船舶經營人無法忽視網路安全

在調查某起船上發生的網路事件時，美國海岸警衛隊發現，船員在事件發生前早就清楚其船載網路存在的安全風險。

在近期發佈的**第 06-19 號海上安全警告**中，美國海岸警衛隊公佈了對某商船上發生的一起網路事件的調查結果:

“2019 年 2 月，一艘開往紐約港和紐澤西州、執行國際航程的深吃水船報告稱，其正在經受一起影響其船載網路的重大網路事件。一支由海岸警衛隊領導的跨部門網路專家小組做出反應，並對該船的網路和基本控制系統進行了分析。該小組得出結論，儘管惡意軟體大大削弱了船載電腦系統的功能，但該船的基本控制系統並未受到影響。然而，跨部門反應小組發現，該船在未採取有效網路安全措施的情況下航行，從而使關鍵的船舶控制系統暴露出嚴重漏洞。”

這次調查所得出的最具警示性的結果可能是，船員在事件發生前早就清楚其船載網路存在的安全風險。雖然大多數船員認為，船載電腦網路不足以信賴，因此不會將其用

於檢查銀行帳戶等個人事務，但同一網路卻被用於公務用途——更新電子海圖，管理貨物資料，以及與岸上設施方、引航員、代理人和港口國當局進行通信。

建議

考慮到上述網路事件的調查結果，美國海岸警衛隊強烈建議船舶經營人採取下列基本措施，來提升其網路的安全性：

- 將船載網路分為多個“子網路”，以防止基本系統和設備遭到未經授權的訪問；
- 為每位元雇員創建受密碼或 ID 卡保護的獨特網路檔案，從而杜絕多人使用通用登錄憑據的情況；
- 授予每個使用者有限的特權集合，也就是說，將使用者的網路訪問權完全限制在執行其工作所需的最低權限；
- 建立關於使用外部介質（例如隨身碟和其他通過 USB 驅動器傳輸資料的設備）的明確程序；
- 安裝基本的防毒軟體；及
- 建立軟體補丁/更新管理制度。影響作業系統和應用程式的漏洞處於不斷變化之中，及時更新電腦系統是保護系統免受網路犯罪分子侵害的最重要措施之一。

美國海岸警衛隊曾精闢地指出：“*隨著人們通過點擊滑鼠來控制發動機，而且越來越依賴電子海圖和導航系統，採用適當的網路安全措施來保護這些系統，已經與防控實際登輪或對傳統機械進行日常維護一樣至關重要了。*”

本協會 2018 年 12 月 12 日發佈的 Insight 文章“**船上網路安全程序亟待加強**”中還提供了額外的建議。

Gard 關於網路安保的安全意識宣傳活動

儘管國際海事組織規定，船東和經營人可以到 2021 年再將網路風險納入船舶安全管理體系，但網路犯罪分子現已著手實施犯罪。資料是一種資產，保護資料需要在保密性、完整性和可用性之間找到良好平衡。網路安全不僅取決於船上系統和程式是如何設計的，還取決於它們是如何使用的——即人為因素。

因此，應該對海員進行適當培訓，以說明其識別和報告網路事件。基於我們對網路安全案例的分析，Gard 和 DNV GL 製作了一段**防損意識視頻**和一份演示文稿，其中對海運業如何解決該問題提出了一些建議。這些資料並不旨在宣導行業變革或規則變更，而是建議改變人們的行為方式。