

Digicentre 确保业务安全可靠

Digicentre 实现业务运营与信息安全之间的平衡，效果十分显著



从源头上实时阻止恶意软件攻击



实现全面和严格的监控

5

信息安全保护服务的各个方面

您是否认为您已围绕部署在公司内外的 IT 资产实现了完整的信息安全？这是 Digicentre 总经理 Paul Ding 在接受采访时被问到的第一个问题。他表示：“我们需要明白，每个行业都有自己的特殊要求。”他补充道，尽管信息安全的部署对所有大中型企业来说都是一项艰难的任务，这句话同样适用于所有小型公司（无论其运营、管理、人员部署或网络逻辑如何）。但是，Digicentre 部署了适合公司现阶段运营的信息安全解决方案，只有这样，运营和信息安全保护才能达到有效平衡。

从实际应对黑客攻击，到成为完整的信息安全服务提供商

在爆发新冠疫情的两年里，台湾的许多行业都受到了打击或被迫转型。但是，有两个行业却在蓬勃发展：电商和网络游戏。只要向世界各地的手机网络游戏或棋盘游戏的玩家说起“Lineage”或“Lineage M”，他们大多都能认出来。这些游戏之所以流行，Gamania Digital Entertainment 功不可没。这是一家拥有不到 30 年商业经验的公司，收入超过 100 亿新台币。云运营和交易是企业业绩的关键，但该公司是如何持续取得成功的？

Ding 记得 10 多年前，他在 Gamania Digital Entertainment 担任技术总监，那时这家公司正处于游戏行业的最前沿。当时许多公司正在考虑扩展计算机设备或更新软件方面的信息安全，而 Gamania Digital Entertainment 则已经在打击黑客了。这一挑战迫使 Gamania 与国外一些知名的信息安全公司联手，这使该公司比同行业的其他公司更早地获得了对抗黑客攻击的知识和技能。



Digicentre

Digicentre
中国台湾台北市
www.digicentre.com

行业
技术

解决方案
• Prolexic



Ding 强调，Gamania Digital Entertainment 是一家完全采用虚拟运营的游戏公司。云端的游戏稍有差错，就会对运营和收入产生直接且严重的影响。因此，该公司全力以赴支持和投资其信息安全部门。2009 年，Gamania Digital Entertainment 成立了 Digicentre 研发子公司。四年后，Digicentre 也开始正式向外部公司提供信息安全服务。这是其运营方面的一大飞跃，使其从过去的第三方角色，转变为值得信赖的合作伙伴和第三方信息安全服务提供商。

在疲于应对云攻击之际，直接进行云部署

2013 年，Ding 从 Gamania Digital Entertainment 的技术总监一职直接晋升为 Digicentre 的副首席运营官。2016 年，他被晋升为 Digicentre 的总经理，一直担任至今。他表示，Digicentre 在全力以赴提供第三方服务，同时继续专注于它的主要任务（维护 Gamania Digital Entertainment 的信息安全）。Digicentre 在进行日常维护的同时，也在加紧应对不断变化的信息技术环境。

现实情况是，云网络会受到攻击。这些攻击的方法越来越新颖，比如，利用物联网设备作为跳板，或者增加数倍的攻击流量。Ding 强调，Gamania Digital Entertainment 不能继续采用过去使用的那套方法（比如横向扩展设备以承载负载流量），因为这最终会面临设备的使用和空间限制。因此，Gamania Digital Entertainment 不再采用从设备上阻止恶意攻击的方法，而是转变为了云 CDN 防御模式，从而在云上实现更广泛、更深入的信息安全部署。

Digicentre 为 Gamania Digital Entertainment 部署了一个从设备到云的云安全框架，还与全球内容交付网络 (CDN) 安全供应商 Akamai 展开合作。依靠 Akamai 云防御核心的完整性和专业性，Digicentre 获得了来自世界各地的丰富实时更新的数据库，以从源头上实时阻止恶意软件攻击。同时，还可以进行全面、严格的监控。Akamai 是一家专业的云安全供应商，可提供各种强大的解决方案（从深入的垂直保护，到水平信息安全解决方案）。Akamai 多年来一直广受好评，该公司也是信息安全和保护领域的优秀合作伙伴。

NIST 检测有利于加强信息安全部署

云提供了无限的空间，它是在线游戏和电商运营商的生命线。从收入、客户忠诚度、企业形象、客户体验等方面来看，它对在线游戏和电商企业极为重要。根据 Ding 的分析，过去 Digicentre 为企业客户提供服务时，往往通过分享过去的经验来进行操作，因为 Gamania Digital Entertainment 通常会比其他企业更早受到攻击。这也使 Digicentre 团队能够设身处地为客户着想，与客户的需求和紧迫感产生共鸣，并考虑客户目前的能力和资源是否能够胜任。然后，该团队可以进一步协助部署信息安全防御措施或提供有效的解决方案。



企业在部署信息安全防御系统时的基本方法应该是“假设黑客最终会入侵网络结构”。

Paul Ding
Digicentre 总经理

Ding 进一步补充道，当企业和个人社交互动都基于云时，企业必须围绕内部和外部的云环境维持警觉的防御措施。企业在部署信息安全防御系统时的基本方法应该是“假设黑客最终会入侵网络结构”。因此，他认为企业应该采取“监控 + 多级保护”的方式，以构建整个信息安全保护区域。

以 Digicentre 为 Gamania Digital Entertainment 提供的信息安全保护服务为例。第一步是按照 NIST 网络安全框架的五个功能，依次加强检测。游戏行业面临的挑战之一是应对正在进行的攻击带来的各种压力。例如，我需要多长时间才能知道自己被攻击？如何知道黑客入侵了我的网络层的哪个区域？如何在尽可能短的时间内启动响应机制，以尽可能降低损失和损害？Ding 表示，通过部署检测功能，企业不仅可以尽早发现攻击，还可以立即加固防御，在攻击发生前准备好主动应对措施。

信息安全与运营

Ding 拥有丰富的行业经验（包括多年领导 IT 团队的经验），因此，他特别善于将业务运营纳入信息安全规划中。他深刻认识到，运营必须是可持续的，同时也必须考虑到帐户信息安全。这两者是相辅相成的。今年，Digicentre 进入了开展业务的第 10 年。Digicentre 现在发挥着国际供应商的作用，它不断通过技术、服务和专业合作伙伴来扩大服务范围，包括与 Akamai 合作以保护在线运营。

Ding 表示，Gamania 的董事长曾经说过：“没有信息安全，就没有业务。”这句话与台湾金融监督管理委员会主席 Huang Tien-Mu 的说法一致，后者以金融业的在线平台为例，说明了为客户提供服务的重要渠道。Tien-Mu 提醒金融业生态网络链上的所有参与者：“没有信息安全，就不存在所谓的运营。我们呼吁大家密切关注信息安全的重要性，这与企业的其他方面一样重要。”

此案例是对 IT Home 文章的转载和翻译，该文章可在此处访问：<https://www.ithome.com.tw/pr/150956>



Digicentre 最初是一家大型游戏公司的 IT 部门。该团队将其 IDC、安全和集成服务剥离出来，以便为其他公司提供独特的服务和经验。Digicentre 的三个主要数据中心都建立在与主要电信提供商的直接对等网络上。它的业务和服务在持续增长，旗下的全天候服务处理超过 45 万个并发用户和超过 2.4 亿个月度会员的业务。Digicentre 由上市股东 Gamania 和 MDS 控股。www.digicentre.com。



扫码关注，获取最新 CDN 前沿资讯