CSA-云计算的顶级威胁

深度解析报告

北京六方云科技有限公司

二〇一八年八月

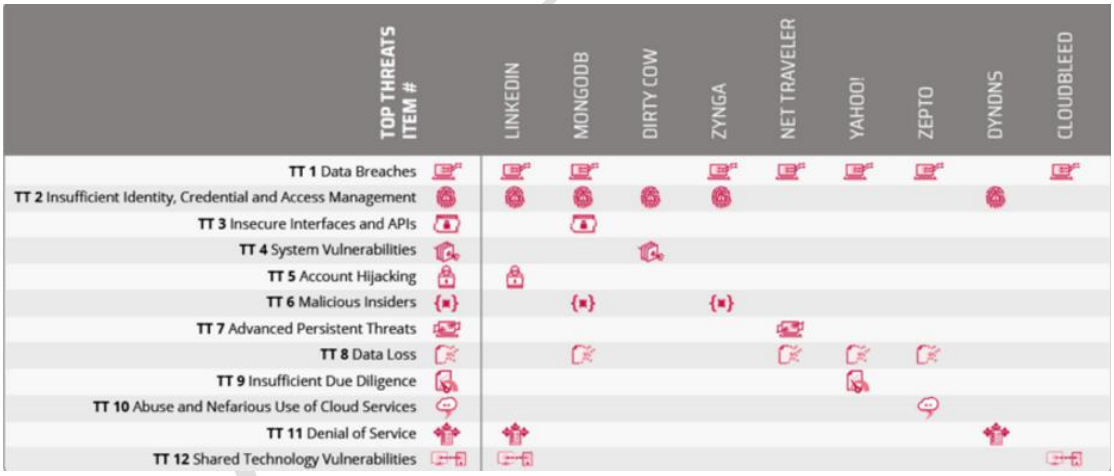
六方云：CSA-云计算的顶级威胁深度解读报告

一、背景概述

近日，在美国拉斯维加斯举办的 2018 黑帽大会的第三天会议上，云安全联盟 CSA 发布了《云计算的顶级威胁:深度解析》报告，该报告是针对 CSA 于 2016 年发布的《十二个顶级威胁：云计算的顶级威胁》 报告的补充(案例分析)，其从安全分析和风险管理的角度，针对每一个云计算威胁和漏洞分别从架构、合规性、风险和缓解措施等方面提供了更全面的技术细节，帮助企业更好地理解安全分析中的顶级威胁来自哪里、如何被应用以及如何在实际场景中缓解与防御此类威胁，六方云作为国内早批云计算安全厂商之一，攻防实验室随即对该报告进行了深度解读与学习。

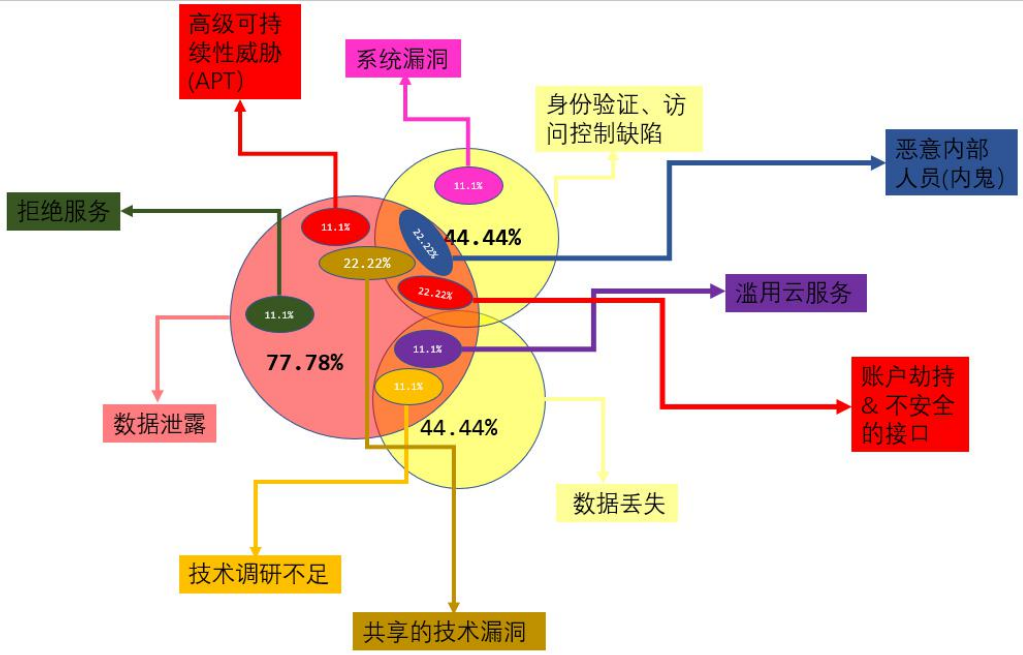
二、报告解读

报告共选取了 9 个典型高级威胁案例来针对 12 个顶级威胁进行分析，进而将企业风险管理的所有安全点衔接起来，如下图：

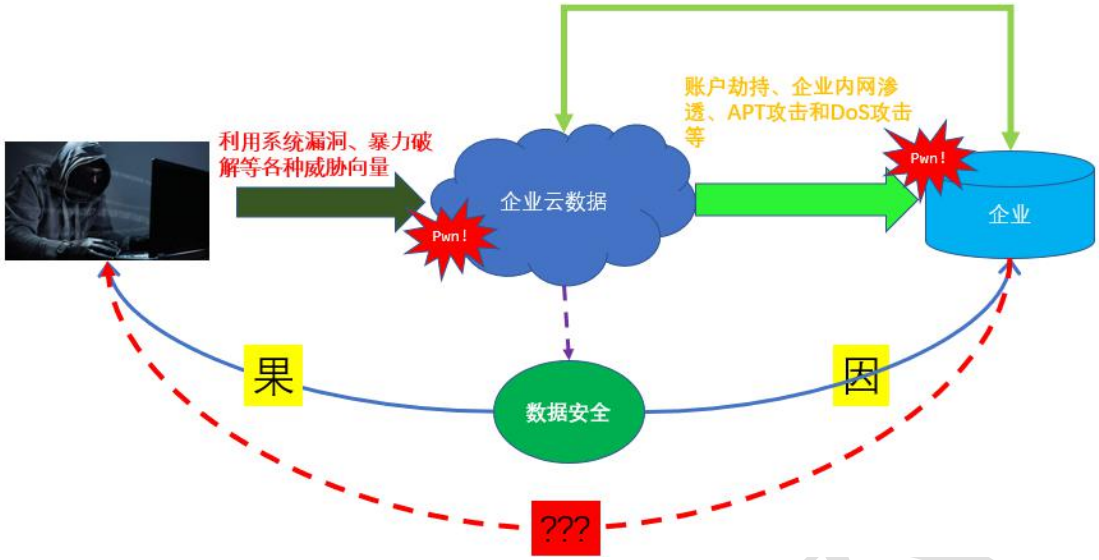


顶级威胁种类 \ 威胁案例	LinkedIn	MongoDB	DirtyCow	Zynga	Net Traveler	Yahoo!	Zepto	DynDNS	Cloudbleed Top Threats
1 数据泄露	✓	✓		✓	✓	✓	✓		✓
2 身份、凭证和访问管理不足	✓	✓	✓	✓					
3 不安全的接口和应用程序编程接口		✓							
4 系统漏洞			✓						
5 账户劫持	✓								
6 恶意内部人员(内鬼)		✓		✓					
7 高级可持续性威胁（APT）					✓				
8 数据丢失		✓			✓	✓	✓		
9 技术调研不足						✓			
10 滥用云服务							✓		
11 拒绝服务(DoS)	✓							✓	
12 共享的技术漏洞	✓								✓

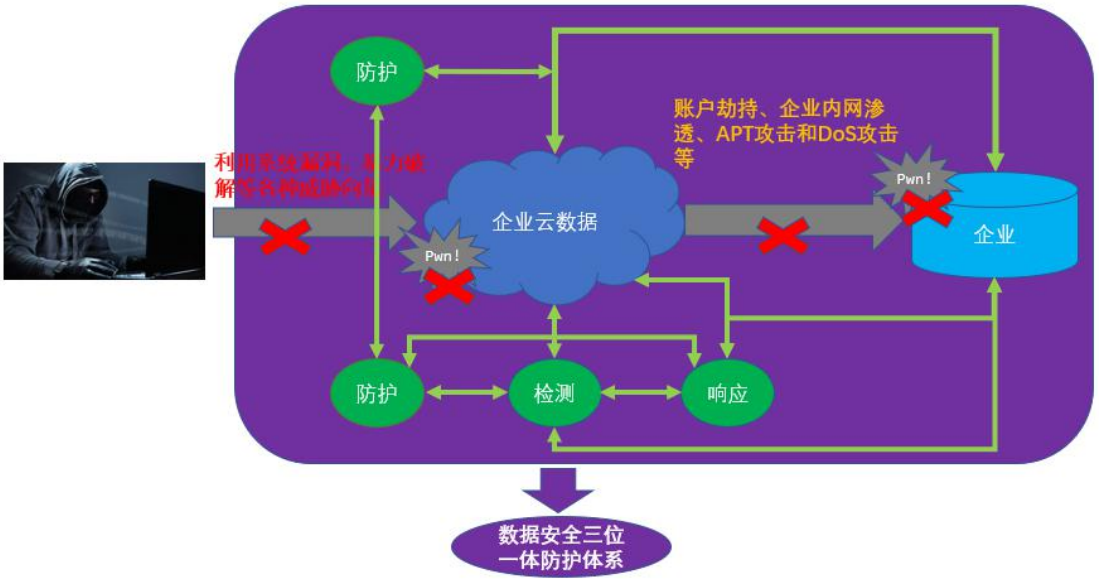
从上图中我们可以看出,12 个顶级威胁中,数据泄露(1)、身份凭证和访问管理不足(2)、数据丢失(8)三者对应的案例数量较多,分别为 7/9,4/9,4/9,且威胁种类 2 和 8 均与威胁种类 1 几乎完全重叠,另外,其中案例 1 LinkedIn 领英用户数据泄露与 案例 2 MongoDB 数据库数据泄露 占用威胁数量较多,均为 5/12,且共同占用威胁种类 1 和 2,为了更直观表示这种关系,我们做了如下饼型交叉图来直观展示:



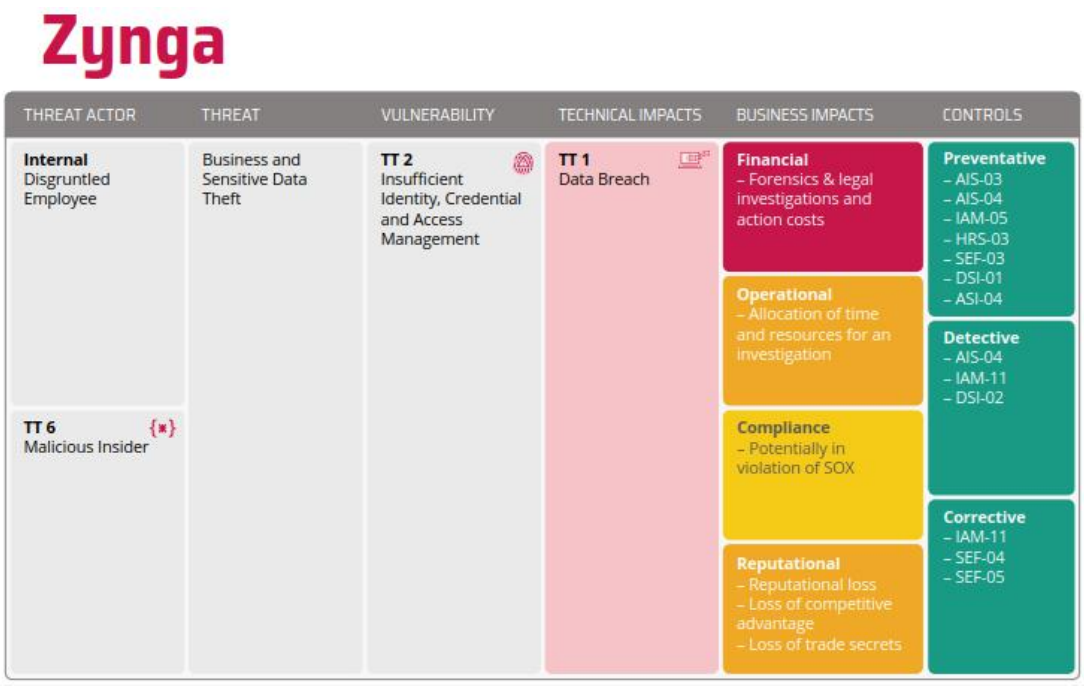
基于以上图表分析,我们可以得知,数据泄露与数据丢失等企业威胁在所列举的案例中占比较大,这其实是当下网络安全现状的一个体现,现如今云计算与大数据高速发展的时代,数据对于企业是至关重要的,没有数据,就没有业务,就没有公司长期稳定的发展,数据成了企业与黑客争夺的至关重要的武器,数据安全既是”因”,又同时是”果”,对于企业来说,因为数据不安全,被黑客盗取才导致后续更为严重的攻击(如账户劫持、APT 攻击等),这表现为”因”(被入侵了);同时,对于攻击者来说,通过系统漏洞、或弱口令攻击各种方式进入企业内部系统拿到数据,这表现为”果”(入侵成功),如下简图所示:



正如上图红色虚线所示，我们认为作为企业安全人员更值得思考的是**数据为何不安全了?攻击者从哪里来？攻击者怎么进来的？**等问题，这些对于企业来说是一种先知防护，安全界常说”未知攻，焉知防”，只有变被动防护为主动，摸清楚整个攻击详情(攻击向量、攻击路径、攻击目的或目标、攻击方式或手法等)才能更好地进行防护，自古以来攻防不对称，攻击者只要找到系统的一个弱”点”便能够攻破，而防护者需要保障系统”面”没有弱点才有可能不被攻破，这便是传统的”以面防点”，这便对企业安全防护系统提出了更高的要求，六方云一直认为企业至少应该具备如下防护-检测-响应等全方位立体防护体系：



在CSA的深度解析报告里，CSA针对每一个顶级威胁，从威胁向量(攻击向量/感染与传播源)、威胁类别、威胁利用的漏洞、威胁带来的技术影响和商业影响以及应对威胁的安全措施(防护-检测-响应)等方面全面直观的展示了企业应对当下云安全威胁所应具备的立体安全体系，其中的应对威胁的安全措施，也是从防护、检测、响应等三个方面来呈现，这与六方云的安全防护理念是相吻合的，接下来我们将以Zynga数据泄露这一具体威胁案例来解读CSA呈现的安全防护体系(注:这里不一一解读所有案例，感兴趣的读者可以联系六方云)：



如上图所示,CSA 在应对威胁的缓解中采用了云安全矩阵 CCM(云计算安全的行业黄金标准,对云计算服务进行全方位的安全评价)中相应的域内安全控制来作为安全措施,基于此六方云对此案例分析图进行了简单阐述,供国内厂商参考,如下图(参考 CSA_CCM_v.3.0.1-09-01-2017_FINAL):

威胁向量	威胁类别	漏洞利用	技术影响面	商业影响面	安全防御措施
内部威胁 心怀不满、充满怒气的员工 顶级威胁6 内鬼/恶意内部人员	商业和敏感数据泄露	顶级威胁2 身份、凭证和访问管理缺陷(不足)	顶级威胁1 数据泄露	财务：获得Zynga内部知识的竞争对手可能获得了相当大的商业和技术竞争优势。对于Zynga来说，这可能会导致长期收入的减少，以及股票价值的下降。 运营：Zynga被迫为调查（技术、法律和操作）分配时间和资源。此外，业务策略和产品路线图将需要新的开发策略。 遵从性：与数据盗窃相关的薄弱控制可能违反了Sarbanes-Oxley法案，并可能导致罚款。 声誉：客户和合作伙伴更加质疑Zynga所承诺的的保密性，从而阻碍了该公司的产品销售和市场开拓的能力。	**防护:** AIS-03 数据完整性控制(数据输出控制,如下载等) AIS-04 数据安全/完整性(即将离职员工) IAM-05 职责划分 HRS-03 员工雇佣协议(法律义务) SEF-03 应急事件报告 DSI-01 数据分类管理(分类存储并设定权限访问) AIS-04 数据安全/完整性(建立和维护策略) **检测:** AIS-04 数据安全/完整性(建立日志审计和检测控制) IAM-11 用户访问撤销(撤销拥有高度特权数据的员工访问权限) DSI-02 数据清单/数据流 (建立数据丢失防护方案) **响应:** IAM-11 用户访问撤销(防止雇佣终止后出问题) SEF-04 事件响应法律准备(雇员保密协议执行等) SEF-05 事件响应指标(保险)

Zynga数据泄露案例分析

在此次 CSA 的报告里,针对选取的 9 个典型威胁案例,CSA 给出了如下所示的云控制矩阵域内控制分布图:

CCM CONTROL DOMAIN	LINKEDIN	MONGODB	DIRTY COW	ZYNGA	NETTRAVELER	YAHOO!	ZEPTO	DYNDNS	CLOUDBLEED
TVM	X	X			X	X	X	X	X
HRS		X	X	X	X	X	X		
SEF	X			X	X	X	X	X	
IAM	X	X	X	X			X		X
GRM	X		X			X		X	
BCR			X		X		X	X	
AAC			X		X			X	
IVS	X							X	X
AIS			X	X					
CCC			X						X
EKM	X								X
DSI				X					
IPY									
MOS									
DCS									
STA									

可以看到9个案例的安全防御措施涵盖了16个域中的12个,其中TVM(**威胁和漏洞管理**)覆盖9个案例中的7个,能够有效的检测这些案例中所利用的漏洞,HRS(**人力资源安全**)和SEF(**安全事件管理、电子发现和云取证**)、IAM(**身份和访问管理**)均覆盖6个案例,由此我们可以得知,预估攻击后果并按计划执行对处理大多数的应急突发事件是非常重要的!

针对CSA发布的12种顶级威胁,六方云也针对性推出全方位立体解决方案来为企业的云安全保驾护航,如下图:

产品与措施 / 安全威胁	★ 六方云盾							★ 六方云密	★ 六方云安全服务	
	身份与访问控制	基础设施与虚拟化安全	威胁和脆弱性管理	安全事件管理与取证	治理与风险管理	审计保障与合规性	应用程序和接口安全	加密与秘钥管理	业务连续性管理与运营恢复	数据中心安全管理
数据泄露	√	√						√		
脆弱身份、凭证和访问管理							√			
不安全的API	√						√			
系统漏洞		√	√				√			
账户劫持	√			√						
恶意的内部人员								√		√
高级持续性攻击		√	√						√	
数据丢失					√				√	
技术调研不足					√	√			√	
滥用云服务				√						
拒绝服务攻击		√							√	
共享技术问题		√	√							

三、总结

随着云计算技术的发展，云安全日益成为人们关注的焦点,近几年不断发生的云安全事件也表明黑客正密切关注云安全这一块肥沃的土地,目前,很多企业已经意识到了云安全的重要性,对云安全产品的需求逐渐增加。云安全未来具有广泛的市场空间,但要实现快速发展,还需要解决国内外云安全标准统一的问题，规范市场秩序。六方云作为国内早批云安全服务提供商之一,积累了多年的经验,能够提供业界独创领先的云计算安全解决方案,帮助企业与用户实现安全上云。

四、参考

1.CSA Top Threats to Cloud Computing: Deep Dive
2.CSA Treacherous 12: Top Threats to Cloud Computing
3.CSA_CCM_v.3.0.1-09-01-2017_FINAL.xlsx