時間：107年6月22日（五）下午 1:30

議程：

時間	分鐘	內容	講者
13:30~14:00	30	來賓報到	
14:00~14:10	10	開場 & 致詞	經濟部商業司 許福添專委
14:10~14:50	40	電商選擇開店系統的資安風險管理指南	Deloitte 勤業眾信 陳鴻棋協理
14:50~15:30	40	內容管理系統（CMS）的資安風險與工具檢測	中華電信數據通信分公司 林俊賢產品經理
15:30~15:40	10	中場休息	
15:40~16:20	40	網際網路零售業因應歐盟 GDPR之個資暨資安法遵建議	資策會科技法律研究所 蔡淑蘭副分析師
16:20~17:00	40	商譽優先！網路賣家的資安旅程	CloudRiches 雲馥數位 王育民技術總監

電商選擇開店系統的資安風險管理指南

Deloitte勤業眾信　陳鴻棋協理

Deloitte.

中華民國無店面零售商業同業公會
Chinese Non-Store Retailer Association

電商選擇開店系統的資安風險管理指南

勤業眾信聯合會計師事務所
風險諮詢服務/陳鴻棋 協理
2018.6.22

大綱

- 電商系統環境分析
- 電商系統資安事件相關案例
- 電商系統資安成熟度分析
- 資安強化三要素
- 意見交流

電商系統環境分析

電子/行動商務發展趨勢

Digital Trends – 行動裝置與自助式服務

Digital Trends – 數據應用

Digital Trends – 個人化互動與社群應用

電子商務的監理挑戰

身分識別及交易風險管理

數位商業模式將造成傳統KYC程序莫大的困難，如何**利用科技達成事前徵審、事中監控與事後調查來核實身分及信用紀錄**，進一步控管交易風險(如反洗錢、反詐欺及反資恐)，成為虛擬環境風險管控的重點。

新興科技安全

新興科技導入衍生出許多科技管理的議題，例如：**數位金融服務架構規劃、人才培育、新型資安風險**等，都是未來金融業者在科技導入時必須面對的議題。

消費者權益及資料保護

消費者權益保障及資料保護一直是監理機構的監管重點。**金融商業模式變形時，如何有效執行消費者權益保障，並且在跨界跨業整合中，保護消費者資料**，是重要課題。

跨產業監理

金融發展已逐漸打破現行業務建構的模式，強調以「客戶」為出發點、從「價值創新」思考、到「營運模式」落實，**根據使用者場景發展的商業模式將使產業間的界線逐漸模糊。**

跨國境稅務監理

服務提供者藉由各式跨境與跨業的整合串聯技術與機制，讓金融服務逐漸變成一種內嵌式的服務或是基礎架構，同時，**由於網路無遠弗屆的特性，網路金融服務可以輕易地推廣給全世界的使用者。**

電子商務系統平台面臨之風險與挑戰

電商套裝系統	環境分析	自建電商系統
通常不使用開源程式碼，被駭客攻擊的風險相對較低		較常使用開源程式碼，開源程式碼已知漏洞較多，若未適時更新修補程式，則易成為駭客攻擊目標
基礎設施非使用者負責建置及維護，無法掌握設施狀態，但也不必負擔相關費用		基礎設施由使用者負責建置及維護，能即時掌握設施狀態，但維護應委外或指定專人負責
資料庫非使用者負責建置及維護，較無法掌控資料安全		資料庫由使用者負責建置及維護，應有專人負責，較能掌控資料安全
網路架構視廠商規劃而有不同的安全程度，應列入選擇系統所要考量的因素		能依據安全需求進行網路架構
密碼原則普遍不符合資安要求，較容易被駭客破解		密碼原則能視安全需求進行設定

電商系統資安事件相關案例

惡意程式攻擊 - 駭客攻擊

電商	來源(時間)	內容	影響
○碁	HackRead (2016/06)	○碁北美區線上銷售網站會員資料遭駭，導致美國、加拿大與波多黎各三地區之會員資料未加密而外洩。遭洩漏的個資包括會員個人姓名、信用卡號、到期日、驗證碼及會員地址等。	約3.4萬名用戶個資外洩。
三○網○書○	聯合新聞網 (2017/10)	詐騙集團駭入知名書商「三○網○書○」，取得會員交易個資與明細後，假冒書店及銀行客服，謊稱民眾訂單誤設為重複訂購，將從民眾的銀行戶頭自動扣款，要求民眾按照指示操作ATM解除，藉機詐財得逞。	詐騙集團藉外洩個資詐騙民眾，兩週受害民眾達108人。

惡意程式攻擊 - 惡意軟體

電商	來源(時間)	內容	影響
臺灣證券商	iThome (2017/02)	臺灣史上第一次券商集體遭DDoS攻擊勒索事件，全臺先後有十多家券商收到勒索信件，其中13家的網站下單系統更實際遭DDoS攻擊，平均短暫停擺了半個多小時。駭客大都挑選早上8點和10點之間，鎖定券商發動洪水式DDoS攻擊。攻擊對象呈現隨機，包括交易金額第二、第二的龍頭券商。	證券商下單系統平均停擺半個多小時，若券商下單網站因DDoS攻擊而停擺過久，容易造成交易量的降低。
Nayana	TechNews (2017/06)	南韓的主機代管商 Nayana 遭到 Ransom.Erebus 攻擊，在與勒索軟體斡旋後，決定支付贖金。Nayana 代管了 3,000 多個南韓網站，其中 153 台伺服器被勒索軟體綁架。此外，由於駭客不但攻擊線上伺服器，同時也成功攻陷了用來備份資料的伺服器。	153 台伺服器被勒索軟體綁架，共支付110萬美元。

惡意程式攻擊 - 網路釣魚信件

電商	來源(時間)	內容	影響
尼泊爾NIC亞洲銀行	iThome (2017/10)	尼泊爾NIC亞洲銀行國際匯款轉帳SWIFT系統遭到駭客以假匯款通知，企圖轉帳4.6億盧比。當地媒體的報導，國際駭客之所以可以順利入侵尼泊爾NIC亞洲銀行的SWIFT系統，是因為該行行員可以在提供國際轉帳匯款SWIFT系統的伺服器上，開啟個人的郵件帳號導致。這樣的手法則和其他國家SWIFT系統遭入侵的手法類似，有內部員工點選網路釣魚信件，導致內部網路電腦被駭客植入惡意程式。而這幾起SWIFT系統受駭的過程，彼此都有異曲同工之妙。	駭客將盜轉金額轉入的銀行，以亞洲為主，歐美其次以及歐洲的德國和美國等國家的銀行帳號。尼泊爾NIC亞洲銀行已追回1.1億盧比。

個資外洩 - 用戶個資外洩

電商	來源(時間)	內容	影響
○○ 人力銀行	TechNews (2018/03)	經過人力銀行內部清查，發現台灣宅經濟商務公司與保險業務人員勾結，雙方談好只要業務員付清人力銀行每季8000元的廣告刊登費，就能借台灣宅經濟商務股份有限公司名義進入人力銀行網站，搜尋原本保險、傳銷公司看不到的求職名單，取得總共2萬筆求職者的個資。 此案是近年來首見透過官民合作保障求職者個資的成功案例，這是由人力銀行主動發覺，主動糾舉不法。	總共2萬筆求職者的個資遭不法人士取得。

服務遭中斷 & 用戶個資遭外洩 - 內部人員疏失

電商	來源(時間)	內容	影響
GitLab	TechNews (2017/02)	GitLab 的工程師在處理其他問題時，誤將正在運行的1號伺服器刪除，且該伺服器最近的備份是六小時前。	造成共5,037個項目受影響、707名用戶遺失等。
Time Warner app	iThome (2017/09)	美國有線電視業者時代華納（Time Warner）因為手機app外包商線上資料庫設定疏忽，致使超過400萬名用戶資料在雲端一度不設防曝光於網路上。這批外洩資訊來自軟體及服務外包商BroadSoft，可能是這家軟體廠商為時代華納開發多項app使用的相關資料。因工程師設定錯誤，導致不應公開的資料夾被曝露出來。	400萬名用戶資料(如姓名、財務交易ID、帳號號碼、MAC位置、用戶付款地址、電話號碼等)外漏。 除了用戶資料，BroadSoft自家基礎架構資料像是服務及類別明細等也遭公開。

臺灣資通安全管理法規範重點

總統府已於於6月6日正式公布資通安全管理法，行政院預計6月底前公布施行時間。

資通安全推動組織
行政院、委託或委任單位、各公務機關
中央目的事業主管機關權責

公務機關資通安全管理
資安責任等級分級
資安維護計畫之制定與實施
資安長設置
年度資安報告提出與資安查核
資安事件通報應變
建立情資分享機制
獎懲制度

特定非公務機關資通安全管理
資安責任等級分級
中央目的事業主管機關得要求訂定與執行資安維護計畫，並進行查核
資安事件之通報應變 **(應通報而未通報處新臺幣三十萬元以上五百萬元以下罰鍰)**
行政檢查
罰則 **(按次處新臺幣十萬元以上一百萬元以下罰鍰)**

資通服務之委外管理
委託機關應監督受託者資安之維護

促進資通安全產業
資通安全專業人才之培育。
資通安全科技之研發、整合、應用、產學合作及國際交流合作之推動。
資通安全產業發展及推動。
資通安全軟硬體、設備技術規範、資通安全相關服務及審驗機制之發展及推動。

法案架構

資通安全管理法

資通安全推動組織
- 行政院、委託或委任單位、各公務機關
- 中央目的事業主管機關權責
- 權限委託(6)

公務機關資通安全管理
- 資安責任等級分級(7I)
- 資安維護計畫之制定與實施(10)
- 資安長之設置(11)
- 年度資安維護計畫實施情形之提出(12)
- 資安稽核(13I)
- 改善報告(13II)
- 資安事件通報應變(14IV)
- 獎勵辦法(15II)
- 懲處辦法(19II)

特定非公務機關資通安全管理
- 資安責任等級分級(7I)
- 資安維護計畫之制定與實施(16III、17I)
- 年度資安維護計畫實施情形提出 (16IV、17II)
- 資安稽核(7II)
- 資安事件通報應變(14IV、18IV)
- 改善報告(7III 、16VI、17III)
- 公告(18V)
- 罰則(20~21)

資安整體環境與產業發展
- 資安專業人才之培育(4)
- 資安科技之研發、整合、應用、產學合作及國際交流合作(4)
- 資安產業發展(4)
- 資安軟硬體、設備技術規範、資安相關服務及審驗機制之發展(4)
- 定期公布國家資安情勢、對公務關稽核概況之報告及資安發展案(5)
- 資安情資分享(8 II)

資通服務之委外管理
- 委託機關應監督受託者資安之維護(9)

註：1. 粗體藍字部分，係以個別子法規範。
2. 其頭規範事項，由施行細則補充(22)。

資通安全維護計畫應包含之控制領域

資通安全管理法 §7

- 關鍵基礎設施提供者應訂定、修正及實施**資通安全維護計畫**。
- 考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件

資通安全維護計畫

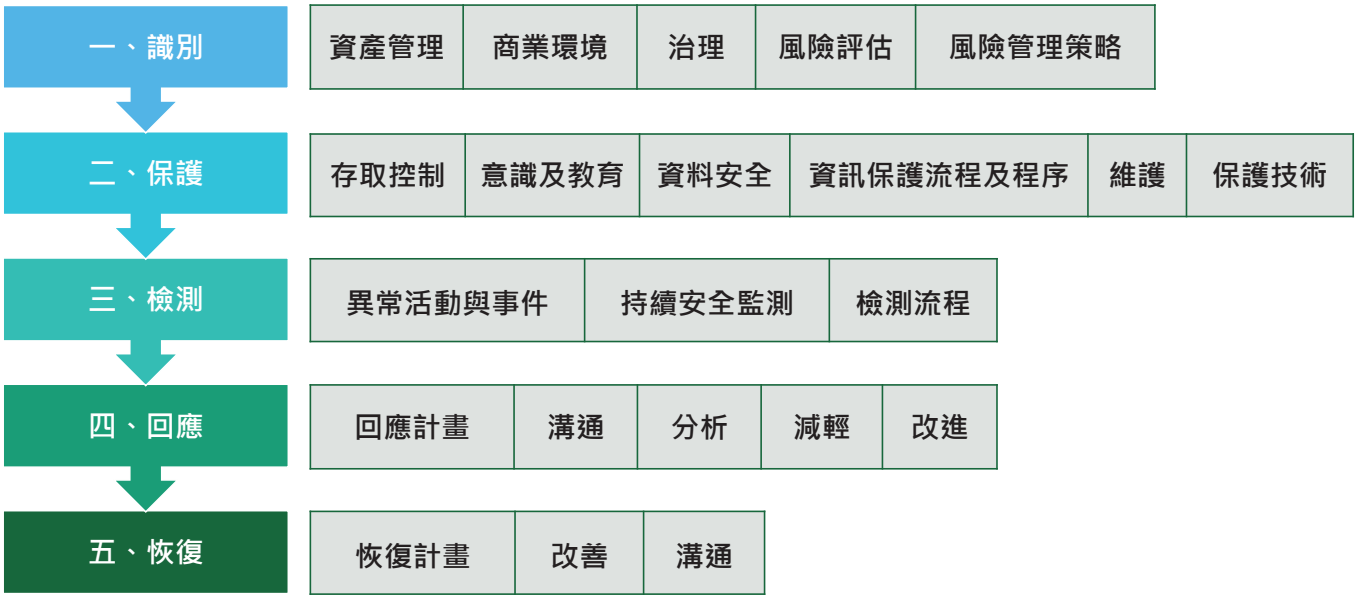
資通安全管理法實行細則§5

1.核心業務及其重要性	3.資安推動組織	5.營運持續管理	7.防護及控制措施	9.安全事件管理	11.持續改善
2.政策及目標	4.人力及經費	6.風險評估	8.系統委外管理	10.人員獎懲	

資安評估框架

電商系統資安成熟度分析

資安成熟度評估方法



電商系統資安成熟度評估

一、識別	控制項
1.1 資產管理	是否根據組織風險控管策略的相對重要性進行識別和管理和可以實現業務目的的資料、人員、設備、系統和設施
1.2 商業環境	理解組織使命、目標、及利害關係團體和組織活動;並定義資安人員其角色、責任和風險管理決策
1.3 治理	理解組織的規則、法規、風險、環境和營運要求的政策、程序和流程，並為管理層提供網絡安全風險相關資訊
1.4 風險評估	了解組織營運 (包括使命，職能，形像或聲譽)、組織資產的網路安全風險
1.5 風險管理策略	建立組織的風險管控優先次序、資源限制、風險容忍度並用於支持風險決策

電商系統資安成熟度評估

二、保護	控制項
2.1 存取控制	資訊資產和相關設施的存取權限止於授權用戶、流程、設備、授權的活動和交易
2.2 意識及教育	向組織的人員和合作夥伴提供網絡安全意識教育，並進行充分的培訓，以履行相關政策，程序和協議相一致的資訊安全相關職責和責任
2.3 資料安全	資訊和記錄的管理與組織的風險策略一致，以保護資訊的機密性，完整性和可用性
2.4 資訊保護的流程及程序	安全策略（涉及目的，範圍，角色，責任，管理承諾以及組織實體之間的協調），流程和程序均得到維護並用於管理資訊系統和資產的保護
2.5 維護	工業控制和資訊系統的維護和修復符合政策和程序
2.6 保護技術	管理技術安全解決方案以確保系統和資產的安全性和彈性符合相關政策、程序和協議

電商系統資安成熟度評估

三、檢測	控制項
3.1 異常活動與事件	及時發現異常活動並了解事件的潛在影響
3.2 持續安全監測	對資訊系統和資產進行不連續的監測，以確定網絡安全事件並驗證保護措施的有效性
3.3 檢測流程	檢測流程和程序得到維護和測試，以確保及時和充分地了解異常事件

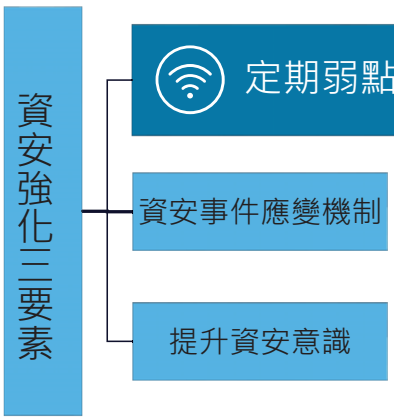
電商系統資安成熟度評估

四、回應	控制項
4.1 回應計畫	執行及維護回應的流程和程序，以確保及時響應檢測到的網絡安全事件
4.2 溝通	協調內外部的利害關係團體，並斟酌適當地納入外部法律機構的援助
4.3 分析	進行分析以確保充分回應並支持恢復活動
4.4 減輕	防止事件的擴大，減輕事件的影響並消除事件
4.5 改進	通過從當前和以往的檢測/回應活動中吸取的經驗來改進組織回應活動

電商系統資安成熟度評估

五、恢復	控制項
5.1 恢復計畫	執行維護恢復流程及程序，以確保受到網絡安全事件影響的系統或資產的及時恢復
5.2 改善	納入以往的經驗來改善恢復計畫及程序
5.3 溝通	恢復計畫均應納入：內外部組織，協調中心，ISP業者，資安事件應變小組，供應商...等

資安強化三要素

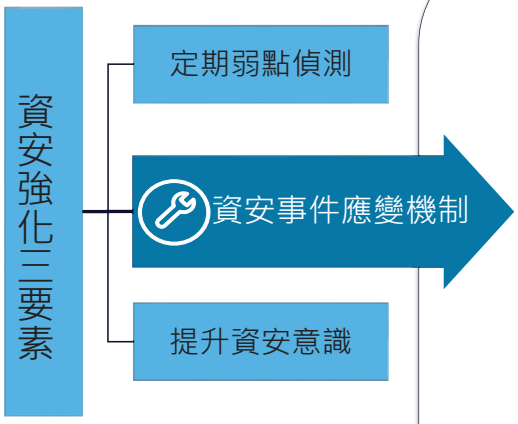


- **<u>滲透測試</u>**

  委託技術人員模擬駭客手法攻擊網路或主機，找出系統漏洞。

- **<u>弱點掃描</u>**

  使用工具進行掃描，以人工判斷、交叉比對分析數據，判讀風險對單位的影響程度。



- **資安事件通報程序**

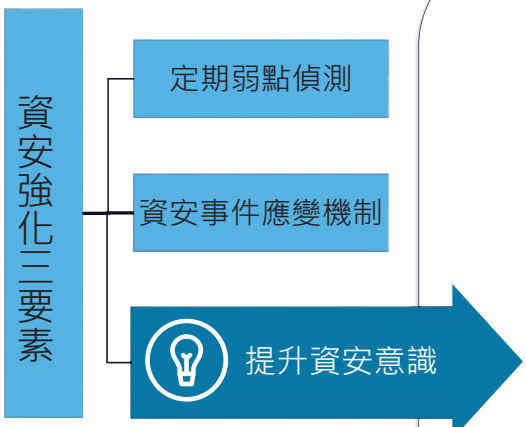
  建立適切管道盡速通報資訊安全事件。

- **資安事故回應程序**

  針對資安事故的類型、數量和損失，應建立可實施與監控的作法，以避免資安事故效應持續擴大。

- **營運持續計劃與演練**

  為確保業務活動減少所受到的影響，快速回復正常服務，以風險管理為基礎，建立切合組織業務與目標的營運持續計畫，並且依照適當的管理程序，定期測試與維護。



- **資安教育訓練**

  定期舉行資安認知教育訓練，提升組織內部基礎資安意識。

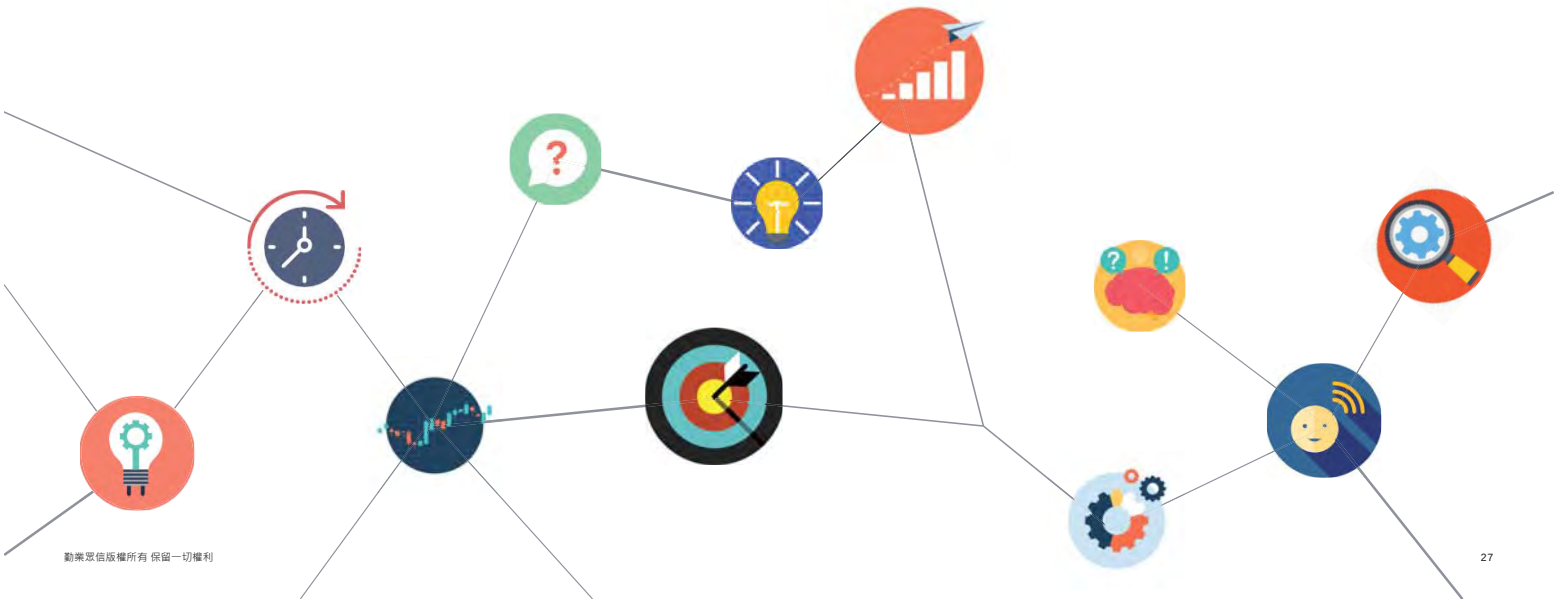
- **資安宣導郵件**

  針對近期重大資安事件，透過郵件加強資安意識宣導。

- **社交工程演練**

  由公司內部不定期發送釣魚郵件，以檢視同仁資安意識。

意見交流



Deloitte.

勤業眾信

About Deloitte
Deloitte 泛指Deloitte Touche Tohmatsu Limited(即根據英國法律組成的私人擔保有限公司，簡稱"DTTL")，以及其一家或多家會員所。每一個會員所均為具有獨立法律地位之法律實體。Deloitte("DTTL")並不向客戶提供服務。請參閱 www.deloitte.com/about 了解更多有關Deloitte及其會員所。

Deloitte為各行各業的上市及非上市提供審計、稅務、風險諮詢、財務顧問、管理顧問及其他相關服務。Fortune Global 500大中，超過80%的企業皆由Deloitte遍及全球逾150個國家的會員所，以世界級優質專業服務，為客戶提供因應複雜商業挑戰中所需的卓越見解。如欲進一步了解Deloitte約245,000名專業人士如何致力於"因我不同，惟有更好"的卓越典範，歡迎瀏覽我們的Facebook、LinkedIn、Twitter專頁。

About Deloitte Taiwan
勤業眾信(Deloitte & Touche)係指Deloitte Touche Tohmatsu Limited("DTTL")之會員，其成員包括勤業眾信聯合會計師事務所、勤業眾信管理顧問股份有限公司、勤業眾信財稅顧問股份有限公司、勤業眾信風險管理諮詢股份有限公司、德勤財務顧問股份有限公司、德勤不動產顧問股份有限公司、及德勤商務法律事務所。

勤業眾信以卓越的客戶服務、優秀的人才、完善的訓練及嚴謹的查核於業界享有良好聲譽。透過Deloitte資源整合，提供客戶全球化的服務，包括赴海外上市或籌集資金、海外企業回台掛牌、中國大陸及東協投資等。

Deloitte.

勤業眾信

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte Taiwan
Deloitte & Touche, the only member firm of Deloitte Touche Tohmatsu Limited in Taiwan (“Deloitte Taiwan”), is part of a broader network including Deloitte & Touche Consulting Co, Deloitte & Touche Tax Consulting Co., Ltd, Deloitte & Touche Financial Advisory Corp., Deloitte & Touche Risk Management Advisory Co., Ltd, Deloitte & Touche Real Estate Consulting Co., Ltd, and DTT Attorneys-at-Law.

The professional services provided by Deloitte Taiwan include timely updates on regulatory changes, enterprise risk management, integrated financial advisory services, and solutions to enhance competitive strength. Deloitte Taiwan holds a significant position in the market and provides globalized services and resources to help its clients in overseas IPOs, fund raising, listing in Taiwan by foreign issuers, IFRS compliance, China investment services, etc.

內容管理系統（CMS）的資安風險與工具檢測

中華電信數據通信分公司　林俊賢產品經理

內容管理系統(CMS)的資安風險與工具檢測

講師:林俊賢
lin.jsian@gmail.com

2018/06/22

經歷背景

現職

中華電信 資通安全處

經歷

亞洲搜尋行銷協會顧問

資策會 資安科技研究所

遠東銀行 資安部

刑事局科技犯罪防制中心

研發替代役

著作

網站入侵現場鑑證實錄

證照

Network Security of Packet Analysis，NSPA

EC-Council Certified Ethical Hacker，CEH v8

TQC-行動裝置應用程式設計認證(Android APP)

勞委會-軟體設計丙級、軟體應用乙級

參與活動

賽門鐵克 網路安全攻防戰(War Game)

103年行政院國家資通安全網路攻防演練 攻擊手

102年行政院國家資通安全網路攻防演練 攻擊手

研究領域

- 系統日誌檔分析
- 惡意程式分析(電腦/手機)
- 資安檢測
- 惡意中繼站追查
- 駭客入侵手法解析
- APP安全性檢測

著作–網站入侵現場鑑證實錄

於105年1月出版資訊安全專書「網站入侵現場鑑證實錄(ISBN:9789863478812)，出版社:碁峰」，其書籍主要是幫助企業資安、網管人員了解駭客入侵後所遺留下的數位證據來輔助分析，以找出駭客入侵手法後修補網站漏洞。

- 臉書社團
  https://www.facebook.com/groups/1730797680472868/

大綱

第一部分

- 資安現況
- 我國現行資安法規
- 電子商務業者面臨的資安
- 為什麼駭客鎖定電商

第二部分

- 常見攻擊手法(OWASP)
- 基本駭客攻擊介紹
- CMS介紹
- CMS風險
- CMS檢測工具

第三部分

- 解決方案
  - 事前:資安檢測
    定期做資安檢測
    弱點掃瞄與APT測試
  - 事中:資料保留
    相關設備日誌保留與稽核
  - 事後:補救措施
    建立消費者與公司補救方案
- 結語

第一部分

第一部分

- 資安現況
- 我國現行資安法規
- 電子商務業者面臨的資安
- 為什麼駭客鎖定電商

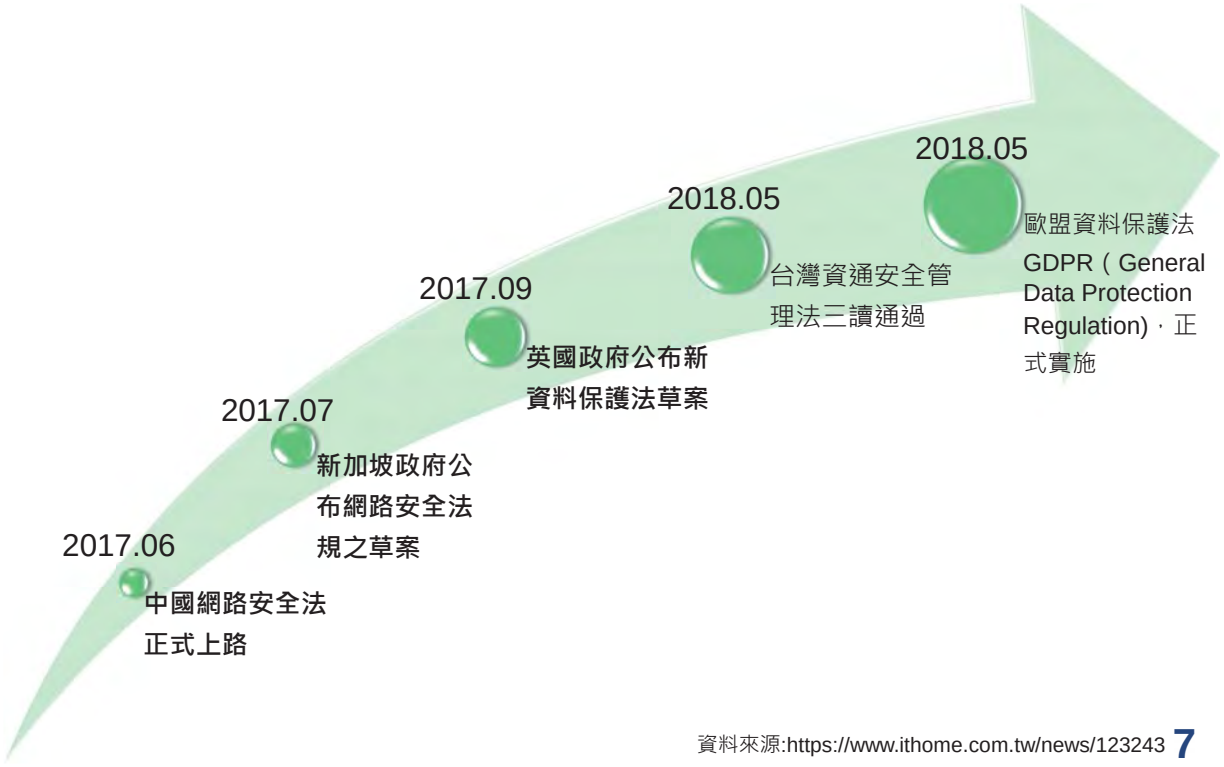
第二部分

- 常見攻擊手法(OWASP)
- 基本駭客攻擊介紹
- CMS介紹
- CMS風險
- CMS檢測工具

第三部分

- 解決方案
  - 事前:資安檢測
    定期做資安檢測
    弱點掃瞄與APT測試
  - 事中:資料保留
    相關設備日誌保留與稽核
  - 事後:補救措施
    建立消費者與公司補救方案
- 結語

資安現況

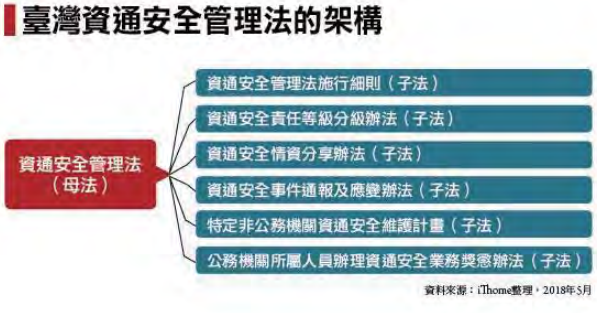


資料來源:https://www.ithome.com.tw/news/123243

我國現行資安法規

台灣資安法規三讀通過(2018.05.11)

- **建立明確資安制度，以讓各政府機關、各級產業間有遵循的制度。**
- **對各資安人員有明確的指標性法規可遵循。**



資料來源:
https://www.ithome.com.tw/news/123243
https://www.ithome.com.tw/news/123266

電子商務業者面臨的資安風險

駭客攻擊的主要趨勢:

1. **以APT進階持續性威脅 (Advanced Persistent Threat ，APT) 攻擊手法**
2. **以竊取個資為主要目的**
3. **以加入挖礦程式為主要營利目的**

為什麼駭客要鎖定電子商務平台

1. **因為，網站資安防護薄弱** ✓
2. **因為，擁有大量的會員敏感性資料** ✓
3. **因為，轉賣詐騙集團後更容易詐騙成功** ✓
4. **因為，事後獲利高** ✓

第二部分

第一部分	第二部分	第三部分

• 資安現況
• 我國現行資安法規
• 電子商務業者面臨的資安
• 為什麼駭客鎖定電商
	• 常見攻擊手法(OWASP)
	• 基本駭客攻擊介紹
	• CMS介紹
	• CMS風險
	• CMS檢測工具
		• 解決方案
		  • 事前:資安檢測 定期做資安檢測 弱點掃瞄與APT測試
		  • 事中:資料保留 相關設備日誌保留與稽核
		  • 事後:補救措施 建立消費者與公司補救方案
		• 結語

基本駭客攻擊介紹

弱密碼(weak password)
使用簡易或系統預設的密碼輕易登入管理者頁面(如:admin、123456、p@ssw0rd)

暴力破解(brute force)
利用大量字典檔去運算組合常見的密碼規則，藉此找出管理者設定的密碼

資料庫隱碼攻擊 (SQL injection)
在輸入的字串中，塞入有關SQL的字元送至後端資料庫認證時，讓資料庫發生異常，以繞過認證機制取得權限(如admin ‘or 1= ‘1)

釣魚網站(Phishing)
製作與原先頁面極類似的網站，並誘導使用者點擊不明連結後，騙取輸入帳號密碼

基本駭客攻擊介紹

目錄穿越攻擊(Directory Traversal)
因伺服器設定不完善，導致網頁目錄結構出現可利用特殊字元的代碼(../)，穿越過正常一般的目錄設定後，未經授權存取至後端伺服器環境

ASP、PHP後門(WebShell)
利用網站上傳功能，上傳偽裝後的檔案格式，例如將*.asp改成*.asp;.jpg格式，騙取系統檢查機制

滲透測試(Penetration Test)
以駭客工具來測試網站找出漏洞或傳送方法(GET/POST)不安全機制，最後加以利用，以達到駭客預期的攻擊效果

Google hacking
在搜尋引擎中下達特殊字元(如:index of，INURL:admin，FILETYPE:php)來找出網頁中可能隱藏的敏感訊息，而被搜尋引擎建立索引的內容

常見攻擊手法(OWASP)

1 Injection 注入攻擊
包括所有的SQL、NoSQL、作業系統以及LDAP的注入攻擊，通常會發生在惡意的程式語法在輸入時，沒有經過妥善的檢查和驗證所造成的資安風險

2 Broken Authentication 失效的身份認證
許多應用程式經常需要處理身分認證及Session管理，但導入方式若不正確，反而可能會讓駭客取得密碼、金鑰、Session令牌，或者是利用其他導入時的錯誤疏失，暫時或永久取得使用者的身份資訊

3 Sensitive Data Exposure 敏感訊息洩漏
主要是因為不少網路應用程式對於金融資訊、健康資料及個人資料的保護不足，若遭當駭客取得，就可以進行信用卡詐欺、身份竊取或是其他的犯罪行為等。因此，針對敏感性資料去需要做額外的保護措施，例如不使用或傳送時的資料必須加密，或者是瀏覽器瀏覽時，也必須要特別注意

4 XML External Entities (XXE) 微軟平臺XML外部處理器漏洞
微軟平臺在處理很多XML語法時，沒有做好相關權限保護而造成機敏資料外洩的風險
許多以XML為基礎的應用程式或網路服務，沒有管控權限，直接接受XML語法的請求（Request）或上傳（Upload），此時，只要插入一個惡意XML文件，就能鎖定XML處理器漏洞攻擊，而有資料外洩的風險
XML編碼的SOAP（Simple Object Access Protocol，簡單物件存取協定）訊息，是可被第三方用來簡化網頁伺服器訊息傳遞的標準化格式
因為SOAP 1.2版之前的XML編碼沒有寫好，所以，只要使用SOAP 1.2版的訊息交換格式，預設都有XML外部處理器漏洞（XXE）的風險，這也意味著這樣的Web服務，容易遭受到DoS（阻斷式服務）攻擊

常見攻擊手法(OWASP)

資料來源:
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
https://www.ithome.com.tw/news/118411

5	Broken Access Control 無效的存取控管	藉由嚴格的存取控管，降低駭客利用這些漏洞去存取沒有經過授權的功能或察看敏感資料、修改使用者數據、更改訪問權限等
6	Security Misconfiguration 不安全的組態設定	經常是使用不安全的預設值，或者是錯誤配置像是HTTP標頭或者是系統顯示的錯誤資訊已經包含敏感性個資所造成的，除了要安全設定所有作業系統、框架、函示庫以及應用程式外，更必須做到系統更新與升級，以確保系統安全與時並進
7	Cross-Site Scripting (XSS) 跨站腳本攻擊	主要就是發生在，當應用程式缺乏適當的驗證，如允許網頁可出現不可信任的資訊時，或者是允許在使用者瀏覽器中執行腳本程式，恐導致有心人士劫持使用者Session、網頁置換或者是轉址到其他惡意網站等
8	Insecure Deserialization Java 平臺不安全的反序列化漏洞	常見的攻擊方式，除了會導致遠端程式碼執行（RCE）外，也可能成為駭客發動攻擊的工具，例如重播攻擊（Relay Attacks）、注入攻擊（Injection Attacks）以及特權升級攻擊（Privilege Escalation Attacks）等
9	Using Components with Known Vulnerabilities 使用已知漏洞的套件	這些元件包括函示庫、框架以及其他的軟體模組，而元件會和應用程式以相同的權限執行。如果有一個容易受到攻擊的元件被駭客利用，就可能會導致嚴重的資料儀式或者伺服器被駭客接收，而使用有漏洞元件的應用程式或者是API，都會破壞應用程式的防護並啟用各種攻擊形式
10	Insufficient Logging & Monitoring 紀錄與監控不足風險	系統監控與紀錄的不足，缺少有效率的整合事件回應功能，造成駭客進一步攻擊目標系統後轉向更多系統作攻擊。通常要超過二百天以上，使用者才可能察覺到有資料外洩事件發生，而這樣的資料外洩，通常也都不是透過內部的監控系統發現，往往是從外部才會發現到資料外洩的事實

主流CMS介紹

提供多種免費且快速的架站平台

是目前免費架站平台的主流

- **Joomla!**
- **Drupal**
- **WordPress**

CMS風險

比較CMS易用特性與資安風險

CMS易用特性	CMS資安風險
1. 使用者架站快速容易 2. CMS提供常見模組 3. 行銷人員易增加行銷曝光度 4. 網站擁有大量會員個資 5. 初學者不懂程式也可以營運 6. 經營者對資安較無概念	1. 網站程式碼開放特性，易遭駭客研究可利用漏洞 2. 架站平台與伺服器版本過舊且無專人作系統更新與驗證 3. 使用者不熟悉操作功能與後續資安影響 4. 使用者對於網站Robots.txt規範不完全 5. 易遭駭客猜中預設admin管理平台進而攻擊 6. 系統被發掘0day漏洞後，無資安人員進行系統更新

CMS檢測工具

免費漏洞檢測工具:

平台類型與檢測工具	Joomla!	Drupal	WordPress
自建版	joomscan	Drupwn	wpscan
SSL掃瞄	A2SV-Auto Scanning to SSL Vulnerability https://github.com/hahwul/a2sv		
Port scan	Nmap https://nmap.org/		

CMS檢測工具

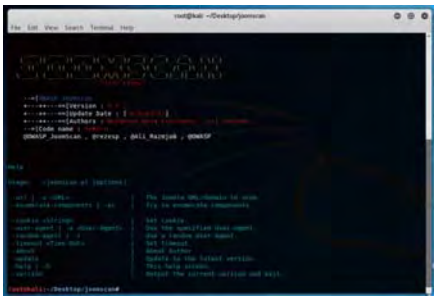
Joomla!

Joomscan

- 針對Joomla平台進行常見模組檢測

官方網址:

- https://github.com/rezasp/joomscan



CMS檢測工具

Joomla! scan online

提供線上掃瞄服務，以利即時確認Joomla! 系統安全性

優點:

- 線上提供新的檢測模式，以容易檢測出漏洞

缺點:

- 目標平台遭檢測後的結果有可能被第三方單位所紀錄下來
- 使用者對檢測過程完全不熟悉

檢測網站:

- https://hackertarget.com/joomla-security-scan/

CMS檢測工具

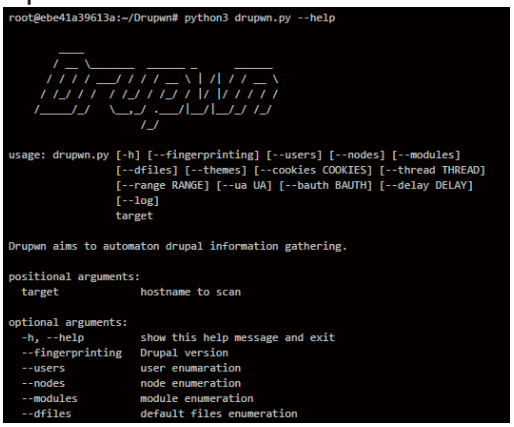
Drupal scan 自建平台

Drupwn

- 針對Drupal平台進行常見模組檢測

官方網址:

- https://github.com/immunIT/drupwn



CMS檢測工具

Drupal scan online

提供線上掃瞄服務，以利即時確認Drupal系統安全性

優點:

- 線上提供新的檢測模式，以容易檢測出漏洞

缺點:

- 目標平台遭檢測後的結果有可能被第三方單位所紀錄下來
- 使用者對檢測過程完全不熟悉

檢測網站:

- https://hackertarget.com/drupal-security-scan/

CMS檢測工具

WordPress scan online

提供線上掃瞄服務，以利即時確認WordPress系統安全性

優點:

- 線上提供新的檢測模式，以容易檢測出漏洞

缺點:

- 目標平台遭檢測後的結果有可能被第三方單位所紀錄下來
- 使用者對檢測過程完全不熟悉

檢測網站:

- https://wpscans.com/
- https://hackertarget.com/wordpress-security-scan/

CMS檢測工具

WordPress scan 自建平台

官方網址:

- **https://wpscan.org/**
- **https://github.com/wpscanteam/wpscan**

CMS檢測工具

專業漏洞檢測工具:

- **網站漏洞掃瞄(Acunetix Vulnerability Scanner)**
  - 該檢測工具含有各種檢測模式及常見CVE弱點程式模式，支援不同網站類型進行弱點掃瞄並作風險評估，並產出相對應報表，具有一定的水準。
- **系統弱點掃瞄(Nessus)**
  - 知名的系統檢測工具，可針對伺服器的版本進行檢測，發掘出尚未修補的漏洞或有重大的資安風險進行評估，並產出相對應報表。

ROBOTS.TXT與SECURITY.TXT

robots.txt

- 告知搜尋引擎那些目錄是允許被爬取，反之哪些是不允許的。
- 但容易成為被有心駭客利用找隱藏敏感目錄的手法

security.txt

- 當白帽駭客找出目標網站漏洞時，藉以通知該網站聯絡人的一種方式
- 參考網址:https://securitytxt.org/

第三部分

第一部分	第二部分	第三部分

• 資安現況
• 我國現行資安法規
• 電子商務業者面臨的資安
• 為什麼駭客鎖定電商
	• 常見攻擊手法(OWASP)
	• 基本駭客攻擊介紹
	• CMS介紹
	• CMS風險
	• CMS檢測工具
		• 解決方案
		  • 事前:資安檢測 定期做資安檢測 弱點掃瞄與APT測試
		  • 事中:資料保留 相關設備日誌保留與稽核
		  • 事後:補救措施 建立消費者與公司補救方案
		• 結語

解決方案
事前:資安檢測

定期做資安檢測

- **弱點掃瞄**
  - 業者應針對自身的營運平台作好事前預防，定期檢測平台弱點並作即時修補，以防止漏洞遭利用後擴大災情。
- **APT郵件測試**
  - 針對需面對客戶的信件往來之業務人員或主管，應建立相關檢測制度，以防遭駭客攻擊：

1. 定期實施APT電子郵件測試模擬。
2. 建立不點擊來路不明之郵件之反射動作。
3. 若有**附加檔案**需開啟，則可轉至內部特殊環境下開啟。

解決方案
事中:資料保留

相關設備日誌保留與稽核

需建立一套標準保留各種日誌系統之流程

- **針對存取敏感個資的軟體**
  - 例如:處理各不同電子商務平台之客戶下訂軟體，是否會去除客戶敏感性資料後產生日誌。
- **針對一般營運平台**
  - 例如:客戶個資處理完畢後保留期限、存取客戶檔案之系統紀錄、人員存取敏感性資料權限控管等。

解決方案
事後:補救措施

建立消費者與公司補救方案

- **明確通知消費者勿遭受詐騙之訊息，以多重方式善盡告知責任**
  - 官方網站於明顯處放置防詐騙之宣傳公告。
  - 以近期遭詐騙消費者購買商品之時間區段作電子郵件或手機簡訊之公告。
  - 或於官方APP上推播通知防詐騙訊息。
- **盡速尋找資安團隊進行全面性資安健診**
  - 檢測各系統平台是否有遭駭客入侵痕跡
  - 全力配合執法單位的後續調查

結語

- 各國將資安列為主要法規已是國際間的趨勢，我國各企業應需建立資安制度，以確保企業制度完整。
- 各企業應培養內部專業資安人材並視為主要投資，以防範未來遭受駭客攻擊後面臨的損失。
- 各企業內部作業流程或系統開發流程應參考相關資安規範，擬定執行政策，以符合後續資安稽核與資安法規。
- 各企業應落實建立資安處理程序3步驟，並定期自我實施與檢視，並改善不足之處。
- 當企業面臨駭客攻擊所造成損害時，應立即尋求可協助的管道及依法規立即通報政府單位，併請專業資安團隊立即作全面性的安全檢測。

其他問題

關於本次的演講有什麼問題?

- 歡迎寄信詢問
- 歡迎填寫問卷

網際網路零售業因應歐盟GDPR之個資暨資安法遵建議

資策會科技法律研究所

蔡淑蘭副分析師

107年度網路購物產業價值升級與環境建構計畫
網際網路零售業資安防護推廣
【商譽優先！網路開店系統的選擇指南】

網際網路零售業因應歐盟GDPR之個資暨資安法遵建議

簡報人：蔡淑蘭
職稱：法律研究員
財團法人資訊工業策進會
科技法律研究所
2018.06.22

大綱

1. 前言
2. 歐盟通用資料保護規則(GDPR)法遵要求
3. 電商面臨個資暨資安挑戰與因應建議
4. 結論與意見交流

創建線上個人身材模型，試衣間無處不在

AI

最貼心的服務背後是？

VR

Big data

人臉辨識

生物辨識

圖片來源：https://www.freepik.com/free-vector/hipster-character-pack_1536714.htm?utm_campaign=flaticon&utm_medium=banner

資料來源：http://startuplatte.com/2017/07/13/understanding-customer-behavior/

個資侵害？

大量個人資料的利用

個資保護規範

大綱

1. 前言
2. 歐盟通用資料保護規則(GDPR)法遵要求
3. 電商面臨個資暨資安挑戰與因應建議
4. 結論與意見交流

GDPR規範架構綜覽

- 總則
- 個人資料處理原則
- 資料主體之權利
- 控管者與處理者的責任
- 個資移轉至第三國或國際組織
- 獨立監管機關
- 合作與一致性
- 救濟務與處罰
- 個人資料的特殊處理規範

GDPR基本原則篇

GDPR個資定義

一般個資

「個人資料」係指得以直接或間接地識別該自然人之任何資訊。例如姓名、識別碼、位置資料、IP/cookie 。

特種個資

種族、政治意見、宗教哲學信仰、參與工會、基因、生物特徵資料、有關健康的資料、性生活或性取向。

GDPR適用範圍

➢**域外適用效力（Article 3）**

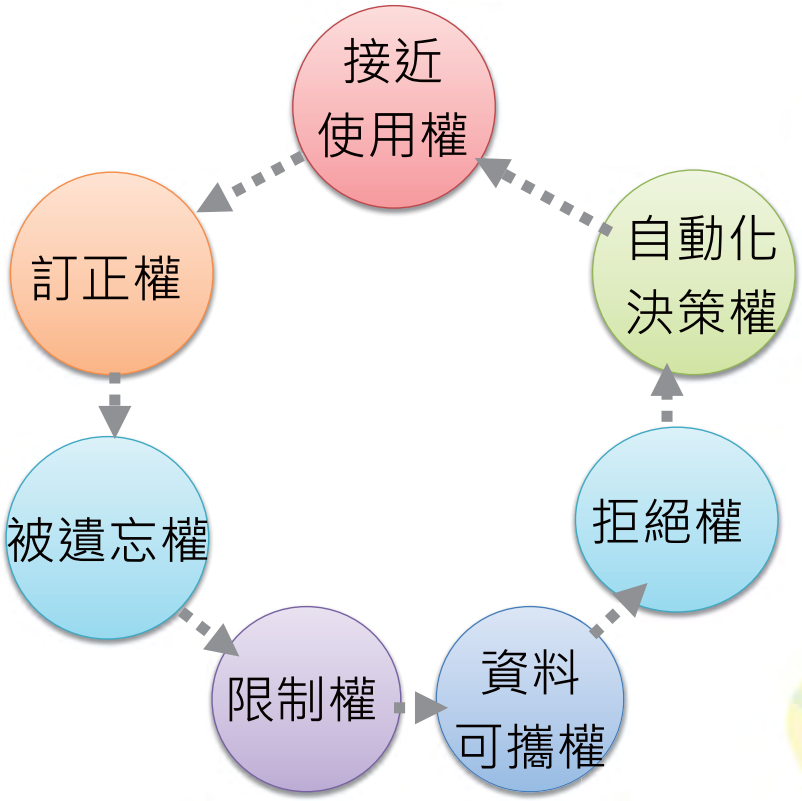
✓無論企業是否位處歐盟境內，凡跨境提供商品或服務，並蒐集處理歐盟居民個人資料，應適用之。須在歐盟境內指派代表。

控制者或處理者	域內行為	域外行為
歐盟境內企業	V	V
歐盟境外設立企業	★ 1.對歐盟境內人民提供商品或服務（無論是否有償） 2.監控其於歐盟境內活動之行為	
歐盟境外設立企業（控制者）	V 依國際公法原則適用成員國法適用之	

GDPR之六大原則

GDPR資料主體權利篇

資料主體權利



GDPR企業責任篇

GDPR要求的企業責任

罰則加重(1/2)

◆最高可處1,000萬歐元或前一年度全球營業總額2%的罰款，取其金額較高者：

罰則加重(2/2)

◆最高可處2,000萬歐元或前一年度全球營業總額4%的罰款，取其金額較高者：

GDPR跨境傳輸

GDPR跨境傳輸原則(1/2)

GDPR跨境傳輸原則(2/2)

例外允許

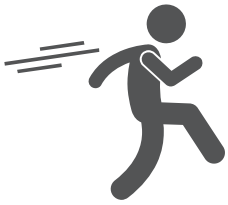
1. 歐盟以外國家/地區取得適足性認定
2. 企業自主採行符合規範之適當保護措施
3. 其他例外情形

- 標準個資保護契約條款（Standard Contractual Clauses）
- 拘束性企業規則（Binding Corporate Rules）
- 行為守則（Codes of Conduct）
- 取得認證（Certification）

大綱

1. 前言
2. 歐盟通用資料保護規則(GDPR)法遵要求
3. 電商面臨個資暨資安挑戰與因應建議
4. 結論與意見交流

電商面臨的GDPR法遵挑戰與因應



個資法遵要求太多或不需適用GDPR

從國內個資法遵要求做起，逐步增加GDPR要求

未掌握保有個資之處理移轉狀況

全面盤點並掌握企業保有之個資處理與移轉狀況

無法決定法遵對策實施的順位

分析現況與法遵落差，考量成本，以決定實施優先序、對應方針與措施

法遵措施增加營運成本

GDPR法遵要求非一次到位，可逐年編列預算改進

電商面臨的GDPR實務挑戰與因應(個資篇)

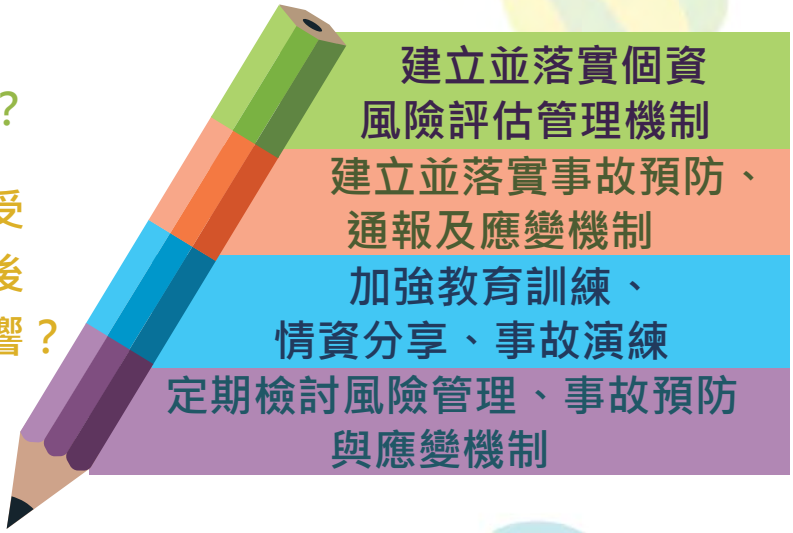
個資侵害的行為態樣？

個資侵害的類型與發生原因？

個資受侵害後的影響？

如何預防與應變個資受侵害？

如何避免侵害再度發生？



電商面臨的GDPR實務挑戰與因應(資安篇)

資安措施要求的參考指南或作法？

不使用ISO標準，如何證明符合GDPR？

歐盟中小企業個人資料處理安全指南可作為參考

中小企業個人資料處理安全指南(Guidelines for SMEs on the security of personal data processing)連結：
https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

電商面臨的GDPR實務挑戰與因應(資安篇)

資料加密後，可排除GDPR適用？

資安需求控制清單可協助檢視遵循GDPR？

審查解密技術，以評估資料被解密的合理可能性是否符合匿名化的要求

控制措施因組織而異，建立並落實風險評估管理機制

大綱

1. 前言
2. 歐盟通用資料保護規則(GDPR)法遵要求
3. 電商面臨個資暨資安挑戰與因應建議
4. 結論與意見交流

結論

◆GDPR法遵挑戰之因應建議

➢從國內個資法遵要求做起，逐步落實GDPR要求

◆GDPR實務挑戰之因應建議

➢個資篇

✓落實並定期檢討組織的風險管理、事故預防與應變機制。

✓加強教育訓練、情資分享、事故演練。

➢資安篇

✓歐盟中小企業個人資料處理安全指南(Guidelines for SMEs on the security of personal data processing)可作為組織性與技術性安全措施參考。

✓建立並落實風險評估管理機制，訂定合適的資安控制措施。

GDPR服務項目

法遵協助

- 企業GDPR內控與法遵因應
- 相關流程、文件及表單整備

教育訓練

- GDPR修法重點
- GDPR重要發佈文件解析等
- 跨境資料傳輸或其他特定議題

諮詢服務

- 個資法律、資安及管理專業諮詢服務
- 制度建置協助
- 外部驗證檢視


蘇律師


林經理


楊博士
(法律)


蔡研究員
(資安)

TEL：02-6631-1000

意見交流

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

商譽優先！
網路賣家的資安旅程

CloudRiches雲馥數位

王育民技術總監

網路賣家的資安旅程

CloudRiches
Dino Wang
Microsoft Partner

Agenda

- 資安內控
- 安全賣場

網路安全隱憂

- 個資、交易資料外洩，網路詐騙案件頻傳
- 平台經常為攻擊重心
- 安全隱憂層出不窮
- 特定對象癱瘓網站疑似報復行為

宏碁美國電子商務網站遭駭客入侵!!
105/6/20

可樂旅遊被駭洩個資
訂票民眾遭詐騙數萬元 106/4/14

駭客入侵！證券市場首次遭大規模攻擊
勒索市值31萬比特幣!!
106/02/3

駭客入侵美國信調機構 Equifax，
超過 1.43 億消費者個資、信用卡
資訊外洩
106/9/8

ＸＸ美國電商網站遭駭客入侵!!

遭駭客竊取的資訊包括用戶姓名、地址、信用卡號碼、有效截止月年，以及安全檢核碼等。至於用戶在該網站上的登入密碼、美國社會安全碼等資訊，則並未落入駭客手中。

Ｘ旅遊被駭洩個資　訂票民眾遭詐騙數萬元

旅行社說，11日開始接獲民眾反映，部分資料確實被駭客竊取，包括出遊行程、訂票價格、姓名身分證等細節，詐騙集團都掌握清楚，已經協助消費者處理後續，配合檢警調查，但是否賠償被詐騙的民眾，目前無法做出承諾。

用什麼角度看電商資安

- 作為開發者，檢視還沒做的工作
- 作為管理人員，建立基礎概念與工具認識
- 作為採購人員，資安工作責任的範圍定義

選擇平台的資訊來源

- 如何選擇一個相對安全的開店軟體或平台
  - 資安事件少
  - 回應速度快

選擇平台的資訊來源

- 運用搜尋技巧交叉比對
  - 網址搜尋法 + 產品介紹頁面
  - https://www.miniinthebox.com
  - http://www.business-arena.ro

資安內控

作業資料的保護

問個問題，這些資料需要怎麼樣的保存？

- 信用卡號

- 密碼

作業資料的保護

這些資料需要怎麼樣的保存？

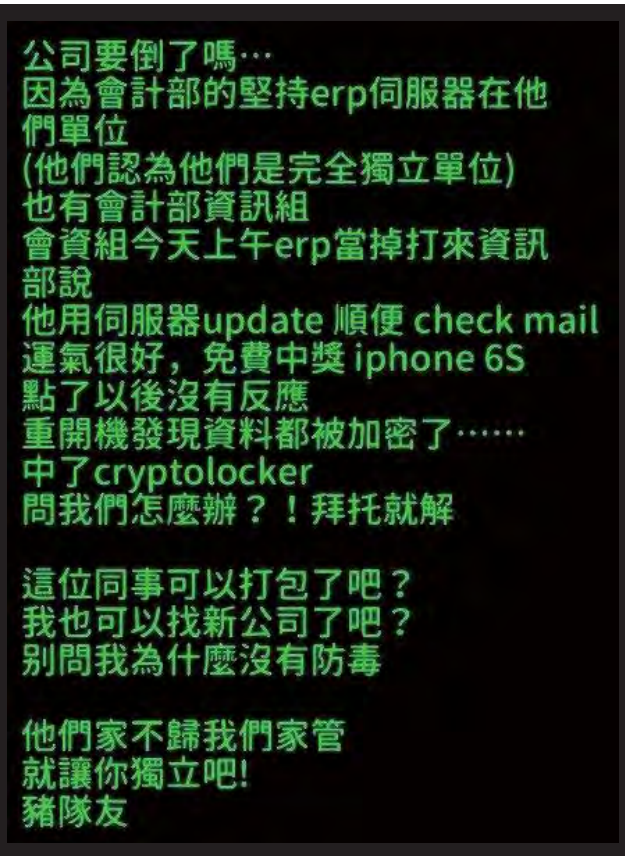
- 信用卡號
  - 透過第三方金流或 3D 驗證了為什麼需要保存用戶信用卡號？
- 密碼
  - 密碼加密、加鹽

資料保存期

考慮交易資料該保存多久？

- 個資
  - 電話、身分證、詳細地址
- 訂單
  - 三個月、六個月？
  - 離線存放？

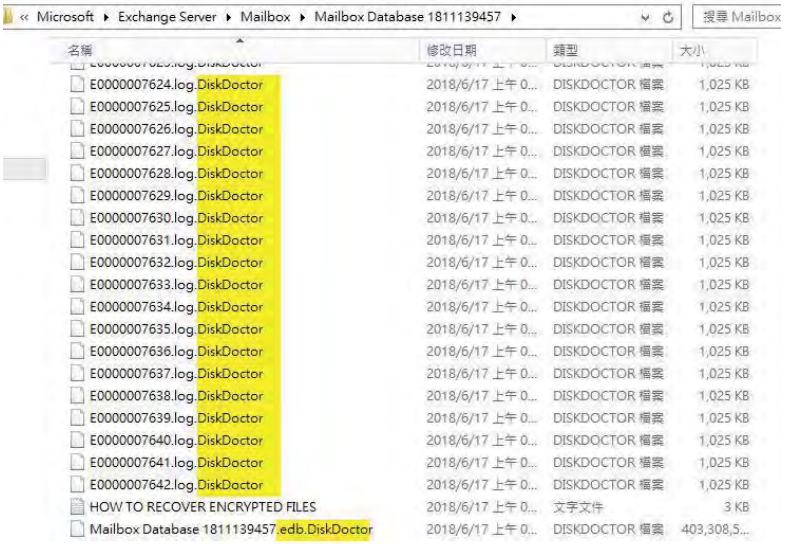
慘劇



資料來源：靠北工程師

盛行的加密勒索 Ransomware

- WannaCry
- DiskDoctor
- CryptoLocker
- TorrentLocker
- ...



盛行的加密勒索 Ransomware

- 被加密了，沒有更快的解決方式 ...
- 由內部發起的硬碟被加密悲劇，有可能接二連三的發生
- 未來如何防杜加密勒索？

從內部發動攻擊

- 如何防範？
  - 連結
  - 釣魚信件
- 如何杜絕？
  - 備份
  - 委外、託管、或採用 軟體即服務 (SaaS)

如何防範被從內部攻擊

內部攻擊的發起，通常因內部工作機執行代理程式，或被綁架由外部操控惡意軟體發動攻擊，其來源可能有：

- 釣魚信件、惡意軟體
- 不安全的網路環境

如何防範被從內部攻擊

- 釣魚信件
  - 不隨意接受與點擊信件中的連結
  - 在沙箱引爆（沙箱為虛擬機器模擬電腦開啟附件）
- 惡意軟體
  - 不使用來路不明的應用程式
  - 安裝可信賴的防毒

如何防範被從內部攻擊

- 不安全的網路環境
  - 軟體或硬體防火牆
    - 透過存取控制界定出可信任的網路存取行為

Windows 防火牆的保護範圍相對的小，用來保護以及限制個人電腦

自有開發團隊的考量點

自行開發可能有的風險

- 產生特殊的破口，無法為工具所識別

程式碼品質掃描 Quality

程式碼品質是白箱測試針對原始碼進行脆弱點的偵測

- 寫作是否符合規範
- 檢查可能的臭蟲
- 檢查可能出現的漏洞

例如：SonarQube

OWASP

- Open Web Application Security Project

  開放網路應用程式安全專案

  OWASP 是一個由全球超過 4 萬名義工共同參與的非營利組織，

  主要是針對各種網頁安全漏洞提出各種研究成果。

- OWASP Top 10 Project

OWASP
Open Web Application
Security Project

OWASP Top 10 2017

① 注入攻擊
(Injection)

② 無效的身份認證
(Broken Authentication)

③ 敏感資料外洩
(Sensitive Data Exposure)

④ XML 外部處理器漏洞 NEW
(XML External Entity, XEE)

⑤ 無效的存取控管
(Broken Access Control)

⑥ 不安全的組態設定
(Security Misconfiguration)

⑦ 跨網站腳本攻擊
(Cross-Site Scripting, XSS)

⑧ 不安全的反序列化漏洞 NEW
(Insecure Deserialization)

⑨ 使用已有漏洞的元件
(Using Components with Known Vulnerabilities)

⑩ 記錄與監控不足風險 NEW
(Insufficient Logging and Monitoring)

OWASP Top 10 2017

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

跨網站腳本攻擊 XSS

- 通常用來盜取網站使用者的登入階段身份

加強防護

- 我們無法確保網站在資安方面上的縝密考慮，因為
  - 促銷活動是一檔一檔的推，每一個時程是短促的
  - 對外，對內網站也需要逐一照顧，每一個改版都是重新的檢核
- 最佳的做法是在應用程式之外架設保護層

加強防護

- WAF (Web Application Firewall) 與網頁應用程式的防護力
  - Injection (SQL Injection)
  - XSS

- 建置分為
  - 軟體版本，適合雲端和地端
  - 硬體版本，適合地端

滲透測試

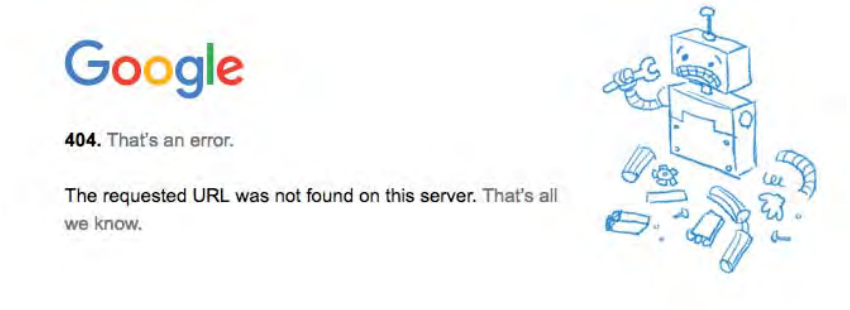
具備資安知識與經驗、技術人員受僱主所託，為僱主的網路設備、主機，模擬駭客的手法對網路或主機進行攻擊測試，為的是發掘系統漏洞、並提出改善方法。

也有提供漏洞回報的公開平台，如 https://zeroday.hitcon.org/

網站連結斷裂 Broken Link

網站動不動就出現壞掉的連結，也是損害服務品質的脆弱點

- 運用工具自動化檢查網站中連結的有效性
  - 例如：LinkChecker



Thanks