LARGE DATA BREACHES CAUSE INCREASED SOCIAL ENGINEERING ATTACKS

ENTERPRISE INTEGRATION

WHO IS THIS CASE STUDY ABOUT?

Enterprise Integration (EI) conducted a case study starting in 2016 on a business that fell prey to an attack based on information provided through social engineering. As an update to that research, EI has investigated another attack which is partially similar in nature but significantly more sophisticate. The term social engineering means that rather than attacking your systems directly, hackers use psychology and publicly available information to manipulate the people operating those systems to gain entry into your organization and access to your data. The results of our study demonstrate that social engineering continues to be an effective tool used by hackers to commit corporate fraud. Furthermore, as a result of the massive data breaches of 2017 like Equifax and Yahoo!, hackers have more sensitive data available to them than ever. Once obtained, hackers search the data for personal information that can be used to plan or execute a social engineering attack against their targets.

HACKERS
WERE ABLE TO
OBTAIN ENTRY
INTO THE CLIENT'S SYSTEM
3 OUT OF 7 TIMES

WHAT IS YOUR MOTHER'S MAIDEN NAME?

WHICH OF THE FOLLOWING 3 CITIES DID YOU RESIDE IN DECEMBER 2005?

EXECUTIVE SUMMARY

We believe that there is a strong correlation between availability of personal information due to large data breaches (e.g. answers to personal questions like 'What is your mother's maiden name?' and 'Which of the following 3 cities did you reside in December 2005?') and the ability of hackers to answer questions regarding a victim's personal details asked by a call center agent or in an online form. Widespread availability of such personal details obtained through large corporate security breaches coupled with social media provides a perfect base from which to research a potential victim. That collective information is then utilized along with any user login credentials which may have been harvested via other means or obtained by conducting dictionary attacks (high-speed automated password guessing) to gain access to a system. In this particular case study, the hackers were able to obtain entry into the client's system 3 out of 7 times.

CHALLENGES

PHISHING

VISHING

IMPERSONATION

"The three most common exploits are: phishing or sending email that seems to be from a reputable source; vishing (or voice phishing) over the telephone; and impersonation, where an individual pretends to be another person to gain access to people or systems in an organization."

Prior to an attack, the hackers pose as high-level managers and use proprietary information obtained through compromised information or through social engineering to access then gain the trust of employees. Reconnaissance is then carried out for days or weeks using one or more social engineering attacks. The three most common exploits are: phishing or sending email that seems to be from a reputable source; vishing (or voice phishing) over the telephone; and impersonation, where an individual pretends to be another person to gain access to people or systems in an organization. Using information obtained through these means allows a hacker to execute highly sophisticated attacks. Because they have studied behavior patterns, reviewed standard procedures, and looked for patterns when information is exchanged with internal colleagues, 3rd parties and vendors within a victim's email system and social media platforms these attacks are much more likely to succeed.

ENTERPRISE INTEGRATION'S STRATEGY

In a recent case investigated by Enterprise Integration, **40% of the attacks using information from a large corporate breach on a single company were successful**. The attackers used strong social engineering techniques and non-technical means to scam the company. In this instance, the attack was implemented in two distinct phases – Reconnaissance and Execution of Attack.

During analysis of the Reconnaissance phase, Enterprise Integration determined that the scammers used multiple sources of information to acquire personal details about a list of targeted individuals.

In reviewing details of the Execution of Attack phase, it was determined that information used by hackers posing as customers of the business and were able to authenticate themselves by accurately answering questions asked by call center agents. After successfully being authenticated, the hackers were able to take actions causing significant financial damage to the real account holders.

Given the widespread availability of compromised information, the threat landscape has significantly evolved. It is more critical than ever for companies to enforce information security policies, follow established processes and procedures (e.g. regularly update security questions) and implement multi-factor authentication (MFA). For companies dealing with health or financial information, if possible, MFA should include biometrics as part of authentication. For processes involving transfers of money internally within a company or externally with 3rd parties or vendors, a multi-stage out of band, or OOB, approval process should be implemented where a voice or in-person approval is required after an electronic request is made.

The frequency of socially engineered attacks has increased significantly compared to what we observed in previous years. Enterprise Integration has worked alongside legal authorities and companies recovering from the aftermath of these attacks. **As part of remediation, Enterprise Integration has helped businesses implement cyber security controls and frameworks and document comprehensive policies to mitigate further incidents.**

RESULTS

Since obtaining the initial case study results, humans have remained the weakest link within any organization when it comes to allowing hackers into your systems – largely since they can fall prey to electronic and non-electronic methods of exploitation. Thanks to the numerous recent corporate data breaches, hackers have the distinct advantage of knowing exactly who to contact, what information to share and how to manipulate the information gate keepers (administrative assistants, help desk, software support, etc.) in order to gain access into the system. With all the personal data available through large corporate breaches and social media, Enterprise Integration wants to give their clients a list of best practices.

1. Implement strong cyber security controls – using all, or only applicable portions, of the National Institute of Standards and Technology (NIST) 800-171 Cybersecurity Framework (CSF) standards
2. Provide Security Awareness Training to employees
3. Review what is shared publicly: website, newsletters, mass emails, social media as well as any files shared internally
4. Limit corporate access to social media for general users
5. Utilize an automated system to keep operating systems and other software patched and updated and install antivirus/anti-malware
6. Remove local administrative rights from general users
7. Build an OOB verification procedure for any process dealing with transfer of funds, intellectual property or any other valuable items via phone
8. Develop an incident response process and keep an updated list of local and government contacts in the incident response documentation
9. Conduct routine Physical and Technical Vulnerability Assessments, especially social engineering tests
10. Practice good password management as stated in the NIST 800-171 guidelines

SECOPS

ENTERPRISE INTEGRATION CAN HELP

The Enterprise Integration (EI) Security Operations (SecOps) team provides customized security solutions to reduce the overall risk and minimize threats. This team of certified professionals ensures that hardware and information business assets are fully protected by developing and executing a security strategy. EI SecOps combines experience with innovation and automation and provides monitoring, prioritized alerts, incident management and customized reporting 24/7/365.

SDI™ SERVICE DELIVERY INTELLIGENCE

Integrations' Service Delivery IntelligenceTM (SDI) companies can discover, map, and visualize all core components and know the health of the total business technology supply chain.

The Digital Robotics Engine (DRE) is another solution from Enterprise Integration that provides enterprise monitoring, alert management, event correlation and aggregation, a real-time capture and normalization of system logs, and utilizes load balancing for scalability and performance.

If you need help with any of the above, contact Enterprise Integration Information Security at 904-928-8137.