El hacking ético y sus beneficios en el mundo empresarial

En un mundo en el que la tecnología sigue su ruta, avanzando y evolucionando de forma imparable, es lógico que ésta se implemente en nuestra vida cotidiana al nivel y la rapidez con la que lo está haciendo. En los últimos años, ha aumentado el ratio de dispositivos por habitante, y, por ende, esto se traslada al ámbito profesional.

Son muchas las ventajas que aporta el uso de la tecnología al mundo de la empresa: reduce los errores en los procesos, impulsa la innovación, estimula la competitividad y la productividad, disminuye los costes, facilita la gestión de la información... Por eso, la mayor parte de las compañías están llevando a cabo auténticos procesos de digitalización. Pero, al igual que los beneficios son innumerables, los riesgos que se derivan de su uso y aplicación, también lo son.

Los delitos cibernéticos están a la orden del día. Los métodos empleados por los ciberdelincuentes para hacerse con el control de los dispositivos o de la información, cada vez son más innovadores, más dañinos y más difíciles de detener. Pensemos, por ejemplo, en las técnicas de ingeniería social, en las cuales se busca obtener información confidencial de los usuarios a través de la manipulación (engaño) ilícita de los mismos.

Por ello, resulta necesario adoptar unas buenas medidas de seguridad y una protección rígida frente a estas amenazas, mucho más, si cabe, en el ámbito empresarial, en donde la ciberseguridad constituye un elemento muy importante para la viabilidad de la misma.

Entonces, ¿qué podemos hacer para proteger nuestra empresa de los ciberdelincuentes?

Para empezar, debemos cambiar el concepto negativo que normalmente asociamos al término hacker, pues no son ellos los que se dedican a cometer delitos online, sino los ciberdelincuentes. Es aquí donde entra en juego el conocido como ‘hacking ético’. Bajo esta denominación, se recogen todas aquellas conductas que pretenden buscar y explotar fallos o vulnerabilidades en los sistemas informáticos de las empresas con el fin de protegerlos frente a futuros ataques de ciberdelincuentes.

A través de esta técnica, se persigue reforzar la seguridad informática de la empresa. Su objetivo es perpetrar ataques controlados a la seguridad de las compañías, con el fin de anticiparse a ataques que puedan conllevar peores consecuencias.

En estos días que vivimos ‘los hackers éticos’ son piezas claves en el seno de las grandes empresas. Trabajan haciendo una labor de consulting, precisamente en esa función de ciberseguridad.

Para ello, utilizan un conjunto de pruebas de penetración, pentesting, con las que comprueban el funcionamiento de los procedimientos de seguridad de una red o dispositivo con el objetivo de hallar vulnerabilidades. Estas pruebas de penetración siguen unas fases bien marcadas:

- **Recolección**. Consiste en recolectar toda la información que sea posible para los pasos posteriores. En esta fase, se identificarán los sistemas a auditar.
- **Escaneo**. Una vez recopilada esta información, se realizará un análisis de vulnerabilidades de los sistemas.
- **Acceso y explotación**. En este momento se intentará explotar las vulnerabilidades encontradas. Todo ello, siempre, bajo los límites que se hayan acordado con el cliente.
- **Reporte**. Como fase final, se creará un reporte con los detalles de la prueba, desde las vulnerabilidades que se han detectado durante la misma y la criticidad de estas, hasta las posibles consecuencias y las soluciones para mejorarlas.

Generalmente, en compañías con un número considerable de empleados, es el propio personal interno quien se responsabiliza de poner en jaque la infraestructura informática. En cambio, en las pymes y empresas de menor tamaño, se suele recurrir a empresas externas especializadas en estos procesos de ciberseguridad.

No debemos olvidar que, en cualquier caso, debe existir un acuerdo bajo contrato entre ambas partes. Este contrato ha de manifestar la autorización expresa de la empresa para ejecutar el intento de ataque, y determinar los términos de confidencialidad, integridad, secreto profesional y límites de acción.

Beneficios que aporta el hacking ético

Esta protección de la que venimos hablando, se ha vuelto fundamental a nivel empresarial. Es necesario que estos 'White hat hackers', no sólo conozcan las técnicas, herramientas e intenciones de los 'Black hat hackers'; sino también, que dispongan de un profundo conocimientos de las redes y sistemas de la compañía, así como de sus políticas en ciberseguridad que les permita realizar de una manera más eficiente su trabajo.

A modo de resumen, podemos hablar de varias ventajas:

- Mejora la ciberseguridad detectando posibles vulnerabilidades y, en consecuencia, aportando soluciones eficaces para evitarlas.
- Impide que los equipos de la empresa queden inutilizados, reforzando para ello los protocolos de seguridad.
- Previene el espionaje corporativo y mantiene toda la información sensible contenida en la empresa bajo salvaguarda, cumpliendo con ello el Reglamento de Protección de Datos.

Es primordial entender que el hacking ético puede convertirse en una pieza clave en la actividad empresarial actual. Como hemos dicho, vivimos en un mundo en el que todos los procesos se están informatizando día a día, aumentando el campo de actuación de los conocidos como 'Black hat hackers'.

Crear medidas de seguridad que preserven los equipos de trabajo y mantengan toda la información contenida en una compañía a salvo, debe convertirse en una de las principales motivaciones. Por eso, es fundamental conocer y entender esta metodología que tantas soluciones puede aportar en el ámbito de la ciberseguridad.

Fuente: incibe.es

Link: https://www.incibe.es/protege-tu-empresa/blog/el-hacking-etico-y-sus-beneficios-el-mundo-empresarial