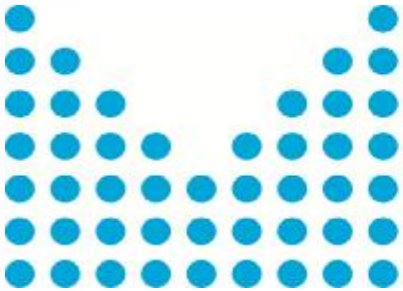

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Cloud pro utajované informace

Utajované informace (UI)

- **Zákon č. 412/2005 Sb.,** o ochraně utajovaných informací a o bezpečnostní způsobilosti
- **Vyhláška č. 523/2005 Sb.,** o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, **ve znění vyhlášky č. 453/2011 Sb.**
- **Informační systém pro zpracování UI (IS)** = systém pro zpracování UI (jeden nebo více počítačů, programové vybavení, periferní zařízení, správa tohoto IS , vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací).
- **IS musí být certifikován NBÚ.**
- **Komunikační systém pro zpracování UI (KS)** = systém zajišťující přenos UI mezi koncovými uživateli (koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy)
- **KS musí mít projekt bezpečnosti KS schválený NBÚ**. KS NBÚ **necertifikuje** (jádro KS je certifikovaný kryptografický prostředek) .

CLOUD

Klíčovým problémem pro bezpečnost CLOUDu je **použití VIRTUALIZACE**

- **Tradiční přístup** vybudovaný na stabilní HW a SW infrastruktůře umožňuje relativně jednoduché, transparentní zajištění bezpečnosti – vybudování obranného perimetru, nacílení bezpečnostních opatření na konkrétní místa. Využívají se ověřené metodiky a postupy.
- **Virtualizace** – přechod od fyzických serverů k virtuálním. Nelze postupovat v zajištění bezpečnosti tradičním způsobem - **mizí(rozmývá se) jasně definovaný obranný perimetr** , cílená statická bezpečnostní opatření. V rámci fyzických serverů většina komunikace probíhá mezi virtuálními stroji (VS). Kriticky důležitá pro sdílení zdrojů (multitenancy) je přísná kontrola přístupu pro správce, uživatele, stejně jako kontrola změn na úrovni systému. Současně mohou pracovat uživatelé i administrátoři.
- Při využití cloudu v IS pro zpracování UI není nutńé vynalézat už vynalezené. Je možné použít standardní postupy a metodiky, ale je nutné brát do úvahy specifické provozní a bezpečnostní vlastnosti technologie cloudu zejména použití virtualizace.

Bezpečnostní problémy virtualizace

- Absence ochrany hypervizoru. Neoprávněné získání přístupu k řízení systému virtuálních serverů.
- Při slabé izolaci VS může VS útočníka proniknout přes hypervizor a získat řízení fyzického serveru (VM Escape)
- Neoprávněné interakce mezi VS útočníka a fyzickým serverem obvykle přes sdílené paměťové zdroje (např. přes sdílenou paměť (shared clipboard) apod.)
- Neoprávněný síťový přístup VS útočníka dovnitř virtuální infrastruktury a monitorování síťového provozu mezi VS.
- Útoky na jiné VS prostřednicvím VS útočníka (VM Hopping)
- Monitorování činnosti VS ze strany fyzicického serveru.
- Neoprávněný přístup uživatelů k virtuálním strojům (VS) a instalace škodlivého SW. Chybějící kontrola činností uživatelů a jimi prováděných změn konfigurace virtuálního prostředí.

Bezpečnostní problémy virtualizace

- **Dynamika provozu virtuálních strojů** – jednoduchost a rychlost vytvoření, spuštění ,zastavení, zrušení , klonování a migrace mezi fyzickými servery. Variabilita infrastruktury sebou nese problémové vytvoření konzistentního bezpečnostního prostředí , nekontrolovatelnou, časově nesynchronizovanou migraci bezpečnostních rizik (např. při opětovném spuštění VS).
- **Prostor pro hrozby a útoky se použitím VS podstatně zvětšuje,** zejména proto, že se pro fyzické a virtuální prostředí používá tentýž software (OS a aplikace) .
- **Zastavené (vypnuté) VS jsou napadnutelné**). Na zastavené VS není možné spustit bezpečnostní mechanismy. Je možná neoprávněná modifikace vypnutých VS a kompromitace uložených obrazů VS.
- **Vliv tradičních bezpečnostních opatření na výkon.** Spuštění bezpečnostních opatření (např. antivirového skenování) na několika VS (na jednom fyzickém serveru) může rapidně snížit výkon.
- **Zajištění integrity a kontrola aktivity aplikací a dat,** zejména pokud v cloudu sdílejí různé fyzické prostředí.
- **Obranný perimetr a segmentace sítě.** Tradiční způsoby obrany s využitím firewallů nefungují v prostředí virtuálních serverů cloudu.

Požadavky na bezpečnostní mechanizmy

- Je nutné mít spolehlivý okamžitý přehled o stavu systému bezpečnosti cloudu nezávisle na stavu a umístění cloudu.
- Bezpečnostní systém musí být schopen detekovat útok nebo hrozbu na úrovni VS nezávisle na tom, kde je fyzicky spuštěna.
- Bezpečnostní mechanizmy musí být implementovány na úrovni hypervizoru (např. aby se zamezilo útokům na zastavené VS)
- Bezpečnostní mechanizmy musí být určeny a certifikovány speciálně pro prostředí cloudu.
- Musí existovat kontrola integrity a audit aktivity dat a aplikací na různých úrovních (systémové i užívatelské)
- Obranný perimetr je nutné realizovat už na úrovni VS.
- Pro zabezpečení přístupu k systému, datům a aplikacím v mnoho uživatelském prostředí, je nutné použít silnou antentizaci (více faktorovou, jednorázová hesla, autentizaci na bázi analýzy historie, aktuálního kontextu a dalších rizik spojených s požadavkem na přístup.

Návrh IS pro zpracování UI s využitím cloudu

- Celý IS musí být řešen tak, aby ho bylo možné certifikovat pro požadovaný stupeň utajení.
- Použijeme soukromý (private) cloud, v tomto případě provozováný pouze pro organizaci a to organizací samotnou**.**
- Síťová propojení mezi lokalitami kde jsou umístěny fyzické servery jsou realizovaná jako KS s šifrováním end-to-end.
- Koncové stanice jsou řešeny jako certifikované IS s šifrovaným připojením
- Fyzická bezpečnost, Tempest apod. Jsou řešeny v souladu se zákonem č. 412/2005 Sb.
- Bezpečnostní mechanizmy jsou realizovány SW třetích stran certifikovaným pro použitý virtualizační SW.

Děkuji za pozornost !