Virtualios infrastruktūros sauga

VI komponentų sauga (hypervizorius)

IT infrastruktūros sauga

Nevirtualizuotos infrastruktūros saugos komponentai:

- Duomenų centro sauga
  - Fizinė sauga (stebėjimas: kameros, praėjimo kortelės)
  - Energijos tiekimo kontrolė
  - Vėdinimo sistemų kontrolė
- Tinklo sauga
  - Saugi tinklo architektūra (ugniasienės, VLAN, IDS/IPS, monitoringas, auditavimas)
- Serverių sauga
  - OS sauga (autentifikacija ir autorizacija, log įrašai, saugi konfigūracija (hardening), antivirusinės/antispaminės programos, ugniasienės
  - Serverių sauga (HA, prieigos prie fizinės konsolės (klaviatūra, monitorius) ribojimai, nenaudojamų programų trynimas

IT infrastruktūros sauga

Tęsinys

- Programų sauga
  - Programų integravimas į autentifikacijos sistemą (pvz. IDM)
  - Programų saugus konfigūravimas (hardening)
  - Programos kodo šifravimas
  - Dekompiliavimo ribojimų taikymas
  - Objektų, funkcijų pavadinimų keitimas
  - Savalaikis atnaujinimas
- Vartotojų sauga
  - Esmė – autentifikuoti, sekti ir kontroliuoti vartotojo veiksmus (tinkami slaptažodžiai, pirštų spaudų skeneriai, ID kortelės, RSA raktai, monitoringas, žurnalai)

Virtualios IT infrastruktūros sauga

Virtuali IT infrastruktūra – tai fizinės infrastruktūros komponentas, todėl ji paveldi visus anksčiau minėtus reikalavimus.

Papildomi saugos reikalavimai virtualiai infrastruktūrai:

- Duomenų centro sauga
  - Dedikuotas monitorius ir klaviatūra prie virtualizacijos serverio – tai vienintelis būdas prisijungti prie VM, griuvus VM.
- Virtualizacijos serverio sauga
  - Serverio saugus konfigūravimas, priegos kontrolė, monitoringas, auditavimas, tinkama autentifikacija. Papildomai paveldimi tie patys reikalavimai kaip fizinio duomenų centro.

Virtualios IT infrastruktūros sauga

Tęsinys

- Virtualaus tinklo sauga
  - Virtualaus tinko sauga siejama su fizinio tinklo sauga. Čia naudojami IDS/IPS, pažeidžiamumo (vulnerability) valdymo įrankiai
  - Virtualus tinklas apima VM‘ų tinklą, virt.serverio administravimą, VM migraciją, IP saugyklų tinklą.
- Fizinio tinklo sauga
  - Virtualizacijos serverio fizinio tinklo sąsajai taikomi minėti fizinio tinklo saugos reikalavimai įskaitant ugniasienes VLAN ir t.t.
- VM sauga
  - Tai siejama su hypervisoriaus (VMM) tinkamos konfigūracijos ir autentifikacijos reikalavimų vykdymu. Hypervizoriaus saugos problemos paveldimos ir VM lygmenyje.

Virtualios IT infrastruktūros sauga

Tęsinys

- Programų sauga
  - Iš esmės programų sauga nesiskiria nuo fizinės saugos, nes aplikacijų lygmuo nepriklauso nuo virtualizacijos lygmens. Čia atsiranda niuansai siejami su bendrų resursų naudojimu. Pvz. KPKV skenavimas vienu metu gali „nugriauti“ serverį.
  - Vieno VM programų saugos problemos įtakoja visos VI problemas.
- Vartotojų sauga
  - Tas pats kaip fizinės IT infrastruktūros atveju + hypervisoriaus vartotojų autentifikacija, stebėjimas ir kontrolė, žurnalinių įrašų agregavimas ir centralizuotas valdymas.

Serverio sauga

Fizinio virtualizacijos serverio grėsmės - operacinės sistemos lygmens KPK (rootkit). Šis KPK kraunamas serverio startavimo metu, migruoja į aparatūros valdymo dalį, sunkiai aptinkamas.

VI rootkit tipai:

- Hypervizoriaus lygmens KPK
- Aparatūrinio lygmens PKP (firmware root kit) – ypatingai sunkiai aptinkamas, nebijo perkrovimo. Aptinkamas lyginant hash kodą originalaus ir esamo serveryje firmware hash arba stebint resursų sunaudojimą buferiuose.

Virtualizacijos serverio sauga

Pavyzdys - Blue Pill (Vitriol) rootkit

- Hardware VM rootkit
- Veikia procesoriaus lygmenyje
- Migruoja į VM jų krovimosi metu
- Aptinkamas stebint buferių išnaudojimą ir firmware hash kodą.

Hypervisoriaus grėsmės (CPU)

- **Hypervizorius** – tarpinis sluoksnis tarp aparatūrinės dalies ir VM. Jis pateikia aparatūrinių komponentų atvaizdą VM.
- Hypervizorius sukuria iki 8 vCPU t.y. loginių procesorių, kas atitinka fizinius branduolius arba gijas.
- Saugumo grėsmės:
  - Visi VM priskirti vienam vCPU – generuojamas didelė apkrova vienam vCPU, krenta VM našumas
  - Migravimas (vMotion) tarp fizinių serverių nepalaikančių 32 ir 64 bit OS. Pasekmė – sugadingta VM.
  - Migravimas tarp fizinių skirtingų modelių ar gamintojų serverių gali sugadinti VM dėl HAL (hardware abstraction layer).

Hypervisoriaus grėsmės (RAM)

- Hypervizorius kontroliuoja VM prieigą prie fizinės atminties taip pat taiko įvairius būdus siekiant sumažinti atminties panaudojimą.
- Netinkamas atminties dalinimas VM‘as (administratoriaus klaida) – gali sumažinti jų našumą dėl swap atminties naudojimo.
- Atminties prieigai kontroliuoti naudojama:
  - VM lygmens „balloon“ tipo atminties tvarkyklė
  - Virtualus swap failas (*.vswp)
  - Content-based page sharing tarp VM

Atminties kontrolė

Prieš priskiriant atmintį VM, jai skirtas fizinės atminties segmentas užpildomas nuliais. Tai garantuoja duomenų apsaugą.

Atminties dalinimas galimas tik jei naudojamas VM Tools įrankis VM OS.

Hypervizorius negali pateikti VM‘ams kitų VM atminties atvaizdų.

Content based page sharing

- CBPS paskirtis – dalinti tuos pačius atminties puslapius tarp skirtingų VM.
- Naudojamas nuorodų principas.
- Atminties puslapio dydis 4KB arba 8KB.
- Praktinė nauda, kai turime keletą VM su ta pačia operacine sistema.
- Veikimas paremtas atminties puslapių hash kodų lyginimu (md5 arba sha2).
- Radus puslapius su vienodais hash kodais, atliekasmas *bit-to-bit* tikrinimas.
- Tai saugi technologija

Atminties keitimas (balloon)

Vmware tools t.y. branduolio *vmmemctl* modulis.

Veikimo principas:

- Jei VM priskirta daugiau atminties nei tam pvz. startavimo metu yra laisva, trūkstamas atminties dydis gali būti laikinai skolinamas iš kitų VM.
- Šis metodas nesukelia jokių saugumo grėsmių, nes prieš priskiriant atmintį, ji užpildoma nuliais.

Swap failas

Kiekviena mašina turi virtualų swap failą.

Swap failo dydis = alokuotos atminties dydis – VM rezervuota atmintis.

Pagal nutylėjimą swap failo dydis lygus alokuotos atminties dydžiui.

Naudojamas tik tuomet, kai vis dar trūksta atminties pritaikius ballon ir CBPS technologijas.

Swap failą galima kopijuoti norint gauti atminties dalinį atvaizdą. Tai naudojama tiriant elektroninius nusikaltimus. Root vartotojas turi pilnas teises prieiti prie šių failų, kas iššaukia saugumo grėsmę.

Hypervisoriaus tinklinė dalis

- Hypervizorius sukuria virtualų VM tinklą. Tam naudojami:
  - Virtualus komutatorius vSwitch
  - Paskirstytas virtualus komutatorius dvSwitch
  - Cisco Nexus 1000V virtualus komutatorius cSwitch (reikalingas vSphere plugin)
- Virtualūs komutatoriai – tai Layer2 lygmens tinklo įrenginiai.
- vSwitch palaiko *trunk* tipo sujungimus į fizines tinklo plokštes.

Hypervisoriaus tinklinė sauga

- vSwitch galima apsaugoti ugniasiene naudojant VMsafe įrankį (prieinamas su vSphere)
- vSwitch palaiko VLAN t.y. 802.1Q protokolą.

- vSwitch apsaugotas nuo:
  - MAC flooding, nes virtualus komutatorius saugo MAC adresus nenaudodamas apklausų, todėl nejautrus tokio tipo atakoms.
  - Dvigubos inkapsuliacijos atakų, t.y. paketų turinčių 2 VLAN įpakavimo sluoksnius. Tokio tipo paketai yra atmetami.

Hypervisoriaus tinklinė sauga

- Multicast Brute force atakos nėra leidžiamos serveryje esančių vSwitch rėmuose.
- vSwitch nepalaikti STP (spanning tree protocol), todėl STP atakos nėra aktualios.
- Random frame attack (skirtingo dydžio paketų atakos) nėra leidžiamos vSwitch rėmuose.

Saugos aspektai failų sistemose

Failų sistema apibrėžia bloko dydį (4KB, 8KB, 16KB, 32KB), kuris turi unikalų adresą.

Jei duomenų įrašas mažesnis už bloko dydį, likusi dalis lieka neužpildyta t.y. ten lieka ankstesni duomenys.

Tokios tuščios vietos gali būti talpinti informaciją, kuri gali būti pasiekiama ir nuskaitoma.

Priega prie diskų

vmkernetl palaikomi virtualių diskų konceptai:

- Virtual machine disk file (vmdk)
- Raw disk (rdm)
- Virtual machine disk delta files (delta)

VM pateikiami diskų tipai:

- Thick provisioning lazy zeroed disk
- Thick provisioning eager zeroed disk
- Thin provisioning

Hypervisoriaus API

Vmware pateikia visą eilę API:

- **Vmsafe** – prieiga prie atminties ir saugyklų skirta antivirusinėms programoms.
- **vSphere API** - prieiga prie atminties ir saugyklų, skirta trečių šalių programinės įrangos gamintojams.
- **VIX API** – VM valdymui, valdymo procesų automatizavimui
- **Gest SDK** – skaitymo teisė į VM konfigūracinius parametrus ir VM alokuotus resursus.

Saugus VI valdymas

VI valdoma per serviso konsolę, kuri paleidžiama kaip atskira VM (ESX) arba valdymo įrankis (ESXi).

VI valdymas apima:

- Visą VI infrastruktūrą
- Specifinį virtualizacijos serverį
- Virtualias mašinas

Valdymo įrankis – tai demonas, kuris atsakinėja į VMware kliento, Web access ir RCL užklausas.

Saugus VI valdymas

SSH/RCL grėsmės

- Tiesioginis prisijungimas per SSH/RCL prie ESX serverio yra potenciali grėsmė saugumui.
- ESX valdymui naudojamas VM (serviso konsolė) RedHat Enterprise Linux pagrindu. Tai leidžia instaliuoti įvairią papildomą programinę įrangą, kas sukelia saugos grėsmes.
- Net ir paprastas konsolės vartotojas gali naršyti po katalogų medį, peržiūrėti log įrašus, konfigūracinius failus.

Saugus VI valdymas

- Vartotojų valdymui patartina naudoti direktorijų paslaugą – pvz. MS Active Directory.
- Naudoti tinkamo stiprumo slaptažodžius
- Uždrausti nuotolinius prisijungimus (SSH/RCL) iš viso arba bent jau su root teisėmis.
- Uždrausti prisijungimus prie konsolės su root teisėmis.
- Naudoti nuotolinį įvykių žurnalą (remote logging)
- Atlikti savalaikį ESX serverių programų atnaujinimą.