Retail Cyber Security – Are You at Risk?

零售網絡安全 - 你是否處於風險中？

We live in a connected world that offers unrivalled convenience, efficiency and access to information. With this connectivity, however, comes threats. Recently the retail industry has been a prime target for cyber-attacks. Retail cyber security is essential to guard against hackers and it is critical that retailers know the risks they face and how to protect themselves against attacks.

我們所生活的世界互相聯繫，令我們享受到前所未有的方便和效率，更可輕鬆獲取資訊。然而，這種聯繫亦帶來威脅，最近零售業就成為了網絡攻擊的主要目標。零售網絡安全對於防範黑客來說非常重要，零售商必須了解他們面臨的風險，並學會如何保護自己免受攻擊。

Why are retailers a prime target for cyber-attacks?

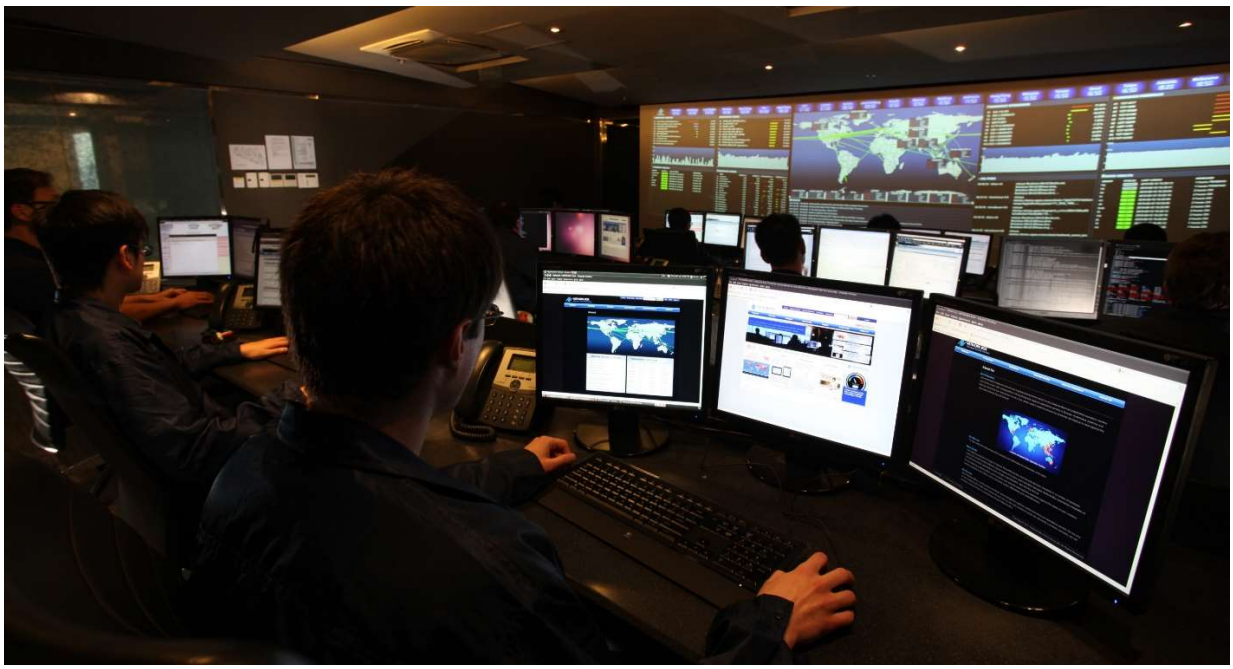
為何零售商會成為網絡攻擊的首要目標？

Retailers are targeted for cyber-attacks due to the rapid expansion of e-commerce. As part of their regular operations, retailers operating online portals store personally identifiable information (PII), including customers' names, addresses and card numbers, for payment processing and marketing purposes. The practice is no doubt convenient as customers can shop and purchase quickly and easily, and retailers can make their marketing efforts more targeted. But then the price to pay for delivering a hassle-free and personalised shopping experience is exposure to cyber security. Combined with the increased use of cloud-based systems and web applications, e-retailers could become easy pickings for hackers.

Many retailers also see cyber security as an added cost because the development, testing and maintenance of solid network security measures takes time and manpower. They are reluctant to erode the bottom line, but this way of thinking could prove costlier down the road.

零售商成為網絡攻擊的首要目標，主要是因為電子商務的快速擴張。作為正常業務過程的一部分，經營網上門戶網站的零售商會儲存顧客個人資料。一方面，這令逛街購物變得更輕鬆快捷，方便了顧客，而另一方面，零售商可更有效地針對營銷目標。然而，這些方便亦意味著網絡安全可能被人乘虛而入，加上越來越多人使用雲端系統及 web 應用程序，使其容易成為攻擊目標。

由於開發、測試和維護穩固的網絡安全措施需要時間及人力，繼而影響到盈虧，所以不少零售商均將網絡安全視為一項額外成本，可是這種思維方式在日後可能會換來更大代價。



What are the risks in retail cyber security?

Data is now one of the most valuable commodities, and retailers have plenty of it. They also deal with a large volume of traffic, especially during peak sales periods such as Christmas, Black Friday and Golden Week. The high traffic could be exploited by hackers as a cover for cyber-attacks.

Exposing customer or other important company information to theft or ransom is not only financially damaging but also potentially disastrous for brand reputation. Worse still, the compromised information could lead to identity theft, follow-on fraud and further phishing campaigns. This is a sure way to lose consumers' trust and turn them away from an e-commerce portal permanently.

Most common cyber-attacks in the retail industry

According to the 2019 Verizon Data Breach Investigations Report (DBIR), most retail cyber-attacks target web applications, trying to access the server to obtain customers' payment data for the perpetrators' financial gain. As stated in the report: " The number of physical terminal compromises in payment card-related breaches is decreasing when compared to web application compromises.

Attacks against e-commerce payment applications are satisfying the financial motives of the threat actors targeting this industry."

Top cyber-attack methods include malware (particularly through third-party applications), hacking and phishing. Cloud-based Internet of Things (IoT) devices connected to a network such as CCTVs, POSs and payment terminals are at risk in particular due to the sheer number of potential access points, often outdated firmware, configuration errors or bugs.

零售網絡安全的風險何在？

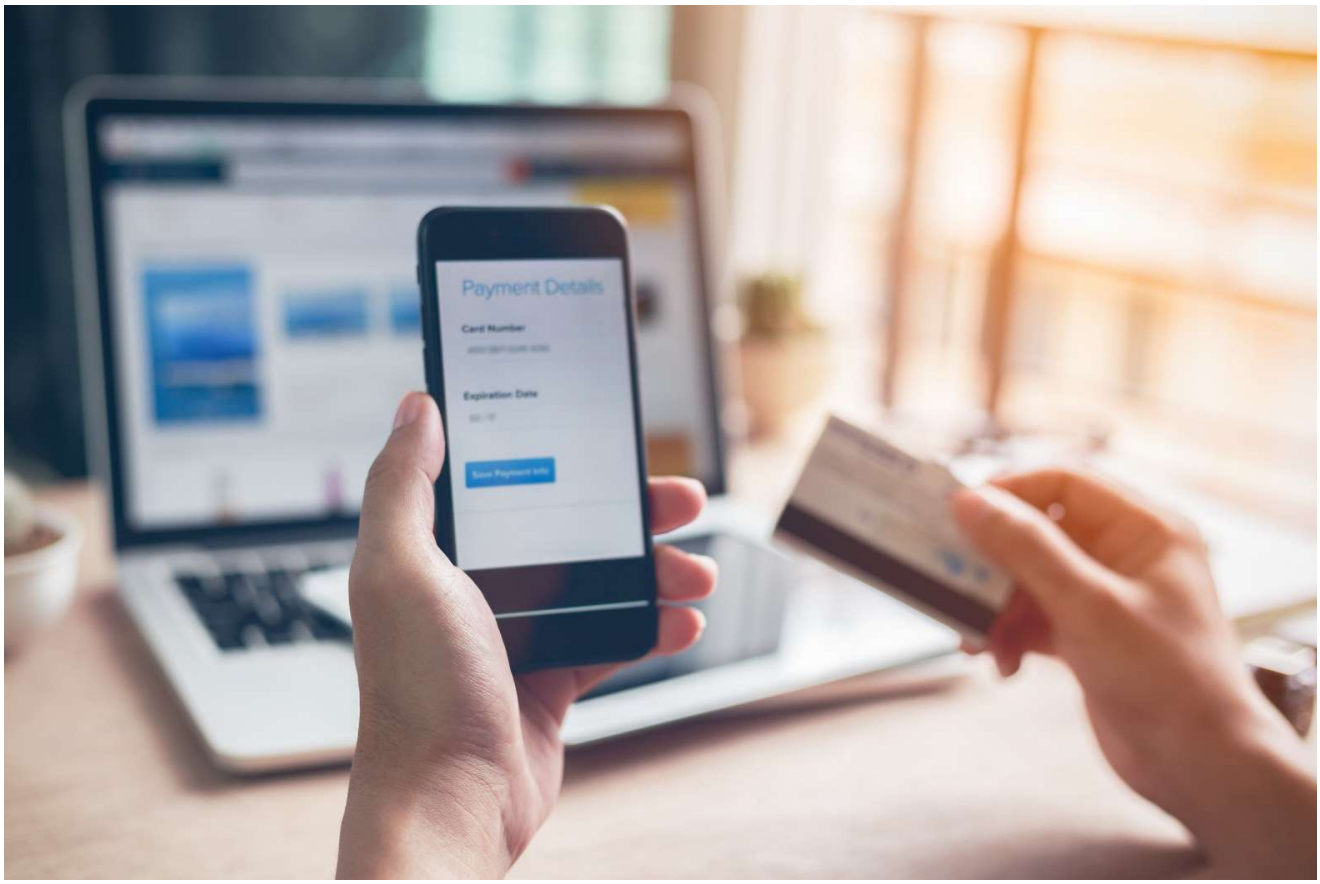
數據是最具有價值的商品之一，零售商會儲存並獲取大量數據，尤其在購物高峰期，流量甚至更多。黑客偶爾就會把這些數據當作網絡攻擊的掩護。

當然，客戶資訊或其他重要的公司資料遭盜竊或勒索，招致的後果不僅是經濟損失，更甚者可能為品牌聲譽帶來災難性影響。資料更可能被人用來盜用身份、詐騙和其他網絡釣魚活動。

最常見的零售業網絡攻擊

根據 Verizon「2019 年數據洩露調查報告」(DBIR)，大部分零售網絡攻擊的攻擊對象都是 web 應用程序，不法之徒會試圖侵入伺服器來獲取客戶的付款數據，以牟取利益。

最常用的網絡攻擊方法包括惡意軟件（特別是通過第三方應用程序）、黑客攻擊和網絡釣魚。往往由於固件過時、配置錯誤或者程序錯誤等問題，潛在接入點的數量並不在少數，以致連接到 CCTV、POS、付款終端機等網絡的雲端物聯網（IoT）設備特別面臨風險。



How retailers can protect themselves against cyber security threats

No retailer is too small or too large to take action against cyber-attacks. Basic measures include educating staff on how to spot a phishing email, being familiar with the Open Web Application Security Project (OWASP) and employing experienced cyber security professionals operating under a comprehensive cyber security strategy.

Instead of trying to hire cyber security experts at high cost, consider cost-effective alternatives, such as Guardforce Real-time Insured Defence (GRID) solution, which is designed to provide comprehensive protection for all networked devices, such as POSs, CCTVs, access controls and other devices that people easily overlooked as potential access points for their IoT infrastructure. With GRID in place, businesses can protect themselves against data or security breach and maintain their brand reputation. The solution also comes with 24x7 monitoring by cyber security professionals and a Cyber Crisis Management Expenses insurance protection.

With just a monthly subscription and no up-front costs, it is a truly budget-friendly cyber security solution for the retail industry.

零售商可如何保護自己免受網絡安全威脅

不論公司大小，都應該採取行動防範網絡攻擊。基本措施包括教育員工如何發現釣魚郵件，令員工熟悉開放式 Web 應用程序安全項目(OWASP)，並實行全面網絡安全策略，聘請經驗豐富的網絡安全專業人員來運作。

與其花費大筆開支自行聘請網絡安全專家， 不如考慮引用市面上更具成本效益的方案，例如衞安即時網絡保障方案(GRID)。該方案為各種聯網工具，包括銷售終端機、閉路電視網絡、門禁系統等，提供全方位保障。大家很容易忽略各種物聯網切入點都可能成為黑客入侵網絡的缺口，裝設 GRID 即時網絡保障方案後，即可保障企業網絡及數據安全，保障企業的品牌聲譽。而且方案由網絡安全專家提供全日 24 小時無間的監控，並附加網絡事故管理費用保險，提供多一重保障。

採納方案後只需支付月費，毋須安裝費用。對於零售業的網絡安全而言是非常具有成本效益的解決方案。

In conclusion …

Regardless of the size of a retail business or the type of information a retailer holds, there is someone always trying to steal its data. It is therefore vital that retailers have a good understanding of the threats they face, focus resources on those threats, and take sufficient measures to address them.

結論 ...

無論零售業務的規模如何，或者擁有什麼類型的資訊，都必定有人試圖竊取這些數據。因此，零售商必須充分了解他們面臨的威脅，將資源集中於處理這些威脅，並採取充分措施來解決這些威脅。

Guardforce

Incorporated in 1977, Guardforce has long been Hong Kong's leading security services provider offering a comprehensive range of reliable security services, from cash logistics to manned guarding and electronic security, to support major banks and retail organisations in Hong Kong.

As well, Guardforce is bringing in cutting-edge technology to creative innovative solutions to expand the group's security service offerings. Our latest solutions, including facial recognition of VIPs, smart cash deposit machines, retail analytics solution and GRID cyber security solution, will help the retail industry enhance security efficiency at lower costs.

衞安自 1977 年成立以來，一直被譽為香港領導性的保安服務供應商，為香港各大銀行、零售企業等機構，提供優質保安服務。衞安的保安服務全面，由現金押運至保安人手及電子保安裝置等，一應俱全。

目前，衞安亦正在積極引用最先進的科技打造創新的方案，從多角度擴展集團的服務效能。其中包括容貌識別技術貴賓辨認，智能存鈔機，零售分析方案及「即時網絡保障方案」等，能有效地助零售業降低成本，提升效率及保安。

Website 網址: https://www.guardforce.com.hk/tc/
Email 電郵: mkt@guardforce.com.hk
Tel 電話: (852) 2765 2861

Information is provided by Guardforce Limited
資料由衞安有限公司提供