Hackers Lurking in Vents and Soda Machines

Companies' Networks Prove Vulnerable to Third-Party Links

By NICOLE PERLROTH

SAN FRANCISCO — They came in through the Chinese takeout menu.

Unable to breach the computer network at a big oil company, hackers infected with malware the online menu of a Chinese restaurant that was popular with employees. When the workers browsed the menu, they inadvertently downloaded code that gave the attackers a foothold in the business's vast computer network.

Security experts summoned to fix the problem were not allowed to disclose the details of the breach, but the lesson from the incident was clear: Companies scrambling to seal up their systems from hackers and government snoops are having to look in the unlikeliest of places for vulnerabilities.

Hackers in the recent Target payment card breach gained access to the retailer's records through its heating and cooling system. In other cases, hackers have used printers, thermostats and videoconferencing equipment.

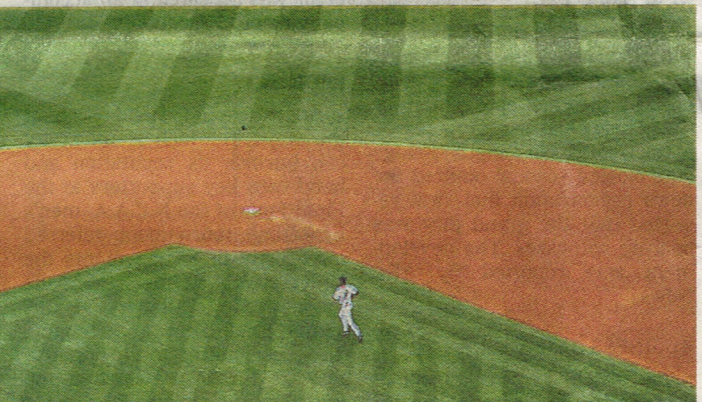
Companies have always needed to be diligent in keeping ahead of hackers — email and leaky employee devices are an old problem — but the situation has grown increasingly complex and urgent as countless third parties are granted remote access to corporate systems. This access comes through software controlling all kinds of services a company needs: heating, ventilation and air-conditioning; billing, expense and human-resources management systems; graphics and data analytics functions; health insurance providers; and even vending machines.

Break into one system, and you have a chance to break into them all.

"We constantly run into situations where outside service providers connected remotely have the keys to the castle," said Vincent Berk, chief executive of FlowTraq, a network security firm.

Data on the percentage of cyberattacks that can be tied to a leaky third party is difficult to come by, in large part because victims' lawyers will find any reason not to disclose a breach. But a survey of more than 3,500 global I.T. and cybersecurity practitioners conducted by a security research firm, the Pone-

Continued on Page B4



Hackers Lurk in Vents And the Soda Machines

From Page A1

mon Institute, last year found that roughly a quarter — 23 percent — of breaches were attributable to third-party negligence.

Security experts say that figure is low. Arabella Hallawell, vice president of strategy at Arbor Networks, a network security firm in Burlington, Mass., estimated that third-party suppliers were involved in some 70 percent of breaches her company reviewed.

"It's generally suppliers you would never suspect," Ms. Hallawell said.

The breach through the Chinese menu — known as a watering hole attack, the online equivalent of a predator lurking by a watering hole and pouncing on its thirsty prey — was extreme. But security researchers say that in most cases, attackers hardly need to go to such lengths when the management software of all sorts of devices connects directly to corporate networks. Heating and cooling providers can now monitor and adjust office temperatures remotely, and vending machine suppliers can see when their clients are out of Diet Cokes and Cheetos. Those vendors often don't have the same security standards as their clients, but for business reasons they are allowed behind the firewall that protects a network.

Security experts say vendors are tempting targets for hackers because they tend to run older systems, like Microsoft's Windows XP software. Also, security experts say these seemingly innocuous devices— videoconference equipment, thermostats, vending machines and printers — often are delivered with the security settings switched off by default. Once hackers have found a way in, the devices offer them a place to hide in plain sight.

"The beauty is no one is looking there," said George Kurtz, the chief executive of Crowdstrike, a security firm. "So it's very easy for the adversary to hide in these places."

Last year, security researchers found a way into Google's headquarters in Sydney, Australia, and Sydney's North Shore Private hospital — and its ventilation, lighting, elevators and even video cameras — through their building management vendor. More recently, the same researchers found they could breach the circuit breakers of one Sochi Olympic arena through its heating and cooling supplier.

Fortunately, the researchers were merely testing for flaws that could have been exploited by real hackers.

Billy Rios, director of threat intelligence at Qualys, a security firm, was one of those researchers. He said it was increasingly common for corporations to set up their networks sloppily, with their air-conditioning systems connected to the same network that leads to databases containing sensitive material like proprietary source code or customer credit cards.

"Your air-conditioning system should never talk to your H.R. database, but nobody ever talks about that for some reason," Mr. Rios said.

The Ponemon survey last year found that in 28 percent of malicious attacks, respondents could not find the source of the breach. Ms. Hallawell compared the process of finding the source of a breach to "finding a needle in a haystack."

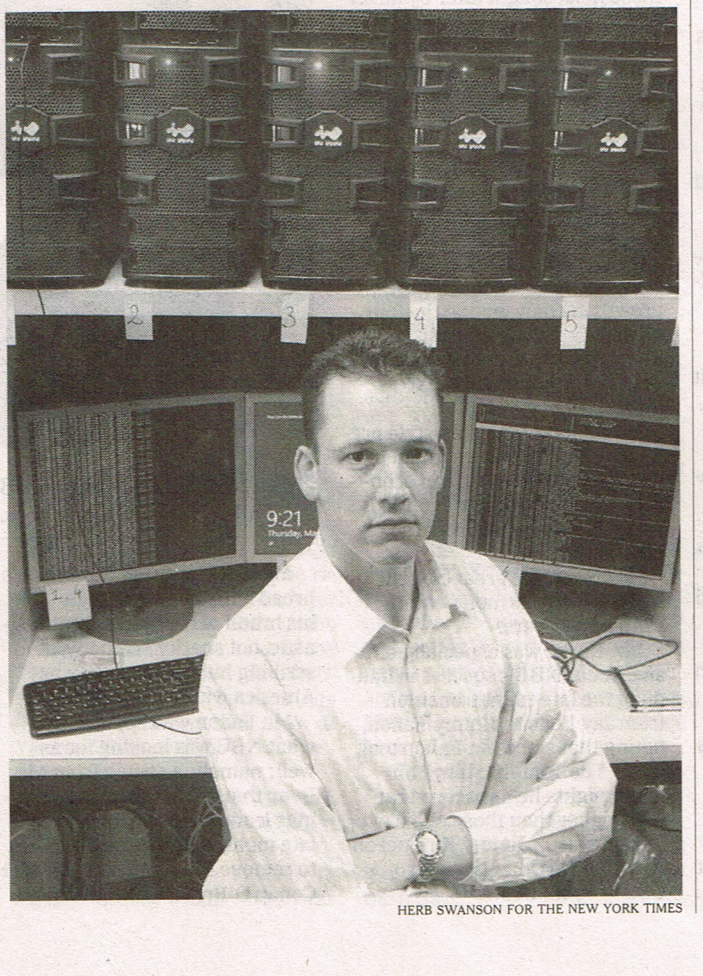
Ideally, security experts say, corporations should set up their networks so that access to sensitive data is sealed off from third-party systems and remotely monitored with advanced passwords and technology that can identify anomalous traffic — like someone with access to an air-conditioning monitoring system trying to get into an employee database.

But even then, companies require security personnel with experience in detecting such attacks. Even though Target used security technology supplied by FireEye, a company that sounds alerts when it identifies such anomalous activity, its I.T. personnel ignored the red flags, according to several people who confirmed the findings of a Bloomberg Businessweek investigation last month but could not speak publicly about Target's continuing internal investigation.

Like all else, security experts say, it's simply a matter of priorities. One Arbor Networks study found that unlike banks, which spend up to 12 percent of their information technology budgets on security, retailers spend, on average, less than 5 percent of their budget on security. The bulk of that I.T. spending goes to customer marketing and data analytics.

"When you know you're the target and you don't know when, where or how an attack will take place, it's wartime all the time," Ms. Hallawell said. "And most organizations aren't prepared for wartime."

JESSICA LIFLAND FOR THE NEW YORK TIMES



HERB SWANSON FOR THE NEW YORK TIMES

Security experts like Billy Rios, above, of Qualys, and Vincent Berk, right, of FlowTraq, say computer-equipped machinery like air conditioners can be used to gain access to sensitive company data.