中華電信 Chunghwa Telecom X 中華資安國際 CHT Security

上市櫃資安管控指引與建議舉措

①110年重大訊息影響回顧

②111年起資安要求與管控指引

③依管控指引建議之舉措

中華電信高雄營運處 第一企業客戶科 郭裔辰 07-5507103

中華資安國際 南區資安管理科 王致傑 07-2626260#117

金融監督管理委員會 Financial Supervisory Commission R.O.C. (Taiwan)
證券期貨局 Securities and Futures Bureau

110/4/27重大訊息影響修正

資安事件造成影響需揭露

臺灣證券交易所股份有限公司 公告
中華民國110年04月27日
臺證上一字第1100007692號
修正本公司「對有價證券上市公司重大訊息之查證暨公開處理程序」第4條及第11條之條文如附件，並自即日起實施，請查照。
案經報奉金融監督管理委員會110年4月27日金管證發字第1100339846號函同意備查。
考量發生資通安全事件對財務業務之影響性逐漸上升，且對公司商譽等可能有重大影響，為強化該類事件重大訊息發布之重要性暨使法源依據明確，爰修訂旨揭重訊處理程序第4條及第11條相關文字。

- 第四條，上市公司重大訊息，係指下列事項：

  第二十六款發生災難、集體抗議、罷工、環境污染、**資通安全事件**或其他重大情事，致有　下列情事之一者：(一)造成公司重大損害**或影響**者；

- 第十一條，上市公司重大訊息說明記者會之重大訊息，係指上市公司主動提供或經本公司主動查證之下列事項：

  第九款發生災難、集體抗議、罷工、環境污染、**資通安全事件**、遭主管機關處分或其他重　大情事致造成公司重大損害**或影響**，且扣除其依保險契約設算獲賠金額後之預估損失超過該公司股本百分之二十或新台幣三億元以上者。無面額或每股面額非屬新台幣十元之公司，前開有關股本百分之二十之計算應以淨值百分之十替代之。

來源： http://www.selaw.com.tw/LawAttachment.aspx?LawID=G0100104&ModifyDate=1100427

修法後揭露之上市櫃公司

主旨	公告本公司遭受駭客攻擊
符合條款	第 26 款
事實發生日	110/08/06
說明	1.事實發生日:110/08/06 2.發生緣由:技嘉科技於110/08/06遭受駭客網路攻擊 3.處理過程:本公司資安團隊已與多家外部資安公司技術專家合作，共同處理此次針對技嘉科技少部份伺服器的網路攻擊，並已將所監測到的異常網路狀況,通報予政府相關執法部門與資安單位，並保持密切連繫。 4.預計可能損失:目前公司生產、銷售及日常營運未受影響。 5.可能獲得保險理賠之金額:尚未無法確定。 6.改善情形及未來因應措施:技嘉科技已於第一時間啟動資安防禦查，受到影響的內部服務均已陸續回復運作，我們亦同步檢視並，全面提升網路安全等級以保護資料安全及完整性。 7.其他應敘明事項:無。

主旨	威剛針對部分資通系統遭病毒攻擊事件說明
符合條款	第 53 款
事實發生日	110/05/26
說明	1.事實發生日:110/05/26 2.公司名稱:威剛科技股份有限公司 3.與公司關係(請輸入本公司或子公司):本公司 4.相互持股比例:不適用 5.發生緣由:不適用 6.因應措施:本公司5/23偵測到部分資通系統遭病毒攻擊，公司資安團隊第一時間啟動防禦機制及備援系統，並立即與資安專業人員合作清除病毒，全面提升網

主旨	代子公司Grand Home Holdings INC.公告遭受駭客網路攻擊
符合條款	第 26 款
事實發生日	110/08/30
	1.事實發生日:110/08/30 2.發生緣由:本公司美國子公司Grand Home Holdings INC.(以下簡稱GHHS)於110/08/30遭受駭客網路攻擊 3.處理過程:子公司GHHS資安團隊已與外部資安公司技術專家合作，共同處理此次針對GHHS部份伺服器的網路攻擊，並已將所監測到的異常網路狀況，通報予政府相關執法部門與資安單位，並保持密切連繫。 4.預計可能損失:目前GHHS銷售及日常營運未受影響。 5.可能獲得保險理賠之金額:無。 6.改善情形及未來因應措施:GHHS已於第一時間啟動資安防禦，並進行網路攻擊清查，受到影響的內部服務均已陸續回復運作；本公司亦敦請GHHS同步檢視並強化現有的基礎架構，全面提升網路安全等級以保護資料安全及完整性。 7.其他應敘明事項:無。

Yahoo奇摩新聞

獨家／慘！技嘉遭駭7GB主機板檔案 被PO上駭客論壇供人下載

板卡大廠技嘉科技（2376）在6日時透過證交所公告，指出遭到駭客攻擊，但 ... 總大小為7GB；而被洩漏出來的檔案中疑似是intel、AMD主機板的設計圖，...

2021年8月16日

修法後揭露之上市櫃公司

本資料由 (上市公司) 6605 帝寶 公司提供

序號	2	發言日期	110/10/18	發言時間	16:37:48
發言人	呂理豐	發言人職稱	經理	發言人電話	(04)772-2311
主旨	說明本公司部分工廠廠區伺服器遭受病毒攻擊及影響				
符合條款	第 26 款	事實發生日	110/10/18		
說明	1.事實發生日:110/10/18 2.發生緣由:帝寶工業部分工廠廠區伺服器遭受病毒攻擊，已通報政府執法部門。 3.處理過程:本公司偵測到公司內部部分工廠廠區伺服器遭受病毒攻擊，本公司資安團隊已於第一時間啟動防禦機制及備援作業，且與外部資訊技術專業人員共同合作處理，並已將所監測到的異常狀況，通報予政府相關執法部門，並保持密切聯繫。 4.預計可能損失:目前對本公司生產、銷售及日常營運無重大影響。 5.可能獲得保險理賠之金額:不適用 6.改善情形及未來因應措施:本公司已於第一時間啟動資安防禦，並對網路攻擊進行清查，受到影響的內部資訊系統均已陸續回復運作，本公司亦同步持續檢視並強化現有的基礎架構，全面提升網路安全，以保護資料安全及完整性。 7.其他應敘明事項:無。				

本資料由 (上市公司) 2014 中鴻 公司提供

序號	1	發言日期	110/10/27	發言時間	17:25:51
發言人	羅嘉文	發言人職稱	行政副總經理	發言人電話	(07)6118244
主旨	說明本公司輔助性伺服器遭受病毒攻擊及影響				
符合條款	第 26 款	事實發生日	110/10/27		
說明	1.事實發生日:110/10/27 2.發生緣由:本公司輔助性伺服器遭受病毒攻擊。 3.處理過程:本公司偵測到公司輔助性伺服器遭受病毒攻擊，本公司資安團隊已於第一時間啟動防禦機制及備援作業，且與外部資訊技術專業人員共同合作處理，並保持密切聯繫。 4.預計可能損失或影響:對本公司生產、銷售及日常營運未受影響。 5.可能獲得保險理賠之金額:不適用。 6.改善情形及未來因應措施:本公司已於第一時間啟動資安防禦，並對網路攻擊進行清查，亦同步持續檢視並強化現有的基礎架構，全面提升網路安全，以保護資料安全及完整性。 7.其他應敘明事項:無。				

修法後揭露之上市櫃公司

本資料由　(上市公司) 1504 東元　公司提供

序號	2	發言日期	110/12/20	發言時間	17:52:08
發言人	簡世雄	發言人職稱	處長	發言人電話	2655-3333
主旨	說明本公司部份資訊系統遭受駭客網路攻擊				
符合條款	第 26 款	事實發生日	110/12/20		
說明	1.事實發生日:110/12/20 2.發生緣由:　本公司部份資訊系統遭受駭客網路攻擊。 3.處理過程:　本公司偵測到部份資訊系統遭受駭客網路攻擊，資安部門已全面啟動相關防禦機制與備援作業，同時協調外部資安公司技術專家共同合作處置，將於彙集完整異常資料後，通報政府執法部門與資安單位，並保持密切聯繫。 4.預計可能損失或影響:經查對公司營運並無重大影響。 5.可能獲得保險理賠之金額:不適用 6.改善情形及未來因應措施:本公司於查知網路異常狀態後，立即啟動資安防禦機制與備援作業，目前資訊系統陸續回復運作中，本公司同時進行強化資安基礎架構、全面提升網路防護等級及保障資料安全性。 7.其他應敘明事項:無				

本資料由　(上櫃公司) 6697 東捷資訊　公司提供

序號	6	發言日期	110/12/20	發言時間	17:53:47
發言人	洪龍珠	發言人職稱	財務長	發言人電話	26552525
主旨	說明本公司部分資訊系統遭受駭客網路攻擊				
符合條款	第 26 款	事實發生日	110/12/20		
說明	1.事實發生日:110/12/20 2.發生緣由:本公司部分資訊系統遭受駭客網路攻擊 3.處理過程:本公司偵測到部分資訊系統遭受駭客網路攻擊，資安部門已全面啟動相關防禦機制與備援作業，同時協調外部資安公司技術專家共同合作處置，將於彙集完整異常資料後，通報政府執法部門與資安單位，並保持密切聯繫。 4.預計可能損失或影響:經查對公司營運並無重大影響。 5.可能獲得保險理賠之金額:不適用。 6.改善情形及未來因應措施:本公司於查知網路異常狀態後，立即啟動資安防禦機制與備援作業，目前資訊系統陸續回復運作中，本公司同時進行強化資安基礎架構、全面提升網路防護等級及保障資料安全性。 7.其他應敘明事項:無。				

111~112年需完成資安專責編制

預告修正「公開發行公司建立內部控制制度處理準則」第九條之一、第四十七條條文草案

2021-11-25

為強化公開發行公司資訊安全管理機制，金融監督管理委員會（以下簡稱金管會）研擬修正「公開發行公司建立內部控制制度處理準則」（以下簡稱處理準則）第九條之一及第四十七條，修正重點如下：

為提升公開發行公司對資訊安全之重視，明定應配置適當人力資源及設備進行資訊安全制度之規劃、監控及執行資訊安全管理作業，其符合一定條件者，本會得命令指派綜理資訊安全政策推動及資源調度事務之人兼任資訊安全長，並設置資訊安全專責單位、主管及人員，以利進行差異化管理。有關上市（櫃）公司應配置資訊安全人力之一定條件，將於處理準則實施後發布令釋規範，以循序漸進方式推動辦理，其實施範圍及時程如下：

分級標準	資安單位暨人力編制	實施時程
第一級： 符合下列條件之一者： 1. 資本額100億元以上 2. 前一年底屬臺灣50指數成分公司 3. 藉電子方式媒介商品所有權移轉或提供服務（如電子銷售平台、人力銀行等）收入占最近年度營業收入達80%以上，或占最近二年度營業收入達50%以上者	應設資安長及設置資安專責單位（包含資安專責主管及至少2名資安專責人員）	111年底設置完成
第二級： 第一級以外之上市（櫃）公司，最近三年度之稅前純益未有連續虧損，且最近年度財務報告每股淨值未低於面額者。	資安專責主管及至少1名資安專責人員	112年底設置完成

預計此修正草案將在通過預告期後，也就是明年初，就會正式發布施行。

111年起年報需揭露資安作為

修正「公開發行公司年報應行記載事項準則」部分條文及第十一條附表七、附表九、第十九條附表二十二、附表二十三(金管證發字第1100364979號)

2021-11-30

性質別：募集發行

金融監督管理委員會　令

發文日期：中華民國110年11月30日

發文字號：金管證發字第1100364979號

修正「公開發行公司年報應行記載事項準則」部分條文及第十一條附表七、附表九、第十九條附表二十二、附表二十三。

附修正「公開發行公司年報應行記載事項準則」部分條文及第十一條附表七、附表九、第十九條附表二十二、附表二十三

關於11月30日所發布的新版「公開發行公司年報應行記載事項準則」，資通安全管理的重點在**第十八條**營運概況記載事項中所增訂的第六款，明確要求公司年報必須揭露資安管理政策與風險管理架構，以及投入的資源，同時必須說明資安事件的因應，另在**第二十條**中，也要求需揭露資通安全風險對公司財務業務的影響與因應措施。

金融監督管理委員會 Financial Supervisory Commission R.O.C. (Taiwan)
證券期貨局 Securities and Futures Bureau

臺灣證券交易所 TWSE

工商時報 | 39 人追蹤 ☆ 追蹤

證交所發布資安管控指引

呂淑美 / 台北報導

2021年12月27日 週一 上午4:10 · 1 分鐘 (閱讀時間)

配合金管會強化上市公司資通安全管理政策，上市公司應配置適當人力資源及設備進行資通安全制度規劃、監控及執行資通安全管理作業，證交所發布「上市上櫃公司資通安全管控指引」，以協助上市公司有效規劃資通安全管理政策，建構完備的資通環境，強化資通安全防護及管理機制，進而保障投資人的權益。

證交所訂定「上市上櫃公司資通安全管控指引」，指引內容涵蓋政策面、管理面及執行面，提供上市公司作為資通安全相關規劃及執行計畫時參考，上市公司可衡諸產業特性、規模大小及資安風險適度採行。

另強化上市公司資安情資共享，提升資安事件通報應變能量，證交所鼓勵上市公司免費申請成為台灣電腦網路危機處理暨協調中心（TWCERT/CC）會員。

上市公司 / 文件下載

上市上櫃公司資通安全管控指引

https://dsp.twse.com.tw/

下載連結↑

資安管控指引

- 資安技術面基本上參考資通安全管理法(對象為關鍵基礎設施、公家機關、非特定公家機關如學校或公家法人)
- 本法於107年6月發布執行至今，今年110年8月因應資安威脅驟升，進行施行細則修正，以強化國家資安防護

行政院公報資訊網
The Executive Yuan Gazatte Online

每日即時刊登行政院及所屬各機關公布之法令規章等資訊
對於本網站提供之相關資訊，如有任何疑義，請逕向公（發）布機關洽詢。

行政院 令

中華民國110年8月23日
院臺護字第1100182012號

修正「資通安全管理法施行細則」第六條、第七條、第十三條、「資通安全責任等級分級辦法」第五條、第六條、第七條及第十一條附表一至附表八、附表十、「資通安全事件通報及應變辦法」第六條、第十三條、第二十一條、「特定非公務機關資通安全維護計畫實施情形稽核辦法」第三條、第六條、第十條、「資通安全情資分享辦法」第三條、第十一條及「公務機關所屬人員資通安全事項獎懲辦法」第四條、第七條。

附修正「資通安全管理法施行細則」第六條、第七條、第十三條、「資通安全責任等級分級辦法」第五條、第六條、第七條及第十一條附表一至附表八、附表十、「資通安全事件通報及應變辦法」第六條、第十三條、第二十一條、「特定非公務機關資通安全維護計畫實施情形稽核辦法」第三條、第六條、第十條、「資通安全情資分享辦法」第三條、第十一條及「公務機關所屬人員資通安全事項獎懲辦法」第四條、第七條

院　　長　蘇貞昌

資安管控指引與資通安全法比較

左側為管控指引，右側為資安法要求

第十六條、對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。

一、 定期辦理弱點掃描。

二、 定期辦理滲透測試。

三、 系統上線前執行源碼掃描安全檢測。

第十八條、具備下列資安防護控制措施：

一、 防毒軟體。

二、 網路防火牆。

三、 如有郵件伺服器者，具備電子郵件過濾機制。

四、 入侵偵測及防禦機制。

五、 如有對外服務之核心資通系統者，具備應用程式防火牆。

六、 進階持續性威脅攻擊防禦措施。

七、 資通安全威脅偵測管理機制(SOC)。

端點偵測及應變機制	一、 初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。

安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
	滲透測試	全部核心資通系統每年辦理一次。

資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
	網路防火牆	
	具有郵件伺服器者，應備電子郵件過濾機制	
	入侵偵測及防禦機制	
	具有對外服務之核心資通系統者，應備應用程式防火牆	
	進階持續性威脅攻擊防禦措施	

資通安全威脅偵測管理機制	初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。

中華資安：為了資安法而成立之子公司

中華電信關係企業 Chunghwa Telecom

資料時間：110.09.01

民國92年
中華電信資安處

民國106年
子公司籌備成立

3.09億元
實收資本額

200+人
員工總數

技術能力

- ✓ **具國家級資安專案建置能力**，如國發會雲端資料中心、政府GPKI、行政院技服二線SOC等
- ✓ 108-110年已**挖掘40個CVE漏洞**，包含電子郵件、保全系統、網銀數位簽章元件及IoT設備
- ✓ **整合集團資源**，包含HiNet上網安全服務、大數據處、全台IDC機房與中華電信研究院SDN平台等
- ✓ 為響應國家資安政策，106年籌備資安子公司中華資安國際，107年**完成轉移並裁撤原中華電信數據通信分公司資安處**
- ✓ 中華電信自**92年開始經營資安業務**，含資安檢測、事件鑑識、設備整合、SOC監控通報與資安攻防等

110年

92年

專案實績

- ✓ **OO府「SOC監控通報服務」**
- ✓ **16個縣市政府「前瞻計畫資安區域聯防專案」**
- ✓ 國發會/電信技術中心-亞洲·矽谷計畫「強化物聯網資安防護」
- ✓ 勞動部勞保局 「資訊安全防護作業委外服務」
- ✓ 中華郵政「資安監控中心管理系統委外建置監控服務」
- ✓ 中油「資安監控中心委外監控及技術服務」
- ✓ 台灣高鐵「 MMD工控系統資安檢測暨控制措施評估」
- ✓ 台電「建置智慧電網入侵偵測系統(IDS)先導計畫」

中華資安：高雄辦公室實際服務客戶(資安SOC監控服務)

高雄市政府 Kaohsiung City Government
屏東縣政府
臺南 TAINAN
財團法人電信技術中心 TELECOM TECHNOLOGY CENTER
嘉義市政府
嘉義縣政府 Chiayi County Government
海洋委員會 Ocean Affairs Council
金門縣政府 Kinmen County Government
澎湖縣政府 Penghu County Government
台灣國際造船股份有限公司 CSBC CORPORATION,TAIWAN
南農中心
臺東縣政府 Taitung County Government
台糖 台灣糖業股份有限公司
WEI WU YING 衛武營 國家藝術文化中心
高雄市立聯合醫院 Kaohsiung Municipal United Hospital
奇美醫療財團法人 奇美醫院 Chi Mei Medical Center
NARLabs 國家實驗研究院 台灣海洋科技研究中心 Taiwan Ocean Research Institute
成大醫院 NCKUH
高雄榮民總醫院
國軍高雄總醫院 KAOHSIUNG ARMED FORCES GENERAL HOSPITAL
Zuoying Branch of Kaohsiung Armed Forces General Hospital
中榮總嘉義分院 Chiayi Branch, TCVGH
高醫醫學大學附設中和紀念醫院 KAOHSIUNG MEDICAL UNIVERSITY HOSPITAL

- 行政院資安服務廠商評鑑全項目A級

項目 / 廠商	SOC監控	資安健診	弱點掃描	滲透測試	社交郵件
中華資安國際	A	A	A	A	A

- 滲透測試連續7年及SOC與資安健診連續6年A級(含中華電信時期)

- 資安鑑識實驗室
- 金融安全評估能力
- 工控多樣場域
- 紅隊演練實力
- 北中南在地資安工程師

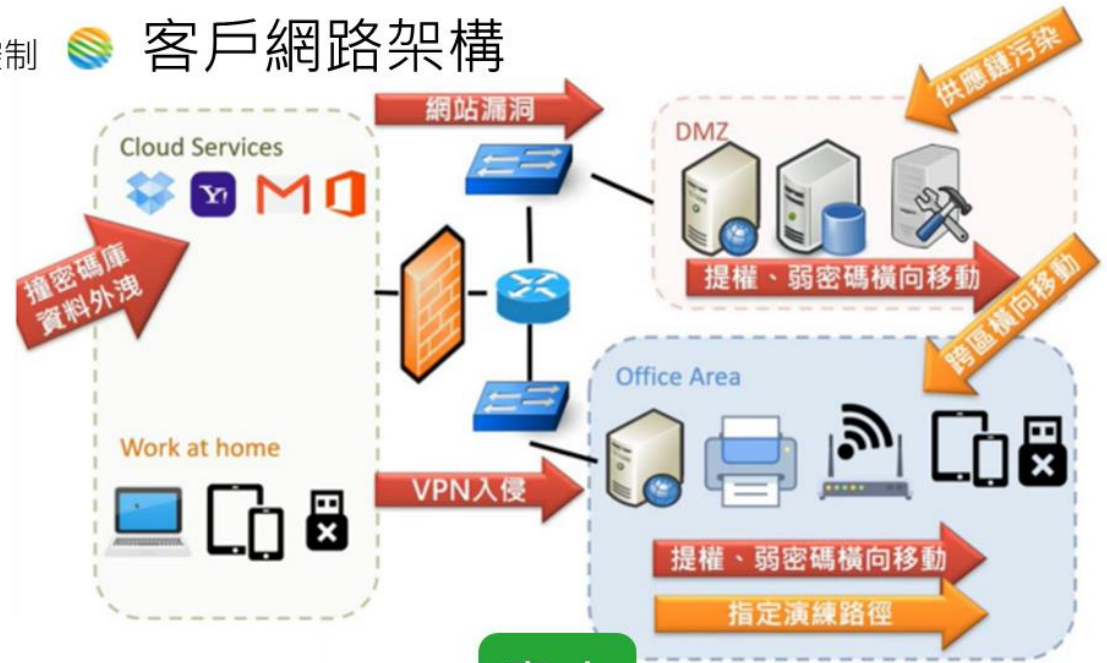
資安牽涉：事前、事中、事後

弱點管理平台
資產管理軟體

NAC軟體
網路存取控制

資安健診服務

檢視網路架構、防火牆與伺服器權限控管與前頁的各項檢測類型服務等...



SOC監控

即時監控客戶資安設備、重要伺服器日誌，並結合客戶使用習慣進行關聯性分析，讓客戶可第一時間洞察駭客攻擊，降低損失

事 前

- 資產盤點與管理
- 資安政策與計畫
  - ✓風險評估
  - ✓改善計畫
  - ✓追蹤精進

事 中

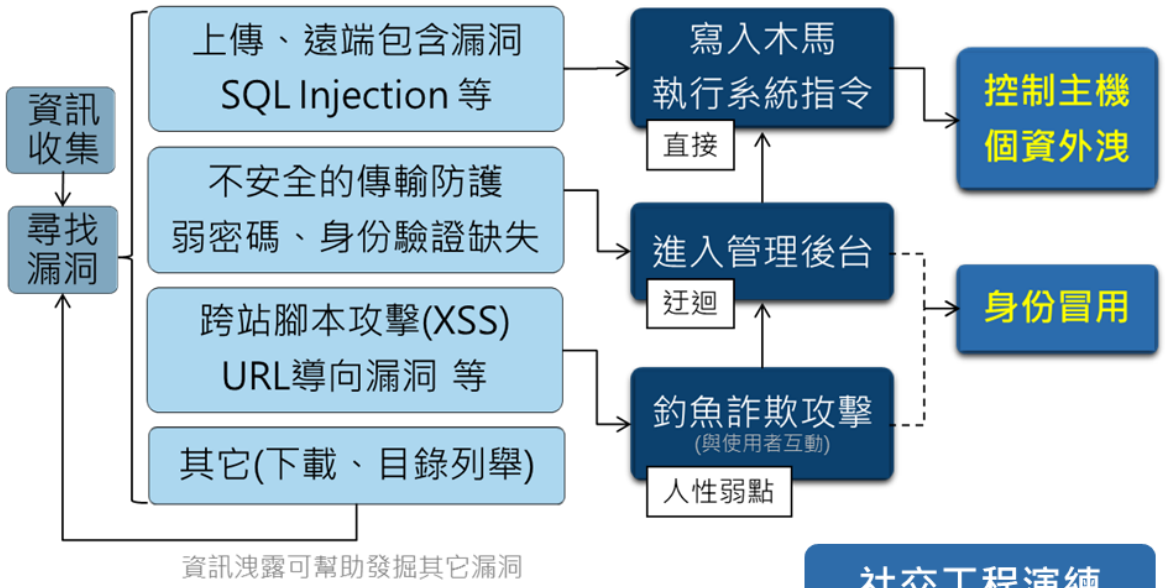
- 網路可視性
  - SSL解析
  - MDR
- 偵測機制(資安監控中心SOC)
  - 資通安全管理法B級以上之要求

事 後

- 事件應變IR
  - ✓逆向程式分析
  - ✓找出入侵管道
  - ✓改善處理措施
- 災害復原DR

事前：弱點檢測與弱點管理

客戶系統網頁



網站防火牆 WAF
Web Application Firewall

社交工程演練

模擬真實釣魚
信件寄送
彌補教訓訓練不足

傳統CBT
Computer Based Training

主機弱點掃描

自動化工具探測
透過回應版本與設定
以驗證是否存在已知漏洞

Web網頁弱點掃描

自動化工具探測
透過網頁所有輸出
找出各項常見漏洞

OWASP TOP 10
2017→2021

滲透測試

模擬駭客入侵
各項工具與高強度手法
並提供截圖佐證

紅隊演練

模擬駭客APT攻擊,利用情資蒐集與各攻防技術對於目標系統進行整體測試

程式碼撰寫安全

程式弱點超過80%在開發階段產生，治本在於遵循安全設計原則

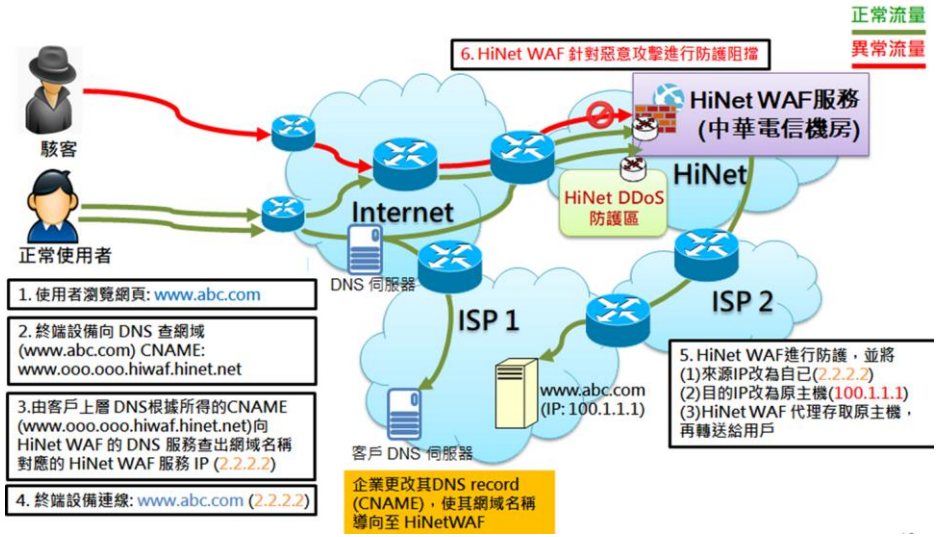
程式源碼檢測

靜態檢測可涵蓋範圍的不足，且開發階段就能檢測

事前：針對弱點進行強化防護

- Palo Alto Networks 官方新聞稿連結
- ISP端建置電信級防火牆，並於閘道端提供資安服務
- 讓原先的硬體式防火牆專注執行VPN、Policy等工作

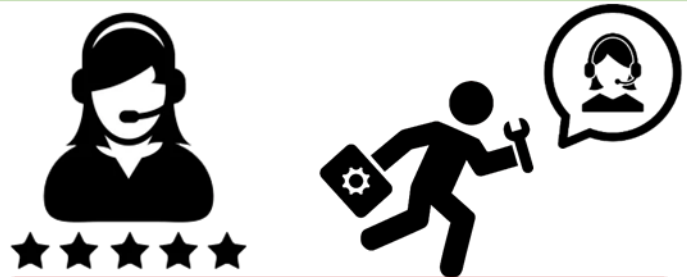
- 程式碼開發的不安全、攻擊套件濫用(MaaS)
- 漏洞發佈速度遠高於企業修補速度
- 應用程式防火牆WAF屬於高費用投資、高技術門檻，建議考慮ISP端WAF服務包含協助調教，採用設備為領導廠牌F5



事中：資安SOC監控與通報

People

7x24小時資安監控



資安專家遠端電話/到場處理

Process

資安事件通報
管理作業流程

軟、硬體異常
偵測處理程序

事件關聯性
規則制定流程

資安事件處理
與鑑識作業

Product (Security)

Event Log

AD/DNS　Firewal/IPS　Anti-Viurs

日誌紀錄收集

日誌管理系統

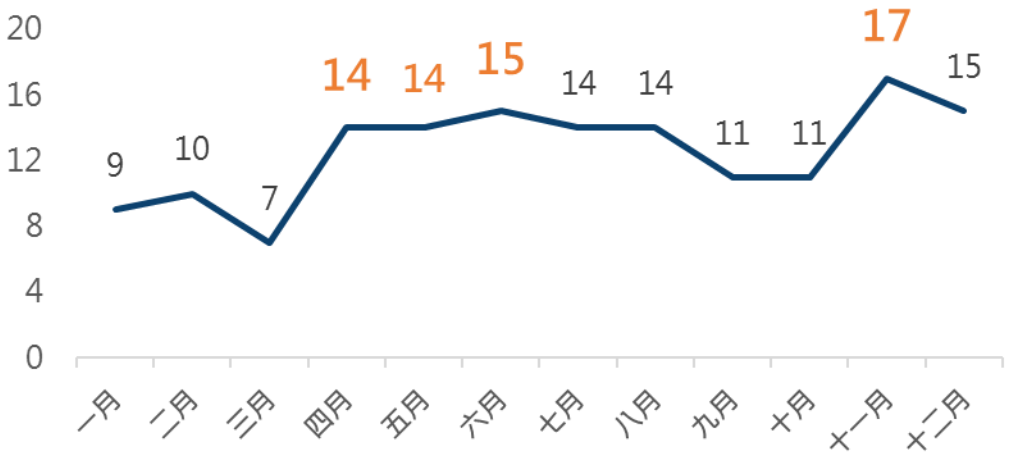
事件分析

事件開單

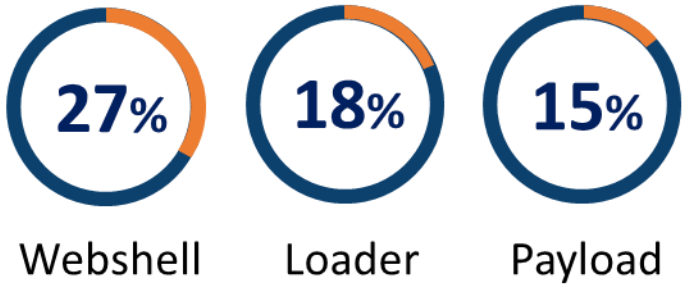
資安監控分析系統

事後處理：中華資安實績 - 2020資安事件處理統計

資安事件調查數量

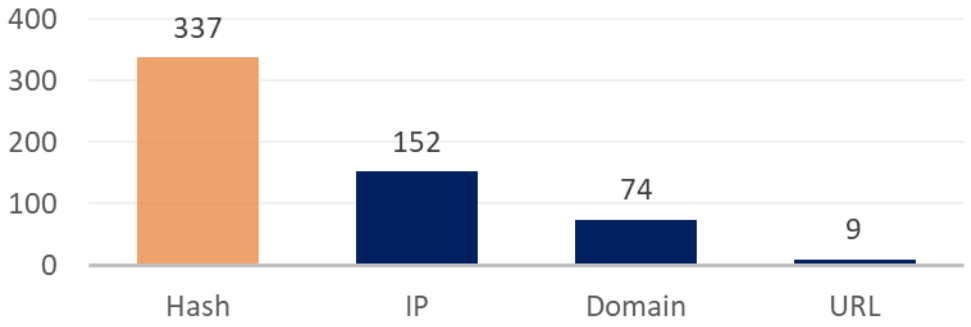


惡意程式類型



Hacktool12%　Script2%
Trojan7%　Keygen2%
Backdoor5%　Ransomware2%
Downloader4%　Dropper1%
Stealer4%　Miner1%

新發現威脅情資



駭客入侵手法

資安服務地圖

中華電信關係企業 Chunghwa Telecom

資安專業服務

專業顧問

資安防護架構評估與規劃設計、PKI建置規劃

ePKI Authentic Site

資安監控與處理

SOC(MDR)監控通報、IR事件應變與鑑識、工控(ICS)及關鍵基礎設施資安

eyeLAN

專業檢測

弱點掃描、滲透測試、紅隊攻擊、資安健診、源碼檢測、社交工程演練

CHT Security

ISP端資安方案

ISP骨幹網路

DDoS防護 | IPS防護 | WAF保護 | 新世代防火牆 | 防駭守門員 | 資安防護閘道器 | 色情守門員 | 上網時間管理

資安軟硬體整合監控

自有研發產品

1. 資安管理平台：資安監控平台(SOC)、弱點管理平台、社交工程演練平台
2. MDR戰情牆系統 / AI巡檢包
3. 通用日誌管理系統Logger
4. 資安資訊分享與分析平台(ISAC)
5. SecuTex 網路側錄與防護
6. CryptoCortex 安全晶片與應用

SecuTex

Acunetix by Invicti

tenable

資安硬體

企業閘道端 (WAF、UTM、IPS、NGFW、ISFW)

paloalto NETWORKS

資安管理平台

MICRO FOCUS ArcSight

ELK Stack

FIREEYE CROWDSTRIKE

CHT Security MDR

Web DB Mail

OTP 2FA + Device憑證

384629

外部管理者

Endpoint

資安軟體

端點(防毒、EDR)

弱掃、檢測軟體

中華電信
Chunghwa Telecom

“WE CERTAINLY AREN’T HERE TO DO WHAT’S BEEN DONE BEFORE.”

中華資安國際
CHT Security

第一企業客戶科 郭裔辰

0972-268-332 07-5507103

shanguo@cht.com.tw

高雄市左營區至聖路200號9樓

南區資安管理科 王致傑

0905-505-815　07-2626260#117

Line ID: joyee07

joyee07@chtsecurity.com

高雄市左營區至聖路200號5樓505室