and organized a conference call

for members of its Multi-State Information Sharing and Analysis Center — known as the MS-ISAC — to warn others of the danger and tell them how to block it.

The incident, in a nutshell, demonstrates why the CIS may be one of the most potent weapons that states and localities can bring to bear against increasingly sophisticated cybercriminals and terrorists. Every state in the union now shares cyberthreat information through the MS-ISAC, and the CIS is working to pull in more local governments. The organization also has formed key relationships with the Department of Homeland Security and others, allowing it to tap into federal funding and cyberthreat intelligence.

Most of what the CIS provides comes at no cost to public agencies. Membership in the MS-ISAC is free, as is access to a storehouse of best-practice information, including standard templates that show agencies how to secure their computers, and shopping lists for the types of tools needed to lock down government systems and data. The CIS also offers an expanding number of paid services and programs that give agencies access to more sophisticated security capabilities at steeply discounted prices.

The seeds of what is now the CIS were planted in the years immediately after 9/11. The country was scrambling to safeguard its critical infrastructure, and Will Pelgrin, then director of the New York State Office of Cyber Security, saw the need to strengthen cybersecurity in the nation's 50 state capitals. The best way to do that, he recognized, was for state governments to share with one another information about the cyberattacks hitting their computer networks.

Pelgrin talked 10 states into joining the fledgling MS-ISAC. That number grew to 15 before the group's first official meeting, an event that drew a visit from Howard Schmidt, who was then in his first tour of duty as White House Cyber Security czar.

"It wasn't your typical government meeting. Our attitude was, 'Let's don't talk this to death; let's get something done,'" Pelgrin recalled. "I remember Howard sitting next to me, and he just leaned over and said, 'This is a good meeting. Can you do this for the rest of the country?'"

And that's what Pelgrin did. Somewhat miraculously, he built and maintained support for the multi-state information sharing group under five New York governors, running the organization within the state cybersecurity office. Eventually he coaxed all 50 states to voluntarily join the MS-ISAC, along with a number of local governments and territories.

Pelgrin is quick to credit MS-ISAC members for the group's success. But industry veterans say Pelgrin is the driving force. A trained lawyer, former state CIO and passionate security advocate, he has a nearly perfect skill set for leading the organization.

"What he does is focus on the pieces of the puzzle that we can agree on," said Lohrmann. "He fixes those and then moves onto the next thing."

In addition, Lohrmann describes Pelgrin as a master networker, easily rubbing elbows with federal lawmakers and unafraid to testify on Capitol Hill. And, in an industry that's often obsessed with secrecy and legal protections, Pelgrin tends to cut through bureaucracy. For instance, Lohrmann says the MS-ISAC was built on a foundation of trust, common purpose — and very little red tape. " Will's approach was, 'Send me an email and you are in.'"

Pelgrin may be a lawyer himself, but he admits to steering clear of legalities — at least as much as possible, given the sensitive nature of the group.

"For the longest time I kept lawyers away from the table," he said. "I didn't want nondisclosure agreements; I didn't want contracts. I wanted people to come in with a common passion and a commonunderstanding. It was very informal within a formal context. We developed a code of conduct that you respect the other person's information and you don't use it without their approval — and that we're all in this together."

One fundamental goal of the MS-ISAC was lifting the shroud of secrecy that surrounds information security breaches so that states could learn from one another.

"In the past, people just hid it. You didn't know that you had a breach because the person who is responsible probably fixed it really quickly and didn't say anything," Pelgrin said. "We can't have a culture that feels that way. We need this to come to the surface; we need to be able to talk about it."

That starts with a painful admission from Pelgrin. Years ago, his own home computer was infected by a virus. He still keeps the compromised PC in his basement — a reminder to stay vigilant — but said he intends to take a sledgehammer to it someday. "I start out a lot of my speeches by saying, 'Hi, I'm Will Pelgrin and I've had a security breach,'" Pelgrin said. "If I'm not going to say it, who is?"

Desire for better information sharing drove the biggest change in the MS-ISAC's existence — a shift to nonprofit status in 2010. After nine years of operation within New York state government, the MS-ISAC joined with the Center for Internet Security, a nonprofit group that had been providing checklists for securely configuring computer systems since 2000. The combined organization, which retained the CIS name, moved into a state-of-the-art facility just outside of Albany, N.Y., and Pelgrin became its CEO.

The move to nonprofit status eases turf disputes with other government entities, Pelgrin said. And positioning the MS-ISAC as a trusted third party opens the door to greater information sharing between the public and private sectors, as well as new types of partnerships. "We're doing things now that I don't think would have been possible as a for-profit or government entity," he said.

The heart of the CIS is the Security Operations Center (SOC), where teams of analysts monitor customer networks and scan the Internet for emerging threats 24 hours a day. In the room's dim light, banks of monitors glow with news coverage and maps showing cyberalert levels for all 50 states. MS-ISAC members agree to follow a standard color-coded, five-level alert protocol. During a recent visit, most states on the map were

shaded blue, indicating a “ guarded” condition. The rest were green, signifying low threat activity.

Analysts in the SOC receive an alert when state conditions change. Should a state move to one of the higher alert levels — signifying a possible attack or data breach — the facility springs to life. CIS analysts and senior executives immediately contact the impacted state, gathering information and tracing the source of the problem. And within hours of the first notice, a team of CIS executives conducts a 50-state conference call to alert the rest of the country to the danger and how to prevent a similar attack.

“We’ve done it time and time again. It’s really a tribute to how the states work together,” said Brian Calkin, assistant director of the SOC. “We’re able to reach out to them and have everyone come together in a short amount of time.”

A fully equipped computer lab located a few feet from the SOC also can be called in to identify malware and figure out how to stop it. “We can reverse engineer malicious code. We can do computer or network forensics,” said Adnan Baykal, director of the CIS Computer Emergency Response Team. “If the state or local entity is not mature enough from the incident response perspective, we can handle the entire incident for them and tell them the steps they need to take so that it doesn’t happen again.”

The lab also gives the CIS a unique ability to connect the dots on complex incidents. Inside a room crammed with high-powered computer hardware, agents from local police; the FBI; Secret Service; Customs; and Alcohol, Tobacco, Firearms and Explosives work shoulder-to-shoulder to unravel cybercrime or terror cases. Since 2010, a CIS analyst also has been embedded in the National Cybersecurity and Communications Integration Center, the federal government’s cyber-operations center.

In 2005, while still part of the New York state government, the MS-ISAC broke more new ground by offering low-cost network monitoring and related services to other governments. Alaska was the first customer, according to Darrell Davis, Alaska’s chief security officer. Davis says the deal literally was worked out on a napkin, although he and Pelgrin spent another year getting approval from their respective state management.

Today, Alaska remains a CIS network monitoring client, and Davis says collaborative efforts such as these hold the key to improving information security. “I’m a firm believer that leveraging our talent and leveraging our services is the only path to success,” he said. “We all have declining budgets and declining staff. We can’t afford to stand alone.”

Davis adds that Alaska was a natural first customer for the new services. “We have a built-in culture to want to promote this. We are isolated and our resources are limited, so we always look to partner with different entities for the greater good.”

Davis may have been first, but he’s not the only one buying into the concept. Bob Cheong is the chief information security officer for Los Angeles World Airports, the city agency that operates three Los Angeles-area airports, including LAX. Like Davis, Cheong is a member of the free MS-ISAC and a customer of CIS paid services.

Even though Cheong has a top-notch security staff and an airport workforce that is extremely security conscious, he uses CIS services to augment his internal resources. “I need 24-hour network monitoring, but my crew is 8-5,” Cheong said. He relies on 24-hour monitoring from the CIS for after-hours protection, and those services provide an extra level of safety during the business day. “ Because we’re an airport, we need multiple layers of protection,” he said.

Cheong has been a CIS services customer for three years, and he intends to sign up for another five years when his current contract ends in 2013. “Their service is really good and so is their pricing,” said Cheong. He’s also a fan of information provided by the MS-ISAC. “They work closely with Homeland Security to give us inside information about any threats coming at us, so we can block them before they happen.”

Despite its move into paid services, the CIS isn’t viewed as a competitor by one of the nation’s biggest security vendors. Mike Maxwell, director of Symantec’s state and local government organization, said the company shares cyberthreat information from its massive global intelligence network with the CIS under a partnership that goes back some 10 years.

Although both Symantec and the CIS sell security services, the CIS offerings tend to be aligned much more closely to public-sector needs. “CIS covers a much broader range of requirements, capabilities and specialized information,” Maxwell said. “Whereas Symantec has managed solutions targeted at some very specific areas.”

Maxwell said free and low-cost services from the CIS play a vital role in improving information security for state and local governments. Those efforts, he adds, often can generate interest in private-sector offerings. “The intelligence that state and local agencies get from CIS can be the foundation for enhancing their cybersecurity programs,” Maxwell said. “Our experience is that they see with a new set of eyes some of the threats they need to manage, and they might need hardware or software tools from the private vendor community.”

Making some of that hardware and software more affordable is the newest mission for CIS. In April, the organization launched a program designed to drive down the price of security products by combining state and local government purchases into bulk buys. The Trusted Purchasing Alliance works with public agencies to pinpoint the areas of greatest need, and then negotiates with vendors for discounted pricing. Product choices are vetted by a review board stocked with analysts and security experts.

The alliance already offers deals on several categories of security products and is soliciting vendor proposals for mobile device management, two-factor identification, and hardware and software encryption. The approach already appears to be working. L.A.’s Cheong noted that the alliance lets him buy popular training programs from the SANS Institute at prices that are “five to 10 times cheaper” than he can get on his own.

Kristin Judge, a former county commissioner in Michigan, was hired by the CIS earlier this year to be executive director of the alliance and to expand local government participation in the MS-ISAC. Judge said one of her tasks is to raise local awareness

of CIS resources. Another is to improve understanding between elected officials and IT departments.

“It’s easy to cut an IT budget because you can’t really see the impact of it as clearly as feeding or sheltering the homeless,” said Judge. “Elected officials making those decisions need to understand cyberthreats and the role they play in keeping residents safe.”

Pelgrin agreed that information security still struggles for executive attention, despite evidence that cybercrime is growing both in sophistication and severity. Years of economic recession hasn’t helped the cause either.

“We need to get beyond the point that this is the first place to cut in bad fiscal times,” he said. “I don’t think security wins out on everything, but there is a risk/benefit analysis. The people making decisions need to hear from the cyberpeople about the potential consequences of those decisions.”

One of the biggest mistakes officials can make, Pelgrin added, is to cut cybersecurity spending because they haven’t had a security breach. Just because you haven’t seen a breach, he warned, doesn’t mean you haven’t had one. “A lot of this is happening under the covers. The bad guys may be in your system at this point watching everything you’re doing, and your system still looks and acts as if it were OK.”

On the other hand, the news isn’t all bad. State and local governments have dramatically raised their awareness of cybersecurity over the past several years. And a majority of cyberthreats can be defeated through basic steps like requiring strong passwords and clicking the right boxes when setting up computer equipment.

“I think we’re doing a lot right, and there’s a lot that we can do to move forward,” said Pelgrin.

Thanks to the growing array of services available from the CIS, state and local agencies don’t need to figure out their next steps by themselves. “I think the message out of all this,” he said, “is that you’re not alone.”

Photo: Analysts in the CIS security operations center watch for cyber-attacks 24 hours a day. By Jessica Mulholland

http://www.govtech.com/security/The-Center-for-Internet-Security-Boosts-Government-Cybersecurity-VIDEO.html