



Audity systémů a zařízení

Provedli jste penetrační testy, a přesto si nejste jisti, zda je zabezpečení konkrétního serveru nebo jiné aplikační platformy dostatečné? Potřebujete důkladně prověřit zabezpečení klíčových prvků vašeho informačního systému?

Řešením těchto a řady dalších problémů je provedení detailního auditu zabezpečení konkrétních systémů a/nebo zařízení v rámci informačního systému organizace.

Zatímco při penetračních testech se specialisté AEC staví spíše do role potenciálního útočníka, při auditech technického zabezpečení přistupují ke zkoumanému prvku spíše v roli systémového administrátora a implementátora doporučených opatření ke zvýšení jeho bezpečnosti. Při kontrole nastavení jednotlivých systémů využíváme znalostí a zkušeností bezpečnostních a systémových specialistů AEC, doporučení výrobců pro hardening daných systémů apod.

Všechny nalezené nedostatky jsou podrobně popsány ve zprávě z auditu. Jsou zde popsána rizika těchto zranitelností a nechybí samozřejmě i návrhy na jejich odstranění (případně minimalizaci rizika).

Audit konfigurace aktivních síťových prvků.

Jedním z nejvíce rizikových míst sítě, se kterým je spojeno velké množství neoprávněných průniků, jsou právě aktivní síťové prvky. Při jejich analýze se proto zaměřujeme zejména na oblasti nastavení statických tabulek na aktivních síťových prvcích, NAT – nastavení překladu adres, síťový monitoring, zabezpečení administrativního rozhraní atd.

Audit konfigurace operačních systémů na serverech.

Prověrka konfigurace operačních systémů (OS) na serverech je prováděna pomocí systémových prostředků a specializovaných nástrojů.

Prověrku provádějí specialisté na bezpečnost jednotlivých platforem. Prověrka systémů Windows je zaměřena např. na posouzení nastavení politiky hesel (password policy), politiky auditu (audit policy), active directory apod. Operační systémy typu UNIX jsou prověřovány zejména z hlediska konfigurace a bezpečnosti služeb (/etc/conf/) atd.

Přínosy našich služeb

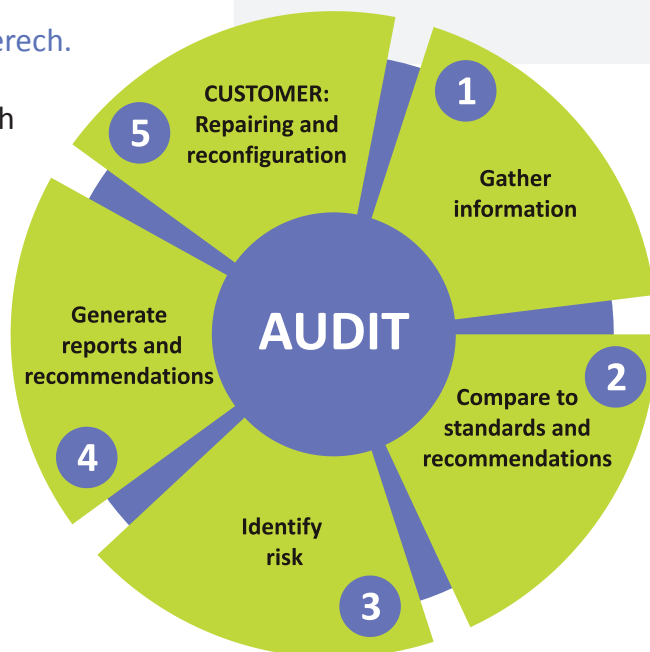
Více jak 20 let zkušeností na poli bezpečnosti v České a Slovenské republice.

Široký tým certifikovaných auditorů a administrátorů se zkušenostmi z několika desítek provedených auditů ročně.

Využíváme komerčních, free a také vlastních nástrojů a skriptů pro sběr dat a následnou analýzu.

Vyhodnocení úrovně zabezpečení ICT společnosti a definice reálných rizik v kontextu předpokládaného dopadu na business.

Provádíme audity v souladu se standardy PCI-DSS a PA-DSS.



Audit konfigurace firewallů a systémů IDS/IPS.

Analýza je prováděna specialisty na firewally, kteří z pozice administrátora analyzují nastavení těchto klíčových bezpečnostních prvků.

U firewallů se mohou auditovat jak samotná bezpečnost aplikace, tak i definovaná pravidla.

Výsledkem analýzy IDS/IPS je především posouzení vhodnosti nastavení systémů klienta a případné návrhy jejich optimalizace.

Audit bezpečnosti speciálních systémů, aplikací a služeb.

Prověrka vybraných aplikací z pohledu spolehlivosti, konfigurace, integrity, autentizace a důvěrnosti dat. Jedná se např. o prověrky aplikačních serverů, databázových serverů, webových serverů a mnoho dalších aplikací a služeb, které mohou zahrnovat oblasti jako bezpečnost kritických datových toků, chyby aplikací, možnost zneužití aplikace, stabilita aplikací, implementace šifrování, PKI apod.

Další specializované audity a testy (dle individuálních požadavků klienta).

Audity v souladu se standardy PCI-DSS a PA-DSS.

Specializované komplexní audity, kde je brán ohled na typ auditovaného zařízení a jeho umístění a návaznost na další IT infrastrukturu. Neřeší se jako jednotlivý audit, ale jako audit celé infrastruktury.

Audity topologie a infrastruktury - prověření provozované topologie sítě, případně cloudů z pohledu bezpečnosti přístupů třetích stran, partnerů, zaměstnanců, navržených DMZ oddělení a zabezpečení core systémů atd.

Metodiky

Při realizaci bezpečnostních auditů využíváme ucelenou a průběžně aktualizovanou metodiku AEC vycházející z metodik a doporučení předních organizací zabývajících se bezpečností informačních technologií:

- Doporučení výrobců o hardeningu auditovaných HW, OS a SW.
- Doporučení organizace IETF (Internet Engineering Task Force) – organizace vydávající RFCs, tzv. standardy internetu.
- Doporučení organizace NIST (např. NIST SP 800-44 Guidelines on Securing Public Web Servers).
- CVE – Common Vulnerabilities and Exposures – standardizovaný slovník obecných zranitelností a ohrožení.
- Common Criteria (ISO/IEC 15408) – standard pro hodnocení úrovně bezpečnosti systémů a další.

Reference

Pokud se chcete přesvědčit o kvalitě výstupů, které Vám poskytneme, můžeme předložit vzorový report z auditů k nahlédnutí. Pokud máte zájem zjistit více o tom, jak pracujeme, neváhejte se na nás zeptat v některé z následujících společností. Jedná se pouze o vybrané a schválené reference z poslední doby.

- **Volksbank** – banka si nás vybrala jako spolehlivého partnera. Provedli jsme audity vybraných kritických systémů této banky.
- **ING bank, a.s.** – provedli jsme rozsáhlé penetrační testy a audity IS ING, a to nejen pro ING Česká republika.
- Pravidelně testujeme bezpečnost pro zákazníky, jako jsou T-Mobile, Komerční banka, Česká spořitelna, ČSOB, Zuno bank AG či Poštová banka.

AEC, spol. s r.o.
Purkyňova 2845/101
612 00 Brno, Czech Republic
Phone: +420 530 507 200
Fax: +420 530 507 220

AEC, spol. s r.o.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC

DATA SECURITY