Bezpečnostný audit

Audit informačnej bezpečnosti je prostriedkom na overenie, či informačná bezpečnosť alebo jej časť spĺňa požiadavky na ňu kladené. Požiadavky môžu byť definované vašou organizáciou, zákonom alebo normou. Audítor v priebehu auditu identifikuje všetky možné riziká, ktoré sa vzťahujú na aktíva spoločnosti. Kvalita auditu závisí vo veľkej miere od použitej metodiky, nástrojov a od kvality audítorov. Spoločnosť ESET ponúka služby profesionálnych špecialistov, ktorí sú držiteľmi medzinárodného certifikátu CISA (Certified Information System Auditor) a členmi organizácie ISACA (Information Systems Audit and Control Association).

Výsledkom auditu je jedna alebo viac auditných správ, ktoré obsahujú zoznam zistení. Ku každému zisteniu je pridelená úroveň možného rizika. Táto klasifikácia umožňuje so zisteniami ďalej narábať, napríklad prostredníctvom systému riadenia informačnej bezpečnosti (ISMS). Audit informačnej bezpečnosti od spoločnosti ESET prináša možnosť nezávislého pohľadu na situáciu vo vašej organizácii.

PONÚKANÉ SLUŽBY

Spoločnosť ESET ponúka tieto druhy auditov:

Audit procesov – v rámci tohto auditu skontrolujeme nastavenie procesov, ktoré organizácia v oblasti informačnej bezpečnosti používa. Typickým prípadom môžu byť procesy riadenia prístupu alebo skupina procesov súvisiacich s prevádzkou IT (správa zraniteľností, konfiguračný manažment...).

Audit informačnej bezpečnosti alebo voči ISO/IEC 27002:2005 (ISO/IEC 17799:2005) – vysokoúrovňový audit, pri ktorom sa kontroluje nastavenie bezpečnostných mechanizmov voči ISO norme. Pokrýva všetky oblasti informačnej bezpečnosti a zahŕňa výber dobrých praktík. Je vhodný v prípade, že začínate s budovaním informačnej bezpečnosti.

Audit ISMS – posudzuje zhodu zavedeného systému riadenia a implementovaných opatrení voči norme ISO/IEC 27001:2005. Spoločnosť ESET nie je certifikačným orgánom na normu ISO 27001:2005, avšak túto službu je možné využiť ako predcertifikačný audit. Môže taktiež slúžiť ako „interný" audit, v prípade, že organizácia nemá vlastného interného audítora.

Technický audit – audit technického nastavenia informačného systému alebo jeho časti (napr. sieť, DMZ, doména Windows...) voči existujúcim odporúčaniam výrobcu alebo medzinárodne uznávanej inštitúcie (NSA, NIST, CIS...). Tento typ auditu je vhodné kombinovať s vyššie uvedeným auditom procesov. Ak sa napríklad odhalí nedostatočné zaplátanie doménových radičov, pričom proces správy zraniteľností je nefunkčný, tak jednorazové odstránenie nedostatkov zistených prostredníctvom technického auditu problém nevyrieši.

Penetračné testovanie – špecializovaná forma auditu z pohľadu útočníka. Zákazník má možnosť overiť si skutočné fungovanie bezpečnostných prvkov na ceste medzi útočníkom a aktívami organizácie, či už ide o firewally, IPS, hardening serverov, alebo fungovanie bezpečnostného monitoringu. Rozdielom oproti skutočnému útoku je systematická identifikácia čo najväčšieho množstva zraniteľností na cieľových aktívach bez negatívnych dopadov na prevádzku.

HLAVNÉ VÝHODY

Všeobecné výhody auditu informačnej bezpečnosti je možné zhrnúť do nasledovných bodov:

- Nezávislé posúdenie stavu informačnej bezpečnosti
- Detailný zoznam zistení spolu s návodom na ich odstránenie
- Zvýšenie úrovne informačnej bezpečnosti

Druh auditu	Výhody
Audit procesov	Identifikácia slabín v dizajne procesov Zvýšenie efektívnosti bezpečnostných procesov
Audit podľa ISO/IEC 27002:2005	Získanie celkového prehľadu o stave informačnej bezpečnosti Vysokoúrovňový pohľad na problémy a odporúčania na ich riešenie Získanie podkladu pre manažment spoločnosti o potrebe implementovať bezpečnostné opatrenia Zlepšenie efektívnosti opatrení
Audit ISMS	Získanie prehľadu o rozdiele implementovaného ISMS voči norme Prehľad o stave opatrení voči norme Annex A
Technický audit	Prehľad o problémoch v konfigurácii zariadení Návod pre administrátorov na odstránenie zistených slabín Zlepšenie efektívnosti technických opatrení aplikovaných na zariadenia
Penetračné testovanie	Pohľad útočníka na vaše aktíva Návod na odstránenie zistených slabín

O ESET Services Spoločnosť ESET, založená v roku 1992, je svetovým výrobcom bezpečnostného softvéru pre domácich i firemných zákazníkov. Rozširovanie portfólia služieb vyústilo v roku 2008 do akvizície Šetrnet, českej spoločnosti s dlhoročnými skúsenosťami v oblasti IT a bezpečnosti. V roku 2009 bola vytvorená divízia ESET Services, ktorá poskytuje produkty manažovanej bezpečnosti a konzulting pre malých a stredných podnikateľov (SMB) a pre veľkých firemných (Enterprise) zákazníkov. Výhradné zameranie sa na služby informačnej bezpečnosti sleduje poskytnutie maximálnej pridanej hodnoty v tejto oblasti. Zázemie ESET, globálne uznávaného dodávateľa bezpečnostných riešení a dôraz na odbornosť pracovníkov ESET Services je garantom kvality poskytovaných služieb.