船舶经营人无法忽视网络安全

在调查某起船上发生的网络事件时，美国海岸警卫队发现，船员在事件发生前早就清楚其船载网络存在的安全风险。

在近期发布的**第 06-19 号海上安全警告**中，美国海岸警卫队公布了对某商船上发生的一起网络事件的调查结果：

“2019 年 2 月，一艘开往纽约港和新泽西州、执行国际航程的深吃水船报告称，其正在经受一起影响其船载网络的重大网络事件。一支由海岸警卫队领导的跨部门网络专家小组做出响应，并对该船的网络和基本控制系统进行了分析。该小组得出结论，尽管恶意软件大大削弱了船载计算机系统的功能，但该船的基本控制系统并未受到影响。然而，跨部门响应小组发现，该船在未采取有效网络安全措施的情况下航行，从而使关键的船舶控制系统暴露出严重漏洞。”

这次调查所得出的最具警示性的结果可能是，船员在事件发生前早就清楚其船载网络存在的安全风险。虽然大多数船员认为，船载计算机网络不足以信赖，因此不会将其

用于检查银行账户等个人事务，但同一网络却被用于公务用途——更新电子海图，管理货物数据，以及与岸上设施方、引航员、代理人和港口国当局进行通信。

建议

考虑到上述网络事件的调查结果，美国海岸警卫队强烈建议船舶经营人采取下列基本措施，来提升其网络的安全性：

- 将船载网络分为多个“子网络”，以防止基本系统和设备遭到未经授权的访问；
- 为每位雇员创建受密码或 ID 卡保护的独特网络档案，从而杜绝多人使用通用登录凭据的情况；
- 授予每个用户有限的特权集合，也就是说，将用户的网络访问权完全限制在执行其工作所需的最低权限；
- 建立关于使用外部介质（例如 U 盘和其他通过 USB 驱动器传输数据的设备）的明确程序；
- 安装基本的防病毒软件；及
- 建立软件补丁/更新管理制度。影响操作系统和应用程序的漏洞处于不断变化之中，及时更新计算机系统是保护系统免受网络犯罪分子侵害的最重要措施之一。

美国海岸警卫队曾精辟地指出：*“随着人们通过点击鼠标来控制发动机，而且越来越依赖电子海图和导航系统，采用适当的网络安全措施来保护这些系统，已经与防控实际登轮或对传统机械进行日常维护一样至关重要了。”*

本协会 2018 年 12 月 12 日发布的 Insight 文章“**船上网络安全程序亟待加强**”中还提供了额外的建议。

Gard 关于网络安保的安全意识宣传活动

尽管国际海事组织规定，船东和经营人可以到 2021 年再将网络风险纳入船舶安全管理体系，但网络犯罪分子现已着手实施犯罪。数据是一种资产，保护数据需要在保密性、完整性和可用性之间找到良好平衡。网络安全不仅取决于船上系统和程序是如何设计的，还取决于它们是如何使用的——即人为因素。

因此，应该对海员进行适当培训，以帮助其识别和报告网络事件。基于我们对网络安全案例的分析，Gard 和 DNV GL 制作了一段**防损意识视频**和一份演示文稿，其中对海运业如何解决该问题提出了一些建议。这些资料并不旨在倡导行业变革或规则变更，而是建议改变人们的行为方式。