网络空间安全丛书

零信任计划

[美] 乔治·芬尼(George Finney) 著

贾玉彬 甄明达 译

清華大學出版社

北 京

北京市版权局著作权合同登记号　图字：01-2023-5727

图书在版编目(CIP)数据

零信任计划 / (美) 乔治 • 芬尼 (George Finney)著；贾玉彬，甄明达译. —北京：清华大学出版社，2024.1
(网络空间安全丛书)
书名原文：Project Zero Trust: A Story about a Strategy for Aligning Security and the Business
ISBN 978-7-302-64871-0

I. ①零… II. ①乔… ②贾… ③甄… III. ①计算机网络—网络安全 IV. ①TP393.08

中国国家版本馆CIP数据核字(2023)第215137号

责任编辑：王　军
装帧设计：孔祥峰
责任校对：成凤进
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：https://www.tup.com.cn，https://www.wqxuetang.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-83470000　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：艺通印刷（天津）有限公司
经　　销：全国新华书店
开　　本：148mm×210mm　　**印　　张**：6.125　　**字　　数**：201 千字
版　　次：2024 年 1 月第 1 版　　**印　　次**：2024 年 1 月第 1 次印刷
定　　价：59.80 元

产品编号：100603-01

译者序

当清华大学出版社的王军老师问我有没有兴趣翻译一本关于零信任的书时，我的第一反应是零信任有点超出了我的技术能力范围。但当王老师告诉我这是一本“特别的”关于零信任方面的书籍时，引起了我的好奇心。虽然零信任框架已经诞生相当长一段时间了，但就我个人的认知和经历，我认为目前大部分网络从业人员并没有真正理解零信任框架，如果能有一本书以“特别的”方式讲清楚零信任就太好了。

于是我先粗略地阅读了一遍王老师给我的电子版，发现这确实是一本“特别的”关于网络安全方面的书籍，一本关于零信任的小说。没错，是一本小说。

零信任的概念诞生于 2010 年，由约翰 • 金德瓦格提出。之后关于零信任重要的时刻发生在 2021 年，当时美国的乔 • 拜登总统发布了关于改善联邦政府网络安全的行政命令，该命令要求所有联邦机构朝着采用零信任架构的方向迈进。零信任达到了它的巅峰状态，在全世界的网络安全领域都大受欢迎。

许多组织机构在网络安全方面都做得不好——不是因为它们什么都不做，而是因为它们没有一致的网络安全保护策略。零信任是一种保护组织机构核心资产的策略。 该策略的重点是通过消除信任来防止攻击行为，因为信任是计算机和网络方面最大的盲点之一。

这部关于零信任的小说的主角一直从事管理 IT 基础设施方面的工作，在入职新公司任职 IT 基础架构总监的第一天经历了一场网络攻击事件，很快就被任命为公司零信任计划的负责人，需要带领临时组建的零信任团队用 6 个月的时间在公司内部实施零信任计划，帮助公司将网络安全事件造成的恶性影响消除，并帮助公司积极推动新产品的发布。因为公司将在 6 个月后推出一款全新的产品，它将改变世界看待健身、工作与生活平衡等的方式。 公司承担不起可能无法率先进入市场带来的业务损失。男主角带领临时团队使用约翰 • 金德瓦格的零信任设计方法成功地在 6 个月内实施了零信任计划，化解了网络安全攻击造

成的影响，保障了新产品的成功按期发布，实现了网络安全能够和业务很好地保持一致。

本书具有很好的故事性，时间线非常清晰，并且很好地结合了组织网络安全和业务的真实情况，通过对网络安全事件的处置很好地诠释了什么是零信任以及组织机构应该如何实施零信任计划。非常适合网络安全从业人员快速理解和掌握零信任的概念，并可以作为组织实施零信任计划的详细指南。

在此我想感谢王军老师给了我翻译这本优秀书籍的机会。感谢上海碳泽信息科技有限公司全体同仁对我的支持和帮助。

最后，引用书中的一句话作为结束语：流程先于技术，每一步都很重要。

贾玉彬

2023 年 8 月 31 日 于北京

作 者 简 介

乔治 • 芬尼(George Finney)是一名首席信息安全官(CISO)，他认为人是解决网络安全挑战的关键。乔治是多部网络安全畅销书籍的作者，包括获奖书籍 *Well Aware：Master the Nine Cybersecurity Habits to Protect Your Future*(Greenleaf Book Group Press，2020)。他在 2021 年被 CISOs Connect 评为全球 100 名最杰出的首席信息安全官之一。他在网络安全领域工作超过 20 年，帮助初创企业、跨国电信运营商和非营利组织提高了其安全水平。乔治也是一名律师，但请不要因此对他有所偏见。

致　谢

如果没有这些愿意花时间与我分享经验的人的帮助，我是无法写出这本书的。首先，我要感谢我的朋友和导师约翰•金德瓦格，在我带领组织走过零信任之旅的职业生涯中，以及在我编写这个故事的过程中，他一直给予我帮助。

我还要感谢我的出版商吉姆•米纳特尔，他不仅相信这个计划，而且相信我有能力实现它。同时，我要感谢 Wiley & Sons 出版社，特别是约翰•斯利瓦、皮特•高恩和梅丽莎•伯洛克，他们的宝贵贡献使这本书达到了现在的水平。

网络安全是一项“团队运动”。如果我们不互相分享经验，就无法完成我们的工作。当我拿起手机寻求帮助时，社区团结起来回应了我的呼声。我想亲自感谢扎克•文杜斯卡在整本书的创作过程中一直与我并肩作战。我还要感谢亚当•肖斯塔克提供的见解和帮助，使得所有细节得以实现。

我还要感谢我的朋友和同事们，他们是杰森•弗鲁吉、海伦•巴顿、夏娃•马勒、拉斯•柯比、罗伯•拉马格纳-赖特、埃克斯德斯•阿尔马苏德、蔡斯•坎宁安、乔什•丹尼尔森、乔丹•毛列洛、马尔科姆•哈金斯和史蒂夫•金。我觉得自己非常幸运能认识他们。

最后，我要感谢我的妻子阿曼达和女儿斯塔瑞，在我追求成为一名作家的梦想时，她们给予了我支持、灵感和理解。

——乔治•芬尼

序　言

当我的朋友乔治•芬尼告诉我他要写一本关于零信任的小说时，我最初的反应是：“为什么？”写一本让任何人都想读的关于零信任的小说，这样的想法有点匪夷所思。当然，这是一件令人高兴的事情，但仍然很奇怪。当我首次提出零信任的概念时，人们认为我疯了。不只是像我们这样的 IT 和网络安全领域的人那样古怪的疯狂，而是真正的疯狂。

多年来，我一直努力说服人们保持开放的思维，考虑构建零信任环境。有人想要写一本以我创造的理念为核心的小说，这个想法让我震惊不已。所以，乔治最终坐在我家客厅的沙发上，听我讲述零信任的由来。

要理解零信任，首先必须了解网络安全的起源。“网络安全”是一个相对较新的术语。在此之前，我们称之为 “信息安全”，这是一个更好的名称(什么是网络？为什么需要安全？)。多年来，网络首先在大学和极个别的“前卫”公司中被使用起来，但没有威胁存在——因此，也没有内置的安全性。实际上，我们都熟知和喜爱的 TCP/IP v4 直到 1983 年才被开发出来。因此，有许多研究人员和远见者都对如何利用“互联网”并从中获利垂涎三尺。甚至没有人想到有人可能想要攻击这些新生的网络系统。

然后，在 1983 年，一位名叫罗伯特•H. 莫里斯 (Robert H. Morris) 的美国国家安全局计算机科学家和密码学家在国会作证，警告了网络威胁的新现象——“计算机病毒”。1988 年，他的儿子罗伯特•塔潘•莫里斯(Robert Tappan Morris)创造了可以说是第一个计算机蠕虫，即同名的莫里斯蠕虫，这是计算机时代最伟大的讽刺之一。莫里斯蠕虫感染了 2 000～6 000 台计算机，这在当时的背景下是一个巨大的数字，因为当时整个互联网只连接了大约 6 万台计算机。根据不同的说法，莫里斯蠕虫造成了 10 万～1 000 万美元的损失。突然之间，网络安全变得备受关注。

遗憾的是，当时没有人知道如何保护网络，因为没有人考虑到网络威胁。因此，一些有远见和雄心的人(我不是其中之一)创造了名为“防火墙”和“杀毒软件”的产品，将它们销售给各种公司和组织，并在此过程中变得非常富有。

快进到世纪之交，我在达拉斯-沃斯堡地区以安装防火墙谋生。我部署的主要防火墙是思科的 PIX 防火墙。PIX 防火墙无处不在，推动了很多信息安全的思考。其核心组件被称为自适应安全算法(ASA)。当然，它并没有什么自适应性，而且提供的安全性很有限，但是思科能够非常成功地推销它。

安装 PIX 防火墙的第一步是设置接口的“信任”级别。默认情况下，连接到互联网的外部接口是“不受信任”的，信任级别为 0；而连接到客户网络内部的接口是“受信任”的，信任级别为 100。通常还会使用几个接口作为 DMZ(非军事区)使用，这是从越南战争中借用的一个术语，听起来很酷，专门用于部署特定的资产，如 Web 或电子邮件服务器。这些接口会被分配一个任意的信任级别，介于 1 到 99 之间。因此，“信任”级别决定了数据包如何穿过 PIX 防火墙。思科在其产品文档中是这样写的：

“自适应安全算法遵循以下规则：允许任何从内部网络发起的 TCP 连接”。

由于“信任”模型的流量在默认情况下可以从更高的“信任”级别(内部)流向更低的“信任”级别(DMZ 之外)而不需要特定规则。这非常危险。一旦攻击者进入你的网络，没有任何策略可以阻止他们建立命令和控制通道或渗出数据。这是技术上的一个重大缺陷，但可悲的是，每个人似乎都对此无动于衷。当我添加出站规则时，客户和同事都会感到不满。“这不是应该的配置方式！”我离开了许多客户现场，因为对我来说，客户未来可能会遭遇糟糕的情况，这是不言自明的。

因此，我开始讨厌“信任”。不是人与人之间的信任，而是数字领域中的“信任”。于是我开始研究信任的概念，思考它，并提出问题，比如“为什么数字系统中需要‘信任’？”很明显，这个“信任模型”是有缺陷的，也是许多数据泄露的直接原因。

我发现与“信任模型”相关的还有其他问题。第一个问题是将技术拟人化。为了让复杂的数字系统更易于理解，我们试图通过语言将其人性化。例如，我

们会说“乔治在网上”。但我很确定我的朋友乔治这辈子都没有上过网络。他从未被缩小成亚原子粒子并被发送到某个目的地，比如邮件服务器或公共互联网。这几乎从未在电影中发生：比如《割草人》或《虚拟战士》，甚至在《黑客帝国》中，角色也必须插入接口。但我该如何讲述这个故事呢？

现在，这就是命运介入的地方。我接到 Forrester(福雷斯特)研究公司的电话，问我是否想成为一名分析师。当然想！ 虽然我真的不知道分析师是什么。但 Forrester 是一种恩赐，它给了我提问的自由。在我们最初的分析师培训班上，我们被告知我们的使命是“思考宏观问题”。没错，就像乔治所说的那样。

我开始探究的第一个重要想法是，将“信任”注入数字系统是一个愚蠢的想法。我现在可以自由地探索那个有争议的说法。没有供应商或同事来阻止我的思考。自由——这是 Forrester 赋予我的伟大礼物。

加入 Forrester 仅几个月后，一个供应商联系我并问道：“您正在研究的最疯狂的想法是什么？”我告诉他我想从数字系统中消除信任的概念。他完全认同这个想法。他一直在寻找一些激进的想法来证明他想安排的高尔夫旅行是合理的。

在 2008 年秋季，我在蒙特利尔、费城、波士顿、纽约和亚特兰大的 5 个苏格兰风格的高尔夫球场举办了一系列的活动。在每个球场，我都给与会者做了一个关于“零信任“的新生概念的演讲。之后，我们和与会者一起打一轮高尔夫球。有许多问题和精彩的交流。另外需要注意的是：我只带了我的高尔夫鞋和一个装满了高尔夫球的大袋子，因为我在那些苏格兰式的球场上丢了很多球。

这是最早的 5 次零信任演讲，留下了许多回忆。因此，零信任诞生于蒙特利尔的一家乡村俱乐部。我不确定这项研究会走向何方，但我知道在第一次演讲结束后我发现了一些重要的东西。

于是我开始了为期两年的初级研究之旅，我与各种各样的人进行交流，包括我敬佩的 CISO、工程师和网络安全专家。我寻求反馈，“请帮我找到这个想法的漏洞”。最终唯一的负面反馈是“这不是我们一直以来的做法”。于是我开始在小型演讲和网络研讨会上测试这个信息。有一批核心人群理解了这个概念，他们成为了最初的倡导者。

2010 年 9 月，我发表了最初的“零信任报告：‘不再有软肋：信息安全零信任模型介绍’”。人们阅读报告，来电询问，邀请我发表演讲和设计基于零信任模型的网络。

对许多人来说，零信任是一个新的理念，但我在过去 14 年里一直专注于此。零信任带我走遍了亚洲、欧洲和中东。它让我结识了世界上许多伟大的领袖和思想家。我曾与首席执行官、董事会成员、国会议员、将军、海军上将以及无数从事 IT 和网络安全的人士会面，他们正在与我们的数字对手进行艰苦卓绝的斗争。对于一个来自内布拉斯加州农村的孩子来说，唯一的目标就是不用在清晨 5 点起床喂牛和灌溉玉米地，这样的成就还不错。

看到这么多人发表演讲、撰写论文甚至出版关于零信任的书籍，这让我感到非常满足。我曾为写关于零信任的硕士论文或博士论文的学生提供过指导。我也尝试过自己写一本书，但同时进行工作和写作确实很困难。

最重要的时刻发生在 2021 年，当时乔 • 拜登总统发布了关于改善联邦政府网络安全的行政命令，该命令要求所有联邦机构朝着采用零信任架构的方向迈进。如果十年前你告诉我这会发生，我会告诉你回到你的 DeLorean 车里并将它加速到 88 英里/小时，因为那永远不可能发生。但它确实发生了，而且它改变了一切。主要是颠倒了激励结构。过去，只有组织内部的激进分子才是零信任的倡导者。现在，由于拜登总统的支持，采用零信任是可以的。他改变了现状。

但我职业生涯中最令人满意的时刻是当一个年轻人在飞机上看到我并走到我的座位时。他递给我他的名片，上面印着“零信任架构师”的职位。他伸出手说：“谢谢您，因为您，我有了工作”。

所以，乔治，谢谢你成为我坚定的朋友和零信任倡导者。感谢你撰写这本书，感谢你将所有疯狂的创造力应用于这个疯狂的行业。网络安全需要更多的乔治 • 芬尼。

——ON2IT 网络安全战略高级副总裁　约翰 • 金德瓦格

前　言

在网络安全方面，我们可以用来保护自己的最有效手段是预防。而最有效的预防策略是零信任。要想在任何事业中取得成功，你都需要策略。许多组织在网络安全方面都难以取得成功——不是因为它们什么都不做，而是因为它们没有一致的数据保护策略。零信任是一种保护组织最重要资产的策略。该策略的重点是通过消除在计算机和网络方面最大的盲点之一 —— 信任，来防止攻击行为。

零信任是企业独特目标与保护业务所需的特定策略之间的桥梁。Okta 在 2020 年的一份报告中指出，北美 60%的组织目前正在开展零信任计划，拜登总统已向联邦机构发布行政命令，要求在政府中实施零信任。

《零信任计划》通过引导读者完成实施零信任的每个步骤来改变被攻击企业的安全性。这本书讲述了迪伦的故事，当该组织发现自己成为勒索软件的受害者时，他甚至还没有开始担任新工作(基础设施总监)一职。当 CIO 处理攻击响应和调查时，迪伦负责使用约翰 • 金德瓦格的零信任设计方法改造公司。读者将能够把这些经验教训带回他们自己的组织，并拥有可操作的示例，可以将这些示例应用于组织中的特定角色和场景。

读者将学习：

- 约翰 • 金德瓦格的五步法
- 实施零信任的方法
- 4 个零信任设计原则
- 如何限制突破口的影响范围
- 如何使安全与业务保持一致
- 实施零信任时的常见误区和陷阱
- 在云环境中实施零信任

由于零信任侧重于预防策略，因此除了提高安全性之外，读者还会发现提高效率和降低成本的机会。

对于那些有志成为专业技术人士以及经验丰富的 IT 领导、网络工程师、系统管理员和项目经理来说，本书对于在他们的组织中实施零信任计划至关重要。本书展示了如何使用易于理解的示例将零信任集成到任何组织中，弥合技术参考指南、供应商营销和组织战略之间的差距。

目　录

第1章

零信任案例

房间里仍然很暗，但是迪伦已经睡不着了。他看了看表，才凌晨 4 点 45 分，没有再尝试入睡的必要，但现在起床又太早。今天迪伦要开始一份新工作，如果一切顺利的话，这也许是他梦想的工作。尽管如此，他可能还是有点焦虑。但他也真正感到兴奋，这是很长一段时间以来或者说可能是从未有过的感觉。他闭上眼睛，希望能再睡几分钟。

迪伦睁开眼睛，又看了看表，现在是 4 点 46 分了。他决定不再等闹钟响，而是现在就起床。床头柜前他的居家拖鞋和跑步鞋并排放着。他穿上跑步鞋，打开台灯，走到房间对面的跑步机旁。他用右手抓住右脚踝，拉伸大腿四头肌，再拉伸另一条腿，然后跳上跑步机。

他听到跑步机通过人脸识别后加载他的个人资料时发出的低柔声音。他最喜欢的 3 个锻炼项目在弧形 LED 屏幕上弹出。他点击底部的第四个图标，可以看到来自世界各地的 9 个跑步者的直播。他选择了在哥斯达黎加海滩上的那个，并开始跑步。他能听到来自几位他曾经一起跑步直播的观众的欢呼声，他们也看到他加入了直播。

但接下来发生了一件有趣的事情：直播卡住了。然后跑步机开始减速到安全速度，最后停了下来。March Fitness 的标志出现在屏幕上，就像几个月前他的 Wi-Fi 出问题时一样。迪伦从跑步机上下来，检查一下手机，但 Wi-Fi 似乎工作正常。

他决定冲个澡，开始为工作做准备。穿好衣服后，他开始早上的例行公事，即煮咖啡和查看电子邮件是否有任何新闻提醒。自从他接受这份新工作后，他

创建了一个提醒，即每当在有关 March Fitness 的新闻报道中提到“IT”或“中断”时，都会向他发送电子邮件。令他恐惧的是，他的收件箱里塞满了电子邮件。他的跑步机并不是唯一有问题的。由于停电，整个公司都停工了。更糟糕的是，一名网络安全记者在推特(Twitter)上声称该公司刚刚经历了一场大规模的网络攻击。

迪伦站在那里，愣住了。这怎么可能发生？在他新工作的第一天？这时闹钟突然响了，迪伦过了好一会儿才意识到那是他的闹钟。终于到了他该醒的时间了。

迪伦跑上 March Fitness 公司总部大楼的台阶时，空气中还弥漫着一丝寒意。楼梯中央有一双巨大的金属丝网跑鞋，只有鞋头连在下面的大理石板上。他穿过旋转门，更多的铁丝网鞋将走廊一分为二，每一只的跑姿都略有不同，就好像有个巨人刚刚跑过，每跑一步都掉落了一只新鞋。March Fitness 公司总部的大堂贯穿整栋大楼，将公司总部分为北侧和南侧。

大楼的北侧是公司所有高管以及营销、人力资源、财务和销售部门的办公室。大楼的南侧是信息技术以及研发人员办公室所在的地方。与他面试时不同的是，保安处没有人，大楼两边的安全门都敞开着。迪伦看到一大群他认为是实习生的人在南北两侧的办公室之间快速地来回穿梭，手里都拿着皱巴巴的文件。这是一个坏兆头，这意味着不仅电子邮件出现故障，而且即时消息和电话系统也出现了故障。或者他们可能已经关闭了网络以防止攻击进一步传播？

迪伦不知道该去哪里报到，就往南侧走去，因为那是他之前面试的地方。他自然而然地小跑着跟上来回穿梭的人们，虽然他的身材健壮，一米八几的身高也让步幅比一般人要大，但人们却像他站在原地不动一样在他身边飞奔。

他经过一排电梯，走进一个通常能容纳 100 名员工的小隔间。所有的显示器都是黑的，每个显示器上都贴着一张纸条，上面写着“请勿开机”。

他跟着气喘吁吁的人们来到一间会议室，在那里他终于见到了一个他认识的人。首席信息官努尔 • 帕特尔(Noor Patel)博士坐在房间中央一张会议桌的首位。努尔身穿黑色西装和白色衬衫，系着她标志性的黑色丝绸领带。坐在桌子对面的是 March Fitness 的创始人兼首席执行官奥莉维亚 • 雷诺兹(Olivia Reynolds)。坐在桌旁的其他人都穿着西装，除了雷诺兹，她穿着 March Fitness

自有品牌的跑步服。

“迪伦？”一个女人在他耳边低语。她悄无声息地穿过聚集在周围的只能站着的人群，吓了迪伦一跳。她一头黑发，几乎和迪伦一样高，身上散发着丁香花的香味。她拿着一个装满文件的活页夹，上面写着业务连续性计划。

“我是伊莎贝尔，我负责项目管理办公室。努尔今天早上让我留意你。见鬼的第一天。”她转身站在迪伦旁边，看着房间中央正在进行的讨论。

她把员工卡递给他，可伸缩的卡夹已经装好了。“你很幸运，我们上周打印了这个。现在整个读卡器系统都宕机了，就像其他系统一样。周日晚上的某个时候，我们开始在网络上看到一些不寻常的活动，”伊莎贝尔对迪伦耳语道。“到今天早上，事情已经失控了。”

他把员工卡别在腰带上，“我猜你们把网络关掉了，以防万一。他们知道是什么原因吗？”

“你猜对了，迪伦。实际上，许多计算机似乎已经感染了勒索软件。我们仍在调查原因，但公司在网络中断的每一分钟都在亏钱，所以他们现在关注的是让我们的业务重新上线的最快方法。”

奥莉维亚•雷诺兹轻声开口，所有人立即停止说话，转头看向她。“我们怎么知道这笔赎金不仅仅是某种骗局？”她问，“即使我们付钱给他们，我们怎么知道他们真的会解锁我们的计算机？”

“女士，”努尔身边的一名穿西装的人说道。与努尔不同，他的西装皱巴巴的，看起来不太合身。“我们经常遇到这样的问题，现实中有不少勒索软件攻击行为存在。我们可以判断出来，因为他们会用同一个比特币钱包向所有受害者进行勒索。在这种情况下，可以看到许多受害者试图付款的交易记录。”

“那是我们的安全顾问，彼得•刘，”伊莎贝尔悄悄地向迪伦解释道。

“那我们呢？”奥莉维亚问道。

“我们的情况是，”努尔在顾问回答之前回应道，“比特币钱包是全新的，我们认为只有一笔交易，我们相信那只是网络犯罪分子测试账户的记录。”

“这怎么解释？”一名穿着蓝色细条纹西装的白发男子问道。

“那是我们的法律总顾问科菲•阿巴拉(Kofi Abara)，”伊莎贝尔澄清道，“他是我见过的最聪明的人之一。而且，他每月都会组织一次扑克锦标赛。几年前，

他还参加过世界扑克锦标赛。千万不要和他赌。”

“这是一个会计问题，”彼得解释道，“网络犯罪分子需要知道哪些受害者已经付款，哪些没有。做到这一点的唯一方法是为每个受害者准备一个不同的比特币钱包。看到比特币钱包是空的，说明这个网络犯罪分子是认真的。”

“我们的下一步行动是什么？”奥莉维亚问道。

努尔站起来并向房间里的所有人讲话：“如果有其他办法的话，我们不会付款给这个网络犯罪分子。我们有备份，我们的团队将加班工作，从头开始恢复计算机系统。我们已经推迟升级防病毒软件，以采用更现代的 EDR 解决方案，因此我们将在恢复设备的同时进行这些升级。这将提高我们对系统的可见性，以便能够检测和防止进一步的攻击。我们的顾问将与我们一起工作，确保整个过程只需要几小时，而不是几天。”整个房间里紧张的 IT 员工们发出欢呼声，准备开始工作。

伊莎贝尔靠向迪伦问道：“什么是 EDR 工具？”

“就像打了兴奋剂的杀毒软件，”迪伦低声说道，“是指端点检测和响应。老的防病毒程序会使用指纹来查找恶意软件，但攻击者已经发现了这一点并会使用不同的指纹。EDR 的工作原理类似于面部识别，因此无论你留胡子还是戴眼镜都没有关系。它还可以采取行动将攻击者踢出系统”。

房间里的谈话结束后，伊莎贝尔若有所思地点了点头。

“这听起来是个不错的计划，帕特尔博士，但如果它花费的时间比你预期的要长，怎么办？”科菲问道。

一位穿着亮红色西装的金发女士说道：“我们的网络安全保险公司将继续代表我们与网络犯罪分子进行谈判。”她向站在她身后的几位顾问点了点头。“他们将与勒索软件团伙保持沟通，以减少赎金，就好像我们打算支付赎金一样，为我们争取更多的时间”。

“那是金 • 塞尔夫(Kim Self)。”伊莎贝尔补充道，“她是我们的首席风险官。我稍后会介绍你认识她。”努尔再次发言，这次她身边还有两名董事，在他们的记事本上记录着她的话。

“如果我们的恢复时间超过 36 小时，”努尔澄清道，“我们将轮班工作并且建议支付赎金。但我们预计将在 3 天内完全恢复运营”。

“那会对我们造成多大的损失？”奥莉维亚转向迪伦的方向问道。

当身旁的那位粉色头发女子回答时，迪伦感到有些惊讶。“我们将为所有订阅者免费提供一个月的信用额度，作为这次故障的补偿。”迪伦看到她的工牌上写着首席财务官唐娜 • 常(Donna Chang)。“无论停机时间是一天还是一周，都会造成同样的影响。我们暂时可以承受，但需要开始考虑长期的影响。客户流失是一个问题。但坦白讲，更大的问题将是恢复成本，这还是未知数”。

奥莉维亚站起来对着房间里的所有人说：“谢谢大家，我不会撒谎，接下来的日子将很具有挑战性。我们将渡过这个难关，而且我们将因此变得更加强大。明天同一时间我们再次在这里集合，视频会议也将继续进行。如果你有任何新的发现，请及时通知。此外，在我们能够恢复电话系统之前，请确保你的团队成员都保存了每个成员的手机号码”。

接下来的几小时，迪伦努力帮助任何他能帮助的人。但是由于没有访问权限，也没有关于网络的详细信息，他几乎无能为力。他大部分时间只是像一个打杂的，拿着补给品为管理员们提供帮助，协助他们重新建立计算机系统。

“你在这儿啊。”伊莎贝尔从一个隔板上面探头看着，此时迪伦正在桌子下面拔电源线，以便把计算机带给他正在协助的管理员。出来的时候，他的头撞到了桌子底部。

“请告诉我你有哪些事情可以让我去处理。我整个上午都在搬计算机”。

“老板在找你。”她已经快步离开了，迪伦必须跑起来才能跟上她。

她带他走出了大厅，经过一个悬挂在半空中的巨型运动鞋，进入了大楼的北侧。

迪伦的手机在口袋里嗡嗡作响。他把手机掏出来看，发现来电的是查克，是他在 MarchFit 谋得这份工作时合作的猎头。他把电话静音，继续跟在伊莎贝尔的后面。

浓郁的咖啡香气弥漫在高管的房间里。这让迪伦感觉更加清醒。“那是奥莉维亚发明的最早的立式办公桌跑步机吗？”当他们经过几个办公桌跑步机的概念原型时(迪伦的那台 TreadMarch+跑步机就是基于这些原型)，迪伦问道。

他们走过一张高高的会议桌，每个椅子的位置都有一个小型跑步机。“一边慢跑一边开会，”伊莎贝尔说，“在疫情暴发之前，我们有几个大客户准备下

订单的。”

伊莎贝尔转身对他微笑，但继续走着。他们来到一扇亮橙色的双开门前。伊莎贝尔敲了敲门，然后为迪伦推开了门。他走了进去，但伊莎贝尔没有跟进来。她走开时只说了一句“祝你好运”。

这间办公室由两面玻璃墙构成，一张 TreadMarch+立式办公桌面向窗户。第三面墙看起来像纳斯卡车库，到处都是红色的工具箱和工作台，电动工具和跑步机零件散落一地。房间的中央是一张白色的小桌子，周围是 4 张看起来很现代的红色沙发。桌子上放着一堆活页夹。最上面的那个是迪伦早些时候看到的伊莎贝尔拿着的那个——业务连续性计划。

“就是这个人吗？”一位坐在沙发上的陌生男人问道。迪伦终于意识到这是奥莉维亚的办公室。努尔双臂交叉坐在奥莉维亚对面，奥莉维亚靠在她的桌子上。努尔点点头回答了那个男人的问题。

“告诉我，托马斯先生，你认为刚刚发生在 MarchFit 的那件事是可以预防的吗？”

迪伦看向努尔和奥莉维亚，她们都是一脸茫然，显然在等他回答。这是一个严肃的问题。

“我对我们所有的技术并不是很了解，无法回答……”迪伦回答道，但被打断了。

“这不是技术问题，这是哲学问题。你认为预防是可能的吗？”那个男人竖起手指等待迪伦回答。

“我认为，”迪伦开始说，“我们必须相信预防是可能的。”

那个男人等了几秒钟，然后问道：“为什么你一定相信预防是可能的，托马斯先生？”

“你不认为要想获得成功，必须先相信成功是可能的吗？如果我们不相信我们可以预防网络犯罪分子的入侵，那么会在潜意识中让这种事情发生。此外，我选择将这作为我的职业，如果我不相信我能够改变现状，那我就是疯了”。

“下一个问题。网络安全的目的是什么？”男人交叉着双臂问道。

迪伦想了想。“安全只是为了让业务保持平稳运行”。那个男人点了点头，久久没有说话。“还有其他问题吗？”迪伦转向努尔和奥莉维亚问道。

“最后一个问题，”那个人说，“你喜欢学习吗？”

“当然，”迪伦回答道，“在 IT 领域，必须热爱学习。我们一直在学习以跟上新技术的发展。”

男人飞快地从座位上跳了起来，还没等迪伦意识到，那个男人就已经握住了他的手。“你即将学到很多东西，”他对迪伦说道，“他可以胜任。”他对奥莉维亚和努尔说，然后走出了门。“明天见，托马斯先生”。

“迪伦，对于这一切我感到非常抱歉。”努尔说着转向奥莉维亚。她在男人刚刚坐过的沙发上坐下，示意迪伦坐在她对面。奥莉维亚坐在努尔旁边。

“没有什么需要道歉的，”奥莉维亚反驳道。她转向迪伦，面带微笑。“这是一个很好的机会，迪伦。很高兴认识你。我通常会见我们所有的员工，但我并不希望我们是在这样的情况下见面。”

“我们至少应该先问问他，这样他就知道自己将要面对什么了。”努尔说，“迪伦，我知道你计划今天和你的团队见面。”

“我已经看到几个了。”迪伦回答道。

“是的，但是显然出现了一些问题。”努尔说，“别担心，你不会被解雇或其他什么的。但由于你还没有接受过培训，也还没真正有过任何入职时间，你在事件响应方面可能没有太多的帮助。”她拿起咖啡杯，慢慢地喝了一大口。

“现在听起来我被解雇了。”迪伦紧张地笑着说。

“迪伦，”奥莉维亚回答，“你绝对不会被解雇。几小时前，我在这里问帕特尔博士，世界上最前沿的安全项目是什么。帕特尔博士，你的答案会是什么？”

“零信任。”努尔回答。

“你知道什么是零信任吗，迪伦？”奥莉维亚问道。

他双臂交叉，交叉腿坐着。“我听说过，但不太了解。那不就是网络安全公司的一个营销术语吗？”

两个女人对视了一眼，眼神中透露出了一种默契。迪伦感到有些不安，觉得这次谈话好像已经发生过一次了。

“我了解了一下，结果发现全球最杰出的零信任专家之一就住在我们附近几分钟车程的地方，”奥莉维亚解释道，“你刚刚见过他了。他曾经与约翰•金

德瓦格(John Kindervag)和蔡斯•坎宁安(Chase Cunningham)博士共事，这两位Forrester的分析师是零信任的先驱。顺便说一句，他的名字叫艾伦•拉帕波特，虽然他没有进行自我介绍”。

“那么，我将会汇报给他吗？”迪伦问道。

“从技术上讲，你仍然是汇报给我。”努尔纠正道。

迪伦把头转向一边。“技术上讲？”

“努尔的意思是，在接下来的六个月里，你将虚线向我汇报。”奥莉维亚说。

“哦，”迪伦只能说出这个词，“所以这位顾问就是我的奥比-旺(Obi-Wan)？他会教我零信任之道吗？”[1]

“这就是为什么我相信零信任会适用于我们。”奥莉维亚向迪伦和努尔说道，“我注意到总统发布了一项行政命令，要求政府机构采用零信任作为确保政府机构免受其他国家攻击的战略。刚才跟艾伦交流的时候，他说服了我。迪伦，告诉我为什么我会被他说服”。

“如果政府机构采用它，那它就一定是对的吗？”迪伦嘲讽地说道。三人哈哈大笑起来。努尔终于在座位上放松了下来。

“不。我相信零信任是因为它实际上是一种安全策略。这是努尔和我一直在争论的问题。对于我们业务中的任何其他目标或目的，我们都有实现它的战略。我们在安全方面的目标是防止糟糕的事情发生。我知道可以去购买工具或实施更多技术措施来增加安全性，但我们如何知道我们是在正确的轨道上呢？在业务的每个其他领域，我们都有一项战略，而零信任将成为我们未来的安全策略”。

“我将领导事件响应和恢复工作”，努尔解释道，“但与此同时，我们将为公司的所有技术启动转型计划，以全面实施零信任”。

“你听说过一项预防措施胜过十项补救吗？”奥莉维亚问迪伦。他点了点

1 译者注：“Obi-Wan”指的是《星球大战》中的角色奥比-旺•肯诺比(Obi-Wan Kenobi)，他是一名绝地武士，是主人公卢克•天行者的导师，教导他如何成为一名绝地武士。因此，“Obi-Wan”一词经常用于描述某人的导师或指导者。

头。“这就是我对零信任的期望。这就是为什么艾伦问你是否相信预防。我们相信预防是阻止攻击行为的最有效方式，而零信任是实施技术预防的最佳策略”。

“这是有道理的。”迪伦说。

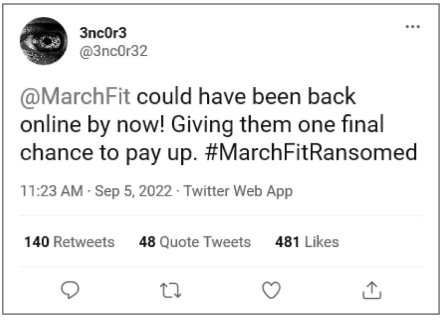
“这是一个很好的职业机会。你将负责在一个家喻户晓的公司实施零信任。拒绝这个机会是疯狂的。”奥莉维亚看着努尔说道。

“那么六个月后会发生什么？”迪伦问道，“您说我只向您汇报六个月？”

“六个月后，我们将推出一款全新的产品，它将改变世界看待健身、工作与生活平衡等一切的方式。我们承担不起可能使我们无法率先进入市场的失误。”奥莉维亚说。

“迪伦，我们不会理所当然地认为你已经接受了这个新挑战，”努尔说，“你应该花点时间考虑一下。你在整个职业生涯中都专注于管理 IT 基础设施，这是一种不同的挑战，也不是你昨天所预料的。我不希望你盲目地接受这个工作机会”。

门外传来轻轻的敲门声，一个身穿黄色西装的红头发女子没等回应就走了进来。“哦，太好了，你们都在这里，”她走近奥莉维亚和努尔时说，“我们的媒体监控服务刚刚看到一条消息。黑客公开了他的要求。”她把手机递给奥莉维亚，努尔和迪伦也走近了一些，这样他们三人就可以看到黑客发的推文。



一条来自黑客 3nc0r3 的推文公开威胁 MarchFit，并确认网络攻击的传言。

“迪伦，这是我们的公共关系负责人艾普莉尔。”努尔说。艾普莉尔伸出手和迪伦握手。

“Encore 是谁？”奥莉维亚问道。

“从他的个人资料来看，他似乎住在东欧或俄罗斯的某个地方，但不清楚他具体来自哪里。他过去的推文表明他已经勒索过其他几个组织，但我们是他迄今为止攻击的最大目标。”艾普莉尔解释道，然后拿回了她的手机。

“我会和谈判代表核实一下，看看这是否是他们一直在谈判的同一个人。”努尔说着站了起来。“谈判代表应该尽量拖延。这可能会改变我们的时间表。”她走到门口，迪伦跟在她身后，然后她拦住了他。“只要你在接下来的几小时内做出决定，你就可以考虑所有你需要的时间。”她对他使了个眼色。“另外，如果你决定成为我们的零信任计划负责人，明天之前你需要做一些功课。”努尔指了指桌上的一摞文件夹说道。

迪伦开始往外走。他背着奥莉维亚的一个设计师背包，里面装满了他必须阅读的所有文件，显得非常重。在走出门口的时候，他注意到大楼入口上方写着 MarchFit 的座右铭“每一步都很重要”。新鲜空气有所帮助，但他真正需要的是去跑步。当他跑步时，压力通常会消失。

他将要从事的工作与他以前做过的任何事情都不一样。这是一个机会，但不是他几小时前所想象的那种机会。

他解锁了手机，才想起自己有一个未接来电。他没有注意到自己有一条语音邮件，所以他按下按钮，把手机放在了耳边。

“迪伦，我是查克。我知道你刚开始在 MarchFit 工作，我听说了网络攻击的事情。我刚刚收到你与 MarchFit 同时期面试的另一家公司的消息，他们给你提供了一个薪水更高的相似职位。迪伦，你会有更多的收入，担任非常相似的角色。如果你想接受这个更好的职位，请给我回电。”

迪伦筋疲力尽地倒在长椅上。事情发展得太快了。他已经太累了，无法冷静地思考。

他抬头看到一对夫妇正一起跑过大楼。他们经过时向他挥手示意。接着更多的人跑了过去。他意识到总部大楼周围的跑道上到处都是跑步的人。每当筋疲力尽的 MarchFit 员工离开大楼时，他们都会高呼支持。

他拨通了查克的电话。

“迪伦。我就知道你会打电话。你不需要让这份工作拖累你……”

“查克，谢谢你给我提供的新职位建议，但我不想放弃目前的这份工作。”

“你确定吗？有些公司在遭遇网络攻击后表现不佳。一般会进行裁员。我给你提供了一条安全的出路。你可以到任何地方担任云基础架构总监，并且很快就会成为首席信息官。”

“查克，March Fitness 让我度过了疫情时期。3 年前你就认识我了。如果我没有那台跑步机，我可能就不会在这里。我是认真的，减肥对我来说很重要。我知道这也会对其他人产生影响，我会坚持下去，确保这家公司还可以继续帮助其他人。”

关键要点

信任是一种漏洞。

零信任(Zero Trust)是一种网络安全策略，它指出我们面临的根本问题是信任模型被破坏，不受信任的一侧是邪恶的互联网，而受信任的一侧是我们控制的设备。因此，组织不会在受信任的一侧做任何真正的安全。然而，几乎所有数据泄露和负面的网络安全事件都是对这种破碎的信任模型的利用。零信任是指在技术方面消除信任。应该对数字系统有多少信任？答案是零。因此，有了零信任的概念。

零信任对于网络安全领域的成功至关重要。零信任与董事长、首席执行官和其他领导者产生共鸣的原因是，因为他们认识到在任何领域中制定一项成功的策略都是至关重要的。每个组织都是不同的，这意味着战略的实施方式因组织而异。成功的零信任实施将为每个组织进行量身定制，以满足其独特的需求、工具和流程。

零信任的主要目标是预防攻击(数据泄露)。预防是可行的。事实上，从业务角度来看，防止数据泄露比尝试从数据泄露中恢复、支付赎金以及处理宕机或客户流失的成本更具成本效益。

零信任不仅仅是一个营销流行术语。零信任不是你可以购买的任何一种特定工具，因为你可以使用许多不同的工具实现相同的目标。零信任不是参考架构，因为零信任的每个实现都将是完全定制的。

《零信任计划》将带你走上一个组织成功实施零信任的旅程。你将学习最重要的概念、方法和设计原则，并带回你自己的组织。要使任何策略发挥作用，你都需要具备一些关键要素。March Fitness 已经准备好备份、风险登记、资产和业务连续性计划(BCP)，因此他们能够恢复而不是支付赎金。他们还购买了网络安全保险，并且已经与网络安全漏洞响应服务提供商签订了合同，他们能够进行协助恢复和谈判。此外，他们已经把所有关键文件都打印成纸质文档，以确保即使他们的计算机处于离线状态也可以使用。但即使你今天不具备这些条件，你仍然可以采用零信任策略。

注意，March Fitness 有一位首席信息官(CIO)，他同时兼任首席信息安全官(CISO)。根据行业的不同，许多大型组织可能有也可能没有专门的 CISO 或专门的信息安全人员。无论你的组织处于网络安全成熟度的哪个阶段，你都可以成功实施零信任策略。如果你还没有开始你的零信任之旅，那么最好的开始时间就是今天。