mimecast®
unified email management

Recognizing Five Sources of High-Profile Data Security Breaches

TechTarget® Custom Media

www.mimecast.com

SECURITY ARCHIVING CONTINUITY

Data security is increasingly becoming a bigger problem for organizations of every industry and geography. Security breaches have quickly escalated into a major source of reputational damage, business interruption, erosion of customer confidence and economic loss.

How big has the problem become? The average economic cost to a company that suffered a security breach in 2014 was $3.5 million—a 15% jump compared with the earlier year. High-profile breaches in retail, entertainment, government and other industry sectors are becoming more commonplace; research indicates that 43% of firms had a data breach in the past year. Finally, to make things even more challenging, firms feel their annual security budgets are only about 50% of what they really need to adequately address the problem.[1]

A big challenge for organizations is to understand and overcome the many different sources for security breaches, and to install the right security defenses to address those problems. Of course, IT and security professionals are looking for multilayered solutions that eliminate vulnerability gaps and don't require a number of different point solutions for specific threats, such as endpoint security, email, antivirus and password theft.

It's also important to remember that technology solutions, while essential to solving the problem, often aren't enough. End-user awareness training is a vital part of preventing security breaches by creating an increased level of security awareness through adherence to data governance policies, adoption of security best practices and other steps centered on identifying and eliminating human risks.

One of the few positive byproducts from the increasing number of high-profile security breaches that have taken place recently is to raise awareness of both threats and potential solutions that spot, thwart and remediate security problems. For instance, because of the astonishing impact of credit and debit card theft on global retailer Target, organizations have a clearer understanding of the threat and what to do about it—as well as the potentially catastrophic effect such breaches can have on an organization.

Among the valuable lessons learned from security breaches is an understanding of the different sources of intrusions. While there are many different types of security threats, there are probably five major categories of vulnerabilities that IT and security professionals need to account for in their solutions planning:

1. **Retail system vulnerabilities.** Numerous high-profile security breaches have dominated the headlines in the past few years, including events at global retail leaders such as Target, Home Depot and Staples. Many of those breaches occurred through point-of-sale systems, where a variety of factors compromised customer identities linked to credit and debit cards. In the Staples breach, nearly 1.2 million payment card numbers may have been affected, as well as transaction data including cardholder names, expiration dates and verification codes. Staples also said it suffered breaches caused by point-of-sale malware at most of its U.S.-based stores.[1] A big challenge for retailers has been the changing nature of point of sale, transitioning from traditional cash registers to self-checkout kiosks, mobile device purchases and other formats, as well as the increasing frequency of online retail fraud.

[1] "Ponemon Institute Releases 2014 Cost of Data Breach," Ponemon Institute, May 2014

[2] "Staples data breach update: 1.16 million cards, 1400 stores affected," SearchSecurity.com, December 2014

2. **Email and spear phishing.** The huge growth in the volume and diversity of email has resulted in concurrent increases in email-based vulnerabilities, including spear phishing. As traditional spam and phishing have been addressed by a combination of increased user awareness, IT vigilance and improved solutions, spear phishing (attacks targeted at specific individuals or organizations) has been on the rise.

   Another source for email-based vulnerabilities has been the increased use of email on mobile devices, often carrying advertising-based malware that looks like legitimate email marketing offers. For instance, a faculty physician at the University of California at San Francisco replied to a phishing email and revealed his or her email username and password. As a result, private medical information for about 600 patients was exposed.[3] In other cases, breaches were initiated through email-based approaches from what appeared to be a reliable source. Experts advise organizations to step up their use of improved data governance policies and security best practices by educating end users to think more proactively about security, especially when it comes to clicking on links embedded in emails. Another key step organizations should consider is to check the Domain-based Message Authentication, Reporting & Conformance (DMARC) specification. DMARC enables service providers to segment legitimate email from spoofed email that failed authentication verification.

3. **Trusted insider.** Sometimes, the "trusted insider" approach is so widespread that it transcends multiple systems and points of access, rather than simply being represented by phishing attempts. The most egregious example here was the case of Edward Snowden, the disgruntled government contractor who used his access to highly sensitive and top-secret systems and files at the National Security Agency to reveal government practices on data-gathering practices.

   Political motives aside, Snowden's efforts highlighted how critical it is to ensure that employees—including contract workers and others non-employees with access to proprietary information—are granted only the access privileges to which they are rightfully entitled. Snowden's work not only demonstrated the NSA's apparently lax oversight when it came to access privileges for contractors, but also subjected the NSA specifically and the entire U.S. government to widespread ridicule at home and internationally.

4. **Regin.** This malware has actually been around for a number of years, but its presence was signaled after several high-profile breaches. Security researchers have characterized Regin as an astonishing piece of malware because of its capabilities and the extensive amount of development work that went into it—as well as its ability to remain undetected for so long. Regin infects entire networks, as opposed to other malware that attacks individual computers, and can be used for a variety of purposes such as collecting passwords, retrieving deleted files and monitoring entire networks and infrastructures. The European Union and Belgacom Group—Belgium's partly state-owned service provider—are two of the most prominent victims of Regin, which also has been detected in a wide variety of organizations throughout Europe and Asia.

5. **Social engineering.** Some of the most clever—and most devious—breaches occurred as a result of social engineering. In social engineering, hackers use psychological tactics to gain users' confidence in order to make them divulge proprietary information. Social engineering is believed to have been one of the approaches cyberterrorists used to conduct the recent headline-grabbing theft of Sony Pictures' proprietary email content. While social engineering isn't a new tactic, it's an approach utilized with greater frequency in recent years, in part because technology-based defenses have become more sophisticated to prevent certain breaches. As a result, hackers have increasingly turned to time-honored tactics like flattery and other seemingly innocent ways to build trusted relationships with people—only to have them violate those confidences by using their passwords and privileges.

[3] "Security breach examples and practices to avoid them," University of California at Santa Cruz, April 2014

Considering Your Options: Threat Protection from Mimecast

Protecting your organization's proprietary information and your employees' privacy requires a multi-layered defense against vulnerabilities, especially email-borne threats. As data breaches increase, and as the consequences of those breaches become more damaging, organizations must raise their game when it comes to protecting intellectual property, employee data, customer records and other proprietary information.

Organizations need to look for new solutions that protect their data and their teams against targeted, clever attacks often embedded in inbound email. Mimecast offers a Targeted Threat Protection solution that addresses this challenge. The Mimecast solution provides such capabilities as:

- Rewriting URLs in inbound email in order to scan destination websites in real time for potential risks before the user can open the email.
- Displaying a warning page if the site is identified as unsafe, and denying access to the user.
- Scanning links on every click in order to help ensure that they are safe, and to protect against the risk of a legitimate site being compromised at a future date.

The Mimecast solution protects all devices, from the desktop to the smartphone, without disrupting users' service, and enables rapid service activation through Mimecast's cloud platform. It also provides a single administration interface for comprehensive security monitoring and reporting.

Mimecast also offers a wide variety of security solutions to address potential vulnerabilities, including data leak prevention, email encryption, content controls, journal archiving, large-file send and federated services.

Conclusion

Security threats are becoming more diverse and numerous, putting intense pressure on IT and security professionals to stay ahead of the curve when it comes to spotting new problems, and to respond more rapidly than ever to remediate problems. Failure to do so increases the chances of high-cost, high-profile data breaches that result in tremendous damage to organizations' reputations, finances and overall operations.

The only silver lining from the many headline-grabbing security breaches that have taken place in recent years is heightened awareness of the problem and a commitment to fortify defenses against all forms of threats, particularly email-borne risks, social engineering and simple human error.

Organizations need to combine a commitment to sufficient investment in security tools and services to prevent threats from entering the workplace and to eradicate them quickly if and when they do.

To learn more, visit **Mimecast.com**.

About Mimecast

Mimecast is a leader in enterprise cloud services for the protection and management of email and corporate data. The company's cloud email security, continuity and archiving services are built on Mimecast's world-leading secure cloud platform and optimized for Microsoft Exchange and Office 365. Founded in 2003, the company has over 10,000 customers, and over 3 million users worldwide. Mimecast has offices in Europe, North America, Africa and Australia.