疫情中公司远程办公安全指南

作者 | 孙鹏程

办公安全是公司信息安全核心之一，旨在为员工提供安全的办公环境，保护公司商业资产等。其承载着公司诸多部门的办公应用安全、办公网络安全、办公终端安全等使命，提供基础安全能力包括但不限于黑客入侵、钓鱼攻击、木马种植、病毒感染、账密泄露以及数据勒索等恶意行为的加固防护、安全检测以及应急响应等能力。

受到疫情影响，不少企业开始执行远程办公的临时应对方案，拥有信息安全管理体系的公司有完整的安全措施，但是大部分公司并没有相关的经验，疫情还未结束，无论何时办公，无论何地办公，公司需要高度重视办公安全尤其是远程办公中需要的安全措施。

远程办公安全分为几个层次，最基础层是办公环境，其次上层是办公方式，包含 PC 办公和移动办公，然后再上层是办公入口，包括微信、钉钉等第三方应用、邮箱、内部 OA 应用以及其他办公协同软件，最上层是我们办公所接触到的商业资产，例如财务数据、人事数据和交易数据等，每一层所面临的风险综合起来有黑客入侵、钓鱼攻击、账密泄露、数据泄露以及数据勒索等。

一、办公环境主要是网络安全

在家办公时应进入路由器管理地址，确保路由器升级到最新版本。查看当前连接的设备情况，确认有无陌生设备。同时也一定记得修改路由器出厂默认管理员账号的密码，部分路由器在设置 WI-FI 密码时会同时修改掉管理员账号，如果 WI-FI 密码泄漏可以能导致管理员账号密码同时泄漏。在发现有陌生设备接入时应及时拉黑并更换 WI-FI 密码。
在外出移动办公时，应尽量避免连接公共场所的 WI-FI，可以通过共享手机热点来满足网络需求。

二、办公方式安全主要是终端安全

应保持设备系统版本更新，及时安装补丁，Windows 系统应保持定期杀毒，OSX 系统本身安全性较高，仍应避免安装未知软件。
采取清理桌面和屏幕策略，重要的文件不应放置在桌上或电脑桌面，以防止无意中泄漏给亲朋好友或其他可能接触办公电脑的人员。
由于本次疫情属于突发事件，很多员工可能并没有使用公司的办公设备在家进行远程办公，当使用完别人设备后，应删除所有公司信息，当有重要信息时，应当反复几次覆盖删除操作，以防止重要信息被恢复。

三、办公入口主要是应用安全

远程办公会用到许多必备的软件，包括协同工具、邮箱、OA 应用等，应尽量从官方下载。同时保持软件处于最新版本，及时更新安全漏洞。另外，部分企业远程办公需要使用 VPN 进入内网，这类工具关系到企业内网重要信息安全，需要进行高级别防护，防止黑客入侵。对于高风险软件管理，应建立黑白名单机制。对于部分已经授权的人员，可以根据形势及人员的不同情形，取消或给予相应的授权。

四、办公资产主要是信息安全

在远程办公场景下，协同办公软件等工具成为公司分享文件的途径之一，在共享前建议对文件加密保存，云端共享时也需要设置提取码。传输重要文件时，尽量避免使用第三方聊天工具传输，应使用 HTTPS 等加密通道传输。对于部分企业而言，对于公司内部文件不建议以微信、QQ 或者其他聊天软件的形式进行传输。
做好文件备份工作，现在大部分公司都会采用云服务，但是由于对于云计算缺乏足够的了解，当发生数据丢失时，导致公司造成严重损失。应对重要数据做好本地备份工作。
建立访问控制策略，仅向用户提供已获授权使用的网络和网络服务的访问。

办公运营策略

针对远程办公公司应实现相应的策略及其支持性的安全措施，以保护在远程工作地点上所访问的、处理的或存储的信息。
针对敏感人群应建立分层运营策略。
网络钓鱼作为 2019 年最常见的安全威胁，公司应提醒员工不要点击来历不明的链接、附件等，谨防中招钓鱼攻击。
一半以上网络安全事件都是人为因素造成，由于个人的不良习惯导致黑客有机可乘，信息泄漏，所以公司进行信息安全教育培训是非常必要的。
应建立办公安全威胁以及事件的应急响应处置制度。该制度建议以公司内部高级管理成员为核心，成立应急相应处置小组，并将其常态化，因为未来企业可能还可能面临一系列其他风险。

以上远程办公安全建议参考了信息安全管理体系，但是每家公司应根据自身情况、人员岗位、信息资产敏感程度等，制定相应的安全策略。

没有百分百的安全，谁也无法预料到全部的风险和意外，就像无法阻止和预测黑天鹅事件一样；安全是一个长期的过程，我们需要在万千变化中尽可能地做好准备，无论是在风险发生之前还是之后的准备。

孙鹏程

北京大成（杭州）律师事务所律师

浙江省法学会网络法制研究会理事

擅长互联网、金融领域，提供互联网企业合规、个人信息安全影响评估等专项法律服务。

邮箱：pengcheng.sun@dentons.cn