Conferencia No. 7

Tema: Ciberseguridad
Conferencista: Frederick Nicolai Ferro Mojica
Fecha: sábado 27 de mayo de 2023
Hora: 11:00 a.m. a 12:45 p.m.

El ponente comenzó su presentación hablando sobre los orígenes de los hackers y los primeros ataques registrados en la historia. Mencionó que los primeros ataques surgieron con la convergencia de las tecnologías de telégrafo para detectar las comunicaciones. A medida que avanzaba la tecnología, surgieron ataques a los sistemas. También mencionó al primer hacker conocido como Mil.

Luego, el ponente se centró en los conceptos básicos de ciberseguridad. Explicó que la ciberseguridad se refiere a las prácticas y medidas tomadas para proteger los sistemas informáticos y los datos contra amenazas cibernéticas. Estas amenazas pueden incluir ataques de hackers, malware, robo de identidad, entre otros. Resaltó la importancia de la ciberseguridad tanto para las organizaciones como para las personas individuales.

Además, el ponente mencionó algunos protocolos ampliamente utilizados en ciberseguridad. Uno de estos protocolos es IPv6 (Internet Protocol versión 6), que es la última versión del protocolo de comunicación de Internet. IPv6 tiene como objetivo resolver el agotamiento de direcciones IP en IPv4 y ofrece mejoras en seguridad, escalabilidad y eficiencia de la red. Sin embargo, es importante tener en cuenta que existen muchos otros protocolos utilizados en ciberseguridad, como HTTPS, SSL/TLS, IPsec y SSH, que proporcionan capas adicionales de seguridad en diferentes niveles de comunicación.

Después de abordar estos conceptos básicos y protocolos, el ponente concluyó enfatizando la importancia de implementar medidas de ciberseguridad adecuadas para reducir los riesgos y proteger la información sensible. Además, señaló que la analítica de datos desempeña un papel fundamental en la ciberseguridad debido a varias razones importantes:

Detección de amenazas: La analítica de datos permite identificar patrones, anomalías y comportamientos sospechosos en grandes volúmenes de datos. Al analizar el tráfico de red, los registros de eventos, las actividades del sistema y otros datos relevantes, se pueden detectar signos de posibles amenazas cibernéticas, como intrusiones, ataques de malware o intentos de robo de datos. Esto ayuda a las organizaciones a tomar medidas preventivas y responder de manera oportuna antes de que se produzcan daños significativos.

Prevención de fraudes: La analítica de datos también desempeña un papel crucial en la prevención de fraudes. Al analizar patrones de transacciones, comportamientos de usuarios y otros datos relacionados, es posible identificar transacciones sospechosas o actividades fraudulentas en tiempo real. Esto permite a las organizaciones tomar medidas rápidas para bloquear transacciones fraudulentas y proteger los activos financieros.

Gestión de incidentes: La analítica de datos es fundamental en la gestión de incidentes de seguridad. Al recopilar y analizar datos relevantes, como registros de eventos, registros de acceso y registros de auditoría, se puede obtener una visión completa de un incidente de seguridad, su origen, alcance e impacto. Esto ayuda a los equipos de respuesta a incidentes a comprender mejor la naturaleza de la amenaza, tomar decisiones informadas y coordinar una respuesta efectiva para minimizar los daños y restaurar la seguridad.

Mejora de la postura de seguridad: La analítica de datos permite realizar análisis exhaustivos de seguridad y evaluar la postura general de seguridad de una organización. Al analizar datos de vulnerabilidades, métricas de cumplimiento, registros de incidentes y otros datos relevantes, se pueden identificar brechas de seguridad y áreas de mejora. Esto permite a las organizaciones tomar decisiones basadas en datos para fortalecer su infraestructura de seguridad, implementar medidas preventivas adicionales y mejorar su capacidad de respuesta ante posibles amenazas.