制定2020年网络安全规划时
需要注意的3种安全趋势

（来源：网络安全和信息化公众号，2020-01-09）

进入2020年，这意味着企业团队到最终确定网络预算、战略和目标的时候了。但是，在为新的一年做准备时，务必要注意2020年网络安全趋势将如何变化。

从投资者对网络安全问题的关注到网络保险的多样化，网络安全人员应准备应对 3 个关键的安全趋势——如果他们想要度过一个平稳而安全的2020年的话。

网络风险成为投资者分析的新选项

在2020年，网络安全将在金融投资中被提升到前所未有的地位。Equifax是第一家因数据泄露而被信用评级下调的公司，这使得投资者在不了解其网络风险的情况下对该公司的投资失去信心。

这种担心是可以理解的：我们的研究表明，大多数《财富》1000强公司的开放端口上都运行着至少一个远程管理服务。如此糟糕的安全性，发生网络攻击可以说是不可避免的。

精明的投资者是不愿意投资那些缺乏良好安全性的公司的。他们开始注意到网络安全状况良好和公司股票表现良好之间的关联。尽管该研究仍处于起步阶段，但笔者相信许多投资者很快会将网络安全纳入其ESG分析中。

对于安全专家来说，这是向上级领导展示其价值的机会。拥有强大的安全性将不再仅仅是合规行为，这也意味着无论是打算购买股票

还是投资企业，都可以更好地吸引投资者。

相比零日漏洞，攻击者将更多地关注“钝力攻击”（ Blunt-force Attacks）

一直以来零日漏洞最受媒体关注，但在 2020 年，黑客可能不会再为这些受安全人员高度关注的攻击而“烦恼”。相反，他们会采用简单的策略，例如通过第三方或未打补丁的系统访问网络。

实际上，这种趋势已经开始出现。例如，APT33 在攻击关键基础设施时几乎只使用暴力破解密码。这些方法在面对 Shamoon 和 Shapeshifter（这是 APT33 的两个首选的部署方式）的攻击而受损害的公司中获得了成功。过去一年中，商务电子邮件攻击（BEC）的数量猛增。日本经济新闻社（Nikkei）就曾因受这种攻击而损失了 2900 万美元。除了这些近期的例子外，美国国家安全局（NSA）曾在报告中称，攻击者很少响应零日漏洞的入侵，相反，其主要集中在利用未打补丁的硬件和软件的攻击。

为了应对这些趋势，网络安全规划应回归并专注于建立强大的安全基础。这包括持续监测新威胁和漏洞，持续评估第三方合作伙伴的安全状况等。企业员工网络安全培训的重要性也不可低估。通常，安全态势中最薄弱的环节仍然是人的因素。

网络保险将在网络安全规划中扮演更重要的角色

从勒索软件到 BEC，应对网络攻击的成本在不断增加，而 2020 年将成为网络保险的引爆点。许多公司，尤其是规模较小的公司，正在尝试在没有足够的资源的情况下来缓解网络攻击的应对方法，尤其是来自第三方、第四方甚至第五方合作伙伴的公司。

尽管大多数网络保险不会直接为 BEC 或网络钓鱼攻击中造成的

损失提供赔偿，但它们将有助于为法律调查取证和相关费用提供资金。随着越来越多的公司采用网络保险政策，保险行业也将会学习有关网络攻击的细微差别，并开始提供其他附加的网络覆盖计划，其中包括覆盖网络攻击之外所连带产生的后果和损失。

无论是因停电而导致的抢劫，还是由于通讯错误导致的意外，公司都需要在进入新的一年里，为网络攻击对物理世界造成的影响而做好充分准备。一种方法是让公司重新评估其当前的网络保险政策或增加安全投入。

针对新趋势做好规划

凡事预则立，不预则废，新的一年将为网络安全人员带来一系列挑战，因此现在尝试预先制定规划有助于将来面临威胁时能够减轻对自身的影响。

首先，企业需要确保其 CFO 和其他利益相关者充分了解网络安全对企业财务的影响。因为随着安全工具变得更加高效，管理者可能会倾向于降低这方面的预算，但他们并不了解网络攻击将不仅严重影响其日常运营，而且还会影响企业的长期财务稳定性。

此外，建立强大的信息基础设施需要成为新的一年的重点。我们看到黑客依靠的是“久经考验”的方法，而不是追逐最新的零日漏洞，这意味着例行升级补丁程序，并与具有持续监控能力和完善安全保障措施的第三方合作伙伴合作，是保护企业的关键。

最后，网络保险在企业中扮演的角色将越来越受重视。网络保险

业也正在扩展，以减轻来自供应链中任何环节（包括外部）的损失；无论是您自身是否受到网络攻击，或者是您的隔壁邻居是否受到威胁，都将囊括其中。

原文链接：

https://mp.weixin.qq.com/s/4Odf2EkXJmM2iOmvFdcc3A，转载请注明。