世界卫生组织

执 行 委 员 会
第一四八届会议
临时议程项目 18.1

EB148/30
2021 年 1 月 11 日

信息管理和技术最新情况

总干事的报告

1. 在 2020 年 1 月执委会规划、预算和行政委员会第三十一次会议上，秘书处报告了其开展的网络安全活动情况[1]。此外，规划、预算和行政委员会第三十二次会议审议了内审计员最近提交的报告。内审计员报告阐述了网络安全路线图审计工作的各项重要内容[2]。秘书处应规划、预算和行政委员会的要求编写了本份网络安全管理情况报告。

在大流行之前取得的进展

2. 网络安全是信息管理和信息技术战略的一大工作领域，用于保护秘书处的数字资产，加强数据安全，确保具备以可接受的风险水平提供服务的能力。

3. 为加强网络安全而采取的举措有：强制实施全组织网络安全意识培训；每月例行开展反“网络钓鱼”操练；发起年度网络安全意识活动；建立信息系统日志中央储存库，以备查索；防火墙管理标准化；部署全球应对电脑病毒方案；提供互联网流量过滤服务；收集风险情报，采取积极措施，以防未来发生本可避免的事件。

4. 秘书处还设立了一个专门和独立的网络安全小组。此外，它还在着手建立一处实用的综合安全行动中心，以开展识别、预防、发现和保护工作，应对网络攻击。

5. 通过采取以下措施加强了治理结构：公布了经核准的网络安全战略、网络安全路线图和全球政策、规则、标准和标准作业程序；设立了网络安全委员会；修订了全球信息技术指导委员会章程，使该委员会能够根据需要全盘负责网络安全事务。

[1] 文件 EB146/40。
[2] 文件 A73/28。

在 COVID-19 疫情期间应对攻击

6. 据秘书处观察，自宣布 COVID-19 大流行以来，有针对性的网络攻击事件日益增多。冒名顶替、鱼叉式网络钓鱼和其他形形色色的网络钓鱼（包括语音网络钓鱼）以及对信息技术基础设施和应用程序的攻击事件持续不断。2020 年 3 月至 5 月，注册的与 COVID-19 相关的域名高达 13 万以上，据研究人员估计其中 70%为假域名，用于反复发动网络攻击。

7. 网络攻击的复杂性大大加剧，而且数量继续显著增加。最初的威胁情报解决方案有所不足。于 2020 年 5 月 7 日采用新的解决方案后，发现了来自黑客高手持续不断的进一步威胁，秘书处得以较快调整现有的信息技术基础设施、系统和工具。

8. 根据网络安全专业公司进行的趋势分析，预计网络攻击事件将持续不断。需要不断加紧努力，识别、预防、防范、发现和应对这些网络攻击，并在受到网络攻击后恢复正常运转。秘书处为此加快了网络安全规划的实施工作。**已采取重要行动**，包括采取了下文所述的各项行动。

(a) **筹资。**内审计员 2020 年 10 月公布的报告[1]指出，130 万美元经费不足以实施网络安全路线图。全球信息技术指导委员会为此又提供了 470 万美元，拨款总额达 600 万美元。

(b) **网络安全小组。**网络安全小组人员从 6 名增至 11 名，部署在日内瓦和布达佩斯。成立了一个“红色小组”，负责主动大力采取行动检查信息技术系统安全性，包括识别系统漏洞和进行风险评估。

(c) **设立了综合安全管理行动中心。**于 2020 年 6 月设立了一处安全管理行动中心，整合了安全行动与安全信息和事件管理服务。该中心负责关注所有安全事件，协助秘书处重点处理严重的安全事件。2020 年 8 月至 11 月期间，发现的安全事件总数为 145 亿件。随着安全行动中心投入运转，秘书处过滤、关注、分析和集中处理了 243 起严重安全事件。

(d) **妥善验证用户身份。**秘书处正采用多重认证手段（例如软令牌）增强传统认证方法（如用户名和密码认证），以证明用户身份。已完成对秘书处通过因特网提供的所有服务的多重认证项目。

[1] 文件 A73/28。

(e) **持续监测本组织的信息技术资产。**秘书处根据需要实施了端点检测和应对解决方案，通过使用有关工具识别、遏制（如有必要）和调查可疑活动，持续监测和应对本组织信息技术资产面临的威胁。它增强了整个工作环境的安全性，创建了及时识别、保护和应对的能力。迄今已覆盖本组织88%的计算机和服务器。正开展工作，力求到2021年第二季度实现100%覆盖率。

(f) **建立系统，防止发生冒充本组织向公众发送电子邮件行为。**以@<who.int>名义发送的邮件平均每月达230万封。2020年4月，这些邮件中约有80%是冒名发送的邮件。秘书处于2020年5月实施了基于网域的消息认证、报告和一致性（DMARC）解决方案，以尽量减少这种行为，仅允许已获授权者以本组织名义发送消息。此后，96%的电子邮件为合规邮件，4%的电子邮件是冒名邮件，已予删除，使其无法送达已实施DMARC解决方案的各机构的邮箱。

(g) **停用旧版应用程序。**使用过时技术开发的旧系统容易受到恶意攻击。采用了安全修补程序，但在某些情况下，由于系统设计和构架已过时，此类修补程序不足以抵御恶意攻击。秘书处为此更换了大量无法再补救或修补的应用程序。

9. 为有效管理网络安全规划，需要不断进行沟通和协调。特别是：

(a) 由网络安全团队负责全球内部协调。该团队由网络安全小组和各区域的代表组成。网络安全团队协调世卫组织开展的与网络安全有关的活动，其中包括实施网络安全程序、标准和解决方案；

(b) 与众多计算机应急团队、政府机构和私营公司建立了直接联络渠道，以便接收和分享有价值的威胁情报。每天都会相互分享“失陷标识”。

10. 此外，持续监控全组织系统和应用程序（包括全球管理系统、电子邮件、网站、协作平台、开发平台），并毫不拖延地应用安全修补程序，减少或消除网络安全风险。

持续开展网络安全工作

11. 破坏和攻击网络安全行为如果成功，会造成高昂代价。可能造成的代价有：秘书处的价值和声誉受损；直接财务损失（补救、工作时间、法律费用、公关费用和通知费用等）；影响系统的运作；关键数据丢失；并影响数据可靠性。

12. 尽管秘书处作出这些努力，但仍存在差距，还有一些领域的工作尚需改进。以下八个新的工作领域对于保护秘书处免受黑客长期持续威胁至关重要，已被列入网络安全规划范畴。

(a) **通过安全链接和附件进一步保护电子邮件。**超过90%的网络攻击使用链接和附件，开始进行电子邮件网络钓鱼。内置电子邮件安全功能增强了对电子邮件附件的自动检查，通过检查恶意内容和验证电子邮件中的点击时间提供保护。

(b) **增强互联网使用的安全性。**使用全球云代理服务有助于保护在本组织办公室内外访问互联网的端点设备，通过提供网站验证、过滤和防范恶意软件，建立对端点设备上网控制。

(c) **应用程序漏洞扫描。**这将在开发、测试和操作期间为移动应用程序和网络应用程序提供一致和更好的安全评估，以识别系统、网络和应用程序的漏洞。

(d) **网络应用程序防火墙。**这是对网络应用程序提供的新一代保护。网络应用程序防火墙是网络应用程序与互联网之间的屏障和通道，可防止应用程序受到攻击，并对外部访问进行跟踪、过滤和监视。

(e) **漏洞跟踪控制**。这能够创建在线自动验证和报告系统，与事件、更改和修补程序管理流程结合起来。它有助于补救那些未修补系统和应用程序的漏洞。

(f) **特许访问管理。**这不仅使本组织能够了解各种类型的特许访问可能构成的威胁，而且通过采用适当的工具，使本组织能够防止高权限帐户（如系统管理员）滥用权力行为。

(g) **妥善管理责任分工。**这能确保在访问系统方面明确划定职责和作用。在任何情况下都不应允许任何人既能发起交易又能批准交易，以防网络犯罪（通过盗窃或欺诈谋取私利）。

(h) **欺骗技术。**这指的是设置陷阱或诱饵，诱使黑客误以为已打入本组织（窃取身份或机密等）。这将提高秘书处识别外部入侵者行为的能力，并利用这些知识加强系统的安全。

13. 保持良好势头至关重要。将这些工作领域纳入秘书处网络安全工作将进一步加强识别、发现、预防、保护和应对方式，有助于实施网络安全路线图。

可持续供资

14. WHA70(16)号决定（2017 年）授权总干事在每个双年度结束时，在可行情况下，为基础设施基金内的信息技术投资需要划拨至少 1500 万美元的资金[1]。目前的网络安全规划由基础设施基金供资。

15. 秘书处认为网络安全是高度优先事项。必须维持迄今作出的一切努力，并继续开展工作，以维护本组织的运作。已初步估算了完成网络安全规划所需的费用。但在完成该规划后，为维持网络安全工作，还需今后投入大量资金。

16. 独立专家监督咨询委员会建议，应在总体规划周期对本组织的信息技术支出进行全面审查[2]。不仅应审查秘书处业务运作费用，还应审查信息技术领域各项变革举措，包括网络安全措施。在编列 2022-2023 年规划预算方案草案过程中，秘书处目前正在开展这项审查。

17. 秘书处将通过规划、预算和行政委员会第三十四次会议向会员国提供现行业务与变化情况，包括对今后信息技术支出的最新全面审查结果。

执行委员会的行动

18. 请执委会注意本报告。

= = =

[1] 见文件 WHA70/2017/REC/1。
[2] 见文件 EBPBAC30/2。