KnowBe4.com
Human error. Conquered.

Cyber Birds Of Prey Hunt Small Business

SITUATION

Small businesses are notorious for lack of security procedures. Little or no IT staff, busy owners, inadequately trained staff and lax procedures open the door to cybercrimes. In fact the door is wide open. And to make matters worse, banks are refusing to be the fall-guy and accuse account holders of poor security practices. Small businesses thus become easy targets for cyber-attacks with few financial or technical resources to stop them. Often times, the banks involved are small as well. Small-town banking just does not have the same security resources as the bigger banks. Moreover, companies simply do not have legal protection from identity fraud, unlike individual consumers, and are forced to absorb the losses caused by cyber theft.

But who is really to blame?

CASE IN POINT – MODESTO, CALIFORNIA FEBRUARY 8, 2010

When David Johnston woke up that morning, the last thing on his mind was cybercrime. But unfortunately, his company Sign Designs Inc., an electric-sign maker in Modesto, California was on a hacker's mind. And then there was the phone call from their bank, Bank of Stockton, inquiring about a $9,670 electronic payment to a Chase customer in Michigan. Sign Designs confirmed it hadn't set up the payment and the banks halted the transaction.

However, they were a little late on the chain. Close to $100,000 had been transferred out of their account and distributed to 17 money mules. The Bank of Stockton responded as rapidly as they could once they discovered the online deception. They managed to secure a little more than half of the absconded funds but $48,000 was already in the hands of the hackers.

Naturally, Bank of Stockton declares no responsibility since its security systems were never actually penetrated. The bad guys had planted malicious software on the computer of Sign Designs' controller and used it to steal his online-banking credentials. The bank also says Sign Designs failed to take advantage of security measures that might have averted losses, such as requiring two staff members to sign off on every payment.

DIGITAL CRIME OUTPACES REAL-WORLD ROBBERIES

Digital crime now outpaces real-world bank robberies in terms of losses. In 2009, there were 8,818 bank robberies netting criminals an average of $4,029 -- a total of about $35.5 million, according to the FBI's Uniform Crime Reporting (UCR) program. However, 60 percent of bank robbers were caught, often very quickly.

Compare that to fraud statistics of Automatic Clearing Houses (companies in charge of electronic funds transfers and credit card payment processing). The recent arrests connected with Zeus accounted for some 390 reported cases where $70 million was stolen from accounts. The criminals had attempted to steal some $220 million. The investigation mainly netted the lowest ranks of the criminal network -- the so-called money mules that remove stolen funds from their accounts and transfer the money to international accounts abroad. In general, the money mules are people who are duped into believing they are working for a legitimate company processing payments.

ANALYSIS

Small business and regional banking attacks are on a major upswing. As indicated both lack creditable security procedures and open themselves up to attack. However, in this case it was proven once again that the financial attack was the result of an earlier malicious program attack. This program did not insert itself onto the controller's computer. He had to have done something to initiate the attack. Ignorance not maliciousness was the culprit.
Sign Designs President David Johnston argues that Bank of Stockton should cover the losses because it didn't flag the highly unusual account activity nor did it bar two computers—the controller's and hacker's—from accessing the account with the same credentials at the same time. "I don't think they should offer a service that is not safe," Mr. Johnston says. "Do you expect I'm going to solve this? I'm going to take on these Russian thieves? Clearly I'm not going to be able to do it."
Actually, Mr. Johnston with all due respect, you can take them on. Educate your staff. Don't let them fall for fishing expeditions.

"Small-town banking just does not have the same security resources as the bigger banks. Moreover, companies simply do not have legal protection from identity fraud, unlike individual consumers, and are forced to absorb the losses caused by cyber theft."