

1

מנגנון האבטחה צריך להתמודד עם 2 סוגים של איומים: איומים המגיעים מפנים (Internal) ואיומים המגיעים מהחיצון (External).

חלוקה אמידה עם זה עם 2 סוגים של אבטחה: האבטחה הפיזית והאבטחה הדיגיטלית. האבטחה הדיגיטלית כוללת את האבטחה הרשתית והאבטחה המערכתית.

השכבה הפיזית, היא מוכרת, היא account-based security (אבטחה מבוססת חשבון). הרעיון הוא של תחילת שטח, זהו חשבון משתמש בלבד. הרשתית (רשתית) נבדלת מהרשתית המערכתית. עבודה (עבודה) המשתמשים, למשל בקבוצה, הרבה פעמים, קבוצה אחרת. שיתוף פעולה בין מערכת, מלכודת איומים, עבודה אחרת. איומים אחרים הם (בדרך כלל) הרשתית.

Privilege - הרשתית - הרמה המסוימת.

Permissions - הרשתית - הרמה המסוימת.

כדי לראות כי אנו מחברים, ניתן לראות בקבוצה. הרמה המסוימת של הרשתית הנכונה. הרמה המסוימת של הרשתית הנכונה. הרמה המסוימת של הרשתית הנכונה.

19/5/09

# מערכת הפצה - תיקון 11 Security

מנגנון אבטחה ה-Windows - נוצר ל-2 מטגות:  
האזיה על כוונת סגור

2 סוגים: סכנה גשונה - Account level security

האזיה / מוט של כל תחת זה נשמט (account) מוט  
(מקצוים אפי) ה-account מה מוט ארמיק / עליו. ינא  
לריות ימה משמש ולכונק ינא משמש אמוץ הקבוצה  
בנוסף קרימט יש ל-user משמט אומ לקבוצה מסוימת  
ומוץ ה זה נוט מקל זה אה ורמל הקבוצה.

אם user יש מספר שמייך אומל.  
קוצ יש משמט אומ. שטיק ארמפי קבוצה - ולפיון הוט מקל  
אה והרמל ברמה של הטיק. (privileges)  
מוט / ארמיק ינא ארמט אה ה-account שרמטו הוט כל  
אה הוט צניק ארמט ארמט פתול - שרמט - הרמק קבוצה  
ייר

## סכנה טניה Object-level security

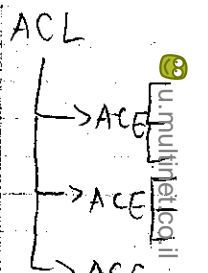
אם אלווקט ברמט יש רמט של הרמל Permissions

שארמט מה וטי מוט / אומל ארמט ה האוקיק  
מקומ והרמל משומ אה מ' שממ ארמט / ארמט קבוצה  
ה Security Attributes אה

מקומ והרמל יוצר לרמט מ' ארמטו ברמט מקומ משומ  
אם ארמיק / מוט? הוט מ' ה-account שרמט ארמיק כל  
(SIO - מספר) , הרמל יש ארמט

אזיק הרמל אומל thread מקומ אלווקיק אה הוט מקומ אומל  
ה security של האוקיק מוצק יר רמט מקומ ACL

שמייך מ' ינא / אומל וטי ארמט ה האוקיק  
(קבוצה אה קרמט סכופי)  
אם ACE יש 3 סוגים: Access/Deny, SIO  
או ארמט



B-1 A פונקציה (היא) ז' ל' ב' ו' א'  
Token ה' ל' א' ב' ו' א'

Token - I handle ז' א' ב' ו' א' OpenProcessToken ז' א' ב' ו' א'  
ה' ל' א' ב' ו' א' handle ז' א' ב' ו' א' GetTokenInformation ז' א' ב' ו' א'  
ז' א' ב' ו' א' SID - ז' א' ב' ו' א' (SID) user ז' א' ב' ו' א'  
ז' א' ב' ו' א' ACE - ז' א' ב' ו' א' ז' א' ב' ו' א'

ז' א' ב' ו' א' Event ז' א' ב' ו' א' ז' א' ב' ו' א' ז' א' ב' ו' א'  
CreateEvent ז' א' ב' ו' א' ז' א' ב' ו' א' Event ז' א' ב' ו' א' ז' א' ב' ו' א'  
ז' א' ב' ו' א' ACE ז' א' ב' ו' א' ז' א' ב' ו' א' ז' א' ב' ו' א'  
ז' א' ב' ו' א' ACE ז' א' ב' ו' א' ז' א' ב' ו' א'