新形势，新思维，新举措

企业网络安全新思考

Contents

企业安全的新形势

LOGO

企业信息安全进步

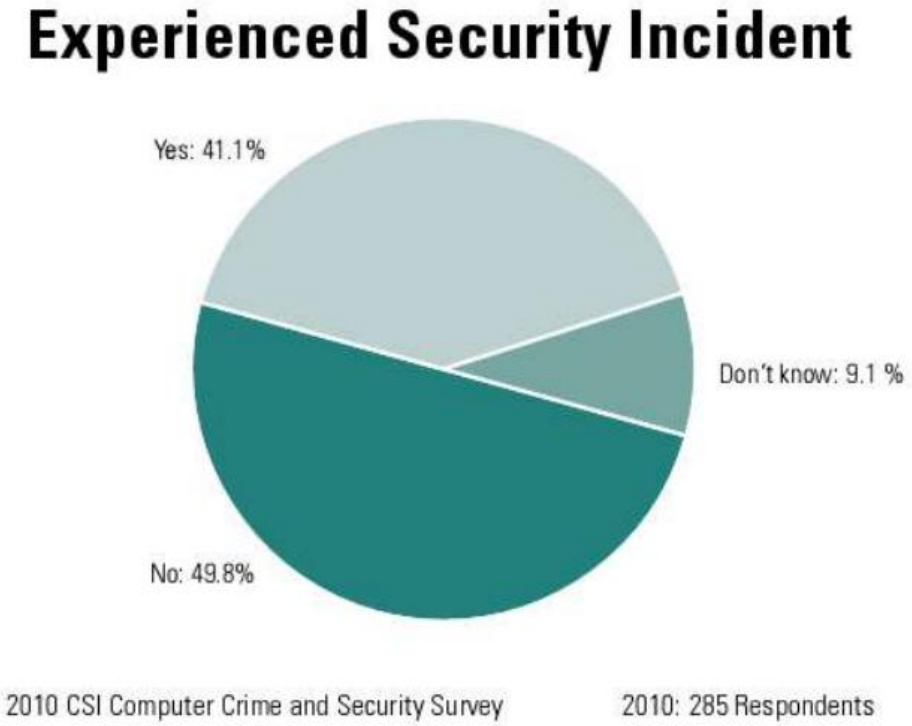
- 信息安全规范普及
- 安全设备广泛使用（IDS,IPS,FIREWALL）
- 信息安全培训普及
- 信息安全体系完善（安全开发，运维安全，IT安全基线）

企业安全的新形势

LOGO

已知遭受入侵的机构/企业比例：

- CSI 《2010/2011 Computer Crime and Security Survey》
- 41.1%的机构/企业遭遇到了计算机安全事件，9.1%无法确定



调查范围：

- 世界351位计算机安全从业人员；
- 涉及咨询、金融、教育、政府机构、零售业、制造和信息行业；
- 所在公司的人数从100到50000不等。

企业安全的新形势

LOGO

超级工厂病毒攻击简介:

- 超级工厂病毒（Stuxnet）在2010年7月开始爆发。它利用了微软操作系统中至少4个漏洞，其中有3个全新的0day漏洞，为衍生的驱动程序使用有效的数字签名，通过一套完整的入侵和传播流程，突破工业专用局域网的物理限制，利用WinCC系统的2个漏洞，对其开展攻击。
- 它是第一个直接破坏现实世界中工业基础设施的恶意代码。据赛门铁克公司的统计，目前全球已有约45000个网络被该蠕虫感染，其中60%的受害主机位于伊朗境内。伊朗政府已经确认该国的布什尔核电站遭到Stuxnet的攻击。

企业安全的新形势

企业安全的新思维

LOGO

企业安全难点

- 企业业务复杂（复杂的供应链，技术水平参差不齐的供应商）
- 安全部门尴尬地位（业务为先）
- 企业安全防御系统的孤岛状态（各种系统独立工作）
- 安全体系的问题（策略推广困难）

企业安全的新思维

LOGO

职业黑客组织

- 专业的技术团队
- 完善的信息收集分析机制
- 完善的技术研发体系（漏洞研究和挖掘，专业工具开发，对抗技术研究）
- 完善的模拟环境和测试环境

企业安全的新思维

LOGO

新思维

- 安全部门地位
- 安全部门组成（更多部门的人员参与）
- 安全培训的侧重
- 安全架构新体系（增加安全纵深，新的安全账户体系）
- 安全新系统（更智能化的分析系统，SOC系统，应急响应体系）

企业安全的新举措

LOGO

新举措

- 安全部门建设
- 安全培训设计
- 新安全架构体系
- 新安全系统

企业安全的新举措

LOGO

安全部门建设

- 更多业务部门参与
- 安全人员参与业务设计
- 安全人员对企业整个供应链环节都参与

企业安全的新举措

LOGO

安全培训设计

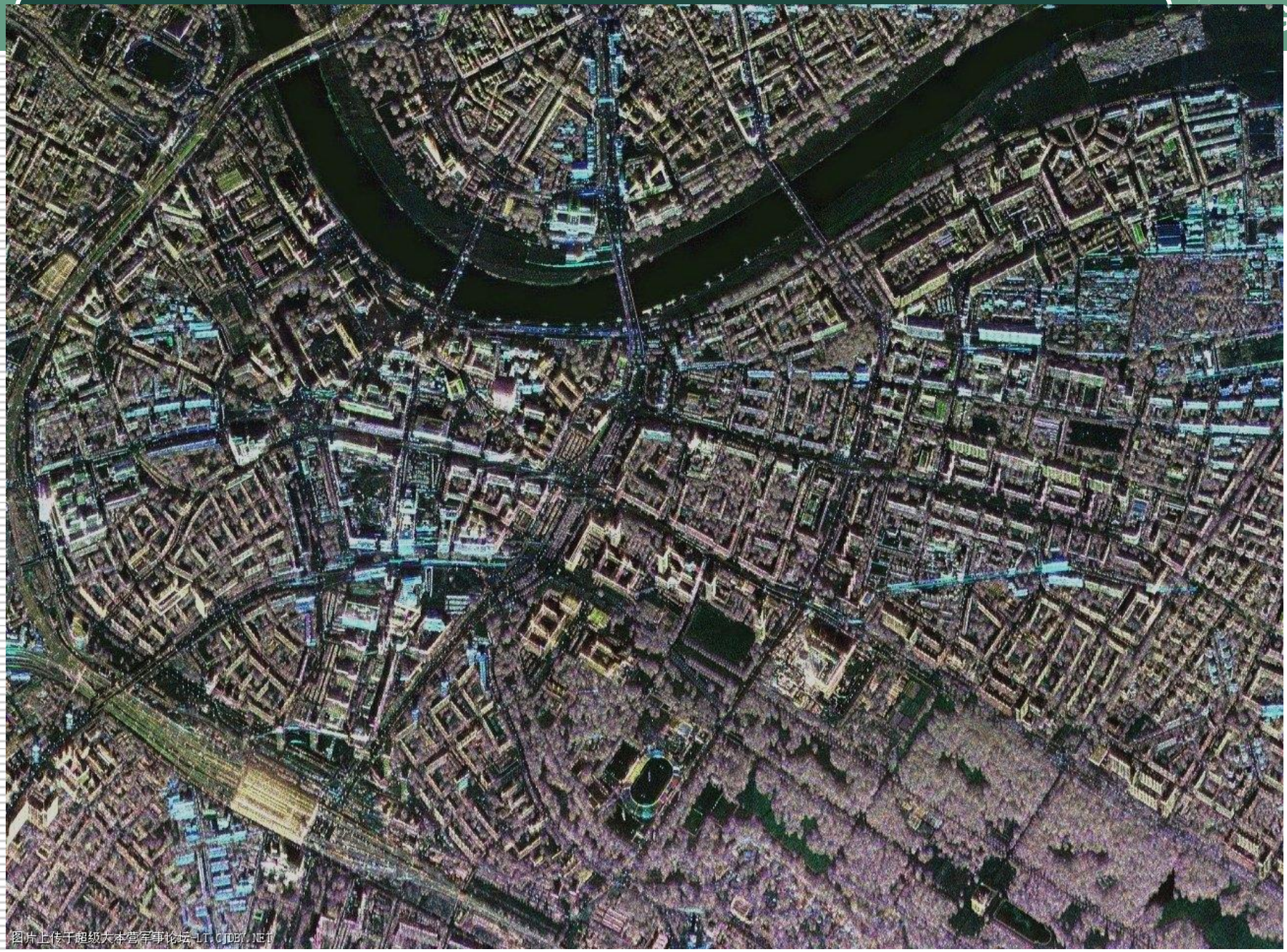
- 加强安全意识教育(使员工承担企业信息安全中的个人责任)
- 针对员工个人安全培训(让员工认识到防护技术可能被突破)
- 企业高管教育

企业安全的新举措

LOGO

新安全架构体系

- 增加网络纵深（延缓攻击）
- 更新员工账户体系
- 应用系统设计逻辑安全检查
- 完善的监控系统


图片上传于超级大本营军事论坛-LT.CJDBJ.NET

企业安全的新举措

LOGO

新安全系统

- 更多的信息收集系统（网络异常，系统异常，应用异常）
- 更智能化的数据分析系统（更多分析方法）
- 良好的监控系统（半智能化的分析）
- 更科学的分析机制
- 专业的安全运营团队
- 良好的业界信息合作交换体系

总结

LOGO

转变

- 重视运营和重视创新
- 从全面保护到重点保护
- 安全保护围绕保护数据为中心
- 从传统的保护和阻止到监控和分析
- 对安全事件深度挖掘
- 从无法接受安全事件到损失可控
- 业界合作是主流

Thank You !