

אבטחת מחשבים ניידים

אחד הסיוטים הגדולים של הארגון הוא בתחום איבוד מחשבים ניידים. הבעיה היא כמובן חוסר הידע של מה נשמר על הנייד בזמן שנגנב ומה יכול הגנב לעשות עם חומר זה. לצערנו, עובדים רבים נוטים לזלזל ולהשאיר את המחשבים הניידים לא מוגנים, בין אם משאירים אותם ברכב (ברור זה הרי כבד) או משאירים אותם לא נעולים פיזית במקומות שונים (אצל הלקוח, בשדה התעופה וכו').

נחלק את ההתמודדות לשני חלקים - האחד התמודדות לוגית והשני התמודדות פיזית. בתחום הלוגי הפתרון כולל התקנת תוכנת הגנה/איתור על המחשב הנייד. בתחום הפיסי - נעילה וגלאי קרבה.

נתחיל ביישומי הגנה - לשמחתנו תוכנות אלה קיימות שנים רבות, הן אמינות ומבצעות היטב את העבודה. בשורה התחתונה, יישום הגנה כזה יבצע הצפנה של כל המידע על המחשב הנייד (או על חלקים נבחרים) (אני ממליץ להצפין הכל)). ברגע שהלך לאיבוד מחשב כזה, לא ניתן יהיה להיכנס לתוך המחשב הנייד ולהביט בקבצים ללא הזדהות של שמתמש. אל תטעו עם זאת להתבלבל בין הגנה של יישום ייחודי זה אל מול ההגנה של מערכות ההפעלה. הרי גם מערכת ההפעלה יכולה להקפיץ חלון הזדהות למשתמש טרם ביצוע שימוש במחשב. לצערנו קל מאוד לפרוץ את מערכות ההפעלה, למשל ע"י הכנסה של CD ועליו היישום. CMD. התקנה של יישום הצפנת המידע תקנה רמת הגנה טובה ושקט ברגע האמת כשמחשב נייד אכן ייגנב או יאבד.

הצפנת כל הדיסק הקשיח תקנה את רמת האבטחה הטובה הנכונה. גם אם אבד נייד הרי שאיבדנו את המחשב אבל נוכל לדעת לכל הפחות כי לגנב לא תהיה כל גישה למידע הרגיש ששמור עליו.

לפני ביצוע התקנה של יישום הגנה/הצפנה על המחשב הנייד מומלץ לבצע גיבוי של הכונן הקשיח כולו למיקום זמני ורק אז לבצע את ההתקנה.

לעיתים מועלה טיעון שאומר שאם נשכחה הסיסמא הרי שלא ניתן יהיה לגשת יותר למידע. טיעון זה אינו נכון שכן בדרך כלל מוגדר גם "מנהל מערכת" על המחשב אשר יכול תמיד להיכנס למחשב ולהפעילו, לשנות את הסיסמא שנשכחה וכו'.

לגבי הגנה פיזית על המחשב הנייד. ישנם כמובן כבלים אשר מאפשרים נעילת המחשב לשולחן - טובים אבל פרימיטיביים. שיטה אחרת היא גלאי קרבה. ברגע שהנייד נגנב והגנב מתרחק ממך, רכיב אשר נמצא אצלך מתריע כי הנייד רחוק ממך יותר ממספר מטרים ומעיר את תשומת ליבך.

שיטה נוספת היא איתור מחשב נייד לאחר שנגנב על בסיס העובדה שהגנב יחבר אותו לאינטרנט. בשיטה זו, מתקינים תוכנה על הנייד שמסדרת בשגרה את המיקום שלו בכל התחברות לאינטרנט למערכת ניהול מרכזית. במידה ונגנב הנייד והגנב מחברו לאינטרנט, המחשב הנייד שולח פרטים שונים אודות המחשב כגון כתובת ה IP ממנה מתחבר הגנב לאינטרנט, בעזרתה ניתן להתחקות אחר המחשב בדיוק רב. בצורה זו ניתן לאתר את כתובת ה IP לברר מול חברת האינטרנט מי השתמש בה ולאחר את הגנב בזמן קצר ביותר.

יישומי הצפנה:

<http://www.sophos.com/products/enterprise/encryption/safeguard-easy/>

יישומי הגנה פיזיים:

גלאי קרבה

<http://www.defensedevices.com/laptop-security-alarm-monitor-notebook.html>

איתור מחשב לאחר גניבתו

<http://www.ztrace.com/zSecuritySuite.asp>