Email leaks investigation

Technology, Information Technology

As the Chief Information Technology Administrator for XYZ Company, my senior vice president called me into his office this morning for a confidential meeting. He has been concerned for some time that his emails sent from his office computer have been leaked to unauthorized individuals, both inside and outside of the company. For instance, XYZ has been contemplating purchasing the struggling ABC, a competing company with similar products. When the vice president emailed the Chief concerning possible stock prices for the takeover bid, it seemed the leadership at ABC knew about it as early as the next day, even though it was an internal XYZ email. Therefore the VP asked me to investigate as to where the attacks were coming from. The following is the plan for my investigation. XYZ uses Exchange 2010 and Microsoft (MS) Outlook. Additional security for the PC's is provided by the use of smart card technology. E-mail also uses Secure Multipurpose Internet Mail Extensions (S/MIME) so that confidential letters such as the example above are automatically encrypted. On their website for Exchange, MS says S/MIME " help control access to data and ensure trusted communications both inside and outside the network" (2012). Knowing that the vast majority of security leaks are internal I asked the VP point blank if there could possibly be anybody inside the company that could possibly have his credentials, such as a secretary or trusted assistant. He assured me that was absolutely not the case, as he had come there from the Defense Department. His supervisor there was having an affair with an employee. Having gained access to the woman's computer, the employee sold top secret information to a friendly nation. They both went to jail and since then the VP took great pains to ensure his technical equipment was secure. Through confidential investigation, I was able to determine neither the CFO nor her staff was the culprit either. Therefore the leaks had to come from some sort of attack on the system. The emails had to have been intercepted somehow and I set out to find out how that was possible. Anybody can be hacked and hit with service interruptions and it is not a reflection on any one employee. All one has to do is ask the myriad of companies that have lost credit card and personal data of their customers. The Department of Veterans’ Affairs had an infamous incident a few years ago where they misplaced the personal data of thousands of vets. The hacker group Anonymous launched a cyber attack against Texas police in 2011 in “ retaliation for the arrests” of several members and many hundreds of such things as passwords, SSN, and dates of birth were stolen (2011). For some time, at my suggestion, the company has employed Websense and we currently use its version 7. 7. It is a data security program that attempts to interrupt any threats and attacks and destroy them. Yet any IT person will tell you no system is completely foolproof and even Websense only claims to be 99. 999% effective. Yet the software has a tool that will be invaluable to me in my inquiry. Its Exchange Discovery Wizard (EDW) will allow one to institute a policy to scan the Exchange servers for threats and attacks. EDW can even be set to crawl through individual mailboxes and the nice thing about it is the time of the scan can be set to maximize privacy and minimize time spent in the search. I plan to do exactly that for the mailboxes of both the VP and CFO. With the time and date stamp of the letter in question and matching the email in both boxes, Websense should then be able to issue a detailed report and I will be able to work from there (2012). There is another distinct possibility for the email leaks. Our company’s leadership has embraced smart phone technology and the executives have grown quite used to being in constant contact. Their email has been mapped to the phones. MacAfee cyber security specialists have been tracking the Chinese for technology espionage and have identified 72 government and corporate sites that have targeted for attack by agents of that country. Especially vulnerable are the Google Android operating systems which our company’s phones unfortunately employ (2012). If the Websense investigative report entails the email was either sent or received from a mobile device, I will ask permission from the VP to examine both phones for security leaks and attacks. There is a new company called CrowdStrike powered by former MacAfee investigators which specializes in such things and with their help I should be able to determine if a threat exists and neutralize it. References: Microsoft Exchange, 2012, Advanced Email Security, viewed October 14, 2012, Poeter, Damon, 2011, PC World, Anonymous Hack of Texas Police Contains Huge Amount of Private Data, viewed October 14, 2012, . Websense, 2012, Performing Exchange Discovery, viewed October 14, 2012, Dilanian, Ken, 2012, Los Angeles Times, Smartphone security gap exposes location, texts, email, expert says, viewed October 14, 2012,