Pre- and post-breach risks and ways you can protect your data

Prepared by:
Daimon Geopfert, Partner, RSM US LLP
daimon.geopfert@rsmus.com, +1 312 634 3400
October 2014

Most industries are vulnerable to data attacks and security breaches, but according to recent statistics, the consumer products industry is near the top of the target list. That’s one group where you don’t want to be leading the charge. What are the weaknesses that are allowing attackers to compromise the data of consumer products companies, and just as important, what are some of the missteps organizations are making post-breach that increase the duration and expense of the incident?

Common data breach methods

Client-side attacks
A client-side attack is when an attacker breaches a target system through an indirect method other than exploiting the underlying operating system. In a common version using Web pages, the attacker constructs a website that contains malicious code. The attacker then either waits for someone to randomly encounter the page (a pure target of opportunity) or entices a specific target to visit the page.
This malware had been altered from prior versions so that the system can be compromised if they are running unpatched versions of Web browsers or plug-ins such as Java or Quicktime. Other versions of the attack will embed malicious code into documents such as PDFs, hoping the user will open them with an old, vulnerable version of a reader. Client-side attacks are effective because many organizations struggle with patching nonoperating system software such as Web browsers, Java, Adobe or Quicktime. In addition, users have been taught not to download or run suspicious executables, but visiting a Web page or opening a document is often viewed as a safe activity. A high-profile example would be the breach of RSA, the manufacturer of IT security equipment. Users were sent emails which included a malicious Excel spreadsheet, and within that spreadsheet was an exploit for the Adobe Flash software. When a user opened the document, their system was compromised and then acted as a beachhead for attacks on the rest of the environment.

Custom malware
This attack method uses malicious software (a.k.a. malware) to alter, damage or disable systems. Malware can range from basic *garden variety* versions that were meant to attack home users, to elite versions crafted by skilled technicians who can evade detection for months. Many organizations deal with malware outbreaks, of varying scales, on a monthly basis. The well-publicized Target, UPS and Home Depot breaches are examples of the devastating impact of the power of custom malware. In these cases, after gaining access to the organization, attackers deployed a custom version of malware onto the point of sale (POS) systems. This malware had been altered from prior versions so that they did not match the signatures deployed by anti-virus vendors. This allowed the attackers to remain hidden within the victim environments for months while gathering millions of credit card numbers. In most cases, organizations rely on anti-virus solutions to protect them from such a threat, but in reality, it often takes months for these products to be provided signatures that can find the newest variants of malware.

Social engineering
Social engineering is a fancy name for what really amounts to a traditional con game. While it is a nuanced point, this type of attack compromises the organization via the manipulation of people rather than technology, even though the attack is delivered using mediums such as email and phone calls. The attacker focuses on user habits, mannerisms, human nature, entrenched organizational procedures and activities. The basic model for a targeted campaign consists of:

- An attacker identifying a target. This can be somewhat random or highly selective as they target an industry, company, team within a company or even specific individuals.
- The attackers then interact with the target via email, SMS, phone or other method.
- The attackers convince the targets to perform some action. This can be as simple as clicking a link or resetting a password or as complex as carrying out a full bank transaction.
- Finally, leveraging the results of the action. This could be a direct theft or a full network takeover.

Simply put, this method focuses on getting an authorized user to perform an action in order to bypass standard security controls. For consumer products companies, social engineering attacks range from generic attacks against users to highly targeted campaigns. Recent examples include a campaign targeting the industry which claimed to be from ADP notifying the organization of payroll alerts or problems with ACH transfers.

Web app attacks
There are different variations of Web app attacks, including SQL injection, cross-site scripting, parameter manipulation, and attacks against the Web server software, to name a few. The results can vary from the attacker gaining access to the application, gaining access to the underlying operating system, or even tricking a Web application into providing sensitive data without the attacker having to actually log in to the site. As an example, in a recent security testing engagement involving a large consumer products organization, our ethical hacking teams were able to force a Web application to generate a report that contained all the usernames and password hashes for the application. Using one of those accounts to log in to the application then allowed us to force the application to dump the entire contents of the underlying database which included POS information as well as customer financing data.

Ransomware
These are attacks that do not steal sensitive data, but rather make it unavailable. The current method of choice is to infect a target system, encrypt all the material on that system and force the user to pay a ransom before the attacker will provide the decryption key. These attacks have been targeting all industries indiscriminately, but our digital forensics and incident response (DFIR) teams recently had to execute a response at a consumer products client where a member of their procurement team had his laptop encrypted in addition to all of the network shares that were mounted to his system. This included a share with the majority of the vendor invoice information for the organization. The client was unable to remove the encryption and eventually had to restore the data from backup tapes with a significant amount of lost information.
Post-breach missteps to avoid

So your environment has been compromised. What happens next could include a post-breach containment strategy that helps you ride out the storm and means a brief interruption for your business, or unfortunately, it could also entail a complete failure that ensures chaos for months to come. How do you go about steering the outcome to the more preferable solution?

Security monitoring
The primary issue that needs to be addressed first is any weakness within the security monitoring. It is a logical issue. If you are unable to tell if you’ve been breached, how will you know when to start the response? Comprehensive monitoring for abnormal activity on a system or network is essentially the only method that will allow an organization to identify issues such as compromised credentials or custom malware. Your end-point solutions like anti-virus may not be able to identify a piece of malware, but proper monitoring can alert you to activities such as new processes being started, logs being stopped or cleared, odd command and control traffic, and many other symptoms that will allow you to start your response as early as possible.

Incident response plans
If your organization can detect an issue through comprehensive monitoring, it should have the ability to correct the issue that you’ve found. Many organizations have incident response (IR) plans that boil down to “we’ll get everyone on a conference call and figure it out.” This has not been shown to be an overly effective plan. Organizations must have comprehensive plans for a variety of events, assigned roles and responsibilities, including legal and public relations, and have actively exercised the plans for them to be effective. Not doing so often ends with the organizations entering panic mode during a real incident and either over- or under-responding to the threat.

Third-party management
Many organizations have gone the cost effective route of moving processes, systems and data out to various third parties. However, many have done so without placing contractual controls around how those third parties must act in the case of an incident. In a recent case, our DFIR teams worked with a client that had been breached, and the source of the breach appeared to be within an environment hosted by a third party. When we contacted the hosting provider and asked for access to the client’s materials, we were denied because there was no language in the hosting contract that stipulated the provider had to cooperate in an investigation. By the time law enforcement and lawyers were involved to resolve the situation, critical evidence was lost and the case still remains unresolved.

Most importantly, companies need to know their limits. Understanding the capabilities of your internal resources and maintaining standing relationships with specialty providers is key. Call them early when a breach occurs and stay connected.

For more information about this topic, contact your local RSM representative.