Hacking Ètic

Auditar la Seguretat

www.abast.es

L'objectiu de les auditories de seguretat, conegudes com "Hacking Ètic", és comprovar els nivells de seguretat reals dels sistemes d'informació i elaborar un pla d'acció en base a recomanacions que redueixin o eliminin els riscos associats a les vulnerabilitats detectades.

De vegades, l'objectiu d'aquest tipus de serveis és trobar indicis i / o evidències d'activitats il·lícites per part de personal antic o actual de l'organització en perjudici d'aquesta: fuites d'informació, amenaces o espionatge industrial. Aquest tipus de serveis es coneixen com Auditories forenses.

Beneficis

- Coneixement del grau de vulnerabilitat dels sistemes d'informació. Coneixement que ha de permetre la reducció d'aquells riscos que poden comprometre la confidencialitat i integritat de l'actiu més valuós de qualsevol organització que és la informació que gestiona.
- Millora de la seguretat de l'organització. L'auditoria de seguretat ha de contribuir a millorar la robustesa dels sistemes d'informació davant de possibles atacs i mals usos externs i interns.
- Formació i conscienciació dels empleats de l'organització per fomentar un comportament i actitud en la seva operativa diària que permeti millorar la seguretat de la informació, evitant riscos innecessaris.

Retorn de la Inversió en Seguretat (ROSI)

Els costos associats a un servei de seguretat com el que es presenta són molt inferiors als costos que la nostra empresa o organització hauria de suportar en cas que es materialitzessin les amenaces associades a les vulnerabilitats existents.

És difícil quantificar les pèrdues associades a un escenari en què els nostres sistemes es veuen compromesos.

Els elements a tenir en compte són:

- Hores de treball associades a la determinació de la causa de l'atac i a l'avaluació de les pèrdues en integritat i confidencialitat de la informació.
- Hores necessàries en establir i reparar els sistemes afectats.
- Possibles multes, sancions i indemnitzacions.
- Costos d'inactivitat.
- Costos associats a una possible pèrdua de confiança dels clients, dany a la imatge corporativa i pèrdua de confiança del públic general.
- Possible trencament de contractes de confidencialitat amb clients o proveïdors.

Per què ABAST?

ABAST disposa d'una gran experiència en aquest tipus de projectes en multitud de clients com ara entitats esportives professionals, empreses constructores, empreses del sector logístic, empreses de gestió patrimonial, etc.

ABAST, com a empresa de serveis integrals, l'ajudarà a establir i implementar aquelles recomanacions que sorgeixin de l'auditoria, que millor s'adaptin a les necessitats específiques del seu negoci o organització. Tan important com detectar les vulnerabilitats existents, és determinar i prioritzar aquelles mesures organitzatives i tècniques que permetin establir un nivell de seguretat acceptable per al seu negoci.

La nostra metodologia

Un projecte complet de hacking ètic comprèn tots els punts que s'enumeren a continuació. No obstant això, cada projecte s'estudia individualment i es realitza una proposta de serveis que pot combinar diversos dels àmbits d'auditoria que es descriuen a continuació en funció de les necessitats específiques de cada client.

1. Auditoria tècnica de seguretat perimetral. Es desenvolupa un atac perimetral cec des de l'exterior en el qual es desconeix la infraestructura informàtica de l'empresa (atac de "caixa negra").
2. Auditoria tècnica de seguretat d'aplicacions web. Una de les principals portes d'entrada des de l'exterior als repositoris d'informació de les organitzacions és l'accés via web. En aquesta fase s'audita el codi desenvolupat en les pàgines que donen accés a informació no pública.
3. Auditoria tècnica de seguretat interna. Es desenvolupa un atac en el qual l'atacant està connectat físicament a la xarxa interna de la companyia, podent adoptar dos perfils diferenciats: connectat sense usuari autenticat i connectat com a usuari autenticat.
4. Auditoria tècnica de seguretat wireless. En aquesta fase s'audita la seguretat real dels accessos via wireless a l'interior de les xarxes privades de l'organització tant lògicament (validació de la seguretat dels protocols WEP, WPA ...), com físicament (ubicació de punts d'accés i antenes).
5. Auditoria tècnica de seguretat d'accessos. En aquesta fase s'audita la implementació dels sistemes d'autenticació segura com RSA, no segura com a usuari / contrasenya i via VPN.
6. Aplicació de tècniques d'enginyeria social. L'enginyeria social es defineix com el grup d'atacs associats a l'actitud dels usuaris en la seva operativa diària. Un cop acordat un protocol d'actuació amb el client es desenvolupen tres tipus d'accions: accés telefònic amb suplantació de rol, perfil de neteja deshonest i revisió de papereres.
7. Documentació i formació. A l'acabar les auditories es lliurarà un informe resultant que contingui l'anàlisi de la situació, el camí seguit per l'atacant, recomanacions i una proposta de pla d'acció. Per finalitzar el projecte es realitza una sessió de conscienciació en aspectes pràctics de la seguretat per als usuaris dels sistemes informàtics de l'empresa.

CYBALL. Serveis de seguretat global d'Abast

ABAST ofereix una àmplia oferta de serveis i solucions per donar resposta a les seves necessitats en ciberseguretat i seguretat del negoci. Les estructurem en 4 capes:

GOVERN: Alineació estratègica seguretat / negoci. Tractament del risc. Anàlisi cost / benefici. Medició de la maduresa de la seguretat.

GESTIÓ: Auditories de Seguretat. Continuïtat del negoci. Compliment normatiu / legal. Gestió de crisi i d'incidències. Formació i conscienciació.

OPERACIONS (SOC/MDR): Monitorització de la Seguretat 24x7. Detecció d'Amenaces i incidents. Prevenció de bretxes. Resposta als incidents.

INFRAESTRUCTURA: Assessorament i implantació de infraestructura / solucions de seguretat TI. Administració de la seguretat TI.

abast cyball 360º

Per a més informació:
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