DELL Technologies

从 Universitat Autònoma de Barcelona 勒索软件攻击事件中

吸取的经验教训

Gonçal Badenes
Universitat Autònoma de Barcelona 首席信息官。
为确保清晰阐述，采访内容已经过精简和编辑。

这所大学在遭受勒索软件攻击后，迅速采取了应对措施，保持了整个环节公开透明，并且重新承诺提升网络安全防护。

Dell Technologies 网络安全市场部门的 Sameer Shah 就此事件与该校首席信息官 Gonçal Badenes 进行了沟通。

Shah：我们一直在讨论如何帮助组织逐步提升其网络安全成熟度。你们之前遭受过一次网络攻击。在我们深入讨论这次攻击的细节之前，能否先介绍一下贵校及贵校的 IT 环境？

Badenes： Universitat Autònoma de Barcelona 是西班牙的一所知名高校。IT 部门负责监督校内运营所需的各种服务。

在攻击发生之前，我们已经制定了一套完整的计划来改进校内网络的安全态势。我们部署了多因素身份验证 (MFA) 技术，但并未覆盖所有服务和用户。学生和所有 IT 员工都启用了 MFA，但仅限于在 Microsoft 365 平台上启用。其他服务并未受到保护。未能全面部署 MFA 是攻击事件发生的重要原因，稍后我们会说到。

这次攻击是什么时候发生的？是什么类型的攻击？

这是一次勒索软件攻击，发生在一个长周末，这种情况很常见。凌晨四点左右，我接到团队成员的电话，告知我一些校内服务一个接一个地接连瘫痪。这些团队成员发出了警报，我们立即组建了之前为此类情况预设的响应团队。

你们是怎么知道这是一次勒索软件攻击的？攻击者有留下勒索信吗？

攻击者在受到攻击的系统中留下了勒索信。他们还发动了一次小规模的攻击，运行了一个脚本来加密在周末在线运行的计算机。尽管攻击造成的影响有限，但攻击者的主要目的可能是让教职员工和学生也察觉到这次攻击，而不仅仅是让 IT 团队知道。

贵校曾考虑过支付赎金吗?

没有。

为什么呢?

就伦理而言，我们无法这样做。幸运的是，我们对数据进行了备份，有两份备份存放在校园内两个不同的数据中心内，并且在校园外还存有一份磁带备份。

确认一下，这些备份并不是数据保险库，对吗?

对，当时我们并没有数据保险库，它只是我们未来路线图规划中的一个优先事项。但在这次攻击事件过后，我们将该事项的优先级大幅提高了。

在遭遇攻击的情况下，沟通至关重要。听起来你们是通过清晰和透明的沟通，包括与媒体的沟通，成功应对了攻击带来的影响，对吗?

是的，从一开始我们就是这样做的。我们必须完全保持透明，尽可能公开地解释所发生的事件。我们要确保其他人能够做好准备，并从我们的经验中吸取教训。我猜有些媒体实际上看过勒索信并联系了网络攻击者，而我们自己从未这样做过。发动攻击的团伙自称为 PISA (Protect Your System, Amigo) 组织。

很多时候，组织都倾向于保密，以避免暴露他们的弱点或补救策略。这是一个需要顾虑的问题吗?

这些顾虑非常合理。但我敢肯定，所有组织都知道自己会受到网络攻击。当我们试图保护自己的家时，即使购买了最好的防盗门，如果小偷真地想进来，他们总会找到办法，无论是破门而入还是采用其他途径。网络攻击也是如此。

我们遭到攻击并且存在漏洞这一点并不丢人。重要的是，我们虽然制定了非常清晰的保护路线图，但仍然遭受了攻击，这一点值得与大家分享。即使我们采取了严密的保护措施，但仍然存有会被不法分子利用的漏洞。通过开展额外的保障活动，我们能够处于更为有利的安全态势。

为此你们立即采取了哪些措施来应对这个问题?

我们关闭了网络和所有系统。我们联系了警方和当地数据保护机构，这是我们在法律层面需要做的事情。然后我们立即组建了两个团队：取证团队和恢复团队。我们联系了戴尔，戴尔立即将该事件升级为高度优先事件，并派遣了出色的团队全天候为我们提供协助。他们设法完全恢复了第二个数据域上的所有数据。

所以取证工作是在恢复过程中开始的吗?

在某些数据恢复过程中，我们不得不等上片刻。这就是我说的要先开始进行取证的意思。为了弄清楚问题的原因和影响，我们对所有数据和系统都进行了隔离。我们不得不组建另一套系统，以便能够恢复数据。我们决定，所有上线的系统都必须符合最高的安全标准，即使这样会花费更多时间。

“最重要的是要认识到，我们迟早都会面临网络攻击，因此需要制定详细的缓解和恢复计划。”

你之前提到 MFA 仅在 Microsoft 365 上启用，这也是导致攻击的部分原因。那么，现在 MFA 已经全面启用了吗?

这次攻击的目标是一位凭据遭到泄露的用户，该用户所在的团队已经在 Microsoft 上启用了 MFA。但当网络攻击者尝试访问该用户的电子邮件时，发现无法通过 MFA 验证以继续访问，因此他们只能继续寻找漏洞。然后他们发现我们有一个不受 MFA 保护的 VPN。他们通过 VPN 获得访问权限后，就开始对网络进行分析。

攻击者在我们的大型网络中找到了一个有安全漏洞的系统，并开始在网络内部进行横向移动。所以在开始恢复系统后，我们决定在没有全面启用 MFA 保护之前，任何系统都不能上线。

如果要给同行提供一条避免勒索软件攻击的关键建议，您会说些什么?

虽然很难只给出一条建议，但我认为最重要的是要认识到，我们迟早都有可能会遭到网络攻击，因此需要制定详细的缓解和恢复计划。

例如，需要掌握取证和恢复领域关键合作伙伴的联系信息，制定详细的服务恢复时间表并按优先级排序，同时制定与关键业务部门协调一致的战略，包括内部和外部的沟通策略。当然，让用户保持警惕，并接受有关攻击者使用技术的培训也至关重要。

你觉得贵校加强网络安全能力后，大家对于继续完成使命和开展各项工作变得更有信心了吗?

是的。在这次攻击发生之前，大家普遍认为，任何新的保护措施都会引发大量质疑，并担心这些措施是否真的必要。事实上，采取保护措施绝对必要，否则整个组织都会处于危险之中。当然，也有一些人仍然认为这些措施影响了他们的工作。但大多数人都觉得系统得到了更好的保护。

谢谢。相信所有致力于提升网络安全成熟度的个人和组织，都能从你开诚布公的分享中获益。