Publicado en enero 27, 2020

Cómo reducir los riesgos de seguridad en las empresas

Grupo CMC ha presentado en su encuentro "Sh3llCON–Congreso de Seguridad Informática de Cantabria", que celebra su sexta edición esta semana en Santander, como las organizaciones pueden mejorar su seguridad si incluyen auditorías periódicas y el uso de equipos Red Team.

Así lo ha constatado Telmo Miguel Xavier Ferreira, Cybersecurity Red Team de Grupo CMC, pues durante su ponencia,mostrará lo fácil que puede resultar comprometer los sistemas informáticos de una organización y la importancia que tienen los servicios de Read Team en una correcta estrategia de ciberseguridad.

"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", afirma Xavier Ferreira.

Reducir los riesgos de seguridad

Uno de los puntos esenciales para reducir el riesgo de seguridad es conocer al enemigo, pero también debemos tener en cuenta otros principios;

- **No se debe atacar con prisas,** es aconsejable tomarse el tiempo necesario para planificar y coordinarse
- **La mejor victoria es vencer sin combate,** para ello es necesario conocer muy bien al enemigo y adelantarse a su ataque.

Para ilustrar todas estas ideas, Ferreira mostrará 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.

LAS ORGANIZACIONES PUEDEN MEJORAR SU SEGURIDAD SI INCLUYEN AUDITORÍAS PERIÓDICAS Y EL USO DE EQUIPOS RED TEAM

Del mismo modo, hará 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 el transcurso de la ponencia se ha reiterado lo desprotegidos que se encuentran algunos sectores, más concretamente el industrial, el cual es extremadamente atractivo para los hackers.

En dicho sector, las tasas de ciberataque son elevadas, pues cuentan con sistemas obsoletos que no les protegen, además las recompensas que se pueden obtener a través de la extorsión mediante sabotaje son muy altas.

"*Actuar ahora que aún estamos a tiempo.* El ejército que actúa aisladamente, que carece de estrategia y que toma a la ligera a sus adversarios, inevitablemente acabará siendo derrotado", concluye Ferreira.

Revista Byte TI https://revistabyte.es/seguridad-informatica/seguridad-4/