TeamViewer
Remote Management

白皮书

不再错过一个补丁：

自动化补丁管理

减少安全风险

保持 IT 基础设施安全

目录

引言:
补丁管理解决方案是什么?

想要保持您 IT 基础设施的稳定与安全，就需要对所有的计算机和设备进行定期维护和及时更新。忽略计算机和设备更新可能会导致由软件过时带来的安全漏洞。

由于企业设备、应用程序和网络漏洞的不断增加，IT 组织在确保设备始终最新或“打补丁”问题上面临着新的挑战。

在 IT 领域，“补丁”是一系列为计算机程序升级、优化或修复而专门设计的更改。补丁适用于修复软件漏洞及其他错误，通过软件更新的方式来供用户使用。监管补丁的可用性以及安装缺失的补丁就需要一个自动化的补丁管理解决方案。

使用补丁管理解决方案，您可以检测过时、易受攻击的软件，并为其打补丁。

因此，补丁是 IT 安全的一项重要组成部分。没有它，安全问题将永远无法解决，企业数据也将任由黑客或网络罪犯盗取。美国国家标准技术研究所（NIST）的一项研究表明，90% 的成功对企业的网络攻击，是由已知漏洞造成，而这本可以通过正确及时地打补丁来预防。[1]

补丁管理对企业的**重要性**

恶意软件攻击会对企业造成重大损害。数据丢失、图像损坏或生产停机可以造成企业数百万的损失。恶意软件的变体数量几乎每日都在增加，这就意味着您的 IT 基础设施需要行之有效的安全管理。

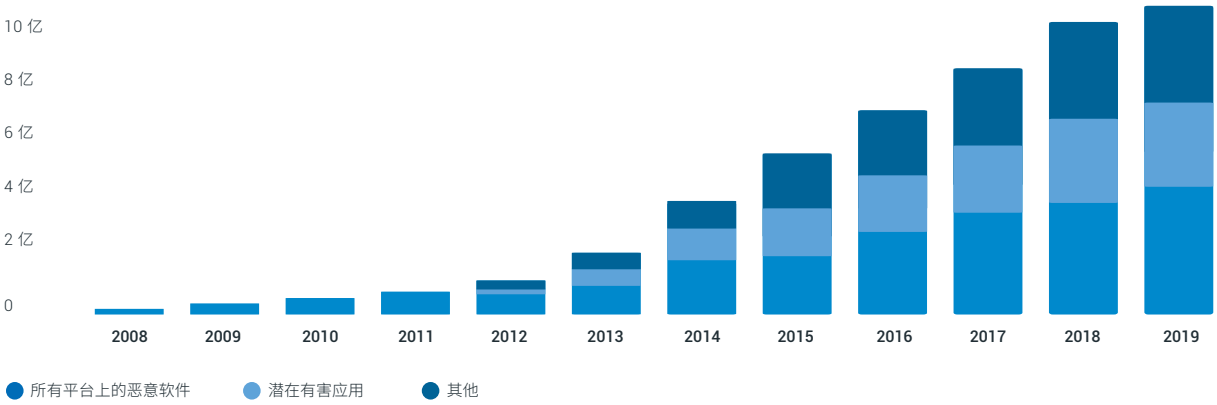

图 1：已知恶意软件的变体总数 *潜在有害应用[2]

网络攻击，比如 2017 年的 "WannaCry" 勒索软件攻击，再一次展示了保护硬件软件不受网络攻击所侵害的重要性。现在，大型企业的多数系统和应用都可以通过互联网来访问，这使得网络罪犯有了可乘之机。仅仅依靠杀毒软件来保护企业 IT 基础设施是不够的。由于软件的复杂程度越来越高，在软件开发过程中会出现比过去更多的错误，从而给软件留下漏洞。

德国联邦信息安全办公室（BSI）表示："网络攻击之所以得逞，通常是通过未知的漏洞或因为缺少补丁管理。"[3] 这是因为近年来标准 IT 产品中关键漏洞数量急剧增加。

仅在 2017 年，10 大最知名的应用里共有 450 多个已知漏洞。据 BSI，没有任何迹象表明这种情况将在未来几年内有所改变。在 2019 年，50 大最常用的软件产品已有 12174 个漏洞被证实。[4]

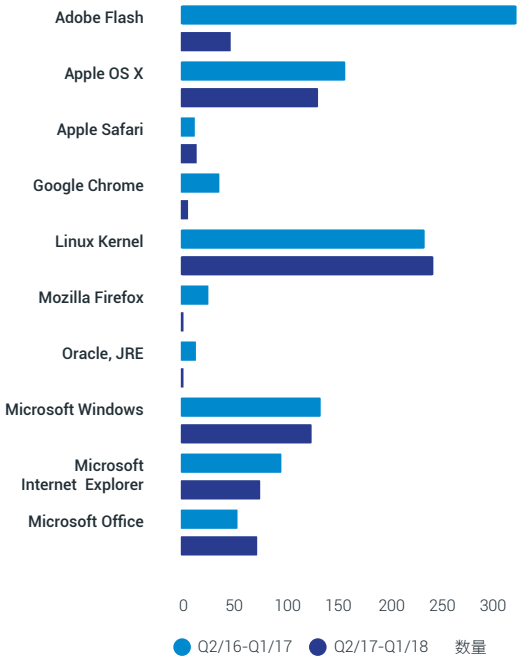

图 2：关键公共漏洞与披露（CVE）条目，数据截至 2018 年 3 月 31 日[5]

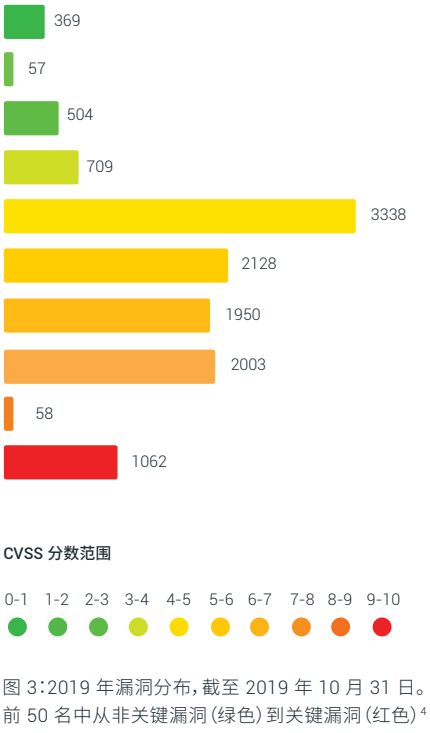

图 3：2019 年漏洞分布，截至 2019 年 10 月 31 日。前 50 名中从非关键漏洞（绿色）到关键漏洞（红色）[4]

90% 被利用的软件漏洞都发生在其刚发布的前 40-60 天里。由于 IT 管理人员是相关责任人，他们需要尽快采取行动，必须部署、测试和推出补丁。对于 IT 管理人员来说，这不仅会消耗大量时间，也是重要的成本因素。

随着漏洞数量的增加，手动打补丁这项工作变得单调乏味，并且作为日常工作来确保所有设备都成功打好补丁也不切实际。手动打补丁后续的流程也需要手动进行，这也增加了 IT 管理人员在时间和资源上的负担。

在涉及到手动补丁程序时，根据系统的复杂程度，可能需要依靠终端用户来打补丁。这通常会影响补丁程序的实施能否成功。

修补服务器端相对容易，因为 IT 管理人员对其有完整的控制权限，但客户端才是安全漏洞主要出现的地方（约占 95%），而保持客户端最新比较难。组织问题会和人为因素一样产生影响；人们推迟打补丁是因为不想扰乱当前的工作。出于这些原因，打补丁通常会被忽视，往往尽管补丁已经上线很久了，却因为时间和成本的原因而总是没有安装。然而，如果没能正确地打好补丁，网络罪犯可以系统地利用这些漏洞来攻击。

这些软件漏洞可以引发应用或 IT 网络出现严重安全漏洞，这就是为什么企业如今面临着优化组织和管理 IT 基础设施的巨大挑战。补丁管理将是最佳的解决方案，可以减轻 IT 管理人员的的压力，提高 IT 基础设施的性能、工作效率和效能。一个有效的补丁管理解决方案会检查系统最适用哪些补丁，自动分配和部署补丁，并根据紧急程度对补丁进行分类。因此，补丁管理不仅能增强了部署补丁的能力，也最大程度地减少手动打补丁的步骤和人为错误带来的风险。

补丁管理不善带来的**风险**

代价高昂的系统停机

失去客户信任

冗长的修复时间

不可靠的数据完整性

负面舆论

不安全的 IT 环境

补丁管理的**优势**

定期的自动修补能显著提高 IT 系统的安全性和网络的完整性，这是补丁管理最明显的优势。不过，自动补丁管理解决方案也为企业带来了其他的重要优势。

提升 IT 生产力，减少计划外停机时间

手动补丁管理对于 IT 管理人员来说十分耗时。识别漏洞、确定哪些终端需要打补丁，以及最终推出补丁程序并将其正确应用到受影响的计算机和笔记本电脑，将花费大量的时间和资源。

此外，这将导致需要访问其设备的员工经历计划外的停机。因此，自动补丁管理解决方案不仅可以帮助 IT 人员提高工作效率，也可以为员工最小化计划外的停机的时间。

实现安全性与数据合规，降低风险

在IT部门，安全合规准则至关重要，不可小觑。IT 合规可以保护公司免受处罚和对其品牌形象的潜在危害。例如，软件漏洞可以导致严重的数据泄露，是主要的安全风险。

如果员工或客户的敏感数据被暴露，企业可能会因为违反数据保护规定而受到处罚。这可能会导致客户流失或负面宣传。而有效的补丁管理解决方案可以检测安全漏洞，帮助降低上述风险。

TeamViewer 补丁管理解决方案

修补终端可以保护您的整个网络不受网络黑客的攻击。但您是否知道，即使只有一台设备未打补丁，也可能导致您的整个 IT 基础设施面临风险?

使用 TeamViewer Remote Management 的补丁管理解决方案，**漏洞可以被自动检测到**，让您可以轻松保持所有设备最新并安全地打好补丁。

使用 TeamViewer 补丁管理保护您的IT网络

使用自动补丁管理，随时掌握关键补丁。可立即查看是否有可用更新，并通过集中平台大规模部署更新。

通过中央控制面板管理和部署 Windows 更新，确保您所有的 Windows 设备最新。

降低风险，自动监控第三方应用程序和操作系统更新，并自动部署补丁。

在单个控制面板上查看设备的补丁状态和所有可用的补丁。

为不同部门及客户制定单独的策略，以定制并自动执行修补任务。

确定补丁的优先级，查看哪些补丁更为关键、紧急或是否可以根据优先级排序将其推迟。

从任意地点远程管理和检查补丁。TeamViewer Remote Management 与TeamViewer 远程访问解决方案的无缝集成让您只需点击几下鼠标便可访问所需设备。

核心**优势**

通过快速全面的 IT 系统更新，来节省时间

自动应用补丁程序，以修复软件漏洞

集中管理计算机

提高员工的生产力

充分利用从详尽的跨网络报告中获得的洞察

通过系统状态概述了解您的 IT 基础设施

减少计划外的设备停机时间

降低安全性和合规性方面的风险

主要**功能**

识别漏洞

通过自动检测过时软件导致的漏洞，获得对整个网络的可见性。

快速推出，已与 TeamViewer 集成

只需点击几次鼠标，便可为您的整个网络部署补丁管理

自动补丁部署

自动检测和部署基于策略的，针对过时、易受攻击的软件、操作系统以及第三方应用的补丁，以保持您的 IT 基础设施安全和最新

结论

IT 部门明确知道，他们必须持续保护公司免受网络罪犯的攻击，以及自动补丁管理解决方案是增强终端安全性的关键。尽管补丁管理很关键，却无需过于复杂。

凭借易于使用的特性，TeamViewer 补丁管理帮助您主动保护您的 IT 基础设施、避免无聊的手动修补任务，同时提高您网络的安全性、稳定性和完整性。

资源

获取有关 TeamViewer Remote Management（包括补丁管理）的免费演示

了解更多，请访问 teamviewer.com/patchmanagement

开始免费试用补丁管理

TeamViewer

参考资料

1. National Institute of Standards and Technology (November 2019): Automation Support for Security Control Assessments: Software Vulnerability Management, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8011-4-draft.pdf
2. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf
3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf;jsessionid=F64FE0EE50A281C976D952B395DCD531.2_cid369?__blob=publicationFile&v=5 S.11
4. CVE Details (2019): Current CVSS Score Distribution for all Vulnerabilities, https://www.cvedetails.com/cvss-score-distribution.php
5. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3 page. 43
6. CVE Details (2019): Vulnerabilities by Date, https://www.cvedetails.com/browse-by-date.php

关于 TeamViewer

TeamViewer 是一家领先的跨国科技公司，为用户提供一个远程访问、控制、管理、监控和维修任何类型设备的平台，从笔记本电脑和移动电话，到工业机器以及机器人。TeamViewer 帮助各种规模和行业的公司通过流畅的连接，实现业务关键流程的数字化。在设备分散、自动化和新工作模式等全球大趋势的背景下，TeamViewer 积极塑造数字转型，并在增强现实、物联网或人工智能领域不断创新。自 2005 公司成立以来，TeamViewer 软件已经安装在全球 22 亿多个设备上。公司总部位于德国，TeamViewer AG (TMV) 在法兰克福证券交易所上市，隶属于 MDAX。

www.teamviewer.com