INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 8

9 DE NOVIEMBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado.

Incibe en su página web provee de una serie de métodos para que las empresas puedan notificarles los incidentes. Estos procedimientos se encuentran en la web.

https://www.incibe.es/protege-tu-empresa/reporta-tu-incidente.

Claves públicas para reportar incidentes : https://educacionadistancia.juntadeandalucia.es/profesorado/mod/url/view.php?id=546896

CCN-CERT Notificación de Incidentes : https://www.ccn-cert.cni.es/gestion-de-incidentes/notificacion-de-incidentes.html

Como ejercicio, se propone que examines los distintos modos de notificar los incidentes propuestos, y generes un esquema informativo donde se expliquen los pasos para realizarlo.

Partes del Informe a realizar :

1º.- Cómo se notifican los incidentes al INCIBE y al Centro Criptológico Nacional .- Pasos a seguir .-

2º.- Como se van a notificar los incidentes en nuestro Centro Educativo .- Formulario + E-mail.-

Cómo se notifican los incidentes al INCIBE y al Centro Criptológico Nacional.

Para reportar los incidentes al incibe, podemos hacerlo desde la pagina https://www.incibe.es/empresas/te-ayudamos/reporta-tu-incidente .

Después tinene 4 tipos de incidentes, mediante fraude, ransomware, botnet y “denuncia tu incidente”

Fraude

Si te has visto afectado por un caso de fraude electrónico, puedes reportarlo al equipo de respuesta a incidentes de INCIBE-CERT, aportando:

- Una descripción detallada del incidente y tus datos de contacto.

- El correo sospechoso junto con sus cabeceras y ficheros adjuntos.

De esta forma, el equipo de respuesta a incidentes identificará mejor tu caso y te ayudará a resolverlo.

Ransomware

Si te has visto afectado por un ataque de tipo ransomware, puedes reportarlo al equipo de respuesta a incidentes de INCIBE-CERT, aportando:

- Una descripción detallada del incidente y tus datos de contacto.

- La nota de rescate original (ransom note) en el formato en el que se encuentre en su equipo. - Si no dispones de ella o no localizas el archivo, envía una captura de pantalla donde se visualice el contenido de la nota.

- Dos archivos cifrados por el ransomware (que no contengan datos de carácter personal, cuyos originales fueran formato Word o Excel y ocupen menos de un MB).

Si la incidencia afecta a datos de carácter personal, el incidente tiene que ser notificado antes de 72 horas por parte del «Responsable del tratamiento» a la «Autoridad de control competente». La autoridad competente para resolver cuestiones legales relacionadas con el RGPD es la AEPD (Agencia Española de Protección de Datos) o las análogas Autoritat Catalana de Protecció de Dades, de Cataluña, y Datuak Babesteko Euskal Bulegoa, del País Vasco.

También es recomendable que denuncies el incidente para que se investigue el origen del delito. Así colaboras en las labores de prevención a otras empresas y en las acciones para capturar al ciberdelincuente.

Botnet

Si has recibido una notificación de tu operador de servicios de Internet indicándote que perteneces a una botnet, o crees que puedes sufrir este tipo de incidente, puedes reportarlo al equipo de respuesta de incidentes de INCIBE-CERT, aportando:

- Una descripción detallada del incidente y tus datos de contacto.

- La dirección IP pública y fecha y hora de la detección (ejemplo de fecha y hora: 2019-10-30 T 10:45 UTC)

- El nombre de la botnet.

Denuncia tu incidente

Además de notificar el incidente al equipo de respuesta a incidentes de INCIBE-CERT para que te ayuden a resolverlo, también puedes interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado en cualquier comisaría o a través de sus diferentes portales web:

Policía Nacional	*Guardia Civil*	*Ertzaintza*	*Mossos d'Esquadra*	*Policía Foral*
Brigada de Investigación Tecnológica de la Unidad de Investigación Tecnológica (UIT) de la Policía	*Grupo de Delitos Telemáticos (GDT) de la Guardia Civil*	*Sección Central de Delitos en Tecnologías de la Información (SCDTI) de la Ertzaintza*		

Para notificear un incidente en el Centro Criptológico Nacional podemos hacerlo desde la página https://www.ccn-cert.cni.es/es/gestion-de-incidentes/notificacion-de-incidentes.html

Son varias las vías para notificar un incidente al CCN-CERT:

- Herramienta LUCIA para aquellas entidades del ámbito del Esquema Nacional de Seguridad.

- A través del correo electrónico Incidentes (incidentes@ccn-cert.cni.es)

- Se aconseja ofrecer una descripción lo más detallada posible del incidente y la información de contacto (al menos una dirección de correo y un teléfono). En este caso, se deberán cifrar los mensajes y autenticar la identidad. En nuestro sitio Web, encontrará nuestra clave PGP/GPG.

Herramienta lucia

LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) es una herramienta desarrollada por el CCN-CERT para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora.

LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

Con la herramienta LUCIA, el organismo podrá gestionar tres tipos de ciberincidentes:

- Los incidentes propios del Organismo

- Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA).

- Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).

Las claves para la gestión de ciberincidentes son:

1. Disponer de herramientas, mecanismos, y procedimientos de detección que alerten al organismo de comportamientos anómalos en sus sitemas y redes. Para ello, se recomienda la adhesión al Sistema de Alerta Temprana (SAT) del CCN-CERT.

2. Es fundamental identificar la amenaza, la peligrosidad potencial y prevenir de esta manera el posible impacto sobre el servicio.

3. El organismo debe conocer su grado de madurez para responder al incidente en base a la tipología y peligrosidad definidos en la guía CCN-STIC 817.

4. Actuar con prontitud, sin dilación indebida. Notificar el incidente a la autoridad competente a través del CSIRT de referencia para establecer una comunicación directa. En el caso del sector Público, los organismos víctimas de posibles ciberincidentes deberán notificar al CCN-CERT. La notificación es un paso fundamental: el incidente puede estar afectando a otro organismo de forma simultánea.

5. Priorización y ejecución de procedimientos y medidas para evitar la propagación del incidente. El procedimiento de notificación de incidentes tiene que ser una realidad dentro del

marco normativo que desarrolla el plan de implantación para dar respuesta a la política de seguridad del organismo.

6. Recopilar toda la información del incidente. Revisar los eventos de seguridad y determinar los activos internos que han sufrido el intento de ataque y lo que es más importante priorizar en base a la peligrosidad y el contexto (triaje).

7. Documentar el incidente y las acciones llevadas a cabo en el momento de su detección.

8. Contener y mitigar la amenaza. Llevar a cabo labores de investigación, auditoría, bastionado, análisis forense e ingeniería inversa.

9. Restauración de sistemas y servicios siguiendo un plan establecido. Se determinará técnicamente el riesgo de reconexión de un sistema indicando los procedimientos a seguir y las salvaguardas a implementar para reducir el impacto para, en la manera de lo posible, evitar que se den de nuevo las circunstancias que lo propiciaron.

10. Resolución y cierre del incidente. Determinar el impacto del ciberataque y revisar y reforzar las políticas y medidas de seguridad necesarias.

Desde aquí podemos ver la documentación, acceder al sistema Lucia y descargar las calves PGP.

Documentación y descargas

- Claves para la gestión de ciberincidentes (infografía)
- Compartir información, crear comunidad: cómo la notificación de incidentes contribuye a mejorar la ciberseguridad nacional (infografía)
- Cómo agilizar la gestión y notificación de ciberincidentes con LUCÍA (infografía)

Sistema LUCIA y actualizaciones | contraseña: LUCIA

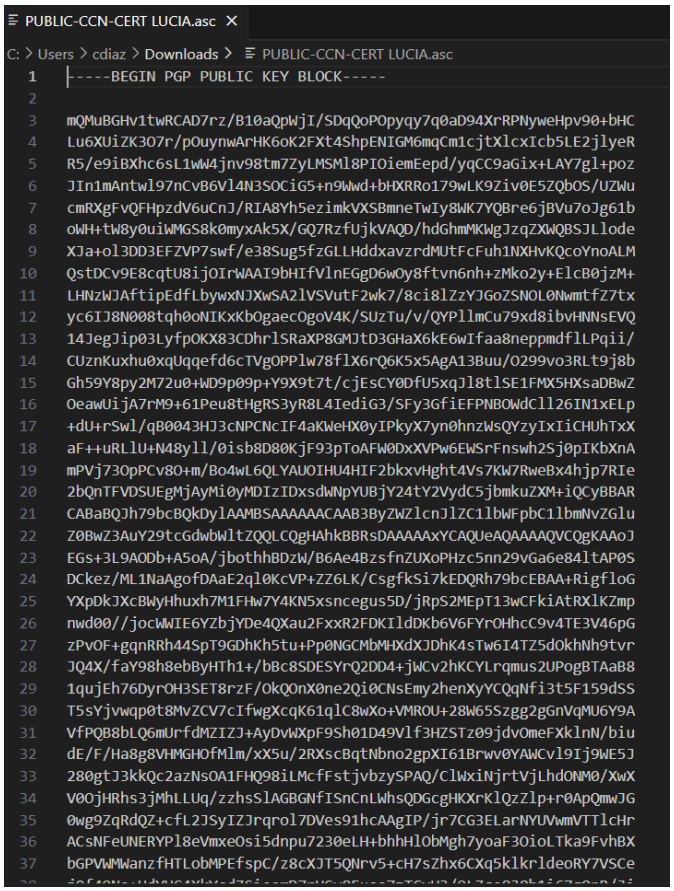
Contacto: **lucia@ccn-cert.cni.es**

Clave PGP Descargar

FINGERPRINT 05BF 19A8 3D73 2273 A0E3 5D6F 6B3E DCBF 4038 36FE

Podemos usar el sistema lucia (la contraseña es : LUCIA)

Podemos ver las claves publicas PGP:



Como se van a notificar los incidentes en nuestro Centro Educativo. Formulario + E-mail.

Lo primero que vamos a hacer es irnos a la página web oficial del centro:

Si bajamos a pie de página podemos ver las distintas formas de contactar con el centro educativo: