标准服务

网络安全 | 数据安全 | 应用安全

网络安全

钓鱼邮件训练

通过向员工发送类似病毒邮件，以钓鱼邮件的点击率对员工的信息安全意识进行确认，达到提高员工安全意识的目的，可有效避免员工从可疑邮件中感染病毒，保护企业免受钓鱼邮件攻击。

训练目的

- 通过定期邮件训练，提高员工信息安全意识，降低企业信息安全风险
- 通过演练模拟，帮助企业和组织对内部人员进行针对性的安全意识培训

服务价值

- 提高员工安全意识
- 掌握员工安全意识状况

核心要素

- 邮件正文的形式(HTML链接类型)
- 邮件模板可自行定义
- 演练数据报表以及图表化报告

安全网络接入

本服务以解决内网安全问题为目的。在现实中，办公网络经常会存在一些安全漏洞，例如个别计算机终端疏于安装操作系统安全补丁、未及时升级防病毒软件等，这些安全漏洞易于被黑客用作攻击企业内网的入口或跳板，造成内网阻塞并瘫痪、内部关键数据失窃，给企业带来巨大的经济损失。

解决课题

- “非法”设备无法接入
- “合规”用户全无感知
- “脱缰”终端限制访问
- “流程”管理一目了然

实现功能

- 用户身份入网管理
- 终端安全检测检查
- 动态授权访问资源

实施效果

- 合规的人做授权的事
- 不合规的电脑禁止入网

系统运维及安全审计

当公司需要运维的设备越来越多，需要参与运维的人员也越来越多时，如果未建立起一套有序的机制，就难免会产生运维混乱，导致无法高效地掌握究竟哪些人被允许以哪些身份访问哪些设备。通过导入安全运维审计系统让“运维混乱”变得“运维有序”。

解决课题

- 管理和分配全部账号，对运维人员的运维操作进行严格审计和权限控制，确保运维安全合规和运维人员最小化权限管理
- 不改变现有网络环境和网络拓扑的情况下，接入核心交换机中

实现功能

- 统一运维入口
- 统一自然人与主机帐号间的权限关系
- 统一运维操作审计管控点

导入工具

- 安全运维审计系统

多因子身份认证

属于一种计算机访问控制方法，旨在提高安全性。用户只有在通过两种以上的认证机制认证之后，才能获得使用计算机资源的授权。例如，用户需输入PIN码，插入银行卡，然后再经指纹比对后，才能最终获得授权。

解决课题

- 提升应用及系统的登录安全，消除弱身份鉴别带来的潜在信息泄漏风险

认证方式

- 帐号+静态口令
- 短信令牌（短信验证）
- 硬件令牌（UKEY）
- 手机令牌

导入设备

- 认证服务器
- 代理客户端
- 动态密码器

数据安全

数据防泄密系统

为防止用户利用电子邮件、聊天工具、网盘、U盘、打印等途径泄露数据，本系统基于内容识别技术，对设计图纸、源代码、合同文本、财务报表等敏感文件进行数据安全保护，同时还能对用户泄密行为进行记录、警告、阻断，并对用户行为进行审计。

解决课题

- 对终端上的敏感数据进行安全防护，防止通过终端途径泄露敏感数据，保护企业及个人终端的数据安全

核心功能

- 文档透明加解密
- 文档分级授权操作控制及审计
- 外发电子文档管理及控制
- 文档安全网关集成应用

导入设备

- 数据防泄密系统
- 数据防泄密系统服务器
- 文档加密安全网关

磁盘加密系统

作为一项数据保护功能，通过与操作系统集成，来应对计算机丢失、被盗或销毁不当所带来的数据泄露威胁。

解决课题

- 在电脑磁盘、移动存储等存储介质发生丢失或被盗时，保障使用者的磁盘数据不被泄露或窃取

核心功能

- 强大加密功能保护磁盘数据安全
- 透明的验证和授权确保用户无感知
- 可靠访问加密数据
- 集中式管理监控

导入设备

- 磁盘加密控制中心软件
- 磁盘加密控制中心服务器

数据库脱敏系统

作为针对敏感数据进行抽取、漂白和动态掩码的专业数据脱敏产品，可以满足面向测试、开发、培训和数据共享场景的生产数据安全需求，做到“用”“护”结合。

解决课题

- 防止生产库敏感数据泄露、提高数据维护和数据共享安全性、实现隐私数据管理的政策合规性

核心功能

- 依托精准协议解析，准确识别敏感数据访问行为
- 丰富脱敏算法（也可根据自身环境进行自定义），保障数据可用性
- 完善的脱敏审计记录，并提供详细的语句详情页面

导入设备

- 数据库脱敏系统

数据库运维及安全审计

基于多因子身份认证与访问控制的数据准入技术，针对数据库账户、应用工具、主机名、IP地址、数字证书、登录时间、操作行为等相关因子，构建多因子数据库运维及安全审计。

解决课题

- 针对DBA管理员和驻场合作伙伴、运维开发人员运维身份进行合规管理，实现敏感数据隔离，使运维操作规范、透明、可控

核心功能

- 数据库准入、特权账号访问控制
- 运维人员管理、工具访问控制
- 数据对象防篡改
- 动态脱敏
- 工单流程

导入设备

- 数据库运维和审计系统

应用安全

代码审计

通过自动化工具或者人工审查方式，逐条对程序源代码进行检查和分析，查找存在的安全缺陷或者编码不规范之处，发现由此而引发的安全漏洞，并提供代码修订措施和建议。

解决课题

- 代码审计是对编程项目中源代码的全面分析，旨在发现错误、安全漏洞或违反编程约定

核心功能

- 前后台分离的运行架构
- Web服务的目录权限分类
- 认证会话与应用平台的结合
- 数据库的配置规范
- SQL语句的编写规范

实施效果

- 源代码审计工具可用于辅助查找常见漏洞，从而节省时间，但不应依赖深入审计，且该工具仅适用于特定的编程语言，建议将其作为基于政策的方法的一部分

漏洞扫描

作为一种以发现可利用漏洞为目的的安全检测（渗透攻击）行为，本服务基于漏洞数据库，通过扫描等手段对远程或本地的指定计算机系统的安全脆弱性进行检测。

解决课题

- 及时准确地察觉到信息平台基础架构的安全，保证业务顺利、高效开展，维护公司、企业、国家信息资产安全

核心功能

- 定期网络安全自我检测、评估
- 安装新软件、启动新服务后的检查
- 网络建设和网络改造前后的安全规划评估和成效检验
- 网络承担重要任务前的安全性测试

导入设备

- 针对网络的扫描器
- 针对主机的扫描器
- 针对数据库的扫描器

Web应用扫描

通过Web前端与Web应用程序通信，可以自动检查Web应用程序，探测、分析其响应，从而发现潜在的安全问题和架构缺陷。

解决课题

- 通过扫描检测，可以帮助用户充分了解Web应用存在的安全隐患，建立安全可靠的Web应用服务，改善并提升应用系统对抗各类Web应用攻击的能力

核心功能

- 对Web应用深度遍历，以安全风险管理为基础，支持各类Web应用程序扫描
- 提供丰富的策略包，针对各种Web应用系统以及各种典型的应用漏洞进行检测
- 通过当前弱点获取数据库的相关敏感信息，对后台数据库进行配置审计，如弱口令、弱配置等

实施效果

- 通过当前弱点，模拟黑客使用的攻击手段，对目标Web应用的安全性做出深入分析，并实施无害攻击，取得系统安全威胁的直接证据

网页防篡改

对Web页面文件进行完整性保护的技术措施，通过对Web服务器上的文件进行监控，一旦发现恶意更改行为就立即采取相应的处置措施，避免来自外部或内部非授权人员对网站页面文件进行的非法篡改和添加。

解决课题

- 网页防篡改系统可以用于Web服务器，也可以用于中间件服务器，其目的都是保障网页文件的完整性

核心功能

- 对需要保护的文件进行备份
- 事件触发

技术支持

- 定时循环技术
- 摘要循环技术
- 事件触发防范技术
- 底层过滤技术

客户案例及资料获取

咨询电话

欢迎您致电了解产品服务信息

021-5887-1000 转市场营销部

受理时间：9:00~17:00（周末及法定假日除外）

邮件联络

欢迎您通过邮件咨询产品服务信息

mimarcom@fujitsu.com

我们通过技术手段保障您的个人信息安全