KPMG

法证咨询聚焦

– 新型冠状病毒肺炎带来的网络安全思考、威胁和应对

毕马威中国

首席信息官和安全官的思考

新型冠状病毒肺炎（COVID-19）的全球流行正在影响和改变我们生活和工作的方方面面。对疫情的忧虑提升了人们对信息安全的需求，而有组织的犯罪集团正在利用这种担忧和疑虑，通过多种方法对个人和公司进行针对性攻击。

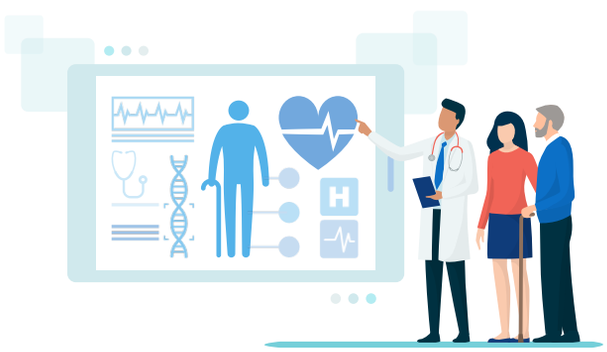
随着新型冠状病毒肺炎全球流行的规模和影响日益扩大，公司需要考虑采取有效措施来维持业务活动。为了确保公司能够正常运营，首席信息官 (CIO) 和首席信息安全官（CISO）在部署相应措施的过程中将起到至关重要的作用。

在远程办公情况下，公司的业务是否能够有效运转?

您需要确保公司的业务支持远程和灵活的办公方式，并且员工对能够做到这一点充满信心。这可能需要您重新考虑关于访问权限、授权机制和风险态势的相关决策。

需要考虑的问题包括：

- 您是否扩展了公司的虚拟专用网络、企业信息门户以及网关的负载能力，以满足更多的远程办公访问需求?
- 在远程办公期间，相关第三方（如供应商和承包商）可能因为业务需要访问公司网络。您是否考虑到这些额外的访问量对公司网络环境的影响?
- 您是否对公司的网络和系统进行过测试，以检验它们处理预期负载的能力?
- 公司的网络和系统是否会发生单点故障？公司是否具备从故障中快速恢复的能力?
- 您是否需要放宽原先的访问控制策略，或者提供额外的远程访问账户和密码?
- 公司是否有足够多的技术支持人员来处理用户因为无法登录或者不熟悉远程办公所提出的问题?
- 公司是否有足够的笔记本电脑满足员工远程办公的需要？是否可以通过更多的设备采购和系统安装来满足这些需求？笔记本电脑分配的优先级应该如何确定?
- 在设备资源有限的情况下，您是否需要优先考虑公司运营的核心服务，并为用户提供多种访问方案（如 Office 365, OneDrive 和内部应用）?
- 您是否考虑采用白名单的方式，在此期间只允许用户访问特定的应用，而禁止他们使用其他非必需服务?
- 公司的视频或语音会议系统是否有容量限制？您是否具备扩展这些相关网络基础设施的能力?
- 您是否需要考虑使用其他基于云技术的远程会议和办公解决方案?
- 是否所有员工都有参加远程会议所需的访问号码或者链接？他们是否随时可以获取相关培训材料？公司是否需要开通服务热线，以应对可能发生的问题?



- 如果技术支持人员不得不在家办公，公司是否能够支持相关业务的远程运行?
- 公司是否准备了简要的指南分发给员工，帮助他们应对可能出现的问题，例如:
  - 如何登录?
  - 如何修改密码?
  - 如何访问关键服务?
  - 如何联系技术支持获取帮助?
  - 如果遇到紧急情况，应该联系谁?

公司是否依赖特定的信息技术人员?

遗憾的是，员工可能会感染病毒，无法出差，或者因为疫情不得不在家照顾家人。针对可能出现的大规模人员缺席情况，公司需要制订相应的计划。

- 如果核心信息技术人员（包括承包商）无法出差或者感染病毒，这会产生什么影响?公司是否依赖这一小部分关键员工?
- 您如何减轻对这些关键人员的依赖?例如，确保公司有一套紧急方案，在特定情况下允许其他管理员暂时访问核心系统。
- 信息安全团队在面临相同情况时该如何应对?哪些是关键人员?如果无法联系到首席信息安全官，谁会对安全态势以及公司可以接受的风险做出相关决策?

如果出现网络攻击会发生什么?

犯罪集团会利用新冠肺炎带来的影响，建立虚假网站并进行有高度针对性的鱼叉式网络钓鱼攻击，从而进一步增加了网络安全风险。

- 您是否与员工进行过充分的沟通，告知他们如何获取有关疫情的权威信息，以及公司的应对措施?
- 犯罪分子会利用新冠肺炎疫情展开网络钓鱼攻击，您是否提醒过员工相关风险在日益增长?
- 如果公司有备用系统或解决方案（包括购买的云服务），谁能够协助您处理涉及这些系统的网络攻击?
- 在新冠肺炎疫情期间，您是否需要调整公司的安全运营方式，包括监控安全事件的策略?

如果出现信息技术故障会发生什么?

铺天盖地的疫情新闻引发了人们的持续关注。与此同时，面对不断变化的系统和网络需求，以及可能发生的机会主义网络攻击，您仍然需要注意信息技术故障的发生。

- 您是否能够远程处理相关故障?您是否拥有必要的远程会议设备，以及访问故障管理系统和相关指南的权限?
- 公司是否设置了一个网络指挥中心，来应对无法现场处理故障的情况?
- 您是否依赖部分重要员工进行网络安全应急响应?如果是这样，可以采取哪些措施来减轻对这些员工的依赖?
- 如果无法联系到主要的应急响应/恢复负责人，公司的应急响应和危机管理流程会进行怎样的调整?
- 您是否确信公司拥有最新的系统数据备份?并且即使在最坏的情况下，也可以恢复重要的系统和数据?
- 当大部分员工在家办公时，您会如何处理在公司网络中大范围传播的勒索病毒?

疫情带来的威胁

自二月中旬以来，毕马威就已经注意到网络犯罪分子正在厉兵秣马，筹划利用疫情的影响展开鱼叉式网络钓鱼攻击，诱导用户访问虚假网站，骗取他们的Office 365 密码。

以下是一些典型的案例：

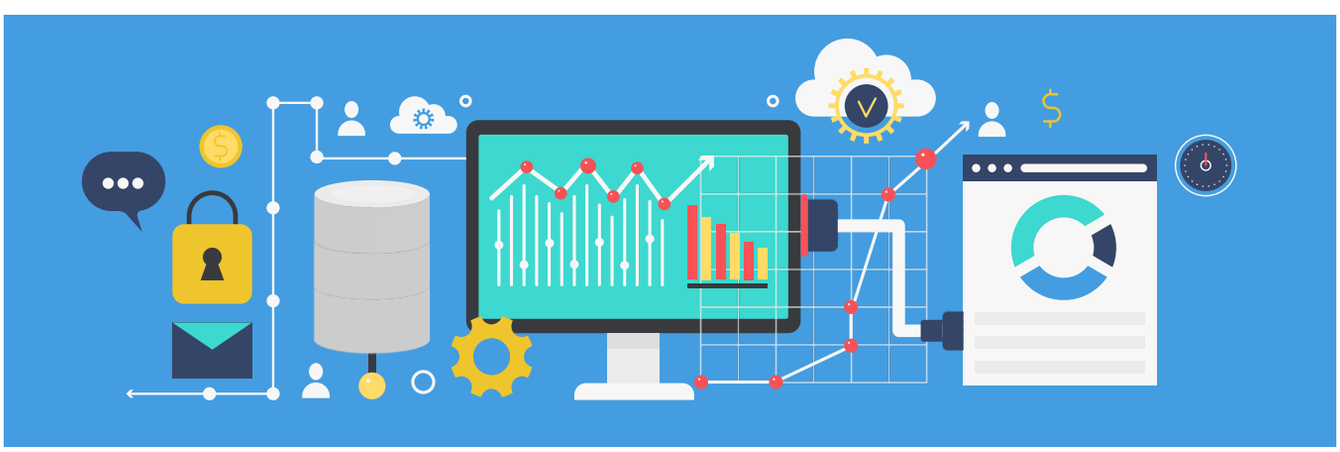
- 通过利用已知的微软漏洞运行恶意代码，犯罪分子以新冠肺炎为主题，发送包含恶意文档的网络钓鱼邮件。
- 犯罪分子发送以新冠肺炎为主题的网络钓鱼邮件，并添加包含医疗健康信息的Word文档为附件，通过利用该文档开启的宏功能，欺骗用户触发Emotet或Trickbot等恶意软件的下载。
- 犯罪分子发送多封钓鱼邮件，欺骗用户访问虚假的美国疾病控制与预防中心 (CDC) 网站，并收集他们的密码。
- 犯罪分子伪装成客户服务顾问，声称可以为用户提供更新来应对由于疫情引起的服务中断，以此欺骗用户下载恶意软件。
- 犯罪分子伪装成各类政府医疗机构或者世界卫生组织（WHO），发送所谓指导疫情防控的钓鱼邮件，而这些邮件往往包含恶意程序。
- 在疫情期间，犯罪分子发送关于退税的钓鱼邮件，欺骗用户在不知情的情况下访问虚假网站，以收集他们的财务和税务信息。

很多网络犯罪集团已经调整了策略，围绕新冠肺炎疫情，发布所谓的健康信息更新、虚假治愈方案、财政激励措施、紧急救助计划，以及供给短缺应对方案，借此对用户发起攻击。

网络钓鱼邮件的可疑特征主要包括：

- 多处语法、标点和拼写的错误
- 邮件设计和内容质量都不尽人意
- 邮件没有直呼姓名，而是使用“亲爱的同事”，“亲爱的朋友”或者“尊敬的客户”这样的称谓
- 邮件暗含威胁或者给人一种十分紧迫的错觉
- 直接询问并收集个人以及财务信息

当然，如果一封邮件看上去十分完美，那它也可能是钓鱼邮件。

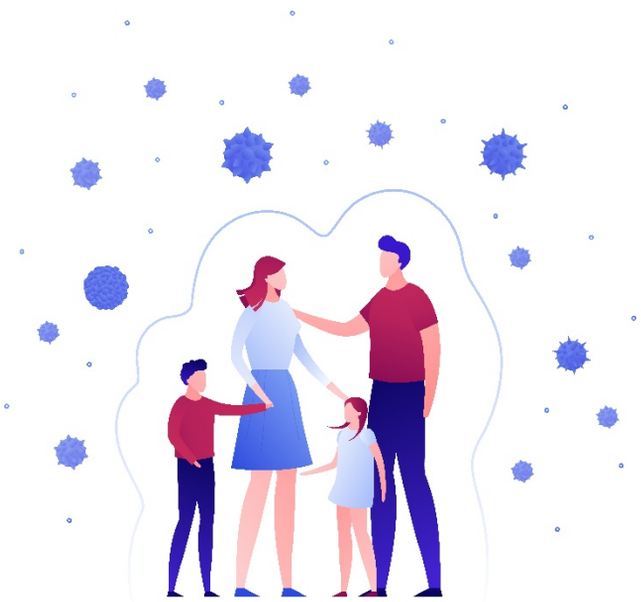


应对方法和策略

当公司开始远程办公时，您可以采取一些措施减轻疫情给公司和员工带来的风险：

- 提高员工的安全意识，提醒他们犯罪分子会利用新冠肺炎展开网络钓鱼攻击，而且相关的风险正在不断增加。
- 与团队分享保护安全的权威信息来源，并且定期传达公司应对疫情的措施。
- 对于所有远程访问账户，特别是Office 365账户，确保员工设置安全的密码，并且最好采用双重认证的方式核验身份。
- 发布简明的指南，帮助员工使用远程办公解决方案，并指导他们如何确保安全，以及如何识别网络钓鱼攻击 。
- 确保所有笔记本电脑都装有最新的杀毒软件和防火墙。
- 开通求助热线或提供在线技术支持，使员工可以快速寻求帮助，或者上报任何安全隐患（例如可疑的网络钓鱼攻击）。
- 由于设备存在失窃的风险，公司需要对远程办公使用的笔记本电脑进行数据加密。
- 为减轻恶意软件攻击的风险，禁止USB设备的使用，并为员工提供备用的数据传输方案或协作办公工具。

此外在疫情期间，公司还需要加强财务流程的控制。针对大额付款请求，财务部门应采取进一步措施，最好通过电话或者短信对邮件请求进行核验，帮助公司规避商务电子邮件入侵和冒充CEO身份欺诈的风险。



确保公司所有IT资产（包括远程办公使用的笔记本电脑）都已安装重要补丁，并更新防火墙和杀毒软件。您需要意识到，在疫情期间，网络犯罪集团会利用信息系统维护的漏洞发起攻击。

公司需要确保对所有关键系统进行备份，并对备份的完整性进行校验。理想情况下，需要定期安排备份的离线存储。同时由于犯罪分子会利用疫情进行网络钓鱼攻击，公司还需要警惕勒索病毒的风险在不断增加。

最后，您还需要与应急响应和危机管理部门通力合作，确保公司拥有备用语音和视频会议系统。当公司遇到勒索病毒攻击导致系统服务中断，这些备用系统将起到关键的作用。此外，当主要的会议系统出现过载或者无法使用的情况，备用方案也会提供额外的支持。

联系我们

浦军华

法证咨询主管合伙人

毕马威中国

Tel: +86 (21) 2212 3780
Email: paul.pu@kpmg.com

刘达恺

法证咨询与网络应急合伙人

毕马威中国

Tel: +86 (21) 2212 3371
Email: dakai.liu@kpmg.com

金毅

法证咨询合伙人

毕马威中国

Tel: +86 (21) 2212 3266
Email: kevin.y.jin@kpmg.com

Ravindranath Patil

网络应急总监

毕马威中国

Tel: +852 2826 7295
Email: ravindranath.patil@kpmg.com

朱锴

法证咨询总监

毕马威中国

Tel: +86 (10) 8553 3650
Email: clark.zhu@kpmg.com

张林

法证咨询总监

毕马威中国

Tel: +86 (21) 2212 3153
Email: carter.zhang@kpmg.com

kpmg.com/cn/socialmedia

有关毕马威中国办事处的名单，请扫描二维码或访问我们的网站：
https://home.kpmg.com/cn/en/home/about/offices.html.