THE BRIDGE

Cybersecurity Bootcamp

U2M2 - Análisis Forense y Respuesta ante Incidentes (DFIR)

Gestión de Ciberincidentes

Índice

Gestión de Ciberincidentes

1.1. Clasifica los siguientes eventos en alerta, incidente o crisis

#	Evento	Alerta	Incidente	Crisis
1	Identificación de un incremento considerable de tráfico hacia la web de la organización desde direcciones IP geolocalizadas en Corea del Norte, Turquía y China	X		
2	Intento de conexión desde una máquina del segmento corporativo de la red de la organización hacia una dirección IP identificada como relacionada con Emotet según una *blacklist* de Karspersky		X	
3	Recepción de un correo en la carpeta de spam del buzón de todos los empleados que parece haber sido enviado desde la cuenta del CEO de la organización	X		
4	Indisponibilidad del software de gestión de pedidos y envíos de la organización debido a una infección por *ransomware*			X
5	Recepción por parte de empleados del departamento financiero de un correo electrónico con varios fallos gramaticales desde la cuenta legítima de correo del CEO solicitando hacer un pago urgente a una cuenta iraní	X		
6	Identificación de registros de actividad en varios equipos y servidores de la organización de un usuario administrador de dominio el cual se encuentra en desuso desde 2017		X	
7	Identificación de datos de clientes de la organización, incluyendo dirección física y número de tarjeta con CCV, publicados en un foro ruso en la Dark Web y públicamente anunciado en la cuenta de Anonymous de Twitter			X
8	Recepción de varias notificaciones de empleados de la organización comunicando que no pueden acceder al portal de la intranet		X	
9	Realización de una transferencia hace 15 días por valor de 3.000€ a una cuenta bancaria localizada en Corea del Norte, perteneciente presuntamente a un proveedor internacional que acaba de notificarnos que aún no la ha recibido		X	
10	Notificación por parte de varios clientes externos de la recepción de mensajes electrónicos tratando de suplantar a varios empleados de la compañía (en dichos mensajes se incluyen documentos Word adjuntos que, al tratar de abrirlos los clientes externos, son bloqueados por su software antivirus)		X	

1. Alerta: Monitoreo del tráfico basado en la procedencia.
2. Incidente: Necesidad de medidas para prevenir la propagación del malware.
3. Alerta: Monitoreo de correos para prevenir ataques futuros.
4. Crisis: Acciones inmediatas para evitar infecciones y restaurar el software afectado.
5. Alerta: información importante para prevenir transferencias de fondos y proteger información.

6. Incidente: Medidas inmediatas para prevenir la expansión del malware.
7. Crisis: Protección urgente de datos valiosos de clientes y sus finanzas.
8. Alerta: Vigilancia para detectar actividades sospechosas.
9. Incidente: Investigación y acciones para recuperar fondos.
10. Incidente: Investigación y medidas para evitar la propagación del malware.

1.2. Realizar un diagnóstico de madurez en materia de ciberresiliencia para una organización ficticia

- La organización Editorial Montes Blancos S.L. sufrió el pasado mes de octubre un ciberincidente que tuvo una importante afección para su negocio.
- Nos han solicitado apoyo en la medición de su madurez en materia de ciberresiliencia de forma que les ayude a identificar puntos de mejora y a mitigar el impacto en caso de sufrir futuros incidentes.
- De cara a determinar el nivel de madurez, completa la siguiente plantilla de diagnóstico de madurez en materia de ciberresiliencia desarrollada por la organización CREST y disponible públicamente en su página web[1]. Se adjunta también un breve manual de ayuda de la plantilla:

Escenario

La organización Editorial Montes Blancos S.L. sufrió el pasado mes de octubre un ciberincidente por infección de ransomware que afectó a gran parte de sus servidores donde almacenaban datos de los pedidos editoriales pendientes y datos necesarios para el desempeño de su trabajo, como versiones de libros a revisar antes de su publicación.
Debido al alto impacto que tuvo este incidente para el negocio, la organización nos ha solicitado apoyo en la realización de un diagnóstico de madurez en materia de ciberresiliencia según les han recomendado desde el comité ejecutivo como parte relevante del plan de renovación estratégica de la compañía.

Para poder realizar dicho diagnóstico, nuestro compañero Fernando se desplazó el pasado jueves 05/02 a las instalaciones del cliente para hacerle una entrevista a Iván González, CISO recién nombrado de Editorial Montes Blancos y antiguo administrador de sistemas de la organización. Esta entrevista primera consistió en una serie de preguntas acerca de la organización y del estado de madurez de la misma que tiene Iván en mente que quiere tratar de conseguir:

"Desde el incidente sufrido, para la editorial resulta de vital importancia el ser capaces de responder de forma ágil a cualquier potencial incidente que podamos afrontar. La detección debe ser prácticamente inmediata, sobre todo para aquellos incidentes que supondrían una interrupción completa del negocio, ya que un intento de fraude en transferencia o similar podríamos gestionarlo e investigarlo a más medio plazo, mientras que, para un ataque de denegación de servicios dirigido, debemos ser capaces de detectarlo y mitigarlo en cuestión de segundos.

[1] https://www.crest-approved.org/2018/07/20/cyber-security-incident-response-maturity-assessment/index.html

Por ello, el llevar a cabo este diagnóstico y determinar de manera precisa los procesos que resultan más críticos para el negocio se considera tarea de máxima prioridad desde el departamento de seguridad. Adicionalmente, los técnicos IT que se encargan del mantenimiento de los equipos y software de la organización soy realmente buenos a nivel de administración de sistemas, aunque es cierto que suelen preferir la usabilidad frente a la seguridad, por lo que podría ser interesante poner sus capacidades de respuesta a prueba con pruebas y escenarios simulados.

En cuanto a la inversión realizada por la organización en materia de ciberseguridad, contamos con un sistema de monitorización bastante bueno de todos los equipos de empleados y control industrial, y disponemos siempre al menos de un operario en 24x7 por si saltara alguna alerta, poder escalarme la alerta a mí y en caso de necesidad, activar a algún proveedor externo que pueda echarnos una mano con la gestión del incidente. No obstante, nuestra meta para antes de fin de este año es conseguir una madurez lo suficientemente alta como para ser capaces de tomar las decisiones relevantes en cuanto a la gestión del incidente y tener muy claros los pasos a seguir a nivel técnico para aplicar las medidas de contención y recuperación necesarias.

El problema frente al que nos encontramos el pasado mes de octubre cuando nos pasó lo del ransomware fue que, aunque el operario detectó que había comenzado el cifrado de varios servidores tan solo unos segundos después de que se lanzara simultáneamente en casi todas las máquinas de la organización, al no disponer internamente de un protocolo de respuesta bien definido que recogiera las medidas de contención iniciales a aplicar directamente, incluso antes de avisarme a mí del incidente, para cuando fuimos capaces de convocar un comité de crisis por llamada y tomar la decisión de desconectar todas las máquinas de la red y aislarlas, aproximadamente el 70% de los servidores ya se habían visto cifrados e irrecuperables.

No obstante, disponíamos de un sistema de copias de seguridad bastante potente, que se realizaban para todos los servidores y almacenaban diariamente sobre las 3 de la mañana en servidores NAS locales conectados al resto de la red de la organización, por lo que también parte de estas copias de seguridad se vieron cifradas. Menos mal que semanalmente, estas copias se replicaban a un servicio en cloud que tenemos contratado con Amazon, por lo que realmente sólo perdimos información nueva de la organización generada en los últimos 6 días previos al incidente. Los archivos de los puestos de usuario se vieron afectados e irrecuperables, ya que no realizamos copias de seguridad de los equipos de los empleados. Sin embargo, se les incita siempre a trabajar en local y almacenar el trabajo en las carpetas en red, precisamente para que, si pasan temas de este estilo o se pierde el portátil, no pierdan todo el trabajo.

Si me preguntaras qué fue lo que pasó exactamente, la verdad que sólo te sabría decir que nos infectamos con un ransomware por lo que me contó uno de mis técnicos, Tomás, que tiene algo más de idea de malware que yo, y me comentó que el malware se llamaba algo así como Ryky. Cuando descubrimos el nivel de afección y la paralización que había supuesto la infección, nos olvidamos por completo de tratar de identificar qué había pasado y nos pusimos a recuperar los sistemas caídos como locos. Simplemente desconectamos todos los equipos de la red, creamos una VLAN paralela vacía, y fuimos restaurando y reconectando uno a uno todos los equipos hasta que volvimos a estar operativos al 90% aproximadamente.

En la reunión de seguimiento del estado del incidente, que la verdad fue algo caótica y más larga de lo necesario seguramente, Tomás nos comentó que, aunque los equipos ya estaban restaurados, sería muy interesante revisarlos todos para ver si encontramos algún ejecutable sospechoso o similar, ya que lo mismo el malware se ha quedado residente y vuelve a despertarse en unos días y nos volvemos a infectar. Hemos solicitado a una empresa consultora de ciberseguridad de aquí de Toledo que nos eche una mano con este tema, que más vale prevenir que curar, aunque sin duda alguna creo que deberíamos recibir todos algo más de formación en materia de ciberseguridad porque andamos muy verdes.

No sé si puedo ayudarte con alguna pregunta más que tengas, pero básicamente te resumo el estado y las necesidades de la editorial: tenemos capacidad para detectar de forma muy ágil los incidentes, pero no tenemos ni idea de qué hacer a continuación, y eso es lo que nos ha penalizado."

Una vez completada la entrevista con Iván, nuestro compañero Fernando pasó a preguntar una serie de aspectos en cuanto a operación con los técnicos de seguridad de la editorial, Christian y Roberto, que se encontraban en esos momentos en sus instalaciones:

"La verdad es que nosotros no llevamos mucho tiempo en la compañía, y aunque ambos venimos del grado superior de administración de sistemas y sí tenemos idea de sistemas y redes a nivel de organización, si saltara una alerta en el sistema de monitorización haciendo referencia a algún nombre de malware, no sabríamos decir de primeras qué tipo de acciones realiza ese malware y cómo evitar que se propague, cifre o infecte más equipos. En ese sentido, Tomás es el que más sabe de esos temas, pero no puede estar él siempre de guardia de monitorización, así que entre todos tratamos de leer, informarnos y estar actualizados en materia de campañas recientes y demás.

Lo que sí es cierto es que todos los equipos de la organización tienen antivirus Karspersky actualizado, tanto servidores como portátiles, y excepto unas 4 máquinas creo que son de la planta de impresión que cuentan aún con Windows 7, todos los demás tienen Windows 10 o Windows Server 2016 por lo menos. En este aspecto, nuestro jefe, Iván, ha sido siempre muy estricto con mantener actualizados los sistemas a la última versión posible siempre.

Los Windows 7 que he comentado no los hemos podido actualizar aún porque el software principal con el que operamos para controlar las imprentas y encuadernadoras no soporta Windows 10, pero sabemos que Iván ha estado los últimos días presionando al proveedor para que actualice el software y tenga compatibilidad con Windows 10, o buscaremos otro software."