Ryan Leatherman

Professor Sabal

System Administration

4/22/2020

Paper #3

Employees that are fired or are just leaving a business for personal reasons tend to stay connected or have access to their old accounts. There is no specific reason for this other than that the IT department either is not informed of that person leaving, or that they just do not take the time to make sure those people are deleted from the system. During the times of someone being fired or even just leaving the company, it can be easy for them to be convinced that it is a good idea to take the company information and try to make money off of it. The reasons an employee takes confidential company information vary from being benign and misguided to intentional for the purposes of personal gain. According to a survey by Intermedia, “89% of users retained access to accounts from previous places of employment. And 45% said they still had access to “confidential” or “highly confidential” work data from previous jobs.” Even if the ex-employee was a great employee and well respected, the company should never just disregard a well thought out exit plan for every employee that is leaving the organization. There are some things that companies should do in order to make sure that the exit plan is executed for all employees that are leaving the company. The IT department needs to stay in the loop for everyone that is leaving the company and revoke their cloud accounts, account for all shared credentials, and require regular password changes. By doing this it helps make sure that every employee that is leaving does not have the opportunity to take any of the information from their former employer.

What are the effects of leaving an employee in a company's system or forgetting to delete their account even after they are terminated? In many cases there is no effect and it turns out fine, the employee moves on with their life and forgets about their old company without any malicious attempts. This however is not always the case and leaving an account open or allowing an employee to still have access to the company’s network can be a crucial mistake and is often more of a problem than hackers outside the company. When an employee still has access to their old account or still has access to a network, they are easily able to take the information from the company and are able to give that information away to competitors and to the public. Not only are ex-employees a threat to stealing data from the company they once worked at, but they are also a threat of putting malware onto a server or just deleting important information off the servers. Surprisingly, some companies do not address the danger of stealing electronic information through smart phones which include the BlackBerry, iPhone and the emerging Android phones. Devices like smartphones are easily connected to the corporate email system. They can also access WiFi wireless networks for high transfer speeds and even have the ability to connect to a company’s private network. Because of these attributes of the smartphone it can make them a huge threat for a company if the employee still has access to their work email or just stays connected to the company network.

Allegro Microsystems is a technology company that is looking to create more sustainable and efficient solutions for their customers. They develop products such as, sensors, regulators, and drivers for different situations. Back in April of 2017, an employee with the name Nimesh Patel was sued by his ex-employer and accused the IT bod of planting a ticking time-bomb on company's servers to wipe crucial data. Patel worked at high-performance computing chip biz Allegro MicroSystems as a sysadmin for 14 years, with particular responsibility for programming the shop's Oracle financial database system. He resigned on January 8, 2016 but is accused of then trying to sabotage the company. After Patel was fired, he still had access to the company's network because he still possessed one of the work computers that he had acquired from working with the company. “Patel trespassed on company property to get within wireless range of the network, and then used the laptop to log into the network using the account of his subordinate staffer. He then uploaded malware into the Oracle financial gear.” (Thomas). What Patel did was designed software to delete key financial figures and records from the system. It worked, and Allegro found the malicious code with help of investigators and found evidence that Patel was the one who had accessed the network with his second computer.

Even though Allegro took the correct steps in taking back the computers that they issued Patel, the company was not careful enough to make sure it was the correct laptop and that Patel was completely out of the system. “Patel gave back one of the original laptops, and another unissued laptop, after completely wiping the hard drive.” (Thomas). Patel had full intentions on getting back at the company that he fired and did it very successfully. Allegro claims that the cost for the meddling that Patel did was going to be $100,000. The steps that they should have taken was they first should have made sure both computers that they had originally given him were accounted for. Also if they had any suspicion for retaliation, they should have changed some passwords for their network or for important information. Overall, by forgetting or just not taking the steps needed to make sure the employee leaving a company does not have any access to their data can be a huge part of keeping the company safe. Even with the technology we have today and how often cyber attacks happen, former employees are the most threatening if they have the information in their hands.

Works Cited

Vacca, John R. *Computer and Information Security Handbook*. Vol. 2nd ed, Morgan Kaufmann, 2013. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=nlebk&AN=485997&site=eds-live.

Thomson, Iain. “Sysadmin 'Trashed Old Bosses' Oracle Database with Ticking Logic Bomb'.” • The Register, The Register, 15 Apr. 2017, [www.theregister.co.uk/2017/04/14/sysadmin\_crash\_former\_employers\_oracle\_db/](http://www.theregister.co.uk/2017/04/14/sysadmin_crash_former_employers_oracle_db/).

Mehan, Julie E. *Insider Threat : A Guide to Understanding, Detecting, and Defending Against the Enemy From Within*. ITGP, 2016. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=nlebk&AN=1437066&site=eds-live.

“Magnetic Speed Sensors.” *Magnetic Speed Sensors | Allegro MicroSystems*, [www.allegromicro.com/en/products/sense/magnetic-speed](http://www.allegromicro.com/en/products/sense/magnetic-speed).

Rayome, Alison DeNisco. “Why Ex-Employees May Be Your Company's Biggest Cyberthreat.” *TechRepublic*, TechRepublic, 2 Aug. 2017, www.techrepublic.com/article/why-ex-employees-may-be-your-companys-biggest-cyberthreat/.