ManageEngine 卓豪

# 医疗行业网络安全: 遏制医疗行业IT网络攻击和数据泄露的10种方法

# 目录

# 医疗行业挑战：
## 自信应对

从冠状病毒到气候变化，几乎不可能在没有现代医学帮助的情况下，人类可以应对的全球性系统性威胁。随着IT技术子在医疗行业的应用，信息化和数字化给IT管理带来了各种新的挑战，这些年来，我们可以看到IT在医疗行业得到了越来越受到重视。从采用网络安全和数字化转型到重新构想公共卫生和医疗服务，IT成为医疗行业是否具备可持续增长所需的能力，这种增长能够极大地改善我们的生活。科技让工作与生活更轻松美好！

在本电子书中，我们将主要关注医疗信息技术和运营技术面临的挑战，也就是IT和OT这对表亲。IT指的是信息技术，包括硬件和软件，主要关注数据。相较之下，OT是操作运营技术，处理的是流程和设备，在医疗行业环境中，这通常包括遗留和不一致的设备。我们将分析当前医疗行业IT的状态，并寻找减少网络威胁风险的方法，旨在提供无缝和安全的医疗服务。

# 医疗行业面临的主要IT障碍

## 医疗行业的IT管理员面临哪些挑战？

01
安全事件

02
数据泄露危及
患者隐私和敏感商业信息

03
缺乏网络可视化

04
适应数字化转型

05
采用新技术

06
处理合规性

## 01 减少安全事件

医疗行业中的安全事件可能是勒索软件攻击瘫痪医院IT系统，也可能是入侵患者隐私（如个人身份和健康信息泄露）。

除了这些导致运营中断的安全时间之外，近年来不断演变的网络攻击方式也造成了严重影响。

一例因网络攻击导致的死亡事件发生在2020年9月，当时一家德国医院遭遇勒索软件攻击，无法接收一名身患动脉瘤而急需就诊的78岁女性患者。原因是负责协调医疗团队和医院床位的数字系统发生故障。当她能够被送入另一家医院时，已经为时已晚。

## 02 遏制数据泄露

在医疗和制药行业，黑客主要针对两个特定群体：一是客户，即患者，二是医疗行业供应商或组织。这两个群体都有大量的敏感数据和资源可能被访问和篡改。大量数据还由多个供应商存储和维护，这些供应商代表医院处理数据。由于有这么多变数，同时数据被多个实体存储和处理，映射和保护这些数据变得非常困难。

## 03 对医院IT/OT网络缺乏可视化

除了IT资产，如计算机、笔记本电脑和移动设备外，医院的网络还包括OT系统和设备，例如暖通空调（HVAC）系统、患者监测系统、重症监护室中使用的设备等等。由于更多的智能设备和物联网设备被整合并相互连接，其使用量也快速增加。

在网络中存在如此多不同类型的设备时，IT管理员可能对所有设备的完整理解和相应工具掌握不足，导致IT盲点。这些网络盲点基本上是被忽视的“黑暗区域”，却又在医院IT/OT系统中扮演着重要角色。当发生组织变更时，情况可能会变得更糟，IT很难掌握网络、数据和应用程序的行为。在这种情况下，可能会导致更多的盲点。

## 04 适应数字化转型和颠覆性创新

虽然医疗行业在很大程度上是由创新驱动的，但它也因最容易受到网络攻击而意外频出。医疗数据泄露的平均成本为923万美元，几乎是金融行业（在数据泄露成本排名中位列第二）的两倍。

随着医院和医疗团队大量采用新的技术和变革实践来拯救生命，他们的关键基础设施也面临着风险，入侵者和风险行为更加肆意，越来越难防备。根据第三方数据泄露报告，在2021年，医疗行业成为网络攻击中最受针对的受害者，占33%，而政府部门的比例则远远低于这一数字，位列第二。然而，一方面要进行数字化改革，一方面在适应新技术所需的IT投资却很有限。这可能是一个巨大的限制因素。

## 05 合规性与监管

大多数医疗组织将合规性（如HIPAA）视为障碍。实际上，这些合规性更像是保护神，帮助组织以安全和保密的方式处理电子保护健康信息（ePHI），避免受到网络犯罪分子的窥探。虽然执行监管机构的严格政策可能面临挑战，但最终的结果是值得的。

# 分析和学习近期医疗领域的网络攻击

一个典型的医疗生态系统由多个IT和OT系统组成，从计算机和服务器到特定设备，如床边监视器和呼吸机。随着医院用创新设备和智能物联网解决方案现代化其基础设施和公用事业，他们也冒着将这些资产暴露给各种攻击者和威胁行为者的风险。根据波诺曼研究所编制的2021年数据泄露成本报告，医疗组织连续第11年经历了最高的平均数据泄露成本，且与前年相比几乎增长了30%。

2021年医疗数据泄露的平均成本为：923万美元。

相比2020年（713万美元）增长了29.5%。

**医疗行业是最容易受到网络攻击的领域**，其次是金融服务。

根据美国健康与公共服务办公室的《未加密保护健康信息泄露报告》提供的数据，仅在2022年1月，就有超过230万医疗患者因数据泄露而受到影响。在总结和了解医疗领域网络攻击的性质后，一些常见的数据泄露可以归因于：

- 被盗的商业电子邮件
- 未经授权的访问
- 数据盗窃
- 勒索软件
- 被黑的网络服务器钓鱼
- 不安全的服务器/数据库

这里不再深入探讨上述每种网络攻击的细节和方法（你可以在篇文章中了解更细的介绍），我们重点讨论如何降低这些风险，并保护IT免受网络攻击。

# 医疗行业遏制网络攻击的10种方法

## 01 启用零信任

零信任是一种网络防御模型，旨在限制对网络和应用程序的访问。它是一种基于“没有人应该被信任”这一前提的网络模型。零信任网络访问（ZTNA）将每个网络设备视为潜在风险，直到被证明是可信的，这与传统网络方法相反，传统网络中一旦设备通过安全层即可视为可信。

“默认情况下不信任任何用户或实体”的零信任网络访问方法可应用于VPN和代理服务，以及其他依赖于客户端与服务器之间信任的服务。

## 02 强制多因素认证

多因素认证（MFA）是一种在登录过程中为验证身份增添额外安全层的方法。启用MFA后，用户需要以两种或更多方式进行身份验证，才能访问组织的信息。这样，即使员工的密码被泄露，其他身份验证方式也会阻止风险行为者登录。

这些额外的身份验证方式通常是基于时间的一次性密码、生物特征扫描或来自认证应用的代码。MFA提供了许多好处，或许是组织能设置的最简单的网络防御机制。

## 03 减少攻击面

攻击面是您网络中所有物理和数字资产的组合，未授权用户可以通过这些资产访问您的网络并提取私人数据。常见的攻击面包括计算机、交换机、应用程序、代码、端口、服务器和网站。需要通过云端和本地的系统来管理这些资产，发现潜在漏洞或弱点，审核用户角色和权限级别，从而管理和保护您的攻击面。

随着医疗行业变得越来越智能，创新解决方案将我们带入下一个前沿，扩大企业的数字足迹不应成为担忧的理由。监控和保护您现有的攻击面比试图减少它要好。简而言之，引入新技术不应该因潜在网络攻击的威胁而放弃。

## 04 操作系统及应用程序的自动化补丁管理

及时应用最新的补丁和更新软件及应用程序仍然是任何网络攻击预防计划的重要部分。IT 管理者不能轻视修补和保持软件最新的重要性。

由于及时应用补丁和软件更新至关重要，因此自动化这些流程以限制医疗IT系统的潜在漏洞暴露是非常重要的。未修补的系统仍然是网络攻击的主要目标，因此自动化软件更新并在补丁发布后及时安装是正确的做法。

## 05 确保强有力的设备和应用控制

攻击者利用存储设备侵入医院系统并非只是科幻电影中的刺激场景。攻击者可以将设备插入您的 USB 端口并运行一个脚本，使医疗设施失去功能。

解决这一问题的一种方法是阻止使用外部存储设备。可以通过使用设备控制解决方案来实现，这样可以监控外设和端口。您还可以审核接入的设备并分析用户行为，以防止内部威胁。

除了监控与硬件相关的潜在有害行为外，您还可以通过仅授予特定群体访问权限或限制在公司机器上使用未经授权的应用或软件来增强企业的终端安全措施。

## 06 强化访问控制

从主任医生到初级护士，所有医院工作人员都需要快速、轻松地访问数据，以实现患者更好的体验。充分的访问控制确保每个用户有适量的访问权限，避免所有人都使用管理员权限的情况。

如果医疗人员需要访问那些管理员权限的资源，可以暂时提升他们的权限，以便他们高效地完成工作。访问控制保护您的数据，通过跟踪用户访问情况提供问责机制，并确保符合IT法规。

## 07 修复漏洞

传统的修复方法只针对厂商有记录的已知漏洞。其余的未知漏洞没有被记录，通常在造成破坏之前都是隐蔽的。漏洞管理解决方案确保持续可见性，检测弱点，评估风险并修复。这样的话，您可以按照合规基准基线审核和维护系统，并保持获得最新的修复方法。

## 08 整合多层安全防护

您的企业安全指标包含在多个层面，需要在各个层面提供深入的保护。例如：

- → 防火墙
- → 入侵检测和预防系统，
  如杀毒软件和恶意软件保护
- → 网络监控系统
- → 安全认证

## 09 实施加密和数据备份

加密可以保护敏感信息（如医院信息和病人记录），拒绝未授权用户或黑客等不应获得访问权限的人访问。这在勒索软件攻击中尤其有用。即使您的数据受到威胁，恶意行为者也无法泄露数据的内容，从而保护敏感数据。

没有足够的数据备份，加密是不完整的。备份重要和敏感的信息至关重要。这样，您可以在数据泄露发生时无缝过渡。拥有数据备份和恢复计划也是一个至关重要的过程。

列出需要离线保存的数据项目，包括存储设备或云存储中的数据文件和文件夹、操作系统镜像、客户数据库、机器镜像、操作系统和注册表文件。需要关注每个部门的需求，按需管理。许多供应商提供符合HIPAA标准的备份和数据恢复解决方案，以简化这一过程并确保中断最小化。

## 10 确保终端管理和保护

终端可以是办公室计算机、移动电话、平板电脑、路由器及其他设备，它们可以从本地或远程位置访问网络。终端保护是一个广泛的术语，包括多个方面，如漏洞管理、浏览器安全和应用控制。

ManageEngine的Endpoint Central 作为终端保护解决方案，以多种方式保护您的终端，从保护最终用户浏览器到控制外部设备和应用程序。这些安全保护都包含在其终端安全套件中。此外，Endpoint Central 可以集中管理和监控分布在多个平台和网络的所有终端。

# 医疗行业IT/OT路线图

## 01
## 实现可视化

- 通过获取资产列表确定攻击面
- 识别网络盲点
- 执行合规检查
- 进行安全分析和健康检查
- 分析需求

## 02
## 强化各安全指标

- 利用防火墙
- 启用零信任
- 安装入侵检测系统
- 部署风险预防系统
- 利用MFA进行安全认证
- 实施密码管理
- 使用VPN

## 03
## 持续监控

- 部署终端安全工具
- 实施数据泄漏防护策略
- 采用设备和应用控制
- 强制实施特权访问
- 引入漏洞扫描工具

## 04
## 确保医疗服务的最大正常运行时间

- 确保关键健康服务的可用性
- 进行数据备份
- 加密信息
- 平衡网络韧性与生产力
- 利用终端保护

## 05
## 验证和进化

- 测试网络安全
- 验证和检查设备升级及技术部署
- 加密信息
- 建立测试环境以检查软件更新和补丁

# 关于ManageEngine卓豪
## 统一的终端管理和安全

ManageEngine卓豪的统一终端管理系统为希望创新和变革的团队开发的终端管理和安全工具。我们的统一终端管理（**UEM**）解决方案实现管理自动化、提供深入分析，是提升管理和保护终端的可靠方案。使用一个平台，您就可以保护您的组织。更敏捷地工作，掌握最新信息，提升操作效率，消除技术瓶颈。

开始尝试ManageEngine UEM 方案吧 >>>

找到我们：

sales@manageengine.cn

400 660 8680