Zero Trust Architecture

Zero Trust and Zero Trust Architecture

- Zero Trust（ZT, 零架構）是面對資訊系統與服務在被視為已被入侵的網路環境中運作時，為了讓每個存取請求決定的不確定性最小化，並是在執行準確且最小權限下去執行，所提供的一系列概念與想法
- 就 Zero Trust Architecture（ZTA, 零信任架構）言，這是一種企業網路安全計畫，當中利用了零信任概念，包含元件關係、工作流程規畫與存取政策。

> 就整個網路安全策略而言，當企業決定採用零信任作為網路安全核心戰略，就需要根據零信任原則來制定計畫，以產生零信任架構，之後，將需要部署與打造零信任環境，讓企業來使用。

零信任所要解決的問題

1. 防止未經授權存取資料與服務
2. 使存取控制盡可能做到更精細

> 目的 : 讓未經授權存取的風險降到最低

- 只讓經過授權與允許的主體可以存取資料，而不讓攻擊者等其他主體能存取，而這裡的主體，包括使用者、應用程式或服務，以及裝置
- 在零信任（ZT）與零信任架構（ZTA）所指的資源存取，不僅僅包含資料存取，也包含像是印表機、運算資源與物聯網設備等

如何存取 ??

- 由於存取控制有其不確定性，因此存取決策的重點將放在身分驗證、授權與限縮默示信任區域 ，同時，需要盡可能減少身分驗證機制的時間延遲，以保持可用性，並盡可能讓存取規則更精細，讓每次資源存取請求的操作，只提供所需的最小權限。

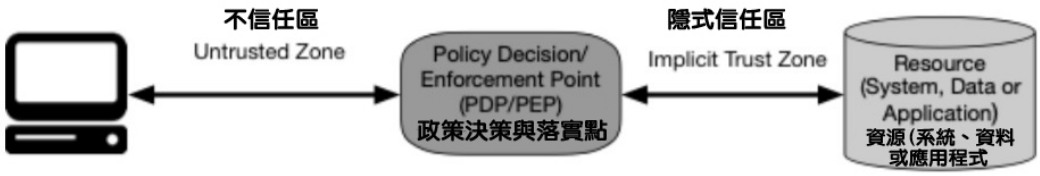

Figure 1: Zero Trust Access

- 當使用者或機器需要存取企業資源時，需要經過政策落實點（Policy Enforcement Point， PEP）進行把關，並由相應的政策決策點（Policy Decision Point， PDP），來決定權限。
- 系統必須確保左邊的主體是**真實的**，以及**請求是有效的**，而中間的政策決策點（PDP）與政策落實點（PEP），需提供適當的判斷，允許主體存取資源。在此當中，將考慮主體身分的信任程度，像是請求設備的安全現況等種種因素。
- Implicit Trust Zone（默/隱示信任區）

    - 如同機場航站位於登機區的改念，通過機場安全檢查站 (PDP/PEP) 進入登機口的人員與旅客，將被視為是可信的
- 如何讓PDP/PEP做到嚴謹的決策??
    - 透過即時且基於風險評估的結果，給出適當的判斷，以決定是否能夠存取

> 企業需要為資源存取，制定與維護一個基於風險的動態政策，並建立一個這樣的系統，已確保每次的資源存取請求，都能透過這個動態政策來執行。NIST也強調，為了使PDP/PEP盡可能具體明確，隱式信任區必須盡可能小

零信任原則(ZTA 的設計與部屬的基本原則)

1. 所有的資料來源與運算服務，都要被當作是資源
2. 不管與哪個網路位置的裝置通訊，都需確保安全
3. 對於個別企業資源的存取要求，應以連線為基礎去判斷是否許可
4. 對於資源的存取需要有動態政策來決定，包括要基於客戶端識別、應用服務，以及要求存取資產可觀察到的狀態，可能還包括其他行為或環境屬性
5. 企業對於所有自有與相關的資產，需監控與衡量其完整性與安全狀況
6. 在允許存取之前，所有的資源的身分鑑別與授權機制，都要依監控結果動態決定，並且嚴格落實
7. 企業應該要盡可能收集有關資產、網路基礎架構與通訊的資訊現況，並用這些資訊來增進安全狀態

> 網路上每個服務與可被存取的設備，都應被視為資源而要管控其存取，且所有通訊都需要確保安全

- 資源的存取請求
    - 基於每次連線請求來進行，並要先評估請求者的可信度，以及僅給予完成任務所需的最低權
    - 需要建立相關系統來監控與評估資產的安全狀況，以及要有動態政策來判斷是否能夠存取
    - 企業必須要有身分憑證與存取管理（ICAM），以及資產管理系統，當中也包括多因素身分驗證（MFA）的採用
    - 在存取管控策略的定義與執行上，將包含基於時間的因素，以及新資源的請求、資源修改、偵測到的異常活動等
    - 這樣的策略需要在安全性、可用性與成本效益上取得平衡

零信任視角下的網路

- 零信任角度下對於網路的6大假設
    - 企業私有網路不能預設為信任的區域
    - 網路中的裝置可能不是企業所有，也不能被企業設定
    - 沒有資源是原本就可信賴
    - 並非所有企業資源都位於企業擁有的基礎架構上
    - 遠端使用者存取企業主體與資產時，不能完全信賴本身的網路
    - 在企業與非企業基礎建設之間移動的資產與工作流程，應具有一致的安全政策與安全狀況
- 觀念理解
    - 必須設想攻擊者存在於企業網路中
        - 要以儘安全與可行的方式來溝通，這將需要對所有連接做鑑別，以及加密所有流量
    - 有資源是原本就可信賴

        - 在存取企業擁有的資源之前，每個資產都必須經過PEP評估其安全狀況，確保所有設備盡可能是在最安全的狀態
    - 考慮企業環境的複雜性
        - 並非所有裝置都是企業所擁有，資源也被非都是在自己擁有的基礎建設上