CASE STUDY: EXTERNAL ATTACK AND PENETRATION TESTING

Situation

Financial institutions have always been a prime target for malicious hackers because of the immediate potential for profit. Beyond actually transferring funds away, hackers can exploit the wealth of personally identifiable information found in a bank or credit union by selling the data or using it for identity theft. According to the July 2016 Beazley Breach Insights report, banks and credit unions with less than $35 million in annual revenue accounted for 81 percent of all hacking breaches in 2016, up from 51 percent in 2015. RSM recently performed penetration tests for a small credit union as part of the credit union's annual security program. The goal: Gain an accurate picture of the credit union's current state.

Solution

The external penetration test began with a quick kickoff and a brief outline of potential targets accessible from the internet. As with most smaller organizations, the credit union's digital footprint was limited to a few critical systems, including their website, email portal and internal login page. This limitation opened opportunities for an attacker. First, a smaller network means that there is likely only one information technology (IT) administrator on-site. While larger companies often segment networks to prevent the wide access of digital resources, smaller businesses usually have a flat-styled network in which the IT administrator has full access to all machines and servers. If that administrator's account is compromised, an attacker gains unlimited access to the entire company. Secondly, a smaller external web presence means hackers have a more difficult time finding vulnerabilities since there are fewer systems to track and test. Most issues in larger networks come from out-of-date and forgotten systems or devices that are still visible to the open internet. Low-profile organizations will naturally not have as many of these targets, so attackers typically utilize a different technique to gain a foothold in the internal network: social engineering.

Once a network appears to be locked down technically, an attacker will often resort to the social element to gain a foothold. Phishing is a common technique which relies primarily on human error to execute successfully. While most people associate phishing with generic Nigerian prince scams, these
attacks have evolved to become more targeted and clever. As part of testing the external presence of this client from the point of view of an attacker, RSM performed a phishing assessment using our in–house custom tool, King Phisher.

To create a convincing and enticing premise, RSM first consulted public documents, press releases and social media pages. Upon analysis of these sources, we identified the full names and usernames of approximately 30 employees. We pared this list down to include only workers who would most likely have access to critical systems, such as teller workstations or ATMs. With the targets identified, we only needed to find a way to create an email that guaranteed a user response. The inspiration for our premise came from another publicly accessible place: social media.

In this case, the small credit union was holding a monthly raffle as part of their marketing efforts. On Facebook, the company posted pictures of the monthly winners with their themed baskets. Since the timing of this assessment coincided with the Independence Day holiday, it made for a perfectly believable setting for a regular email from their newsletter email address. The second key to the email came from the credit union’s marketing page, since any user could sign up for their internal newsletter using their email marketing service. This newsletter came from a valid domain email and contained the full stationery and signature template that was used internally. By simply consulting open–source information, an attacker could gain insight into the internal culture and contests, and deduce a list of employees, the proper username schema (e.g., Jsmith) and valid signature templating.

Armed with this information, we created a malicious Excel document to send to these targeted employees. This document was crafted to look like a raffle ticket generated for a fictitious upcoming Independence Day raffle. The email was sent with the full internal stationery and was spoofed to appear as if it came from the newsletter email address. Once a person downloaded this document and enabled macros, a payload would be launched to connect back to RSM with the privileges of a logged in user.

Within minutes of sending out the email, several connections from different users were made, indicating that the document was successfully opened. Interestingly, some of the users were not part of the original target list, which indicated that the email was forwarded to other employees. Had this not been a simulated attack, the consequences would have been financially devastating. Two of the machines compromised were teller workstations with full access to the credit union’s entire customer database, which included information like names, Social Security numbers, addresses, balances and credit history. An attacker would have been able to silently watch the screen and stealthily capture keystrokes for as long as he desired. While we were unable to directly compromise an administrator account in the short time frame, a malicious actor with enough time and resources could have easily sat undetected for weeks or even months, harvesting data and siphoning funds in the background.

Results

As a result of our testing, RSM made tactical and strategic recommendations from the acquired data. On the tactical side, we advised the client to remove all metadata on files before making them publicly available and disallowing the spidering of sensitive directories. Next, we recommended implementing a finely tuned email filtering solution and properly configured firewall to block future phishing attacks. Finally, we suggested restricting employees’ email and internet access on the workstations used to access client information in order to safeguard customer information.

Based on this tactical information, we then developed a long–term strategic plan to prevent incidents like this in the future. For example, an effective security awareness program would help educate users and minimize the risk from phishing attacks. Second, this credit union had no incident response program in place to detect breaches and prevent them from spreading further. A proper system to detect, report and recover from an attack would greatly help to contain these threats. Finally, a vulnerability management program would help to rectify the issue of outdated software on the internal network and would proactively limit future exploitation.

As ideal targets for hackers, small credit unions need to be proactive about their security. Rather than relying on automated data to make security decisions, a penetration test helps piece together vulnerabilities that a hacker would detect. As demonstrated above, a hacker just needs one small foothold to cause great harm. While annual tests help to pinpoint these weak spots, many high–profile institutions conduct assessments more frequently due to the fast–moving nature of technology. RSM offers these testing services and can also help develop specific strategic security programs customized to individual needs.

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed. RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International. RSM® and the RSM logo are registered trademarks of RSM International Association. The power of being understood® is a registered trademark of RSM US LLP.