Akamai

白皮书

面向医疗保健提供商的网络安全保护

简介

为了在日新月异的市场中占据一席之地，医疗保健提供商企业积极采用新设备和应用程序，以便为患者提供优质护理和提升患者体验。随着这些新设备和应用程序的引入，企业在为患者提供便利的同时，也面临着一系列安全风险。

这种复杂的 IT 环境，加之受保护的健康信息 (PHI) 所蕴含的高价值，无疑为网络犯罪分子提供了极具吸引力的机会，使他们不断对企业系统发起攻击。美国卫生与公共服务部的一份报告以及 IBM 的研究显示，自疫情爆发以来，医疗保健行业遭受的网络攻击激增了 50%。这些攻击造成了巨大的经济损失，平均每次攻击造成的损失高达 713 万美元。IBM 报告着重指出，勒索软件攻击成为了最常见的威胁（恶意攻击者抓住了医院和医疗系统需要迅速恢复运营的软肋），紧随其后的则是数据窃取和服务器访问。而医疗保健提供商尤其是勒索软件攻击者的主攻阵地，因为每份电子健康记录 (EHR) 在暗网上的售价达 1,000 美元，信用卡信息的售价约为 110 美元，社会保险号的售价仅为 1 美元。

企业系统遭受的威胁数量不断攀升，但许多企业尚未做好充分的准备来抵御这些挑战。更令人担忧的是，有些企业甚至已经遭到攻击，却对此一无所知。攻击者可能已在暗中窃取数据，或正在等待合适的时机发动攻击。

因此，现在是时候对您企业的攻击面进行全面审查了，包括盘点所有设备以及它们如何与基础架构相连接。通过更好地了解漏洞所在的位置，实施可靠的抵御策略，我们将能够预防或充分减轻网络攻击带来的潜在影响。

如何防范您企业面临的最大网络安全风险

威胁 1：网络钓鱼攻击

网络钓鱼是所有行业中极为常见的一种网络攻击手段。根据卫生部网络安全协调中心公布的数据，2021 年医疗保健领域遭受的网络钓鱼攻击数量出现了显著增长。实际上，在 2020 年全年，Akamai 发现犯罪分子利用新冠疫情和经济援助承诺或者财务困境方面的压力，通过网络钓鱼对全球各地的人们发起攻击。

网络钓鱼企图通过发送欺诈性电子邮件或网页来骗取敏感数据。如果诈骗成功，受害者会在不知不觉中输入自己的登录凭据，这相当于为犯罪分子敞开了网络的大门。

这种情况曾真实发生在纽约申请失业救济的人们身上。CSO Online 前编辑、现任 Akamai 安全研究人员 Steve Ragan 在其发布的一份网络钓鱼报告中指出，2021 年初，一些针对疫情失业援助 (PUA) 计划的网络钓鱼工具包浮出水面。这些计划旨在为新冠疫情封锁期间需要帮助的人们雪中送炭，并为数百万美国人提供了急需的基本服务。

在 CBS News 向全国播放的新闻节目中，Ragan 讨论了一个专门针对纽约居民的失业网络钓鱼工具包，并揭示了犯罪分子是如何通过这一骗局来收集和贩卖个人信息的。自从该新闻报道播出后，他又发现了类似的 PUA 骗局，攻击的是威斯康星州、印第安纳州、宾夕法尼亚州和马萨诸塞州的居民。

如何发现并抵御网络钓鱼攻击

由于权限设置和安全防护措施的不同，犯罪分子在获取单个用户帐户的访问权限后，可能会有机会自由操控您网络的关键部分。一旦他们成功侵入企业的网络，往往会进一步扩大攻击范围。

通过实施微分段，我们能够约束攻击者的行动范围，使其只能访问他们最初获得权限的网络部分，难以进行横向移动，进而避免在其他区域造成进一步的破坏。这样做能够防止犯罪分子利用任何入口点来访问企业更广泛的网络，从而限制入侵所造成的影响。

除了微分段，多重身份验证 (MFA) 也是抵御网络钓鱼攻击的重要防线之一。MFA 为企业提供了额外的保护层，要求用户通过额外的身份验证后才能访问帐户，从而防止了被盗凭据被恶意利用的风险。

MFA，特别是经 FIDO2 认证的解决方案，确保了企业可以免受最新攻击的威胁。它要求用户输入由其移动设备上的文本或身份验证应用程序生成的独特验证码。这个额外的登录步骤有助于阻止网络钓鱼攻击，即使犯罪分子拥有准确的登录凭据也难以得逞。

让员工了解网络钓鱼等社会工程攻击策略至关重要。事实上，网络钓鱼问题目前没有绝对有效的解决办法，因为其中涉及大量多变的活动环节。人们很难预测犯罪分子下一步会做什么。由于人始终是网络钓鱼中的一个重要因素，他们将会成为整个链条中最薄弱的一环。

这意味着简化安全流程变得至关重要。Akamai 提供了一种流畅的防网络钓鱼 MFA 解决方案，确保即便是最狡猾的网络犯罪分子也无法轻易攻破。

威胁 2：不受支持的遗留软件

过时的软件是另一个严重的漏洞隐患。未能及时安装新的安全更新（补丁）会在您的网络上留下敞开的后门。尤其是对于那些老旧的设备，由于它们已经失去了支持并且不再接收更新，情况更加严峻。

这些不受支持的软件可能隐藏着零日漏洞，而企业在面对这些漏洞时可能会犹豫不决，不确定是否应该自己进行修补。创建自定义补丁有时会导致设备保修失效，从而在设备出现问题时产生高昂的维修费用。

尽管医疗设备的生命周期相对较长，但如果未能及时更新至最新版的操作系统，或运行不受支持的操作系统，黑客就可能会利用这些漏洞窃取敏感数据，甚至渗透到整个医院网络中，导致医疗服务中断。事实上，《财富》杂志曾报道过，高达 83% 的联网医疗成像设备（乳腺 X 光机及 MRI 核磁共振设备等）都非常容易受到攻击。

设备使用年限越长，特别是有些设备甚至超出了维护生命周期，犯罪分子就越有可能发现这些设备的弱点，通过第三方设备来访问您企业的网络。

以 Windows 95 为例，尽管该操作系统已停止维护多年，但许多 MRI 核磁共振设备（以及其他设备）仍在使用，因为它是最后一个支持直接写入的操作系统。虽然内部开发人员有能力修补这一漏洞，但所安装的补丁可能会使设备的保修失效。唯一安全的选择是彻底更换 MRI 成像仪，然而，这种做法对许多机构来说成本过于高昂。

网络管理员尝试将不受支持的系统排除在网络之外，但这并不总是可行的，特别是在设备需要用于患者护理且必须迅速向医生提供关键数据的时候。如果连接到网络的所有设备的映射不完整，隔离措施也会失效，从而留下后门。对于不在监测范围内的资产，您很难保护它们。

如何保护易受攻击、不受支持的设备

为了防范犯罪分子利用这些设备潜入您企业的网络，转向 Zero Trust 网络访问 (ZTNA) 架构变得至关重要。ZTNA 将每个传入请求都视为潜在威胁，直到证明其安全为止。这种框架能够在攻击者尝试访问设备之前有效阻止他们，即使您的软件已经过时，他们也无可乘之机。

转向 ZTNA，意味着我们从过去几年所依赖的城堡和护城河模式，转向（先验证后信任）Zero Trust 模式。虽然 Zero Trust 方法不能百分百地防止网络攻击，但它却能将潜在的损害从灾难性级别降低到可控范围内。正如 HealthITSecurity 所说：“即使攻击者成功窃取凭据并操纵一台设备，但在 Zero Trust 架构下，他们也很难继续深入攻击。”

Akamai 提供了一个可靠的计划来帮助提供商迁移至 Zero Trust 架构，无需停机，同时还能保持现有工作流程的灵活性。使用这份蓝图指南，开始转向 ZTNA。

威胁 3：居家办公和利用自带设备工作的提供商

在 21 世纪，患者护理方式变得更加多样化。患者可以在自己舒适的家中接受护理。提供商可以通过其移动设备提供护理，而非亲自到场。但是，随着可访问性日益增强，提供商面临的网络安全风险也急剧升级。这是因为员工在实地和家庭之间频繁切换网络登入点，同时使用非受管理的设备进行登录。

尽管在疫情之前，您的团队成员偶尔会从家庭网络登录到您的系统，但在疫情期间，访问您企业网络的个人设备数量不可避免地大幅增加。这些笔记本电脑、平板电脑或智能手机如果感染了恶意软件，都可能成为勒索软件攻击的突破口。

例如，如果您的团队成员不慎在虚假网页上输入了登录信息，就会成为网络钓鱼攻击的受害者。攻击者将能够获取与受害者相同的访问权限，他们可能会加密文件，锁定您的团队，甚至要求您支付高额赎金以换取文件的解密。

如何保护您网络的边缘

通过紧密监控谁正在访问您企业的网络，包括确定他们的地理位置、IP 地址以及使用的设备等信息，您可以显著降低发生类似事件的几率，防患于未然。

如果您的团队使用个人设备或居家办公，那么不妨问自己以下问题：

- 我们是否采用了 Zero Trust 网络访问 (ZTNA) 方法，以便严格审查所有传入请求，并在攻击发生之前及时阻止它们?
- 我们是否实施了微分段，在犯罪分子成功侵入企业的网络后，限制其访问权限并防止其在网络中横向移动?
- 我们是否采纳了安全访问服务边缘 (SASE) 框架，从而保护我们的网络安全，同时尽可能地降低延迟，确保提供快速且愉悦的用户体验?
- 我们的团队是否为每台设备和每个帐户登录使用访问码、强大且唯一的密码，以及多重身份验证 (MFA)?

Akamai 的远程员工安全解决方案能够助您简化网络访问管理。

威胁 4：糟糕的数据流映射

一只脚还踏在本地，而另一只脚已步入云端，这会导致您很难理解数据的确切位置及其流动路径。这种情况的发生，背后存在着多种不同的原因。

首先是数量。想要跟上每天（甚至每小时）网络中设备和应用程序的数量变化会非常困难，因为供应商、承包商和顾问使用的设备、工具和解决方案五花八门。

其次，用于跟踪硬件和软件的系统已变得过时，而且团队成员的流动、流程变动或冲突的业务重点导致这些系统不再准确或可靠。

无论出于何种原因，监测您的网络和联网设备是非常重要的，因为您无法保护看不见的资产。

如何映射联网设备的数据流

拥有一个监测工具来绘制联网设备的路线图至关重要。特别是 HIPAA 杂志 2019 年的一篇文章曾指出，过去 12 个月内，高达 82% 的医疗保健企业遭受了针对其联网设备的网络攻击。

选择一种能够追踪网络中数据流的解决方案至关重要，它能揭示数据的来源和流向，包括那些未与您网络连接的设备，这是您映射联网设备的第一步。通过这种解决方案，您将能够获取一张实时的网络图，清晰地展示信息流动情况，从而帮助您发现网络上具有恶意企图的设备。通过在核心系统、资产和数据（如 PHI）周围部署软件定义的微分段环，您的企业能够限制攻击者在网络中横向移动。借助 Akamai 的微分段工具，获得所需的监测能力。

威胁 5：管理网络、应用程序和系统的复杂性

您是否知道哪些应用程序和软件可以读取您的数据？某些软件应用程序（如社交媒体平台）在其隐私声明或服务条款中明确声明会读取用户数据。其他软件应用程序（如电子邮件服务提供商）虽然较为隐蔽，但仍然构成重大风险（例如，如果照片中包含 PHI，这些应用程序可能会访问设备中的照片）。

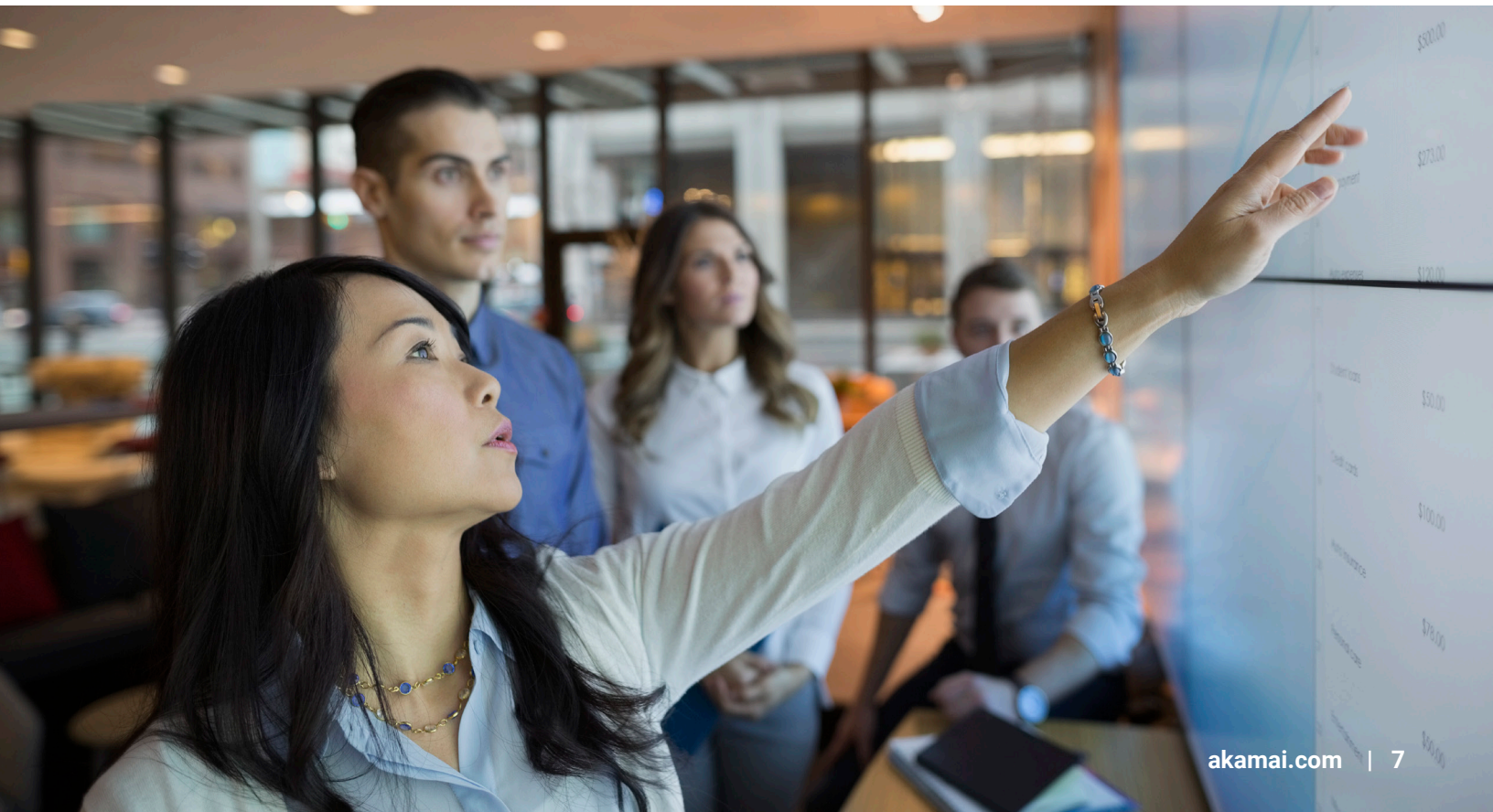
此外，应用程序还可能被授权查看剪贴板上的内容，这包括患者的识别信息或密码。如果设备中存储了患者信息，那么第三方（或恶意攻击者）就有可能会看到（甚至记录）这些信息。

培训您的团队，监测您的整个网络，保护您的边缘

至关重要的是，让您的提供商企业中的每位成员接受相关培训，以了解使用个人设备可能带来的风险，并严格遵守保护患者私人信息的规定。

同样重要的是，要监测您的企业是否具有攻击面和潜在攻击媒介。您的安全团队是在监控跨越多个云服务提供商和本地数据中心的整个网络？还是他们被分配到不同的小组，各自专注于企业基础架构的不同方面？全面监测企业整个网络及其活动至关重要，特别是在遭遇攻击时。

与威胁 4 类似，Zero Trust 架构结合微分段和面向帐户登录的 MFA 构成了保护网络边缘的最优防御选项。聘请一家提供商来统一保护所有系统，不论它们归属于哪个部门，也不论它们部署在云端还是本地环境，这样既可以保护网络，又不影响用户体验。



什么也不做会产生怎样的后果?

代价多种多样。其中财务损失尤为显著，IBM 的《2021 年数据泄露成本报告》指出，美国医疗保健公司因一次数据泄露所承受的平均总成本高达 923 万美元。另一些代价是难以可量化的，例如患者安全和信任，这些代价对医疗保健企业的影响同样重要，甚至可能更为关键。

患者安全不能得到保障

在网络安全领域，保障患者安全被视为首要任务。一旦 IT 系统遭受攻击导致瘫痪，患者护理工作将会中断。治疗和预约的推迟可能对患者健康产生不利影响。事实上，最近发生的一起诉讼案件首次指控了勒索软件攻击直接导致患者死亡。

与此同时，用于远程监测患者（如心率、血糖水平等）的联网医疗设备带来了更直接的护理风险。例如，如果患者的血压读数受到干扰，可能会导致危险状况被忽视或未得到及时治疗，从而可能引发严重的医疗事件。

丧失患者的信任

无法提供可靠的护理服务和保护患者信息，会导致丧失患者的信任。超过 90% 的患者表示，如果他们的私人信息在数据泄露中遭到盗用，他们将会更换医护机构。虽然真正会选择离开的患者可能比较少，但我们来算一笔账：即使只有一半或者说十分之一的病人选择离开，这将对您的患者群体产生怎样的影响？一边缓慢地吸收新患者，一边面临持续的患者流失，这种情况您能支撑多久?

收入流失

38% 的受访者认为业务损失是与数据泄露相关的最大成本因素。当核心提供商系统出现宕机，例如 EHR 或电子邮件服务器无法正常运行时，业务将会戛然而止。简而言之，没有预约、没有访问、没有接触、没有收入，更不用说对患者护理造成的影响。

2020 年 5 月，总部位于圣地亚哥的 Scripps Health 遭受了一次严重的网络攻击，导致急诊科护理和选择性手术数量减少，进而造成 9160 万美元的收入损失。

即使卫生系统网络的部分功能仍然可用，但在找到攻击媒介、修复漏洞以及完成取证分析之前，您无法保证整个系统的安全。

增加开支

招聘、雇用和维持一支出色的网络安全工程师团队需要投入大量资金，但这仅仅是冰山一角。在您的企业中组建一支自己培养的网络安全团队可能会带来更高的成本。

通常，您的企业在识别和清除攻击者方面所需的时间越长，所需承担的成本就会越高。Ponemon 研究所的一份报告指出，在前 200 天内检测到网络攻击可以为企业节省超过 126 万美元的成本。遗憾的是，根据同一份报告，识别和控制一次攻击平均需要 287 天。*287 天！*这意味着攻击者往往在网络基础架构中潜伏超过 9 个月，期间精心策划和准备攻击，以对医院声誉和财务状况造成最大损害。

因此，量化您的安全团队在识别攻击并采取相应行动所需的时间至关重要。通过整合安全供应商，选择那些既提供托管服务又能为员工提供工程支持的供应商，您可以显著节省成本。

法规罚款

由于您掌握大量宝贵的个人信息，数据泄露可能引发监管机构开出巨额罚单。截至 2021 年 11 月 30 日，卫生与公众服务部民权办公室已对 106 家受 HIPAA 法规约束的实体进行了罚款或达成和解，累计金额超过 1.31 亿美元。这意味着，平均每次罚款金额超过了 120 万美元（除了此处提及的其他费用外）。

如何让您的医疗保健企业做好应对网络攻击的充分准备

在当今的网络威胁形势下，提供商企业必须实施出色的安全保护机制。这不仅关乎患者的安全，也直接关系到您的业务存亡，什么也不做的代价太高了。

由于财务约束、冲突的业务重点或风险的不确定性，您可能会承担过多的风险。但是，您的安全工作必须全面、有战略性、保持警惕且敏捷。

即使今天的生态系统得到了充分的保护，明天它们仍然可能面临威胁。因为威胁演变得非常快。新的漏洞可能在一天甚至更短的时间内被攻击者利用。

提供商希望减轻这一领域所受到的威胁，并采纳联邦警告中概述的备份方法建议（以至少两种不同的格式保存三份副本，其中一份离线保存），同时也越来越倾向于采用混合型方法。内部数据存储让他们能够更好地控制安全性，但成本过高，也很难以所需的速度实现扩展，尤其是在受疫情刺激，健康数据呈现爆炸式增长和医疗数字化逐步转型的情况下。公有云数据存储更具成本效益，但企业需要承受停机和数据保护缺乏透明度的风险。

采用混合型方法后，就可以将敏感数据保存在本地，而将不太敏感的数据存储在云端。即使这样也称不上尽善尽美，因为必须采取安全措施来保护两种存储类型之间的数据传输，并确保只有那些获得授权传输和查看数据的人才能访问。通过满足实施 ZTNA 架构的七个关键要求，授权用户只能访问其角色所必要的应用程序，有助于机构保护其数据，同时采用 MFA 进一步增强其安全性。

Akamai 致力于帮助您做好充分准备，在攻击发生时能够从容应对。让我们携手合作，严密监测您的网络，从而迅速发现攻击并有效减轻其带来的损害。我们的业务核心在于构建一道坚实的防线，保护网络免受分布式拒绝服务和勒索软件攻击的侵扰，从而交付无缝且安全的网络体验（包括应用程序和 API）。

我们在您网络的边缘筑起坚固的堡垒，降低入侵的风险，并在威胁发生时缩小其影响范围。同时，我们还会保持用户访问的灵活性，使您的机构能够面对不断变化的运营和护理需求，专心于更好地照护患者。

保护患者信息免受日益狡猾的网络犯罪分子和不断扩大的基于云的攻击面的侵害，这已经是企业的当务之急。以患者为中心的企业和政府实体均对 Akamai 的边缘平台寄予了高度信任，这不仅使他们的数字体验更加贴近患者需求，同时也确保了远离威胁。

信赖 Akamai，让我们携手将网络安全保护从负担转变为竞争优势。

请联系我们了解详细信息，或者致电 +1-877-425-2624。

Akamai 支持并保护网络生活。全球众多颇具创新力的公司纷纷选择 Akamai 来提供安全的数字化体验，为数十亿人每天的生活、工作和娱乐提供助力。凭借全球企业信赖的大型边缘平台，Akamai 可使您提供的应用程序、代码和体验更贴近用户，并使威胁远离用户。如需了解有关 Akamai 的安全、内容交付以及边缘计算产品和服务的详细信息，请访问 www.akamai.com 或 blogs.akamai.com，或者扫描下方二维码，关注我们的微信公众号。发布时间：2022 年 2 月。

扫码关注 · 获取最新CDN前沿资讯