tenable®

使用案例：

医疗保健行业中的网络安全

数据论点：

- 经过确认的数据外泄数量较去年增加了 71%[1]
- 医疗保健行业的内部攻击者数量最高，内部网络罪犯的数量几乎与外部相同
- 紧随在数据外泄之后，第二大最常见的网络攻击手段是通过 Web 应用程序

近期大事件：

- **2020** 年 **5** 月：一场针对 BJC Health System 的鱼叉式网络钓鱼攻击得逞，近 288000 份患者记录遭到外泄
- **2020** 年 **4** 月：第三方安全记录存储和处置供应商未正确处置患者档案，导致 550000 份患者记录遭到曝光
- **2020** 年 **1** 月：一场针对 Ambry Genetics 的电子邮件攻击得逞，近 233000 份患者记录遭到外泄
- **2020** 年上半年：41 家医院和医疗保健机构供应商报告称遭到勒索软件攻击的实际影响，这一数量自 2018 年以来增长超过两倍

*上述数据论点和近期大事件指美国市场。

背景

过去几年以来，医疗保健行业发生了翻天覆地的变化，技术革新将医生接诊和高级诊断服务直接送达患者身边，每周 7 天，每天 24 小时，从世界上任何一个接入互联网的地方皆可享受。

这些创新使得医疗保健服务比以往任何时候都更贴近患者：自助式门户网站能够快速获取检测结果；基于视频的远程预约方便医生接诊脆弱且行动不便的患者；对存在可能危及生命病况的患者进行持续监控，一旦发生重大变化，立即通知主治医生；以上仅仅试举几例。

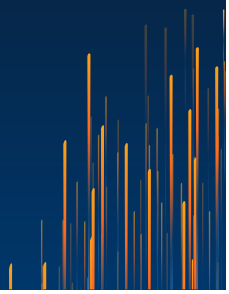
这些服务中有些给患者带来更多便利，另一些则显著改善了危重患者的预后和生存率。此外，这些创新大部分旨在减少诊室预约、昂贵的诊断检测和住院数量，使得医疗保健机构能够大幅降低运营成本。

尽管这种程度的创新带来了诸多优势，但也使医疗保健机构暴露于广泛的网络安全威胁之下。因此，IT 和安全团队需要面临艰难决定，即如何在不牺牲医疗保健机构安全态势的情况下支持创新。

[1] Verizon，“*2020* 年数据简报调查报告”。https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

主要挑战

- 医疗保健机构网络内外连接着无数医疗设备，这些设备往往以患者可直接控制的平台为基础构建，导致网络容易遭到攻击
- 重要患者数据对持续可用性的要求导致系统难以停机，无法满足更新和维护需求
- 全天候的患者护理服务要求设备和 IT 系统随时在线，但这往往与健全的安全措施相背离



医疗保健行业网络攻击：危险显而易见

医疗保健机构经常成为网络攻击者针对的目标。针对医疗保健机构的常见网络攻击形式有网络钓鱼、暴力破解攻击和勒索软件等，使得患者数据和医疗保健机构的声誉时刻危如累卵。

一旦发生外泄，最主要的担忧在于可能有损机构声誉并侵犯患者隐私，同时也可能对日常业务运营产生巨大影响。锁定内含预约数据等系统的勒索软件和其他攻击可能导致整个机构陷入混乱，医生诊室、诊所和检测机构都将无从得知患者就诊日期和检查安排。

电子病历 (EHR) 一度是最大胆的技术进步，冒着牺牲网络安全的风险推进患者护理，而在过去几年中诞生的每一项创新，各自都代表着一条更容易遭到利用的新途径，可能被攻击者入侵。更令人触目惊心的事实是，许多创新利用了由患者操作和管理的设备，使得从任何网络访问成为可能，而互联医疗设备等另一些创新则建立在无数物联网 (IoT) 平台上，往往缺乏适当的安全协议。总之，医疗保健机构面临着众多全新的漏洞。

传统的漏洞管理无能为力

传统的漏洞管理工具从设计上就无法应对现代攻击面及其爆发式增长的威胁数量。另一方面，这些工具可见性仅限于传统 IT 环境，整个遗漏掉了现代攻击面中变化最为迅速的各类漏洞，包括云、运营技术 (OT) 和容器环境。在医疗保健行业，容易遭到利用的切入点包括远程患者监控设备、床边互联设备（如 PCA 机器）和便携式 EKG 机器等资产。

传统的漏洞评估工具还缺乏风险认知，完全依赖于通用漏洞评分系统 (CVSS) 的基础评分来确定要修复的漏洞。由于 CVSS 基础评分是静态得分，并且没有任何程度的业务上下文或威胁情报，这会导致安全团队将大部分时间浪费在错误的事务上，错失了大量对机构与企业构成最大风险的最重要的漏洞。

企业与机构中最常见的方法是将每个漏洞按 CVSS 基础评分是否达到 7.0 或以上进行优先级分析。但根据 Tenable Research 的研究，有超过一半的漏洞能够落入这一范围。但漏洞数量缩减到这种程度还远远不够，工作负荷很快就会失控。尽管许多机构都面临着这样的问题，但在医疗保健行业中尤其值得关注，因为工作积压可能会导致重要漏洞的修复工作延迟，从而影响到直接参与患者护理的资产。

安全需要持续可见性

为确保安全，企业必须持续评估整个攻击面中的每个资产险，而且使用基于风险的分析方法来动态评估漏洞、威胁和资产重要性数据的变化。如果未能清晰了解每一刻都有哪些因素在影响网络，安全团队就无法确定哪些漏洞构成最大风险，必须在网络中每次发现新漏洞利用或零日漏洞利用引起媒体关注时被动做出应对。

优先处理构成最大风险的漏洞

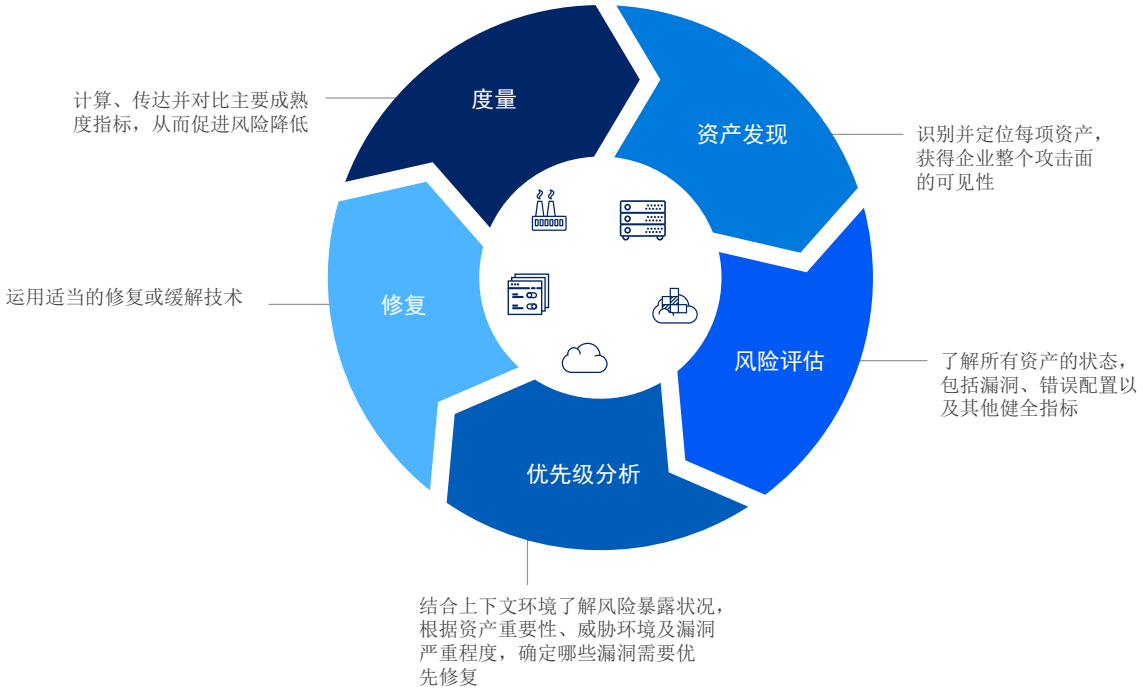
在不断变化的庞大网络和技术创新不断引发的漏洞之间，机构面临的漏洞数量远超安全和 IT 团队可预期的应对能力。此外，面对着技术高超的大量对手，机构难以负担在不构成真正业务风险的漏洞中浪费时间。

升级到基于风险的漏洞管理策略，有助于机构从高度被动、以业务中断为驱动、容易出错的方法进化到更为主动、更具战略性的方法，从而最大限度提高效率和有效性。

关于为何要升级到基于风险的漏洞管理策略，首先要理解的是，该解决方案远比使用传统漏洞管理工具的解决方案更为全面。不同于传统方案仅仅发现和评估漏洞，采用基于风险方案的机构还能有效分析漏洞优先级、确定要采取的适当措施、计算关键指标，并与医疗保健领域的各项标准进行比较。该方法不仅可以帮助确定如何调整优化策略，支持在管理层中建立并维持信心，避免在遇到重大漏洞利用时出现恐慌。

利用基于风险的漏洞管理，安全团队能够将精力聚焦于 3% 构成最高风险的漏洞，从而解决机构真实的业务风险，而不是将宝贵的时间浪费在遭利用可能性较低的漏洞上。通过了解每个漏洞的完整上下文（包括严重程度、威胁制造者活动和受影响资产的重要性），以及采用机器学习技术预测攻击者在未来 28 天内最可能利用哪些漏洞，就可以采取果断措施，以最少的工作量减少最大的业务风险。

基于风险的漏洞管理生命周期



总结

对于医疗保健领域的网络安全专业人员，应当时刻谨记需要保护机构数据以及敏感的患者数据。这些数据不仅对机构具有重要价值，同时患者护理的质量，有时甚至生命也取决于这些数据是否始终安全可用。持续创新为别有用心之人创造了源源不断的攻击载体。因此机构需要排除干扰，专注于处理构成最大风险的漏洞。基于风险的漏洞管理有助于机构专注于处理风险最高的漏洞，从而充分利用有限的资源，始终领先对手一步。

关于 Tenable

Tenable®, Inc. 是一家 Cyber Exposure 公司。Tenable 帮助全球 30000 多家企业了解和减少网络风险。Tenable 是 Nessus® 产品发明者，凭借在漏洞方面的专业技术，推出了全球首个检查和保护各种计算平台上数字资产风险的平台。Tenable 的客户包括 50% 以上的《财富》500 强企业、30% 以上的全球 2000 强企业和大型政府机构。详情请访问 zh-CN.tenable.com。

082020 v1