T2025_11 Disable Unused Network Ports to Reduce Attack Surfaces (April 10th, 2025)

An important and often overlooked security practice is disabling unused network ports both physical and logical. Open but inactive ports can be exploited by attackers or used for unauthorized access. Network administrators should routinely audit switch and firewall configurations to identify ports that are not actively in use and disable them as a preventive measure.

Additionally, many managed switches and enterprise-grade network equipment offer features such as auto-shutdown or idle-timeout settings, which allow ports to be automatically disabled after a defined period of inactivity (e.g., 24 or 48 hours). Enabling these settings ensures that ports are not left open unnecessarily, especially in environments where devices are frequently moved or disconnected. This approach helps minimize your attack surface and strengthens overall network security.

References

- Administrator, T. W. (2025, January 2). Why is it essential to disable or safeguard inactive ports in OT environments? Retrieved from Mangan Cyber Security. https://www.mangancyber.com/why-is-it-essential-to-disable-or-safeguard-inactive-ports-in-ot-environments/
- What is an Attack Surface? Definition and How to Reduce It | Fortinet. (n.d.). Retrieved from Fortinet. https://www.fortinet.com/resources/cyberglossary/attack-surface