

关键词：企业信息安全

内容概要：

现在企业信息安全态势不容乐观，黑客对漏洞进行重复利用实施长期的潜伏攻击，其实被黑客利用的漏洞并非用了什么高深的手法所得，而往往是些老掉牙的已知漏洞。漏洞发现的早不表明企业已然进行了防护，企业没有及时进行打补丁也是多种因素的合力，系统老化、不...

正文：

现在企业信息安全态势不容乐观，黑客对漏洞进行重复利用实施长期的潜伏攻击，其实被黑客利用的漏洞并非用了什么高深的手法所得，而往往是些“老掉牙”的已知漏洞。

漏洞发现的早不表明企业已然进行了防护，企业没有及时进行打补丁也是多种因素的合力，系统老化、不允许业务中断、底层加补丁后上层应用的兼容性问题等等，这些都导致了企业以业务优先，安全优先级不高的局面。除此之外，配置错误仍是一个显著的问题。服务器配置错误是最为常见的漏洞，会让攻击者轻易潜入系统访问文件，致使企业受到攻击和侵害。且比以往，现在的漏洞给企业造成的损失将更大。



现在的威胁变得更为立体，没有哪个企业敢号称100%的安全。企业始终应居安思危，让安全和响应成为常态。协作和威胁情报共享是整个安全行业联合应对威胁的关键，企业应主动获取可信、可靠的安全情报，更好地采取应对措施和方法，打造更安全的整体环境。同时，也应采用补充防御策略，让防御系统更加牢固。

首要一个就是关于企业信息安全风险意识的话题。老实讲，棱镜门事件引发的蝴蝶效应让网络安全上升到国家高度，而国内企业，特别是银行、电信等支柱行业领域的大企则已对安全问题分外敏感，这与国家主唱的自主可控密不可分，当然，也是一件件突发安全事件折腾教育的结果。总之，企业开始关注IT安全，这是一个好现象。

企业信息安全风险管理不是个立竿见影的活儿，若非出了事故，很难了解安全短板所在，自然也无从评判安全管理的效果。传统IT安全问题可以通过设备采购填补不足，但现在，已不能再孤立地看待安全问题了，盲目堆叠可能还会适得其反，影响效率，更何况你不能置那些财大气粗的企业于不顾。安全事件的发生会让需求变得明显，好过企业在威胁中不知不觉。

人是承担具体运作的主体，若有安全事故发生时，自然也应成为承担责任的主体。且在对事故进行事后分析时，恰恰发现很多时候是人为管理失误造成的；那么在机器学习大规模来临前，企业还是要重视对安全管理团队的培训及建设。

无论是已知的漏洞威胁还是新技术带来的新兴威胁，都处在一个变化的状态，企业的防御也应是灵动而富于变化的，且无论是身处何种行业，企业都必须提高安全的优先级，毕竟没有安全，一切业务也都枉谈。有些安全损害是可以避免的，对企业来说，应当把那些能避免的先避免了，剩下的，交给时间。

西安弈聪信息技术有限公司简介

西安弈聪立足陕西西安，为西安企业提供网站优化，软件开发，软件外包，电子政务，网站建设、企业网络营销咨询服务及实施为主体业务，为客户提供一体化IT技术服务。

西安弈聪现有技术架构包含PHP,asp,.NET.C++,VB,J2EE等，在MYSQL,MSSQL数据库系统，ORACLE大型数据库管理系统开发方面专长，经验丰富，是业内技术服务最全面，技术实力最雄厚的IT技术服务企业之一。

联系电话：029-89322522 4006-626-615 网址：<http://www.xaecong.com> 邮箱:admin@xaecong.com