網路安全策略：最佳實踐白皮書

目錄

簡介

如果沒有安全策略，網路的可用性可能會受到損害。策略首先評估網路風險，並組建一個響應團隊。要繼續執行此策略，必須實施安全更改管理實踐，並監控網路是否存在安全違規行為。最後，審查過程修改了現有政策，並適應了經驗教訓。

本檔案分為三個方面：準備、預防和響應。讓我們詳細瞭解其中的每個步驟。

準備

在實施安全策略之前，必須執行以下操作：

- 建立使用策略語句。
- 進行風險分析。
- 建立安全團隊結構。

建立使用策略語句

我們建議建立概述使用者與安全有關的角色和責任的使用策略語句。您可以從涵蓋公司內所有網路系統和資料的一般策略開始。本文檔應向一般使用者群提供有關安全策略、其目的、改進安全實踐的准則以及安全責任定義的瞭解。如果您的公司已經確定了可能導致對員工採取懲罰或紀律措施的特定措施，則本文檔中應明確說明這些措施以及如何避免這些措施。

下一步是建立合作夥伴可接受的使用宣告，使合作夥伴瞭解他們可獲得的資訊、該資訊的預期處置情況以及貴公司員工的行為。您應明確解釋任何被識別為安全攻擊的具體行為，以及在檢測到安全

攻擊時將採取的懲罰性行動。

最後，建立管理員可接受的使用語句，解釋使用者帳戶管理、策略實施和許可權稽核的過程。如果貴公司對使用者密碼或後續的資料處理有特定的策略，請清楚地說明這些策略。對照合作夥伴可接受的使用和使用者可接受的使用策略語句檢查策略以確保一致性。確保培訓計畫和績效評估中反映了「可接受的使用策略」中列出的管理員要求。

進行風險分析

風險分析應確定網路、網路資源和資料面臨的風險。這並不意味著您應該識別網路的所有可能的入口點，也不意味著識別所有可能的攻擊方式。風險分析的目的是識別網路的各個部分，為每個部分分配威脅等級，並應用適當的安全級別。這有助於在安全和所需網路訪問之間保持可行的平衡。

為每個網路資源分配以下三個風險級別之一：

- **低風險系**統或資料，如果受到危害（未經授權人員檢視的資料、資料損壞或資料丟失），不會中斷業務或導致法律或財務問題。目標系統或資料可以很容易恢復，並且不允許其它系統進一步訪問。
- **中等風險系統或數**據，如果受到危害（未經授權人員檢視的資料、資料損壞或資料丟失），將導致業務的中等中斷、輕微的法律或財務影響，或者提供對其他系統的進一步訪問。目標系統或資料需要進行適度還原操作，或者還原過程會破壞系統。
- **高風險系統或數**據，如果受到危害（未經授權人員檢視的資料、資料損壞或資料丟失），將導致業務嚴重中斷、導致重大法律或財務影響，或威脅人員的健康和安全。目標系統或資料需要大量的還原工作，或者還原過程會中斷業務或其他系統。

為以下各項指定風險級別：核心網路裝置、分佈網路裝置、接入網路裝置、網路監控裝置（SNMP監控器和RMON探測）、網路安全裝置（RADIUS和TACACS）、電子郵件系統、網路檔案伺服器、網路列印伺服器、網路應用伺服器（DNS和DHCP）、資料應用伺服器（Oracle或其他獨立應用程式）、台式電腦和其他裝置（獨立列印伺服器和網路傳真機）。

交換機、路由器、DNS伺服器和DHCP伺服器等網路裝置可以進一步訪問網路，因此它們是中等或高風險裝置。此外，此裝置的損壞也可能導致網路本身崩潰。這樣的故障可能會對業務造成極大的破壞。

一旦您指定了風險級別，就有必要標識該系統的使用者型別。最常見的五種使用者型別是：

- **管理員** — 負責網路資源的內部使用者。
- **需要更**大訪問許可權的特權內部使用者。
- **使用者具**有一般訪問許可權的內部使用者。
- **合作**夥伴需要訪問某些資源的外部使用者。
- **其他**外部使用者或客戶。

識別每個網路系統的風險級別和所需訪問型別是以下安全矩陣的基礎。該安全矩陣為每個系統提供了快速參考，並為進一步的安全措施提供了起點，例如制定適當的策略以限制對網路資源的訪問。

系統	說明	風險水準	使用者型別
ATM交換器	核心網路裝置	高	裝置配置管理員（僅限支援人員）；所有其它用作傳輸裝置

網路路由器	分散式網路裝置	高	裝置配置管理員（僅限支援人員）；所有其它用作傳輸裝置
配線間交換機	接入網路裝置	中	裝置配置管理員（僅限支援人員）；所有其它用作傳輸裝置
ISDN或撥號伺服器	接入網路裝置	中	裝置配置管理員（僅限支援人員）；合作夥伴和特權使用者可獲取特殊訪問許可權
防火牆	接入網路裝置	高	裝置配置管理員（僅限支援人員）；所有其它用作傳輸裝置
DNS和DHCP伺服器	網路應用程式	中	管理員進行配置；普通使用者和特權使用者使用
外部電子郵件伺服器	網路應用程式	低	管理員進行配置；用於在Internet和內部郵件伺服器之間郵件傳輸的所有其他裝置
內部電子郵件伺服器	網路應用程式	中	管理員進行配置；供使用的所有其他內部使用者
Oracle資料庫	網路應用程式	中或高	管理員可進行系統管理；資料更新的特權使用者；一般資料存取使用者；用於部分資料存取的所有其他裝置

建立安全團隊結構

建立一個由安全經理領導的跨職能安全團隊，該團隊由來自貴公司每個運營領域的參與者組成。團隊代表應瞭解安全策略以及安全設計和實施的技術方面。通常，這需要團隊成員接受額外的培訓。安全團隊有三個責任領域：政策制定、實踐和響應。

策略開發側重於制定和審查公司的安全策略。至少每年審查一次風險分析和安全策略。

實踐是安全團隊執行風險分析、批准安全變更請求、稽核來自供應商和CERT Mail List的安全警報，以及將簡單語言的安全策略要求轉化為具體技術實施的階段。

最後一個責任領域是響應。雖然網路監控經常識別安全違規，但實際進行此類違規故障排除和修復的是安全團隊成員。每個安全小組成員應詳細瞭解其行動區內的裝置所提供的安全功能。

雖然我們已經定義了整個團隊的責任，但您應該定義安全策略中安全團隊成員的各個角色和責任。

預防

預防可分為兩部分：批准安全更改並監控網路安全。

批准安全更改

安全更改是指對網路裝置進行的更改，這些更改可能對網路的整體安全造成影響。您的安全策略應識別非技術方面的特定安全配置要求。換句話說，不是將要求定義為「No outside sources FTP connections will be permitted through the firewall」，而是將要求定義為「Outside connections should not be able to retrieve files from the inside network」。 您需要為您的組織定義一組唯一的要求。

安全團隊應檢視簡單語言要求清單，確定滿足要求的特定網路配置或設計問題。一旦團隊建立了實施安全策略所需的網路配置更改，您就可以將這些更改應用到任何將來的配置更改。雖然安全團隊可以審查所有更改，但此過程允許他們只審查構成足夠風險的更改來保證特殊處理。

我們建議安全團隊檢查以下型別的更改：

- 對防火牆配置的任何更改。
- 對存取控制清單(ACL)的任何變更。
- 對簡單網路管理協定(SNMP)配置的任何更改。
- 與批准的軟體修訂版本級別清單不同的軟體更改或更新。

我們還建議遵循以下准則：

- 定期更改網路裝置的密碼。
- 將訪問網路裝置的許可權限制在經批准的人員清單中。
- 確保網路裝置和伺服器環境的當前軟體版本級別符合安全配置要求。

除了這些批准指南，變更管理審批委員會中還應有一名來自安全團隊的代表，以便監控董事會稽核的所有變更。安全團隊代表可以拒絕任何被視為安全更改的更改，直到安全團隊批准該更改。

監控網路安全

安全監控與網路監控類似，但重點在於檢測網路中表明安全違規的更改。安全監控的出發點是確定什麼是違規。在執行風險分析中，我們根據系統面臨的威脅確定了所需的監控級別。在批准安全更改中，我們確定了網路面臨的特定威脅。通過檢視這兩個引數，我們將清楚瞭解您需要監控的內容和監控頻率。

在風險分析矩陣中，防火牆被視為高風險網路裝置，這表明您應即時監視該裝置。在Approving Security Changes部分，可以看到您應該對防火牆的所有更改進行監控。這表示SNMP輪詢代理應監控登入嘗試失敗、異常流量、防火牆變更、授予防火牆的存取以及通過防火牆建立的連線等情況。

按照此示例，為風險分析中確定的每個領域建立監控策略。我們建議每週監控低風險裝置，每天監控中等風險裝置，每小時監控高風險裝置。如果需要更快速的檢測，請在更短的時間範圍內進行監控。

最後，您的安全策略應解決如何通知安全團隊安全違規的問題。通常，您的網路監控軟體會首先檢測到違規。它應該觸發向操作中心的通知，操作中心反過來應通知安全團隊，並在必要時使用尋呼機。

響應

響應可以分為三部分：安全違規、恢復和審查。

安全違規

當檢測到違規時，保護網路裝置、確定入侵程度和恢復正常操作的能力取決於快速決策。提前做出這些決策使得對入侵的響應更易於管理。

檢測到入侵後的第一個操作是安全團隊的通知。如果沒有適當的程式，在得到正確的人來做出正確回應方面將會出現相當長的延遲。在安全策略中定義一個每週7天、每天24小時可用的過程。

接下來，應定義賦予安全團隊進行變更的許可權級別，以及變更的順序。可能的糾正措施包括：

- 實施更改以防止進一步訪問違規。
- 隔離違規的系統。
- 聯絡運營商或ISP以嘗試跟蹤攻擊。
- 使用錄音裝置收集證據。
- 斷開違規的系統或違規源。
- 聯絡警方或其他政府機構。
- 關閉違規的系統。
- 根據優先順序清單恢復系統。
- 通知內部管理人員和法律人員。

請務必詳述在安全策略中無需管理層批准即可執行的任何更改。

最後，在安全攻擊期間收集和維護資訊有兩個原因：確定安全攻擊對系統的危害程度，並起訴外部違規行為。資訊的型別和收集方式因目標而異。

要確定違規的程度，請執行以下操作：

- 通過獲取網路的監聽器跟蹤、日誌檔案的副本、活動使用者帳戶和網路連線，來記錄事件。
- 通過禁用帳戶、斷開網路裝置與網路的連線以及斷開與Internet的連線，來限制進一步的危害。
- 備份受損系統，以幫助詳細分析損壞情況和攻擊方法。
- 尋找其他妥協跡象。通常，當系統受到威脅時，還會涉及其他系統或帳戶。
- 維護和審查安全裝置日誌檔案和網路監控日誌檔案，因為它們經常提供攻擊方法的線索。

如果您有意採取法律行動，請您的法律部門審查證據收集程式和相關部門的參與。這種審查提高了法律訴訟中證據的有效性。如果違規屬於內部性質，請與您的人力資源部門聯絡。

恢復

恢復正常的網路操作是任何安全違規響應的最終目標。在安全策略中定義如何執行、保護和提供正常備份。由於每個系統都有自己的備份方法和程式，因此安全策略應作為元策略，為每個系統詳細說明需要從備份恢復的安全條件。如果在執行恢復操作之前需要審批，還應包括獲得批准的過程。

檢閱

審查過程是建立和維護安全策略的最後努力。您需要檢查三件事：策略、狀態和實踐。

安全政策應該是一個適應不斷變化的環境的活的檔案。根據已知的最佳實踐檢查現有策略，使網路保持最新。此外，請檢視CERT網站 ，瞭解可以納入安全策略的有用提示、實踐、安全改進和警報。

您還應檢視網路的安全狀態，並與所需的安全狀態進行比較。專門從事安全工作的外部公司可以嘗試滲透網路，不僅測試網路的狀態，還可以測試組織的安全響應。對於高可用性網路，我們建議每年進行一次此項測試。

最後，實踐的定義是對支援人員進行的演練或測試，以確保他們清楚地瞭解在違反安全規定時應該怎麼做。通常，此演練是管理層未宣佈的，並且與網路狀態測試結合進行。這項審查查明了程式和人員培訓方面的差距，以便採取糾正行動。

相關資訊

- 更多最佳實踐白皮書
- 技術支援 - Cisco Systems