美國公布實施零信任架構相關資安實務指引

美國公布實施零信任架構相關資安實務指引

資訊工業策進會科技法律研究所
2022年09月10日

美國國家標準技術研究院（National Institute of Standards and Technology, NIST）所管轄的國家網路安全卓越中心（National Cybersecurity Center of Excellence, NCCoE），於2022年8月前公布「NIST SP 1800-35實施零信任架構相關資安實務指引」（NIST Cybersecurity Practice Guide SP 1800-35, Implementing a Zero Trust Architecture）系列文件初稿共四份[1] ，並公開徵求意見。

壹、發布背景

此系列指引文件主要係回應美國白宮於2021年5月12日發布「改善國家資安行政命令」(Executive Oder on Improving the Nation's Cybersecurity) [2]當中，要求聯邦政府採用現代化網路安全措施（Modernizing Federal Government Cybersecurity），邁向零信任架構（advance toward Zero Trust Architecture）的安全防護機制，以強化美國網路安全。

有鑑於5G網路、雲端服務、行動設備等科技快速發展，生活型態因疫情推動遠距工作、遠距醫療等趨勢，透過各類連線設備隨時隨地近用企業系統或資源進行遠端作業，皆使得傳統的網路安全邊界逐漸模糊，難以進行邊界防護，導致駭客可透過身分權限存取之監控缺失，對企業進行攻擊行動。為此NIST早於2020年8月已公布「SP 800-207零信任架構」（Zero Trust Architecture, ZTA）標準文件[3] ，協助企業基於風險評估建立和維護近用權限，如請求者的身分和角色、請求近用資源的設備狀況和憑證，以及所近用資源之敏感性等，避免企業資源被不當近用。

貳、內容摘要

考量企業於實施ZTA可能面臨相關挑戰，包含ZTA部署需要整合多種不同技術和確認技術差距以構建完整的ZTA架構；擔心ZTA可能會對環境運行或終端客戶體驗產生負面影響；整個組織對ZTA　缺乏共識，無法衡量組織的ZTA成熟度，難確定哪種ZTA方法最適合業務，並制定實施計畫等，NCCoE與合作者共同提出解決方案，以「NIST SP 800-207零信任架構」中的概念與原則，於2022年8月9日前發布實施零信任架構之實務指引系列文件初稿共四份，包含：

一、NIST SP 1800-35A：執行摘要（初稿）（NIST SP 1800-35A: Executive Summary (Preliminary Draft)）

主要針對資安技術長（chief information security and technology officers）等業務決策者所編寫，可使用該指引來瞭解企業於實施ZTA所可能遭遇挑戰與解決方案，實施ZTA所能帶來優點等。

二、NIST SP 1800-35B：方法、架構和安全特性（初稿）（NIST SP 1800-35B: Approach, Architecture, and Security Characteristics (Preliminary Draft)）

主要針對關注如何識別、理解、評估和降低風險的專案經理和中層管理決策者所編寫，闡述風險分析、安全/隱私控制對應業務流程方法（mappings）的設計理念與評估內容。

三、NIST SP 1800-35C：如何操作指引（初稿）（NIST SP 1800-35C: How-To Guides (Preliminary Draft)）

主要針對於現場部署安全工具的IT 專業人員所編寫，指導和說明特定資安產品的安裝、配置和整合，提供具體的技術實施細節，可全部或部分應用指引中所揭示的例示內容。

四、NIST SP 1800-35D：功能演示（初稿）（NIST SP 1800-35D: Functional Demonstrations (Preliminary Draft)）

此份指引主要在闡述商業應用技術如何被整合與使用以建構ZTA架構，展示使用案例情境的實施結果。

參、評估分析

美國自總統發布行政命令，要求聯邦機構以導入ZTA為主要目標，並發布系列指引文件，透過常見的實施零信任架構案例說明，消除零信任設

計的複雜性，協助組織運用商用技術來建立和實施可互操作、基於開放標準的零信任架構，未來可預見數位身分將成為安全新核心。

此外，NIST於2022年5月發布資安白皮書－規劃零信任架構：聯邦管理員指引[4] ，描繪NIST風險管理框架（Risk Management Framework, RMF）逐步融合零信任架構的過程，幫助聯邦系統管理員和操作員在設計和實施零信任架構時使用RMF。

我國企業若有與美國地區業務往來者，或欲降低遠端應用的安全風險者，宜參考以上標準文件與實務指引，以建立、推動和落實零信任架構，降低攻擊者在環境中橫向移動和提升權限的能力，與保護組織重要資源。

[1] Implementing a Zero Trust Architecture, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture (last visited Aug. 22, 2022).

[2] Executive Order on Improving the Nation's Cybersecurity, THE WHITE HOUSE, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity (last visited Aug. 22, 2022).

[3] SP 800-207- Zero Trust Architecture, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://csrc.nist.gov/publications/detail/sp/800-207/final (last visited Aug. 22, 2022).

[4] NIST Releases Cybersecurity White Paper: Planning for a Zero Trust Architecture, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://csrc.nist.gov/News/2022/planning-for-a-zero-trust-architecture-white-paper (last visited Aug. 22, 2022).

相關連結

Implementing a Zero Trust Architecture, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Executive Order on Improving the Nation's Cybersecurity, THE WHITE HOUSE

SP 800-207- Zero Trust Architecture, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

NIST Releases Cybersecurity White Paper: Planning for a Zero Trust Architecture, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

你可能會想參加

→ 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
→ 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
→ 供應鏈資安國際法制與政策趨勢分享會
→ 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 商業服務業個資保護宣導說明會
→ 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

阮韻蒨
副法律研究員 編譯整理

上稿時間：2022年10月

文章標籤

資訊安全

推薦文章