Circular From LONDON
Date: 8 September 2016

网络风险 - 航运业新领域的漏洞

随着信息技术在商业中的广泛应用，网络攻击风险成为船东及其船舶潜在的最大威胁。2015年波耐蒙研究所(Ponemon Institute)发布的研究报告表明，过去一年中39家基准机构的网络损失增长了14%，而这些机构的年均成本为每年410万英镑(分别从628,423到160万英镑不等)。

金融和数据风险

对于航运公司，目前面临这类损失的是业务里的“后台”——会计、付款和银行业务。金融数据、船员信息和交易方的保密材料均容易受到黑客入侵，在此领域的管理规范日益增多－主要由欧盟主导，要求公司采取预防措施，汇报数据损失。并通过常规部署良好的网络安全、最新的防火墙、渗透测试以及员工培训来防范此威胁。

即便如此，风险仍会通过第三方出现。如港口代理，他们的电脑系统可能易于被攻击，而其职员在这方面得到的培训也甚少。最近几起案件显示，他们的系统能轻而易举地被入侵，诈骗犯通过诈骗邮件将款项转移到自己的账户。一些基本的措施，譬如通过电话确认付款指示，对于防范此类骗局大有帮助。

实体风险

鲜为人知的风险是对于船舶本身的实体风险。我们发现，这种情况在传统船公司和他们的船队中尤为显著。虽然该风险在目前而言并不高，但由于船载资讯科技(IT)使用的增加，即便在无单一网络控制多个系统和网络连接信号弱的时候，网络攻击对船舶操作性都存在着潜在的严重风险。普遍使用此类技术的例子有自动识别系统(AIS)、电子海图显示与信息系统(ECDIS)、全球导航卫星系统(GNSS)和电子航海系统(E-Nav)。主要和辅助推进系统也日渐依靠电脑取得高效操作。

尽管网络攻击可以是有意为之，目前的风险看来主要是关键系统无意招致了病毒。比如说，一个船员在ECDIS系统连接USB给手机充电，从而感染病毒导致整个系统无法运行。这是个代价昂贵的错误。船舶的维护系统和推进系统也一同曝露在黑客/恶意程序的风险中，如果网络攻击使关键系统在关键时刻失效，带来的后果可能很严重。所有成功的攻击都要花费巨额成本来解决。

庆幸的是，网络攻击所导致的实体危害事故仍不多见。原因有几个，但目前主要是因为航运业一般不多见于公众(黑客落手目标)网络以及网络犯罪者有较多相对更容易得手的目标。但我们也听说过

海盗操控GPS数据以诱导船舶偏离航线；以及海盗入侵船舶管理系统来辨认那些船舶没有武装保安人员随行；以及毒贩入侵码头集装箱管理系统以监视和控制藏有毒品的集装箱动态，以躲避检测。

随着“物联网”被航运采用，船舶系统通过中央控制，持续性对岸联系，维护和诊断越来越多通过设备的USB端口处理，风险只增无减。网络犯罪数量的增长从任何角度来看都是令人震惊的，随着其他行业安全性的提高，航运业也将成为攻击目标。因此航运业是时候主动考虑这些问题的对应之策。

未来之路

跟处理任何操作问题一样，都需采用经过试验的可靠风险评估方法。考虑风险，衡量后果，采取适当方法以降低风险。与一般的海运风险类型不同的是，IT和网络在大部分海事专家的经验之外，故此需向资深的IT顾问寻求帮助。培训是关键，毕竟目前最高的风险来自船员非故意将病毒导入设备或通过点击不良链接所导致。但如果风险评估能做到足够彻底、船员通过培训以加强警觉性、懂得如何应对攻击，那么在网络犯罪瞄准你的公司时，船舶和船公司将得到更好的保护。

信息来源：London P&I Club