YA ESTAMOS CONCIENCIADOS EN CIBERDEFENSA, PERO... ¿ESTAMOS PREPARADOS?

Felipe AREAL FERNÁNDEZ

N los últimos tiempos nos hemos familiarizado con ciertos términos de los que no habíamos oído hablar antes: *Phishing, Spam, Ciberdefensa, Hacking*, son algunos de ellos. La gran mayoría de nosotros, si no todos, hemos participado de una u otra manera en algún tipo de jornadas de concienciación en ciberdefensa y, por tanto, tenemos una idea de lo que hablamos. De esta manera nos hemos dado cuenta de que es un aspecto muy importante en nuestro día a día, tanto en nuestros hogares como en el ámbito profesional.

Sin embargo, es probable que el lector no dedicado a estos temas, asocie estos asuntos a personas o grupos de ellas escondidas detrás de una pantalla negra con letras verdes, en una habitación oscura, tratando de atacar servidores de grandes empresas, bancos, o incluso gobiernos. «A mí no me hackean, yo no soy el objetivo de nadie», dicen muchos con el teléfono inteligente encima de la mesa, el *smartwatch* conectado a este y después de decirle a su altavoz inteligente que ponga su serie preferida en el televisor, mientras descarga en el *USB* que usa para todo, la última película para los niños…

Sin tratar de ser alarmista, ya que soy de los que utilizan todos estos dispositivos que solucionan problemas que antes no tenía, con este artículo simplemente pretendo asociar conceptos, y ver las posibles relaciones entre ellos, y como esto hace que en todo momento podamos ser un objetivo para cualquier ciberatacante, ya sea en el ámbito profesional, como en el doméstico, y así, formular la siguiente pregunta: Ya estamos concienciados en Ciberdefensa, pero, ¿Estamos preparados?

Anatomía de un ataque

Un ciberataque, aunque puede ser extremadamente complejo, se puede resumir en algo tan simple como el mecanismo o procedimiento por el que un atacante trata de obtener acceso a un sistema y privilegios dentro de este para manejarlo a su antojo.

El ataque se puede realizar de tantas formas como seamos capaces de imaginar: aprovechando vulnerabilidades del sistema (errores en el propio sistema que permiten el acceso al mismo), utilizando ingeniería social (engaño al usuario para que proporcione, sin darse cuenta, acceso al mismo), y un sinfín de procedimientos técnicos, o no, para tener acceso, ya sea físico o virtual al sistema. Todos estos mecanismos se pueden combinar entre sí o con cualquier ingenio propio de películas del mismísimo James Bond, para que, finalmente, el resultado sea el mismo, acceder y manejar el sistema objetivo al antojo del ciberatacante.

Ejemplo: en un teléfono móvil, el atacante trata de acceder al sistema y obtener privilegios de administrador para tener el control de este. Con este privilegio, podría ver los archivos guardados, activar o desactivar cámaras, micrófonos, *GPS, Bluetooth*, o cualquier subsistema/sensor del aparato en cuestión. Esto, se puede trasladar a cualquier sistema informático conectado a una red (o no).

La información es poder

Cuando pensamos en que no somos objetivo para nadie, estamos equivocados. Cometemos el error de pensar en que los atacantes solo buscan las claves de lanzamiento de los misiles, o el PIN de la cuenta corriente del señor Forradez, y no nos damos cuenta de que cualquier tipo de información es útil, ya sea únicamente con fines comerciales, o con otros más oscuros.

En los tiempos que corren, el análisis de grandes volúmenes de información personal, permiten sacar conclusiones incluso «no observables» por el ojo humano. Y aunque esto es otro campo infinito, en donde entran términos como *Big Data*, «IA» y otros muchos, el resultado es que del análisis de la información obtenida mediante un ciberataque, se pueden sacar conclusiones muy útiles para empresas proveedoras de servicios o de ventas de productos, y/o de otros muchos campos.

¿Y si trasladamos esto al ámbito profesional? ¿Y si fuéramos capaces de analizar el comportamiento del personal de una unidad en la red?

Ejemplo: durante el último mes, he estado monitorizando el comportamiento de cierto personal destinado en la misma unidad. Este personal ha realizado numerosas búsquedas de alojamiento en la ciudad A, además, buscan con asiduidad, excursiones en el país X y han hecho también varias

búsquedas de clubes de buceo en Y. También he observado que hasta el día 15, las búsquedas han estado repartidas, principalmente, entre las 08:00 horas de la mañana y las 23:00 horas de la noche y a partir del 15, se realizan en las 24 horas del día, cada dispositivo en unas franjas horarias determinadas.

¿Vemos con que poco podríamos tener una idea de que puertos va a visitar la unidad en cuestión, que día salió de su base e incluso quien está activo en cada franja horaria? Si además analizamos los perfiles de redes sociales de todo este personal, es muy probable que la «fotografía» fuera mucho más nítida.

El ciberatacante siempre va por delante del ciberdefensor

En cuestiones de ciberseguridad, la mayor parte de las veces lo que se hace es «tapar agujeros». Los ciberatacantes tratan de aprovechar vulnerabilidades conocidas de los sistemas no solventadas y/o buscar nuevas vulnerabilidades que les permitan el acceso. La forma de «tapar agujeros» es básicamente, mantener actualizados los sistemas con todos los parches y actualizaciones de seguridad. Ante nuevas vulnerabilidades, no nos queda otra cosa que confiar en que las normas de seguridad establecidas para la red en cuestión funcionen y, sobre todo, en su cumplimiento estricto por parte de los usuarios, quienes son, comúnmente, el eslabón más débil en aspectos de ciberseguridad.

En resumen, el «agujero» o «brecha de seguridad» se tapa una vez detectado. Son los expertos en seguridad quienes trabajan en la búsqueda de estas brechas para corregirlas, pero muchas veces, son las fugas de información, la detección de intrusos o el mal funcionamiento de los sistemas los que alertan de que algo pasa, es decir, los ciberatacantes las han detectado y explotado antes de ser detectadas. El ciberatacante suele ir por delante del ciberdefensor.

La ciberseguridad empieza por lo más básico, la ciberdefensa viene después

Sabiendo a grandes rasgos qué y cómo buscan los ciberatacantes el acceso a los sistemas, y teniendo claro que siempre vamos a ir por detrás, debemos de pensar en cómo protegernos.

La única forma de protegerse es establecer barreras de protección, la seguridad en capas, incluyendo todos los elementos que afecten al sistema. Desde el usuario, hasta la electrónica de red, incluyendo las medidas de seguridad física contempladas en la acreditación de seguridad del local que alberga ese sistema.

La parte técnica, aunque está en manos de los expertos en el asunto, suele requerir de la intervención del usuario, instalando actualizaciones o cumplien-

do con los procedimientos de seguridad establecidos y aquí es donde normalmente fallamos, ya sea cargando un dispositivo particular en el *USB* de un ordenador de una red corporativa, mezclando dispositivos de memoria en diferentes redes sin utilizar los procedimientos TASO establecidos, o introduciendo información o enviándola por correo en una red que, por su clasificación, no debería contenerla.

La ciberseguridad, comprende, o debería de comprender, todas las medidas, desde las más básicas hasta las más técnicas, que debemos de adoptar para asegurar que el plan de protección de un sistema funcione, y es algo que deberíamos de tener todos presente en nuestro día a día, y así adiestrar, evaluar y certificar a todas las unidades en el cumplimiento de estos aspectos, al igual que hacemos con otras guerras.

La ciberdefensa va un poco más allá e incluye, además de la autoprotección de nuestros sistemas, otras capacidades que a día de hoy no parece factible implementar en la mayor parte de las unidades.

Casos posibles, ¿o reales?

Habiendo visto porqué cómo y cuándo podríamos ser víctimas de un ciberataque, veamos varios casos, reales o no, en los que se podría haber llevado a cabo una intrusión no autorizada en un sistema, hubo fugas de información o simplemente se puso en riesgo algún sistema.

Hace un tiempo, la unidad X, desplegada en el país Y, recibió la visita de autoridades del país. El habitual *briefing* de capacidades fue tan interesante que algunos de los asistentes pidieron al ponente si se lo podían copiar en su *USB*, para consultarlo más adelante. ¿Podrían estar los *USB* infectados para acceder a nuestra red? ¿Se podían haber infectado para que al introducir ese *USB* en la red de trabajo habitual nos proporcionara acceso a esta? La respuesta es sí en ambos casos. Pero imagino, que al igual que nosotros utilizamos un ordenador aislado, y analizamos los *USB*, ellos harían lo mismo. La sorpresa fue que uno de los *USB* contenía gran cantidad de información de interés...

El sistema de recopilación de datos de la unidad X, aunque antiguo proporciona mucha información que además es muy cómoda de copiar y pegar para realizar los informes reglamentarios. Es un sistema aislado, no conectado a ninguna red. Únicamente, recibe los datos de los sensores y además los proporciona al sistema de navegación. El teniente de navío Fulanitez, para realizar su informe utiliza su *USB* para copiar los datos del sistema. Sí, es el mismo *USB* que utilizó la semana pasada para descargar series «de la isla del pirata», y el que utiliza habitualmente para infinidad de tareas, profesionales y domésticas… ¿El ciberatacante podría haber infectado los sistemas del teniente de navío Fulanitez para que, aprovechando una vulnerabilidad conocida del

antiguo sistema X, modificara los datos que proporciona al sistema de navegación? La respuesta también es sí.

En un ejercicio avanzado, el principal sistema de MyC era a través de un *chat* en la red Y. Durante un ejercicio SURFEX Encounterex, al CIS de la unidad se le ocurrió acceder a la sala de *chat* BLUE (no recuerda si no estaba protegida, o si el *password* era 123456, que es lo mismo) con el nombre de una unidad BLUE y enviar el mensaje «Request PCS». Al minuto todas las unidades del bando Blue, mandaron su posición, rumbo y velocidad, tras lo que salió de la sala y pintó en el sistema de combate la posición de las unidades… Poco después se fueron observando contactos radar de todas las unidades en las mismas posiciones relativas que estaban pintadas…

Conclusiones

Aunque todos somos conscientes de la amenaza y tenemos cierta concienciación básica en estos aspectos, no hemos llegado al punto en el que asociamos estos conceptos con nuestra actividad particular y profesional en el día a día.

Cualquiera podemos ser objetivos de un ciberataque, aunque no dirigido contra nosotros en particular, con otros fines que pueden afectar a nuestras unidades, institución y/o a la seguridad.

La preparación no solo debe incluir la concienciación. Deberíamos de incluir todos estos aspectos en nuestros planes de I + A, así como en las evaluaciones y certificaciones de las unidades, con el fin de convertir estos puntos en los que fallamos y que se pueden convertir en «brechas de seguridad», en algo rutinario, en lo que estemos adiestrados y no cometamos errores básicos que comprometan la seguridad de los sistemas.