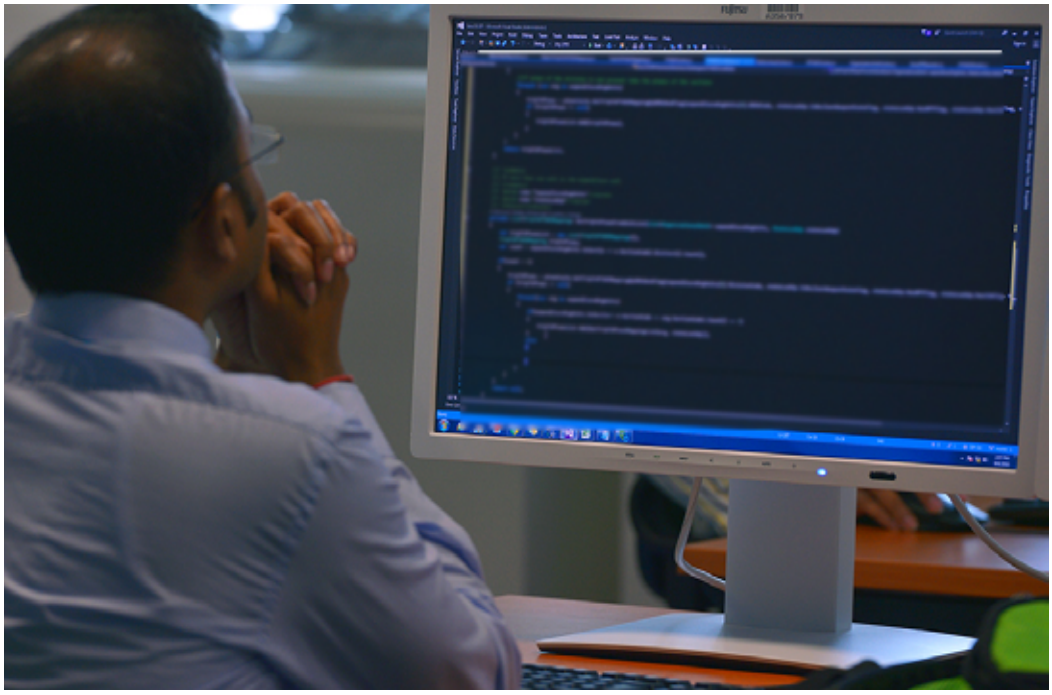
枪支、守卫、大门和极客：罗马尼亚加强核装置的计算机安全

文/Laura Gil



（图/国际原子能机构D. Calma）

网络攻击可以刷取存储在您的计算机上的所有信息，甚至阻止计算机工作。这够糟糕了。但是对核电厂的网络攻击可能导致核材料被破坏或被盗。计算机安全涉及保护数字数据和防止系统和网络受到恶意行为攻击，是核安保的一个关键组成部分。

“计算机的发展及其在核业务各个方面的使用改变了安保模式。”原子能机构信息技术安全官员Donald Dudenhoeffer表示。“信息和计算机安全必须被视为整个核安保预案的组成部分。”

核安保长期以来主要集中于实物保护——通常指枪支、守卫和大门，但如今的犯罪分子还将计算机作为袭击的手段和目标。网络攻击可能导致核安保信息丢失、核装置被破坏，以及在伴随实物攻击的情况下，使核材料或其他放射性物质被盗。计算机目前在核设施的安全、安保和管理方面发挥着重要作用；所有系统都能准确防范恶意入侵至关重要。

“我们都需要准备好保护自己免受互联网和数字时代的非良性环境的影响。”Dudenhoeffer说。“我们都使用计算机，我们都需要提高对威胁、风险和保护手段的认识。”核装置的监管者和营运者越来越认识到计算机安全的重要性，并正在寻求加强其核安保计划。Dudenhoeffer认为，罗马尼亚便是一个示例。

“我们了解防范可能影响我们的核装置安全和可靠运行的各种威胁，包括针对计算机和信息安全的威胁的

重要性。”罗马尼亚布加勒斯特国家核活动管理委员会核法规标准机构协调员Madalina Tronea说。

2012年，一组原子能机构专家对罗马尼亚开展了一次国际实物保护咨询服务工作组访问。他们向当局提供了一份建议清单，以进一步发展适当的监管框架，保护核装置免受各种威胁，包括网络攻击。

不久之后，国家核活动管理委员会的一个核监管小组开始制定一项法规。这项法规于2014年11月生效。法规的重点是保护对核安全、核安保、核保障和核应急响应至关重要的系统、设备和部件，包括用于仪器仪表和控制系统的软件。除监管之外，国家核活动管理委员会还发布了一份文件概述网络威胁，其中考虑了世界各地工业界的新威胁和最近的计算机安全事件。

“我们关注全球背景以及威胁和对策的变化。”Tronea说。“我们还尽最大努力确保针对计算机安全事件提供充分的预防和保护，并在发生这类事件时有效应对此类事件。”

同年，罗马尼亚政府还批准了“国家核安全和核安保战略”，其中包括致力于不断改进核部门计算机安全的目标。

人：问题和解决方案

研究表明，大多数计算机安全事件是由人为错误引起的。

“人：人力资源能力发展是最好的投资领域之一。”Dudenhoeffer说。“我们并不需要世界上到处都是计算机安全专家。我们需要世界上人人都认识到计算机安全风险和基本防御措施。

（图/国家核活动管理委员会）

我们需要一支见多识广的劳动队伍和领导者。”

得益于罗马尼亚自2013年以来参加的原子能机构培训班，该国建立了一个可持续的利益相关者网络。通过网络，利益相关者现在共享核安保经验，共同努力构建健全的信息和计算机安全计划。

通过国家培训班、在线学习、专家会议和培训教员计划，原子能机构与核工业的国家领导者和利益相关者合作，更好地了解网络威胁并制定加强计算机安全的良好实践。Dudenhoeffer说，国家培训班是原子能机构在计算机安全领域开展的最宝贵活动的一部分。

“在实物保护中，你能够看到你正在保护的东西，并能够想象可能的攻击场景。”Dudenhoeffer说。“但在网络空间中，犯罪分子有更多的目标，包括那些不在设施的目标；你甚至可能在家里就会被攻击。我们必须学会想犯罪分子之所想，以便更好地了解如何随时随地防范网络攻击。”