前瞻科技與管理　5卷2期，95-122頁（2015年11月）
Journal of Advanced Technology and Management Vol.5, No.2, 95-122 (November, 2015)
DOI: 10.3966/222014242015110502004

進階持續性威脅之防護與認知初論：根基於黑暗首爾資訊安全事故及其防禦方法

季祥[1,*]　樊國楨[2]　韓宜蓁[3]

[1]趨勢科技股份有限公司客戶技術專案經理
[2]臺灣網站防護協會祕書長
[3]中國文化大學推廣教育部遠距教學中心數位教學規劃師

摘要

2013年3月20日，經由修補（Patch）伺服機之雲端運算服務的取徑，使用擦拭磁碟開機主引導紀錄（Master Boot Record, MBR）之攻擊方法，致使韓國3家廣播電視網與3家銀行金融網及2家保險公司，共超過四萬八千部伺服機、電腦以及提款機無法啟動的資訊安全事故，彰顯防禦「禍起蕭牆之內」的資訊安全威脅之重要性。根基於已納入（資訊）安全內容自動化協定（Security Content Automation Protocol, SCAP）1.2版應用範疇之屬性基存取控制（Attribute Based Access Control, ABAC），自其可信賴計算基底之內部威脅的保護（Trusted Computing Based Insider Threat Protection, TCBITP）之標準化的進程，闡明其實作框架，並經由5個構面、二十九項策略對40位專業人士進行問卷調查，探討我國對此議題認知之差異性，期待能對雲端運算服務面對進階持續性威脅之資訊安全實作提供參考，供相關人士參考。

關鍵詞：主引導紀錄、可信賴計算基底之內部威脅的保護、進階持續性威脅、認知、屬性基存取控制

* 通訊作者：樊國楨
電子郵件：kjf.nctu@gmail.com

前瞻科技與管理　5卷2期，95-122頁（2015年11月）
Journal of Advanced Technology and Management Vol.5, No.2, 95-122 (November, 2015)

Preliminary Study on Protection and Awareness of Advanced Persistent Threats: Based on Dark Seoul Information Security Incidents and Defensive Approach

Hsiang Chi[1], Kwo-Jean Farn[2,*], and I-Chen Han[3]
[1]Technical Account Manager, Trend Micro Incorporated
[2]Secretary General, Taiwan Internet Protection Association
[3]e-Instructional Planner, School of Continuing Education, Chinese Culture University

Abstract

March 20, 2013, via the approach of patching cloud computing services of the servo, through the attack method of wiping the disk boot master boot record (MBR), it caused that more than 48,000 servos, computers and cash machines of three broadcast networks, three banking and financial networks and two insurance companies in South Korea could not work. This information security incident highlights the relevance in defense of the information security insider threats. Based on the Attribute Based Access Control (ABAC), which has been already included in the applications within the scope of version 1.2 of the (information) Security Content Automation Protocol (SCAP), the standardization process of the Trusted Computing Based Insider Threat Protection (TCBITP) clarified its implementation framework; and via 5 dimensions and 29 strategies, a questionnaire survey was conducted on 40 professionals to discuss the differences in cognition of this topic, hoping for providing a reference for the implementation of cloud computing services face of advanced continuity information security threats for the persons concerned.

Keywords: master boot record, trusted computing based insider threat protection, advanced persistent threat, awareness, attribute based access control

* Corresponding Author: Jewel Chen
E-mail: cyc7986@gmail.com