Did E-Vote Firm Patch Election?

by Kim Zetter

Diebold Election Systems has had a tumultuous year, and it doesn't look like it's getting any better.

Last January the electronic voting machine maker faced public embarrassment when voting activists revealed the company's insecure FTP server was making its software source code available for everyone to see.

Then researchers and auditors who examined code for the company's touch-screen voting system released two separate reports stating that the software was full of serious security flaws.

Now a former worker in Diebold's Georgia warehouse says the company installed patches on its machines before the state's 2002 gubernatorial election that were never certified by independent testing authorities or cleared with Georgia election officials.

If the charges are true, Diebold could be in violation of federal and state election-certification rules. The charges also raise questions about the integrity of the Georgia election results and any other election that uses patched Diebold systems that have not been re-certified.

According to Rob Behler, an engineer hired as a contractor to work in Diebold's Georgia warehouse last year, the Diebold systems had major functioning problems.

Behler said 25 to 30 percent of the machines in one shipment to the warehouse either crashed upon booting or had problems with their real-time clocks, causing the systems to register the date inaccurately then boot improperly or freeze up altogether.

"They did not meet what I would deem standard operation," he said.

Behler said Diebold provided warehouse workers with at least three patches to apply to the systems before state officials began logic and accuracy testing on them. Behler said one patch was applied to machines when he came to the warehouse in June, a second patch was applied in July and a third in August after he left the warehouse.

Behler first informed Bev Harris, owner of the BlackBox Voting site, of the situation. Harris has spent a year investigating problems with electronic voting systems, and is the author of a forthcoming book on the technology. She said the practice of patching systems after they've been certified opens the possibility for anyone—from Diebold employees to local election officials—to install malicious code on a machine that could alter election results and then delete itself to avoid detection.

According to Harris, this scenario is particularly worrisome in light of what happened in the Georgia gubernatorial race, which ended in a major upset that defied all polls and put a Republican in the governor's seat for the first time in more than 130 years.

Republican candidate Sonny Perdue managed to unseat Democratic incumbent Roy Barnes with only 51 percent of the vote. It was the first time an incumbent governor had not won his second term since Georgia law allowed back-to-back terms in 1978.

Pundits have attributed the upset to dissatisfaction with the incumbent for altering a Confederate symbol on the state flag and to effective stumping by President George W. Bush on behalf of Perdue.

Harris acknowledged no proof exists that anyone rigged the election systems, but she said, "We'll never know exactly what happened in Georgia because there's no paper trail

to verify the votes."

Harris and other voting activists around the country are calling for states and certifying authorities to open the election process and electronic voting systems to public scrutiny to ensure public confidence in elections.

Officials in Georgia's secretary of state's office did not respond to repeated calls for comment.

Behler was hired by Automated Business Systems and Services, a large contracting agency, to work in Diebold's Georgia warehouse from mid-June to mid-July 2002, five months before the gubernatorial election.

He was in charge of assembling about 20,000 machines for the election, testing them and shipping them to 159 counties. But, he said, the work was complicated by misbehaving machines that presented few clues to their problems.

"It's hard to track down a problem when you go out to your car and the first time it starts, the next time the headlights don't work, the next time you start it the brakes are out, and the next time you start it the door falls off," Behler said. "That's really the way they were."

Behler said Diebold programmers posted patches to a file-transfer-protocol site for him and his colleagues to apply to the machines.

Diebold did not respond to repeated calls for comment, but in an interview with Salon a few weeks ago, company spokesman Joseph Richardson denied the company applied any patches to the Georgia machines.

"We have analyzed that situation and have no indication of that happening at all," he said.

Rebecca Mercuri, a computer science professor and research fellow at Harvard University's Kennedy School of Government who is an expert on voting machines, says an unregulated change to voting software would raise big concerns for her.

"Having any change to the operating system allows someone to slip in anything to the code. If (a patch) was not run through the inspection process, then there could be a violation of the Georgia state law," she said.

Indeed, Georgia law requires that companies that make changes to fix defective systems after they are certified must let state officials know about the changes and provide test documentation showing that changes do not do anything to the system other than fix the defect.

Before machines are used in an election, state election boards conduct logic and accuracy tests (PDF) on them with a mock election to make sure the machines perform properly. Academics at Kennesaw State University, led by professor emeritus Brit Williams, have a contract with the state to perform this testing.

But Behler said Diebold instructed him and his colleagues to fix problems with the machines before Kennesaw State would see them.

"If they started erring in mass quantities, Kennesaw State's going to raise a red flag, the secretary of state's going to raise a red flag and Diebold wouldn't get paid," Behler said.

He said the machines were patched not only in the Diebold warehouse, but also in county warehouses after they were shipped from Diebold.

At one point, Behler said he went to a warehouse in DeKalb County with "a high-level Diebold executive" to examine systems that were freezing up. Behler patched 1,387 machines but said, "We were still running upwards of 20 to 25 percent errors."

Diebold programmers contacted him and his colleagues and told them the patch was incorrect and they'd have to load a new one.

"JS equipment is what we were calling it at the time," said Behler. "Junk shit. Everyone in the warehouse was familiar with the term, to say the least."

Behler said the patches he applied were never certified. No third party, other than the Diebold engineers who created the patches, knew what was in the patches. And once machines were patched, they did not undergo re-certification.

When he told Kennesaw professor Williams in July that the machines were being patched, Behler said Williams told him: "Do whatever you need to do now, but you won't be touching the machines once we start our systems-testing on them."

Diebold officials, including company president Bob Urosevich, were angered that he had talked to Williams, according to Behler.

"I literally got called on the carpet and . . . told that I was not to speak a word to any of the Kennesaw State people," Behler said.

Behler said as far as he knows, election officials in the Georgia secretary of state's office were never told about the patches.

"That's the last thing Diebold wanted," said Behler. "They made that very clear. . . . I sat around tables where (Diebold people) discussed whether they were going to tell them the truth, the half-truth or a complete lie.

"I understand if a company has information that they need to keep under tight lip. But when you sit around discussing lying to a client in order to make sure you're getting paid . . . it's an ethics issue."

Williams of Kennesaw State University denies Behler ever mentioned patches to him and said, to his knowledge, no uncertified patches were applied to the machines. He said he would be very concerned if this happened.

"If they were changing the configuration of the machine, that would certainly be a concern because that would violate the certification," he said.

Williams does acknowledge, however, that a month and a half before the November election, he worked with Diebold to apply a patch to the Windows CE operating system. The voting machines run on version 3.0 of Windows CE, he said, and they patched it to correct problems they were having with the system.

But he said this patch was passed by Wyle Laboratories, the independent testing authority that originally certified the machines.

"We asked (Wyle) to take a quick look at it, but we didn't have time to do a full qualification on it. This was a month and a half before the election. To go through the full ITA qualification and state certification takes about six months. We asked them to look at it from the point of view of whether or not it would have any impact at all on the main line of the voting software."

As for other patches, Williams said, "We have no idea what Diebold or anybody else does when they go in their warehouse and shut that door."

Williams said they compare the system when it comes out of the Diebold warehouse to make sure it's the same software version that was certified by the ITAs. But he acknowledges that this does not include reading the source code.

He added, however, "We have absolutely no reason to believe that Diebold did anything in that warehouse that we're unaware of."

As for Behler, Williams said he's a disgruntled employee who was fired from the project by Diebold and Automated Business Systems and Services. ABSS, however, said this isn't true.

Initially, Terrence Thomas, ABSS vice president for the southwest region, told Wired News that Behler was dismissed for "lack of performance." But when pressed to elaborate, Thomas consulted Behler's employee file, which he said he had previously not read, and admitted there was no indication that Behler was fired or that anyone at Diebold or ABSS had been disappointed with his performance.

"He was released because his part of the project was completed," Thomas said. He repeated that it wasn't a performance issue. "Officially in my files, there's nothing to indicate that," he said.

James Rellinger, another contractor who worked in the Diebold warehouse until November, confirms that both Diebold and ABSS seemed happy with Behler's work.

Rellinger said workers were surprised when they learned Behler had been replaced and hinted that internal politics were likely the cause. Behler was replaced by a friend of an ABSS project manager, who was later hired as a full-time employee of Diebold.

Behler denies he's a disgruntled employee, saying he is going out on a limb by revealing information that could cost him future work.

"I have seven children to support," he said. "This is not the kind of thing I would say if it wasn't the truth."