資訊技術服務中心

114年度資安攻防演練說明會

114年5月22日

大綱

1. 演練概述
2. 單位配合事項說明

演練概述

1

背景說明

依教育部4月來文「教育部114年度國私立大專院校資安攻防演練計畫」，教育部為落實資通安全管理法、資通安全事件通報及應變辦法之規定。規劃每年對**教育體系國立大專院校**及**私立大專院校**實施資安攻防演練，以**了解演練單位遭受資安攻擊時其內外部防護與通報應變實施情形**。

- 強化大專院校資安防護工作之完整性及有效性
- 增進發生資安事件時之緊急應變、系統復原及協調管控等能力
- 檢討防護改善降低資安風險

實施對象與範圍

實施對象

- 全國國立大專院校（**含本校**）及部分私立大專院校

作業時程

- 演練作業：114年7月至9月之工作日，共3個月

範圍標的

- 使用本校之**學校校名**、**網域名稱**或**IP位址**，並可**透過外部Internet連線之服務(此次實施範圍主要為：網站、主機)**。

※範圍標的包含**單位網站系統、實驗室網站、教師個人網站、活動網站**。

弱點測試方式

演練方式：

- 教育部檢測團隊將以**白帽駭客身份於外部網路遠端檢測本校之資訊服務**，找出資訊服務存在之弱點，並**通知本校於時限內完成資安事件通報、應變、修補程序**。

資產盤點：

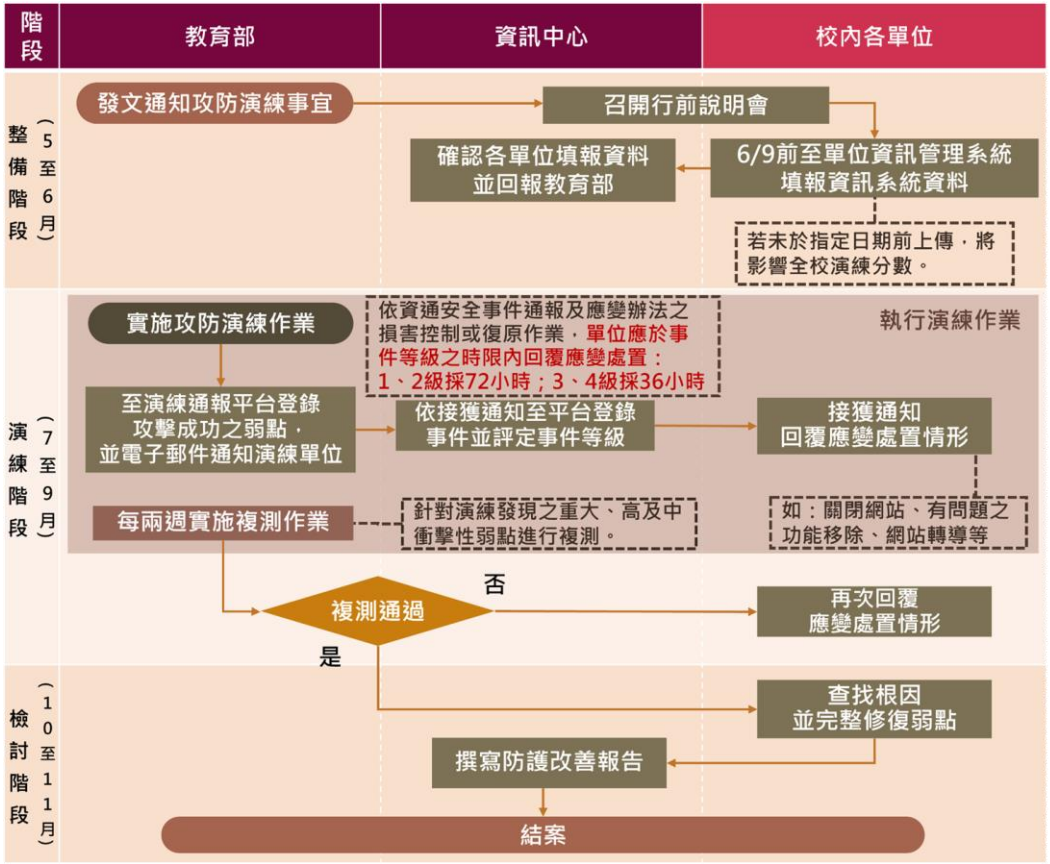
- 教育部要求盤點校內系統網站清冊，以作為演練事前繳交資料。

項次	對外網路位址IP	名稱	防護分級	業務單位	網頁位址 (URL/服務埠)
範例	123.123.123.123; 123.123.123.125-126; 123.123.123.128;	招生系統	中	學務處	https://www.test.edu.tw

單位配合事項說明

2

整體流程


階段
教育部
資訊中心
校內各單位
整備階段（5至6月）
發文通知攻防演練事宜
召開行前說明會
確認各單位填報資料並回報教育部
6/9前至單位資訊管理系統填報資訊系統資料
若未於指定日期前上傳，將影響全校演練分數。
演練階段（7至9月）
實施攻防演練作業
依資通安全事件通報及應變辦法之損害控制或復原作業，單位應於事件等級之時限內回覆應變處置：1、2級採72小時；3、4級採36小時
執行演練作業
至演練通報平台登錄攻擊成功之弱點，並電子郵件通知演練單位
依接獲通知至平台登錄事件並評定事件等級
接獲通知回覆應變處置情形
每兩週實施複測作業
針對演練發現之重大、高及中衝擊性弱點進行複測。
如：關閉網站、有問題之功能移除、網站轉導等
複測通過
否
再次回覆應變處置情形
是
檢討階段（10至11月）
查找根因並完整修復弱點
撰寫防護改善報告
結案

評分方式

總計	類別	項目	評量占比
總成績 (100%)	**1.系統盤點能力(20%)**	調查表正確率	15
		調查表回復時間	5
	2.通報應變作業(20%)	通報登錄時間	10
		應變處置時間	10
	3.防護能力(50%)	各衝擊性弱點數量	50
	4.弱點複測(10%)	複測通過率	10

單位配合事項 - 整備階段(5 - 6月)

1. **資通系統盤點**：請單位資安窗口盤點單位內之符合範圍標的之網站，並**於6/9(一)前，由該系統負責人透過單一入口登入「單位資訊管理系統」，填報資通系統使用情形。**
   - **確認已填之資通系統**：請於「系統清單」確認過去已填之資通系統基本資訊是否為最新資料，確認無誤後點選「系統資訊確認」，並確認所有資通系統皆取得綠色標記。
   - **尚未填寫之資通系統**：請於「新系統建檔」填寫相關資訊與等級（普 / 中 / 高），點選「產生簽核表格」後列印「資通系統安全等級評估表」，**經主管簽核後，將其掃描為電子檔，並電子郵件傳至資訊中心張小姐**(信箱：cxxuan@nycu.edu.tw，分機：#31706)。

單位資訊管理系統 - 系統畫面

- **確認之前填報之資通系統，依照以下步驟，取得綠色標記**

單位資訊管理系統 - 系統畫面

- 尚未填寫之資通系統，請於新系統建檔填完送出後，將產生的評估表印出簽核(管理人及單位主管)，送交資訊中心資安負責人，經審核後受理建檔。

單位配合事項 - 整備階段(5 - 6月)

2. **帳號清查：**
   - 若網站帳號使用弱密碼請更改為強密碼。
   - 長時間不使用之帳號、測試帳號請停用或移除。
3. **弱點掃描：**
   - 在線使用之網站及主機，可至弱點掃描平台(https://va.nycu.edu.tw)進行掃描確認是否無中高風險漏洞。
4. **建議事項：**
   - 若單位內存在**長時間無使用、無維護之網站及主機請於6/9(一)之前關閉(包含：實驗室網站、活動網站)**，避免暴露風險。

單位配合事項 - 演練階段(7 - 9月)

1. **注意網站服務是否正常**
   - 避免演練過程發生非預期狀況，導致系統發生當機或資料異動等情形發生，**建議各單位於演練期間每日備份重要資料**。
   - **每日檢視網站、系統服務有無異常狀況**，並維持網站日常連線狀態及日常防護作業。

單位配合事項 - 演練階段(7 - 9月)

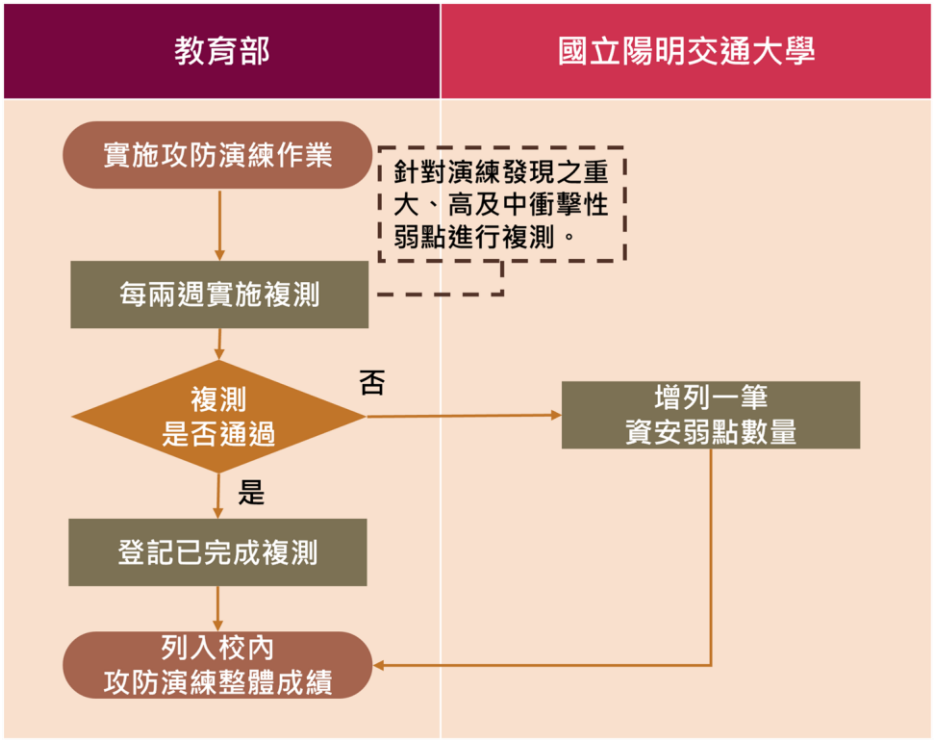
- **若網站被發現有弱點時，請單位配合以下事項：**
  2. **應變處置措施：**
     - 資訊中心於接獲漏洞後，通知單位資訊管理系統上之**單位資安窗口或網站管理員**，**請同仁於指定時間內回覆漏洞應變處置措施 。**
       （**1、2級資安事件：72小時，**
       3、4級資安事件：36小時）
     - **常見應變處置措施**：網站暫時關閉、有問題之功能移除、網站轉導。

資安事件等級評估方式

類別	機密性 (資訊洩漏)		完整性 (資訊/資通系統遭竄改)		可用性 (業務/資通系統運作遭中斷)	
業務性質/資通系統別＼影響程度	洩漏程度		竄改程度		可否於可容忍時間內回復	
	輕微	嚴重	輕微	嚴重	輕微	嚴重
非核心業務	1級	2級	1級	2級	1級	2級
非核心資通系統	-	-	1級	2級	-	-
未涉及CI維運之核心業務	2級	3級	2級	3級	2級	3級
未涉及CI維運之核心資通系統	-	-	2級	3級	2級	3級
涉及CI維運之核心業務	3級	4級	3級	4級	3級	4級
涉及CI維運之核心資通系統	-	-	3級	4級	3級	4級
一般公務機密、敏感資訊	3級	4級	3級	4級	-	-
國家機密	4級	4級	4級	4級	-	-
※國家關鍵基礎設施(Critical Infrastructure, CI)						

單位配合事項 - 演練階段(7 - 9月)

- 教育部將於通知弱點後每兩週進行複測：



單位配合事項 - 檢討階段(10 - 11月)

1. **查找根因：**
   - 針對本次弱點進行深入分析，追蹤問題發生的源頭，釐清導致弱點出現的實際原因，作為後續改善依據。
2. **完整修復漏洞：**
   - 針對發現的弱點，進行具體的修補方案，確保該措施能有效杜絕類似情形再次發生。資訊中心將追蹤修補情形並進行測試與驗證，以確保弱點完成修復。

相關負責人

1. **攻防演練相關問題：**
   - 請洽 廖先生(#52861)
2. **弱點掃描平台相關問題：**
   - 請洽 許先生(#52856)
3. **單位資訊管理系統相關問題：**
   - 請洽 劉先生(#52822)
4. **資訊中心資安窗口：**
   - 請洽 張小姐(#31706)