A **TrendLabs** Security in Context Paper

TREND MICRO™

The Enterprise Fights Back (Part III): Building an Incident Response Team

Risks Enterprise Networks Face

Enterprises and large organizations face a plethora of security threats and are at risk of data breach incidents and targeted attacks. At present, it is no longer a question of "if" but "when" with regard to becoming a threat target. Enterprises can, however, prevent threat actors from penetrating their networks and consequently stealing confidential data or their "crown jewels" by using robust security technologies and implementing security-related procedures.[1]

"An organization can become a target not only for its own products or the information it holds but also because it is somehow connected to an ultimate target."

—Jim Gogolinski
Trend Micro senior threat researcher

A study indicated that the majority of enterprises consider securing data one of their top challenges.[2] Targeted attacks, which are high-risk threats, aim to exfiltrate and transfer stolen data to an undisclosed location that threat actors manage. They remain undetected in target networks for a long period of time and laterally move within in order to gain access to valuable enterprise data such as intellectual property rights, trade secrets, and customer data. To stay protected, enterprises must assume they have been compromised even before their IT administrators detect any malicious activity within their networks.

In our security predictions for 2014, we noted that clickjacking and watering hole attacks will become more prevalent, along with the use of new exploits.[3] Threat actors will likely leverage other points of entry such as mobile devices to infiltrate target networks.

We also believe that one major data breach incident will occur each month. Cybercriminals will find stealing information a steady source of profit while threat actors consider this as a means to instigate espionage and sabotage. Earlier last year, Evernote, an app for organizing videos, images, and so forth also suffered a breach, which allowed attackers access to its database of usernames and passwords.[4]

---

1 Trend Micro Incorporated. (2013). *TrendLabs Security in Context Paper*. "The Enterprise Fights Back (Part I): Securing Your Network Infrastructure Against Targeted Attacks." Last accessed January 15, 2014, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/the-enterprise-fights-back-p01.pdf.

2 Trend Micro Incorporated. (2013). "Keeping Corporate Data Safe." Last accessed January 15, 2014, http://apac.trendmicro.com/apac/enterprise/security-suite-solutions/esdp-suite/infographic/index.html.

3 Trend Micro Incorporated. (2013). "Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond." Last accessed January 15, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf.

4 BBC News Technology. (March 2, 2013). *BBC.CO.UK*. "Evernote Says Security Has Been Breached by Hackers." Last accessed January 15, 2014, http://www.bbc.co.uk/news/technology-21644317.

Establishing Security Controls

Removing all traces of a targeted attack from a corporate network is, however, no guarantee that attackers will not target it again after a period of dormancy. In a previous primer "Securing Your Network Infrastructure Against Targeted Attacks," we tackled how configuring your network infrastructure can aid in proactively combating targeting attacks.[5] In another primer, we recommended that enterprises classify their data in order to better protect it.[6]

While these procedures can incur additional costs, the money enterprises will spend cannot be greater than the potential cost and damage data breaches or any form of network infiltration can cause.

Why Is an Incident Response Team Critical for Enterprises?

Apart from configuring their network and building data protection infrastructure, enterprises should also form an incident response team comprising members with different functions, which will be responsible for detecting and containing ongoing network attacks. A study, for instance, considered incident response and management a critical security control that every enterprise should implement.[7] Not having an incident response team within your enterprise can lead to the following scenarios:

- The IT team may not be able to prioritize the investigation should an incident occur because it is primarily tasked to maintain the enterprise's operations. This can affect the investigation and can delay mitigation, which is detrimental to an enterprise, given that acting fast is crucial when an attack occurs.
- Threat intelligence refers to indicators such as tools and techniques used to tell if an attack is currently occurring. Lack of it would make it arduous for enterprises to probe deeper into how an attack occurred.
- The absence of an incident response team can make it harder for an enterprise to deal with legal and compliance issues should an incident arise. A dedicated incident response team can more properly and quickly address legal and compliance concerns.

---

5 Trend Micro Incorporated. (2013). *TrendLabs Security in Context Paper*. "The Enterprise Fights Back (Part I): Securing Your Network Infrastructure Against Targeted Attacks." Last accessed January 15, 2014, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/the-enterprise-fights-back-p01.pdf.

6 Trend Micro Incorporated. (2013). *TrendLabs Security in Context Paper.* "The Enterprise Fights Back (Part II): Protecting Sensitive Data from Targeted Attacks." Last accessed January 15, 2014, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/the-enterprise-fights-back-p02.pdf.

7 Sans Institute. (2013). *Sans.org.* "Twenty Critical Security Controls for Effective Cyber Defense." Last accessed January 15, 2014, http://www.sans.org/critical-security-controls/.

- Customer notification is also an important aspect of managing security breaches. Improper handling of external communications may further damage an enterprise's image and reputation and even cause it to incur legal or regulatory penalties. Internal communication is, however, also critical with regard to raising awareness within the enterprise.

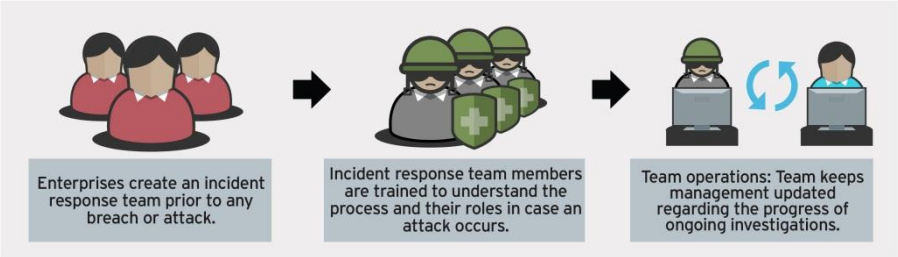

Figure 1: Overview of what an incident response team does

Forming an Incident Response Team

"The overall goal is to quickly detect the problem, analyze all the variables related to the event, adapt, and respond with the appropriate processes and countermeasures to contain the event and mitigate future risks using a similar attack vector no matter where your infrastructure resides."

J.D. Sherry
—Trend Micro vice president for technology and solutions

An incident response team is composed of members with various functions such as technical, threat intelligence, human resources, legal, public relations, and executive management. The roles and responsibilities of this group differ from those of the IT team and should be documented and cascaded to every member. Ideally, its members should undergo sufficient training to ensure fast response time and efficiency should an attack occur.

Enterprises should form an incident response team before a breach or an attack occurs since properly responding to and mitigating an intrusion requires specific skill sets and training. During an attack, the incident response team should keep track of their investigation progress and constantly inform the management team of any update.

Trend Micro vice president for technology and solutions, J.D. Sherry, discussed how next-generation incident response teams should operate and why knowing this is important for enterprises in his webinar, "Next-Generation Incident Response."[8]

Trend Micro senior threat researcher, Jim Gogolinski, on the other hand, provided guidelines and suggestions on how to secure networks in his paper, "Suggestions to Help Companies with the Fight Against Targeted Attacks."[9]

[8] J.D. Sherry. (August 21, 2013). *BrightTALK.* "New-Gen Incident Response: 3 Key Challenges." Last accessed January 27, 2014, https://www.brighttalk.com/webcast/1506/84547.

[9] Jim Gogolinski. (2013). "Suggestions to Help Companies with the Fight Against Targeted Attacks." Last accessed January 27, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-suggestions-to-help-companies-with-the-fight-against-targeted-attacks.pdf.

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