2019年七大网络安全威胁预测

时间 : 2018-10-15 编辑 : DNS智能解析专家 分享 :

网络安全是公司的主要关注点，因为安全性差可能导致代价高昂的停机和数据丢失。尽管如此，RSA研究发现73%的组织认为其威胁检测能力不足。以下是您可能在2019年会面临的七大网络安全威胁。

一、勒索软件

这是攻击者在目标计算机上安装软件，锁定对文件的访问权并要求勒索以返回访问权限的地方。FBI声称每天都会对商业网络和家用电脑进行4,000多次勒索软件攻击，Verizon报告发现勒索软件去年造成了39%的恶意软件数据泄露事件。勒索软件是数据意识型企业的主要威胁，这就是为什么只打开可信电子邮件和运行安全软件非常重要。

二、加密劫持

这是一种越来越常见的攻击，网络犯罪分子悄悄地利用计算机挖掘加密货币并从收益中获利。Quick Heal Security Labs的统计数据显示，今年前五个月就有超过300万次这样的点击，而检测到的手机变种数量同比增长了两倍。验证软件的来源以避免攻击者窃取计算机资源是至关重要的。

三、智能手机访问

现代世界越来越流动，这对企业安全构成了新的威胁。戴尔的研究发现，中小型企业中有22%的员工丢失了公司发布的工作设备。与此同时，Ponemon Institute的一项研究发现，只有35%的人表示他们使用密码或PIN码来保护他们的设备。在没有密码锁定的情况下，公司发放的设备在丢失或被盗用的情况下，很可能会造成麻烦。

四、软件缺陷

过时的软件可能会给攻击者留下开放的安全漏洞，特别是随着WannaCry和其他漏洞的崛起。虽然这一直是台式机的一个问题，但智能手机和物联网设备的兴起意味着更多设备能够保持最新状态。确保智能连接设备保持安全是至关重要的。

五、网络钓鱼

网络钓鱼是攻击者伪造合法网站或电子邮件以诱骗受害者移交凭据和敏感信息的地方。Wombat Security发现 6 企业是过去一年中网络钓鱼攻击的受害者。员工需要了解如何在到达收件箱时发现诈骗，验证URL并确保他们 会 向未经验证的来源提供数据。

六、密码错误

一些攻击者可以通过安全等级低的密码练习获得访问权。BBB指出，在网络攻击期间，密码是受影响数据的第一组。要使用安全等级高的密码，字母、数字和符号的组合，以避免攻击者的任何猜测是很重要的。在不同地方最好使用不同密码。

七、缺乏员工培训

在许多情况下，最薄弱的环节是人为因素。有研究发现，各组织中有45%的员工承认没有参加安全培训，而FN伦敦的年度调查发现，大多数员工认为其雇主的IT系统提供了足够的防御攻击保护。攻击者可能会利用警惕意识不高的员工。

来源：https://www.pocket-lint.com/apps/news/dell/145975-7-of-the-biggest-cyber-security-threats-you-ll-face-in-2019-and-how-to-keep-safe

相关推荐：

- 网络钓鱼活动直指对冲基金和金融公司
- DDoS攻击被企业列为最大威胁
- 什么是DNS劫持攻击以及如何避免此类攻击?
- 深入了解最近普遍存在的DNS劫持攻击
- 密码的创建是门学问，要如何鼓励创建更安全的密码是个考验
- 全球DNS劫持活动延伸至联邦域名?
- 玫瑰是红色的，情人节诈骗者是欺骗你的
- 奇怪的网络钓鱼活动使用链接近1,000个字符
- 使用谷歌翻译作为伪装的网络钓鱼攻击被发现
- 帝恩思SSL证书正式上线！！！

客服热线

400-008-0908

企业QQ 9:00-18:00

值班QQ 18:00-9:00

帮助文档
免费DNS
高防DNS
DNS加速
常见问题
销售问题

解决方案
域名注册商
CDN厂商
移动应用
游戏云
硬件

运维工具
域名诊断
IP/本地DNS检测
拨测工具
同步助手