建立證券商

資通安全分級防護

臺灣證券交易所

TAIWAN
STOCK EXCHANGE

基本概念

TAIWAN
STOCK EXCHANGE

2020資安事件

預防重於治療

連續三天遭到網路攻擊，紐西蘭證券交易所暫停交易

這是個針對紐西蘭重要基礎設施的罕見大型攻擊行動

文/ 陳曉莉 | 2020-08-27 發表

讚 6.2 萬 按讚加入iThome粉絲團 讚 319 分享

圖片來源: New Zealand Exchange，NZX

東京證交所系統異常首度全天停盤 名古屋福岡札幌也停止交易

最新更新：2020/10/01 13:36

新局面

資安即國安

107年國家安全會議提出了我國首部資安戰略報告

資通安全分級防護

目的

參照資通安全管理法子法「資通安全責任等級分級辦法」，依業者規模強化證券商資訊安全分級管理機制，明確規範各級證券商應辦理之資訊安全管理及防護事項，降低潛在的資安風險。

依據

依據「108年第一次證券期貨市場資通安全會議」決議辦理，就資通安全管理法之子法「資通安全責任等級分級辦法」所列各資安責任等級應辦事項，研議證券期貨業者分級及其資安防護標準。

依實收資本額或指撥營運資金區分四級
各級對應相關控制項目

實收資本分級(指撥營運資金)

第一級(3)	=	200億以上		
第二級(6)	=	100億以上	+	未達200億
第三級(10)	=	40億以上	+	未達100億
第四級(45)	=	未達40億		

辦理事項

維持

- 資通安全人員配置
- 內部資通安全稽核
- 網站安全弱點檢測
- 資通安全教育訓練(專責)
- 資通安全教育訓練(一般)

新修訂

- 資訊系統分級
- 資訊安全管理系統導入及通過驗證
- 業務持續運作演練
- 系統滲透測試
- 資通安全健診
- 資通安全威脅偵測管理機制
- 防毒軟體
- 網路防火牆
- 電子郵件過濾機制
- 入侵偵測及防禦機制
- 應用程式防火牆
- 進階持續性威防禦措施
- 資安人員應取得並維持資安專業證照

現行規範

規範

建立證券商資通安全檢查機制
(中華民國91年2月8日)

內容

1. 風險評鑑與管理(CC-11000)
2. 資訊安全政策(CC-12000)
3. 安全組織(CC-13000)
4. 資產分類與控制(CC-14000)
5. 人員安全(CC-15000)
6. 實體與環境安全(CC-16000)
7. 通訊與作業管理(CC-17000)
8. 存取控制(CC-18000)
9. 系統開發及維護(CC-19000)
10. 營運持續管理(CC-20000)
11. 符合性(CC-21000)
12. 新興科技應用(CC-21100)
13. 其他(CC-22000)

TAIWAN
STOCK EXCHANGE

新修訂內容

防毒軟體

規定

網路安全管理CC-17010

公司應安裝防毒軟體並適時更新防毒軟體程式、病毒碼及執行掃毒。

實作 110年生效

全體證券商全公司

1. 可偵測病毒、蠕蟲、木馬程式、間諜程式、廣告軟體、Bot、零時差(Zero-Day)攻擊 威脅、Rootkit 等惡意程式。
2. 病毒定義檔需要可以自動更新。
3. 可參考3大防毒軟體評鑑機構(AV-Comparatives, AV-TEST 與 Virus Bulletin)評等。

防火牆

規定

網路安全管理CC-17010

應建立防火牆
防火牆應有專人管理
防火牆進出紀錄及其備份應至少保存三年
重要網站及伺服器系統（如網路下單系統等）
應以防火牆與外部網際網路隔離
防火牆系統之設定應經權責主管之核准

實作 110年生效

全體證券商全公司

1. 可以依黑名單或白名單方式設定連線條件
2. 需具備使用及設定紀錄儲存，並支援遠端存放功能

電子郵件過濾機制

規定

網路安全管理CC-17010

為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定及建立郵件過濾機制。

實作 110年生效

全體證券商全公司

1. 符合公司電子郵件安全管理規範
2. 提供過濾垃圾郵件、惡意威脅信件、進階威脅特定信件、病毒攻擊信件、社交工程信件等機制
3. 具有郵件記錄備份備援、附件管控、遠端調閱、密碼強度檢測、防偽偵測、進階防禦等功能。
4. 提供完善鑑別日誌以及自訂排程寄送鑑識報表。

資訊系統分級

規定

資產分類與控制CC-14000

公司應對自行或委外開發之資訊系統完成資訊系統分級，資訊系統等級應至少區分核心與非核心系統，每年應至少檢視一次資訊系統分級妥適性。

實作 111年生效

全體證券商全公司

機密性(高中低)
完整性(高中低)
可用性(高中低)
法律遵循性(高中低)
證券期貨商資訊安全防護標準研究報告 (核心系統)

資訊安全系統導入及驗證

規定

資訊安全政策CC-12000

公司應依其所屬資安分級辦理核心系統導入資訊安全管理系統，並通過公正第三方之驗證，且持續維持驗證有效性。

實作 111年生效

1~3級證券商核心系統

1. 第1~3級券商於111年完成導入資訊安全系統。
2. 第1~2級券商需於112年內通過公正第三方驗證並持續維持驗證有效性

業務持續運作演練

規定

營運持續管理 CC-20000

公司應訂定營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及定期檢視更新程序，並執行關鍵性業務衝擊影響分析及訂定核心系統可容忍中斷時間，再依其所屬資安分級定期辦理業務持續運作演練。

實作 111年生效

1~3級證券商核心系統

1. 依據風險評估結果更新營運持續計畫，並且提出適切營運持續演練計畫。
2. 定期執行業務持續運作演練，產出業務持續運作演練紀錄。
3. 依業務持續運作演練結果修正計畫。

系統滲透測試

規定

網路安全管理CC-17010

公司應依其所屬資安分級定期對提供網際網路服務之核心系統辦理滲透測試，並依測試結果進行改善。 。

實作 111年生效

1~3級證券商核心系統

1. 項目包含作業系統、網站管理、應用程式、資料庫及密碼破解。
2. 滲透測試工具使用人員須接受專業訓練並具備特定資格(GPEN 、GWAPT 或其他類似訓練證明)。
3. 進行系統滲透測試後，應提供滲透測試結果及修補建議。
4. 依據測試結果修補相關漏洞並進行複測，以確保修正。

資安健診

規定

網路安全管理CC-17010

公司應依其所屬資安分級定期辦理資通安全健診。

實作 112年生效

1~3級證券商全公司

1. 網路架構設計邏輯檢視。
2. 主機網路位置檢視。
3. 現有防護機制檢視。

資通安全威脅偵測管理機制

規定

網路安全管理CC-17010

公司應依其所屬資安分級建立資通安全威脅偵測管理機制(應含括異常分析、事件收集、偵測攻擊)

實作 112年生效

1~2級證券商全公司

1. 異常分析
2. 事件收集
3. 偵測攻擊

入侵偵測及防禦機制

規定

網路安全管理CC-17010

公司應依其所屬資安分級建立入侵偵測及防禦機制

實作 112年生效

1~2級證券商全公司

1. 協助蒐集主機、網路連接、作業系統、應用程式資訊
2. 可識別事故(Incident)的型態
3. 提供執行分析、確認告警正確性、事件及事件紀錄關連

應用程式防火牆

規定

網路安全管理CC-17010

公司應依其所屬資安分級設置應用程式防火牆。

實作 112年生效

1~2級證券商全公司

1. 可針對最新版 OWASP TOP 10 攻擊行為進行偵測與攔截。
2. 符合信用卡國際組織 PCI DSS 規範之要求。
3. 可防止或降低 DOS/DDOS 之攻擊。
4. 具備辨識敏感資料洩露功能，例如身份證字號、持卡人資料。

進階持續性攻擊防禦措施

規定

網路安全管理CC-17010

公司應依其所屬資安分級辦理進階持續性威脅攻擊防禦措施

實作 112年生效

1級證券商全公司

1. 可結合入侵防禦系統、次世代防火牆、安全電子郵件閘道、終端保全以及威脅偵測等工 具，阻絕已知威脅。
2. 具惡意程式分析、內網滲透、隱匿行為、帳號入侵、資料外洩、檢查網路流量行為。
3. 回應可能發生事件，隔離使用者、裝置，確保資源與資料安全。

資通安全專業證照

規定

安全組織CC-13000

公司應依其所屬資安分級要求資安專責人員取得並維持相當資通安全專業證照。

實作 112年生效

1~3級證券商全公司

1. 電腦作業安全概念
2. 資訊安全概論
3. 機關資安管理規定
4. 個人資料保護概論
5. 資通安全相關法律
6. 資通安全管理制度

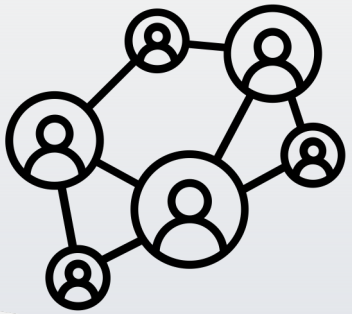
TAIWAN
STOCK EXCHANGE

未來展望

金融資安行動方案

追求安全便利不中斷的金融服務

強化資安管理



深化資安治理

精實金融韌性

發揮資安聯防

建立重視資安組織文化
提升資安治理能力與水準
營運不中斷資料不外洩
強化資安聯防

TAIWAN
STOCK EXCHANGE

簡報結束
敬請指導