信任因素

网络安全在保持业务良势发展中的作用

执行概要

2018年，网络攻击的风险比以往任何时候都要高。引人注目的数据安全事件依旧是新闻热点，其中包括史上最大的分布式拒绝服务攻击，攻击强度为1.7Tbps[1]。在欧盟，《通用数据保护条例》（GDPR）已于2018年5月25日生效，对个人身份信息(PII)的采集、处理和控制实行严格的新规定。此外，密码破译人员渗透入网络寻找快速得手的契机。

我们进入了一个“后信任”时代，企业和个人在接受表面上的安全承诺时越来越谨慎。每次消费者与品牌互动时，他们都会判断是否足够信任一家公司到愿意分享他们的PII。成功的网络攻击会破坏企业努力在品牌和消费者之间建立的信任。被波及的不再只是安全专家们，最高层高管也要对此负责。

Radware发布了一份年度全球应用及网络安全报告，探讨企业在努力保护其品牌时面临的复杂挑战。这已是第八份年度报告，其中汇集了Radware系统研究、真实攻击数据、对发展趋势和技术的分析以及全球行业调查结果。

报告强调了网络安全对企业和技术的影响，包括：

- 从最近的攻击中汲取的教训
- 网络攻击的真实成本，包括了定量及定性分析
- 网络和应用威胁现状概述
- 对新兴技术漏洞的深入见解
- 2019年预测

重要发现

平衡成本与风险计算

防范网络攻击需要大量的投资，而这些投资会体现在资产负债表的运营支出上。从本质上而言，企业总会想方设法节省资金。但当企业面临网络攻击入侵防御系统及业务影响的风险时，多少资金才算足够呢？

请参考Radware 2018年全球行业调查中得出的颇具启示作用的结论：

- 仅短短一年中，网络攻击的初始成本就增加了52%，达到了110万美元
- 对网络攻击总体成本进行建模的企业表示，他们的预估成本几乎是不进行成本建模的企业的两倍。
- 五分之二的企业表示，一次成功攻击会带来不良的客户体验并使声誉受损
- 93%的受访者在过去一年都遭受过网络攻击；只有7%的受访者表示未遭受过攻击
- 三分之一的企业每周都会遭受到网络攻击
- 将近一半的受访者表示，网络攻击的主要影响是服务中断。导致完全或部分服务中断的攻击增加了15%，严重损害了生产力
- 网络勒索仍是黑客的首要目的，也是51%的攻击的发起原因

[1]https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcache-ddos-as-a-service/

新兴攻击矢量

攻击者采用了有效的技术来引发拒绝服务，如：脉冲、放大、加密物联网(IoT)僵尸网络，并对应用层带来了更大损害。

- 应用层攻击带来的损害最大。三分之二的受访者表示遭受过应用攻击。三分之一的人预计2019年应用漏洞仍是一个大问题，尤其是在云环境中。一半以上的企业每月都会进行更改和应用更新，其他企业则会更频繁地进行更新，从而推动了对自动化安全的需求。
- 导致网桥宕机或服务中断的网络攻击增加了15%，六分之一的企业表示遭受过1Tbps的攻击。
- 黑客实施新战术试图击垮网络和数据中心：HTTPS洪水增加了20%，DNS和脉冲式攻击都增加了15%，计算机程序攻击增加了10%。
- 三分之一的企业称遭受过攻击，但无法确定攻击动机。

为接下来可能发生的攻击做好准备

企业表示，他们了解威胁现状改变的严重性，也采取了相应措施保护数字资产的安全，但安全威胁的严重性不容忽视。

- 尽管部署了安全解决方案，但仍有近一半的企业表示尚未做好防御所有类型的网络攻击的准备。
- 在过去一年里，86%的企业探索了机器学习和人工智能(AI)解决方案。将近一半的受访者表示，他们的目的是找到更快的网络攻击响应时间。Radware发现，利用区块链开展业务的企业增加了44%。
- 企业仍然通过多个云提供商实现网络运营的多样化。五分之二的企业采用的是集成了本地和云端防护措施的混合网络安全解决方案。
- 49%的EMEA企业表示，他们还没有针对GDPR做好充分准备。

唯一的选择就是成功

如果无法成功缓解每次威胁，那么网络攻击的代价就太大了。客户的信任可以被瞬间摧毁，对品牌声誉和重建业务成本的影响巨大。GDPR和其他政府法规都能够使违规企业破产。

对企业而言，将网络安全纳入长期发展计划至关重要。保护数字资产不能只交给IT部门。相反，安全规划需要注入到新产品和服务、安全、开发计划和新的业务措施中。CEO和管理团队需要带头设定基调，并在确保客户体验上进行投资。

最高管理层视角

CEO们成为了新的可信管理人员

对于最高管理层的管理者而言，网络安全正在成为一个非常私人的话题。为了建立并保持与客户的稳固关系，CEO们必须承担起“首席信任官”的角色。策划多年的品牌战略可以被一次网络攻击完全瓦解，只把安全战略分配给首席信息安全官(CISO)负责已经远远不够了。风险巨大。

回顾一下Equifax、Yahoo、Moller-Maersk和Anthem Healthcare这些发生过严重数据泄露的企业CEO们的命运吧。这些企业为打造品牌价值所做的所有努力，在因为攻击丧失了客户信任的那一刻，就都付诸东流了。其后不久，多数企业的CEO就开始“从事其他职业了”。

为了确保网络安全是企业业务模型不可或缺的一部分，CEO们需要核实相关工作，并为防护措施提供资金支持。将安全策略委托出去而不进行监督的CEO们必须自己承担风险。

下载免费报告

2018-2019年全球应用及网络安全报告