



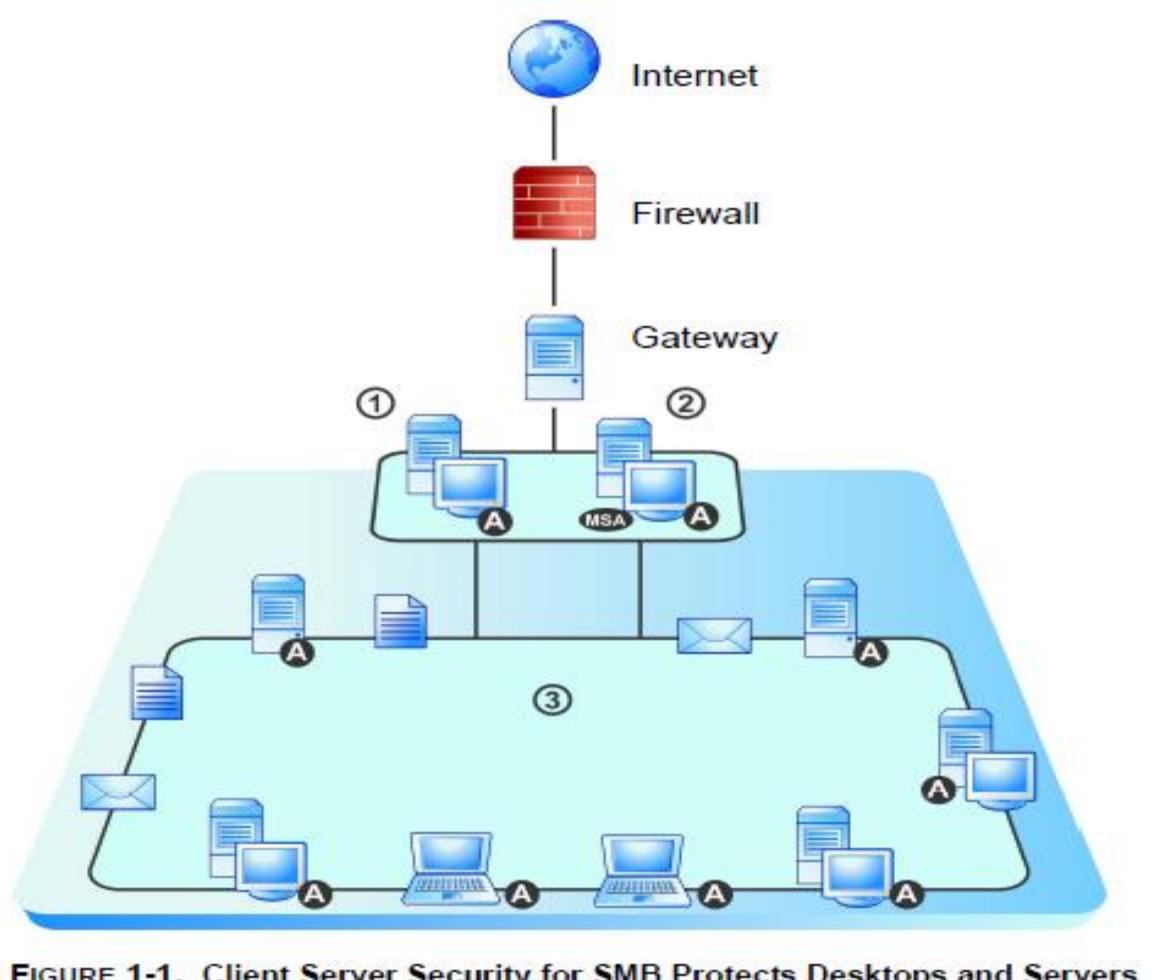
Institucioni i Arsimit
UNIVERSITAR AAB

FAKULTETI I SHKENCAVE KOMPJUTERIKE

SISTEMI KLIENT – SERVER

- ❑ Aplikacioni “**Client Server Security for Small and Medium Business**” ofron pasqyren e rrjetit dhe mbrojtjen e serverit
- ❑ Integrimi i **CSS** ne Microsoft Windows e ben ate me te dobishem dhe krijon nje game me te gjeret te mbrojtjes se serverit nga viruset.
- ❑ Synimi i aplikacionit **CSS** eshte qe te mbroje laptopat, kompjuteret, paisjet tjera dhe serveret ne rrjete.

SISTEMI KLIENT – SERVER



1. The Security Server

**2. Microsoft Exchange Server
(not protected by Client Server Security)**

3. Local network

A. Client/Server

KOMPONENTET KRYESOR (ANTI-VIRUS) NE CSS

- **Modeli i viruseve** – konsiston ne skedar (file) i cili ndihmon ne identifikimin e llojit te viruseve, permabn model unik te biteve dhe byteve qe sinjalizon prezencen e nje virusi
- **Makina kontrolluese** – perdor skedarin e modelit te viruseve per te detektuar viruset dhe rreziqe tjera te sigurise qe klientet e sistemit jane duke u lidhur.
- **Modeli i pastrimit te viruseve** – kjo ndihmon ne identifikimin e skedareve Trojan dhe ky model automatikisht i eliminon ato.
- **Makina e pastrimit te viruseve** – sherbimi i pastrimit konsiston ne kontrollin e skedareve dhe proceseve trojan ne sistem

KOMPONENTET KRYESOR (ANTI-SPY) NE CSS

- ❑ **Modeli spy** – konsiston per te detektuar pergjimet ne sistemin klient-server.
- ❑ **Modeli monitorues** i pergjimeve aktive – eshte e njeje me modelin paraprak, por ky model perdoret nga makina kontrolluese per skanimin e pergjimeve ne kohe reale.
- ❑ **Makina kontrolluese e pergjimeve** – Konsiston ne kontrollimin, detektimin dhe heqjen e pergjimeve nga klientet e infektuar ne sisteme operative te ndryshme.

FUNKSIONI I CSS NE MBROJTJEN E KOMPJUTERIT DHE RRJETIT TONE

- Siguria klient-server eshte sistem qe prefshin aplacione multi-dimensionale
- Siguria e serverit shkarkon komponente dhe “policy” ne menyre qe te jete “up-date” mbi mbrojtjen e sistemit nga viruset.
- Agjendet e sigurise ne sistemin klien/server – perdonin kontrollimin e viruseve dhe firewall-at personal per te mbrojtur sistemet tona nga viruset
- .

INSTALIMI I SIGURISE KLIENT/SERVER

Trend Micro Client Server Security for SMB

Setup Type

Choose the setup type that best suits your needs.



Click the type of setup you prefer.

Typical Installation (recommended)

Typical installation is very similar to Custom installation, but uses Trend Micro default values to configure the Web server and does not install a proxy server.

Custom Installation

Use the Custom installation when you need to configure your Web server or you require a proxy server. Custom installation allows you to set the installation path and port number for the Client/Server Security Agent.

InstallShield

< Back Next > Cancel

INSTALIMI I SIGURISE KLIENT/SERVER



- Rekomandohet Domain name – verifikon emrin e serverit

- IP Adress – verifikon qe IP e serverit jane ne rregull

INSTALIMI I SIGURISE KLIENT/SERVER



- SMTP sever – shembull smtp.aab.com
- Port – zakonisht eshte 25 per komunikim
- Recipients – e-mail adresa e te gjithe klienteve per te pranuar mesazhe dhe raporte nga serveri i sigurimit

INSTALIMI I SIGURISE KLIENT/SERVER

The image shows two overlapping windows from the Trend Micro Client/Server Security for SMB setup process.

Left Window: Administrator Account Password

- Title:** Trend Micro Client Server Security for SMB
- Section:** Administrator Account Password
- Description:** Type a password and confirm that password in the field provided.
- Fields:** Password (text input), Confirm Password (text input).
- Note:** Protect the Security Server Web console and clients with password users from modifying your settings or removing your clients.
- Buttons:** < Back, Next >

Right Window: Select Components

- Title:** Trend Micro Client/Server Security for SMB
- Section:** Select Components
- Description:** Select the components to install on your computer.
- List:** Client/Server Security Agent (checkbox checked)
- Buttons:** Select All, Clear All, < Back, Next >, Cancel

PANELI I APARATURAVE NE SIGURINE Klient/Server

➤ Please type your password to access the product console.

● Password:

● **Install Client/Server Security Agent**

[Click here](#) to start installing the Client/Server Security Agent

Installing the client usually takes only a few minutes.

Icons on the Security Dashboard

Click the Help icon to open the online help.

Click the Refresh icon to refresh the view of current screen.

Click the Hidden text icon to display hidden text.

Click the Quick Tour icon to view a tutorial about current screen features.

Click the Information icon to display information pertaining to a specific item.

KONFIGURIMI I LAJMERIMEVE

Antivirus

viruset detektohen ne desktop/server zakonisht 5 here
ne 1 ore

Anti-spyware

Spyware/Grayware kontrollohen ne desktop/server
15 here ne 1

Network Virus

viruset e rrjetit kontrollohen 10 here ne 1 ore

PANELI I APARATURAVE NE SIGURINE Klient/Server

TREND MICRO Security Dashboard for SMB

Live Status Security Settings + Outbreak Defense + Scans + Updates + Reports + Preferences + Help

Live Status

Last updated: 2006/10/23 15:17:12 Refresh

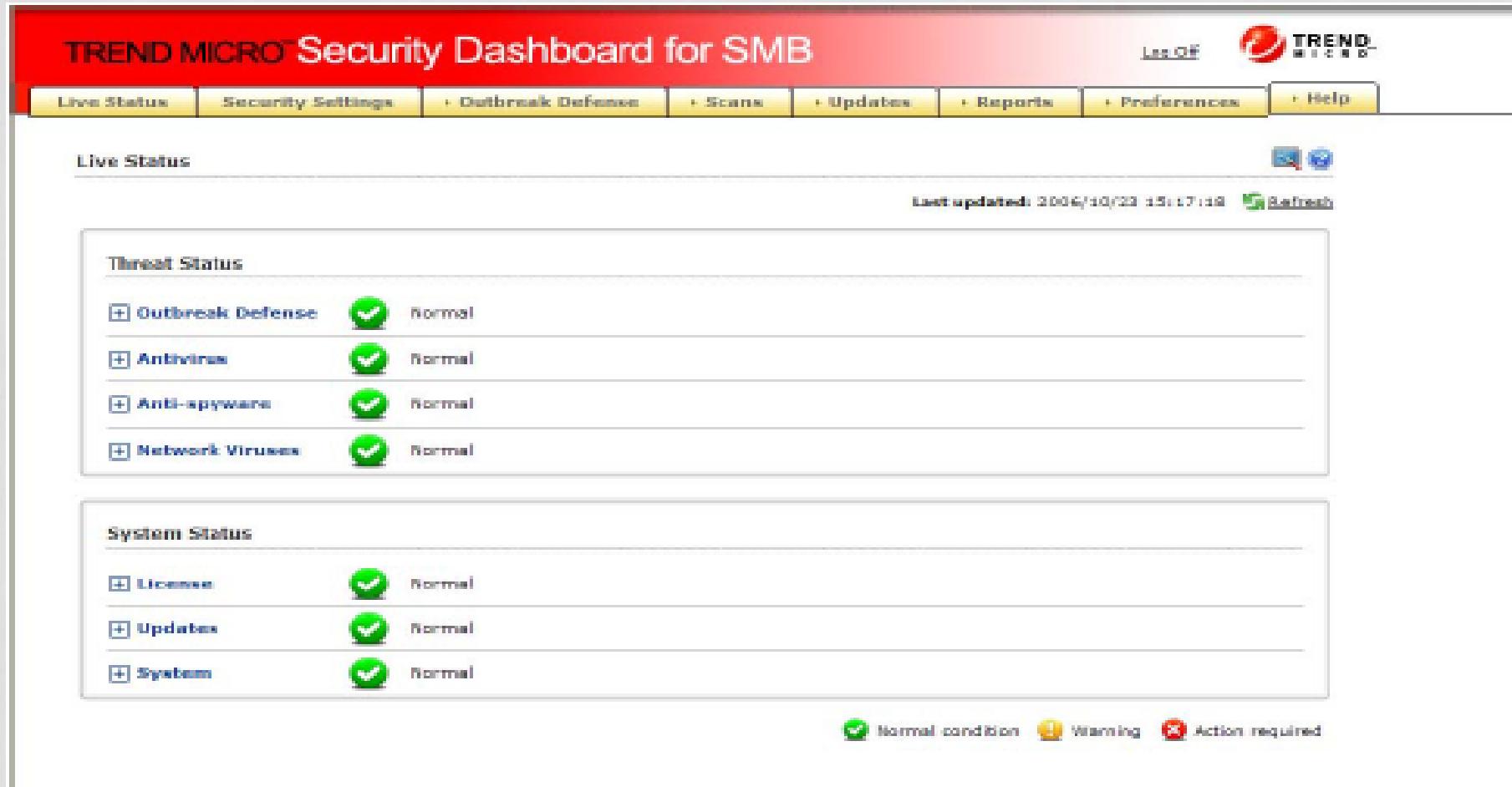
Threat Status

+ Outbreak Defense	Normal
+ Antivirus	Normal
+ Anti-spyware	Normal
+ Network Viruses	Normal

System Status

+ Licenses	Normal
+ Updates	Normal
+ System	Normal

Normal condition Warning Action required



3 FAZAT E MBROJTJES

TREND MICRO[®] Security Dashboard for SMB

[Log Off](#) 

[Live Status](#) [Security Settings](#) **Outbreak Defense** [Scans](#) [Updates](#) [Reports](#) [Preferences](#) [Help](#)

[Outbreak Defense > Current Status](#) 

Threat Prevention → **Threat Protection** → **Threat Cleanup**

Trend Micro Security Server will automatically deploy a response to a world wide virus outbreak. You will find the details of the threat and the actions that you must take below. Any action that the system cannot take automatically will be shown to you in the Vulnerable Computer(s) and Computer(s) Cleanup sections below.

Last updated: 2006/10/25 17:06:42 

Prevention

Threat Information					
Threat	Alert Type	Risk Level	Delivery Method	Vulnerability Exploited	Automatic Response
N/A					<input type="button" value="Disable"/>
Date/Time Initiated	Date/Time End			Automatic Response Details	
N/A	N/A			N/A	

Alert Status of your network:

Alert Status for Online Computers		
Computer Type	Enabled	Not Enabled
Desktop/Servers	N/A	N/A
Exchange servers	N/A	N/A

INFORMATA KYESORE MBI PARANDALIMIN E THREAT

Risk level – niveli i rrezikut dhe ekspozimi i viruseve

Alert status for online computers – shfaq numrin e pote te klienteve qe kane dhe nuk e kane “enable” alrmin automatik.

Vulnerable computers – shfaq emrat e kompjutereve ne rrjetin tone qe jane te ceneshem nga threadet te ndryshme

INFORMATA MBI MBROJTJEN NGA THREAT

The screenshot shows the Trend Micro Security Dashboard for SMB. At the top, there's a navigation bar with tabs like 'Live Status', 'Security Settings', 'Outbreak Defense' (which is selected), 'Scans', 'Updates', 'Reports', 'Preferences', and 'Help'. Below the navigation bar, a red banner displays the title 'TREND MICRO Security Dashboard for SMB'. The main content area has three large boxes labeled 'Threat Prevention', 'Threat Protection', and 'Threat Cleanup' connected by arrows. A sub-header 'Outbreak Defense > Current Status' is above this. Below the boxes, a message states: 'Trend Micro Security Server will automatically deploy a response to a world wide virus outbreak. You will find the details of the threat and the actions that you must take below. Any action that the system cannot take automatically will be shown to you in the Vulnerable Computer(s) and Computer(s) Cleanup sections below.' To the right of this message is a timestamp 'Last updated: 2006/10/25 15:44:15' and a 'Refresh' button. Below the message, there are two status indicators: 'Prevention' (with a plus sign icon) and 'Red Alert Enabled' (with a red alert icon). Under 'Protection for TEST_HALWARE.A', there are two tables: 'Solution Download Status' and 'Solution Deployment Status'. The 'Solution Download Status' table shows the following data:

Component	Version	Status
virus cleanup template	399	Not downloaded yet
virus cleanup engine 32-bit	3.980.000	Downloaded
virus pattern	3.297.00	Downloaded

The 'Solution Deployment Status' table shows the following data:

Computer Type	Up-to-date	Out-of-date
Desktop/Server	2	2
Exchange server	1	0

❑ **Solution download status** – shfaq listen me komponente qe kane nevoje per “up-date”

INFORMATA MBI PASTRIMIN NGA THREAT

TREND MICRO Security Dashboard for SMB

Live Status Security Settings **Outbreak Defense** Scans Updates Reports Preferences Help

Outbreak Defense > Current Status

Threat Prevention → **Threat Protection** → **Threat Cleanup**

Trend Micro Security Server will automatically deploy a response to a world wide virus outbreak. You will find the details of the threat and the actions that you must take below. Any action that the system cannot take automatically will be shown to you in the Vulnerable Computer(s) and Computer(s) Cleanup sections below.

Last updated: 2006/10/29 15:35:31 [Refresh](#)

Prevention  Red Alert Enabled

Protection for TEST_MALWARE.A

Cleanup for TEST_MALWARE.A

Security Server has scanned your network with the latest threat solution. See a list of computers that are scanned below.

Computer Scanning Status for TEST_MALWARE.A		
Computer Type	Scanned	Not Scanned
Desktop/Server	0	2
Exchange server	0	1

Security Server has scanned your network with the latest threat solution. See a list of computers that are scanned below.

Computer Cleanup Status for TEST_MALWARE.A					
Attempts/Total:	4/7				
<input checked="" type="checkbox"/> Export	Total: 1 Record(s) In: 1 Page: 1 of 1 x 10				
Computer	Date/Time	IP Address	Computer Group	Threat Name	Cleanup Result
C-B-S	2006/10/29 16:45:14	10.0.0.108	Servers (default)	TEST_MALWARE.A	Cleaned successfully

KOMPJUTERET E CENUESHEM

Click “**scan for vulnerabilities now**” – siguria klient/server egzekuton procesed mbi cenushmerine e sistemit:

a) identifikon cenushmerite

b) shfaq cenushmerite

c) raporton cenushmerite

PASTRIMI I KOMPJUTEREVE

- ❑ Pastrimi i sistemit nga viruset/trojanet ndodh ne prapavijen e aplikacionit.
- ❑ Pastrimi i sistemit konsiston ne keto detyra:
 - Detekton dhe largon viruset
 - “mbyt”proceset qe viruset i kane krijuar
 - Riparon skedaret e sistemit qe viruset kane infektuar
 - Fshijne skedaret dhe apliakcionet qe viruset kane infektuar
- ❑ Per te gjitha keto detyra “pastrimi” krijohet nga keta komponente:
 - Makina e pastrimit te viruseve
 - Modeli i pastrimit te viruseve

SHFAQJA E GRUPEVE NE RRJETIN TONE DHE VEGLAT E SIGURISE

The screenshot shows a software interface for managing network groups. At the top, there is a toolbar with several icons and labels: 'Configure' (highlighted in blue), 'Replicate Settings', 'Add Group', 'Add', 'Remove', 'Move', and 'Reset Virus Counter'. Below the toolbar, on the left, is a tree view under 'My Company' with three items: 'Servers (default)', 'Desktops (default)', and 'TWEXMAIL04'. On the right, there is a list of members, each represented by a small blue square icon and a name: TW-ARIELKA001, TW-CAUCHY, TW-CEDRICCHEN01, TWCSM01, TW-DENISECHEN, TW-ELLENCHEN1, TW-HUBERXIONG, TW-JERRYWU, TW-JHCHANG1, TW-KEVINYU, TW-MESHWU, TW-MORGANCHEN2, and TW-SIMONLIN2.

VEGLAT E SIGURISE

Tool	Description
Configure	Configure desktop and server settings at a group level for such settings as scanning, personal firewall, desktop privileges, and quarantine directory.
Replicate Settings	Use this tool to replicate configuration settings from one group of Client computers to one or more other groups of Client computers.
Add Group	Use this tool to create a new group of Client computers.
Add	Use Add to install Client/Server Security Agents to Client computers. After adding a new Client computer, drag and drop the icon for that computer to a group of your choice.
Remove	Use this tool to either remove a Client computer or group icon from the Security Dashboard or uninstall the Client/Server Security Agent from the selected Client computer.
Move	Use this tool to move a Client computer from one Security Server to another Security Server.

SUBJEKTET THEMELORE TE APLIKACIONIT SMB

Malware – eshte nje aplikacion qe egzekuton veprime te pa-autorizuara ne sistem. C/S SMB mund te detektoje malware-t ne kohe reale

Viruset – eshte nje aplikacion (pjese e egzekutueshme e kodit) qe ka aftersi unike per iteracion.

SUBJEKTET THEMELORE TE APLIKACIONIT SMB

Viruset e rrjetit – konsistojne kryesosht ne infektimin e protokolleve si TCP, FTP, UDP, HTTP etj etj. Nje firewall personal mund ti identifikoje dhe ti blokoje keta virusa.

Trojans – eshte nje aplikacion me nje qellim te keq. Me dallim nga viruset, trojanet nuk itercionojne proceset, por i jasin kahje destruktive.

Bots – jane skedar egzekutiv qe jane te dizejnuar qe te bjejne dem ne sistemin e kompjuterave dhe ne rrjet. Bots separi egzekutohen, mund te perseriten dhe krijojne nje kopje te tyre ne cdo sistem

KONFIGURIMET E REKOMANDUARA NE ANTIVIRUSIN NE KOHE REALE

- “enable” – skanimin ne kohe reale dhe skano te gjitha skedaret qe hyjne dhe dalin permes klientave
- Skanimi i skedareve – perdor shpejtesi optimale mbi skanimin e skedareve te sistemit
- Aksioni i thredave te infektuar – “clean all” ose “delete all” per skedaret te cilat nuk mund te pastrohen
- Advanced scanning options – Kontrollon te gjitha skedaret per infektime ne nje shkalle me te thelle

PERFUNDIME MBI MBROJTJEN E KOPJUTERIT DHE RRJETIT NE SISTEMIN KLIENT/SERVER

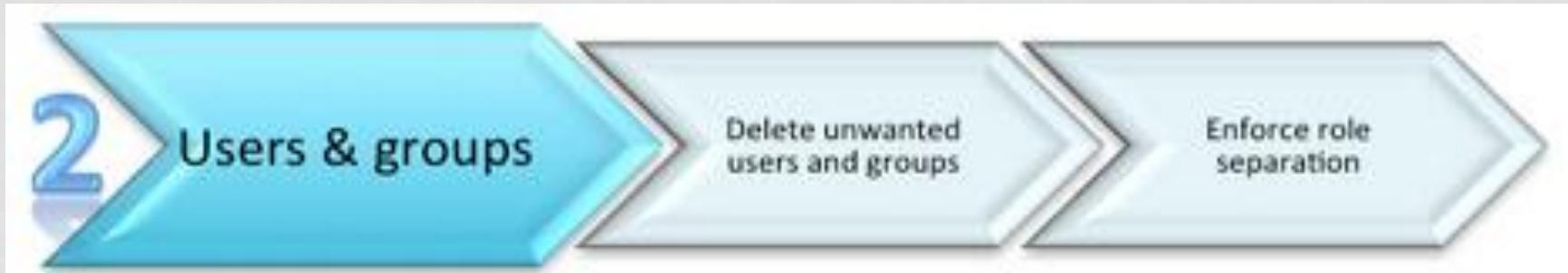
- ❑ Perdor konfigurimet e rekomanduara te Sigurise Client server
- ❑ Mbaje sistemin operative “up-date”
- ❑ Perdor fjalekalim te gjate dhe keshilloj perdoruesit klient te perdonin gjithashtu fjalekalim te gjate
- ❑ Myallo te gjitha aplikacionet dhe sherbimet e panevojshme, ne menyre qe te reduktojme shancet per infektim me viruse
- ❑ Konfiguro shfletuesin ne nje niel te larte sigurie

PRAKTIKAT ME OPTIMALE PER NJE SIGURI TE QENDRUSHEM NE SERVER



1. Preferohet fjalekalim MIX
2. Frekuenca e fjalekalimit varet nga perdorimi i tij
3. Rekomandohet te perdoret autentikimi me celes publik
4. Preferohet te aplikohet ndonje nivel me i larte sigurie shtese mbi autentifikimin
5. Mund ta perdorim password manager per ruajtjen e fjalekalimit, ose i ruajme ne diqe lokale te koduara me TrueCrypt ose FileVault (MAC) etj

PRAKTIKAT ME OPTIMALE PER NJE SIGURI TE QENDRUSHEM NE SERVER



1. Kontrollojme listen e perdoruesve dhe grupeve ne server dhe fshijme ate i cili nje kohe te gjate nuk eshte ne perdorim
2. Nese serveri jone menaxhohet nga nje grup njerezish (IT, web-development), roli i ndarjes se pergjegjive do te ishte e preferushme.

PRAKTIKAT ME OPTIMALE PER NJE SIGURI TE QENDRUSHEM NE SERVER



1. Konsiston per ta shmang ndonje rrezik sigurie te panevojshem
2. Disa procese duhet te aksesohen vetem nga disa IP-adresa te reja.
3. Aplikojme praktikat me te mira mbi proceset e serverit (cPanel, SQL etj)

PRAKTIKAT ME OPTIMALE PER NJE SIGURI TE QENDRUSHEM NE SERVER



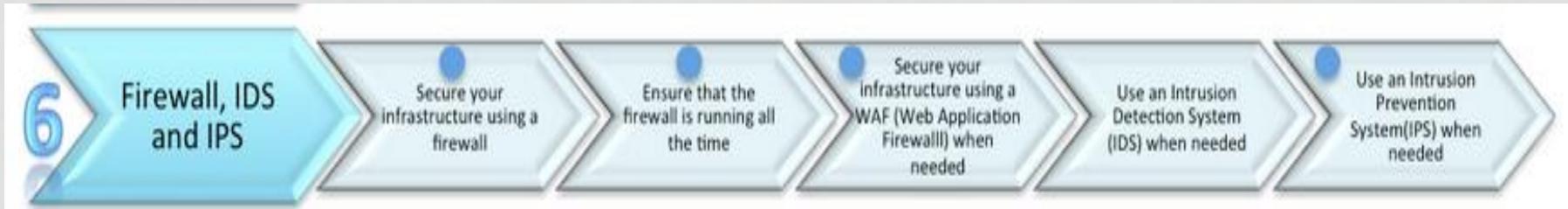
1. Rekomandohet ti vemi autorizime te gjitha folderave, skedareve dhe pjeseve te sistemit
2. Per te mbrojtur te dhenat dhe integriteti e tyre duhet qe te identifikojme leje (pronen) e perdoruesve te cilet lejohen te lexojne, modifikojne skedaret.
3. Per mbrojtje te sistemit kritik, rekomandohet monitorimi i integritetit te skdareve te sistemit.
4. Specifikojme sharing “webhosting”, ku perdorues te ndryshem ejohen te upload skedar ne te
5. Kodimi i te dhenave preferohet

PRAKTIKAT ME OPTIMALE PER NJE SIGURI TE QENDRUSHEM NE SERVER



1. Shumica e aplikacioneve kane menaxhmentin e sistemit, ku mund te gjejme nje lidhje me rekomandime mbi praktikat me te mira per instalimin e aplikacioneve
2. Princip baze i cdo infrastrukturre ne sektorin e IT
3. Aplikimi i “update per programet dytesore
4. Instalimi me kujdes nga serveret e “dyshimte”

PRAKTIKAT ME OPTIMALE PER NJE SIGURI TE QENDRUSHEM NE SERVER



1. Mund te zgjedhim midis aplikacionit ose Hardwaret te firewall-it per te mbrojtur serveret
2. Per ta mbajtur te mbrojtur gjate gjithe kohes serverin, duhet qe gjate gjithe kohes “firewall” te jete i egzekutuar
3. Rekomandohet qe te perdorim WAF (Web Aplikacionin Firewall) per ta mbrojtur infrastrukturen e server/klientit.

PRAKTIKAT ME OPTIMALE PER NJE SIGURI TE QENDRUSHEM NE SERVER



FALEMNDERIT

Pyetje?