Hacking Ético

Auditar la Seguridad

www.abast.es

El objetivo de las auditorias de seguridad, conocidas como "Hacking Ético", es comprobar los niveles de seguridad reales de los sistemas de información y elaborar un plan de acción en base a recomendaciones que reduzcan o eliminen los riesgos asociados a las vulnerabilidades detectadas.

En ocasiones, el objetivo de este tipo de servicios es hallar indicios y/o evidencias de actividades ilícitas por parte de personal antiguo o actual de la organización en perjuicio de esta: fugas de información, amenazas o espionaje industrial. Este tipo de servicios se conocen como Auditorías forenses.

Beneficios

- Conocimiento del grado de vulnerabilidad de los sistemas de información. Conocimiento que ha de permitir la reducción de aquellos riesgos que pueden comprometer la confidencialidad e integridad del activo más valioso de cualquier organización que es la información que gestiona.
- Mejora de la seguridad de la organización La auditoría de seguridad ha de contribuir a mejorar la robustez de los sistemas de información frente a posibles ataques y malos usos externos e internos.
- Formación y concienciación de los empleados de la organización para fomentar un comportamiento y actitud en su operativa diaria que permita mejorar la seguridad de la información, evitando riesgos innecesarios.

Retorno de la Inversión en Seguridad (ROSI)

Los costes asociados a un servicio de seguridad como el que se presenta son muy inferiores a los costes que nuestra empresa u organización debería soportar en caso de que se materializasen las amenazas asociadas a las vulnerabilidades existentes.

Es difícil cuantificar las pérdidas asociadas a un escenario en el que nuestros sistemas se ven comprometidos.

Los elementos a tener en cuenta son:

- Horas de trabajo asociadas a la determinación de la causa del ataque y a la evaluación de las pérdidas en integridad y confidencialidad de la información.
- Horas necesarias en establecer y reparar los sistemas afectados.
- Posibles multas, sanciones e indemnizaciones.
- Costes de inactividad.
- Costes asociados a una posible pérdida de confianza de los clientes, daño en la imagen corporativa y pérdida de confianza del público general.
- Posible rotura de contratos de confidencialidad con clientes o proveedores.

¿Por qué ABAST?

ABAST dispone de una gran experiencia en este tipo de proyectos en multitud de clientes tales como entidades deportivas profesionales, empresas constructoras, empresas del sector logístico, empresas de gestión patrimonial, etc.

ABAST, como empresa de servicios integrales, le ayudará a establecer e implementar aquellas recomendaciones que surjan de la auditoría, que mejor se adapten a las necesidades específicas de su negocio u organización. Tan importante como detectar las vulnerabilidades existentes, es determinar y priorizar aquellas medidas organizativas y técnicas que permitan establecer un nivel de seguridad aceptable por su negocio.

Nuestra metodología

Un proyecto completo de hacking ético comprende todos los puntos que se enumeran a continuación. No obstante, cada proyecto se estudia individualmente y se realiza una propuesta de servicios que puede combinar diversos de los ámbitos de auditoría que se describen a continuación en función de las necesidades específicas de cada cliente.

1. Auditoría técnica de seguridad perimetral. Se desarrolla un ataque perimetral ciego desde el exterior en el que se desconoce la infraestructura informática de la empresa (ataque de "caja negra").
2. Auditoría técnica de seguridad de aplicaciones web. Una de las principales puertas de entrada desde el exterior a los repositorios de información de las organizaciones es el acceso vía web. En esta fase se audita el código desarrollado en las páginas que dan acceso a información no pública.
3. Auditoría técnica de seguridad interna. Se desarrolla un ataque en el que el atacante está conectado físicamente a la red interna de la compañía, pudiendo adoptar dos perfiles diferenciados: conectado sin usuario autenticado y conectado como usuario autenticado.
4. Auditoría técnica de seguridad wireless. En esta fase se audita la seguridad real de los accesos vía wireless al interior de las redes privadas de la organización tanto lógicamente (validación de la seguridad de los protocolos WEP, WPA ...), como físicamente (ubicación de puntos de acceso y antenas).
5. Auditoría técnica de seguridad de accesos. En esta fase se audita la implementación de los sistemas de autenticación segura como RSA, no segura como usuario/contraseña y vía VPN.
6. Aplicación de técnicas de ingeniería social. La ingeniería social se define como el grupo de ataques asociados a la actitud de los usuarios en su operativa diaria. Una vez acordado un protocolo de actuación con el cliente se desarrollan tres tipos de acciones: acceso telefónico con suplantación de rol, perfil de limpieza deshonesto y revisión de papeleras.
7. Documentación y formación. Al finalizar las auditorías se entregará un informe resultante que contenga el análisis de la situación, el camino seguido por el atacante, recomendaciones y una propuesta de plan de acción. Para finalizar el proyecto se realiza una sesión de concienciación en aspectos prácticos de la seguridad para los usuarios de los sistemas informáticos de la empresa.

CYBALL. Servicios de seguridad global de Abast

ABAST ofrece una amplia oferta de servicios y soluciones para dar respuesta a sus necesidades en ciberseguridad y seguridad del negocio. Las estructuramos en 4 capas:

GOBIERNO: Alineación estratégica seguridad/negocio. Tratamiento del riesgo. Análisis coste/beneficio. Medición madurez de la seguridad.

GESTIÓN: Auditorías de Seguridad. Continuidad de negocio. Cumplimiento normativo/legal. Gestión de crisis y de incidencias. Formación y concienciación.

OPERACIONES (SOC/MDR): Monitorización de la Seguridad 24x7. Detección de Amenazas e incidentes. Prevención de brechas. Respuesta a los incidentes.

INFRAESTRUCTURA: Asesoramiento e implantación de infraestructura/soluciones de seguridad TI. Administración de la seguridad TI.

abast cyball 360º

Para más información:
seguridad@abast.es

abast
www.abast.es · info@abast.es

Tel. 933 666 900
Fax 933 666 910
Carrer Equador 39-45
08029 Barcelona

Tel. 914 061 601
Fax 914 061 604
Calle de la Basílica 19, 9° B
28020 Madrid

Tel. 97 170 68 82
Calle Fluviá 1, Bajos dcha.
Despacho 25 (Son Fuster)
07009 Palma de Mallorca