Bezpečnostní Audit

Audit informační bezpečnosti je prostředkem na ověření, jestli informační bezpečnost nebo její část plní požadavky na ní kladené. Požadavky mohou být definované Vaší organizací, legislativou nebo normou. Auditor v průběhu auditu identifikuje všechny možná rizika, které se vztahují na aktiva společnosti. Kvalita auditu závisí ve velké míře na použité metodice, nástrojích a kvalitě auditorů. Společnost ESET nabízí služby profesionálních specialistů, kteří jsou držiteli mezinárodního certifikátu CISA (Certified Information System Auditor) a členy organizace ISACA (Information Systems Audit and Control Association).

Výsledkem auditu je jedna nebo více auditních zpráv, které obsahují seznam zjištění. Ke každému zjištění je přidělená úroveň možného rizika. Tato klasifikace umožňuje se zjištěními dále pracovat, například prostřednictvím systému řízení informační bezpečnosti (ISMS). Audit informační bezpečnosti od společnosti ESET přináší možnost nezávislého pohledu na situaci ve vaší organizaci.

NABÍZENÉ SLUŽBY

Společnost ESET nabízí tyto druhy auditů:

Audit procesů - v rámci tohoto auditu zkontrolujeme nastavení procesů, které organizace v oblasti informační bezpečnosti používá. Typickým případem můžou být procesy řízení přístupu nebo skupina procesů související s provozem IT (správa zranitelností, konfigurační management, ...).

Audit informační bezpečnosti nebo vůči ISO/IEC 27002:2005 (ISO/IEC 17799:2055) - vysokoúrovňový audit, při kterém se kontroluje nastavení bezpečnostních mechanizmů vůči ISO normě. Pokrývá všechny oblasti informační bezpečnosti a zahrnuje výběr dobrých praktik. Je vhodný v případě, že začínáte s budováním informační bezpečnosti.

Audit ISMS - posuzuje shodu zavedeného systému řízení a implementovaných opatření vůči normě ISO/IEC 27001:2005. Společnost ESET není certifikačním orgánem na normu ISO 27001:2005, avšak tuto službu je možné využít jako předcertifikační audit. Může také sloužit jako interní audit v případě, že organizace nemá vlastního interního auditora.

Technický audit - audit technického nastavení informačního systému nebo jeho částí (např. síť, DMZ, doména Windows ,...) vůči existujícím doporučením výrobců nebo mezinárodně uznávané instituce (NSA, NISIT, CIS, ...). Tento typ auditu je vhodné kombinovat s výše uvedeným auditem procesů. Když se například odhalí nedostatečné záplatování doménových řadičů, přičemž proces správy zranitelností je nefunkční, tak jednorázové odstranění nedostatků zjištěných prostřednictvím technického auditu problém nevyřeší.

Penetrační testování - specializovaná forma auditu z pohledu útočníka. Zákazník má možnost ověřit si skutečné fungování bezpečnostních prvků na cestě mezi útočníkem a aktivy organizace, ať už jde o firewally, IPS, hardening serverů nebo fungování bezpečnostního monitoringu. Rozdílem oproti skutečnému útoku je systematická identifikace co největšího množství zranitelností na cílových aktivech bez negativních dopadů na provoz.

HLAVNÍ VÝHODY

Všeobecné výhody auditu informační bezpečnosti můžeme shrnout do následujících bodů:

- Nezávislé posouzení stavu informační bezpečnosti.
- Detailní seznam zjištění spolu s návodem na jejich odstranění.
- Zvýšení úrovně informační bezpečnosti..

Druh auditu	Výhody
Audit procesů	Identifikace slabin s designu procesů. Zvýšení efektivnosti bezpečnostních procesů.
Audit dle ISO/IEC 27002:2005	Získání celkového přehledu o stavu informační bezpečnosti. Vysokoúrovňový pohled na problémy a doporučení na jejich řešení Získání pohledu pro management společnosti o potřebě implementovat bezpečnostní opatření. Zlepšení efektivnosti opatření.
Audit ISMS	Získání přehledu o rozdílu implementovaného ISMS vůči normě. Přehled o stavu opatření vůči normě Annex A.
Technický audit	Přehled o problémech v konfiguraci zařízení. Návrh pro administrátory na odstranění zjištěných slabin. Zlepšení efektivnosti technických opatření aplikovaných na zařízení.
Penetrační testování	Pohled útočníka na Vaše aktiva Návod na odstranění zjištěných slabin

O ESET Services: Společnost ESET, založena v roce 1992, je světovým výrobcem bezpečnostního softwaru pro domácí i firemní zákazníky. Rozšiřování portfolia služeb vyústilo v roce 2008 do akvizice společnosti Šetrnet, české společnosti s dlouholetými zkušenostmi v oblasti IT a bezpečnosti. V roce 2009 byla vytvořena divize ESET Services, která poskytuje outsourcing bezpečnosti a consulting pro malé a střední podnikatele, ale také pro velké firemní zákazníky. Výhradní zaměření na služby informační bezpečnosti sleduje maximální přínos v této oblasti. Zázemí společnosti ESET, globálně uznávaného dodavatele bezpečnostních řešení a důraz na odbornost pracovníků ESET Services je garancí kvality poskytovaných služeb.