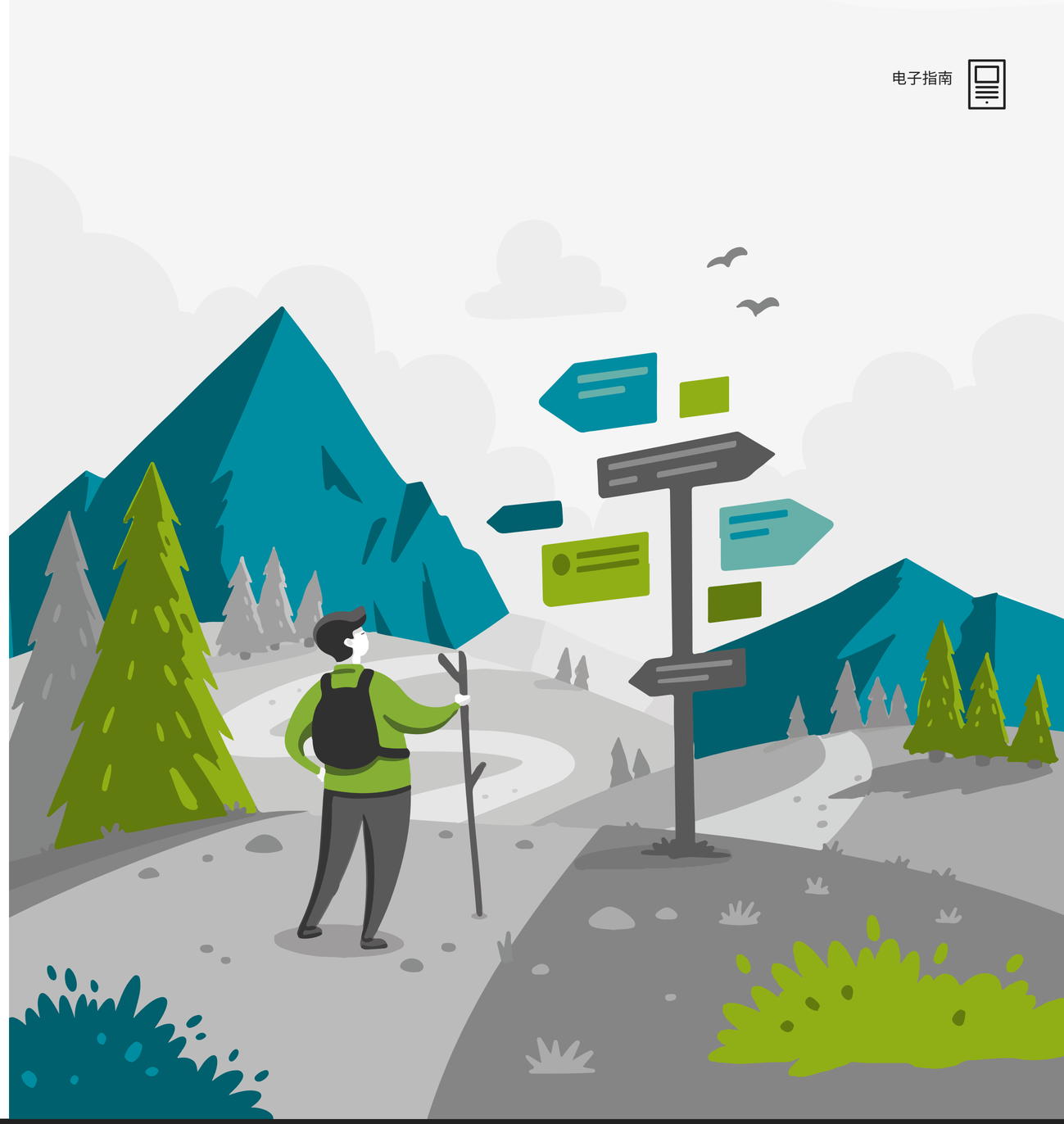
了解网络安全的基础知识。

作者：Trevor Pott
瞻博网络技术安全主管



简介

本文档涵盖信息安全的基础知识、作用及重要性。

信息安全是指与保护信息有关的所有事项：原理、工具、技术、产品、服务以及实践。信息安全与人员密切相关，损害事件几乎全部是由人为失误造成的。

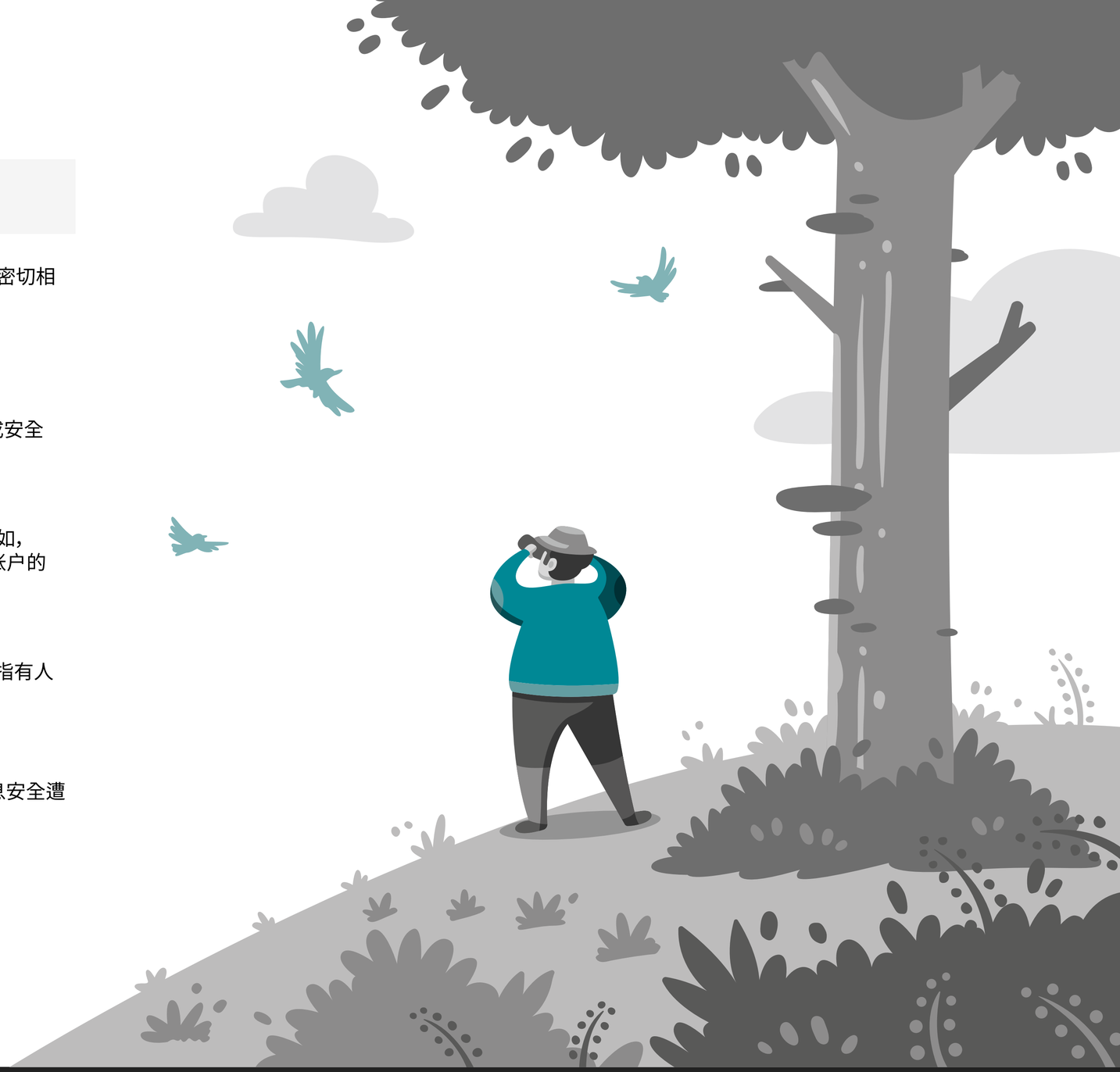
人为损害有三个主要类别：**无知、社会工程陷阱以及过失。**

无知是指缺乏知识，当我们误认为自己知道某些事情而实际上并不知道时，就可能造成安全风险。

社会工程陷阱可能非常简单（例如，冒充“微软技术人员”打来电话），也可能很复杂（例如，指向仿冒网站的鱼叉式网络钓鱼电子邮件）。其目的在于诱导您泄露可以用于访问您帐户的详细信息。

在社会工程陷阱面前，我们可能都有无知和脆弱的一面，但过失却是一种选择：过失是指有人故意选择将自己某些方面的职责搁置一旁，例如进行自我教育或执行任务。

幸运的是，可以利用技术来阻断攻击，向操作员发出提醒，检测恶意、异常或过失行为，从而防止信息安全遭受损害。



基本 IT 信息安全

数据和元数据

大多数信息以数据的形式存储在计算机上的某个位置，其形式不仅包含文件或数据库，还包含照片、Word 文档、记录等。

有关信息的信息（又称为元数据）也非常重要。

照片通常拥有与其相关的元数据，例如 GPS 坐标或拍摄照片设备的详细信息。如果在社交媒体上发布照片时未删除这些元数据，那么恶意使用者可能会利用它们确定目标的位置，甚至手机类型，以达到锁定目标的目的。

想象一下，某人拍了一张与食物的自拍照，然后将其发布到社交媒体消息中。这就为窃贼提供了位置和时间信息；经过简单的数学计算，他们便可知道在行窃完毕之前，机主能否回到家中。

元数据也可能会泄露企业机密。一位电工发布一张他们刚刚在尚未公布的新数据中心完成的电缆敷设工作的照片，这可能会轻易将其位置信息泄露给查看元数据的任何人。同样，Word 文档往往会保留所有编辑者的历史记录，这可能会产生法律后果。

只有防火墙和反恶意软件还远远不够

传统的防火墙和反恶意软件单独使用时并不是特别有效。

传统的防火墙可以阻止某个人远程控制您的电脑，但无法过滤网络钓鱼电子邮件。如果点击了其中包含的链接，就会把某个远程控制的应用程序下载到电脑并绕过防火墙运行，这种应用程序也可能重新配置您的防火墙，从而远程访问您的电脑。

同样，反恶意软件应用程序在防御已知类型的恶意文件时相当出色，但难以防御未知类型，在防御多种可通过互联网浏览器进入电脑的对象时，它们几乎毫无用处。

在企业中，大多数信息安全产品和服务专注于保护传输中的数据，目的是要在威胁到达用户端或离开网络之前将其拦截。

新一代信息安全

上世纪 90 年代，应用层防火墙投入使用，作为应用程序与外界之间的代理。此后出现的新一代防火墙 (NGFW) 深入集成到组织基础架构中，并具备高级功能，例如根据用户名或用户组应用策略，而不是仅仅根据 IP。

一般而言，NGFW 不仅能阻止不法分子利用基本攻击从外部进入网络，而且提供某些形式的传输中数据扫描功能，例如扫描具有网络钓鱼意图的电子邮件。NGFW 可以同时保护数千名用户，还可以为无法使用防病毒保护功能的端点（例如，打印机）进行防御。

新一代反恶意软件 (NGAM) 或新一代防病毒软件 (NGAV) 只能为其所在的主机提供防御。因此，会将其与 NGFW 搭配使用来帮助抵御社会工程陷阱的攻击。

NGFW 首先尝试阻止威胁进入您的电脑，这是最佳且最安全的方案。

一旦威胁进入您的电脑，NGAM（或 NGAV）会尝试阻止它对电脑造成损害，这是最后一道防线。

基本 IT 信息安全

WAF 和应用程序安全

下一步演化是 Web 应用防火墙 (WAF)。WAF 是应用层防火墙，专注于 HTTP 和 HTTPS 传输的应用程序，这类应用程序通常通过互联网进行访问（在网络内部或外部）。

WAF 防御特定应用程序或特定应用程序类别的专有漏洞。例如，WAF 会过滤恶意 SQL 命令，阻止它们的执行。WAF 通常在内部使用，用于防御内部威胁，并可阻止应用程序的一层受到另一层损害的影响。

应用程序并非总是依赖防火墙、反恶意软件或其他任何外部产品或服务来提供安全性。

传统的应用程序安全将保护层直接构建到应用程序本身。与电脑上的反恶意软件应用程序一样，应用程序安全绝对是基于服务器的应用程序的最后一道防线。如果攻击到达这个层面，说明信息安全整体已经出现严重问题。

深度防御

没有一家供应商可以独自抵御当今的网络威胁，而个人也没有足够的人力、研究和开发能力来寻找抵御新兴威胁的创新方法。

防护现代网络的唯一现实方法是让来自多个供应商的多个产品紧密协作，提供多层深度防御。

加密和 DLP

加密和数据丢失防护 (DLP) 旨在防止网络内的数据遭到泄露。

加密技术可确保仅拥有正确密钥的个人或应用程序才能访问数据。

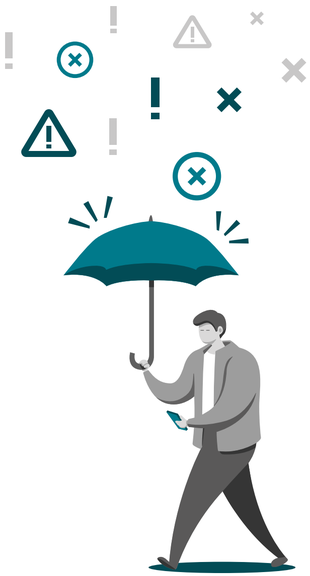
如果一名销售经理的笔记本电脑被盗，而这台电脑上有未加密的客户文件，这就会对企业造成巨大损失。

传输中数据的加密用于确保数据不会被第三方侦听，在访问互联网传输的服务或无线网络上的任何信息时，这一点至关重要（互联网和无线网络永远无法达到 100% 的安全性）。

基本的 DLP 方法是扫描试图离开网络的数据，如果数据不应离开网络，则对其进行阻止。该方法通常构建在 NGFW 和 NGAV 中，用于防止包含特定类型内容的文件被复制到闪存中，或者被上传到云存储文件夹（例如，Dropbox）中等等。

DLP 通常集成在安全工具中，包括云端访问安全代理 (CASB) 和高级威胁防护 (ATP) 产品，可检测信用卡信息电子表格的传输并生成警报或阻止程序等等。

不过，网络上还存在着许多窃取数据的方式，现代 DLP 对即时通信软件、Slack 和社交媒体的覆盖程度很低。



基本 IT 信息安全防御

监控

如果没有监控，IT 从业者将无法了解当前的状况以及需要应对哪些问题。大多数监控产品利用偏差和相关性来检测模式。

偏差依赖于实时观察系统之间的工作负载和数据流来确定"正常"的基线，然后识别偏离标准的事项。

基于相关性的监控会查找同时发生或快速连续发生的多个事件（表示存在问题），通常基于应用程序或基础架构组件生成的事件日志。

理想的基于监控的 DLP 系统会检测整个组织 IT 基础架构中的数据访问活动，寻找异常。因此，如果通常每天仅访问少数客户的信息的销售经理突然拉取所在区域所有客户的信息，系统会认为可能发生了不良事件。此方法需要来自多个供应商的多个产品共同协作。

但是，对一个组织机构的所有数据进行整体监控通常是不可能实现的。企业可以在数千个不同的地点和系统中拥有数据，包括本地数据和公共云中的数据。

即便组织可以监控所有数据访问活动，依然存在这些数据正在用来做什么的问题：异常访问模式可能是员工试图窃取数据，损害事件可能是外部攻击者造成的，也可能是有人在进行他们的工作而已。机器学习越来越多地被用于微调这些模式，在接下来的几年内可能有重大发展。

SIEM 和 ATP

安全信息和事件管理 (SIEM) 产品是信息安全的中枢，越来越多地与 ATP 产品互相交织。它们从多个产品接收数据，最有用的方法是与来自多个供应商的领先产品快速、简单地集成在一起。

最成功的 SIEM 和 ATP 专注于相关性。下面举一个例子。

1. NGFW 将电子邮件数据流发送到 ATP，ATP 检测到一系列以特定用户为目标的携带恶意软件的电子邮件。
2. ATP 指示防火墙阻止电子邮件抵达。
3. 不久之后，该用户端点上的 NGAV 检测到奇怪的行为。
4. CASB 检测到端点正在试图连接到云存储站点并上传文档。

虽然每个事件的警报严重性可能很低，但是如果 ATP 将其相关联，便可判断可能正在发生定向攻击，然后将其宣布为最大威胁，并提醒人员采取措施。

SIEM 主要收集事件和监控数据，许多供应商已开始添加扫描功能，在 DLP 中构建这些功能，或将其与拥有 DLP 的应用程序集成在一起。

基本 IT 信息安全防御

访问控制、VPN 和远程访问

得益于加密等信息安全技术，企业可以在无法访问实际数据的情况下对存储设备进行物理访问。同样，云计算可以让组织在未接触过底层硬件的情况下访问来自世界任何地方的产品、服务和数据。

几乎每个 IT 基础架构、操作系统和应用程序都有某种形式的访问控制功能。其中，虚拟私有网络 (VPN) 和远程访问是两种最重要的访问控制方法。

VPN 是两台计算机系统之间的加密网络隧道，用于让个人安全地连接到其组织的私有网络并在站点之间建立安全的连接。它们还利用加密来防御恶意行为者的侦听。

远程访问是指任何允许个人在不使用 VPN 的情况下访问组织机构资源的技术。

浏览器防御

除了电子邮件之外，Web 浏览器可能是外部攻击者最可能用来损害用户设备或端点的途径。

当今的 Web 浏览器依然非常脆弱，允许用户从互联网下载文件，然后执行这些文件，这是第三种最常见的信息安全损害途径。

主流 Web 浏览器（例如，Chrome 和 Firefox）提供了安装 Adblock、Ghostery 和 Privacy Badger 等扩展工具的功能，这些工具可防御各种形式的互联网不良事件（例如，恶意广告），旨在阻止 Web 浏览器试图请求连接到可疑的互联网资源。

其他浏览器扩展工具（例如，NGAV 供应商提供的扩展工具）则会试图阻止完成对受损资源的访问请求，从而保护最终用户。

基本 IT 信息安全防御

MDM

移动设备管理 (MDM) 产品专为处于组织机构边界之外的设备而设计，例如手机、平板电脑和笔记本电脑。它们在远程和移动设备上应用安全模板、配置文件和策略，并确保这些设备符合组织的信息安全要求，然后才能连接到企业边界之外的资源。

MDM 通过应用商店和虚拟桌面基础架构 (VDI) 等解决方案提供安全的应用程序交付流程。MDM 产品还提供访问控制，确保仅授权用户才能使用设备，并在设备被盗或丢失时进行跟踪或远程擦除。

身份验证

集中身份验证和统一身份验证 (UA) 技术依赖于目录服务，例如 LDAP、SAML 或 Microsoft Active Directory。单点登录 (SSO) 是最为知名的 UA 技术，旨在让用户使用单个用户名和密码访问位于多个基础架构且来自多个供应商的工作负载和服务。

多重身份验证 (MFA) 系统也已广泛使用，但是如果需要根据国家/地区进行区分，则可能导致情况复杂化。例如，短信验证（常用的 MFA 方法）要求用户输入短信中的代码才能登录，但许多国家/地区对短信实施限制，导致这种方法不可靠，或者需要进行额外集成才能正常运行。

自动化

受管理工作负载的数量和种类在快速增长。IT 革新加速已久，在没有帮助的情况下，人工无法跟上这种节奏，而自动化可以一展拳脚。

自动化是最重要的信息安全防御方法。

受制于当今 IT 高度互联的特性、快速消失的网络边界，以及边界之外可能和已经发生的威胁，信息安全必须融入到 IT 的各个层面。IT 基础架构的每一部分、每个工作负载，以及每个网络连接的设备都必须纳入组织的信息安全设计。

网络攻击剖析

制定目标

假设有一名黑客，我们称他为 Bob（虽然也有女性黑客，但在统计学上，犯罪者更可能是男性）。Bob 的目标是本地互联网服务提供商 PotatoCom。PotatoCom 已连续多年多次拒绝安装光纤互联网，Bob 厌倦了糟糕的 ADSL。为了报复，Bob 想要阻止 PotatoCom 访问自己的数据库，从而对其财务系统造成损害。

为了控制系统执行他的计划，Bob 无需成为超级技术专家，只需了解足够的信息即可实现目标。

连接

Bob 需要找到一个执行非法在线活动的方法，但不能追踪到他。他可以使用咖啡店不安全的公共 Wi-Fi，但他不能暴露在监控摄像头下，包括那些在前往咖啡店途中路过的摄像头。为了在经过不可避免（或未能发现）的摄像头时保护好自己，他可能需要进行一些伪装。

他永远不会将同一个 Wi-Fi 热点使用两次，并会改变前往各个免费 Wi-Fi 场所时采用的交通方式，以避免形成引人注意的活动模式。如果 Bob 在足够近的距离处成功连接，他甚至不用走进提供免费 Wi-Fi 服务的店铺中。

Bob 还需要隐藏自己的活动，以免被正在使用的网络上的任何监控技术检测到。他可能需要使用一个或多个 VPN。他还可能租赁一个虚拟机或虚拟私有服务器作为发起攻击的位置。为了进一步隐藏他的互联网流量，他可能会使用 TOR、I2P 或其他匿名加密方法。

付款

Bob 每次想上网时，都需要购买 U 盘、笔记本电脑、两个 VPN 服务帐户和两个租赁的私有虚拟机。因此，他不得不考虑如何在不被发现的情况下做到这一点。他可以使用一些方法，虽然复杂，但是可行。简而言之，Bob（以合法的方式）成功将现金转到预付信用卡中，此信用卡可以在任何地方使用，但无法追踪到使用者。

研究

Bob 需要了解 PotatoCom 使用哪些数据库和备份系统，以及如何进入他们的系统。他可以利用技术手段探查 PotatoCom 的 IT 基础架构；可以将自己伪装成一位知识渊博的人（或内部人士）利用社会工程陷阱与 PotatoCom 的各个员工聊天，给他们提供一个发泄的窗口，这个方法通常是有用的。他还可以在社交媒体上查找抱怨所用工具的 PotatoCom 员工，获得他需要的信息。Bob 甚至可以尝试拨打一些供应商支持热线，假装来自 PotatoCom，以确认 PotatoCom 是他们的客户。

网络攻击剖析

进入系统

进入系统最简单的方法是通过社会工程陷阱诱骗一些人提供他们的有效登录凭证。Bob 无需管理员凭证，他只需诱骗任何可以看到基础架构的人员，即使他们无法进行修改。他可以在这里利用网络扫描探查基础架构，利用内网漫游攻击软目标。一旦系统有多个后门，Bob 就可以尝试通过技术手段进入数据库并破坏条目，但这个方法较难。

要击溃 PotatoCom 的安全防御，Bob 真正需要的是他们的管理密码。

他们的整个基础架构都采用一家云提供商，因此他们生产环境所使用的管理凭据很可能与备份环境相同（虽然这不是一种具有足够安全意识的举措，但确实会发生这种情况）。

了解目标

Bob 不可能像之前一样通过社会工程陷阱诱骗拥有管理凭证的人，因为他们往往更具有安全意识。因此，他找到一个合适的目标并对其进行物理监控。

Bob 了解了他的目标，并利用这些知识找到漏洞，从而让他以某种方式获得想要的管理凭证。

例如，家庭的安全防护从来不如办公室那样全面，待在自己家中的人遭到窥探的几率很高。如果目标没有在家中办公，那么他的办公室在哪里呢？Bob 可以通过社会工程陷阱进入办公室，入侵摄像头或植入键盘记录器，通过窗户窥探，或拦截无线键盘发出的信号。

像黑客一样思考

连接到 PotatoCom 的基础架构之后，Bob 禁用了变更报告功能并破坏了数据库。然后，他对数据库进行了备份，删除了旧的备份，更改了 PotatoCom 的密码，毁掉了所有证据。

PotatoCom 的财务数据库现在已经无法使用，他们无法访问自己的帐户，无法查找问题。他们无法向客户收费、向供应商付款，或者报税。他们可能会由于无法访问所需数据而触发审计流程并惹上麻烦。他们甚至可能会倒闭。

Bob 所做的事情在技术上都不复杂。最重要的是思路缜密。Bob 竭尽所能避免自己被发现。他寻找最简单的办法：任何系统最可能被利用的部分通常是负责它的人。这就是黑客的思维。

要防御黑客，防御者只需要保持正确的思维：安全第一。

防御者需要像黑客一样思考（寻找漏洞），利用技术、业务流程甚至是窗户上的窗帘来填补这些漏洞。防御者一旦知道要防御的是什么，即可确定需要使用的工具。就像黑客一样，最重要的是思路缜密。

先进理念

监管合规性

仅实施信息安全技术，或通过在复选框中打勾来应用 IT 策略（以求通过审计）的方法已经不敷使用。组织机构需要证明他们切实了解信息安全的基础知识及必要性。

例如，欧盟 (EU) 的通用数据保护条例 (GDPR) 要求从事大规模数据处理的任何组织机构都必须聘用一位数据保护官(DPO)。DPO 负责保证组织机构遵守 GDPR 的要求，如果 DPO 或他们供职的组织机构在保护欧盟公民的数据方面出现过失，将会产生个人影响和重大财务影响。

分段和微分段

网络管理员利用分段和微分段，帮助阻止成功跨越网络边界防御的任何攻击者进行内网漫游。每个分段（或仅包含一个应用程序的微分段）均单独防御。这种环形围栏能够抵御内网漫游攻击，在 IT 基础架构拥有多个租户（例如，云服务提供商）的共享环境中特别重要。

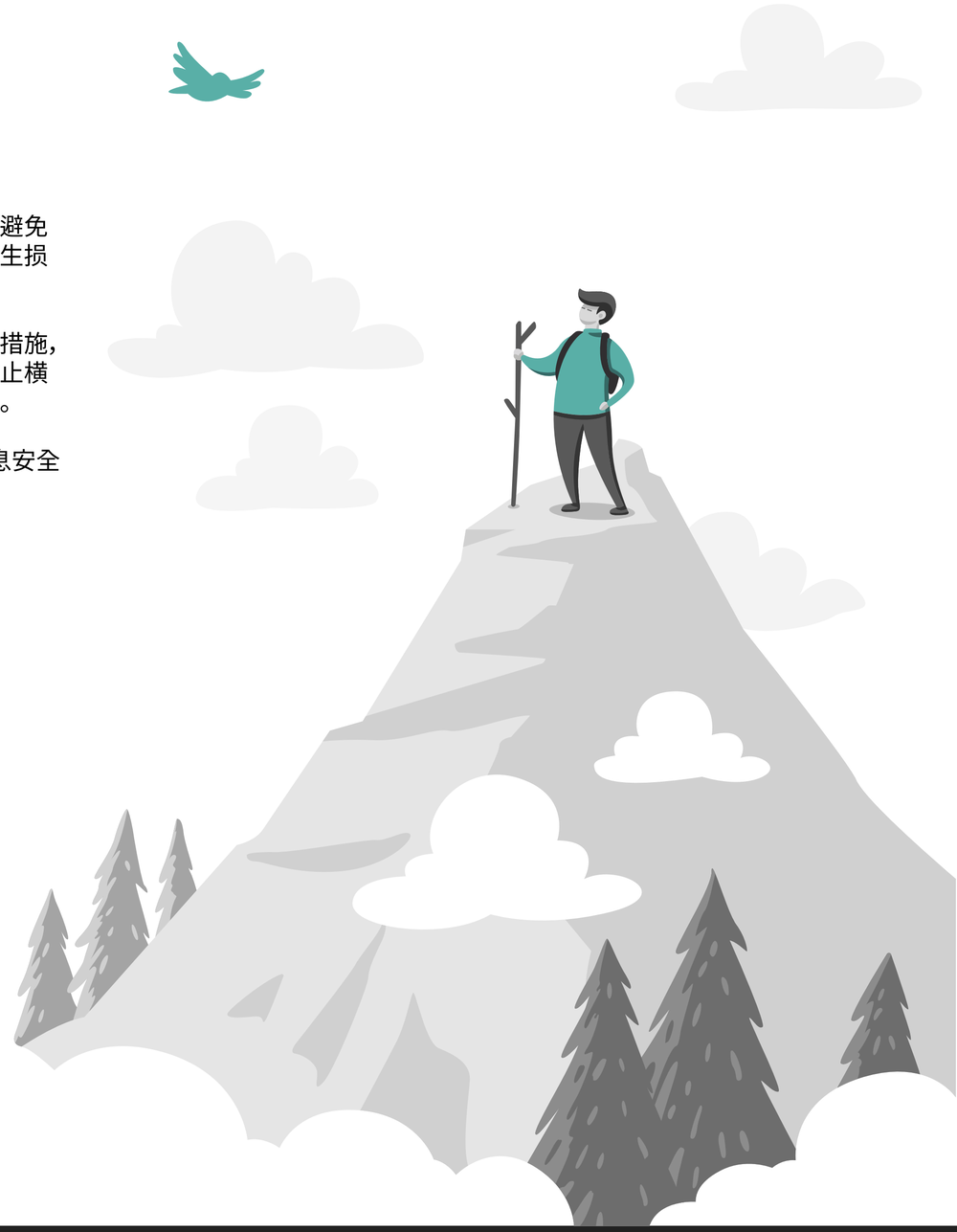
例如，微分段在研究型医院中将是一项优势。将私有云与微分段以及适当的信息安全措施相结合，即可将每个项目作为医院共享 IT 基础架构的租户进行隔离，无需让每个研究项目购买自己的 IT 基础架构。

汇总理念

信息安全损害事件是生活中经常会遇到的状况。损害的不可避免性并不会使预防技术失效，但却意味着组织机构必须针对发生损害时的情况制定计划。

将自动化与检测和缓解技术结合使用时，可以用于触发缓解措施，例如命令网络交换机断开或隔离遭到损害的设备。这可以防止横向扩展，可以在每次事件中为企业节省数千万甚至数亿美元。

预防、检测、缓解和事件响应是组织机构必须承担的四项信息安全责任。请务必牢记，信息安全的根本在于笃思慎行。



Juniper Connected Security

安全需要分层

当今的网络防御意味着防御网络上的一切，这就要求采用有别于大多数组织机构的信息安全方法。

网络和安全是互连的，当人们尝试使用单点解决方案构建网络时，情况往往会变得非常糟糕。有效的网络安全来源于多个安全层的互连，可通过部署来自多个供应商的多种技术来加以实现。

在 Juniper Connected Security 中使用全部集中自动化和编排的交换机、路由器和 Wi-Fi 接入点，可提供深度网络可见性和网络策略实施点。这为组织机构提供了其他方法难以实现的横向保护。

分析师可能认为特定分段的最佳解决方案是专业单点解决方案，但这种方法要求组织使用多个产品，并让各个组件很好地互相协作。这可能会增加网络防御自动化和编排的难度：排列随时会改变，自动化实施的周期通常超过进行自动化的产品的生命周期。

许多供应商拥有各种网络和信息安全产品组合，包括合作伙伴生态系统。还有许多供应商（例如，瞻博网络）可以为在服务提供商规模下运营的客户提供支持，并可以处理任何企业客户能够想象到的最繁忙、规模最大的网络。

Juniper Connected Security 中的“Connected”让瞻博网络独树一帜，这也是我们对互连性的承诺。瞻博网络支持整合和编排，鼓励使用开放标准、开放协议和开放 API，为打造具有竞争力的产品提供支持。我们的目标是帮助客户充分利用他们已有的资源，而不是要求他们进行剥离和更换。

在瞻博网络的产品组合中使用单一操作系统 Junos，使集中管理变得更加简单，也让瞻博网络能够通过在本地、云端或混合式环境中制定的管理计划，来提供功能丰富的管理平台。Junos OS 让产品组合的功能添加变得经济实惠。

通过将安全性扩展到网络中的所有连接点，Juniper Connected Security 让组织机构能够确保用户、应用程序和基础架构的安全；通过在尽可能靠近威胁的地方实施策略，降低威胁扩散的风险；以及通过采用机器学习、高级分析和自动化，让快速事件响应成为现实。

了解有关 Juniper Connected Security 实际运用的更多信息。

立即阅读

在此处阅读完整版的《网络安全基础知识》书籍

JUNIPER NETWORKS | Engineering Simplicity

PN：7400127-001-EN

公司和销售总部
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
电话：888.JUNIPER (888.586.4737)
或 +1.408.745.2000
传真：+1.408.745.2100
www.juniper.net

亚太地区以及欧洲、中东和非洲地区总部
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话：+31.0.207.125.700
传真：+31.0.207.125.701