URMAZ!

Whitepaper

落實DNS的安全性

儘管DNS具有開放性和重要功能，像任何系統一樣，DNS也可能受到各種安全風險的威脅。隨著網絡威脅不斷演變變得更加複雜和精密，有必要檢視DNS安全措施的實用性，這些措施旨在最小化相關風險並保護使用者免受潛在傷害。

 | www.urmazi.com | 台北市中正區忠孝西路一段80號16樓 | SF-WP-31117

安全效益

DNS安全措施還在保護使用者隱私方面發揮奇效。當我們連接到網站或搜索信息時，我們設備留下的查詢蹤跡通常包含有價值的數據。DNS安全系統，如DNS over HTTPS（DoH）或DNS over TLS（DoT），可以保護使用者的查詢免受未經授權的截取或跟踪，使其在安全連接中進行。在DNS層次上保護用戶的隱私確保了保密性，使個人免受監視或被惡意行爲者利用其個人數據的攻擊。

隨著技術的不斷發展和物聯網（IoT）的增長，DNS安全性的重要性變得更加明顯。隨著數十億設備連接，確保它們的安全性至關重要，因爲DNS中的任何弱點都可能允許攻擊者破壞龐大的物聯網設備網絡。通過事先實施強大的DNS安全措施，我們可以減輕與衆多互聯設備相關的漏洞，確保更安全和受保護的IoT生態系統。

雖然沒有系統是完全無懈可擊的，但DNS安全性對我們資通環境的整體安全性有著重要的貢獻。通過整合創新的實踐和協議，我們增強了數位體驗的可靠性、隱私和可信度。迅速適應不斷變化的威脅風險，DNS安全性作爲一種防禦和堡壘，保護用戶免受潛在風險，確保更順暢、更安全的在線構連。

風險性

首先且最重要的是，DNS安全性有助於緩解當今其中一個最強大的安全威脅 - 域名劫持。攻擊者可以劫持DNS記錄，重新配置域名和IP地址之間的轉譯，將用戶重定向到惡意網站或攔截他們的通信。這種可怕的情景可能導致身份盜竊、個人資訊泄露和頻繁的釣魚攻擊。實施DNS安全措施可以增加額外的保護層，使攻擊者更難干擾或利用系統。

此外，通過DNS安全性，使用者可通過降低基於DNS的攻擊風險，如緩存中毒或分散式阻斷服務（DDoS），而獲得連線可靠性。緩存中毒欺騙DNS服務器，將用戶的流量重定向到惡意網站，而DDoS則通過大量請求堵塞DNS服務器，嚴重延遲對於合法用戶的請求作出回應。這些臭名昭著的方法可以有效地控制互聯網通信，操縱結果，甚至將重要的線上服務帶到緩慢的停頓。持續強化DNS安全性可以增強使用者與互聯網之間的信任，培養對抗此類威脅的具有韌性的數位基礎設施。

結論

DNS安全性在鞏固我們在線溝通的完整性、隱私和可靠性方面具有不可或缺的實用性。在我們每天面臨不斷擴大的網路威脅中，投資DNS安全措施是個人、組織甚至國家的一項重要任務。共同努力，我們可以培育一個更安全、更可信、更具韌性的數位生態系統，應對互聯網高速公路上不斷出現的安全威脅。

我們是專精於以網域系統(DNS)爲基礎的資通安全防禦方案的開發團隊，豐富的外商網路安全整合應用經驗。有鑑於網域與線上服務緊密的連鎖關係和威脅影響，開啟我們著手打造符合且眞實解決企業資通安全需要的產品-iSafer。同時，爲能更快速地反應對於未知威脅的前期偵測，我們利用深度學習與人工智慧技術設立專屬的USRA研究小組，提早建立預警情資數據並與全球相關組織進行交換，URMAZI將是您最值得信賴的合作夥伴。

Further Together

