**数字经济在开源基础上运行.以下是如何保护它**

https://hbr.org/2021/09/the-digital-economy-runs-on-open-source-heres-how-to-protect-it

免费的开源软件（FOSS）是我们每天使用的许多技术的基础——从汽车到手机到飞机再到云端。虽然在传统上，它是由一群志愿开发者开发并免费提供的，但越来越多的公司开始在FOSS开发中扮演着更加积极的角色。然而，随着公司收购开源公司、将开发工作内部化，并推出自己的盈利版FOSS产品，它们可能会危及这种关键软件的未来。为了保持FOSS的可用性和安全性，公司应该：1) 制定明确的开源政策——最好鼓励员工在可行的情况下为FOSS做出贡献，2) 提高对所用FOSS的认识水平，并随时了解它的漏洞，3) 考虑到他们所用软件的稳定性，并通过激励员工的贡献来确保其关注对公司有用的功能以及一般安全性和维护。

尽管大多数人没有意识到这一点，但我们每天依赖的许多技术都是在自由和开源软件（FOSS）上运行的。手机、汽车、飞机，甚至许多尖端的人工智能程序都使用开源软件，比如Linux内核操作系统、Apache和Nginx网络服务器，它们都运行着全球60%以上的网站，以及为云计算提供动力的Kubernetes。这些软件包的可持续性、稳定性和安全性是每个使用它们的公司（也是每个公司）的主要关注点。但是不像那些由公司内部开发并销售的传统的闭源软件，开源软件是由一群默默无闻的开发者开发的，他们通常不拿薪水，而且通常是免费提供的。

在过去的几年里，我们观察到企业在开源软件中的积极作用有所增加，要么让员工为现有的开源项目做出贡献，要么开源他们自己的代码，这些代码允许社区利用它并帮助维护它。随着公司将FOSS作为其商业模式的一部分，他们也收购了重要的FOSS生产商。两年前，IBM以340亿美元的价格收购了红帽公司，这个公司是围绕FOSS建立起来的最成功的公司之一。在此之前一年，其他科技巨头也花了巨资收购FOSS的股份，其中最著名的是微软（以75亿美元收购GitHub）和Salesforce.com（以65亿美元收购MuleSoft）。

企业界进入开源的在线社区，引发了一些严重的担忧和摩擦。对FOSS生产商的收购可能会导致志愿贡献者被排挤，从而威胁到FOSS未来的健康。此外，世界上最大的云端提供商已经在FOSS组件的基础上建立了数十亿美元的业务，这让FOSS的贡献者们想知道为什么他们要把自己的空闲时间花在让富人更富上。这样的行为会让志愿者打消做出贡献的念头，威胁到FOSS社区的基本精神。

一个特别有争议的案例是最近Elastic与亚马逊之间的冲突。上市公司Elastic的Elasticsearch软件支持Walmart和Audi等众多企业网站的搜索活动。这个公司就自己采用了开源技术，对其进行了重新包装，并以几乎相同的名称出售给他们的客户这个问题与亚马逊展开了激烈的竞争。Elastic认为，最重要的是亚马逊拿走了为整个社区创造价值的免费代码，并将其隔离开来，这样它就成了唯一可以从中获取利益的人。

在Linux基金会和跨行业开源安全基金会的支持下，我们开展了两项的研究工作——一项专注于对FOSS的使用情况进行普查，另一项专注于理解FOSS贡献者的动机——以更好地理解这些问题。首先，我们与软件组成分析和应用安全公司合作，包括Snyk和Synopsys，通过对这一关键软件进行人工智能普查，以确定最广泛使用的开源软件软件包，从而获得对FOSS在生产应用中的使用的广泛见解。其次，我们对FOSS开发人员社区进行了大规模的全球调查，询问开发人员为什么要为特定的FOSS项目做出贡献，他们如何看待来自公司的重大财务投资，以及他们利用了哪些安全实践（这是FOSS中的一个重要问题）。以下是我们的发现。

关于越来越多的企业参与FOSS，最大的问题是它是否会对FOSS系统的未来健康和福社产生负面影响。创造我们都依赖的软件的开发人员是否会停止参与一个更少受社区认同感驱动、更多受利润追求驱动的系统？公司是否会只关注有利可图的FOSS，而忽视社会所依赖的基础设施的其他关键部分？维护这种软件的安全性是否会变得更加困难？如果更多的FOSS工作是由个别公司完成的，那么寻找bug和潜在漏洞的人会少吗？如果以上任何一个问题的答案是肯定的，那么这对开源软件的未来来说是一个不好的预兆。

我们普查的初步结果揭示了两个有关的趋势，这种趋势可能使FOSS更容易受到安全漏洞的攻击。 首先，我们发现商业软件中许多最广泛使用的FOSS包都是在个人开发人员（而不是更广泛的社区）的帐户下保存的，这不仅引发了安全性问题，而且还引发了可靠性问题。一个个体可能会接受一份新工作，可能会决定退休，或者—一运气不好的话—一受到众所周知的打击，变得无法维护项目。个人账户也可能没有足够的安全措施来防止黑客的潜在危险攻击。其次，我们发现许多公司正在使用过时版本的开源程序一一这是一个令人担忧的事情，如果不一定令人惊讶的话。未能跟上更新意味着软件可能包含已知的错误和安全漏洞。这两种趋势都反映出安全往往是出现故障事后才想到的。

调查结果还显示，贡献者的动机可能需要公司使用非传统的激励措施。虽然越来越多的贡献者是由公司赞助的，但这些贡献者的主要动机并不是钱。这意味着公司传统的激励可能不起作用，而更多的内在动机，包括对学习的热情、对FOSS社区的归属感和程序员的职业身份可能需要依赖。因此，任何希望增强FOSS安全性的公司、组织或政府都需要专注于吸引这些内在动机，而不仅仅是为安全性工作的贡献者付费。或者，公司可以雇佣一些人专门从事安全问题的工作。无论哪种方式，我们的调查显示，期望贡献者自愿解决安全问题是不太可能成功的。

没有人，当然不是我们，建议我们必须回到FOSS的早期，那时它主要是由志同道合的个人自愿努力的。但是我们确实建议像公司和政府这样的大角色——他们越来越多地直接或间接地赞助FOSS——了解他们对FOSS系统未来的影响，并遵循一些指导原则。

首先，公司和国家的目标应该是取得适当的平衡：为了看到FOSS继续增长而不会扼杀一直是贡献的核心动机的社区精神。这意味着，公司应该对开源有一个明确的政策（最好是鼓励员工在可行的情况下为FOSS软件做出贡献的政策）。我们的研究发现，许多员工对他们公司的FOSS政策没有清晰的了解，这使得他们对公开使用和贡献FOSS项目犹豫不决。此外，他们可以主动支持这些项目，以确保他们未来的健康。

其次，使用FOSS的公司（基本上是所有的公司，不管他们是否知道）应该提高他们对所使用的FOSS的认识水平。最近的一项行政命令要求为政府购买的任何产品提供软件材料清单，以便它知道产品中包含哪些FOSS（和专有软件），因此可以意识到出现的潜在漏洞。这是一个所有公司都应该考虑遵循的重要的例子。这样做将允许公司更好地了解他们对FOSS社区的依赖，并将产生更多的透明度，并允许他们知道何时容易受到新发现的漏洞的影响。

第三，随着公司继续参与对FOSS的贡献，我们建议他们牢记他们使用的软件的稳定性，他们激励他们的员工专注于对公司有用的功能以及一般的安全性和维护，并保持认识到这些项目背后的志愿者社区是至关重要的并且应该受到保护。通过这种方式，他们不仅从他们添加的新功能中获益，而且还确保了他们所依赖的FOSS的未来健康和福祉。

免费的开源软件是经济中至关重要的一环，就像州际高速公路、电网或通信网络一样。考虑到我们已经对这些关键的基础设施系统有了这么多的了解，对它们在21世纪的同类系统学习同样多的知识不是很有意义吗？由于FOSS系统中涉及的利益相关者数量众多，任何一个参与者都很难解决所有问题。因此，很可能需要包括公司、政府组织和个人贡献者在内的多方努力来确保未来FOSS系统的安全性和活力。然而，首先必须了解问题的范围。我们相信，我们的努力是朝着这个方向迈出的第一步。