White Paper

WINDOW OF COMPROMISE

Limit damage caused to your cardholder data environment

securityMETRICS®

WINDOW OF COMPROMISE

LIMIT DAMAGE CAUSED TO YOUR CARDHOLDER DATA ENVIRONMENT

CYBER ATTACK PROCESS

The cyber attack process is simple. First, the business has a vulnerability, a flaw or weakness that can be exploited. Second, the attacker exploits the vulnerability and accesses the system. Third, the attacker sets up a way to capture cardholder data. Finally, the attacker exfiltrates the data for illegal use.

When we refer to the window of compromise, it starts from the date an intruder accesses a business network and ends when the breach is contained by some act of security remediation on part of the merchant.

Decreasing the window of compromise time decreases the amount of cardholder data captured and exfiltrated, hopefully avoiding compromise all together.

In recent years data breaches have been highly publicized, especially with so many big brands involved. However, data breaches were by no means limited to the well-publicized large industries. In fact, the Ponemon Institute reported that 43% of all US companies experienced a data breach of some sort in the past year. Based on 2014 data collected by SecurityMetrics Forensic Investigators, the average breached merchant was vulnerable for 618 days. That's a lot of time for attackers to find vulnerabilities and exploit them to their benefit.

Nearly every business in America is going to experience cyber attacks from a variety of sources. Many merchants are vulnerable (meaning there is a system, environment, software, or website weakness that can be exploited by attackers) from the day their environment was set up. In other cases, a merchant becomes vulnerable because they fail to apply a security patch or update, or they make modifications to their systems without also properly updating related security protocols.

On average, it took 470 days from a time the merchant had a vulnerability in their environment, to the time an attacker was able to compromise the system (the beginning of the window of compromise). Attackers were then able to capture cardholder data for an average of 176 days. That is plenty of time for an attacker to damage your brand.

HACKER TRENDS: CARD DATA AGGREGATION

The seemingly high number of days that card data was compromised in 2014 (average 176 days) may be attributed to an aggregation method often employed by card data thieves.

Attackers have been known to aggregate card data from scraping or other tools without using or selling the data for four to six months (after six months, some payment card data begins expiring).

The aggregation method prevents card brands from flagging Common Points of Purchase (CPP, a method used by card brands and banks to identify potential malicious account activity) too early, which would expose the data breach much sooner, thus bringing a quicker end to the card data loss and greatly limiting the use of stolen credit card accounts.

DECREASE YOUR WINDOW OF COMPROMISE

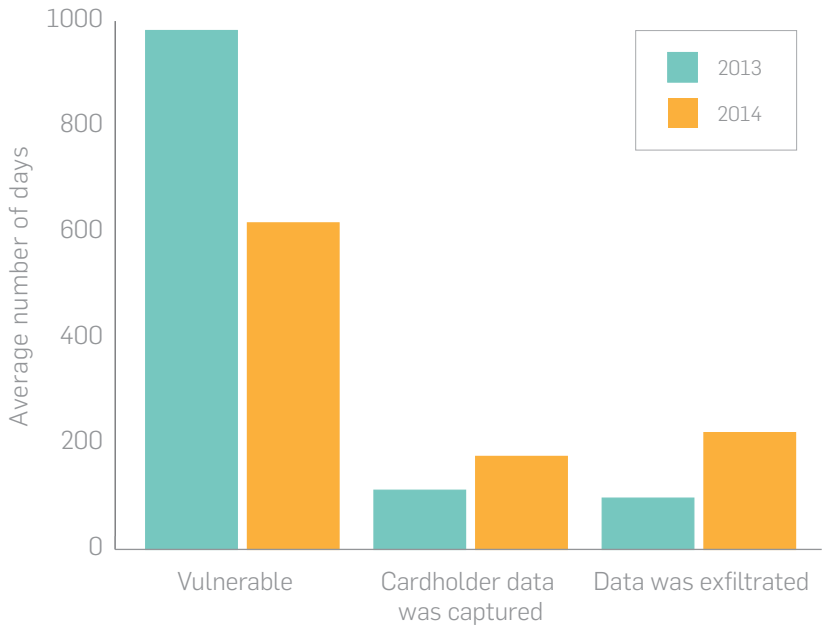
When an environment isn't actively monitored, breaches are more likely to go undetected for longer periods of time. As such, an ounce of protection really is worth more than a pound of cure. The sooner a breach is detected, the less damage an attacker can do to a business. The goal of each business should be to create and practice the necessary procedures to protect against and warn of abnormal behavior in an environment.

LOGGING/AUDIT TRAILS AND SUSPICIOUS ACTIVITY

From a forensic point of view, logs and audit trails are crucial to proving how, or if an organization was compromised. Keeping track of critical actions (e.g., access to files, login attempts, etc.) can help identify key elements of an attack. Logs can track actions to an individual user and can help determine suspicious activity. Assigning unique user identification also helps create an atmosphere of accountability and can help deter internal system abuse.

Once suspicious activity has been defined within an environment, intrusion detection systems (IDS) and intrusion prevention systems (IPS) can be configured to give notification of suspicious activity that might indicate an attack. Change detection programs, like file integrity monitoring (FIM) are especially useful for ecommerce environments because they track the original state of a file and report any changes, such as when an attacker hides malware within an otherwise legitimate file or application.

WINDOW OF COMPROMISE DATA



SECURITY TESTING

The two major types of vulnerability testing that should be performed to reduce the window of compromise are penetration testing and vulnerability scans.

In the case of custom, in-house applications, code testing and independent internal penetration testing can expose many of the weaknesses commonly found in application code (especially the home-grown varieties) and is the best first line of defense in identifying vulnerabilities before the application is put into use. Having code and function tested by objective third parties helps find vulnerabilities that otherwise might have been missed.

Vulnerability scans are automated, affordable, high-level tests that identify certain weaknesses in network structures. Robust vulnerability scans can identify more than 50,000 unique external weaknesses. In addition to locating and reporting vulnerabilities, typical vulnerability scans also encourage a recurring and reliable process for repairing discovered problems. After a scan completes, the need to repair located vulnerabilities goes without saying.

Sadly, in a few instances, SecurityMetrics Forensic Investigators have discovered that the investigated merchant previously knew of the vulnerabilities that led to a breach. However, the merchant did not give sufficient priority to enhancing their IT security by spending the necessary time and money to correct it as soon as the weakness was identified. In the end, the merchant paid for the cost of a mandated forensic investigation, fines from their bank, fees from credit card issuers and card brands, as well as paying to bring their IT security up to par. Their failure to correct the weak link in their system when they first learned of it cost them vastly more than if they had made a proactive correction.

“No matter the advances in security technology and regardless of increased government cyber security initiatives and regulations, attackers are not going to abandon their pursuit for unprotected payment card data.”

–David Ellis, SecurityMetrics Director of Forensic Investigations

SECURITY POLICY AND EMPLOYEE TRAINING

One pitfall, of even the most protected environment, involves the introduction of malicious content by human error. Activities as simple as employee email access or unauthorized Internet browsing can allow paths to and from untrusted networks.

Merchants often inadvertently introduce malware into their systems through email attachments, downloads, or USB drives by simply opening them; unaware of the threat they just allowed into their system. Creating, instructing on, and enforcing a sound security policy is the best way to secure an environment from employee error that could negate the effectiveness of security measures that might already be in place.

RISK-ASSESSMENT AND MANAGEMENT: VULNERABILITY VS. EXPLOITABILITY

Creating a vulnerability management plan is central to decreasing the window of compromise. This process will help identify, classify, remediate, and lessen future instances of vulnerabilities.

However, just because a system is vulnerable does not mean it is exploitable, or even likely to be exploited. Some vulnerabilities may require such a large number of preconditions that the chance of a successful attack occurring is virtually none. Identifying (per the guidelines of PCI DSS Requirement 6) the differing levels of exploitability should help an organization prioritize the actions they will take in enhancing their IT security based on each vulnerability's perceived threat and risk level.

TAKEAWAYS

EARLY DETECTION AND CONTINUAL PROTECTION

Carefully tracking and managing an environment will help with early detection of a breach and has the potential to decrease the window of compromise and thereby mitigate damage caused to your environment. To decrease your window of compromise, make sure to:

- Perform security testing on environments to identify vulnerabilities.
- Develop well-crafted IT security policies to ensure all employees are aware of their responsibilities with respect to the security policy.
- Practice a process to address security vulnerabilities by order of importance.
- Take the time to maintain detailed logs that can be tracked back to individual users to help identify suspicious activity.
- Once you've collected logs, regularly review them and configure IDS/IPS and FIM to help keep watch over your environment.

Remember, if you are actively meeting the Payment Card Industry Data Security Standard requirements you will already be implementing these important security measures.

ABOUT SECURITYMETRICS

SecurityMetrics has tested over one million payment systems for data security and compliance mandates. Its solutions combine innovative technology that streamlines validation with the personal support you need to fully understand compliance requirements. You focus on the business stuff—we've got compliance covered.

For questions about your PCI DSS compliance situation, please contact SecurityMetrics:

CONSULTING@SECURITYMETRICS.COM OR 801.705.5656