უსაფრთხოების ტექნოლოგიები Windows Server 2016 ოპერაციულ სისტემაში

ნატალია გაბაშვილი, თამარ გაბაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ინფორმაციული უსაფრთხოებისა და საიმედოობის საკითხები, რაც ჩვენი დროის ყველაზე მნიშვნელოვანი პრიორიტეტია ინფორმაციულ ტექნოლოგიებში. წარმოდგენილია ინფორმაციის დაცვის პრობლემატიკა არაავტორიზირებული წვდომის, დაზიანებისა და განადგურების თვალსაზრისით. შემოთავაზებულია Windows Server 2016 ოპერაციული სისტემის ახალი და სრულყოფილი ფუნქციებისა და პროგრამული კომპონენტების ერთობლიობა, რომელიც მომხმარებელს სთავაზობს მონაცემთა უსაფრთხოების უზრუნველყოფისთვის მაღალ დონეს.

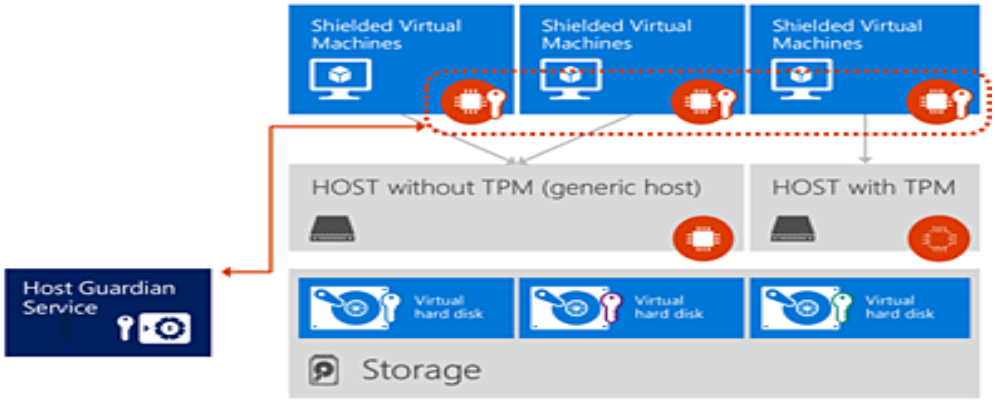
საკვანძო სიტყვები: ინფორმაცია. უსაფრთხოება. ოპერაციული სისტემა. Windows Server 2016 ტექნოლოგია. ვირტუალური მანქანა.

1. შესავალი

თანამედროვე ოპერაციული სისტემების უმნიშვნელოვანესი ფუნქციაა მონაცემთა დაცვის, უსაფრთხოების და საიმედოობის უზრუნველყოფა. უნდა აღვნიშნოთ, რომ კომპიუტერი და ოპერაციული სისტემა მუშაობს ქსელურ გარემოცვაში, რომელზეც გამუდმებითაა შესაძლებელი და ფაქტობრივად, ხდება კიდეც ჰაკერების და მათი პროგრამების თავდასხმა, რომელთა მიზანია კომპიუტერის მუშაობის დარღვევა, მასში შენახული მომხმარებლის კონფედენციალური მონაცემების დაზიანება, სისტემაში შესასვლელი სახელების და პაროლების მოპარვა და ა.შ. Windows Server 2016 უსაფრთხოების უზრუნველსაყოფად გვთავაზობს მრავალ ახალ და გაუმჯობესებულ ფუნქციას და კომპონენტს [1].

2. ძირითადი ნაწილი

ერთერთი უახლესი კომპონენტია Host Guardian Service, რომელიც იცავს ვირტუალურ მანქანებს Shielded Virtual Machines და მათში არსებულ მონაცემებს არასანქცირებული წვდომისაგან (ნახ.1). ვირტუალური მანქანების უფრო მეტი უსაფრთხოების უზრუნველყოფისათვის Windows Server 2016-ში გათვალისწინებულია Shielded Virtual Machines ტექნოლოგია, რომელიც საშუალებას იძლევა ღრუბლოვან ინფრასტრუქტურაში შეიქმნას დაცული ვირტუალური გარემო [2]. ასეთი სისტემების საკვანძო თავისებურებაა ის, რომ მათში შეღწევის მოპოვება შეუძლია მხოლოდ მათ მფლობელს. ადმინისტრატორს ჩამორთმეული აქვს ასეთი უფლებამოსილება, მას მხოლოდ შეუძლია ასეთი ვირტუალური მანქანების ჩართვა და გამორთვა. ამასთან, მას არ აქვს უფლება ჩაერიოს მათ მუშაობაში, არც წაიკითხოს მონაცემები. Microsoft-ში აღნიშნავენ, რომ Shielded Virtual Machines მექანიზმი შესაძლოა ფართოდ იქნეს მოთხოვნილი ჰოსტინგური პროვაიდერების მიერ, რომლებიც სთავაზობენ ვირტუალური მანქანების არენდის მომსახურეობას ღრუბელში.

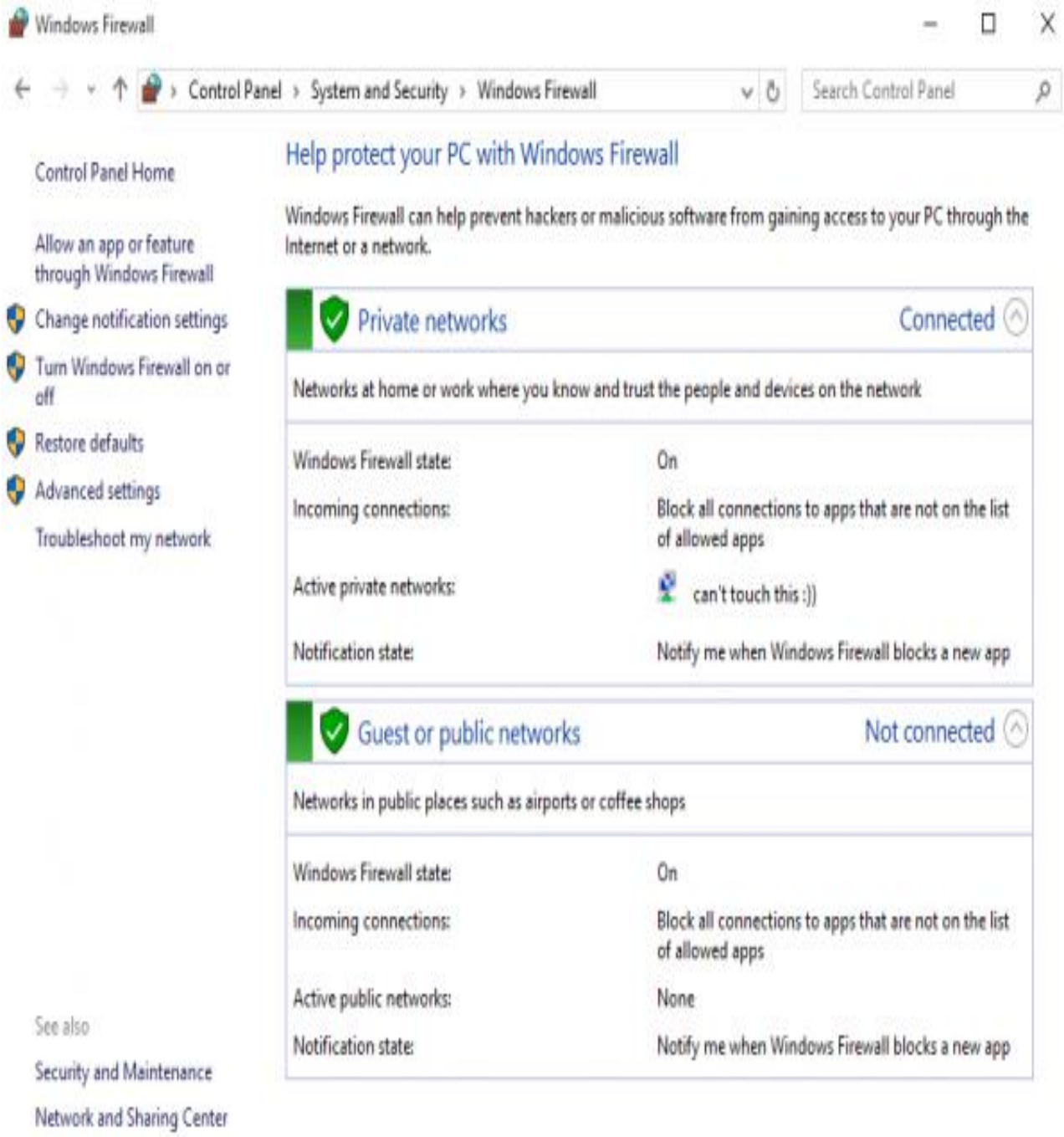


ნახ.1. Host Guardian Service-ს მუშაობის პრონციპი

Shielded Virtual Machines ტექნოლოგია საშუალებას იძლევა ღრუბლოვან ინფრასტრუქტურაში შეიქმნას დაცული ვირტუალური მანქანები, შეღწევა რომელშიც შეუძლია მხოლოდ მათ მფლობელს. ადმინისტრატორს აქვს მხოლოდ ასეთი ვირტუალური მანქანების ჩართვის და გამორთვის უფლება. მას არ აქვს უფლება ჩაერიოს მათ მუშაობაში, წაიკითხოს მონაცემები, ხელთ იგდოს ტრაფიკი, შეცვალოს მათი კონფიგურაცია.

შემდეგი კომპონენტია Device Guard – რომელიც ბლოკავს ყველა იმ დრაივერს, რომელიც არ არის მოცემული უსაფრთხო დრივერების სიაში. ხოლო Creditional Guard ტექნოლოგია საშუალებას იძლევა მხოლოდ პრივილეგირებულ სისტემებს ჰქონდეს წვდომა კონფიდენციალურ მონაცემებთან. ოპერაციული სისტების ინსტალაციისას ჩუმათობით ინსტალირდება Windows Firewall – დამცავი ზღუდე, ესაა პროგრამული ან აპარატურული დაცვა მავნე პროგრამებისაგან; მისი ძირითადი დავალებაა პაკეტების ფილტრაცია. ის ამოწმებს ყველა პაკეტის თავსართს, რომლებიც გადაიცემა კომპიუტერის ქსელურ ინტერფეისებზე და ამ პაკეტებზე ასრულებს იმ მოქმედებებს, რომლებიც შეესაბამება Firewall-ში მომართულ წესებს (ნახ.2). იგი შეიძლება გამოყენებულ იქნას როგორც ერთი კომპიუტერის დასაცავად (მაგალითად, ინტერნეტში ჩართული პერსონალური კომპიუტერი), ასევე მთლიანი ქსელის დასაცავად.[3]

Windows Server 2016-ში ასევე გაჩნდა ახალი საშუალება Just Enough Administration (JEA) სახელწოდებით. ის ნიშნავს, რომ ადმინისტრატორებს შეუძლიათ შექმნან დროებითი სააღრიცხვო ჩანაწერები, შეზღუდული გარკვეული ფუნქციებით. ანუ, ადმინისტრატორი შედის რა სისტემაში, რომელიც დავირუსებულია პერსონალური კომპიუტერის ვირუსით, დიდ ზიანს არ მიაყენებს მას. Windows Credential Guard ასევე ზღუდავს ზიანის მომტანი პროგრამების შესაძლო ზიანს ასეთი სცენარის დროს. ხოლო ადმინისტრირების დროებითი უფლებები (Just in time administration) მიეწოდება Microsoft Privileged Access Manager პროვაიდერების მეშვეობით, რომლებიც მიაწოდებენ ვირტუალური სერვერების არენდის მომსახურეობებს. მსხვილი ინფრასტრუქტურების IT პერსონალი არც თუ იშვიათად აწყდება IP მისამართების კონტროლის და განაწილების პრობლემას, განსაკუთრებით ფიზიკური გარემოს ხშირი გადატანისას ვირტუალურში და პირიქით. აცნობიერებს რა ამ პრობლემის მნიშვნელობას, კომპანია Mivrosoft Windows Server 2016 ის შემადგენლობაში ჩართო IP მისამართების მართვის საშუალება IP Address Management (IPAM), რომელიც საშუალებას იძლევა გაამარტივოს ორგანიზაციის IP სივრცის მართვა და ქსელში წარმოშობილი მოწყობილობების კონფლიქტები მინიმუმამდე დაიყვანოს.



ნახ.2. Windows Firewall-ის ფანჯარა

Windows Sever 2016-ში განვითარება ჰპოვეს უსაფრთხოების უზრუნველყოფის სისტემებმა. კერძოდ, გამოჩნდა ეგრეთ წოდებული Virtual Security Module (VSM). იგი Hyper-V ცალკე კონტეინერია, რომელშიც განთავსებულია ყველაზე ფასეული სისტემური მონაცემები. კიდევ ერთი სიახლეა – Trusted Platform Module (Virtual TPM), რომელიც საშუალებას იძლევა გამოყენებული იქნას დაშიფვრის საშუალებები ვირტუალურ მანქანებში.

3. დასკვნა

Windows Server- ის არსებულ გამოცემებს შორის Server 2016 ყველაზე დაცული, უსაფრთხო და საიმედო ოპერაციული სისტემაა. მის საიმედოობას უზრუნველყოფს პლატფორმა, რომელშიც ჩაშენებულია ახალი და გაუმჯობესებული ფუნქციები, აგრეთვე ინტეგრირებული გარემო, რომელიც უზრუნველყოფს ვირტუალური მანქანების, პროგრამების და მონაცემების დაცვას.

ლიტერატურა - References – Литература:

1. Что такое облачные хранилища и для чего они нужны. http://travelfotosol.ru/obuchenie-/4773-chto_takoe_oblachnyie_hranilischa_i_dlya_chego_oni_nujnyi

2. ღრუბლოვანი საცავები. https://www.slideshare.net/dtedei/ss-42967629

3. 20 лучших облачных хранилищ данных. http://www.internet-technologies.ru/articles/20-luchshih-oblachnyh-hranilisch-dannyh.html

SECURITY TECHNOLOGIES IN OPERATING SYSTEM WINDOWS SERVER 2016

Gabashvili Natalia, Gabashvili Tamar
Georgian Technical University

Summary

The information security and reliability issues are discussed, which is the most important priority of our time in information technology. The information protection problem is presented in terms of unauthorized access, damage and destruction. The combination of new and comprehensive functions and software components offered by the Windows Server 2016 operating system, which offers customers a high level of data security.

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS SERVER 2016

Габашвили Н., Габашвили Т.
Грузинский Технический Университет

Резюме

Рассматриваются вопросы информационной безопасности и надежности, что является одним из важнейших приоритетов нашего времени в области информационных технологий. Представлена проблематика защиты информации от несанкционированного доступа, ущерба и повреждения. Предлагается набор новых и улучшенных функций и компонентов операционной системы Windows Server 2016, который предлагает пользователю высокий уровень обеспечения безопасности данных.