登录

【企业安全】企业安全威胁简述

aerfa / 2018-03-25 22:45:55 / 浏览数 1613 技术文章 企业安全 顶(0) 踩(0)

企业面临的威胁可以说是来自四面八方，既有恶意的外部攻击者，也不排除来自内部的安全隐患。往往在不经意间，又可能引入新的安全因素，也有可能在输出产品时给其他

■■■■

■■■■

■■■■

■■■■

输入威胁分析

■■■■■■■■■■■■

■■■■■■■■■■■■

■■■■■■■■■■■■■■

企业常常需要向其他公司采购软、硬件设备，或采用第三方开源框架与组件进行开发。相关部门如果缺乏安全意识，就很有可能不经过任何安全相关评估，将安全风险带到公

等待信息安全组沟通、验证回归漏洞完毕后，继续走流程购买付款，然后系统正式上线。在整个过程中，可见安全已经介入但出现较晚。在整个过程中，可见安全已经介入但
曾有供应商提起，他们的系统经过某银行严格安全检查，并成功入驻，还向我们展示了部分检测报告。但在我们进行安全测试时，结果却不十分理想。刨根问底一番探究后，
难怪隔行如隔山，此类大跌眼镜、没有把安全落到实处的情形，估计还有不少。那问题来了，如何有效的对输入威胁进行有效控制？显而易见的是需要将安全提前，在业务方

内部威胁浅析

企业内部威胁主要来自于人，如果细分的话可以从安全意识、相关制度、内网管控等方面进行考量，比如：

&内鬼泄露内部机密信息资产

&内部人员主动攻击外部其他系统

&内部系统沦为肉鸡被动攻击外部其他系统

&内部网络混乱，比如访客网络与办公网甚至生产网未做隔离

&内部员工安全意识薄弱，被钓鱼或社工等攻击

&公司内部安全管理制度缺失，员工随意带电脑外出公司或带机密文件出公司

……

实际遇到的情况会比列出来的多、复杂的多、隐蔽的多，但在面对诸多威胁的时候，应该具备发现问题的眼光并深入下去，找到企业欠缺之处的根源，从源头进行修补。没有

外部威胁粗析

竞争对手的长期觊觎，导致雇佣黑客攻击的恶意竞争；

业务发展壮大安全跟不上，导致不法分子的获利攻击；

公司架构采用主流与非主流框架，出现0day时的攻击；

……

“与其落后挨打，不如主动求变”，企业的安全建设只有主动将救火阶段慢慢的转到安全建设，才能在遭受外部攻击时稍微淡定一点。

输出威胁剖析

■■

■■

公司产品（系统）严格控制经过安全测试后，再投入生产及交易。有条件的或时机成熟的公司，落地版的SDL走一遍，不仅是对客户负责，更有可能避免了以后某一天遭到曝

未完待续

企业安全建设系列文章刚开始不久，希望能与大家交流，共同探讨！
本文首发于个人公众号（我的安全视界观），更多文章敬请期待。

点击收藏 | 1 关注 | 2

上一篇：PHP trick（代码审计关注点） 下一篇：客户端 session 导致的安全问题

1. 1 条回复


独自等待 2019-02-14 18:37:12

小兄弟 写的不错，支持。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录