TECNICATURA UNIVERSITARIA EN PROGRAMACIÓN

UNIVERSIDAD TECNOLÓGICA NACIONAL

ARQUITECTURA Y SISTEMAS OPERATIVOS

UNIDAD 6 - ASPECTOS DE SEGURIDAD

GUÍA PRÁCTICA N° 9

PROFESORA: GONZALES TERESITA

ALUMNOS:

Barcos Lía

Blanco West Fabián

Centurión Tomás

Derfler José

Portillo Anahí

Rahn Ana

Rojas Yasmín

Reflexión sobre Panorama de Amenazas en nuestra Vida Digital

Introducción

La revolución digital ha transformado nuestras actividades diarias, desde la comunicación hasta las finanzas. Sin embargo, este avance ha traído consigo un aumento de riesgos relacionados con la seguridad de nuestra información. Tecnologías avanzadas como la inteligencia artificial (IA) han facilitado no solo la automatización y mejora de procesos, sino también la proliferación de amenazas como los deepfakes y la clonación de voz, que los ciberdelincuentes aprovechan para perpetrar fraudes y suplantaciones. Este informe reflexiona sobre las principales amenazas digitales, haciendo énfasis en los riesgos asociados a estas tecnologías, y sugiere estrategias de mitigación en el contexto de ciberseguridad.

La Información como Activo Estratégico

La información digital es un activo de valor económico y estratégico. Cada interacción en línea genera datos que son explotados tanto por empresas legítimas como por ciberdelincuentes. Estos últimos se han consolidado como "adoptadores tempranos" de tecnologías, como menciona Mark Goodman en Futures Crimes: “Cuando aparecen nuevas tecnologías, también aparecen nuevos riesgos”.

Durante la pandemia de COVID-19, este panorama se agravó, con un notable aumento de amenazas como el acceso no autorizado a cámaras web y el uso de deepfakes para fraudes. Estas tecnologías permiten a los atacantes construir perfiles completos de sus objetivos a partir de datos públicos y privados, exponiendo información sensible como ubicaciones, preferencias y relaciones personales.

IA y las Amenazas de Imitación de Voz y Rostro

Entre las tecnologías más alarmantes están los deepfakes y la clonación de voz. Estas herramientas, basadas en IA, replican patrones vocales y expresiones faciales con una precisión asombrosa, facilitando estafas personalizadas, desinformación y daños a la reputación. Los ataques de "SIM swap", combinados con voces clonadas, han permitido a delincuentes acceder a cuentas bancarias y datos personales, aprovechándose de sistemas de autenticación débil.

Además, el mercado negro de grabaciones obtenidas a través de hackeos de cámaras web ha crecido, evidenciando la urgencia de fortalecer los controles de acceso y la gestión de

permisos en los sistemas operativos. Estas amenazas están directamente vinculadas con la arquitectura de sistemas, que debe garantizar una segmentación adecuada y la implementación de medidas como la criptografía para proteger la información.

El Rol Fundamental de los Programadores en la Ciberseguridad

En este entorno de amenazas crecientes, los programadores tienen un papel clave en la creación de sistemas seguros. Más allá del desarrollo de aplicaciones funcionales, los programadores deben incorporar principios de ciberseguridad desde las etapas iniciales del diseño.

Esto incluye:

- Implementar autenticación robusta y cifrado para proteger datos sensibles.
- Asegurar que las aplicaciones no tengan vulnerabilidades comunes, como inyecciones SQL o fallos de validación de entradas.
- Diseñar arquitecturas resilientes que minimicen los puntos únicos de fallo y faciliten la recuperación frente a ataques.

Además, el conocimiento sobre normativas y estándares de seguridad, como el RGPD (Reglamento General de Protección de Datos) o el estándar OWASP (Proyecto de Seguridad de Aplicaciones Web Abiertas), es esencial para garantizar que las soluciones tecnológicas cumplan con las expectativas legales y éticas.

La educación continua en ciberseguridad permite a los programadores anticiparse a las tácticas de los ciberdelincuentes y desarrollar sistemas más resilientes. Esto no solo reduce la exposición de los usuarios a amenazas, sino que también fortalece la confianza en el uso de tecnologías digitales.

Buenas Prácticas para la Protección Digital

Adoptar buenas prácticas de ciberseguridad es esencial para mitigar estos riesgos. Algunas de las estrategias más recomendadas incluyen:

- Contraseñas robustas: Utilizar combinaciones únicas para cada plataforma.
- Autenticación de dos factores (2FA): Aumentar la seguridad en cuentas críticas.
- Actualización de sistemas: Mantener software y dispositivos protegidos frente a vulnerabilidades conocidas.

- Educación continua: Concienciar a usuarios y organizaciones sobre amenazas emergentes y herramientas de detección.

Por otra parte, se están desarrollando algoritmos avanzados para detectar deepfakes y otras imitaciones generadas por IA, aunque la carrera entre creación y detección de estas tecnologías sigue siendo intensa.

Conclusión

En una era donde la información digital tiene un valor incalculable, la ciberseguridad debe ser prioritaria. Las tecnologías emergentes, como los deepfakes y la clonación de voz, representan una dualidad: por un lado, ofrecen oportunidades innovadoras; por otro, desafían nuestra capacidad de protegernos frente a su mal uso.

Los programadores, como creadores de las herramientas tecnológicas que forman parte de nuestra vida diaria, tienen la responsabilidad de garantizar que estas sean seguras y éticas. Incorporar ciberseguridad en el desarrollo de software y educarse continuamente en nuevas amenazas es fundamental para construir un entorno digital confiable. La combinación de diseño robusto de sistemas, educación en seguridad digital y desarrollo de regulaciones permitirá minimizar los riesgos y asegurar un entorno digital más confiable para todos.