Nine Ways That Companies Are Getting Hacked

by Christopher B. Hopkins

The conventional wisdom regarding data breach and identity theft is that it is not if you will be hacked but *when*. Recent breaches such as Ashley Madison, OPM, Michaels, and Target have led to over 100 million people with potentially compromised credit card and personal information. How is this happening?

Many law firms are jumping on the cyber security bandwagon as they proclaim experience assisting with data breach management. But few lawyers understand how these hacks are being accomplished. Even if you and your client rely on competent IT professionals (as you should), it is important to possess a survey knowledge of how hacks and data breaches occur. This article provides a brief introduction to intrusion and disruption techniques.

Physical Access: You can probably name a few infamous hackers such as Snowden, Manning, and Anonymous. But what is the name of the cleaning service company which enters your office every night? Hacking is not just virtual. Physical access – where a hacker gets direct access to your computer – remains the most convenient way to steal data. These are often "inside jobs." This includes installing keyloggers (devices which record your keystrokes) which function like credit card skimmers on ATMs and gas pumps.

Brute Force: In the 1983 thriller WarGames, young Matthew Broderick sets up his modem to dial every phone number in Sunnyvale, California hoping to find a way to access a game developer's system. Instead, he hits upon WOPAR, a government supercomputer. Broderick's dauntless "war dialing" is a form of brute force attack where a hacker repeatedly tries combinations to hack passwords or otherwise obtain access to an account.

Reverse Brute Force: Instead of testing a number of passwords on one account, "reverse" brute force involves testing one or just a few passwords across multiple accounts. In the wake of large hacks, long lists of widely used passwords are available online. A hacker who tries "123456" or "password" against several hundred usernames is bound to get lucky.

Social Engineering: Sometimes it does not always require coding skills to fool people into revealing information. Aside from posing as a government officer or company representative, hackers can even use social media to befriend and interact with people who might be easily fooled into disclosing information. One barebones example of social engineering revolves around testing spouse and pet names from a Facebook profile as that person's password.

SQL Injection: Here, hackers gain access to a vulnerable site by sending queries with special characters (e.g., a single quote) to the target website. That extra character causes confusion and the website sends back an error code in a database language called SQL (pronounced "sequel" or alternatively S-Q-L). By re-sending the special character and then a string of code, hackers can learn which databases exist behind the website. After that, they can again send the special character as well as an SQL command to "list tables." From there, a script can be set up to extract data from all revealed databases. Frighteningly, this can all be accomplished from the username and password screen. Recent examples reportedly include 7-11, Sony, and Johns Hopkins.

Malware / worms: Malware is a secret code which a user unknowingly downloads and installs which, in turn, begins spying or causing damage. Malware can be as simple as code which quietly runs a script after a user clicks a link or it can be more widespread, such as when malware is furtively "baked" into commercial software. Recent examples reportedly include Staples, Sony (recall the film, The Interview) and the Stuxnet attack which plagued nuclear reactors in Iran.

Phishing: A hacker may fool users into thinking that a fake website is real so that the hacker can steal usernames, passwords, and other information. The unwitting user typically hits a link upon receiving an email which insists that "you must change your password." This tricks the person into interacting with a fake version of a bank, social media, or shopping website. The fake website may also inject malware which further exploits the user's mistake. The "celeb-gate" incident in 2014, where nude celebrity cell phone images were spread across the internet, was caused by a widespread phishing scam.

Distributed Denial of Service: If you try to log into an account several times, at some point, the system will lock you out. Imagine now that hackers bombard a website with thousands of login attempts which intentionally fail and, at some point, overload the website which prevents everyone from access. That is a denial of service attack. Hackers then use multiple IP addresses to avoid being blocked (that's the "distributed" part of the hack). At a higher level, more sophisticated attacks can coax the beleaguered website to cough up data.

Backdoors: A backdoor is a means of bypassing a system's main security requirements through a hidden entrance which typically exists for troubleshooting. It is typically created by the software developer or the professional who set up the security features. According to the Snowden disclosures, federal (NIST) encryption standards had a backdoor which permitted law enforcement access to encrypted content. Recent examples reportedly include the OPM, TrendMicro, and RSA.

Christopher B. Hopkins is a member with McDonald Hopkins LLC. If you would like to play a game of chess or global thermonuclear war, plug in your 300 baud modem and send an email to chopkins@mcdonaldhopkins.com.