贵阳大数据 专稿

[即时发布]

大数据犹如“尖刀上的舞蹈”，亚信安全建议多层次安全管控

【亚信安全】-【2016 年 5 月 26 日】“大数据已经成为商业智能的重要方向，但是，没有安全防护的大数据就犹如‘尖刀上的舞蹈’，一不留神就可能导致高价值信息的泄露”。在 5 月 26 日继续进行的贵阳大数据产业峰会上，亚信安全业务发展及产品研发总经理童宁对于大数据的安全风险以及如何保障大数据安全进行了系统分析，他强调：“要想确保大数据安全，就需要从事前、事中、事后、工具这四个层面进行多层次的安全管控。”

大数据成为企业“金矿”，安全生产不能放一旁

随着全球信息化发展步入大数据时代，数据已经成为企业最宝贵的资产，但是风险正在悄悄潜入。一方面，数据的大量聚集降低了泄密难度，很多关联数据更是“牵一发而动全身”；另一方面，大数据时代数据的重要价值也让很多网络犯罪者趋之若鹜，这对企业的信息安全防护系统构成了极大的挑战。数据显示，2013 年，5.52 亿个人信息被泄露，超过 2012 年四倍。2014 年、2015 年数据泄露量不断翻新，Ashley Madison 10G 用户帐户泄露、网易邮箱数亿用户信息泄露、机锋网 2300 万用户信息泄露等事件不断提醒我们，保护大数据安全已经迫在眉睫。

童宁指出：“大数据系统本身不能识别和保护敏感信息，其固有的安全设计缺陷会导致企业陷入风险之中。以最流行的 Hadoop 为例，其存在着访问控制较弱、无合规性设计、无数据加密、策略管理较弱等缺陷。如果没有配套的安全防护系统，黑客很容易通过网络攻击来获取大数据的访问权限，‘谁访问了数据、以何种方式进入、做了什么’这些都无从审计。这不仅会导致数据泄露，而且还可能导致数据被篡改，酿成错误的决策。”

保护大数据安全，多层管控是关键

数据的产生、存储、挖掘利用是一套完整的流程，任何一个流程出现问题都可能导致数据安全事件的发生，因此，要保护大数据安全，童宁建议企业用户从事前的身份认证与访问控制，事中的网络系统应用安全及数据安全，事后的日志审计，以及 API 服务与安全监控工具这四个层面进行全流程的安全管控。

具体来说，就是针对大数据的环境特点，将人员及 API 的帐号权限集中管理、集中认证、集中鉴权数据安全和集中审计作为切入点，集中管理业务系统和运维操作人员对大数据的访问操作；此外，企业用户还要及时修复漏洞，通过网络安全防护系统防护网络威胁防御，设定相关机制，防止网络受到入侵，避免数据被窃取或篡改。基于上述保护策略，就可获得大数据的安全策略模型。

童宁指出：“目前，亚信安全已经着眼于大数据安全落地，打造大数据安全解决方案。不仅通过亚信安全服务器深度安全防护系统（Deep Security）的防火墙、IDS/IPS、防恶意软件/Web 应用防护/虚拟补丁、数据加密、完整性监控等功能，全方位保障网络系统应用的安全性。还可对大数据进行独立非嵌入式管控，并通过便捷的图形化界面进行更多智能分析和可视化安全管理，帮助用户完成大数据安全战略的变革。”

##

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式，助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。更多关于亚信安全公司及最新产品信息，请访问: http://www.asiainfo-sec.com