



提升企业网络复原力的方法

文/安·布莱迪 By Ann Brady

在这个日益数字化、充斥着虚假信息和假新闻的时代，最大的挑战是建立对技术本身的信任。

现在，无人不知网络安全的重要性，无人不晓网络攻击对电脑、智能手机和其他设备造成的威胁。我们总能收到提示，千万不要泄露密码，要小心垃圾邮件和钓鱼邮件，这些邮件会企图操纵用户泄露各类密码、银行账户信息、社会保险或医疗资料等个人信息。

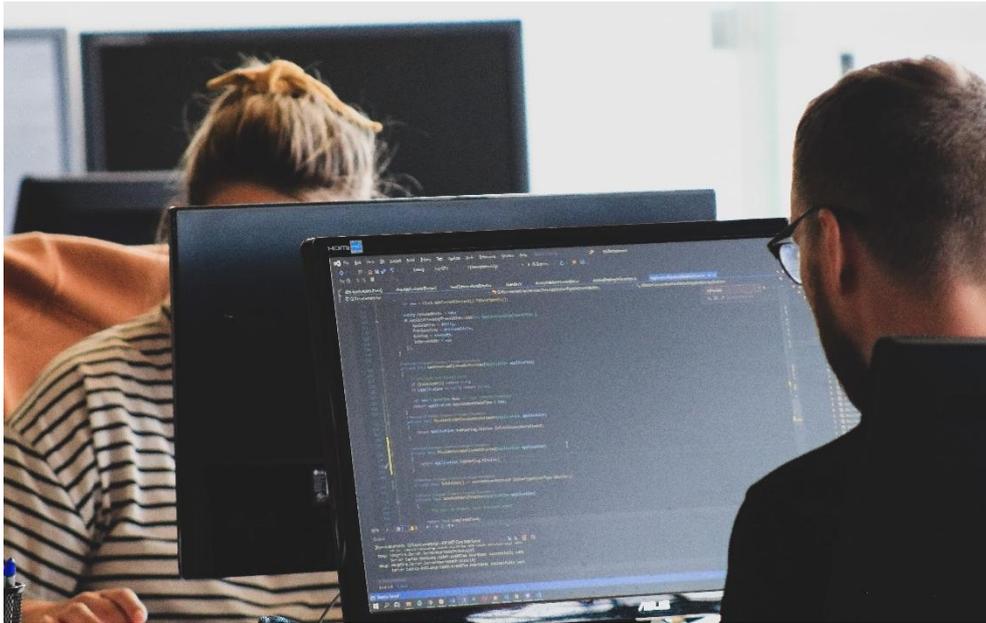
到 2025 年，全世界每年由于网络犯罪造成的损失将达到 10.5 万亿美元。

身份盗窃问题十分棘手，而当受攻击目标是政府和其他主要机构时，情况会更加复杂恶化。由英国广播公司（BBC）出品的热门电视剧《真相捕捉》（The Capture）的宣传语为“眼见为虚”，该剧探讨了被称作“21 世纪 PS”的深度伪造技术所带来的巨大冲击，威胁国家安全，动摇国本，摧毁信任，让人们怀疑现实。

该剧在许多方面可能有些夸张，然而随着第四次工业革命的深入发展，我们发现，该剧突出了飞速发展、愈加复杂的技术带来的潜在风险和威胁。

提高网络风险的优先级

世界经济论坛的[《2022 年全球网络安全展望》](#)报告指出，网络领导者们将网络攻击造成的基础设施故障视为首要风险，其次是身份盗窃。报告也表明，尽管 85% 的网络领导者认为提高所在组织的网络复原力是首要任务，但要将这类风险的优先级别提到其他众多紧迫事项之前，却很难获得决策者的支持，而我们需要严肃对待这个挑战。《网络犯罪》（CyberCrime）杂志认为，网络攻击很有可能令一座城市、一个州，甚至整个国家的经济瘫痪，到 2025 年，全世界每年由于[网络犯罪造成的损失](#)将达到 10.5 万亿美元。



网络安全议题并不新鲜，然而随着世界日益互联和碎片化，个人、组织机构、服务和系统面临网络攻击的风险越来越大。随着技术日益成熟，网络罪犯也越来越精明。在这个充满不确定性的时代，信任弥足珍贵。对系统安全的信任和保证是人们的基本要求，而 ISO 的两项国际信息技术标准 ISO/IEC 15408 和 ISO/IEC 18045 有助于人们恢复对技术的信任。

米盖尔·班侬（Miguel Bañón）是网络安全评估和认证专家，也是 ISO 和国际电工委员会（[IEC](#)）安全评估、测试与规范工作组的召集人。他认为，这两项标准就像“自行车的脚踏板”一样协同工作，ISO/IEC 15408 建立了 IT 安全的评估标准，而 ISO/IEC 18045 明确了 IT 安全评估的方法。不过在实际应用上，这两项标准是相同的。

要想在市场上取得成功，必须取得客户的信任。

及时修订标准

近期，这几项标准的修订非常及时，能不断满足复杂的新时代需求。班侬说，“工作组重点关注技术保障、测试认证，并提供确保技术本身安全性的标准。这

也是解决方案的重要组成部分。”标准有助于采用整体全面的方法进行信息管理，但技术安全是根本性基础。

要想在市场上取得成功，必须取得客户的信任，对于技术来说，也是一样。面对快速涌入市场的琳琅满目的新产品，例如智能互联汽车，如果我们对它没有把握，又怎么能放心让它自动驾驶呢？

班依称，通过 ISO/IEC 15408 和 ISO/IEC 18045 这两项标准，“我们提供了国际公认的最佳、也是唯一的产品和系统安全性测试和评估方法”。他指出，曾经的小众领域网络安全如今成为了主流，而市场本身将网络安全视为先决条件，决策者和领导者们必须要进一步提高对网络风险的重视程度。

市场将网络安全视为先决条件。

建立网络复原力

政府对这一问题也越来越重视。班依表示，网络安全引起了广泛的关注，带来了许多积极成果，例如即将出台的欧盟立法将提出强化网络安全系统。他说，“《欧盟网络安全法案》的实施为全欧洲的认证工作提供了统一框架。过去，如果你想对产品进行安全认证，需要以各国家体系为依据，而现在，首个泛欧洲产品认证体系即将推出，这是基于 ISO/IEC 15408 制定的”。

他还指出，IT 安全并非新议题，此前的标准实施已经给市场上的产品带来积极影响。“通过遵循操作系统或网络设备等标准的要求，许多传统产品不断发展和改进，使黑客不得不另寻‘更容易’攻破的产品或界面了，”他说道。

符合 ISO/IEC 15408 的产品或界面需要高度成熟，对攻击有较强的抵抗力。对于当今我们常听到的重大安全破坏事件，班依认为，很有可能是因为黑客针对

未经该标准认证或分析的产品下手。“假设你是黑客，你会针对整个链条上最薄弱的环节，而现在最简单的途径就是攻击未经标准认证的产品”，他说。

独立而公正

信任是根本性问题。班依指出，“我们的标准首先对产品进行非常严格、独立而公正的审查，再做一系列评估和认证，确保得到用户的信任”。举个例子，谁都不想买到不符合安全规定的洗衣机，所以标准合规是“市场的需求，也是网络安全方案在全球大获成功的基础”，既防范了恶意攻击，又能让用户安心。

ISO 中央秘书处和中国国家标准化管理委员会（SAC）
授权中国标准化杂志社翻译中文版