CYBERX

COVID-19: Keep Calm and Monitor Your Remote Access

https://cyberx-labs.com/blog/cyberx-response-to-covid-19/

冷靜並監視環境的遠端存取

首先，在由 COVID-19 全球大流行引起的危機時刻，CyberX 希望我們的朋友，家人，客戶以及整個網路安全社區的健康和安全。

據我們所知，疾病預防控制中心（CDC）建議通過社會隔離來防止 COVID-19 傳播。 因此企業鼓勵或要求其僱員在家工作 。對於傳統的 IT 安全公司而言，我們處於非常模式 — 必須嘗試採取其他措施，並努力遵守 COVID-19 帶來的新挑戰。

我們能做什麼？ CyberX 建議採取三種行動方案：

1. **監視與 IoT / ICS 網路的所有遠端連接以及可能的橫向移動，並警告出現在網路上的 RDP、SSH 或 VNC 上的新連接或異常連接。**頭號攻擊者是使用從員工或第三方竊取的有效憑據（例如，通過網路釣魚）存取您的 IoT / ICS 網路的攻擊者。如果不確定是否啟用了此警報功能，請聯繫您的服務廠商或通過 support@cyberx-labs.com 給我們資訊以進行查找。

2. **實施具有現代功能（如 2FA，審計跟踪和密碼庫）的安全形式的遠端存取。** 其中包括來自我們的系統整合夥伴 CyberArk 以及其他服務（例如 BeyondTrust）的特權存取管理（PAM）解決方案。

3. **確保您的 IoT / ICS 安全性與其他 IT 安全性整合在一起。** 我們可以幫助您與合作夥伴解決方案整合，例如 Splunk、ServiceNow、IBM QRadar、Microsoft Sentinel 和 Microsoft Azure IoT 安全中心，以及 Fortinet、HP Aruba、Palo Alto、Cisco 和 Waterfall，CyberX 通過 API 與這些解決方案整合，以簡化和自動化事件響應工作流程。 最重要的是，在此期間以更少的人力資源來確保快速響應。

在這些充滿挑戰的時期，我們向您保證 CyberX 盡可能地持續提供最好的支持。

M.TECH
Your Preferred I-Security Partner