Mesa de trabajo "Industria de Telecomunicación"

Autor

Agesic

Fecha de creación

26/11/2024

Tipo de publicación

Informes

Resumen

Informe del intercambio realizado en la mesa de trabajo "**Industria de Telecomunicación**" desarrollada en el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad realizada el 2 de agosto 2024.

Introducción

En el marco del proceso de cocreación de la Estrategia Nacional de Ciberseguridad (ENC) de Uruguay, en el mes de junio, julio y agosto 2024 se realizaron diez mesas de diálogo para recoger aportes respecto a la propuesta borrador. Participaron diferentes actores de instituciones públicas, privados, de la sociedad civil y de la academia, para intercambiar ideas que permitan cocrear la ENC. En este espacio se dialogó acerca de la visión y alcance de la Estrategia, así como los principios, objetivos y acciones específicas a impulsar.

En la jornada del 2 de agosto se realizó el análisis de la visión del sector de telecomunicación en materia de ciberseguridad. En este informe se detallan las propuestas y aportes compilados en esta mesa de diálogo.

Este documento presenta en forma sintética los intercambios en esta mesa.

Participantes

En esta mesa participaron 20 personas de 10 instituciones públicas y privadas.

ANDEBU, Ignacio Cersosimo.

ANTEL, Alejandro Ricarte.

ANTEL, Laura Rovira.

ANTEL, Roberto Monzon.

Claro, Anthoy Rincón.

Claro, Hernan Bonjour.

Flow, Gisella Tomasi.

Montecable, Alexis Ochoa.

Montecable, Gabriel Larrosa.

Montecable, Lucia Garmendia.

SPACEX, Emmanuel Cardenas.

TELCO, Diego Alvarez.

Telefónica, Carolina Matos.

Telefónica, Facundo Payssé.

URSEC, Agustin Hill.

URSEC, Fernando Hernandez.

URSEC, Mauro Ríos.

URSEC, Mercedes Aramendia.

URSEC, Nelson Rodríguez.

VCR, Alejandro Fernandez.

Resumen del intercambio

A continuación bajo cada tema identificado se presentan las acciones propuestas en base a lo conversado

Dirección Estratégica de Ciberseguridad

- Adoptar estándares internacionales (MCU, ISO 27001, NIST) para alinear la estrategia de ciberseguridad del sector de Telecomunicaciones.
- Establecer un marco de medición de riesgos que incluya evaluación de la cadena de suministro y control de proveedores.
- Crear un CSIRT (Equipo de Respuesta a Incidentes) sectorial para colaboración e intercambio de información.

Capacitación y Concientización

- Desarrollar programas de capacitación integral para todos los niveles de la organización, con énfasis en concientización sobre amenazas y riesgos.
- Realizar ejercicios de TableTop para mejorar la preparación y comprensión de incidentes de ciberseguridad.
- Implementar una estrategia de educación para clientes que incluya campañas informativas sobre seguridad digital sin recurrir al miedo.

Gestión de Riesgos e Inversiones

- Crear un modelo de inversión en ciberseguridad que considere la medición integral de riesgos en la organización.
- Desarrollar estrategias para abordar la obsolescencia tecnológica y los desafíos de seguridad en entornos de teletrabajo.
- Establecer un programa de gestión de talento específico para ciberseguridad para mitigar la escasez de profesionales en el sector.
- Identificar eventos masivos de alto perfil a realizarse en Uruguay y desarrollar un plan de ciberseguridad específico para ellos, por ejemplo, Mundial 2030.

Seguridad en Equipos y Servicios

- Implementar políticas de seguridad para equipos distribuidos en hogares, incluyendo gestión de contraseñas y actualizaciones.
- Desarrollar servicios adicionales de ciberseguridad para clientes empresariales (B2B) y clientes finales (B2C) como firewalls virtuales, endpoint security y SOC como servicio.
- Utilizar herramientas de monitoreo en tiempo real con alertas y automatización para respuesta rápida.

Comité de Crisis y Comunicación

- Formar un grupo de trabajo intersectorial con protocolos definidos para manejo de incidentes de ciberseguridad.
- Establecer canales de comunicación formales para compartir información sobre amenazas y vulnerabilidades.
- Diseñar protocolos de comunicación y manejo de crisis que garanticen ética y confidencialidad.

Cultura de Seguridad de la Información

- Integrar seguridad de TI con la Seguridad Industrial (OT) para una protección más completa, por ejemplo, de las plantas industriales.
- Realizar simulaciones de eventos extraordinarios (como preparación para eventos masivos) para mejorar resiliencia.

Educación y Concientización del Cliente

- Crear campañas educativas sobre seguridad digital adaptadas a diferentes tipos de personas usuarias.
- Desarrollar materiales informativos que expliquen los riesgos y consecuencias de la falta de ciberseguridad.
- Implementar programas de orientación sobre uso seguro de internet y aplicaciones.

Anexos

A continuación, se presentan sistematizados y sintetizados los temas conversados en la mesa de trabajo “Industria de Telecomunicaciones”.

Dirección Estratégica

Aportes sobre la visión del sector de Telecomunicaciones para el país en materia de ciberseguridad.

- ¿Hacia dónde debería avanzar el sector de Telecomunicaciones en materia de Ciberseguridad?
- Adecuarnos a un estándar, tener un norte hacia donde ir y avanzar hacia ahí, por ejemplo, MCU, 27001.
- Por ley deben cumplir el marco de ciberseguridad, NIST., sino la 27001 que está homologada. Continuar con la exigencia de los procesos de la empresa a nivel de ciberseguridad.
- Evaluar que otras exigencias sumar.
- Certificación externa e interna.
- Control de riesgos (cadena de suministro, control de proveedores).
- Establecer mediciones.
- Tener una actitud reflexiva respecto al equilibrio entre la seguridad y la libertad.
- Desarrollar un canal de comunicación para intercambiar información clave y poder colaborar.
- Desarrollar CSIRT Sectorial.
- Uno de los pilares de la ENC tiene que ver con la educación. Es clave generar conciencia en autoridades y lograr que a nivel político se cuente con los asesores correctos.

Capacitación y Concientización

Concientización y Capacitación de Personal

- Capacitación de todas las personas que trabajan en las empresas, para trabajar sobre las vulnerabilidades.
- Concientizar sobre amenazas y riesgos, no solo hacia la empresa sino hacia la industria.
- Conocer bien los riesgos.
- Las habilidades son importantes, delegar lo técnico y jugar desde otra postura.
- Trabajar en la concientización, especialmente desde los niveles más altos e incluso político.
- Medir el nivel de madurez tomando en cuenta la capa política y los tomadores de decisiones.
- Ejercicios de TableTop para lograr conciencia, educación y conocimiento.
- Capacitación de todas las personas que trabajan en las empresas para concientizar sobre amenazas y riesgos, no solo hacia la empresa sino hacia la industria. Para conocer mejor los riesgos.
- Conciencia de que son la red para que pasen los incidentes, la base.

Educación y Concientización del Cliente

- Como operador en Uruguay, es necesario concientizar. Proveer internet abre una ventana al mundo, y no podemos exponer a los usuarios a ataques como el phishing.
- Es complejo concientizar al cliente final; se puede hacer a través de campañas, publicidades y uso correcto de aplicaciones.
- Para los bancos, es más fácil decirle al cliente “debes proteger tu dinero”, pero se necesita pensar bien cómo llegarle para tener impacto. Es importante concientizar que es lo que se pierde.
- Sabemos que las campañas del miedo no sirven, que lo que hay que hacer es educar. El factor humano es clave, además que los grandes ataques vienen por ingeniería social.

Postura y Alianzas

- CISO, tiene que entender de gestión y procesos de negocio. La concientización no es un rol exclusivo de ciberseguridad, sino que debe buscar aliados como Gestión Humana y Sindicatos.
- Es crucial educar a los clientes y concientizarlos sobre la seguridad.
- ICP no tiene nada que ver con cable, se abre una ventana diferente de riesgos, la concientización debe estar del lado del cliente también.

Gestión de Riesgos e Inversiones

Inversión y Medición de Riesgos

- Es importante invertir y entender que hay que invertir en ciberseguridad.
- Medir los riesgos en toda la compañía para tener una solución integral.
- La falta de talento es un tema de riesgo significativo.

Problemas de Obsolescencia y Teletrabajo

- La obsolescencia de software y hardware es un problema. Es difícil seguir el ritmo de cambios en endpoints, licencias y actualizaciones.
- El teletrabajo y la educación a distancia han cambiado la seguridad perimetral. Ahora, el endpoint puede ser la computadora de un niño o un trabajador desde su hogar y saber cómo defender eso es crucial.

Seguridad en Equipos y Servicios

Equipos en Hogares y Protección

- Los equipos distribuidos en los hogares deben tener protección de seguridad. Es importante evitar claves genéricas y cambiarlas regularmente. El personal técnico cuando instala el equipo en el hogar del ciudadano ingresa una contraseña que le da el usuario y luego no se sugiere el cambio, queda así indefinidamente.
- Se ofrecen paquetes de antivirus a nivel de PC, aunque la mayoría de los servicios de seguridad que brindan están orientados a empresas.
- Asegurar el tráfico a los clientes y ofrecer servicios adicionales como denegación de servicio y migración de tráfico frente a ataques.

Servicios Adicionales y Automatización

- Evaluar servicios adicionales para ofrecer al cliente.
- Control de herramientas con respuesta en tiempo real, automatizaciones y alertas para mejores decisiones.
- Servicio de firewall virtual, segurity endpoint, soc como servicio.

Gestión de Equipos y Servicios B2B/B2C

Gestión de Equipos y Vulnerabilidades

- Gestionar los equipos instalados en los hogares de los clientes y tener políticas de gestión para incidentes.
- Ofrecer análisis de salud del firewire en el ámbito B2B y posibilidad de contratar este servicio.
- En el ámbito B2C, se desconoce qué medidas específicas se toman.

Estado actual de las empresas del sector para responder a incidentes.

Riesgos internos y Riesgos externos

- Interno: es ser el objetivo de un ciberataque, que es lo que haríamos, cómo reducimos los riesgos, como logramos estar preparados.
- Externo: por otro lado, esta lo externo, como concientizamos para evitar ataques a nuestros clientes o usuarios. O para plantas industriales (ciberseguridad industrial).

Hay que ver donde se ponen los fondos de inversión, además es importante involucrar a los Directores de las Empresas de TELCO, CISO, y demás áreas estratégicas de forma progresiva en estas conversaciones.

Backups / Respaldos

- Realizados de la forma correcta.
- Si telefónica Uruguay recibe un ataque de denegación de servicio, está protegida, se migra y se limpia el nuevo tráfico.
- TELCO lo que es denegación de servicio, firewalls virtuales, pero la necesidad es que tiene que ser enlace TELCO. La dan en enlace TELCO.

Comité de crisis

- Se plantea la conformación de un grupo de trabajo integrado por los diferentes TELCOs con fines de coordinación y comunicación. Para su correctofuncionamiento se deben elaborar protocolos de acción y canales de comunicación definidos donde se envíen/compartan/alerten de diversas amenazas o vulnerabilidades.
- Acordar y tener escrito los pasos a seguir frente a un ataque, para poder facilitar la acción en el momento que se precise. Podría incluir “la posibilidad de Bajar la palanca”, se desactiva el servicio hasta que se solucione el incidente bajo determinadas circunstancias.
- Elemento clave: la ética y confidencialidad de la información que se maneje en dicho espacio de comunicación.

Grupo de comunicación

- Tener en cuenta que es un factor clave, conocer que está pasando y también poder comunicar a un cliente que le está

pasando.
- Garantizar que la ley se cumpla, CERTuy si lo cumple.
- Los informes se entregan impresos en mano.

CSIRT sectorial

- Para garantizar que se pueda tener una respuesta correcta, y hacer frente a las particularidades específicas del sector
- Fundamental la colaboración.

Grupo de trabajo sectorial

- Compartir información en tiempo real.
- Para poder intercambiar, colaborar y trabajar en conjunto.
- Actualmente no se conocen los CISO en Uruguay, no existe un canal de comunicación formal o informal.

Cultura de Seguridad de la Información

- Conocer las normas y exigencias vigentes.
- Desarrollar políticas de seguridad internas, cumplirlas y actualizarlas.
- Conciencia de que son muchas veces el punto de entrada para que se generen incidentes.

Análisis de las infraestructuras de información críticas

- Trabajar especialmente sobre esto.
- Seguridad IT en combinación con OT.

Prepararnos para eventos extraordinarios

- Mundial 2030.

Ejercicios de Table top

- Se sugiere la realización de ejercicios de simulación de incidentes, en los cuales Agesic se ofrece a convocarlos para fomentar dicha instancia.
- Este tipo de instancias fomentan la coordinación y aprendizaje, con miras a evaluar cuan resiliente somos en la materia, cómo reaccionamos y qué áreas de mejora encontramos.