Evolving Data Centers:

Defending Against Data Breach Attacks

Traditional Security in Mixed Environments

Enterprises transform IT structures to include virtualization and cloud computing because they reduce company costs and optimize resource utilization. Adopting these new platforms, however, opens new windows of exposure that attackers may leverage in data breach attacks. Here are some of these mixed environment issues:

- **Outdated agent-based security:** Traditional security doesn't recognize the presence of virtual machines (VMs) in the network and creates these two security issues[1]:
    - **Instant-on gaps:** Dormant VMs with outdated security patches may be exploited when turned on.
    - **Resource contention:** Security scans and patch updates take up a lot of CPU resources, which cause update delays that opens the network to exploits.
- **Communication blind spots:** Traditional network security doesn't have thorough visibility of communications that occur between VMs.
- **Inter-VM attacks and hypervisor compromises:** Threats that affect physical environments such as malware and exploits, may also affect virtual environments since virtual servers run the same OSs and applications as physical servers do.[2] However, security for physical servers doesn't work on virtual servers.

  For example, hypervisor vulnerability "hypercalls" can be used to query CPU activity, manage hard disk partitions, and create virtual interruptions.[3] Hypercall set_debugreg vulnerability (CVE-2012-3494) allowed a malicious guest to

[1] Trend Micro Deep Security. "Agentless Security for VMware Virtual Data Centers and Cloud." Trend Micro. Last updated 2012. Accessed on June 2013 http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_changing-the-game-for-antivirus-vmware.pdf

[2] Irinco, Bernadette. "Looking Beyond the Challenges of Securing Virtual Environments." TrendLabs Security Intelligence Blog. Last updated 06 July 2012. Accessed on June 2013. http://blog.trendmicro.com/trendlabs-security-intelligence/into-the-abyss-of-virtualization-related-threats/

[3] Perez-Botero, Diego; Szefer, Jakub; Lee, Ruby B. "Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers." Princeton University, Princeton. Last updated May 2013. Accessed on June 2013. https://www.princeton.edu/~szefer/papers/scc2013.pdf

cause the host to crash, leading to a denial-of-service (DoS) attack.[4]

- **Mixed trust level VMs:** It becomes difficult to control security when critical applications or data are housed in the public cloud or in other vulnerable VMs.
- **Unprotected web applications:** Web applications created prior to deploying security updates may be exposed once virtualization and cloud platforms are integrated into existing systems.[5]

Addressing emerging problems in evolving IT environments using traditional security is bound to fail because of the inherent differences between physical and mixed environments. Security for physical servers cannot cover the threats that may arise from adopting virtualized and cloud platforms.

96%

of target data are customer records (payment card data, PII, and email addresses).

DATE	BREACHES	COMPROMISED RECORDS
2013 (January - June)	212	4,508,439
2012	447	17,317,184

Table 1. Data breach in the enterprise.[6]

DATE	BREACHES VIA HACKING INCIDENTS
2013 (January - June)	41%

Table 2. Breaches via hacking incidents in the enterprise

[4] Xen Security Advisory 12 (CVE-2012-3494) - hypercall set_debugreg vulnerability. Accessed on June 2013. http://lists.xen.org/archives/html/xen-announce/2012-09/msg00000.html

[5] A TrendLabs Cloud Security Primer. "Web Application Vulnerabilities: How's Your Business on the Web?". Accessed on June 2013. http://www.trendmicro.com/cloud-content/us/pdfs/business/tlp_web_application_vulnerabilities.pdf

[6] http://www.idtheftcenter.org/ITRC%20Breach%20Report%202013.pdf

Growing Sophistication of Data Breach Attacks

Recent sophisticated attacks compound security challenges brought by ongoing structural changes in the enterprise. While there are common elements found in data breach attacks, recent reports show that every security incident is unique and tailored for target organizations. Breaches are complex incidents that call for a multifaceted security approach.[7]

As shown in the table below, attackers use various methods to steal valuable data. Hackers choose a method appropriate for their target networks. The high rate of unknown exploit methods shows that attackers are refining their techniques to elude familiar defenses.

INFILTRATION METHOD	DEVELOPER	SECURITY
SQL injection	42%	46%
Code exploit via Web 2.0 application	29%	24%
Cross-site scripting (XSS)	25%	23%
Privilege escalation	18%	17%
Others (e.g., remote access, session hijacking, authorization flaw, etc.)	5%	8%
Unknown	17%	19%

Table 3. Methods used in data theft.[8]

A deeper understanding of how a data breach attack occurs can help organizations mitigate breaches. Our infographic provides an easy-to-understand explanation of how a hacker enters a network.

[7] Verizon. "The 2013 Data Breach Investigations Report." Accessed on June 2013. http://www.verizonenterprise.com/DBIR/2013/

[8] Adams, Ed; Ponemon, Larry. "2012 Study on Application Security: A Survey on Application Security and Developers." ISACA.org. Accessed on June 2013. http://www.isaca.org/Education/Online-Learning/Documents/Understanding-Your-Organizations-Application-Security-Maturity.pdf

Different Data Breach Attack Methods

There are many ways to carry out a data breach, but here are the top methods used in high-profile attacks:

- **SQL injection** happens when an attacker inserts SQL statements in open, unsanitized entry fields in database servers to execute attacker's goals.

  For instance, the hacker group The D33Ds Company found an SQL injection vulnerability in Yahoo! and exposed 450,000 login credentials.[9]

- **Remote code execution (RCE)** occurs when an attacker runs malicious code on vulnerable servers from another location. The South Carolina breach affected up to 657,000 businesses and exposed 387,000 credit card credentials and 3.6 million social security numbers.[10]

- **Cross site scripting (XSS)** occurs when an attacker sends a malicious link to an unsuspecting user via web applications to gather data. In a recent XSS attack, hackers exploited the XSS vulnerability in Zendesk and compromised Tumblr and Twitter.[11]

[9] Constantin, Lucian. "Hackers Publish Over 450,000 Emails and Passwords Stolen From Yahoo." PCWorld.com. Last updated July 13, 2012. Accessed on June 2013. http://www.pcworld.com/article/259135/hackers_publish_over_450000_emails_and_passwords_allegedly_stolen_from_yahoo.html

[10] Shain, Andrew. "Data security breach expands to 657K SC businesses; suit filed against state" TheState.com. Last updated November 1, 2012. Accessed on June 2013. http://www.thestate.com/2012/11/01/2503354/657000-sc-business-records-also.html

[11] Shu, Catherine. "Zendesk Hacking Affects Tumblr, Pinterest and Twitter Users." TechCrunch.com. Last updated February 21, 2013. Accessed on June 2013. http://techcrunch.com/2013/02/21/zendesk-hacking-affects-tumblr-pinterest-and-twitter-customers/

Integrating Advanced Layers of Protection

Enterprises can't expect traditional security to protect enterprise VMs and cloud platforms the same way it guards physical servers and endpoints. A one-size-fits-all solution cannot provide sufficient protection against complex data breach attacks. Enterprises need a multilayered strategy that has the following advanced layers of protection:

- **Comprehensive monitoring:** Deploy log inspection, file integrity monitoring, and intrusion detection and prevention to identify malicious network activities.
- **Agentless protection:** Integrate advanced anti-malware technology that coordinates agent-based with agentless solutions to provide adaptive security.
- **Encryption:** Automatically encrypt all the files.
- **Virtual patching:** Protect virtual servers from known exploits while waiting for the actual patch to be released and deployed across systems.

These virtualization-aware security elements should be integrated in current enterprise solutions to prevent complex data breaches without cancelling the benefits of virtual and cloud platforms.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud