Referatų temos

Referatų tikslas – savarankiškai susipažinti su virtualių infrastruktūrų saugos technologijomis ir sprendimais. Referatų apimtis ne mažesnė nei dešimt A4 formato lapų. Referato temos numeris pasirenkamas pagal studento numerį grupės sąraše. Pasirinkusiems modulį, kaip laisvai pasirenkamąjį, galima temą rinktis laisvai savo nuožiūra.

Atsiskaitant už referatą reikės padaryti 10 min. trukmės pristatymą bei atsakyti į klausimus. **Referatas vertinamas 2 balais.**

1. **Virtualių darbo vietų infrastruktūros sauga**
   Panagrinėti VDI komponentus, jų saugos problemas. Palyginti VMware View ir Citrix XenDesktop produktų saugą. Kaip koduoti duomenis dirbant su virtualia darbo vieta, ką daryti kai nėra fizinio TPM įrenginio?

2. **Virtualios infrastruktūros saugus veikimas**
   Pasigilinti į virtualios infrastruktūros kasdieninio administravimo veiklas, užtikrinančias IT saugą: monitoringas (įrankiai ir jų galimybės, VM konfigūracija, našumas), saugus nuotolinis prisijungimas, rezervinis kopijavimas.

3. **Rizikų valdymas migruojant infrastruktūrą į debesų kompiuteriją**
   Panagrinėti migravimo procesą iš fizinės į virtualią (ar debesų) infrastruktūrą. Su kokios galimomis rizikomis susiduriama įmonei pereinant iš fizinės infrastruktūros į virtualią infrastruktūrą (debesų kompiuteriją). Kaip valdyti rizikas?

4. **Duomenų nuosavybės problema debesų kompiuterijoje**
   Panagrinėti techninius ir teisinius aspektus taikomus debesų kompiuterijoje įvykus saugos incidentams ir atliekant kibernetinių nusikaltimų tyrimus. Kas yra duomenų savininkas „debesyse“ – tiekėjas ar paslaugos gavėjas? Kaip koduoti duomenis debesyse?

5. **Virtualių lokalių tinklų sauga**
   Panagrinėti IEEE 802.1q tinklo standartą (VLAN), apibrėžti galimas saugos grėsmes ir rizikas bei jų sprendimo/valdymo būdus.

6. **Elektroninių nusikaltimų virtualioje infrastruktūroje įkalčių surinkimas**
   Apibrėžti nusikaltimo elektroninėje erdvėje sąvoką, nustatyti nusikaltimo pėdsakus ir panagrinėti priemones ir įrankius kuriais galima surinkti elektroninius nusikaltimus virtualioje erdvėje.

7. **Veiklos tęstinumo valdymo aspektai virtualioje infrastruktūroje**
   Veiklos tęstinumo užtikrinimas ir kibernetinio saugumo prevencija fizinėje ir virtualioje IT infrastruktūroje. Panagrinėti veiklos tęstinumo užtikrinimo aspektus tokiais lygiai – fizinis, procesų ir technologinis.

8. **Virtualios infrastruktūros ir debesų kompiuterijos informacijos saugos standartų analizė**
   Atlikti egzistuojančių IT saugos standartų, metodikų analizę, nustatant jų tinkamumą virtualioms infrastruktūroms ir debesų kompiuterijai.

9. **Tinklų virtualizavimas duomenų centruose: privalumai, trūkumai, rizikos**
   Pasinagrinėti programinį tinklų virtualizavimą (Software Defined Network), struktūrą, privalumus, trūkumus, saugos grėsmes.

10. **Virtualių mašinų migravimo saugumo aspektai**
    Išnagrinėti galimas rizikas (pvz. Man in the Middle ir kitas) atliekant VM migravimą realiu laiku (Live Migration, vMotion)

11. **Žurnalinių įrašų surinkimas, agregavimas ir analizė virtualioje infrastruktūroje**
    Išnagrinėti virtualių mašinų ir serverių žurnalinių įrašų (log'ų) surinkimo, agregavimo ir orkestravimo (orchestration) ypatybes, palyginti jas su fizinės infrastruktūros analogiškais procesais.

12. **Debesų kompiuterijos saugos aspektai**
    Panagrinėti debesų kompiuterijos principus, architektūrą, panagrinėti viešų debesų (public cloud) saugos grėsmes, susijusias su tapatybės valdymu, privatumu, programų sauga, debesų kompiuterijos saugai. Panagrinėti, kaip resursų dinamiškumas ir plečiamumas įtakoja saugumą.

13. **IT sauga kaip paslauga debesų kompiuterijoje**
    Atlikti literatūros, susijusios su debesų kompiuterijos saugos grėsmėmis ir pažeidžiamumais apžvalgą, sudaryti IT saugos grėsmių taksonomiją debesų kompiuterijoje. Panagrinėti Security as a Service paslaugą ir jos panaudojimo galimybes.

14. **Tapatybės ir prieigos valdymas debesų kompiuterijoje**
    Panagrinėti vartotojų autentifikacijos ir autorizacijos principus naudojamus debesų kompiuterijoje. Kaip realizuojama autentifikacija (*cross-platform*) tarp skirtingų debesų paslaugų tiekėjų, kaip valdoma prieiga, su kokiomis saugos rizikomis susiduriamas ir kaip jos valdomos.

15. **Atstatymas po gedimų ir verslo tęstinumo užtikrinimas virtualioje infrastruktūroje**
    Panagrinėti *Disaster Recovery and Business Continuity* klausimus virtualioje infrastruktūroje ir debesyse. Kuo šie procesai skiriasi nuo analogiškų procesų fizinėje infrastruktūroje?

16. **OpenStack debesų kompiuterijos platforma ir jos saugos aspektai**
    Detaliai panagrinėti OpenStack platformą – architektūrą, komponentus, instaliavimo ir konfigūravimo aspketus, valdymą, plečiamumą, lankstumą. Atskiras skyrius turi būti skirtas OpenStack saugai t.y. grėsmės, pažeidžiamumai, galimos saugos rizikos.

17. **Linux konteineriai ir jų saugos aspektai**
    Detaliai panagrinėti Linux konteinerių platformas, jų architektūrą, komponentus, instaliavimo ir konfigūravimo aspketus, privalumus, trūkumus, valdymo aspektus. Atskiras skyrius turi būti skirtas kanteinerių saugai t.y. grėsmės, pažeidžiamumai, galimos saugos rizikos.

18. **Docker platforma ir jos saugos aspektai**
    Detaliai panagrinėti Docker platformą – architektūrą, komponentus, instaliavimo ir konfigūravimo aspketus, valdymą, plečiamumą, lankstumą. Atskiras skyrius turi būti skirtas Docker saugai t.y. grėsmės, pažeidžiamumai, galimos saugos rizikos.

19. **Hypersusieta IT ir jos saugos aspektai**
    Hypersusieta infrastruktūra (Hyperconverged infrastructure-HCI) – tai infrastruktūra, skirta minimizuoti sistemų suderinamumo ir valdymo klausimus. Tai naujas principas pateikti infrastriktūrines paslaugas: serverius, saugyklas, tinklą ir t.t. Išanalizuoti tokios infrastruktūros privalumus ir trūkumus, saugos grėsmes ir rizikas.

20. **Žurnalinių įrašų surinkimas, agregavimas ir analizė virtualioje infrastruktūroje**
    Išnagrinėti virtualių mašinų ir serverių žurnalinių įrašų (log‘ų) surinkimo, agregavimo ir orkestravimo (orchestration) ypatybes, palyginti jas su fizinės infrastruktūros analogiškais procesais.

21. **Debesų kompiuterijos saugos aspektai**
    Panagrinėti debesų kompiuterijos principus, architektūrą, panagrinėti viešo debesies (public cloud) saugos grėsmes, susijusias su tapatybės valdymu, privatumu, programų sauga, debesų kompiuterijos saugai. Panagrinėti, kaip resursų dinamiškumas ir plečiamumas įtakoja saugumą.

22. **IT sauga kaip paslauga debesų kompiuterijoje**
    Atlikti literatūros, susijusios su debesų kompiuterijos saugos grėsmėmis ir pažeidžiamumais apžvalgą, sudaryti IT saugos grėsmių taksonomiją debesų kompiuterijoje. Panagrinėti Security as a Service paslaugą ir jos panaudojimo galimybes.

23. **Linux konteineriai ir jų saugos aspektai**
    Detaliai panagrinėti Linux konteinerių platformas, jų architektūrą, komponentus, instaliavimo ir konfigūravimo aspketus, privalumus, trūkumus, valdymo aspektus. Atskiras skyrius turi būti skirtas kanteinerių saugai t.y. grėsmės, pažeidžiamumai, galimos saugos rizikos.

24. **Docker platforma ir jos saugos aspektai**
    Detaliai panagrinėti Docker platformą – architektūrą, komponentus, instaliavimo ir konfigūravimo aspketus, valdymą, plečiamumą, lankstumą. Atskiras skyrius turi būti skirtas Docker saugai t.y. grėsmės, pažeidžiamumai, galimos saugos rizikos.

25. **Tinklų virtualizavimas duomenų centruose: privalumai, trūkumai, rizikos**
    Pasinagrinėti programinį tinklų virtualizavimą (Software Defined Network), struktūrą, privalumus, trūkumus, saugos grėsmes.