云计算的顶级威胁：深度分析

“危险的12大威胁：云计算的顶级威胁”案例研究分析以及相关的安全行业违规分析

cloud security alliance®

前言

案例研究创世纪项目

2012年，云安全联盟(CSA)进行了一项调查，帮助阐明了云计算最重要和最紧迫的问题。当时，云是一个相对较新的概念，通过提供有价值的行业洞察力，这一内容填补了一个巨大的空白。

CSA从第一次调查中衍生出最初的“顶级威胁”(Top Threats)，并成为本案例研究的基础。然而，安全专家承认，“众所周知的9大威胁”和“十二大威胁”只提供了整体全景威胁的一小部分。其他需要考虑的因素包括参与者、风险、漏洞和影响等内容。

为了解决这些缺失的因素，云安全联盟顶级威胁工作组决定下一份发布的文档应该表述更多涉及架构、合规性、风险和缓解的技术细节。因此，创建了这个文档。

这个案例研究收集了在顶级威胁（(Top Threats)）文件中确定的经典案例和案例研究的局限性，增加了更多的细节和行动信息。理想情况下，这些数据顶级威胁（(Top Threats)）确定了在更高的安全分析层面，提供一个清晰的理解，即如何在应用真实的场景中应用经验教训和概念。

顶级威胁工作组最近的贡献

“2017年顶级威胁”文档中引用了最近的“十二大威胁”调查结果中发现的多个问题的例子。而这些经典案例可以让网络安全经理更好地与高管和同行进行沟通（并提供与技术人员讨论的内容），从安全分析的角度来看，它们并没有提供关于所有东西如何组合在一起的详细信息。

您将发现的内容

本案例试图通过引用顶级威胁（Top Threats）中引用9个经典案例来连接安全分析的所有要求的基础，这九个案例的每一个都以参考图表（1）和详细叙述（2）的形式进行说明。参考图表的格式攻击者风险的概要信息，从威胁和漏洞到结束控制和缓解。我们鼓励架构师和工程师使用这些信息作为他们自己分析和比较的起点。

较长的叙述提供了额外的案例的上下文（例如，事件是如何发生的，或者应该如何处理）。对于那些没有公开讨论影响或缓解等细节的情况，我们推断了应该包括预期的结果和可能性。

我们希望您认为这项工作是有用的，欢迎您对即将出版的出版物提供任何反馈和/或参与。帮助你在未来成功。

序言

云计算正在以前所未有的速度改变组织的业务模式，云服务模型的开发比以往任何时候都能更有效地支持业务，但同时也带来新的安全挑战。在CSA之前所发布的报告中指出，云服务与生俱来的特质决定了其能够使用户绕过整个组织的安全政策，并在影子IT项目中建立自己的账户。因此，组织必须采取新的管制措施。

2018年月，CSA正式发布《Top Threats to Cloud computing: Deep dive》最新版研究报告。该报告全面深度解析了云计算领域的顶级威胁，为了让企业更深刻理解云安全问题，以便他们能够采用策略做出明智的决策。报告试图通过使用顶级威胁中引用的九个案例作为其基础来连接安全性分析的所有点。九个例子中的每一个都以参考图表和详细叙述的形式呈现。参考图表的格式提供了威胁主题的攻击式概要，从威胁和漏洞到最终控制和缓解。我们鼓励工程师将这些信息作为他们自己分析和比较的起点。

云安全联盟大中华区非常感谢翻译和支持工作者们无私贡献。

李雨航 Yale Li

CSA云安全联盟大中华区主席

目录

鸣谢

感谢让这一切发生的团队;没有他们的参与，这么多工作是不会成功的。

联合主席

Jon-Michael C. Brook,

CISSP, CCSK Scott Field

Dave Shackleford

贡献者

Randall

Brooks

Alex

Getzin

Aiyan Ma

Michael

Roza

Shira

Shamban

Velan

Thangavelu

Mark

Yanalitis

CSA调研员

Victor Chin

Shamun

Mahmud

中文翻译版说明

由云安全联盟**大中华区**秘书处组织翻译《云计算的顶级威胁：深度分析》(top Threats to Cloud Computing: Deep Dive),云安全联盟大中华区专家翻译并审校。

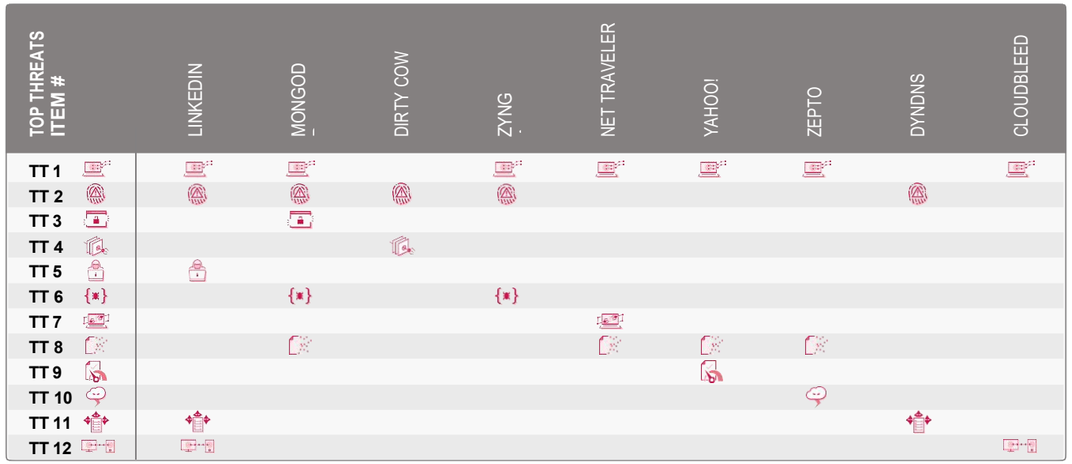
翻译审校工作专家：（按字母顺序排列）

组长：顾伟

组员：陈皓 、郭鹏程、刘广坤、李岩 、马韶华 、欧建军 、姚凯 、周钰

CSA GCR工作人员：史晓婧、胡锦涵

案例研究的顶级威胁报道



案例研究与每一个顶级威胁的对应表

推荐云控制矩阵案例研究的领域

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

分析

缓解和控制适用于9个案例研究覆盖13个16云控制矩阵(CCM)域。数据中心服务(DCS)和互操作性和可移植性(IPY)控制主要涉及云上的数据中心操作。服务提供商的设施，不符合用于云计算的案例研究或“顶部威胁”，移动安全(MOS)控制是用于移动端点保护的，也包括企业中常用的安全措施环境。供应链管理、透明度和问责制(STA)控制也未被提及。

案例研究CCM控制覆盖

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

上表中的行是根据CSA CCM管理域进行各案例研究中的缓解行为相关。

威胁和漏洞管理（TVM），特别是漏洞/补丁管理（TVM-02），将有助于发现这些事件中所利用的许多漏洞。

人力资源安全(HRS)——特别是安全培训——在9个案例研究中有6个被确定为可能的缓解措施，安全事件管理、电子发现和云取证(SEF)也是如此。基于这些结果，我们可以得出这样的结论:对攻击后果的规划和执行对于成功处理三分之二的事件就至关重要的。此外，身份和访问管理(IAM)控制被认为是对半数以上事件的相关缓解措施。

LinkedIn (密码破解2012)

威胁主体	威胁	脆弱性	技术影响	业务影响	控制
内部I 跳过基本标准	**TT 11** 拒绝服务	**TT 2** 数据泄露用户凭证 不充分的身份、凭据和访问管理	**TT 1** 数据用户泄露凭证	**财务** -取证和清理成本一百万美元 -用户诉讼1.25百万美元（不包括律师费用）	**预防** – EKM-02 – IAM-12 – GRM-03 – GRM-06
				运营 —两个电话让用户重置密码	**检测** – IVS-01 – IVS-06 – SEF-04 – GRM-05 – GRM-10 – TVM-02
External 恶意的黑客-东欧	**TT 12** 共享的技术漏洞		**TT 5** 账户劫持,使用被盗密码(密码重用在其他服务)	**合规** —未能保护PII	
				声誉 —对长期的服务使用具有负面影响	**纠正** GRM-07 – GRM-08 – GRM-09 – SEF-01 – SEF-05

攻击细节

威胁主题:俄罗斯公民叶夫根尼·尼库林因涉嫌参与领英(LinkedIn)违规行为被捷克警方逮捕。

威胁:黑客窃取了领英员工的凭证。进入内网后,黑客得到了用户名和密码的数据库。

漏洞:漏洞分为两个主要问题:(1)黑客能够窃取凭证;(2)密码数据库没有“加密”处理

技术影响

数据泄露:可能违反公司知识产权的保密规定;此外，在这次事件之后，还发现了一波暴力袭击。2012年，领英(LinkedIn)披露有600万个密码被盗，但在2016年将这个数字修改为1.67亿。

帐户劫持:由于密码的重用，这种泄漏导致其他服务中的帐户劫持事件。

业务影响

财务方面:取证调查和事后费用估计为100万美元。此外,集体诉讼中有高级账户的受害者获得总计125万美元的赔偿。

运营方面:该公司向用户发出了两次重置密码的通知——第一次是在2012年，第二次是在2016年。2016年,用户的帐户被迫再次重置自己的密码。

合规:LinkedIn未能充分保护用户数据。这是一个违反地方、国家和欧盟(EU)规则/法规(例如GDPR)。违规行为可能导致惩罚，包括罚款。

声誉:LinkedIn因数据丢失被起诉，但没有意识到其对长期服务使用的负面影响。

预防控制

EKM-02: 密钥生成—员工必须妥善保管所有访问管理工具、密钥、密码和密码系统。

IAM-12: 用户ID凭证 – 组织需要采取适当的步骤来验证身份,限制访问和维护对于行业标准和合规的遵从。

GRM-03: 管理监督-不同部门的领导(例如SOC,GRC CIRT)有明确的责任在检测后披露泄露情况。美国在某些行业法规(例如,《萨班斯-奥克斯利法案(SOX)),管理可能是负个人责任和接收罚款或失去以前授予奖金。

GRM-06: 政策-目前尚不清楚LinkedIn的政策是不存在的、有缺陷的，还是简单的没有遵守。对于严重的泄漏,泄漏的信息披露通知不应该被推迟。

检测控制

IVS-01: 审计日志/入侵检测-适当的日志记录需要法律和合规的原因,以及事件相应和取证的需要。这确保了在事件或入侵的情况下具有一个用户行为的清晰文档。

IVS-06: 网络安全—环境和基础设施应该设计成限制访问和监视流量。这个配置应该通过验证和并维护适当的文档

SEF-04: 事件响应法律准备—必须遵循适当的司法调查程序,特别是未来刑事起诉。在事故响应中包括法律代表是很重要的

GRM-05: 管理支持/参与- 事实上一个密码变更只是“推荐”给一些用户，而没有强加给所有的用户,这表明管理层没有意识到问题的严重性或忽略了它

GRM-10: 风险评估-任何独立的内部或外部审计师应该测试组织适当的事件响应政策,流程和程序。在某种程度上，必须清除和纠正政策、审查、支持、监督和/或事件清理之间的分离。

TVM-02: 脆弱性/补丁管理-在渗透测试,密码通常是通过使用各种技术(如彩虹表)测试他们的强壮性

纠正控制

SEF-01: 联系/权威机构的维护-初始事件响应小组中的包括适用的政府当局和执法机构将使披露不足不成为问题。

SEF-05: 事件反应度量-度量对未来会计和预算影响,包括响应时间和资源消耗,将呈现出来给管理层和并为行政领导提供可见性。

GRM-08: 风险评估的政策影响：使用风险评估反馈回路更好地把握初始违约的陷阱，有助于避免第二次违约。

GRM-09: 政策reviews-Business领导应带头政策审议,并确保政策与组织活动和战略方向。首席财务官(CFO)或首席顾问(法律)将指定一个受让人签署底线”——特别是在上市公司,美国证券交易委员会(SEC)和SOX合规发挥作用。

GRM-07: 应该创建和统一执行适当的策略。员工应该知道他们要为自己的行为负责。

关键事项

- 始终对含用户凭据的数据库进行散列和加盐
-- 实施谨慎的日志记录和行为异常分析

MongoDB

攻击明细

威胁角色：威胁角色可以是发现未受保护的MongoDB数据库缺省安装的任何恶意角色

威胁：MongoDB数据库缺省安装在浏览时访问不需要任何授权和访问控制。网络安全专家Chris Vickery发现存储在Amazon Web服务（AWS）上MongoDB数据库中的，9千3百万墨西哥选民的个人识别信息（PII）和投票记录处在危险中。

脆弱性：不安全的MongoDB 27017端口允许外部网络攻击，同时没有其他认证和访问控制措施来防护后端的MongoDB数据库。所有数据可以被任何人操纵（增加，删除，修改和查询）

技术影响

数据泄漏：数据泄露可能导致数据暴露给竞争对手，罪犯，恐怖分子，流氓国家和其他恶意用户

数据丢失：通过破坏和删除导致数据丢失可以使得信息不可接受或不可访问，从而不能为运营，风险和决策所用

业务影响

财务：千万美元的审计费用，事件恢复费用，法律补偿和罚款。

运营：运营影响包括从备份数据恢复文件所需的时间和精力。

合规：指违反美国州和联邦的法规（包括隐私法案），B2B协议及用户隐私义务。根据墨西哥法律，选举人信息是“严格保密”的，未经授权的披露会导致高达12年监禁的惩罚。

声誉：数据泄露严重损害企业商誉。MongoDB广为使用。除了墨西哥选举人信息泄露事件外，其他与MongoDB有关的组织PII数据泄露同样影响了企业底线。

预防控制

IAM-04: 政策和策略-数据所有者复杂提供和实施MongoDB上与识别和访问控制相关的合适的政策和策略。体系需要在数据库创建和用于存储数据前创建。

HRS-09: 培训/意识教育-数据所有者需要对所有合同方，第三方用户和员工提供安全意识培训，确保涉及的每个人收到对于（IAM-04所述）政策和策略合适的，及时的介绍指导。

检测控制

IAM-10: 用户访问检查-数据所有者应该定期检查识别管理和访问权限，检查违规行为并确保用户根据工作职能设定了“最小权限”。

TVM-02: 弱点/补丁管理-数据所有者应该定期进行漏洞扫描或其他检查，确认系统是否足够安全。

更正控制

IAM-02: 凭据生命周期管理/开户管理-数据所有者负责在应用层对数据访问提供认证，授权和可问责性（AAA）规则。这将覆盖整个凭据生命周期。

HRS-09: 培训/意识教育-需要对所有合同方，第三方用户和员工提供安全意识培训，确保每个干系人收到合适的指导。对政策和策略及时的更新教育，特别是在认证和授权方面，同样有益。

IAM-06: 源代码访问限制-通过使用以源代码以外的方式管理的访问密钥或凭据来强化应用对后端数据库的访问控制。整合，变更管理，实施步骤和程序包度可以强化预防性，“最小权限”的访问控制。

IAM-07:第三方访问-使用MongoDB服务中数据的应用程序应被视为第三方访问。云服务提供商（CSP）应负责在提供服务或访问MongoDB服务前检查控制（如访问控制的实施）

IAM-09: 用户访问授权-数据所有者需要提供和测试合适的用户访问授权。用户访问授权测试需要尽早测试案例中的MongoDB缺省配置

IAM-12: 用户ID凭据-数据所有者需要限制公司内部或（租赁）客户的用户账户凭据。

要点

--在所有边界实施政策和预防性控制措施
- 漏洞和系统扫描对受管理的，共享的和公共的环境至关重要

Dirty Cow

威胁主体	威胁	漏洞	技术影响	业务影响	恢复
内部 **外部**	未发现的权限提升 (CVE-2016-5195)	**运营** 内外部威胁角色，未受训的员工，弱治理 **运营** 缺乏或泛泛的 **运营** 对独立的，云容器或虚拟镜像缺乏，不匹配或不完整的度量	**TT 4** 系统脆弱性	**财务** 拒绝服务或者偷窃服务，欺诈，股票下跌 **运营** -运营中断，拒绝服务，偷窃服务 **合规** 罚款，惩处，技术基线，腐蚀 **声誉** -品牌受损	**预防** – AIS-02 – AIS-04 – IAM09 – IAM-12 – IAM-13 – HRS-02 **检测** – CCC-03 – CCC-05 – GRM-10 – GRM-11 **恢复** – BCR-01 – AAC-02

攻击明细

威胁角色：恶意的内外部人员，团体或高级持续性威胁（APT），通过已有用户账户，弱审查或社会工程企图获取根权限。

威胁：没有特权的本地用户使用该漏洞获得对只读内存的写权限，从而提升系统特权。使用该漏洞不会在系统日志留下任何异常行为记录。

脆弱性：通过本地特权提升及其他方法执行非特权代码，开启以root用户身份运行远程UNIX shell。远程访问根目录。

技术影响

系统脆弱性：使用该漏洞导致竞态条件。该漏洞存在于Linux内核2.x到4.x(在4.8.3之前)的mm/gup.c，允许无特权的本地用户通过使用不正确的拷贝写入(COW)句柄特性写入只读内存表，从而导致攻击者在Linux系统上提升权限

业务影响

财务：取决于受影响的系统，对于财务影响可能可大可小。企业可能因为违反隐私调控或数据保护条款，财务犯罪（洗钱，欺诈，账户接管）或非法买卖货物和服务而受到经济处罚。

运营：丢失数据和系统控制减少了对数据完整性、真实度、谱系和来源影响的保证，影响业务质量和运营决策能力。

合规：违规可能属于主权和/或国际范围，如消费者、隐私、安全、财务或数据保护违规

声誉：财务损失，运营中断以及合规罚款和处罚会对品牌价值产生不利影响。 结果，人们对组织管理人员及其有效监督目标和责任的能力产生了怀疑。 这还可能包括消费者信心的丧失和品牌质量的下降。

预防控制

AIS-02: 用户接入要求—访问授权必须使用需要知道、需要访问协议来实现。社会工程识别训练加强现有的访问管理程序，以阻扰账户占用一个初期形式的攻击树到一个Dirty Cow事件。

AIS-04: 数据安全/完整性—多层次的技术基线有助于跨多个系统接口、管辖权和业务功能的数据安全。定期自动基线评估检测数据和系统的披露，改变或破坏，从而减少污牛风险潜力。基线应该包括预期的生产二进制文件、服务和过程的已知配置文件。应引入参考监测或一致性维护运行时检查来定期评估标称系统行为。

IAM-09: 用户访问授权—通过禁用直接交互登录来维护和支持，可能会破坏牛的潜在风险。另外，设置可以配置为通过加密安全的跳转虚拟机（VM）图像或其他加密中间网络使能设备强制图像、容器或应用程序编程接口（API）访问。

IAM-12: 用户ID凭证—系统管理功能应该由基于角色的权限保护，或者是双因素/多因素认证。此外，特权应该在通常的系统级访问和敏感的根或系统帐户的托管凭证访问之间分离。

IAM-13: 实用程序访问—可以删除可能覆盖系统、对象、网络、虚拟机和应用程序控制的实用程序。如果攻击者必须在系统上加载工具（假设网络异常检测已到位），则上传是可被检测的事件。

HRS-02: 背景筛选—所有的系统、承包商和第三方承包商都应该进行与数据分类成比例的背景验证（考虑到业务需求和可接受的风险）。一个Dirty Cow事件可以由内幕人，这是一个已经信任的独特平台。

检查控制

CCC-03: 质量检验—遵循已定义的质量变化控制和测试过程（例如，信息技术基础设施库（ITIL）服务管理），以建立的基线、测试和发布标准为重点，关注系统可用性、机密性和系统和服务的完整性。对生产环境组成和行为的预先了解可以提醒工作人员存在Dirty Cow的异常。

CCC-05: 生产变化—通过记录变更来管理潜在风险：（1）业务关键或客户（租户）-影响应用程序（物理和虚拟）；（2）系统到系统接口（API）的设计和配置；（3）基础设施网络和系统组件。

GRM-10: 风险评估—低Dirty Cow风险通过一个三线支持、全企业范围、风险管理框架进行。正式的、第一线的技术风险评估发生在计划的时间间隔内，并与信息系统的任何变化相结合。第二行风险使用定性和定量方法确定所有识别风险的可能性和影响。与固有风险和剩余风险相关的可能性和影响应独立确定，并考虑所有风险类别。

GRM-11: 风险管理框架 – 将所有Dirty Cow风险潜力降低到可接受的水平；这个过程应该基于符合组织建立的“风险偏好”边界的风险标准。

纠正控制

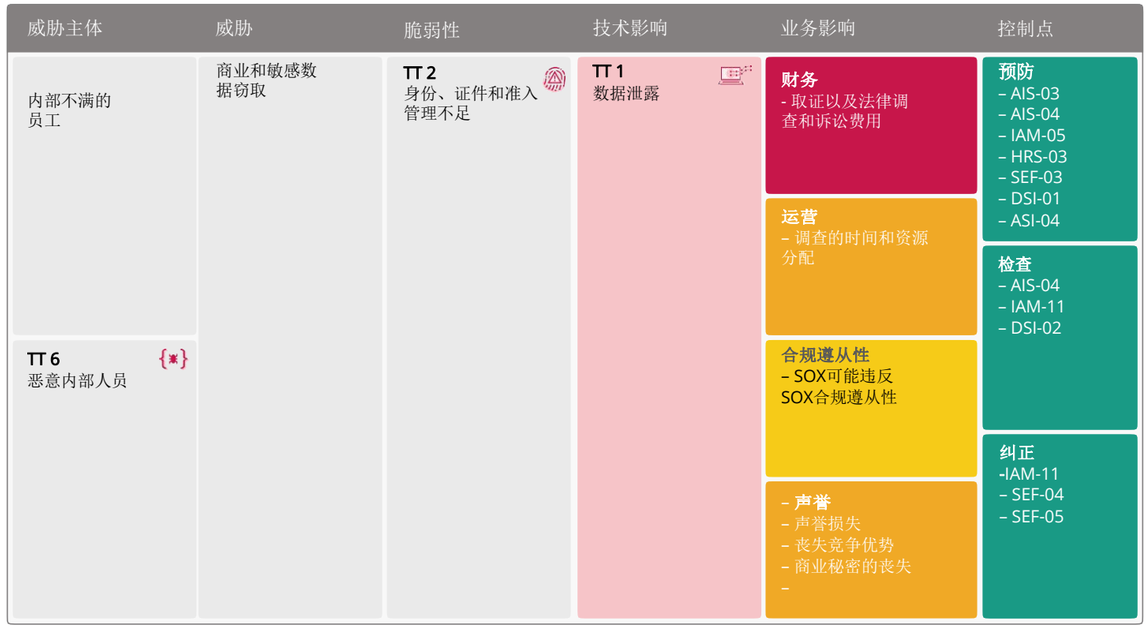
AAC-02:威胁模型的重复性、一线技术风险评估程序，其显示出比可用控制、过程和技术所能减轻的更高的剩余操作风险。

BCR-01: 业务连续性规划—为业务连续性规划和开发建立可测试和一致的统一框架。考虑对Dirty Cow威胁模型的跨功能的桌面练习，演示了比可用控制、过程和技术可以减轻的更高的剩余操作风险。

关键点

- 社会工程培训需要与用户接入策略保持一致
- 从不同角度执行自动化循环活动基线

Zynga



攻击细节

威胁主体：在一个内部，不满的Zynga员工/团队领导（一个有敌意的知情人）的研究和开发。

威胁：恶意内幕人士根据其指定的访问权限和需要知道的原则下载高度机密的商业文件。并在“背叛”竞争对手之前从公司的笔记本电脑（和场所）中删除它们。

脆弱性：没有应用文件级数据丢失预防控制；没有安全控件警告从公司云存储中下载散装文件夹/文件；并且没有实施物理数据丢失预防控制。

技术影响性

数据泄露：业务文件和产品文件的曝光。

业务影响性

财务：获得Zynga内部知识的竞争对手可能获得相当大的商业和技术竞争优势。对于Zynga来说，这可能导致长期收入减少，股票价值下降。

运营：Zynga被迫分配时间和资源进行调查（技术、法律和操作等）。此外，商业战略和产品路线图将需要新的发展战略。

合规遵从性：与数据窃取相关的弱控制可能违反萨班斯-奥克斯利法案，并可能导致罚款。

声誉：客户和合作伙伴更不愿意相信Zynga的机密信息，因为这阻碍了该公司的产品采用和破坏市场的能力。

预防控制

AIS-03：数据完整性—用于防止散装和/或选择性“输出”（在这种情况下为“下载”）的控件将迫使攻击者采取打印屏幕策略，或采用其他无效的技术。

AIS-04：数据安全/完整性—可以为离职员工实施单独的政策和程序。

IAM-05：职责分离—在需要知道的基础上隔离机密数据的访问以及限制复制/下载特权将在限制数据泄露损失方面起到很大作用。

HRS-03：雇佣协议—员工必须了解他们对公司的法律义务，无论是在被雇佣还是离职后。

SEF-03：事件报告—报告事件的能力是至关重要的，既能阻止潜在的犯罪者，又能给告密者提供权力。先前的内幕数据违反案例研究传达了强大的组织事件报告机制的重要性，当涉及到攻击威慑。如果攻击者察觉到这些机制是强的，并且知道敏感数据通常被数据所有者仔细审查和负责任地管理，那么攻击就不太可能发生。

DSI-01：分类—对数据进行分类并适当地限制访问。

AIS-04：数据安全/完整性—对于试图保护自身免受固有风险的组织来说，数据所有者必须准确地了解什么样的数据在其基础设施（或云）中被处理、存储和传输，以及正在使用的应用程序，这是至关重要的第一步。

检查控制

AIS-04：数据安全/完整性—应该建立审计日志和检测控制，以使取证能够主动检测数据泄漏，既减少响应时间，又限制损失。

IAM-11：用户访问撤销—具有高度特权数据的雇员离职应及时撤销其访问权限（根据组织的政策和程序）。

DSI-02：数据清单/流量—数据丢失预防（DLP）解决方案，如集成在云生产力套件中或在过境或端点上执行的，可以基于内容、上下文或高级行为分析/人工智能（AI）场景检测数据泄露，即使这样的动作是允许的政策。

纠正控制

IAM-11：用户访问撤销—在这种情况下，行事者有权访问他们的工作和数据需求。许多内部威胁案件在雇员雇佣关系终止后表现出来，主要是由于访问控制撤销的疏忽所致。

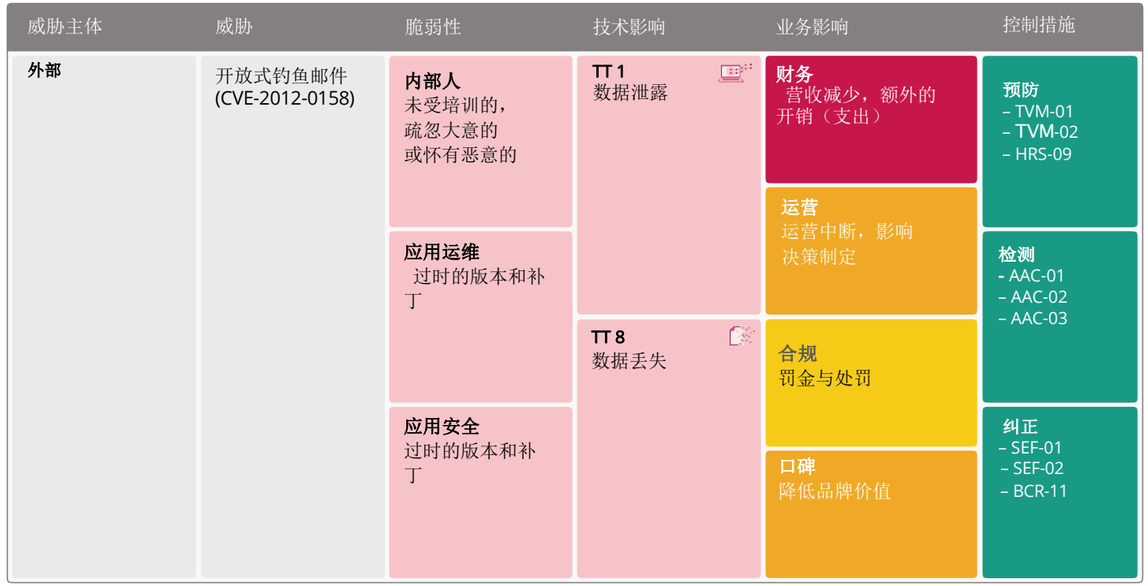
SEF-04：事件响应法律准备—执行雇员的不披露协议、正式的意识行动和相应的法律行动，以应对违反条款，可以产生部分损失恢复，减轻损失和保险覆盖面。

SEF-05：事件响应度量—保险可以防止数据和/或商业/商业秘密的损失，以及在知识产权盗窃案中的部分损失。

关键点

- 数据丢失预防和检测性控制势在必行
- 安全和数据隐私意识是主要的预防控制

Net Traveler



攻击详情

威胁主体：一个外部小组寻求进入目标系统，以获取信息、散布假情报和影响系统操作。

威胁：外部组向员工发送了一封包含以下内容的仿冒“钓鱼”电子邮件：(1) 一个URL链接，指向一个包含RAR可执行文件的WEB站点或 (2) 用 MNKits 生成可执行有效负载的 Word 附件。打开文件将导致Net Traveler利用微软 (MS) Windows 公共控件 (MSCOMCTLOCX)的漏洞，允许远程攻击者执行系统中具有有害特权的任意代码。

漏洞： 没有受过适当培训以识别和处理网络钓鱼攻击的员工是潜在的受害者。此外系统必须经过充分的安全加固（如补丁， 防病毒），以防止成功的攻击。

技术影响

数据泄露： 数据泄漏可以使竞争对手获得公司的生产信息，从而降低了公司的竞争优势。在某些情况下，军事情报可以被提供给恐怖分子（如流氓国家），使一个国家的安全处于危险之中。

数据丢失：通过销毁或删除动作造成数据丢失将使得信息无法无法接受或无法用于操作、分析和决策。

业务影响

财务：数据泄露可能导致竞标销售减少以及 GDPR 罚款和处罚。损坏和丢失数据可能导致低效、无效的分析和糟糕的决策制定-从而导致减少销售和额外成本。

运营： 数据不可用或不能用于处理事务、分析和决策可能会扰乱运营， 延迟或影响决策过程的质量。数据被竞争对手获取会降低竞争优势

合规：不当收集、处理或披露的数据可能导致违反当地、国家和国际规则/条例（例如，GDPR）。

声誉： 财务损失，运营中断和 GDPR 合规罚款和处罚可能影响品牌价值。从而削弱了对组织管理人员的信心--以及他们监督公司安全和其他责任的能力。

预防控制

TVM-01：防病毒/恶意软件
应当实施支持业务流程和技术措施来确保安装更新的防病毒软件。这将防止在连接的接入点设备（如工作站，笔记本，以及移动设备）上执行恶意软件。 这同样适用于IT 基础架构网络和系统组件。

TVM-02：漏洞/补丁管理
应实施支持业务流程和技术措施，来确保漏洞/补丁程序维护是最新的。这将能够及时组织所拥有或管理内的应用程序的漏洞，以及基础结构网络和系统组件， 从而确保安全控制措施的效率和有效性。

HRS-09：培训和意识
必须为所有同组织有关的员工、承包商和第三方用户建立安全和隐私意识培训计划。所有具有组织数据访问权限的个人都必须获得恰当的安全和隐私意识培训，并且获得同他们的专业岗位相关的组织程序、流程和策略方面的定期更新。

检测控制

AAC-01：审计计划
必须制定和维护审计计划，以解决业务过流程中断。审计计划需要重点审查实施和持续执行安全运维工作的效率和效力，包括版本控制、补丁和安全/隐私培训

AAC-02：独立审计
必须进行独立的审查和评估（至少每年一次）以促进最佳实践并确保组织解决了同既定政策、标准、程序和法规遵从义务有关的的不一致性。需要协调独立和内部审计，确保有效覆盖安全运维的诸多方面，包括版本控制，补丁和安全/隐私培训。

AAC-03：法规映射
组织必须创建和维护一个控制框架，该框架能够反映同业务需求相关的标准，法规，法律和要求。该控制框架，包括其对于版本，补丁和安全/隐私培训上的控制（措施）， 需要被（定期）审核（至少每年一次），以确保（那些）影响业务流程的变化能够被正确的反映出来。

恢复控制

SEF-02：事件管理
必须建立策略和过程，以及支持业务流程和技术实施的措施来审核同安全相关的事件，并确保及时和彻底的事件管理（根据IT服务管理策略和过程而建立）。

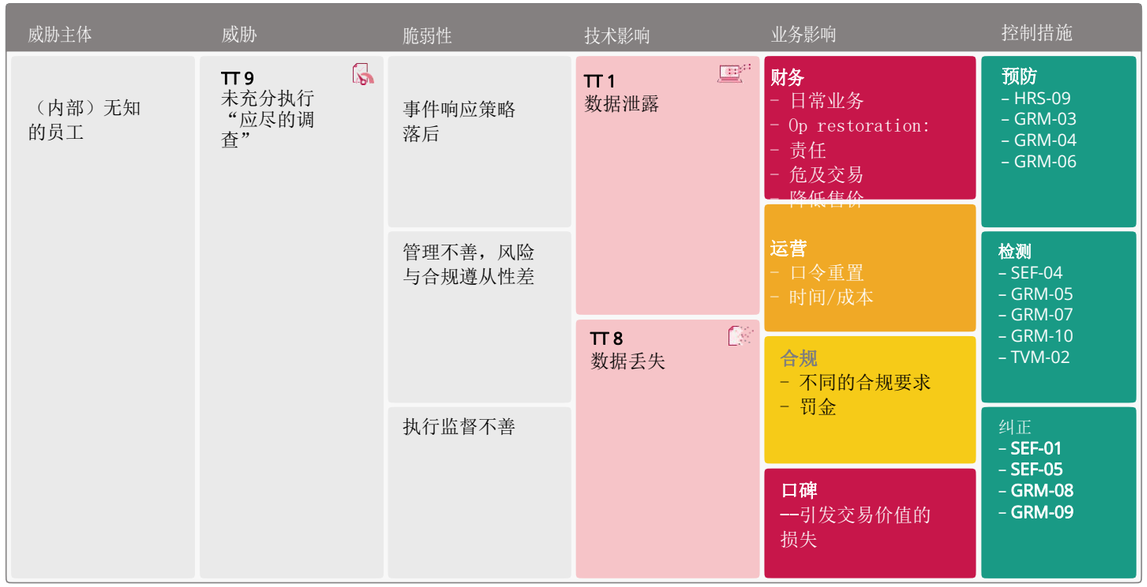
SEF-03:事故报告
工作人员和外部业务伙伴必须了解其责任，并在需要的时候，（口头）同意或以合同的方式同意及时报告所有安全事件。在以遵从适用的法律，法规和规章合规性义务的方式下，及时通过预先定义好的沟通渠道来汇报安全事件。

BCR-11：（数据）保留策略
做为业务连续性计划的一部分，备份和恢复措施必须被纳入且测试通过。基于对威胁影响面的审核（如中断的，损坏了的或删除了的数据或系统）来调用备份和恢复。

关键点

- 内部员工在打开电子邮件时（需要）保持警惕性和疑问
- 及时实施最新的应用和操作系统补丁/版本是至关重要的

Yahoo!



攻击详情

威胁主体： 多雇员意识淡化，忽视或可能未意识到不同的（数据）泄露事件。

威胁： 初始攻击包括利用了不善的密码安全（管理策略），特别是利用MD5哈希码有效期失效。

漏洞： 雅虎员工表现出在多个层面上缺乏适当的尽职调查。这包括：(1) 事件响应政策未包含数据泄露通知;(2) 治理、风险管理与合规 (GRC) 管理程序均未识别和报告对公司今后业务的风险;(3) 高管们忽略了三年以上的情况下所带来的风险。

技术影响

数据泄露： 攻击者在公司知识产权方面可能会违反保密规定。这些信息可能包括源代码、商业机密或其他高度敏感的信息。除了数据泄露之外，（发现也存在）数据损坏的可能，但这在雅虎案中没有证据可以证明。违规的另一个重要方面包括盗窃5亿名用户名和密码。

数据泄露： 攻击者在公司知识产权方面可能会违反保密规定。这些信息可能包括源代码、商业机密或其他高度敏感的信息。除了数据泄露之外，（发现也存在）数据损坏的可能，但这在雅虎案中没有证据可以证明。违规的另一个重要方面包括盗窃5亿名用户名和密码。

业务影响

财务： 根据哪些系统受到损害，与泄露有关的财务费用可能对公司具有重大影响， 从日常业务/销售损失到运营恢复成本不等。最明显的一个受损是发生在2016年的一起悬而未决的对Verizon的收购案。当起收购被最终确定时，由于同泄露有关的原因， 最终的售价减少了大约3.5亿美元。

运营： 这次违约的影响并不仅局限于雅虎自身的感受：因为事关潜在的密码重用的量，整个计算机行业都感受到了运营影响。

合规： 雅虎负责与非 SEC 政府调查有关的现金负债的 50%，以及与违法行为有关的第三方诉讼。此外，股东诉讼和 SEC 调查产生的负债将继续由雅虎负责。

声誉： 由于违约和延迟披露，在公司内部和公开层面上均对公司品牌提出了质疑， 特别是针对有关收购Verizon 的战略价值，以及为解决安全问题而付出的相当大的价格、成本。已经有多起股东诉讼与此有关。

预防控制

HRS-09： 培训/意识 — 雅虎各级员工都将从安全意识培训中受益。这种情况应该对组织内的每个部门产生影响，包括：法律，人力资源（HR），风险和合规以及安全。 所有这些部门都需要了解此事件的影响。

GRM-03： 管理监督 — SOC，IT，GRC和CIRT部门的领导者在检测到入侵后有明确的披露信息的责任。

GRM-04： 管理程序 — 雅虎欠缺或忽略了信息安全管理程序(ISMP)的政策、沟通和风险管理等方面了。文档、审批和实施都为以后的检查和纠正操作创造条件。

GRM-06： 政策 — 尚不清楚雅虎是缺乏安全政策还是根本没有遵循政策。由于此项违规的严重性，披露通知本不应该被延误。

检测控制

SEF-04： 事件响应的法律准备 — 必须遵循适当的法律程序，特别是如果将来会产生刑事诉讼，在事件响应中包含法律代表就显得尤为重要。

GRM-05： 管理层支持/介入 — 任何时候都不揭发组织内部的文化问题，忽视或者掩盖问题，或者没有明确规定问责制和与责任相关的协议，都应该被视为危险信号。

GRM-07： 政策执行 — 信息安全政策执法行动，包括额外的培训或纪律步骤，将确保政策的成功实施。 尽管威瑞森（Verizond）在收购雅虎（yahoo）过程中可能分析了其文档化的安全政策，但尽职调查建议审查执行记录，确保政策真正执行，而不是简单的展示政策文件。

GRM-10： 风险评估 — 任何独立的内部或外部审计师都应该记录如此规模的违规行为。在某种程度上，必须揭露和纠正政策，审查，支持，监督和/或事件清理之间相互脱节的情况。

TVM-02： 漏洞/补丁管理 — 在渗透测试期间，通常使用多种技术测试密码的强度（比如彩虹表）。

纠正控制

SEF-01： 联系/授权维护 —在初始事件响应小组中包括适用的权力机构和执法部门，这会解决缺乏披露的问题。

SEF-05： 事件响应指标 —会计和未来预算影响的衡量指标，包括响应时间和所花费的资源，将在管理层中涌现出来，并为主管领导提供可见性。通过管理来体现会计和未来预算影响的衡量指标，包括响应时间和所花费的资源，并为主管领导提供可见性 （原文是Through management）。

GRM-08： 政策对风险评估的影响 — 使用风险评估反馈闭环来更好地控制初次违规犯下的错误，从而避免重蹈覆辙。

GRM-09： 政策审核 — 业务领导应该在政策审核中起主导作用，并确保政策符合组织活动的战略方向。 首席财务官（CFO）或首席法律顾问（法律）将指定一名受让人“在底线上签字” -尤其是在证券交易委员会和萨奥索斯法案合规生效的上市公司。

关键点

- 长期不披露事件对企业是不利的，除非有警方指示。
- 弱密码和身份验证机制很容易被多因素身份验证（MFA）令牌取代。

Zepto

攻击细节

威胁角色： 无知的员工打开一条包含.wsf或.docm附件的垃圾信息。
威胁： .wsf文件里包含多种编程语言的免杀脚本，（这）使得它能够通过（那些））依赖单一语言的仿真引擎的检测。 恶意文件还使用SaaS云服务（包括Microsoft OneDrive，Google Drive，Box和Dropbox）的共享和协作来感染其他系统。
脆弱性： Windows 修改 .wsf 文件的图标使它看起来像一个有效的电子表格文件。此外，协作软件使.wsf文件在那些缺少培训的员工眼中就像一个本地文件。以上每一项对今后的运营都将是一个风险；并且高管们忽视了此类情况所带来的风险，这种忽视持续了三年以上。

技术影响

数据泄露： 攻击者有可能违反公司知识产权的保密规定。这些信息可能包括源代码、商业机密或其他高度敏感的信息。Zepto的情况可能并非如此，尽管攻击者确实可以访问一些敏感数据，但是Zepto可以用最少的努力来完成对敏感数据（比如PII、社会保险号码（SSN）和信用卡号码（CCN））文件的梳理。

数据丢失： 加密后，所有文件在备份恢复或密钥恢复之前都不可用。

业务影响

财务： 根据哪些系统受到损害，与违约相关的财务费用可能对公司很重大-从日常业务/销售损失到运营恢复成本不等。最近的事件也表明一些组织可能会支付赎金，但这种做法是非常不可取的，为勒索攻击提供资金会使他们变本加厉。（见NororeRangsOM.org）。

运维： 对运维的影响包括文件备份恢复所花费的时间和精力。

合规： 合规性影响可能包括罚款和负债，比如监管机构的披露通知或处罚。

声誉： 如果无法对外提供服务，组织的声誉可能会遭受损失。这种影响对组织的客户和公众来说是显而易见的。违规通知会严重损害组织的声誉，尤其是对于特定行业/地点的组织。

预防控制

HRS-08： 可接受的技术使用——各种云服务的集成应该是一种体系结构活动，而不是由单个用户/组来实现。存储供应商的选择必须由公司IT /安全部门进行。否则可能意味着客户发现的具体风险没有得到解决。

HRS-09： 培训/意识——在网络钓鱼/鱼叉式网络钓鱼攻击中，通过电子邮件最有效地分发勒索软件。针对员工的安全意识培训将降低此类攻击的风险。

TVM-01： 反病毒/恶意软件——安全厂商在恶意软件检测和保护方面取得持续进展。即使是最为训练有素的员工也能从这些工具的实施中获益。

IAM-05： 职责分离——适当的职责分离限制了破坏活动的“爆炸半径（影响范围）”，因为封锁了来自较大人群的关键业务数据集。此外，按功能或组织将关键业务集分组隔离，阻碍恶意软件向整个网络的传播。

检测控制

HRS-05： 移动设备管理——员工网络钓鱼培训在移动设备上效果较差，因为信息被隐藏在一个较小的屏幕上。因此，尽职调查（即，检查链接）就不那么直观。对应用程序部署和集成进行更严格的控制可能有助于弥补移动设备的缺陷。

TVM-03： 移动代码——在移动设备上执行和交互的移动代码保护和控制使得.wsf文件无法与移动设备交互。

SEF-02： 事件管理——事件响应团队应该负责立即清理，并考虑将SaaS存储断开作为修复过程的一部分。

SEF-04： 事件响应的法律准备 — 必须遵循适当的法律程序，特别是如果将来会产生刑事诉讼，在事件响应中包含法律代表就显得尤为重要。

纠正控制

HRS-05： 移动设备管理-员工网络钓鱼培训在移动设备上效果较差，因为信息被隐藏在一个较小的屏幕上。因此，尽职调查(即，检查链接)则不那么直观。对应用程序部署和集成进行更严格的控制可能有助于抵消移动设备的缺陷。

TVM-03： 在移动设备上执行和交互的移动代码保护和控制使得.wsf文件无法与移动设备交互.

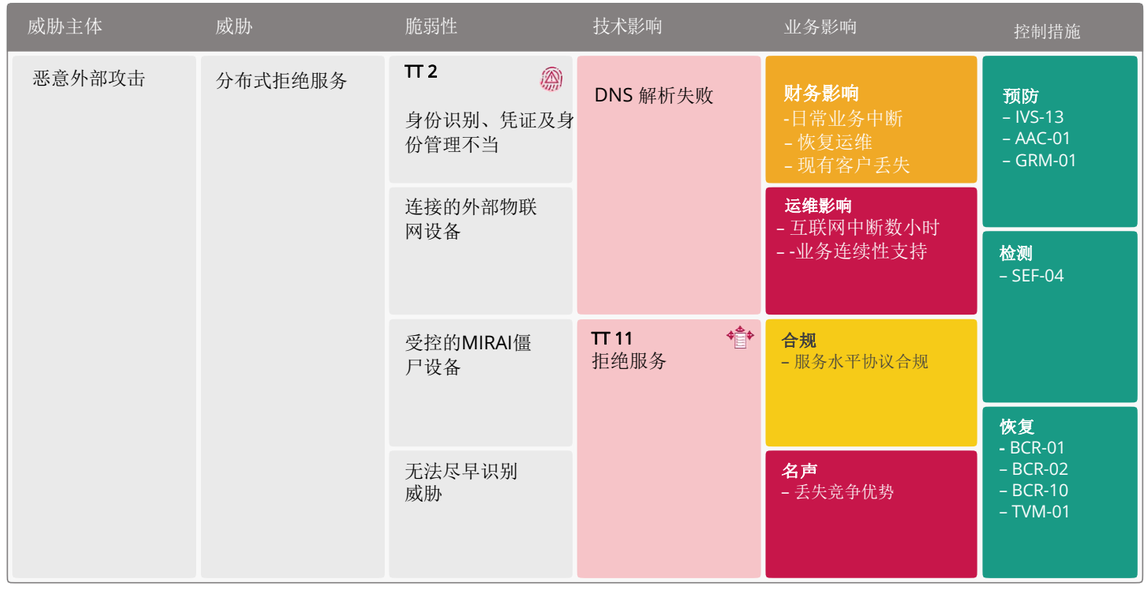
SEF-02： 事件管理——事件响应团队应该负责立即清理，并考虑将SaaS存储断开作为修复过程的一部分

SEF-04： 事件响应的法律准备 —— 必须遵循适当的法律程序，特别是如果将来会产生刑事诉讼，在事件响应中包含法律代表就显得尤为重要。

关键点

- 教育用户使其明白安全的重要性，特别是针对文件附件和链接。
- 对于打补丁和更新端点保护定义保持警惕

DynDNS



攻击细节

威胁主体：通过已联网的物联网设备，恶意外部人员于2016年10月发起了分布式恶意攻击。

威胁： 攻击者通过利用Mirai恶意软件感染了物联网设备，控制了僵尸网络，然后利用该僵尸网络发起了分布式恶意攻击

漏洞： 通过默认账号密码攻破了IoT设备，这些被攻破的设备被控制在一个僵尸网络中，该僵尸网络随后被配置为对一家域名提供商Dyn发起了分布式恶意攻击DDoS.。所有的没有备用DNS提供商的Dyn客户都受到影响，他们网站的DNS解析无法完成。

技术影响

拒绝服务攻击：这次攻击对象是Dyn所管理的一系列域名，目标是影响Dyn所提供的服务。据记录，这次分布式拒绝服务的力度达到了1.2Tb每秒，是有记录以来最严重的攻击。最核心的影响是由于Dyn服务停止，造成DNS失效无法进行正确的IP地址解析。

业务影响

经济损失：这次事件造成两部分损失，1. Dyn客户的损失包含，服务停止而造成的业务损失，以及恢复网站所花的成本，这些都无法计算； 2. Dyn的损失包含， 恢复业务正常运维的成本及大量重要客户丢失的损失，所有损失的明细都没有报告。

业务运维：关键域名都无法访问，包含Twitter 和Snapchat。

法律合规：由于没有数据丢失，Dyn没有直接的法律合规影响。对使用Dyn服务的公司而言，取决于宕机时间的长度，可能会有SLA（服务水平协议）相关的合规问题。

公司声誉：考虑到这次攻击并非是由于Dyn系统本身的设置问题，公司声誉影响很少。这起事件的主要责任方是IoT物联网设备生产方及管理者，以及域名服务协议的设计。

预防控制

IVS-13：网络架构 - 针对DDoS攻击，作为防御措施的一部分，网络架构整体设计应该能快速有效的识别、隔离以及重路由。

AAC-01：审计规划- 应该对内部网络及客户终端进行审计， 同时也推荐对联网的IOT物联网设备进行定期或不定期的审计，这也包含对于客户端的恶意软件识别。

GRM-01：建立基线 -对系统建立合适的基线非常重要。在Dyn事件中，其中最关键的是路由器和DNS服务器，这些设备在DDoS攻击中将会受到严重影响。 对基线的合规检查需要定期监控和审核，这样可以检测出未知变更。这些都有助于尽早识别DDoS攻击。

检测控制

SEF-03： 事件上报 - 事件上报流程应该被归档，相关人员应该接受培训，这样事件发生后可以及时而有效的应对。

恢复控制

BCR -01：业务连续性计划 - 业务连续性计划应该对DDoS攻击或网络占领的攻击建立清晰的响应流程，该计划应该将尽快恢复网络正常运行作为优先级。

BCR-02：业务连续性测试 - 业务连续性计划BCP应该包含针对类似DDoS攻击的应对演练，以有效测试服务恢复的响应时间。可以举行专门的内部DDoS攻击来进行演练，而针对公有云的测试应该事先申请。

BCR-10：政策 - 组织内部应该建立应急响应政策，对应的运维标准和流程应该同时建立（每家公司都应该有贴合实际情况的政策和流程）。

TVM-01：防病毒/反恶意软件 - 尽管Dyn DNS攻击主要是因为消费者的IOT摄像头，公司还是应该建立对应的政策和流程以防公司所管理的终端设备执行恶意软件。

关键点

- 针对物联网安全问题提升安全意识，以及对网络异常情况进行分析
- 对业务连续性进行定期检查、验证和测试，以及对系统运行状态进行监控

Cloudbleed

威胁主体	威胁	脆弱性	技术影响	业务影响	控制措施
恶意外部攻击	TT 1 数据泄露	TT 12 共有技术漏洞	内存泄露	财务影响 - 无	预防 - EKM-03 - IVS-09
				业务运维 - 强制凭证重置 - 凭证丢失	检测 - TVM-02 - CCC-03
	机密信息泄露	缓存溢出漏洞	隔离缺失/失效	合规 - 敏感信息泄露	
				声誉 -客户信任丢失	恢复 - TVM-02 - IAM-12

攻击详情

威胁主体：外部恶意攻击者发送超文本传输协议(HTTP)请求给Cloudflare有漏洞的服务，这漏洞被称为”cloudbleed云滴血”

威胁：成功利用该漏洞需要达到下面条件： 1. 最后的缓存必须以恶意代码或.img标记结束；2. 该缓存必须少于4KB长度，3. 受害者要么启用了邮箱混淆功能(E-mail Obfuscation) 或HTTPS 自动重写/服务端结合执行老版编译器的某项功能，4. 该受害者IP是不受信赖的。

漏洞： 在缓存溢出漏洞中，更多的内存内容返回给请求者，导致内存内存溢出。另外，Cloudflare是共有平台，所以该漏洞在云服务上的影响远不止一个云租户。

技术影响

拒绝服务：API秘钥、密码及其他凭证可能泄露。

信息隔离失败： 导致Cloudflare 将它所有客户残留在内存的信息返回给对应的查询。

业务影响

经济损失：该事件对Cloudflare造成了很少的服务影响，对Cloudflare客户的更大影响并没有披露。

业务运维：运维上影响包含重置密码所花的时间和精力，另外，密码和凭证可能被泄露了。

法律合规：敏感信息，比如PII数据或健康数据，可能由于Cloudbleed云滴血漏洞已经被泄露了。泄露这些信息一般都导致合规问题，幸运的是，并没有相关合规新闻被报道。

公司声誉：作为安全公司，Cloudflare可能有一定程度的声誉影响，因为该漏洞已经导致客户丢失敏感信息。

预防控制

EKM-03：敏感信息保护– 敏感信息被需要被加密保护，一旦发生数据丢失，敏感信息也不会被泄露。

IVS-09：数据分割 – 基于数据机密等级来进行分割保护，将会给数据带来更多保护。

检测控制

TVM-02：漏洞及补丁管理 – 云服务提供商应该告知客户那些数据被泄露，以及他们该如何保护自己。

CCC-03：质量保障测试 – 云服务提供商应该定期对服务进行检测，以及时发现及修复漏洞。

恢复控制

TVM-02：漏洞及补丁管理 – 云服务提供商应该告知客户那些数据被泄露，以及他们该如何保护自己。

IAM-12：用户账号凭证 – 受影响的客户应该马上在受影响的系统上重置密码及其他凭证。

关键点

- 组织供应链上的漏洞还会对组织进行影响
- 云租户隔离取决于实施情况，并且并不能保证百分百隔离

参考文献

LINKEDIN

- https://motherboard.vice.com/en_us/article/53ddqa/linkedin-finally-finished-resetting-all-the-passwords-leaked-in-2012
- https://www.rferl.org/a/us-charges-russian-hacker-nikulin-stealing-date-linkedin-san-francisco-dropbox-formspring-/28068596.html
- https://www.rferl.org/a/russia-hacker-prague-identity-nikulin/28065492.html
- https://www.computerworld.com/article/3077478/security/linkedin-s-disturbing-breach-notice.html
- https://arstechnica.com/tech-policy/2016/10/linkedin-says-hacking-suspect-is-tied-to-breach-that-stole-117m-passwords/

MONGODB

- http://www.informationweek.com/cloud/infrastructure-as-a-service/93-million-mexicanvoter-database-exposed-on-amazon-cloud/d/d-id/1325259
- https://www.csoonline.com/article/3018592/security/database-configuration-issues-expose-191-million-voter-records.html
- https://www.silvertech.com/blog/2017/march/how-to-secure-mongodb-and-get-the-most-out-of-the-sitecore-experience-platform
- https://securityaffairs.co/wordpress/46588/data-breach/mexican-voter-records.html

DIRTY COW

- https://www.scmagazineuk.com/researchers-call-bull-on-dirty-cow-patch-find-flaw/article/711799/
- https://www.theguardian.com/technology/2016/oct/21/dirty-cow-linux-vulnerability-found-after-nine-years
- https://en.wikipedia.org/wiki/Dirty_COW
- https://access.redhat.com/security/vulnerabilities/DirtyCow
- https://www.infoworld.com/article/3134888/linux/how-bad-is-the-dirty-cow-linux-kernel-vulnerability.html
- https://www.cvedetails.com/cve/CVE-2016-5195/

ZYNGA

- https://www.documentcloud.org/documents/3227518-Zynga-Case.html#document/p3/a329534
- https://arstechnica.com/tech-policy/2016/11/zynga-sues-2-former-employees-over-alleged-massive-data-heist/
- https://www.databreaches.net/zynga-sues-2-former-employees-over-alleged-massive-data-heist/

NET TRAVELER

- https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-a4.pdf - Page 18 - Advanced Persistent threats – NetTraveler APT Targets Russian, European Interests
- https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests
- http://researchcenter.paloaltonetworks.com/2016/01/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/
- https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-office-exploit-generators-szappanos.pdf

YAHOO!

- https://en.wikipedia.org/wiki/Yahoo!_data_breaches
- https://www.leahy.senate.gov/imo/media/doc/9-27-16%20Yahoo%20Breach%20Letter.pdf
- http://fortune.com/2016/12/19/yahoo-hack-cyber-security/
- http://www.nbcnews.com/tech/tech-news/your-yahoo-account-was-probably-hacked-company-set-confirm-mass
- http://www.reuters.com/article/us-yahoo-cyber-idUSKBN14420S
- http://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement
- http://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-inhistory.html
- https://www.usatoday.com/story/tech/news/2017/02/21/verizon-shaves-350-million-yahoo-price/98188452/

ZEPTO

- https://www.netskope.com/blog/zepto-variant-locky-ransomware-delivered-via-popular-cloud-storage-apps/
- https://www.tripwire.com/state-of-security/latest-security-news/the-newest-online-threat-zepto-ransomware/
- https://nakedsecurity.sophos.com/2016/07/05/is-zepto-ransomware-the-new-locky/
- http://niiconsulting.com/checkmate/2016/08/zepto-ransomware-analysis-and-how-to-protect-yourself/

DYNDNS

- https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
- https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
- https://securityintelligence.com/lessons-from-the-dyn-ddos-attack/
- https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html

CLOUDBLEED

- https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/
- https://www.troyhunt.com/pragmatic-thoughts-on-cloudbleed/
- https://en.wikipedia.org/wiki/Tavis_Ormandy