如何制定计算机安全计划

文/Vasiliki Tafili 和Trent Nelson

处理核材料或其他放射性物质以及开展相关活动的设施是需要高度安全和安保的关键基础设施。通过对计算机安全采取全面和积极主动的方案，各组织可以保护这些设施中的敏感信息资产和计算机化系统不受损害。原子能机构建议的计算机安全方案的基础在于各国制定有关国家战略或政策的要求，并能够对实物保护、核安全以及核材料衡算和控制相关敏感信息和计算机系统进行保密和保护。这些要求也可以采取国家法规的形式，对制定和实施“计算机安全计划”*作出规定。

“计算机安全计划”是一个总体框架，包括实施计算机安全政策和程序有效计划的关键要素，计算机安全政策和程序将在核设施或放射源设施的整个寿期内采用。“计算机安全计划”的目的是保护敏感信息资产和对维护安全和安保功能至关重要的计算机化系统免受网络威胁，以减轻网络攻击的影响。

国家战略

全面而有效的计算机安全战略需要系统性方案，其中整合各种要素，包括维护国家核安保制度的法规、计划、安全保护措施和应急能力。

法规

有效的法规能为保护敏感计算机化系统提供法律框架，并确保各组织制定和适当实施“计算机安全计划”*。

“计算机安全计划”的关键要素：

作用和责任

具有问责制的组织作用和责任对于有效管理至关重要，特别是涉及关键基础设施的情况下。必须认识到组织层次结构以及权力划分和报告结构，以便在“计算机安全计划”内灌输高效和有效的协作和协同作用。

风险、脆弱性和合规管理

计算机安全风险管理涉及对敏感数字资产和计算机化系统的脆弱性和潜在后果的评价，利用分级方案实施计算机安全控制，抵御网络攻击。所采用的安保措施水平应与受保护的信息和（或）计算机化系统相关的风险水平相称。通过考虑脆弱性或威胁的后果，各组织可以确定减轻风险所需的安保措施水平。

安保设计和管理

计算机安全设计是防范网络威胁的一个关键方面。基本设计原则包括分级方案和纵深防御，即实施多层分区安保控制，以防止和减轻攻击。对安保的要求也必须纳入整个系统开发周期，包括通过明确的政策和协议约束第三方组织，以确保安保措施的一致性和有效性。

数字资产管理

计算机安全的有效性取决于通过系统的过程列出所有设施功能、资产和系统的全面清单，包括对保护核业务或保持核材料和其他放射性物质安全可靠使用至关重要的敏感数字资产。这类清单还要提供对组织支持访问控制、备份和其他安保措施至关重要的数据流和相互依赖关系，以保护这些资产免遭破坏或盗窃。

安保程序

执行的核安保政策和程序为防止盗窃、破坏或未经授权使用核材料和设施提供方向和责任。这些政策确保对敏感信息和资产的访问受到严格控制，并确保对有访问权限的个人进行适当的筛查和培训。

人员管理

诚信、意识和培训对核工业的人员管理至关重要。应进行诚信评价，以确保人员可靠、能够胜任，并且没有任何可能损害安全或安保的利益冲突。保持合格和值得信赖的人员对于确保核安全和核安保至关重要。

---

* 更多细节载于原子能机构《核安保丛书》第17-T（Rev.1）号《核设施的计算机安全技术》。