企业该如何防范由VoIP引发的安全威胁思科认证 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__E4_BC_81_E4_B8_9A_E8_AF_A5_E5_c101_644333.htm 你是否听说过最新的VoIP钓鱼伎俩Vishing的恶名? 它的运行流程如下：易受骗的用户会收到一封电子邮件(或者一个电话)，被告知他的信用卡信息正在被人盗看，然后让他赶紧拨打某个电话号码。这个电话中会有电脑制作的语音提示，让他输入信用卡号码和其他认证信息等等。 这个钓鱼欺诈中与VoIP有关的部分就是这个电话号码。和传统的电话不同，它可以让欺诈者同时用大约800个本地电话号码进行呼叫，只要设置好系统后便可开始自动收集信用卡信息了。而用传统电话，电话公司一般需要确认一项业务是否合法，然后只给在某个特定区域有实际工作场地的公司分配一个本地号码。 Vishing正是最新的VoIP安全恐怖威胁。《Network World》最近就曾报道过，各类VoIP系统，包括很有名气的开放源码系统Asterisk都存在这样的易于被分布式DoS攻击的弱点，这种攻击可以彻底摧毁企业的电话系统。 眼下就有一个相当有名的关于IP犯罪(FoIP)的案子，其中的两名嫌犯侵入了多家企业和服务提供商的网络，“ 卷走 ”了大约1000万分钟的呼叫时长，而受害企业为此付出了人均30万美元的连接费用。此类案例正呈上升势头。 那么，企业该如何防范此类由于VoIP系统而引发的新的安全威胁或者漏洞呢?对于企业来说，需要有专人负责VoIP的安全。这听上去似乎明确而又简单，但你不知道企业里会有多少人认为VoIP的安全理应由安全团队负责，可各个安全团队之间实际上会相互扯皮。假如连该谁负责这样的

小事情都明确不了，那么安全又从何谈起?来源：考试大 再下一步，评估系统的漏洞风险。企业级VoIP威胁一般会有4个主要来源：可用性、隐私、服务窃取以及获得对敏感信息的访问权。可用性涉及是否易受分布式DoS或其他攻击，从而导致VoIP系统掉线。隐私涉及VoIP呼叫的泄密。服务窃取自然是指系统是否易受他人滥用，比如上面所说的FoIP案例。而最后一项则需要考虑Vishing对企业的入侵特性：比如黑客可能会截获某个VoIP呼叫，将其ID修改成“ IT部门 ”，再拨到比如总裁秘书处，精心制造一些场景要求总裁秘书提供总裁的系统口令或其他机密信息。秘书则会认为她是在与IT部门通话，从而轻易地将机密信息泄露给了黑客。 最后，对每一种威胁都需要专门的解决办法。比如要确保可用性，就要确保一般的分布式DoS防范必须准确到位。要确保隐私，可以利用适当的加密技术。要防范服务窃取风险或敏感信息外泄，则需要进行人员培训，具备精准的呼叫监控功能等。 编辑特别推荐: ciscoQOSQueue（队列）一 ciscoQOSQueue（队列）二 ciscoQOSQueue（队列）三 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