AutoCont

Audit bezpečnosti informačních systémů

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

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

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

Co umožňuje audit bezpečnosti IS?

- 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.

www.autocont.cz

Popis řešení

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.

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 v prvé řadě zkoumá stávající stav informačního systému a na základě jeho výstupů je možné provést analýzu rizik spojenou s doporučeními vedoucími k eliminaci rizik.

Komu je řešení určeno

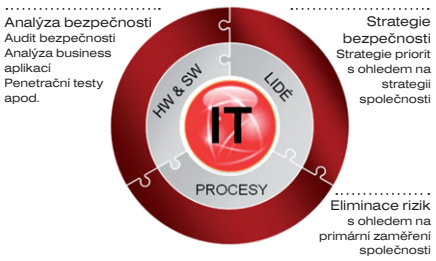
Řešení je určeno všem firmám, které chtějí čelit hrozbám a eliminovat bezpečnostní rizika s ohledem na strategii společnosti. Společnostem, které se snaží nejen ochránit své investice do IS, ale především své dobré jméno.

Způsob řešení

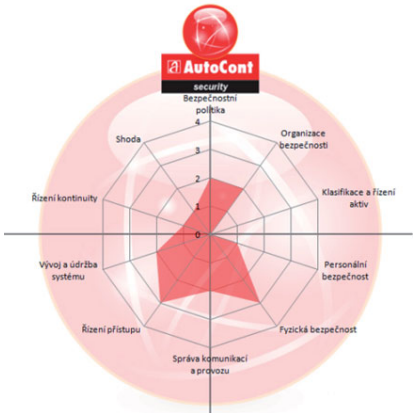
Audit je rozdělen do několika fází, které na sebe navazují. Jedná se o fázi plánovací neboli přípravnou, o sběr dat a informací a v poslední řadě o analýzu těchto dat. Na základě těchto kroků může být uskutečněna prezentace výsledků a připomínkové řízení.

- Příprava a plánování - auditor sestaví vlastní plán auditu, definuje jeho rozsah, požadavky na součinnost a rozsah výstupů
- Sběr dat a informací - identifikace aktiv a následné ověření, zda jsou na aktiva aplikována odpovídající bezpečnostní opatření (technická i procesní). To umožňuje 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.

AutoCont bezpečnostní cyklus



- Analýza dat - zpracování všech zjištěných informací, stanovení pravděpodobnosti zneužití aktiv na základě katalogu hrozeb. Stanovení a kategorizace rizik, navržení odpovídajících opatření.



Ukázka jednoho z grafů

Prezentace výsledků a připomínkové řízení - prezentace zjištěných skutečností a závěrů. Zároveň 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 obvykle obsahuje seznam aktiv, seznam hrozeb, seznam rizik aktivům a opatření, jak uvedené hrozby eliminovat.

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.
- 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.

Praktické přínosy

- Správně a účinně investovat peníze do informačního systému
- Ochránit investice do informačního systému
- Ochránit data 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
- Implementovat technologie, které poskytnou konkurenční výhodu
- Ucházet se o zakázky podmíněné ochranou informací
- Získat certifikaci o kompatibilitě s normou či standardem, který může být vyžadován ve veřejných zakázkách

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).

IT infrastruktura

Problematika IT infrastruktury je velice široká. Začíná u kabelů položených v zemi a naftových generátorů zajišťujících elektrický proud při výpadku, končí školením uživatelů a právními rozbory, zda vaše informační systémy splňují všechny zákonné požadavky. Ne každý zákazník pochopitelně potřebuje a využije vše. Záleží na velikosti podniku, na jeho zaměření a zejména na úloze, která se v danou chvíli řeší. Důležité však je, že ať potřebujete v oblasti informatiky cokoli, my to dovedeme zařídit. V rámci řešení a služeb IT infrastruktury zákazníkům nabízíme tyto oblasti:

- Dodávky hardwaru a softwaru
- Hardwarová infrastruktura a datová centra
- Systémová infrastruktura
- Komunikační infrastruktura
- Klientské prostředí
- Komunikace a spolupráce
- Bezpečnost
- Management a monitoring IT
- Provoz a podpora IT
- Cloud
- Poradenství a strategické plánování IT

Kontakty

V případě zájmu se obraťte na našeho obchodního zástupce, nebo nás kontaktujte telefonicky na +420 596 152 222 eventuálně e-mailem na security@autocont.cz.

AutoCont