采用以数据为中心的零信任方法保护您最关键的资产

2020 年 4 月 13 日 | 作者：Jesse Sedler | 阅读时间：4 分钟

对于我们任何人来说，儿童就是我们“最关键的资产”。为了给与他们妥善的保护，我们一直在努力了解他们在哪里以及他们在做什么，尤其是在令人烦恼的青少年时期。我们还会采取措施保护他们度过童年的地方。我们安装了摄像头、锁和警报系统来监控他们的活动，并保护外围安全，确保我们最宝贵的“内部人员”不会脱离“安全围栏”。这些概念并不新鲜；它们只是我们所生活的世界的产物。

对于尝试保护任务关键数据的组织而言，这些概念同样适用。客户信息、商业秘密和健康记录都属于组织拥有的最敏感信息，但我们往往没有像对待家人那样给与它们同样的保护。

进入“零信任（Zero Trust)”

重大数据泄露事件及全球性法规的增多，可能会导致组织遭受数百万美元的业务损失和/或罚款。为此，企业已经开始实施有助于减缓这些潜在风险的框架，其明确目标便是保护其敏感数据。零信任便是这些框架之一。

零信任（Zero Trust）是以不信任任何人这个概念为基础而建立的一种灵活安全框架。以前的安全模型专注于 IT 外围，但是随着企业向混合多云环境的转变、自带设备（BYOD）模型的增多，以及员工和承包商的混合使用，单单保护外围安全已然不够。相反，采用零信任战略的组织可以保护需要正确访问数据的人员、

需要管理的安全设备，并实施分析和响应机制，确保安全分析人员对其环境具有完全的可视性。

重新思考外围保护，提升数据安全性

数据是 IT 环境中所有事物的基础，但在面向外部的领域（如端点、网络和应用）中，安全性经常会被忽略。组织使用传统的安全方法在网络周围建立“围墙”，并检查进出围墙的每个人员，这对于当今企业而言，并不是一种妥善的做法。

相反，零信任框架和架构方法的特征是微外围（比如将房屋的大门锁上，然后关上孩子卧室的门）和微分段（比如只有祖父母和可信赖的邻居才能拥有房屋的钥匙和警报代码；管道修理工只有在您在家时才能进入房屋）。通过实施这两个原则，组织便可控制谁可以从哪个设备和哪个网络访问哪些数据。

在采用“零信任”方法时，安全架构的起点必须从底层开始，并逐步向上发展到 IT 堆栈（比如在数据层进行微分段和微外围），然后将信息用作移动到框架外部区域时的情境。没有坚实的基础，您就无法建造坚固、美丽的房子。

成功实现零信任的四个步骤

1.定义信任

构建牢固框架的第一步是针对组织所拥有的敏感数据及其所在的位置创建一个清单。一旦知道了拥有什么，便可以制定规则来保护它们的安全（比如我有两个幼儿，那么就需要在楼梯上安装安全门；我有一个 10 多岁的小孩，那么就需要锁上酒柜）。

若要进一步保护数据安全，组织应采用强加密来加固环境。这类似于让您的孩子在骑车时（务必！）戴上头盔、护膝和护肘。

2.执行信任

接下来，若要完全了解您的数据格局，您需要执行活动监控，查看谁在尝试访问所有数据（比如使用家长控制工具跟踪孩子正在跟谁发短信或跟谁一起骑车，以确保他们的安全）。对于任何组织而言，拥有最敏感数据相关用户和行为的清晰视图都至关重要。

3.重建信任

无论您制定了什么规则，随着业务环境的不断变化，仍然会发生一些违反这些规则的事件。育儿也是如此！在发生这种情况时，重要的一点是要迅速做出响应并采取精确的措施来解决问题。对于企业来说，这可能意味着调整网络的分段或擦除用户设备。

4.改善可信度

数据保护是一个持续的过程，涉及到所有的安全领域。强大的分析和机器学习功能可让您深入了解数据环境，并滤除误报带来的噪音。这些分析应向自动化引擎提供数据馈入；如此一来，一旦检测到异常，受感染的用户将无法访问敏感数据。

了解数据位于何处并运用身份和访问管理（IAM）工具，组织便可了解谁有权访问这些数据，以及他们是否应访问这些数据。统一端点管理（UEM）解决方案中的分层功能可为组织提供有关数据、访问数据的用户以及构建端到端安全框架所用设备的完全可视性和情境信息。

使用零信任方法应对混合多云世界的挑战

在当今的环境中，敏感数据无处不在 - 它们可能会一下子从本地数据库“飞”到云文件共享库，而在我们乘坐游艇出海时，也可以在平板电脑上通过虚拟专用网络（VPN）访问敏感数据；因此，组织需要强大、灵活的框架来确保业务连续性、合规性和客户信赖。针对您的“零信任”计划采取以数据为中心的方法，您的组织便可做好充分准备来应对当今混合多云世界带来的挑战。

就像是您让孩子回房，然后设定警报、关灯、关门并上锁一样，我们在保护组织的敏感数据时也应该采取这样的方法。还有一点：别忘了藏起酒柜钥匙！

观看 Think Digital 会议，了解有关零信任安全对您的企业而言有何重要性的更多信息。

Jesse Sedler

IBM Security 数据安全产品经理

Jesse Sedler 是 IBM Security 数据安全团队的产品经理。他于 2018 年加入 IBM Security，首先是负责移动安全领域的网络安全工作，然后是负责数据安全。他先前曾担任过某个贸易协会的游说者，以及国防高级研究计划局 (DARPA) 的分析师。他拥有埃默里大学的历史学士学位和杜克大学的工商管理硕士学位。