立碁電子工業股份有限公司

標題： 網路遭入侵應變處理辦法

文件編號: QW0903-MIS-001

製作單位: 資訊 處

撰 寫 者: 許嘉益

核 準 者:楊文全

版　　本: B

生效日期:

製作日期:109.08.12

立碁電子工業股份有限公司網路遭入侵應變處理辦法

一、目的;

隨著網際網路使用人數激增，網路資安問題也日漸嚴重及近年來勒索病毒事件不定時暴發，被入侵破壞者常不知情，並極少曝光。為防止資訊網路破壞者如駭客集團（Hacker）或怪客（Cracker）等非法入侵本公司網路系統，竊取或損毀或竄改網路伺服器之資料連帶造成生產製造的設備及MES系統實施網路保護，特制定此辦法。

二、權責

資訊網路遭入侵時，資訊處成立網路遭入侵緊急應變小組(以下簡稱緊急應變小組)。

1. 資訊處最高主管為緊急應變小組召集人，負責指揮資訊處全體同仁，並隨時將相關情況呈報總經理。
2. 資訊處全體同仁為緊急應變小組成員，負責資安故障排除及呈報災損壞情形。

三、通報程序

1. 資訊處發現資訊網路遭入侵時，呈報資訊處最高主管。
2. 資訊處成立緊急應變小組，由召集人呈報總經理，並通報公司各部門。
3. 緊急應變小組成員依據資訊網路遭入侵應變程序處理。
4. 狀況排除後，由緊急應變小組召集人呈報總經理，並通報各單位。

四、 資訊網路遭入侵應變程序

1. 立即切斷電腦、網路伺服器之連線，並記錄遭入侵之相關資料。
2. 還原電腦網路伺服器之軟體及資料。
3. 追查電腦網路駭客之入侵方式，檢查網路安全系統漏洞，提昇系統安全，更新修補程式.以防堵電腦網路駭客再次以相同方式入侵。
4. 統計損壞情形，呈報主管，通報受損資料之單位。
5. 追查駭客身分，報請相關司法單位依法究辦並要求賠償。

五、預防措施

1. 本公司已有設置高性能網路防火牆，防止不合法使用者進入本司網路。
   (一)利用防火牆將資料查詢系統與內部及外部資訊網路有效隔開。
   (三)防火牆主機與資料查詢系統主機放置於安全地點。
   (四)防火牆主機系統功能設定最簡化，排除安裝所有非必要系統。
   (五)執行安全稽核，建立自動監測功能。

2、已在各使用者電腦安裝防毒軟體並以中央集中控管方式定期更新病毒碼及系統排程掃毒，補足終端防護。

3、定期備份網路磁碟機資料。

4、每月資安宣導

四、定期參考演練.參考劇本如下:

參考演練劇本

某部門同事因對時常對國外客戶 e-mail 電子郵件往來.某天收到疑似東歐國家客戶詢問產品報價單主旨 e-mail 信件不經意隨手開啟附件出現一些亂碼.隔天上班開啟電腦主機桌面上所有檔案都被綴加副檔名不是打開變亂碼就是無法開啟.畫面馬上會跳出紅色視窗要求支付價值 10 個比特幣當成贖金.警告若未能在 7 天內交付贖金、取得解密金鑰，則受害者將無法恢復電腦內的已被加密的檔案.同仁緊急第一時間電話通知資訊處處理.

資訊處同仁經判斷為近年來流行的 WanaCrypt0r 2.0 電腦勒索病毒第一時間通知資訊處最高主管成立「緊急應變小組」並擔任召集人彙整相關病毒入侵受損情形呈報總經理告知.對中毒被駭同事電腦立即切斷外部及內部網路防護阻絕惡意攻擊以防使用者的電腦可能與辦公室內其他電腦相連互傳檔案.就有機會被肆虐感染危機並對中毒電腦的作業系統及檔案資料進行還原備份.同時間清查機房各伺服器主機系統維運日誌記錄.立即通知各單位同仁最近有無收到來路不明 E-MAIL 請勿隨意開啟並通報資訊處同仁統一處理.

透過防火牆日誌追查駭客之入侵滲透方式網路系統安全漏洞比對封包特徵並攔阻的特性.查經為作業系統漏洞所致協助各同仁迅速上官網下載修補安全更新程式及防火牆新增相關連線規則關閉可能入侵被駭連接埠(Port)提升安全層級.如果有損害到公司實質利益由本公司法務同仁到警察局備案交由國際刑警科會同網路警察偵辦.

經由以上模擬演練已達目前公司網路遭入侵應變處理辦法演練流程並定期更新病毒碼及資安宣導.重層嚇阻電腦遭入侵機會.