网络安全八个潜规则思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_644146.htm IBM ISS安全策划师Joshua Corman日前透露了网络安全行业8个秘密，真是不看不知道，一看吓一跳。 秘密1：安全厂商不需要预防风险，只有用户需要也正是这个原因才导致了后面的7个秘密，Corman说安全厂商一切都是朝钱看，用户的安全永远是摆在第二位的。位于休斯顿的Wartsila公司IM区域经理Tom Vredenburg和Corman的意见是一致的，他说真不知道现在的安全厂商究竟是软件销售商还是风险管理者，是软件服务商还是网络设计师，用户购买的是伙伴关系还是仅仅只有一个许可。其实他们大多不知道自己究竟在扮演什么角色，他们只知道一味地出售东西。 Cloakware产品管理主管Terry Brown说现在很多安全厂商都在卫自己的观念。由于目前经济的不景气，安全厂商和用户正在制定合理的期望，平衡市场和IT支出。 秘密2：杀软认证忽悠虽然杀软工具可以检测复制类恶意软件如蠕虫，但它们不能识别非复制类恶意软件如木马程序，虽然木马已经在恶意代码之前出现过，Corman说杀软在认证测试时认证方也没有尽心尽力，因此给公司造成了一种虚假的安全感，错误地认为他们采购的杀软可以保护所有的恶意软件。 Corman说目前的木马和其它非复制类的恶意代码构成了80%的威胁，杀软指标参数并没有反映威胁的真实情况。 秘密3：没有安全边界Corman说那些真正相信网络安全边界的人可能也相信这个世界真的有圣诞老人，并不是说没有边界，只是说公司正处于一个被大雾笼罩的边界中，安

全厂商正在悄悄做修复工作。正是由于有了第一个秘密，才会有这第三个秘密，导致公司购买的产品并非总是有效地解决了他们的特殊风险。 他说“ 我们需要确定边界究竟是什么，端点是边界，用户是边界，更可能的是业务流程是边界，或信息本身也是边界。如果你设计的安全控制没有假设一个边界，那将无安全可言，这是人们经常犯的错误，如果在边界处加强的控制，情况就会好很多 ”。 秘密4：安全厂商吹嘘风险管理Corman说风险管理真的可以帮助组织理清其业务和他的高风险等级，但一个公司的优先事项并不总是图安全厂商销售的产品，厂商总是将你的注意力吸引到个别问题上，以引诱你采购他们的产品，如果你不清楚你的风险优先级，厂商都非常乐意为你设置。安全需要要符合和支持你的业务重点，而安全厂商往往希望你的业务符合他们设定的采购组合。 秘密5：还有更多风险Corman说安全市场的大部分产品都与软件漏洞有关，但折算下来，软件漏洞只占其中1/3，另外两成分别是配置不当和人为因素。不幸的是，后两者的风险远高于前者。虽然我们需要找到和修复漏洞，但我们也必须弄明白一个组织的薄弱环节在哪里，更需要注意减小后两者造成的威胁。 秘密6：法律遵从在哪个国家呆着就得遵守那个国家的法律，安全厂商也抓住了这个事实，提供各种各样的产品满足法律的需要，当然这也导致了企业采购的安全工具不能正确处理它们面临的特殊风险。 秘密7：厂商对攻击装着看不见僵尸网络正在被复制和改进，最近两年特别活跃，僵尸网络控制者从发送垃圾邮件到哄抬股票进行诈骗赚了不少的钱。厉害的黑客一般喜欢将杀软当作早餐，这正是由于杀软认证一般都是忽悠造成的恶果。 恶意代码并不需

要漏洞，一般利用的是社会工程，如利用节假日或体育赛事，以及重大新闻事件。但厂商却对这些攻击装着看不见。 秘密8：安全DIY已不在安全厂商力图使用户相信，安全由于其复杂性使得用户已不能独自面对，但是由于不同业务的安全需求的不同特点，仅仅选择产品是不够的。Corman说：“ 仅有对的工具仍然是不够的，还需要针对环境实行正确的安装配置。 ”所以需要IT的专业人员来完成这样的工作是最好的。 编辑特别推荐: 成本速度成关键解析 四种宽带接入技术 常用TCP端口作用及其操作建议 统一通信将成为IP语音未来发展趋势 提高企业网络可靠性的捷径 防御攻击策略之保持领先黑客一步 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com