Frequent tests of your digital infrastructure can destroy a hacker’s plan of attack

By Jeffrey Bernstein

The term “kill chain” was first coined by the military. It refers to an attack structure whereby an aggressor identifies a target, deploys its forces and destroys it. Conversely, the idea of “breaking” an enemy’s kill chain is a method of defense or preemptive action. In this digital age, this concept has been applied to cybersecurity. The goal is to foil the hackers’ kill chain before any damage is done.

Commercial mortgage lending is constantly exposed to cybercrime, hackers and digital-system compromise. More than ever, your borrowers’ confidence and brand reputation are on the line. Mortgage lenders and brokers, however, often fail to identify their exposures, ignoring the risks or believing there is no way to meet the attack.

It is true that the threat is constantly there. Almost every aspect of doing business as a mortgage lender or broker relies on technology. As that dependency increases, so do security exposures.

Consider some of the more common problems. Software frequently lacks the most recent updates; web and mobile applications are often riddled with coding flaws; and devices are not always physically secured. A company’s employees often get baited by phishing content in e-mails and links that are intended to trick the user into revealing unauthorized information to the attacker.

Devastating attacks

Predictably, 2019 saw another destructive wave of cyberattacks on financial-services companies. In January of last year, TechCrunch reported that more than 24 million financial documents from major banks were exposed in a server security lapse. The server contained more than a decade of data on loan and mortgage agreements, repayment schedules, and other highly sensitive financial and tax documents. Unfortunately, the exposed database wasn’t password protected, allowing anyone with an internet connection to read the extensive collection of documents and data.

The breach involved mortgages originated by Wells Fargo, a unit of Citigroup, Capital One, HSBC Life Insurance and other companies, according to The Washington Post. The loans had been acquired by Texas-based Rocktop Partners. Its affiliate, Ascension Data & Analytics, converted the paper files into a digital format. Ascension’s vendor, OpticsML, a document-management company, allegedly made a “server configuration error” that led to the exposure of the documents, according to TechCrunch.

That breach, which was hardly unique, demonstrates several problems with data security that persist to this day. First, commercial and residential mortgages involve multiple parties. The overall security is only as good as the weakest link in the chain. Second, many companies not only collect more information than they may need, but they often retain this data in accessible online databases for longer than they need — and often in an unencrypted manner. This mistake alone can be the difference between a data breach that affects hundreds of customers and one that impacts millions.

Another massive compromise occurred in May 2019. First American Financial Corp., a Fortune 500 real estate title-insurance company, exposed about 885 million sensitive digital records dating back to 2003. The leak was caused by an application-security flaw on its website, exposing Social Security numbers, bank-account numbers and statements, tax and mortgage records, wire-transaction receipts, and driver’s license images. The data was not password protected and was viewable to anyone with an internet connection and web browser.

This past July, Capital One announced that a hacker exploited a “configuration vulnerability” to steal sensitive records from credit-card customers held in an Amazon Web Services database, the cloud-hosting company that Capital One was using. The breach exposed information about 106 million U.S. and Canadian citizens. This case provides another lesson to financial-services companies that store data in the cloud: Just because you are using a cloud-based service does not mean that your records are secure. Cloud providers typically provide an opportunity to secure data, but there is no guarantee of security.

Prevention methods

These three massive breaches in 2019 all have one fact in common: each were preventable. Effective cybersecurity vulnerability assessments and penetration testing would have exposed the vulnerabilities before the damage was done.

Frequent tests of your digital infrastructure can destroy a hacker’s plan of attack

By Jeffrey Bernstein

The cyber kill chain is a series of steps that trace the stages of a cyberattack, from the early reconnaissance stages through the theft of the data. The kill chain helps to understand and combat ransomware, security breaches and advanced persistent attacks. Lockheed Martin derived the kill-chain framework from a military model. This system has evolved to better anticipate and identify insider threats, social engineering, advanced ransomware and innovative cyberattacks.

Source: Varonis

Jeffrey Bernstein is the managing director of cybersecurity advisory services for Marcum Technology LLC. He advises clients in highly regulated industries on the protection of their networks, applications, systems, data, devices, people and property. Marcum Technology LLC is based in New York and a member of the Marcum Group, one of the largest independent public accounting and advisory services firms in the nation, with offices in major business markets throughout the U.S. and select locations overseas. Reach Bernstein at jeffrey.bernstein@marcumllp.com and follow him on Twitter @Jeff_Bernstein.
A security-vulnerability assessment finds weaknesses in computing networks, applications, servers, devices and any other networked systems running over the internet. A security-penetration test attempts to find any gaps in security via testing, including running simulations of cyberattacks that can expose vulnerabilities to attackers.

Most security breaches involve some form of human error. Companies need to test and train their staff to recognize the tricks used to lure them into inadvertently exposing the company to an attack, such as being baited via an e-mail attachment or a web link to provide unauthorized information. A company and its valuable data is only as strong as any single individual that has access to the data.

The security tests are performed from two perspectives. The first is known as zero-knowledge testing. The security consultant is provided with little to no knowledge about the networks and systems in question. This method provides a realistic view of how a malicious outsider would hack the company’s systems. The second method is targeted testing. Under this approach, the security consultant will test specific systems armed with IP addresses, authorized credentials and so on.

Testing should be done frequently. Any single security test is a simply a snapshot in time and won’t stay current with new and evolving threats. Many companies find that testing monthly or quarterly allows them to keep up with the latest hacker attack strategies.

Typical mortgage transactions also involve multiple business partners that share and manage sensitive information about your borrowers. Lenders should require their title companies, insurers and appraisers, among other third-party partners, to perform similar security tests.

Because of the time-sensitive nature of mortgage financing, the industry is vulnerable to other forms of cyberattacks, including denial-of-service, ransomware or CryptoLocker attacks. Unlike schemes designed to steal data, these attacks will prevent access to data, often at critical times. A comprehensive security-management program — which includes penetration testing as well as anti-phishing tools and training — can mitigate the impact of these attacks and make them less damaging.

The Federal Financial Institutions Examination Council has developed a worthwhile assessment process for financial-services companies to measure their cybersecurity preparedness over time. The tool is available for free online to mortgage lenders and brokers. Federal and state regulations — such as the Gramm-Leach-Bliley Act, guidance from the Securities and Exchange Commission, and requirements from the New York State Department of Financial Services — also provide a framework for cybersecurity as well as the potential liability for failing to protect consumer data.

Internet technology has made it easier for commercial mortgage brokers and lenders to originate loans, but new technology almost always creates additional security exposures. By performing vulnerability assessments and penetration studies, brokers and lenders can proactively identify and fix many of the deficiencies that can be exploited by attackers. Ultimately, your company can foil the cyber kill chain.