Audity systémov a zariadení

AEC

Urobili ste penetračné testy, a napriek tomu si nie ste istí, či je zabezpečenie konkrétneho serveru alebo inej aplikačnej platformy dostatočné? Potrebujete dôkladne preveriť zabezpečenie kľúčových prvkov vášho informačného systému? Riešením týchto a mnohých ďalších problémov je vykonanie detailného auditu zabezpečenia konkrétnych systémov alebo zariadení v rámci informačného systému organizácie.

Zatiaľ čo pri penetračných testoch sa špecialisti AEC stavajú skôr do roly potenciálneho útočníka, pri auditoch technického zabezpečenia pristupujú ku skúmanému prvku skôr v role systémového administrátora a implementátora odporúčaných opatrení na zvýšenie jeho bezpečnosti. Pri kontrole nastavenia jednotlivých systémov využívame znalosti a skúsenosti bezpečnostných a systémových špecialistov AEC, odporúčania výrobcov pre hardening daných systémov a pod.

Všetky nájdené nedostatky sú podrobne opísané v správe z auditu. Sú tu opísané riziká týchto zraniteľností a nechýbajú, samozrejme, ani návrhy na ich odstránenie (prípadne minimalizáciu rizika).

www.aec.sk

Audity systémov a zariadení

V rámci technických auditov poskytujeme tieto služby

Audit konfigurácie aktívnych sieťových prvkov

Jedným z najviac rizikových miest siete, s ktorým je spojené veľké množstvo neoprávnených prienikov, sú práve aktívne sieťové prvky. Pri ich analýze sa preto zameriavame najmä na oblasti nastavenia statických tabuliek na aktívnych sieťových prvkoch, NAT – nastavenie prekladu adries, sieťový monitoring, zabezpečenie administratívneho rozhrania atď.

Audit konfigurácie operačných systémov na serveroch

Previerka konfigurácie operačných systémov (OS) na serveroch sa robí pomocou systémových prostriedkov a špecializovaných nástrojov. Previerku robia špecialisti na bezpečnosť jednotlivých platforiem. Previerka Windows systémov je zameraná napr. na posúdenie nastavenia politiky hesiel (Pasword Policy), politiky auditu (Audit Policy), Active Directory a pod. Operačné systémy typu UNIX sú preverované najmä z hľadiska konfigurácie a bezpečnosti služieb (/etc/conf/) atď.

Audit konfigurácie firewallov a systémov IDS/IPS

Analýzu vykonávajú špecialisti na firewally, ktorí z pozície administrátora analyzujú nastavenie týchto kľúčových bezpečnostných prvkov. Pri firewalloch sa môže auditovať tak samotná bezpečnosť aplikácie, ako aj definované pravidlá. Výsledkom analýzy IDS/IPS je predovšetkým posúdenie vhodnosti nastavenia systémov klienta a prípadné návrhy ich optimalizácie.

Audit bezpečnosti špeciálnych systémov, aplikácií a služieb

Previerka vybraných aplikácií z pohľadu spoľahlivosti, konfigurácie, integrity, autentizácie a dôvernosti dát. Ide napr. o previerky aplikačných serverov, databázových serverov, webových serverov a mnoho ďalších aplikácií a služieb, ktoré môžu zahŕňať oblasti ako bezpečnosť kritických dátových tokov, chyby aplikácií, možnosť zneužitia aplikácie, stabilita aplikácií, implementácia šifrovania, PKI a pod.

Prínosy riešení

- Viac ako 20 rokov skúseností na poli bezpečnosti v Českej a Slovenskej republike.
- Široký tím certifikovaných audítorov a administrátorov so skúsenosťami z niekoľkých desiatok vykonaných auditov ročne.
- Využívame komerčné, free a tiež vlastné nástroje a skripty na zber dát a následnú analýzu.
- Vyhodnotenie úrovne zabezpečenia ICT spoločnosti a definície reálnych rizík v kontexte predpokladaného dopadu na business.
- Vykonávame audity v súlade so štandardmi PCI-DSS a PA-DSS.

Ďalšie špecializované audity

Audity v súlade so štandardmi PCI-DSS a PA-DSS.

Špecializované komplexné audity, kde je braný ohľad na typ auditovaného zariadenia a jeho umiestnenie a nadväznosť na ďalšiu IT infraštruktúru. Nerieši sa ako jednotlivý audit, ale ako audit celej infraštruktúry.

Audity topológie a infraštruktúry

Preverenie prevádzkovanej topológie siete prípadne cloudov z pohľadu bezpečnosti prístupov tretích strán, partnerov, zamestnancov, navrhnutých DMZ oddelení a zabezpečenie core systémov atď

Metodika

Pri realizácii bezpečnostných auditov využívame ucelenú a priebežne aktualizovanú metodiku AEC vychádzajúcu z metodík a odporučení popredných organizácií zaoberajúcich sa bezpečnosťou informačných technológií.

- Odporúčania výrobcov týkajúce sa hardeningu auditovaných HW, OS a SW.
- Odporúčania organizácie IETF (Internet Engineering Task Force) – organizácie vydávajúcej RFCs, tzv. štandardy internetu.
- Odporúčania organizácie NIST (napr. NIST SP 800-44 Guidlines on Securing Public Web Servers).
- CVE – Common Vulnerabilities and Exposures – štandardizovaný slovník všeobecných zraniteľností a ohrození.
- Common Criteria (ISO/IEC 15408) – štandard pre hodnotenie úrovne bezpečnosti systémov a ďalšie.

Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283
Praha – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466