# 计算机安全演习如何助力提高应对核安保网络攻击的准备

文/Emma Midgley

历史上，核设施一直侧重于通过设置枪支、警卫和闸门等实物保护措施来确保核材料免受恶意攻击。这些措施仍被用来在核设施周围成功构筑堡垒，防止核材料或其他放射性物质遭到盗窃、破坏或对控制系统的未经授权访问。然而，近几十年来，在我们日益数字化的世界中，网络攻击的威胁已经升级。任何国家，甚至那些拥有最先进核电和研究计划的国家，都可能受到攻击。制定计算机安全和应对核设施网络威胁的国家框架已是必不可少。通过大规模演习，原子能机构协助各国改进对网络攻击的防范，并协助各国改进对核设施网络攻击的检测和应对策略。

**“在事件发生之前，为应对计算机安全事件制定政策、明确的作用和责任以及详细的程序至关重要。”**
—国际原子能机构核安保司高级信息和计算机安全官员Trent Nelson

原子能机构为核电厂和辐射设施制定了计算机安全演习，并已在世界各地国家层面开展进行。这些演习使各国能够演练和准备应对核设施网络安全遭到破坏的最坏情景。通过这些理论情景，可以找出政策、程序和流程中的薄弱环节，并确定需要通过缓解技术、能力建设和（或）组织变动来填补的差距。除了协助各国开展大规模演习以测试核设施的计算机安全外，原子能机构关于计算机安全的核安保导则还提供了重要资源，可以使各国采取重要的计算机安全措施，以检测、预防和应对网络攻击。

“在事件发生之前，为应对计算机安全事件制定政策、明确的作用和责任以及详细的程序至关重要。”原子能机构核安保司高级信息和计算机安全官员Trent Nelson说，“这就是原子能机构能够在许多方面提供帮助之处：从演习和导则，到分享最佳实践和程序，以确保有效的沟通和强有力的安全保护。”

使核设施容易受到网络攻击的因素包括人员、供应链的复杂性，以及使用计算机化系统支持核功能的多个利益相关方之间共享敏感信息。

“设想一种攻击，它让一个供应商妥协并伪造一项工作指令，导致一个有授权访问权限的受信任技术人员做出一个微妙的错误行动，”Trent Nelson说，“这只是恶意行为者可以找到绕过安全系统的一种方式。”

减少网络攻击潜在影响的一个重要方面是提高利益相关方的认识和增加利益相关方之间的有效沟通，因为这些群体中的任何一个，或这些群体中的任何个人，都可能成为恶意行为者的目标。谈到核设施的防御，有四个关键参与者：监管机构、设施营运者、技术支持组织（计算机安全事件响应小组和（或）计算机安全操作中心）以及第三方组织，如供应商和支持组织。开展演习是测试利益相关方之间沟通、报告和通知的一种良好方式，也是验证和确认组织结构安全和安保的一种良好方式。

虽然理想的情景是，网络攻击者会发现不可能渗透到核设施的计算机安全系统，但由于恶意行为者在不断

减少任何网络攻击潜在影响的一个重要因素是利益相关方之间提高认识和有效沟通。
（图/Adobestock）

演变，加上人性不可靠，这就意味着几乎不可能预测下一次大规模袭击会如何展开。因此，及时发现攻击是关键。在最近于斯洛文尼亚举行的演习中，通过一次理论上的网络攻击帮助验证和确认了防御网络攻击的检测和响应能力。

“计算机安全不是一个项目或一个过程，而是一个需要持续努力、关注和实践的终身旅程，”斯洛文尼亚核安全管理局网络安全处处长Samo Tomaži说，“像在斯洛文尼亚进行的演习使核部门的所有相关实体能够评估他们在网络攻击成功的情况下其事件响应预案的稳健性。”

如果发生严重的计算机安全事件，并有可能导致核安全事件或核安保事件，除了核设施的通常利益相关方之外，计算机安全事件响应小组也应参与其中。例如，这种事件可能涉及违反安保政策或安保程序，影响敏感的数字资产或系统，或失去敏感信息和对核安全关键功能的控制。

在这种情况下，一旦发现计算机安全事件或损害，计算机安全事件响应小组应与设施利益相关方合作，调查事件、收集取证数据、分析发生的一切和发生地点以及协助遏制和消除入侵，以帮助营运者恢复核设施的正常运行。在应急结束时，收集计算机取证证据，以帮助对攻击事件进行刑事调查，并确保有效的信息共享，以便在未来进一步加强核设施的计算机安全措施。

在斯洛文尼亚的演习中，检测网络攻击对于能够应对这一理论上的安保事件以及测试和验证事件响应程序至关重要。这些演习为测试安全、安保和应急准备之间的关系提供了支持，并通过识别潜在的薄弱环节和提出必要的修改来加强核安保制度，以提高其对潜在网络安全威胁的总体准备。此外，这些演习还提供了测试国家和国际层面进行通知和报告的通讯渠道的机会。总之，定期进行计算机安全演习是维护核设施安保的一个重要方面。