economía de hoy.es

27-01-2020

Tecnología

Los riesgos de seguridad en las empresas se reducirían drásticamente si realizaran auditorías periódicas de sus sistemas y los pusieran permanentemente a prueba

Telmo Miguel Xavier Ferreira, Cybersecurity Red Team de Grupo CMC.

Lunes 27 de enero de 2020, 08:17h

El especialista en hacking y seguridad, Telmo Miguel Xavier Ferreira, mostró en Sh3llCON, que se celebró en Santander, lo fácil que resulta derribar defensas y engañar a personas y sistemas.

Según Grupo CMC, multinacional española en entorno de las TIC, los riesgos de seguridad de las organizaciones se reducirían drásticamente si sus estrategias incluyeran auditorías periódicas y el uso de equipos de Red Team[1] para comprometer sus sistemas TI de forma deliberada y detectar así las vulnerabilidades de su infraestructura tecnológica. Así lo constata Telmo Miguel Xavier Ferreira, Cybersecurity Red Team de Grupo CMC, que participó en el encuentro Sh3llCON – Congreso de Seguridad Informática de Cantabria, que celebró su sexta edición esta semana en Santander.

Durante su ponencia, Telmo mostrará lo fácil que puede resultar actualmente comprometer los sistemas informáticos de una organización y la importancia que tienen los servicios de Read Team en una correcta estrategia de ciberseguridad. En su presentación, se puso de manifiesto cómo las enseñanzas que el filósofo chino Sun Tzu recogió en su obra "El Arte de la Guerra" siguen plenamente vigentes y resultan extremadamente valiosas para la actividad que desarrollan los equipos de Red Team. En este sentido, y según Ferreira, *"la filosofía y la lógica de combate que atesora el tratado de Sun*

http://tinyurl.com/uuujguj

Tzu resulta muy útil a los equipos de Red Team, cuya labor es fundamental para detectar, a través de ataques simulados, cualquier debilidad en las infraestructuras y sistemas de la empresa, y exige, como aconseja Sun Tzu, ***conocer a tu enemigo y conocerte a ti mismo para salir triunfante en mil batallas"****.*

De acuerdo con Ferreira, junto al conocimiento del enemigo, es importante tener en cuenta otros principios de Sun Tzu como que **"nunca se debe atacar con cólera y con prisas; es aconsejable tomarse tiempo en la planificación y coordinación del plan y si utilizas al enemigo para derrotar al enemigo, serás poderoso en cualquier lugar donde vayas".**

Ferreira quiere llamar específicamente la atención sobre lo sencillo que puede resultar para cualquier persona, sin necesidad de profundos conocimientos informáticos, convertirse en un hacker ya que *"actualmente todo está en YouTube". "Se trata, en definitiva,* -apuntó el ponente--, *de cumplir con otro de los principios de esta filosofía milenaria,* ***"la mejor victoria es vencer sin combate"****, y para ello es necesario conocer muy bien al enemigo, adelantarse a su ataque y hacer uso, además, de sus propias armas".*

Para ilustrar estas ideas, Ferreira mostró con ejemplos prácticos algunas de las herramientas que utilizan los hackers para aprovechar vulnerabilidades en Protocolo de Escritorio Remoto, lanzar ataques de phishing, robar información de sesiones y contraseñas o capturar a distancia datos de móviles.

Del mismo modo, Ferreira hizo una demostración de prácticas habituales para los equipos Red Team, como el "pentesting" o "test de penetración", un ataque dirigido y controlado a los sistemas informáticos de una organización que permite identificar posibles vulnerabilidades y fallos en la seguridad.

Industria, un sector en el punto de mira de los ciberdelincuentes

En su ponencia, Ferreira también puso el foco en la industria, un sector extremadamente atractivo para los hackers de sombrero negro al ser un entorno donde es más fácil tener éxito porque sus sistemas generalmente están más desprotegidos y se pueden obtener buenas recompensas a través de la extorsión mediante el sabotaje de activos críticos para la empresa.

Como conclusión, Ferreira hace un llamamiento para *"actuar ahora que aún estamos a tiempo"* y destaca otro de los principios esenciales de Sun Tzu: **"el ejército que actúa aisladamente, que carece de estrategia y que toma a la ligera a sus adversarios, inevitablemente acabará siendo derrotado".**

[1] Equipos de profesionales que ponen a prueba de forma constante la seguridad de sus sistemas TI para asegurar su integridad y asegurar la continuidad del negocio.