Audit bezpečnosti informačních systémů

BUDOVÁNÍ INFORMAČNÍ BEZPEČNOSTI JE NUTNOSTÍ, ALE K JEJÍMU SKUTEČNÉMU VYBUDOVÁNÍ MUSÍ KAŽDÁ ORGANIZACE POCHOPIT HROZBY, KTERÉ JSOU SOUČÁSTÍ PROSTŘEDÍ, V NĚMŽ ORGANIZACE PŮSOBÍ. HROZBY JSOU OBVYKLE URČOVÁNY POMOCÍ METODICKÉHO HODNOCENÍ BEZPEČNOSTNÍCH RIZIK. A PRÁVĚ AUDIT BEZPEČNOSTI IS SLOUŽÍ K NALEZENÍ TĚCHTO HROZEB A RIZIK A ZÁROVEŇ PŘINÁŠÍ ŘEŠENÍ, JAK JE ELIMINOVAT.

Znáte stav svého informačního systému a rizika spojená s ochranou dat?

Chcete své peníze investovat do správných technologií a na správném místě?

Potřebujete vědět, v jakém stavu informační systém je a jaká nebezpečí mu hrozí?

Popis řešení

Informační bezpečnost je nutností, ale k jejímu skutečnému vybudování musí každá organizace pochopit hrozby, které jsou součástí prostředí, v němž působí. Hrozby jsou obvykle určovány pomocí metodického hodnocení bezpečnostních rizik.

Samotný audit bezpečnosti IS je první částí komplexního procesu řízení informační bezpečnosti, který má podobu Demingova procesního cyklu PDCA (kontinuální vylepšování procesů). Audit bezpečnosti informačního systému tedy nejdříve zkoumá stávající stav informačního systému a na základě jeho výstupů je možné provést analýzu rizik spojenou s doporučením vedoucích k eliminaci rizik.

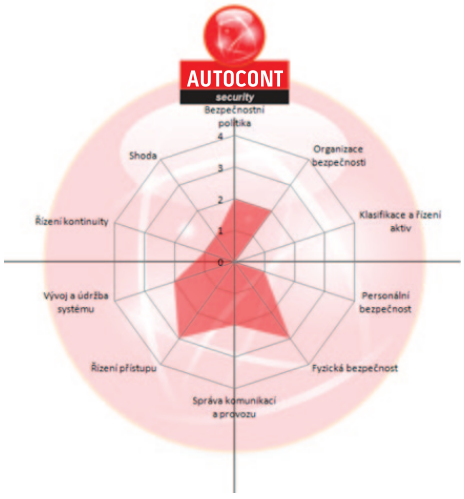
Způsob řešení

Audit je rozdělen do několika fází, které na sebe navazují. Jedná se o fázi plánovací neboli přípravnou, o sběr dat a informací a o analýzu těchto dat. Na základě zmíněných kroků může být uskutečněna prezentace výsledků a připomínkové řízení.

- Příprava a plánování
  Auditor sestaví vlastní plán auditu, definuje jeho rozsah, požadavky na součinnost a rozsah výstupů

PRAKTICKÉ PŘÍNOSY

- Správně a účinně investovat peníze do informačního systému
- Ochránit investice do informačního systému
- Ochránit data, vč. osobních údajů před zneužitím, ochránit firemní tajemství, kontakty, know-how, plány, strategie atd.
- Ochránit dobré jméno a posílit důvěru v tuto organizaci
- Splnit legislativní požadavky související s ochranou dat, včetně požadavků GDPR
- Implementovat technologie, které poskytnou konkurenční výhodu
- Ucházet se o zakázky podmíněné ochranou informací
- Získat certifikaci o kompatibilitě s normou či standardem, který může



- Sběr dat a informací
  Identifikace aktiv a následné ověření, zda jsou na aktiva aplikována odpovídající bezpečnostní opatření (technická i procesní). To umožní identifikovat zranitelnost jednotlivých aktiv.
  V této fázi může klient očekávat, že auditor bude hovořit se zaměstnanci na organizovaných interview/workshopech, bude vyžadovat písemné podklady (politiky, směrnice atd.), žádat prohlídku prostor, anketou se dotazovat zaměstnanců či provádět technická měření.
- Analýza dat
  Zpracování všech zjištěných informací, stanovení pravděpodobnosti zneužití aktiv na základě katalogu hrozeb. Stanovení a kategorizace rizik, navržení odpovídajících opatření.
- Prezentace výsledků a připomínkové řízení
  Prezentace zjištěných skutečností a závěrů. Současně probíhá připomínkové řízení ze strany zákazníka, jelikož se auditor pohybuje v prostředí organizace relativně krátce (cca 2,5 - 3 měsíce) a některé závěry tudíž mohou být zkresleny výjimečnou situací.

Výsledná zpráva z analytické fáze obvykle obsahuje seznam aktiv, seznam hrozeb, seznam rizik a opatření, jak uvedené hrozby eliminovat. Výstupem z auditu je pak auditní zpráva obsahující nálezy typu shoda/neshoda a doporučení k odstranění identifikovaných neshod.

Audit může být pojat jako:

- Čistě technický
  Je posuzována jen a pouze technická stránka bezpečnosti informačního systému. Jsou prováděny penetrační testy, měření v síti apod. Je používán pro ověření technického stavu.
- Procesní
  Posuzuje kompatibilitu bezpečnostního systému s implementovanou bezpečnostní politikou nebo zvolenou normou či standardem, nebo zaměřený na specifickou oblast, jako např. audit shody zpracování osobních údajů s požadavky GDPR.
- Komplexní
  Obsahuje jak technickou, tak procesní část, a to z toho důvodu, že sebelepší technologie nedokáže sama zajistit bezpečnost, protože nedokáže 100% eliminovat lidský faktor.

Podporované nástroje

Audity jsou prováděny certifikovanými auditory, kteří jsou členy ISACA (profesní asociace auditorů), mají certifikaci CISA (certifikát auditora IS) a také prověrku NBÚ (v případě, že daná společnost pracuje s utajovanými informacemi).

Komu je řešení určeno

Řešení je určeno všem firmám, které chtějí čelit hrozbám a eliminovat bezpečnostní rizika s ohledem na strategii společnosti. Také těm, které se snaží nejen ochránit své investice do IS, ale především své dobré jméno.