Seguridad y Ciberseguridad en "Academia Futura Tech"

Dada la especialización tecnológica de la Academia Futura Tech y las limitaciones actuales identificadas (red desorganizada, seguridad segmentada débil, falta de documentación y mantenimiento), la ciberseguridad es crítica. Este análisis se centra en el laboratorio principal, que es el foco del proyecto.

Análisis de Posibles Vulnerabilidades del Laboratorio Principal

Vulnerabilidad de Segmentación Insuficiente:

Escenario: Si la red del laboratorio no está correctamente aislada (VLANs, ACLs) del resto de la red de la academia (administración, profesores), un ataque exitoso en un PC del laboratorio podría permitir el "salto" a segmentos más sensibles, comprometiendo datos críticos o sistemas de gestión.

Causa Raíz: La "seguridad segmentada por áreas" actualmente deficiente y la "organización de la red" limitada.

Vulnerabilidad por Configuraciones Débiles o Desactualizadas:

Escenario: PCs de laboratorio o dispositivos de red (switches, APs) con software/firmware obsoleto, contraseñas por defecto o débiles, puertos abiertos innecesarios, o servicios expuestos. Esto es exacerbado por la "ausencia de políticas de mantenimiento y escalabilidad" y la falta de "documentación técnica estructurada".

Impacto: Permite la explotación de vulnerabilidades conocidas o el acceso no autorizado a la configuración de los dispositivos.

Vulnerabilidad en Puntos Finales (PCs de Laboratorio):

Escenario: Infección por malware a través de USBs, descargas o ingeniería social. Falta de control granular sobre las acciones de los usuarios (ej. instalación de software no autorizado) en los PCs compartidos.

Riesgo: Pérdida de datos, propagación de malware dentro del laboratorio, uso del PC como plataforma de ataque.

Vulnerabilidad por Factor Humano / Ingeniería Social:

Escenario: Estudiantes o personal de laboratorio cayendo en trampas de phishing para revelar credenciales de acceso a la plataforma e-learning o a la red.

Causa Raíz: Posible falta de "políticas de uso y protección de datos" claras y concientización.

Blue Team (Defensa y Prevención - Propuestas del Proyecto)

El Blue Team diseña e implementa defensas. En el alcance del proyecto, esto se traduce en propuestas para:

Segmentación Robusta:

Diseño: Creación de una VLAN específica para el laboratorio principal.

Control: Configuración de ACLs en el switch de capa 3 (simulado) y en el firewall perimetral (simulado) para restringir el tráfico del laboratorio únicamente a los servicios autorizados (e.g., Internet, plataforma e-learning, DNS, DHCP) y prohibir estrictamente el acceso a otras VLANs sensibles.

Direccionamiento: Implementación de subnetting eficiente dentro de la VLAN del laboratorio.

Hardening de Dispositivos y Servicios:

Configuraciones Seguras: Propuestas de configuraciones seguras para los switches y routers simulados (cambio de contraseñas por defecto, deshabilitación de servicios innecesarios, uso de SSH para gestión).

Reglas de Firewall: Definición de reglas de tráfico específicas en el firewall perimetral (simulado) que aplican a la VLAN del laboratorio, minimizando la superficie de ataque.

Parches y Actualizaciones (Recomendación): Documentar la necesidad de un plan de mantenimiento (3.5.4) para mantener actualizados los PCs de laboratorio y el firmware de los dispositivos de red.

Seguridad en Puntos Finales (Recomendación):

Cuentas de Usuario: Proponer el uso de cuentas de usuario con privilegios limitados para los estudiantes en los PCs del laboratorio.

Antivirus/EDR: Recomendar la implementación de una solución de seguridad de endpoint centralizada.

Control de Puertos: Proponer la deshabilitación o control de puertos USB no esenciales en los PCs de laboratorio.

Conciencia y Políticas:

Políticas de Uso: Desarrollar "recomendaciones de políticas de uso y protección de datos" para estudiantes y personal sobre el uso seguro del laboratorio y la red.

Documentación: Asegurar que todas las configuraciones de seguridad propuestas estén documentadas de manera estructurada para facilitar el mantenimiento y la auditoría.