ISO标准认证助力网络安全

编者按

本文原载于《质量世界》(Quality World) 2018年第10期。作者尼科尔•科比 (Nicole Kobie) 是一名长期关注技术、运输和科学领域的自由撰稿人。计算机和网络是现在所有组织须臾不可或缺的基本工具，如果遭到大规模恶意软件攻击，有可能对组织造成严重破坏。本文以2017年WannaCry勒索软件造成的巨大破坏为例，介绍了面对脆弱网络系统带来的严重威胁，如何通过ISO 27001等标准的认证筑造安全网络，以及质量专业人士在其中的作用。

2017年5月一个星期五的下午，英国的媒体滚动出现新闻报道：英国各地的医院和医生办公室都开始停工，因为他们所依赖的计算机和网络遭到大规模恶意软件攻击。医生们不知道发生了什么，不断给同事发短信和打电话。这次攻击带来的混乱和相互矛盾的报道在推特 (Twitter) 上迅速传播。

许多医生办公室的网络出现断线，在很多情况下甚至没有任何警告，这使得医生无法查看他们的文档、预约日记和记录。当天下午，数十家英国国家医疗服务体系 (NHS) 的医院网络陆续关闭，导致手术推迟、预约取消和患者转院。

下午4点，NHS宣布了这一重大事件，启动了持续整整一星期的官方三阶段响应计划。英国首相特蕾莎•梅首次召开应对网络攻击的内阁办公室简报A室 (COBRA) 会议。COBRA会议的参会人员包括高层政府官员和公共机构领导人，目的是解决诸如恐怖袭击等严重性、突发性问题。

但人们很快发现，导致NHS关闭的恶意软件并非针对卫生服务领域和英国。从中国到法国，很多全球公司都受到了影响。西班牙电信业巨头西班牙电话公司遭遇重创，欧洲所有的雷诺工厂关闭。联邦快递后来透露，WannaCry勒索软件攻击使其欧洲业务损失超过3亿英镑。根据欧洲刑警组织的报告，总共150个国家的20万台计算机受到感染。毕马威网络安全专家尼尔•克拉克说："NHS并不是唯一受影响的大型组织，他们并没有被针对，只是他们的网络很脆弱罢了。"

医疗服务体系的网络之所以被攻陷，是因为WannaCry利用了一种名为"永恒之蓝 (Eternal Blue)"的漏洞利用工具。该工具由美国国家安全局开发，随后遭到窃取，利用Windows操作系统中的已知漏洞感染设备。虽然微软发布了一个紧急补丁来阻止其代码中的漏洞被黑客利用，但并非所有的NHS医院都安装了该补丁。一份报告显示，236家医院中有三分之一受到了WannaCry的牵连。这些受影响的医院都没有安装过补丁，尽管他们自己的数字安全部门建议他们采取预防措施。

因为没有听取微软和NHS 数字安全部门的建议，英国的医疗服务受到WannaCry的重创。除了受影响的医院外，8%的医生办公室也被迫离线。WannaCry通过内部网络传播，将加密文件作为勒索软

件攻击的对象，黑客会锁定文件，声称将在收到费用后解锁。在这次事件中，他们开出的价码是等值300美元的比特币。英国电信的网络和物理安全总经理史蒂夫•本顿解释说："病毒暴发后基本上只能通过关闭基于Windows的计算机来应对——实际上就是拔掉电源插头。"这意味着数十家医院和数百家医生办公室在未来几天内无法照护患者。

在一名英国安全研究人员发现所谓的"死亡开关"后，当天晚上WannaCry的传播停止了，但病毒的影响在周末持续发酵。安全人员向受病毒攻击的人发送信件，通知他们立即安装补丁，并对所有受感染机构的计算机系统进行更新。一些设备需要安全人员进行现场处理，其他的则需要更换硬件或重新组装。对于本就繁忙的医疗服务系统来说，这是一个忙碌的一周。

针对WannaCry的响应

作为一家主要的国际电信和安全公司，如果英国电信也进入WannaCry受害者名单，那将是一件令人尴尬的事情，但该公司通过对其计算机进行系统最新和安装补丁的方式避免了此次攻击。本顿解释道："我们已经完成了互联网相关设备的工作，因此WannaCry无法进入我们的设备。在我们的全球运营体系中，英国电信的任何分支机构都没有暴发WannaCry。"

尽管英国电信的网络是安全的，但为了做好准备以防止恶意软件侵入自己的客户，该公司仍然做出了完整的意外事件管理响应，这是在面临安全危机时实施的一整套流程，包括监控自己的系统、修补所有软件漏洞以及组织对其他人的援助等。本顿说："事实上，我们也在帮助NHS应对。"因为NHS之前与英国电信签订了IT和数字服务合同。在英国电信内部，安全团队对正在发生的事情进行了评估，确定了哪些威胁和弱点需要最高的关注，以便考虑其响应的优先顺序。本顿解释道："这次我们将面向互联网的设备（服务器和终端）作为关键优先事项，因为它们被攻击的风险最大。"

这些措施包括制定一个被英国电信称之为"剧本"协议，概述了如何运行紧急补丁，以确保在所有系统中都安装了关键的Windows补丁。其次，该公司禁用了一个名为"服务器信息区块"的Windows系统，该系统允许恶意软件的传播。然后，该公司增加了对网络钓鱼行为的防护，该行为通过电子邮件发送恶意链接或附件以感染计算机，这被视为WannaCry传播的另一条可能路径。

对于任何安全部门来说，这都意味着大量的工作，而且还是一个没有被WannaCry感染的公司。本顿说，受Wannacry攻击的人不得不迅速安装他们漏装的补丁，然后识别、隔离和清理受感染的机器。他说："实际上，这是通过网络完成的网络工作，因此具有病毒进一步暴发的高风险。对于被勒索软件加密的文件，可选择方案是支付赎金，希望文件能够解密，或者从备份中恢复文件和系统，并回滚丢失的进程。"

WannaCry事件的经验教训

所有组织都可以从这次WannaCry事件中学到大量的经验教训，无论它们是否受到了病毒感染。首先是最重要的：要始终为计算机安装最新的系统补丁。WannaCry正是利用微软在两个月前修补过的软件漏洞进行了传播。很多公司经常推迟安装补丁，因为软件的任何变化都可能导致工作中断。但这个补丁比其他补丁更重要，因为这次微软还发布了一个针对

过时的Windows XP系统的补丁版本，尽管微软已不再更新Windows XP。网络安全技术提供商比特梵德的全球网络安全分析师伯格丹•博泰扎图说："当微软针对不再受支持的Windows XP发布补丁时，这是一个警告信号，表明这件事情很严重，需要及时解决。"

除了补丁管理之外，本顿认为受害者这次以很大的代价知道了备份系统和准备恢复数据流程的重要性，因为一些组织的文件因勒索软件而丢失。定期备份和数据恢复准备不再被视为一件麻烦的工作。"这也凸显了了解自己与谁连接的重要性。"本顿补充道，"WannaCry事件揭示出，可能的感染渠道来自我们自己的网络，而不仅仅是公共互联网。"

作为一个公共组织，NHS对事件的响应将面临内部和外部审查。该机构几个月后在报告中详细说明了它正在实施的变革，以避免再次成为受害者，以及在再次发生时能有效应对。WannaCry袭击事件发生后还有一些其他变化，如NHS向其员工发布了一份网络手册，说明了未来受到网络攻击时应该做些什么，确定了负责人、要遵循的协议以及从哪里更新信息等。该组织的数据安全帮助热线现在每天24小时开放，而不是在下午5点关闭。它对数百家医院的安全设置进行了评估和审核，指出了哪些地方需要更多投资，以升级防火墙、提高网络弹性和进行自动化补丁管理等。展望未来，NHS正在研究如何更好地利用其IT投资，改善未来的安全性。

但并非所有公司都吸取了教训。在WannaCry事件一年后，供应苹果iPhone组件的台湾芯片制造商台积电的工厂停运，因为其未修补的Windows系统被恶意软件感染。虽然该公司的生产机器具有"气隙系统"，当计算机没有直接连接到互联网时，恶意软件对其难以感染，但插入该系统的新工具在安装之前未进行病毒检查，导致了病毒侵入。

ISO标准如何提供帮助

对于网络安全，没有万无一失的方法，但一些标准和框架对其有所帮助。

一个是ISO 27001，该认证标准考察你如何管理你的安全风险或者信息安全管理系统（ISMS）。该标准并不会告诉公司应该使用哪种特定技术，尽管它确实包括了需要考虑的100多种安全控制。"它提升了组织内信息安全的重要性，并确保其对业务战略和目标的支持。"英国标准协会（BSI）信息安全全球产品负责人约翰•迪马利亚说，"它事实上是一种业务管理工具，可以帮助企业了解自己拥有哪些信息和信息放在哪里。最重要的是，如何在整个从创建到销毁的生命周期内对信息进行保护。"

因为ISO 27001是全球认证，所以它必然有一定的模糊性。咨询公司IT Governance的执行董事史蒂夫•沃特金斯解释说："它必须具有足够的灵活性，能够适应并适用于每个组织，无论它们对安全问题关注是很高或者略低。"

如果你的组织已经拥有了完善的安全策略，ISO 27001可能不需要你进行任何技术更改。除了提升保护之外，它还有其它好处。首先，它向客户和用户表明你正在认真对待安全问题。毕马威的克拉克说："在某些行业，认证可以让你拥有讨论商机的资格。这是对该组织正在考虑并采取基于风险的方法的事实的良好认可。"IT Governance对其客户进行的一项民意调查显示，80%的客户表示认证激发了对其业务的信任，75%的客户认为可以降低业务风险。

认证还可以帮助组织证明自己会在攻击后试图保护数据。迪马利亚说："它包括了'尽职调查'和'防护标准'的内容。在法律争端中，它们是组织为保护信息所采取的防护水平受到质疑时所涉及的议题。"

此外，沃特金斯指出，公司设立的符合ISO 27001标准的管理系统可用于满足其他法规，如欧盟的《通用数据保护条例》（GDPR）。事实上，IT Governance对其客户的调查显示，68%的人计划使用符合ISO 27001标准的信息安全管理体系来保证对GDPR的合规性，GDPR是2018年5月在欧盟生效的一整套数据保护规则。

在没有外界帮助的情况下，组织也可以满足ISO 27001标准，并且有大量的书籍和课程可以帮助组织完成整个过程。沃特金斯表示，对于那些来咨询公司寻求帮助的组织来说，达到这个标准需要花费2～18个月的时间。IT Governance的研究显示，约60%的组织需要6

个月左右。ISO 27001通常适用于大型组织，但沃特金斯表示它对小型企业也很有用，他曾经帮助一个“单人公司”获得认证，因此不存在业务规模太小的问题。

同时，还有许多其他认证或计划需要考虑。如果你的公司在英国运营，则需要考虑英国政府的网络要件（Cyber Essentials）计划，或美国商务部的国家标准与技术研究院（NIST）网络安全框架。后者为如何避免攻击和进行响应提供指导，特别是那些运行关键基础设施的组织。欧洲大陆正计划为产品、服务和流程建立欧盟通用的网络安全认证框架。澳大利亚政府有一个信息安全管理框架，日本有一个信息安全管理体系合格评定计划。其他的信息安全管理体系包括来自信息系统审计和控制协会（ISACA）的信息技术基础设施库（ITIL），以及信息和相关技术的控制目标（COBIT）。特定行业也有自己的标准。金融公司可能需要满足支付卡行业数据安全标准，而电信公司需要考虑电信商品保证服务（CAST），该标准对安全控制有详细的说明。

如果你已经满足了ISO 27001的要求，还有其他ISO标准需要考虑。“如果数据的机密性、完整性或可获得性受到威胁，可以考虑业务连续性标准ISO 22301，以建立‘信息连续性’。”迪马利亚解释道，“可以添加特定行业标准，作为云服务提供商的范围扩展，例如ISO/IEC 27018（隐私）、ISO/IEC 27017（云的附加控制），以及CSA STAR （云安全联盟的安全、信任和保证登记）。”

但是，如果你正在考虑任何类型的信息安全管理体系认证，特别是ISO 27001，沃特金斯警告说，不要认为这足以保护你的公司免受安全事故的影响——这些标准是关于人员和流程的，而不是关于IT的。他说：“很多人认为信息安全管理是关于IT的，但它不是。它不仅仅是对信息的保密或锁定，更是在认识到可获得性的重要性的同时取得平衡……ISO 27001重点关注机密性、完整性和可获得性，并保护这些事情。”

贴心提示

即使通过了ISO 27001认证，公司仍需要考虑技术防御问题。首先要认识到，完美的安全是不可能的，因为攻击总是在变化，因此公司的防御也应当相应变化。“安全对任何组织都至关重要——股东、官方机构、媒体和客户都希望有适当的安全措施。”本顿说，“有些攻击可能会成功，没有百分之百的安全。ISO 27001让你了解威胁和风险，以及根据你公司的风险偏好进行相应的响应。”

也就是说，要保证一些关键基础工作的正确性：及时进行系统修补并注意漏洞；确保员工接受过良好的培训，以避免人为的安全失误，例如因网络钓鱼攻击而中招；如果不幸被攻击，需要具有经过测试的业务连续性计划。毕马威的克拉克说：“数据证明，80%是正确做好基础工作；20%是你与谁一起工作，以及你的哪些工作可能对他人有价值，并适当地调整安全措施。”

黑客们一直将公司当作攻击目标，对艾可飞（Equifax）、滔客（TalkTalk）和雅虎等公司的重大攻击已经影响了数百万人。然而，英国数据监管机构信息专员办公室的数据显示，80%的数据泄露并不是黑客造成的，而是人为错误或流程错误造成的。

为了保障数据安全，需要在公司的各个层面考虑安全性和数据管理——尤其是在高级管理层。“这在很大程度上关乎领导力和决策、人员和流程，而不是技术。”克拉克说，“如果你没有考虑组织内最高级别的安全性，你就不会正确地做到这一点。”

本顿说，这就是高质量专业人士的用武之地。他说：“质量专业人士可以在以下领域发挥作用：确保并支持在流程、系统、应用程序中设计和构建安全性，这提供了力量和可预测性的基础，以建立和维护安全状态，并利用标准、措施和审计等确认实际操作中控制的有效性。”

换句话说，维持公司安全需要打好基础，以避免遭受像Wannacry那样、其实很容易预防的病毒攻击，同时也要做好培训、计划和协议，以应对无法避免的安全事件。

克拉克说：“安全问题的一个关键组成部分，是当它出错时该怎么做。如果我们用噩梦般的场景来锻炼自己，那么无论发生什么事情，应对起来都可能会比较简单一些。”

（熊英姿 编译）