Universitat Oberta de Catalunya

uoc.edu

Guía de prevención y respuesta frente a ataques de ransomware

Anexo I. Plan de trabajo

Carlos Alberto Crego Sánchez
Master en Ciberseguridad y Privacidad
Privacidad

Albert Jové Canela
Cristina Pérez Sola

28 de diciembre del 2021

Índice

ANEXO I. Plan de Trabajo

Planificación del Trabajo

Listado de tareas

Código	Actividad	Estimación
ACT-1-0	Elaboración del plan de trabajo	14 días
ACT-1-1	Definir la problemática	0.5 días
ACT-1-2	Definir los objetivos del TFM	0.5 días
ACT-1-3	Decidir y explicar metodología	1 día
ACT-1-4	Redactar estado del arte	3 días
ACT-1-5	Estructurar en partes el TFM	4 días
ACT-1-6	Elaborar lista de tareas para cada parte del TFM	3 días
ACT-1-7	Estimar el tiempo de desarrollo de cada tarea	1 días
ACT-1-8	Elaborar planificación	1 día
ACT-2-0	Parte1 – Introducción	8 días
ACT-2-1	Investigación de la evolución del ransomware	2 días
ACT-2-2	Investigación del concepto de malware	0.5 días
ACT-2-3	Investigación de la anatomía del malware	0.5 días
ACT-2-4	Investigación de los tipos de ransomware existentes	0.5 días
ACT-2-5	Investigación de las particularidades del ransomware	0.5 días
ACT-2-6	Investigación de los síntomas de infección por ransomware	2 días
ACT-2-7	Investigación de los principales objetivos de ransomware	2 días
ACT-3-0	Parte2 - Métodos de distribución del ransomware	12 días
ACT-3-1	Investigación de la distribución a través de email	2 días
ACT-3-2	Investigación de la distribución mediante campañas de spam	2 días
ACT-3-3	Investigación de la distribución a través de sitios web inseguros	2 días
ACT-3-4	Investigación de la distribución mediante macros de Office	1 día
ACT-3-5	Investigación de la distribución mediante memorias USB	1 día
ACT-3-6	Investigación de la distribución mediante otros medios	4 días
ACT-4-0	Parte3 - Principales familias de ransomware	8 días
ACT-4-1	Elegir las 8 familias de ransomware más significativas	4 días
ACT-4-2	Investigación sobre familia de ransomware 1	0.5 días
ACT-4-3	Investigación sobre familia de ransomware 2	0.5 días
ACT-4-4	Investigación sobre familia de ransomware 3	0.5 días
ACT-4-5	Investigación sobre familia de ransomware 4	0.5 días
ACT-4-6	Investigación sobre familia de ransomware 5	0.5 días
ACT-4-7	Investigación sobre familia de ransomware 6	0.5 días
ACT-4-8	Investigación sobre familia de ransomware 7	0.5 días
ACT-4-9	Investigación sobre familia de ransomware 8	0.5 días

Código	Actividad	Estimación
ACT-5-0	Parte4 - Métodos para la prevención en entornos de usuario	14 días
ACT-5-1	Investigación de soluciones de antivirus	1 día
ACT-5-2	Investigación de entornos virtualizados	1 día
ACT-5-3	Investigación sobre como configurar el navegador	1 día
ACT-5-4	Investigación sobre copias de seguridad	1 día
ACT-5-5	Investigación sobre como reforzar la seguridad del SO	1 día
ACT-5-6	Investigación sobre como reforzar la seguridad en Office	1 día
ACT-5-7	Investigación sobre como reforzar la seguridad en móviles	1 día
ACT-5-8	Investigación de la importancia de las actualizaciones	1 día
ACT-5-9	Investigación sobre otros métodos de prevención	6 días
ACT-6-0	Parte5 - Métodos para la prevención en entornos corporativos	14 días
ACT-6-1	Investigación de la importancia de políticas de gestión de parches	1 día
ACT-6-2	Investigación de la importancia de la seguridad física	1 día
ACT-6-3	Investigación sobre segmentación de redes	1 día
ACT-6-4	Investigación sobre soluciones antiransomware	1 día
ACT-6-5	Investigación sobre firewalls y sistemas IDS/IPS	1 día
ACT-6-6	Investigación sobre la importancia de usar contraseñas seguras	1 día
ACT-6-7	Investigación sobre la importancia de las estrategias de backup	1 día
ACT-6-8	Investigación sobre la importancia de las políticas de seguridad	1 día
ACT-6-9	Investigación sobre el uso el correo electrónico de forma segura	1 día
ACT-6-10	Investigación sobre otros métodos de prevención	5 días
ACT-7-0	Parte6 - Capacitación en ciberseguridad como método preventivo	6 días
ACT-7-1	Investigación de la importancia de la formación en ciberseguridad	2 días
ACT-7-2	Buenas prácticas en el diseño de programas de capacitación	2 días
ACT-7-3	Investigación sobre la formación en ataques de ingeniería social	2 días
ACT-8-0	Parte7 - Elaboración de plan de respuesta ante una infección	14 días
ACT-8-1	Investigación sobre planes de respuesta ante infecciones	3 días
ACT-8-2	Diseño de la fase de preparación	2 días
ACT-8-3	Diseño de la fase de detección y análisis	2 días
ACT-8-4	Diseño de la fase de contención	2 días
ACT-8-5	Diseño de la fase de erradicación	2 días
ACT-8-6	Diseño de la fase de recuperación	2 días
ACT-8-7	Listado de acciones posteriores	1 día
ACT-9-0	Parte8 - Consecuencias legales derivadas de una infección	8 días
ACT-9-1	Investigación sobre legislación y regulación	3 días
ACT-9-2	Investigación sobre consecuencias legales de una fuga de datos	3 días
ACT-9-3	Investigación de escenarios reales	2 días
ACT-10-0	Revisión	7 días
ACT-10-1	Revisión de ortografía y formato	1 día
ACT-10-2	Revisión de bibliografía	1 día
ACT-10-3	Elaboración de glosario e índice	3 días
ACT-10-4	Elaboración del resumen (castellano/inglés) y de la ficha del TFM	2 días

Código	Actividad	Estimación
ACT-11-0	Preparación del vídeo de presentación	7 días
ACT-11-1	Preparar la estructura del contenido del vídeo	3 días
ACT-11-2	Grabación de prueba	1 día
ACT-11-3	Grabación definitiva	1 día
ACT-11-4	Edición	2 días
ACT-12-0	Preparación de la defensa del TFM	5 días

Hitos

La planificación del plan docente de la asignatura Trabajo Fin de Master se encuentra estructurada de la siguiente forma:

Fecha inicio	Fecha fin	Actividad
15/09/2021	28/09/2021	Plan de trabajo
29/09/2021	26/10/2021	Entrega de seguimiento
27/10/2021	23/11/2021	Entrega de seguimiento
24/11/2021	28/12/2021	Memoria final
29/12/2021	04/01/2022	Presentación vídeo
10/01/2022	14/01/2022	Defensa TFM

Por tanto, estableceremos en la planificación un total de 6 hitos, uno para cada una de las actividades descritas en el plan docente.

Una vez elaborada la lista de tareas y estimado el esfuerzo que conlleva el desarrollo de cada una de ellas y teniendo en cuenta las fechas de cada uno de los hitos establecidos en la planificación del plan docente, la planificación del presente trabajo fin de master resulta de la siguiente manera:

Actividad	Fecha inicio	Fecha fin
Elaboración del plan de trabajo	15/09/2021	28/09/2021
Entrega del plan de trabajo (PEC1)	28/09/2021	28/09/2021
Desarrollo de la Parte 1	29/09/2021	06/10/2021
Desarrollo de la Parte 2	07/10/2021	18/10/2021
Desarrollo de la Parte 3	19/10/2021	26/10/2021
Entrega de seguimiento (PEC2)	26/10/2021	26/10/2021
Desarrollo de la Parte 4	27/10/2021	09/11/2021
Desarrollo de la Parte 5	10/11/2021	23/11/2021
Entrega de seguimiento (PEC3)	23/11/2021	23/11/2021
Desarrollo de la Parte 6	24/11/2021	29/11/2021
Desarrollo de la Parte 7	30/11/2021	13/12/2021
Desarrollo de la Parte 8	14/11/2021	21/12/2021
Revisión	22/12/2021	28/12/2021
Entrega de la memoria final (PEC4)	28/12/2021	28/12/2021
Preparación del vídeo de presentación	28/12/2021	03/01/2022
Preparación de la defensa del TFM	03/01/2022	10/01/2022
Defensa del TFM	10/01/2022	14/01/2022

Breve descripción de los capítulos del trabajo

Capítulo 1 – Introducción al Ransomware

Abordaremos la evolución del ransomware desde su nacimiento, el concepto de malware, su anatomía, los tipos de ransomware existentes, las particularidades del ransomware, los síntomas de infección y los principales objetivos de los ataques de ransomware.

Capítulo 2 – Métodos de distribución

Haremos una lista de los principales vectores de ataque empleados por los ciberdelincuentes para distribuir ransomware, como, por ejemplo, el correo electrónico, las campañas de spam, los exploit kits, los sitios web de contenido pirata, las macros de Microsoft Office, etc.

Capítulo 3 – Defensa y prevención en entornos de usuario

Haremos una lista de las medidas de defensa y prevención que se pueden tomar para prevenir ataques de ransomware en entornos de usuario como, por ejemplo, la instalación de soluciones de antivirus y soluciones de backup.

Capítulo 4 – Defensa y prevención en entornos corporativos

Haremos una lista de las medidas de defensa y prevención que se pueden tomar para prevenir ataques de ransomware en entornos de corporativos como, por ejemplo, diseñar una política de gestión de parches, segmentar la red, gestionar vulnerabilidades, usar firewalls y sistemas de detección de intrusos.

Capítulo 5 – Plan de respuesta a ataques de ransomware

Elaboraremos un plan de contingencia y continuidad para el negocio en caso de que una empresa haya sido infectada con ransomware.

Capítulo 6 – Consecuencias de una infección

Evaluaremos las consecuencias legales de una infección por ransomware, sobre todo en caso de que se sospeche que hay una fuga de datos.