网络安全

新闻资料 | 2017 年 9 月

在电力和供水系统、交通系统和工厂控制系统等利用 IT 系统运营的关键基础设施中，IT 安全扮演着至关重要的角色。随着这些基础设施开放程度的不断提高，它们遭受攻击的可能性也越来越大。加之市场需求和法律规定的影响，对西门子产品和解决方案的安全要求不断提高。

西门子中央研究院有及时防范和系统防御方法领域的专家。特别是处于开发初期的 IT 安全整合能够实现产品增值，避免延迟产品发布时间。

攻击和工业间谍

- 根据德国数字协会 Bitkom（2015 年 4 月的一项研究）的保守分析，由于数字工业间谍、蓄意破坏和数据盗窃，德国每年遭受的损失高达 510 亿欧元。
- 无数黑客集团都试图进行工业间谍活动，并常常通过互联网浏览器和电邮系统进行攻击。
- 社会工程攻击越来越频繁，直接通过物联网（IoT）和不受保护的 IoT 设备进行攻击。
- 西门子每天接收 350 万至 400 万封电邮，其中约有 50%的电邮为垃圾邮件或者携带病毒链接。
- 西门子全球有多家信息安全运营中心（CDC），为自身和客户提供保护。比如，一个 CDC 每个月记录 1000 条左右警报。其中约 30 条是特别紧急事件，由隶属于西门子中央研究院的西门子网络紧急响应小组集中处理。

安全责任

从今年 10 月起，西门子 IT 安全责任被分为两部分：

- 西门子中央研究院负责管理公司范围内的信息安全以及产品和解决方案安全。
- 全球服务信息技术部门负责实施信息安全。

设计安全

西门子中央研究院的专家通过“设计安全”将安全系统性地整合进过程和产品。这意味着安全已被融入产品生命周期，从产品开发直至运行。

技术方面包括：

- 安全通信（授权和加密等）
- 访问控制
- 系统性强化，集成补丁管理和安全测试
- 用户友好性，这样用户能正确使用安全防范措施

我们自己的黑客和金块

- 西门子中央研究院的专家负责监控西门子的系统，常常能及时发现攻击或通过采取保护措施防止遭受攻击。比如说勒索病毒，黑客可以从外部禁用计算机，在拿到赎金前不会提供代码以重新启动计算机。凭借预防性措施，迄今为止西门子几乎从未遭受过此类攻击所带来的损失。
- “金块”指的是具有战略重要性的关键数据，它的丢失会给西门子造成重大损失，因而被划分为特殊类别，由西门子采用综合方法进行单独保护。
- 将应用和系统转移至互联网是当前的趋势，因此云端安全机制也同样重要。西门子中央研究院专家正在这个领域进行努力，比如用户身份监控和访问权限等。
- 为了在遭受网络攻击前找到安全漏洞，西门子中央研究院拥有自己的黑客团队，其工作内容就是渗透西门子系统。

处理西门子产品中发现的薄弱点

- 如果在西门子产品或西门子产品集成的第三方组件中识别到了薄弱点或缺陷，我们成熟的流程可尽快消除这些问题并向客户提供建议或补丁。

网络安全的数据分析

在各类应用中，数据分析都在数据安全中扮演着至关重要的角色，如检测攻击和损坏评估。随着安全相关数据的不断增多和网络攻击复杂性的不断增强，IT 安全分析人员利用高性能分析方法愈发重要。西门子中央研究院的 IT 安全专家和数据分析专家在这方面协作，从数据中生成可用信息和安全情报，从而帮助业务部门获得改进的服务和解决方案。