

Informes

Telmo Miguel Xavier Ferreira (Grupo CMC): “las enseñanzas del filósofo Sun Tzu resultan valiosas para los equipos de Red Team”

03 Febrero 2020
por Redacción



Los riesgos de seguridad de las organizaciones se reducirían drásticamente si sus estrategias incluyeran auditorías periódicas y el uso de equipos de ‘Red Team’ para comprometer sus sistemas TI de forma deliberada y detectar así las vulnerabilidades, recomendó Telmo Miguel Xavier Ferreira, Cybersecurity Red Team de Grupo CMC, en la sexta edición del Sh3llCON celebrado en Santander .



Los postulados del filósofo Sun Tzu recomiendan en conocer bien al enemigo, adelantarse a los ataques y usar sus armas

Durante su participación en el Congreso de Seguridad Informática de Cantabria (Sh3llCON), Telmo Miguel Xavier Ferreira ha mostrado lo fácil que puede resultar comprometer los sistemas informáticos de una organización y la importancia que tienen los servicios de Red Team en una

<http://tinyurl.com/sxc9h2a>

correcta estrategia de ciberseguridad. Los Red Team son equipos profesionales que ponen a prueba de forma constante la seguridad de sus sistemas TI para asegurar su integridad y asegurar la continuidad del negocio.



Además, subrayó cómo las enseñanzas que el filósofo chino Sun Tzu recogió en su obra 'El Arte de la Guerra', no solo siguen plenamente vigentes, sino que "resultan extremadamente valiosas para los equipos de Red Team".

En este sentido, y según Ferreira, "la filosofía y la lógica de combate que atesora el tratado de Sun 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 del filósofo como que "nunca se debe atacar con cólera y con prisa: 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-, 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".



La filosofía y lógica de combate del tratado de Sun 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 conocer a tu enemigo y conocerte a ti mismo para salir triunfante
Telmo Miguel Xavier Ferreira

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

Del mismo modo, realizó 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.

<http://tinyurl.com/sxc9h2a>

Industria, en el punto de mira de los ciberdelincuentes

En su ponencia, también pone el foco en la industria, un sector extremadamente atractivo para los hackers 'black hat', 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". Más información en www.grupocmc.es y en <https://www.sh3llcon.es>

<http://tinyurl.com/sxc9h2a>