

简译版

## 安全应跟上企业的发展速度

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Security at the Speed of Business		
原文作者	Craig Riddell	原文发布日期	2018 年 6 月 20 日
作者简介	Craig Riddell 是 SSH Communications Security 公司高级解决方案架构师。		
原文发布单位	Infosecurity Magazine		
原文出处	<a href="https://www.infosecurity-magazine.com/opinions/security-speed-of-business/">https://www.infosecurity-magazine.com/opinions/security-speed-of-business/</a>		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。</li> <li>本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。</li> <li>译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。</li> <li>本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。</li> </ul>		

## 安全应跟上企业的发展速度

Craig Riddell

2018 年 6 月 20 日

跟上企业发展速度的敏捷安全是这样一个概念：安全应该作为端到端设计的一部分。如果不这样做，则必须随着其他解决方案，对系统打补丁、进行更新和修改，以便拼凑出一个安全的环境。

增加一层安全可能是成本较低的方法，至少在一开始是这样的。但是，拥有多种不同的、作为一次性解决方案的设备，会使得企业环境过于复杂，并增加高昂的成本。这会增加总拥有成本，并使企业依赖于出售该解决方案的厂商。与一开始并非设计内容的设备集成，几乎一定会留下威胁源可以利用的漏洞。

### 速度先于安全

可以肯定地说，从历史上看，企业对待安全问题一直采用“事后诸葛”的做法，相比于可能的安全漏洞以及随之而来的后果，企业更担心严格的安全协议会拖慢企业的发展速度。

安全从业人员面临的挑战是，确保架构的每个部分都尽可能地安全（将风险降低到可接受的水平），同时不会降低现代企业所需的速度和增长。在整个数字时代，随着互联网的出现以及迅速用作推广、销售和营销平台，这个挑战一直都存在。安全是次要问题，企业唯一关心的是保障业务连续性（上线运行）。

我们再说说云应用问题。尽管我们对网络安全威胁有了更多的了解，但是，很多企业仍然将数据托管在其他厂商的服务器上，并严重依赖这些厂商来实现安全。有时候，这会出现问题。

例如，在美国国防部（DoD）的 AWS（亚马逊 Web 服务）泄露事件中，其安全取决于提供服务的厂商——亚马逊。国防部部署了适当的系统和 AWS 主机，但其合同商误将 S3 存储设置为可公开访问，导致国防部的绝密数据可以随 Linux 虚拟机的系统映像一起下载。

企业一直有明确的外围防御边界，但是，对云计算来说，如果设计不恰当，它就是平坦无阻的——横向移动不受限制。威胁形势千变万化，企业的防范重点已经从“把攻击者挡在门外”（当然，这一点仍然很重要）发展为“如何知道攻击者已经攻入以及如何应对”。

## 把安全放在第一位

企业应尽早与安全专家进行谈话，敦促他们制定一个计划，使企业在保持安全的同时发展壮大。企业应确保所有适当的对策都已到位，这样，即使企业在本地或云端的业务不断增加，也会将攻击面控制在尽可能小的水平。

企业应向员工授予最低权限，监督和控制交互式访问，并将所有网络流量都视为不可信。他们应采用“零信任模式”并主动检查所有网络流量，以验证用户活动的真实性。

## 保护企业的未来

在任何垂直行业，高管在组建公司或制定公司计划时，都会认真对待网络安全问题。当领导团队制定企业战略时，网络安全都是必须考虑的内容。对于在网络安全成为必需之前成立的公司来说，安全正在被一点点增强。这将导致网络犯罪分子难以找到可以利用的漏洞。但是，无论企业安全从内强化，还是外部加固，他们都将从上述建议中受益。

## 安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队,安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队,为用户提供端点防护、流量监测、快速处置、深度分析等产品,以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门,提供高级威胁和新兴威胁解决方案和能力体系,产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点,全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴,安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可,安天已连续五届蝉联国家级安全应急支撑单位资质,亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点,在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面,提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动,进行了深度的解析,对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上,安天创始人、首席技术架构师作为网络安全领域的发言代表,向习总书记进行了汇报。2016 年 5 月 25 日,习近平总书记在黑龙江调研期间,视察了位于哈尔滨科技创新城的安天公司,对安天负责人说,“你们也是国家队,虽然你们是民营企业”。

安天实验室更多信息请访问: <http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问: <http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问: <http://www.avlsec.com>