Hewlett Packard Enterprise

2016 年網路風險報告

HPE 安全研究部門發佈的年度網路風險報告旨在幫助企業機構更好地瞭解威脅形勢，並提供資源以最大限度地降低安全風險。本年度報告提供了根據進階資料分析得出的觀點，並重點分析了多個技術領域，包括開放原始碼、行動技術和物聯網領域。

35%

在掃描的應用程式中，有超過三分之一(35%)的應用程式存在至少一個嚴重或高危漏洞。

近 86% 參與調查的企業表明他們正在使用IDS。

應用程式中開放原始碼元件的使用率有所上升。 14%

153%

Android平台中每天發現超過10,000個新威脅，全年同比增長高達153%。

80%

超過80%的開放原始碼和商用應用程式存在安全功能漏洞，給隱私資料管理帶來嚴重隱患。

95%新發現的惡意軟體樣本和42%的漏洞以Windows為攻擊目標，由此可見該作業系統仍是最主要的受攻擊平台。

行動應用程式的內部系統資訊頻遭洩露，加劇了人們對於在易失裝置上儲存關鍵業務資料的擔憂。

在2015年發現的所有漏洞利用樣本中，有29%的樣本仍在使用2010年偵測到的Stuxnet蠕蟲感染媒介，而該漏洞已經修補過兩次。

29%

容易受到間接損害的一年

資料洩露不再僅僅是取得支付卡資訊這麼簡單，竊密者的目標可能是**取得能夠把某人的生活完全打亂的資訊。**

過度監管迫使研究轉入地下

名目繁多的網路安全治理試行條例會迫使合法的安全性研究轉入地下。這些法規條例應有所改變，轉為保護和鼓勵對所有人有益的研究。

從修復單個問題轉變為全方位解決方案

2015 年，供應商轉變研發方向，著力研發可以防範各類攻擊的防禦措施。

政治壓力試圖將隱私和安全分離

美國、英國及其他地方的許多立法者聲稱，只有削減了基本隱私權利和正當法律程序才有可能實現安全。

2015 年，行業並未吸取有關修補程式方面的教訓

2015 年被利用最多的漏洞已存在長達五年之久，該漏洞同時也是2014年被利用最多的漏洞，而且供應商已針對該漏洞發佈過兩次修補程式。

攻擊者將精力轉向直接攻擊應用程式

現在，應用程式被視為攻擊者存取敏感企業資料的最便捷途徑。

利用惡意軟體攫取金錢

與ATM相關的惡意軟體越來越常見，讓網路罪犯以更快的速度賺更多的錢。

欲閱讀報告全文，請瀏覽 www.hpe.com/software/cyberrisk