Ministerio del Interior y Seguridad Pública

Gobierno de Chile

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Agenda/Simposio 2021

	08:45	**Registro en la Plataforma**	
am	9:00-9:15	**Ceremonia de apertura.**	Juan Francisco Galli Basili, Subsecretario del Interior
am	9:15-10:00	**Charla 1**	Director CSIRT Sr Carlos Landeros
am	10:00-10:55	**Taller 1: Usando un SIEM (opensource): WAZUH**	Hernan Espinoza Analista CSIRT
am	11:00- 11:55	**Taller 2: Usando un HONEY-POT (opensource): T-POT**	Miguel Kurte Analista CSIRT
pm	12:00- 12:30	**Charla 2: Seguridad en sitios web (introducción teórica) [1/3]**	Natalia Perez Analista CSIRT
pm	12:35- 13:35	**Taller 3 (primera parte): Seguridad en sitio web (herramientas y verificación práctica) [2/3]**	Juan Sanhueza Analista CSIRT
pm	14:30-15:25	**Taller 3 (segunda parte): Seguridad en sitio web (herramientas y verificación práctica) [3/3]**	Juan Sanhueza Analista CSIRT
pm	15:30- 16:25	**Charla 3: Controles para mitigar amenazas en ciberseguridad (30 controles prioritarios)**	Gonzalo Conch Analista CSIRT
pm	16:30- 17:25	**Revocación de nombres de dominio**	Cristobal Hammersley Abogado CSIRT
pm	17:30-17:40	**Cierre del evento**	

Charla Magistral Director CSIRT

Exponente: Carlos Landeros

Tema: Ciberseguridad en el Estado, análisis del nuevo marco normativo.

Objetivo: Introducir temas sensibles y de importancia contextual para la ciberseguridad de las instituciones públicas. Comentar la nueva institucionalidad que se avisora para la ciberseguridad del país, plasmada en el proyecto de Ley Marco de Ciberseguridad e Infraestructuras críticas de la Información.

Taller 1: Usando un SIEM (opensource): WAZUH

Exponente: Hernán Espinoza

Tema: Instalación de un sistema SIEM de código abierto y sus usos para la ciberseguridad.

Objetivo: Mostrar el concepto de SIEM en ciberseguridad y como se puede aplicar para descubrir potenciales acciones maliciosas que están ocurriendo en la red institucional (perímetro externo o interno). WAZUH per mite integrar a diferentes equipos internos y externos mediante el uso de agentes con toman los logs y los envían al concentrador principal. Con esta herramienta de código abierto es posible implementar un esquema de correlación de eventos que facilite a los administradores de ciberseguridad encontrar eventos de ciberseguridad relevantes en su ecosistema.

Taller 2: Usando un HONEYPOT (opensource): T-POT

Exponente: Miguel Kurte

Tema: Instalación de un sistema HONEYPOT de código abierto y sus uso para ciberseguridad.

Objetivo: Mostrar el concepto de HONEYPOT o señuelo en ciberseguridad y como se puede aplicar para descubrir potenciales acciones maliciosas que están ocurriendo en la red institucional (perímetro externo o interno), tales como ataques de fuerza bruta por sistemas automatizados, escaneos de puertos y nombres de usuarios o contraseñas que están intentando explotar. T-POT permite simular diferentes equipos expuestos a Internet tales como un firewall, un servidor de correo electrónico, un computador con escritorio remoto, un acceso remoto del tipo SSH, entre otros, los que son miel que atrae a los ciberdelincuentes para intentar explotarlos.

Charla 2: Seguridad en sitios web (introducción teórica)

Exponente: Natalia Pérez

Tema: Contextualización de la seguridad, amenazas y vulnerabilidades de sitios y sistemas web.

Objetivo: Ilustrar un marco teórico de las amenazas y vulnerabilidades que se ciernen sobre los sitios y sistemas web de las instituciones, para que la aplicación práctica a continuación sea más fácilmente digerible por la audiencia (Talleres 3 y 4).

Temario Inicial:
- ¿Qué presencia en internet buscan los actores maliciosos?
- ¿Cómo se construye esa presencia en internet de sitios y sistemas web?
- ¿Qué es una amenaza?
- ¿Qué es una vulnerabilidad?
- ¿Qué es impacto?
- Descripción general del concepto riesgo (impacto v/s probabilidad)
- ¿Qué daños o impactos puede facilitar un sistema desprotegido?
- ¿Existe una taxonomía?

Taller 3 (Primera Parte): Seguridad en sitio web herramientas y verificación práctica

Exponente: Juan Sanhueza

Tema: Herramientas para detectar vulnerabilidades, como verificar su existencia y su correcta mitigación.

Objetivo: Ilustrar de manera práctica como detectar las vulnerabilidades más recurrentes en nuestros sitios o sistemas web institucionales, utilizando herramientas opensource.

Taller 3 (Segunda Parte): Seguridad en sitio web herramientas y verificación práctica

Exponente: Juan Sanhueza

Tema: Herramientas para detectar vulnerabilidades, como verificar su existencia y su correcta mitigación.

Objetivo: Ilustrar de manera práctica como detectar las vulnerabilidades más recurrentes en nuestros sitios o sistemas web institucionales, utilizando herramientas opensource.

Charla 3: Controles para mitigar amenazas en ciberseguridad

Exponente: Gonzalo Concha

Tema: Contextualización de los principales controles normativos para mitigar riesgos de ciberseguridad.

Objetivo: Ilustrar los principales controles normativos que se pueden aplicar para mitigar los principales riesgos que se han detectado en nuestros ecosistemas digitales, entendiendo que hay un importante proceso de transformación digital del Estado en curso (Ley N°21180) y un escenario de nueva normalidad laboral para las instituciones públicas (impacto indirecto de la Ley N°21220 para el sector privado).

Temario Inicial:
- La importancia de un estándar internacional (ISO 27001 / ISO 27002)
- Dominios que contempla el estándar
- Estrategia de Políticas y Procedimientos
- Principales controles normativos

Charla 4: Revocación de nombres de dominio

Exponente: Cristóbal Hammersley

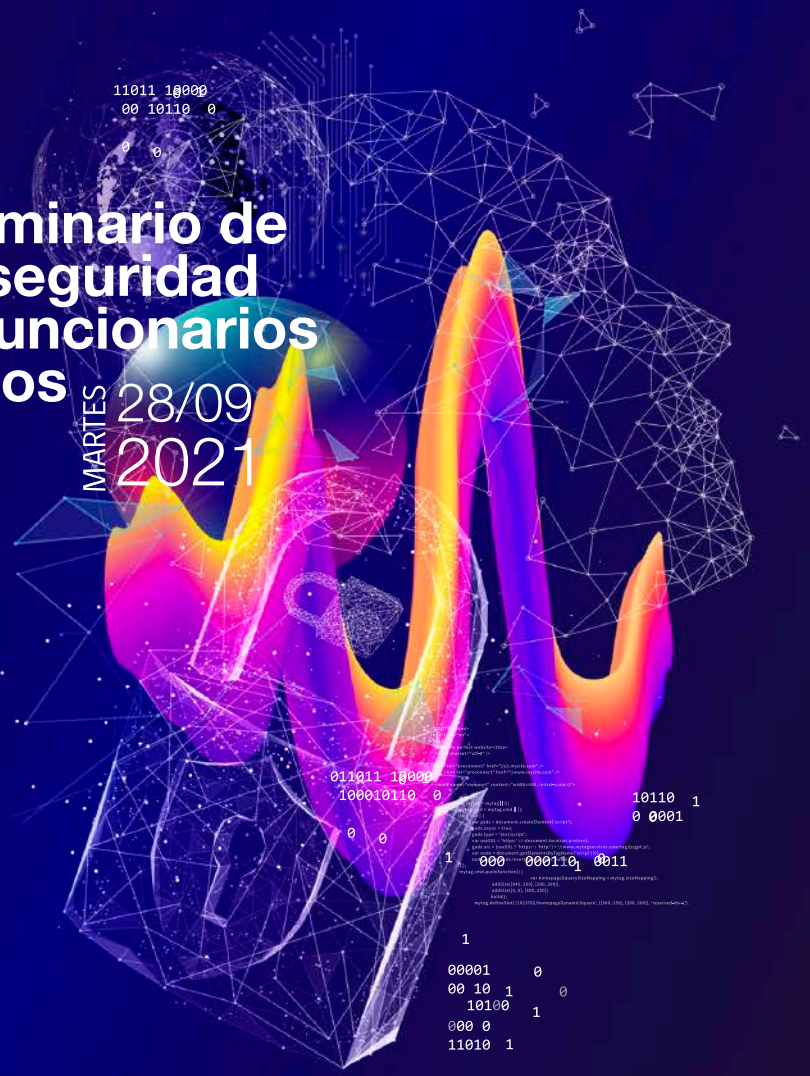
Tema: Procedimiento para revocar nombres de dominio como herramienta para hacer frente a nombres de dominio engañosamente similares o fraudulentos.

Objetivo: Ilustrar los principales beneficios del procedimiento de revocación de nombres de dominio .CL como herramienta para combatir el uso de nombres de dominio similarmente engañosos o fraudulentos en virtud de la política de resolución de controversias de NIC Chile y su uso en conjunto con la herramienta la "campana" desarrollada por el CSIRT GOB. Así como también explicar el paso a paso de los procedimientos disponibles, tanto en su forma temprana como tardía, sus etapas y principios rectores.

Temario Inicial:
- Administración de nombres de dominio
- Conflicto por nombres de dominio
- Revocación temprana
- Revocación tardía
- Criterios para la resolución de conflictos
- Marca vs Nombres de dominio

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile