What the Maroochy Incident taught us about Cyber Warfare

The Shire of Maroochy is one of Australia's delightful treasures—a beautiful and serene rural area that attracts many nature-loving tourists. Maroochy has a local sewage system that handles more than 9 million gallons of sewage every day, using 142 sewage pumps scattered around the shire.

At the heart of the continuous operation of these pumps is, of course, a computer; to be more precise—a computer system called SCADA, which stands for Supervisory Control And Data Acquisition. The title is a mouthful, but the principle is rather simple. A computer gathers information from different sensors—like those that measure sewage levels—and turns the pumps on or off accordingly. Our domestic air conditioning system, for example, is a sort of SCADA. A tiny sensor located in the remote controller reports temperature inside the house to the AC main computer, which then tells the compressor to turn on or off.

In 1999, a man named Vitek Boden was supervising the sewage pumps in Maroochy, working for the company that installed the control system. Boden, then in his forties, had been working for the company for two years until he resigned as a result of a dispute with his bosses. After quitting his job, he approached the district council and offered his services as an inspector. The council declined.

Shortly after, the Maroochy sewage system started having mysterious and seemingly random problems: pumps stopped working; alarms failed to go off; and worst of all, about 200,000 gallons of sewage flooded vast areas. Rivers turned black, nature reserves were destroyed, countless fish and wildlife died, and of course, the local population suffered through the terrible stench for weeks.

Maroochy's water authority hired experts to examine the problems. At first, the experts suspected that disturbances from other control systems in the area were causing the problems, or that there was an error in the hardware. After all the immediate suspects were investigated, the experts were helpless; time after time they examined failing pumps, only to discover new and intact equipment that would simply stop operating, seemingly for no reason.

Sometime later, an engineer working on the sewage system at around 11 o'clock at night, changed one the configurations in the control system. To his surprise, the change was reset and erased a half an hour later. The engineer became suspicious. He decided to thoroughly investigate the data traffic between the different pumps, and discovered that sewage pump number 14 was the one who had sent the order to reset his original configuration change. He drove to pump 14, examined it and its computer, and found them to be in perfect working order.

He was now certain that a human hand was behind the chaos in the system. He decided to set the hacker up. He changed the pump identification code from 14 to three, meaning, all legitimate orders coming from pump station 14 would now be received under identification code 3. He waited until the next error occurred, and then analyzed the data traffic. As predicted, the malicious orders still indicated they were coming from pump 14. In other words, someone had hacked the communication network of the pump and was pretending to be pump number 14.

Vitek Boden became the immediate suspect. Investigators assumed that he was penetrating the network remotely, via wireless communication. It was likely then that during an attack, Boden would be within a few dozen miles from the pump stations.

The water authority promptly hired private investigators that began tracking Boden's movements. On April 23rd, at 7:30 in the morning, another series of errors occurred in the pump stations—but this time the trap set around Boden snapped. A private investigator noted Boden's car on a highway not far from one of the pumping stations, and called in the police. Boden was chased and arrested. A laptop with a pirated copy of the control system software and a two-way radio transmitter were found in his car.

At his trial, Boden claimed that all evidence against him was circumstantial since no one saw him actually hacking the control system. The Australian court wasn't convinced. The circumstantial evidence was pretty strong; especially considering the radio equipment found in his car was designated for operating the control computers of the sewage system. The judge theorized that Boden wanted revenge after having to leave his job, or that perhaps he thought he could win his position back once he was called in to fix the "errors."

Vitek Boden was sentenced to two years in prison, and the crime he committed became a point of interest to IT security experts around the world. They thoroughly analyzed each and every one of his steps, and what they found wasn't very reassuring. Maroochy's control system wasn't designed with cyber-security in mind. As is often the case in the programming world, finding engineering solutions to solve each immediate problem took priority over the less urgent need to secure data. One can guess that security wasn't a top priority for the people who designed the sewage control system, since after all, they had enough s*** to deal with as it was…

Worse yet, the Maroochy incident was only the tip of an iceberg. Industrial control systems, such as the computer system that controlled the sewage pumps in Maroochy, are the foundation on which almost all of our industries and infrastructures are built upon. Millions of control systems are used to control a vast variety of industrial processes all over the world, from assembly lines to nuclear reactors, to making electricity. The ease with which Boden was able to penetrate Maroochy's control system reflected, said the experts, how easily someone could disrupt the gas or electricity supplies to entire cities.

The Maroochy Incident, than, will be recorded in history as an early wakeup call for IT & Industrial professionals—a wakeup call which was later replaced with a blaring train horn when Stuxnet was discovered in 2010, and later Flame & Duqu.