再仔细也不为过

核工业中的网络安全挑战

每年，投入使用的计算机数目不断增加，创造了更多网络攻击的机会。（照片由istockphoto.com网站提供）

人们使用和与之互动的计算机数量每年都在增加，创造了更多网络攻击的机会。例如，当代汽车用于控制发动机、变速器、无线电、防锁死刹车系统、无钥匙系统、入口、防盗、远距离通信系统等装置的数字输入/输出通道不少于12个。所有这些都可能包含容易遭到“黑客”的脆弱性。

计算机和信息技术发展十分迅速，有时我们还来不及对可能的网络脆弱性和最终攻击来源进行了解。此外，网络攻击不限于工作场所，个人私生活有时也会成为攻击目标。

国际原子能机构在提高网络安全方面的一个主要目标是，加强核安保文化，改变人们的思维方式，改变人们对技术选定和使用的评价方式。

杜登霍夫尔说：“如果核专业人员及其家人不仅更多地了解他们的实体空间，而且更多地认识他们的数字空间，那么他们对在线信息共享和技术使用会更加谨慎。看似无伤大雅的信息会与其他地方发现的其他信息混合在一起，会证明具有严重的破坏性。谷歌和类似国际互连网搜索引擎经常是黑客制订攻击计划时的首选工具。”

荷兰安全和司法部反恐与安全国家协调员本•戈韦斯说，对这种威胁的认识正慢慢渗入核工业。“核工业目前面临着必须拓宽和加深其计算机和信息网络抗击网络威胁的现有防御的挑战。核工业在制订、实施和扩大稳健的核设施信息和控制系统保护措施方面近乎处于起点。”

戈韦斯说：“国际原子能机构能够在这种动态发展中起主导作用。”

助手社区

2012年10月，计算机病毒“红色十

月”被发现。估计这种病毒已在长达5年内收集了60多个国家的敏感信息而未被觉察。从被感染网络收集的信息可在未来网络攻击中重新使用。这种高水平网络犯罪变得越来越普遍，是核安保人员必须应对的另一项挑战。

国际原子能机构在每个层面上为成员国建立稳健和经过考验的信息和计算机安全程序的努力提供支持。国际原子能机构组织地区培训计划，为专业人员开设核安保课程，出版核设施网络安全导则，以及定期举办国际会议，使专业人员能够共享专门技术，通过同行从业者和国际原子能机构专家解决最紧迫的问题。

国际原子能机构还将信息安全评定纳入国际原子能机构“国际实物保护咨询服务”中。

“国际实物保护咨询服务”向拥有核材料和核设施的所有国家提供全面评审，就保护各国核材料和放射性材料的更有效方式向各国提供建议。

许多组织正在致力于解决不断增加的网络威胁。在这些领域建立伙伴关系非常重要。国际原子能机构已连同国际刑警组织和欧洲网络与信息安全局共同举行国际演习和制订网络安全导则文件和培训活动。

有关网络安全和核法证等核安保活动的“@ TOMIC 2012”国际演习，便是国际原子能机构参与旨在增加核及其他放射性材料财产保护的网络安全意识国际活动的一个例子。来自40个国家的150名学员参加了这次由荷兰主办的演习。下次演习将于2014年举行，即“@ TOMIC 2014”。

“@TOMIC”活动组织者戈韦斯说：“因为国际原子能机构在全球核领域有着令人尊重的地位，所以它能够在实施导则或议定书方面和在提高人们对网络安全措施的认识方面发挥激励和主导作用。”

同样的旧威胁

杜登霍夫尔认为，成员国认识到目前威胁与其50年前所面临的威胁之间的相似性很重要。

> 国际原子能机构已推行大量计划，对成员国提供有关这些问题的教育，并帮助他们管理和战胜威胁。

这名核安保专家说：“实施威胁者没有改变。企图偷窃或勒索人们的犯罪因素一直存在。反对者——恐怖分子或有不满情绪的雇员——一直存在。核设施和放射性设施总是需要受到针对这些威胁的保护。目前很大不同之处是，这些威胁行动者可以就地或远程利用计算机系统从事其卑鄙勾当。”。

网络威胁是一项国际挑战。在成员国为保护核设施开展的计算机安全措施建设和测试努力方面，国际原子能机构向其提供支持。（照片由istockphoto.com网站提供）

国际原子能机构新闻处萨沙•亨里克斯。