针对工业基础设置的定向攻击

事件背景

- Stuxnet 蠕虫对西门子公司的数据采集与监控系统SIMATIC WinCC 进行攻击，成为了第一个直接攻击现实世界中的工业基础设施的恶意代码。

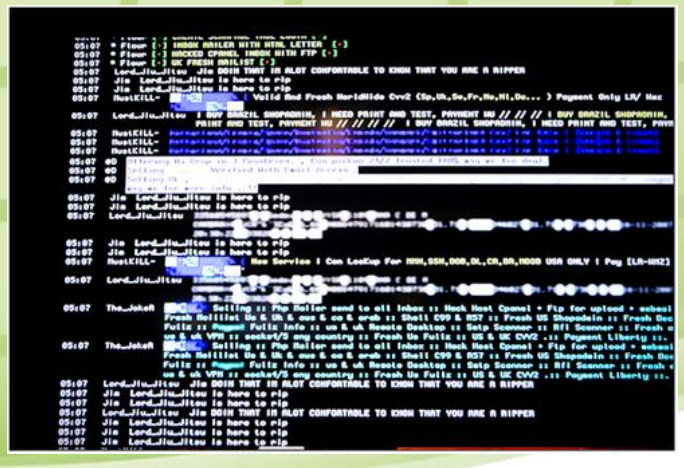
案例特征

- 到目前为止利用了至少4个微软操作系统漏洞（包括3 个新的零日漏洞）和2 个WinCC系统的漏洞。
- 伪造了RealTek驱动程序的数字签名

企业的多重资源成为攻击目标

事件背景

- 零售商TJX18个月内被某入侵者盗取了超过4500万张信用卡和借记卡号码，并最终用于”地下交易”



案例特征

- 黑客呈现很强的趋利性，并有完善的地下经济体系为其创造获利环境

企业面临的合规要求趋紧

行业规范

行业顾问自行补充

信息安全监管

等级保护

资本市场要求

SOX404

通用行业的安全最佳实践

ISO/IEC 27000 系列

NIST SP 800 系列

ITIL

信息系统承载越来越多的业务使命

信息系统安全可靠，风险可控，并最终将系统安全优势转化为业务优势

核心信息资产

行业顾问自行补充

主要信

行业顾

安全服务框架

PSS
规划咨询服务

规划设计

安全战略规划
系统架构设计
安全域划分
ISMS设计

合规咨询

SOX缺陷修补
等级保护咨询
ISO27001认证辅导

风险管理

脆弱性管理
威胁管理

MSS
可管理安全服务

安全测试

产品评价测试
渗透测试
代码审计

配置管理

上线评估
基线核查
补丁管理

安全照料

自有产品代维
产品值守
网站照料
钓鱼监控

事件管理

安全预警
应急响应
调查取证

RSS
安全研究服务

漏洞挖掘和分析

挖掘、分析、监控各类安全威胁和漏洞，预测安全行业趋势发展

ESS
教育&培训服务

安全技能培训

与岗位职责匹配，因事定岗，因岗定人，建设资深安全专家团队

人员安全意识教育

针对内部员工、合作伙伴以及第三方人员，宣贯安全操作风险意识，

ASS
安全评价服务

岗位职责设计

以责任矩阵的形式，通过流程化视角和部门岗位视角清晰定位安全职责

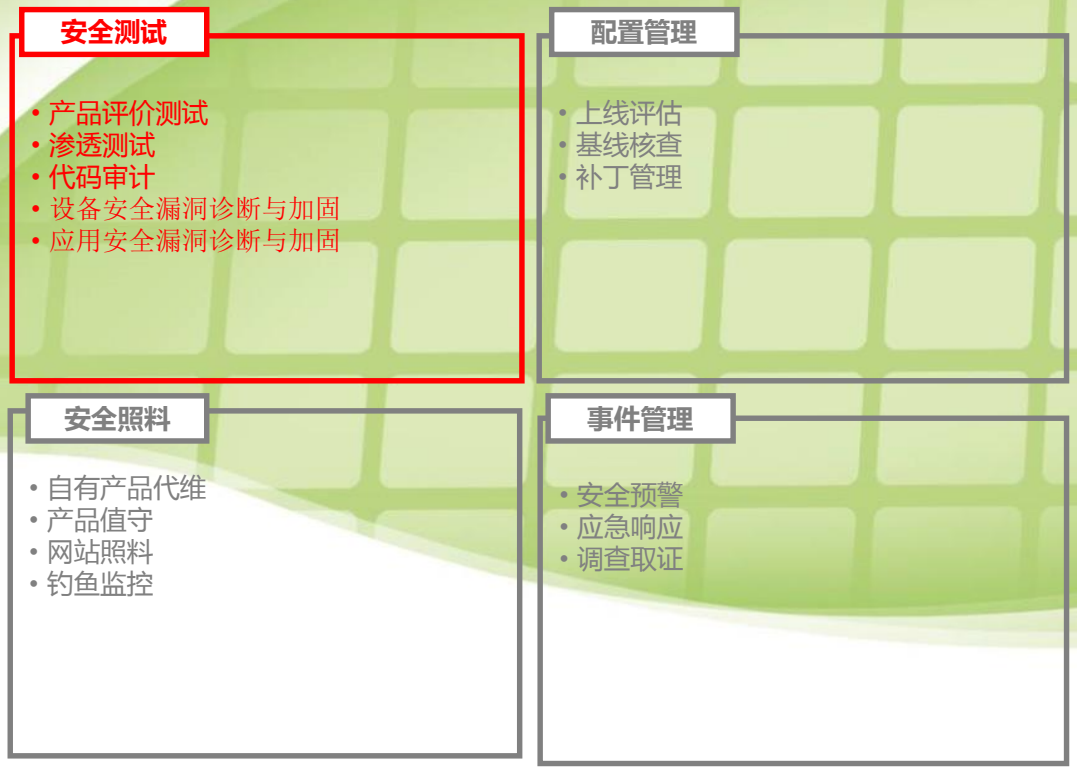
测量和度量

建立安全指标体系，把控安全成本和效率，提供决策支持

审核辅导

针对安全外部审核和检查，提供辅导支持

MSS 可管理安全服务



特色模块

设备安全漏洞诊断与加固

应用安全漏洞诊断与加固

渗透测试

– 专业渗透测试人员依据流程，基于对**攻击者**能力的全面了解，推演可能攻击方式的威胁测试手段

- **MSS 可管理安全服务：** Managed Security Services (MSS) 提供 7x24x365 监控和记录客户端、服务器、各类应用以及其他IT基础设施的脆弱性以及危险事态；提供实时防护和及时响应，降低成本，提升效率

MSS 可管理安全服务

特色模块

基线核查

– 为企业提供定制化的基线模板，全面与各类基线规范兼容，为安全服务提供的开发和标准化的框架

- **MSS 可管理安全服务：** Managed Security Services (MSS) 提供 7x24x365 监控和记录客户端、服务器、各类应用以及其他IT基础设施的脆弱性以及危险事态；提供实时防护和及时响应，降低成本，提升效率

MSS 可管理安全服务

特色模块

- 安全巡检服务
  - 在开展过安全测评或诊断、加固服务的基础上，通过远程或现场方式，对服务器及安全产品安全策略、配置修改、补丁更新、应用系统安全漏洞等情况开展定期的安全巡检，及时发现、抑制、防范网络攻击行为的发生，并提供相应的整改措施与建议。

- **MSS 可管理安全服务：** Managed Security Services (MSS) 提供 7x24x365 监控和记录客户端、服务器、各类应用以及其他IT基础设施的脆弱性以及危险事态；提供实时防护和及时响应，降低成本，提升效率

MSS 可管理安全服务

特色模块

- 安全事件应急响应
  - 通过响应工程师提供远程安全支持和现场安全支持服务，帮助客户分析、定位安全事件，协助客户降低影响，快速抑制和恢复客户系统，并帮助客户追踪取证。

- **MSS 可管理安全服务：** Managed Security Services (MSS) 提供 7x24x365 监控和记录客户端、服务器、各类应用以及其他IT基础设施的脆弱性以及危险事态；提供实时防护和及时响应，降低成本，提升效率

PSS 安全咨询服务

特色模块

- 系统安全架构设计
  - 从企业业务安全需求出发，基于**SDL**的安全生命周期的系统安全设计，通过最小的成本，实现灵活度最大的安全

PSS 安全咨询服务： Professional Security Services (PSS) 提供全方位的企业层面安全评估、合规咨询、规划、设计和部署服务，助力建设企业级安全解决方案。

PSS 安全咨询服务

ISO27001认证辅导

- 通过业界最佳实践指导企业信息安全建设，遵循PDCA思想构建信息安全流程和制度体系

信息安全等级保护评测辅导

针对部分符合和不符合的测评项提供整改支持，包括机房设计缺陷的弥补措施，机房基础实施选型和部署；网络结构调整和优化，网络设备、网络安全设备采购需求设计及安全策略的配置；服务器安全策略的配置及系统加固实施；协助应用系统开发商完成应用系统安全加固；数据安全及备份策略的制定和实施。对于暂时无法整改的问题，提供问题弥补和风险弱化的建议。帮助客户建立由安全方针、安全策略、管理制度、操作规程等构成的全面信息安全管理制度体系

PSS 安全咨询服务：

Professional Security Services (PSS) 提供全方位的企业层面安全评估、合规咨询、规划、设计和部署服

PSS 安全咨询服务

亮点模块

- 威胁管理
  - 通过运用**STRIDE**威胁模型，从业务功能出发，通过受攻击面和数据流找到攻击者的立足点

PSS 安全咨询服务： Professional Security Services (PSS) 提供全方位的企业层面安全评估、合规咨询、规划、设计和部署服务，助力建设企业级安全解决方案。

RSS 安全研究服务

业务逻辑分析

工具开发

漏洞挖掘

逆向工程

黑盒测试

恶意代码分析

RSS 安全研究服务：挖掘、分析和监控包括IT基础设施漏洞、恶意代码等各类安全威胁和脆弱性，预测安全行业趋势与发展

安全评价服务

岗位职责设计

- 以责任矩阵的形式，通过流程化视角和部门岗位视角清晰定位安全职责

测量和度量

- 建立安全指标体系，把控安全成本和效率，提供决策支持

审核辅导

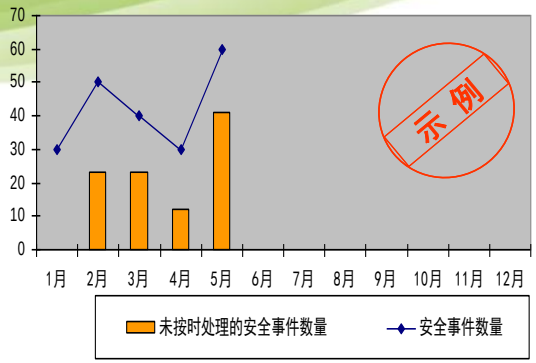
- 针对安全外部审核和检查，提供辅导支持

安全评价服务：着眼安全过程和有效性，为管理层提供安全管理的测量尺度与工具，从而证明安全的必然性

关键指标示例：

- 策略更新频率
- 安全策略总体符合情况
- 单个标准符合情况
- 未及时删除/挂起的帐号或权限数量
- 帐号权限检查的不符合比率
- 定期进行帐号权限检查的执行比率

月度安全事件监控



培训与教育服务

◆第一阶段：满足知识/技能要求

»将安全厂商多年积累的深厚技术功底与业界优秀培训体系相结合
»满足信息安全工作技能要求

◆第三阶段：为企业将“安全”融入公司文化提供氛围

◆第二阶段：协助客户建立安全培训体系

»固化培训课程体系
»降低来自商业伙伴和供应商的风险
»为企业安全岗位人员提供发展路标

»完善知识/技能管理，逐步形成内部安全教育模式和核心团队

培训与教育服务： 提供知识/技能支撑，降低各类人力资源风险；建立企业信息安全知识库