知己知彼，有效抵御网络攻击

由 IBM 服务部撰写

2018 年 10 月 2 日

什么是网络攻击?

网络攻击是利用恶意软件对计算机系统和网络进行蓄意攻击，旨在损坏数据或中断运行的行为。网络攻击的目的是实施信息窃取、欺诈和勒索等网络犯罪行为。

网络攻击的常见类型

恶意软件攻击。这是网络攻击的主要手段，包括病毒、蠕虫、木马、勒索软件、广告软件、间谍软件、机器人程序、程序错误和 rootkit。恶意软件在用户点击某个链接或执行某个操作后就会安装。一旦植入，恶意软件就可以阻止访问数据和程序，盗取信息并致使系统无法运行。

勒索软件是用于敲诈受害人的恶意软件 — 威胁要将敏感信息公开，或锁定系统以使用户无法进入，除非支付赎金，通常使用比特币等加密货币支付。IBM 估计 2017 年全球范围因勒索软件攻击给企业造成的损失超过 80 亿美元。（1）

网络钓鱼通常使用看似来自可信来源的电子邮件。毫不知情的用户打开电子邮件，执行进一步的操作，比如提供受保护的信息或下载恶意软件。

中间人攻击发生在通信双方之间（比如用户和公共 Wi-Fi 集线器之间），旨在访问和盗取数据。

拒绝服务（DoS）攻击会让系统流量过载，以便耗尽资源和带宽，致使系统无法运行。

SQL 注入攻击：SQL 是结构化查询语言的简称。这些攻击将恶意软件安装在服务器上，通过查询服务器来窃取受保护的信息。

零日攻击通过软件或系统的制造商或用户未知的漏洞，引入恶意软件。它之所以被称为“零日”，是因为开发人员根本没有时间来解决或修补漏洞。（2）

实施网络攻击就是为了通过欺诈或勒索等犯罪行为来获取经济收益，就像勒索软件那样。也有一些网络攻击的动机是蓄意破坏或报复。比如心怀不满的员工。网络攻击也有政治方面的因素，主要用于网络战中。

网络攻击并不总是源自于企业外部。“据白帽暗网专业人士在 2018 年黑帽大会上指出，许多黑客是经过认证的专业人员，他们作为受信任的 ‘定时炸弹’，已经渗透到大部分企业中”，ITBizAdvisor 的报告这样说。（3）

资源

企业能否在数字化转型中生存下来?

IDC 阐明数字化转型如何造成更大的网络安全漏洞，以及网络灾备服务如何提供帮助。

观看视频 (02:16)

网络攻击为何后果如此严重?

企业遭受数据泄露等网络攻击的代价和后果是毁灭性的。根据 Ponemon Institute 开展的 2018 年数据泄露成本调研，数据泄露的平均总成本是 386 万美元。[4]

它的影响不止是钱的问题。网络攻击还会……

- 损害品牌和声誉
- 削弱甚至摧毁用户忠诚度
- 造成知识产权损失
- 导致企业无法运营
- 受到监管惩罚
- 损害政府和国家的安全
- 增加未来攻击的可能性

预防网络攻击会让企业节省大量金钱和麻烦，但这可能并不是实用的方法。

IBM 认为攻击只是“时间”问题，而不是“是否会发生”的问题。[5]思科前任首席执行官 John Chambers 表示：“企业只有两种类型：已经被攻击的，和尚未知道自己已经被攻击的。”[2]

网络攻击的数量证实了这一观点。2017 年网络安全事件数量翻了一倍[6]，公开披露的事件中所泄露的记录超过 29 亿条。[1]

Ponemon Institute 开展的 2018 年数据泄露成本调研 *了解数据泄露的影响和后果。*

Ponemon Institute 对全球超过 477 家企业进行了调研，报告详细指出了数据泄露的成本和影响，并按行业和国家/地区进行了细分。

阅读调研报告

有效的网络攻击应对措施的主要特征

鉴于网络攻击非常普遍，如果不可避免，那么企业就需要像预防一样解决应对问题。IT 分析机构 IDC 指出："如果企业采用新技术，那么他们的防护战略也必须与时俱进。这些战略不仅必须包含更强有力、更多样化的安全机制，而且还必须规定在发生信息泄露或安全事件时的快速恢复方法。"（7）

企业纷纷采用**网络灾备**方法来实现预防性安全和快速恢复。

网络灾备包括数据保护、灾难恢复、业务连续性及灾备实践。它将这些方法与先进技术相结合，评估风险，保护应用和数据，以及在网络攻击期间或之后快速恢复。IBM 与 IDC 的观点一致，已经确定一个包含五个阶段的网络灾备生命周期：

发现风险和漏洞 — 通过动态分析（DAST)、静态分析（SAST）和开源测试，帮助精确找出业务关键型应用和相关风险。然后对照业务连续性和灾备准备情况，评估中断可能产生的业务影响。

保护应用和数据 — 目的是有效保护应用和数据，防患于未然。气隙 — 通过物理方式将数据隔离为故障安全区域，这是保护备份数据不受感染的有效方法，尤其适用于抵抗可快速遍历和感染联网系统的恶意软件。

检测数据损坏和配置异常 — 企业希望获得自动化的测试能力，无需中断业务系统，就能检测数据和系统配置文件中的变化。

应对配置和数据中的变化 — 必须快速处理配置和数据中未经授权的变更。仪表板技术可以实时揭示未解决的漏洞，如果不能预防，就支持快速采取应对措施。

恢复对关键应用和数据的访问 — 如果持续遭到攻击，就必须（通过气隙备份）快速恢复任务关键型应用和数据。 指挥与自动化管理技术利用预先确定的工作流程，只需点击操作，即可自动恢复整个业务流程、应用、数据库或离散系统。

资源

IDC：实现网络灾备框架的五项关键技术

网络灾备战略需要考虑数字化转型如何瓦解传统保护措施。了解通过可控可衡量的方式缓解风险和支持恢复的方法和技术。

阅读白皮书

成功案例

观看视频，了解数据保护服务

了解这些服务如何保护企业最为宝贵的资产。

观看视频 (01:22)

观看视频，了解灾备服务

系统出现宕机。仅需数分钟甚至数秒钟即可恢复运行。

观看视频 (3:10)

观看视频，了解业务连续性及灾备服务

无论是遇到人为错误还是病毒，仍可以持续运营。

观看视频 (2:24)

博客

ITBizAdvisor

了解 IT 业务连续性及灾备服务顶尖专家和领导的最新分析和洞察。

访问网站

产品

网络灾备服务

业务连续性及灾备服务

数据备份与保护服务

参考资料

1.*IBM X-Force 2018 年威胁情报索引*，IBM Security，2018 年 3 月 (PDF, 2.85MB)

2.*最常见的网络攻击有哪些？* Cisco, Systems, Inc.

3.业务连续性训练营 — 第 1 部分： 不断变化的网络威胁形势，Anyck Turgeon，ITBizAdvisor，2018 年 9 月 26 日。

4.*2018 年数据泄露成本调研： 全球概述*，Ponemon Institute，2018 年 7 月

5.IBM 业务连续指挥与自动化管理以及网络事件恢复，IBM Corporation，2018 年 8 月

6.*2017 年网络安全事件数量翻了一倍，调研结果*，SecurityIntelligence，2018 年 1 月 30 日

7.*实现网络灾备框架的五项关键技术*，Phil Goodwin、Sean Pike，IDC，2018 年 6 月