Análisis de Servicios de Seguridad

SEGURIDAD INFORMATICA SEMESTRE 8 19:00-19:55

UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

PARCIAL 1

Profesor: Servando López Contreras

LUIS EDUARDO AZNAR CUEVAS 179880

ACTIVIDAD 02- Análisis de servicios de seguridad

Introducción

El análisis de los servicios de seguridad constituye una base fundamental para garantizar la protección de la información, la continuidad operativa y la confianza en las comunicaciones digitales. La recomendación ITU-T X.800, también conocida como Arquitectura de Seguridad para OSI, proporciona un modelo conceptual ampliamente reconocido para la seguridad de las comunicaciones. Por su parte, la RFC 4949, titulada Internet Security Glossary, complementa este enfoque al ofrecer un glosario normalizado de términos y conceptos de seguridad informática utilizados en el ámbito de Internet.

Escenario 01.

Elemento	Respuesta
Servicios X.800	Autenticacion
Definiciones aplicables RFC 4949	Ransomware Data breach
Tipo de amenaza	Externa
Vector de Ataque	Malware
Impacto Tecnico/Operativo	Perdida de recursos y de integridad de los datos
Medida de Control recomendada	Cifrado de datos

Escenario 02.

Elemento	Respuesta
Servicios X.800	Control de Acceso
Definiciones aplicables RFC 4949	Exposure Unauthorized
Tipo de amenaza	Externa
Vector de Ataque	Cifrado débil
Impacto técnico/Operativo	Perdida de integridad de datos
Medida de Control recomendada	Auditorias

Escenario 03.

Elemento	Respuesta
Servicios X.800	Integridad de datos
Definiciones aplicables RFC 4949	Trust exploitation
Tipo de amenaza	Externa
Vector de Ataque	Cifrado débil

Impacto técnico/Operativo	Perdida de confianza e integridad de los equipos
Medida de Control recomendada	Verificacion y cifrar datos

Escenario 04.

Elemento	Respuesta
Servicios X.800	Confidencialidad de datos
Definiciones aplicables RFC 4949	Phishing Authentication error
Tipo de amenaza	Externa
Vector de Ataque	Amenaza interna
Impacto técnico/Operativo	Perdida y filtración de informacion
Medida de Control recomendada	MFA

Escenario 05.

Elemento	Respuesta
Servicios X.800	Disponibilidad
Definiciones aplicables RFC 4949	Destruction Availability attack
Tipo de amenaza	Externa
Vector de Ataque	Malware
Impacto técnico/Operativo	Perdida de información total
Medida de Control recomendada	Respaldos constantes

Escenario 06.

Elemento	Respuesta
Servicios X.800	Confidencialidad de datos
Definiciones aplicables RFC 4949	Insider threat
Tipo de amenaza	Interna
Vector de Ataque	Amenaza interna
Impacto técnico/Operativo	Riesgo de mas ataques y perdida de recursos
Medida de Control recomendada	Restringir acceso a informacion

Escenario 07.

Elemento	Respuesta
Servicios X.800	Integridad de datos y no repudio
Definiciones aplicables RFC 4949	Evidentiary integrity
Tipo de amenaza	Externa
Vector de Ataque	Credenciales Comprometidas
Impacto Tecnico/Operativo	Perdida de informacion
Medida de Control recomendada	MFA y respaldos

Escenario 08.

Elemento	Respuesta
Servicios X.800	Disponibilidad
Definiciones aplicables RFC 4949	Operational failure Service disruption
Tipo de amenaza	Interna
Vector de Ataque	Vulnerabilidad
Impacto Tecnico/Operativo	Falta de disponibilidad a los servicios
Medida de Control recomendada	Prevención de ataques

Escenario 09.

Elemento	Respuesta
Servicios X.800	Autenticacion
Definiciones aplicables RFC 4949	Phishing
Tipo de amenaza	Externa
Vector de Ataque	Suplantacion de identidad
Impacto Tecnico/Operativo	Filtracion de informacion
Medida de Control recomendada	MFA

Escenario 10.

Elemento	Respuesta
Servicios X.800	Integridad de los datos
Definiciones aplicables RFC 4949	Data destruction
Tipo de amenaza	Externa
Vector de Ataque	Acceso a sistemas e integridad de los datos
Impacto Tecnico/Operativo	Perdida de datos
Medida de Control recomendada	Respaldos constantes

CONCLUSION

Los análisis de seguridad con ayuda de los servicios x.800 y la nomenclatura dada por rfc 4949 permite a la ciberpolicia prevenir la perdida de recursos por los ciber ataques, ya que los análisis pueden predecir ataques o nulificar completamente los ataques consecuentes si se toman las medidas de prevención recomendadas.

Esta actividad nos permite estudiar los servicios del estándar X.800 de ITU y los mecanismos de seguridad del mismo, también sobre el glosario RFC 4949 con casos reales y el uso de ello.

REFERENCIAS

Documento RFC 04949

Link hacia ITE-T para descargar X.800