Ochrana a zabezpečení dat

Počítačová bezpečnost je obor informatiky, který se zabývá zabezpečením informací v počítačích (odhalení a zmenšení rizik spojených s používáním počítače). Počítačová bezpečnost zahrnuje tyto úkoly:

- zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému,
- ochranu před neoprávněnou manipulací s daty,
- ochranu informací před krádeží (nelegální tvorba kopií dat) nebo poškozením,
- bezpečnou komunikaci a přenos dat (kryptografie),
- bezpečné uložení dat,
- celistvost a nepodvrhnutelnost dat.

Charakteristika

Počítačová ochrana je často více zaměřená na techniku a matematiku, než některé jiné počítačové oblasti. Spočívá ve třech krocích:

1. prevence – ochrana před hrozbami
2. detekce – odhalení neoprávněných (skrytých, nezamýšlených) činností a slabých míst v systému
3. náprava – odstranění slabého místa v systému

Zlepšení počítačové bezpečnosti může zahrnovat následující kroky:

- omezení fyzického přístupu k počítači pouze pro ty, kteří budou dodržovat bezpečnost při práci s počítačem a daty
- použití hardwarových zařízení, která vynucují bezpečnostní opatření, což snižuje závislost počítačové bezpečnosti na software (počítačových programech)
- využití mechanismů operačního systému, která vynucují pravidla chování programů, aby byl omezen rozsah programů, kterým je nutné důvěřovat
- využití záznamů o změnách v programu (verzování), které je možné využít pro sledování jejich vývoje

Pokud budeme mluvit o počítačové bezpečnosti, nesmíme zapomenout na bezpečnost operačního systému, bezpečnostní projekt a bezpečné šifrování (kryptografie).

Bezpečnostní projekt

Aby byla ochrana počítačového systému efektivní, je potřebné vypracovat bezpečnostní projekt. Cílem tohoto projektu je docílení takového stavu, aby úsilí, riziko odhalení a finanční prostředky potřebné na narušení bezpečnostního systému byly adekvátní v porovnání s hodnotou, která je bezpečnostním systémem chráněna.

Části bezpečnostního projektu

Zabezpečení fyzického přístupu

Zabezpečení fyzického přístupu spočívá v zabránění přístupu nepovolaných osob k částem počítačového systému. Na toto zabezpečení se používají bezpečnostní prvky jako přidělení rozdílných práv zaměstnancům, elektronické zámky, poplašné zařazení, kamerové systémy, autorizační systémy chráněné hesly, čipovými kartami, autentizační systémy na snímání otisků prstů, dlaně, oční duhovky, rozpoznání hlasu, auditovací systémy na sledování a zaznamenávání určitých akcií zaměstnanců (vstup zaměstnanců do místnosti, přihlášení se do systému, kopírování údajů atd.).

Zabezpečení počítačového systému

Zabezpečení počítačového systému spočívá v zabezpečení systému před útokem crackerů, škodlivých programů (viry, červy, trojské koně, spyware, adware, ...). do této části patří i zaškolení zaměstnanců, aby se chovali v souladu s počítačovou bezpečností a dodržovali zásady bezpečného chování na síti.

Zabezpečení informací

Zabezpečení informací spočívá v bezpečném zálohování dat. Záloha dat by měla být vytvořena tak, aby ji neohrozil útočník ani přírodní živelní pohroma (požár, záplavy, pád letadla…). Zálohovaná data je také potřeba chránit proti neoprávněné manipulaci použitím vhodného šifrovacího systému.

Ekonomické a právní zabezpečení

Ekonomické a právní zabezpečení spočívá ve správné motivaci a postihu zaměstnanců.