



יצחקי-וינברגר יועצים בע"מ
ת.ד. 2105, נתניה, מיקוד 42120, ישראל
טלפון: 09-8338972, פקס: 09-8338969

יצחקי-וינברגר יועצים בע"מ גאים להציג את מערכת :

VIPER 1.0

- האם יש במחשבים שלך מידע רגיש, מידע יקר ערך או מידע מסווג עליו אתה רוצה להגן ?
- האם נפילה של מידע זה לידי צד ג' כלשהו עלולה לגרום לאסון מבחינתך או לנזק כלכלי כבד ?
- האם יש לך צורך להעביר מידע רגיש ממקום למקום בארץ או בעולם, ויש לך חשש מכך שהמידע יגיע לידיים הלא נכונות, יהיה מיורט ע"י צד ג' או ישוכפל בזמן ההעברה ?
- האם יש לך צורך שהמידע שלך יעבור את אמצעי האבטחה של מיטב החברות הקיימות בשוק (למשל Intrusion Detection, Firewalls, Systems) אמצעים לניטור תעבורה נכנסת ויוצאת וכו') ויצליח לחדור לתוך רשת מוגנת או לצאת מתוך רשת מוגנת בהצלחה וללא שהדבר יאותר?

מערכת VIPER היא הפתרון האידיאלי לצרכים אלו ואחרים!

VIPER 1.0 – המשך (א)

- ◀ מערכת VIPER פותחה ע"י פז יצחקי-וינברגר, טכנולוג בכיר בעל ניסיון רב באבטחת מידע וקצין יוצא יחידת העלית הטכנולוגית של חיל המודיעין !
- ◀ בפיתוח מערכת VIPER הושקעו משאבים רבים, ידע ייחודי רב והיא מבוססת רעיון ואלגוריתם פורץ דרך. VIPER מהווה את מערכת האבטחה מסוג קו אבטחה אחרון הטובה ביותר בשוק העולמי כיום!
- ◀ מערכת VIPER הופכת את המידע הרגיש שלך ללא זמין בכל צורה ואופן, ולמעשה "מעלימה" אותו לחלוטין.
- ◀ VIPER אידיאלית בהיותה משמשת כקו ההגנה האחרון שלך :
לדוגמא, גם במקרה קיצוני בו המחשב אשר בתוכו מאוחסן המידע הרגיש שלך נופל לידיים הלא נכונות חרף אמצעי אבטחה אחרים שנקטת (למשל ניתוק מהאינטרנט, שימוש בתוכנות וכלי אבטחת מידע – Firewall, הצפנה וכו'), מניעת גישה פיסית למחשבים לאנשים לא מורשים וכו') – גם במקרה קיצוני כזה, המידע הרגיש שלך עדיין בטוח.
דוגמא שנייה להמחשה, שוב מקרה קיצוני :
הנך מעביר מידע רגיש על גבי דיסקט / CD וזאת ע"י בלדר כלשהו. לך קיים החשש כי צד ג' כלשהו יצליח לשים את ידיו על הבלדר ועל הדיסקט / CD תוך כדי ההעברה וכך המידע יהיה בסיכון. בנוסף, תמיד קיים החשש כי הבלדר עצמו ירצה להציף לתוכן המידע המועבר, לשכפל אותו ולמכור אותו לגורם אחר וכו'. גם במקרה קיצוני שכזה, בו חרף כל אמצעי האבטחה האחרים נופל הדיסקט / CD לידיים הלא רצויות, עדיין המידע הרגיש עצמו יהיה מוגן.
מידע מועבר בלדר שכזה יכול לכלול סודות מסחריים, שמות ומספרי טלפון של אנשי קשר, תיאום לביצוע פעולה כלשהי, תמונות של מבנים או אנשים, קוד פתיחה של כספת או מספרי חשבונות בנק, מיקום של טובין / מידע / נקודת איסוף ועוד דוגמאות רבות כיד הדמיון הטובה, כולם יוגנו בקלות בזמן ההעברה ע"י VIPER.
המידע שלך לא יהיה ניתן לאיתור ע"י אף תוכנה ואף כלי מתקדם הקיימים בשוק, וזאת גם אם צד ג' יעסיק מומחי מחשוב ואבטחת מידע מהשורה הראשונה.

VIPER 1.0 – המשך (ב)

◀ VIPER יכולה להיות גם קו ההגנה הראשון שלך :
במקרים רבים, ההגנה ש-VIPER מספקת היא הגנה חזקה מספיק בכדי להוות את קו ההגנה הראשון שלך, ולא רק קו ההגנה האחרון. VIPER מעלימה את המידע באופן בטוח שכזה, שאתה תוכל לחסוך ולקצץ בהוצאות אבטחת המידע / מתקנים שלך, ביציאה מנקודת הנחה משמעותית – גם אם תהיה גישה לצד ג' למדיה בה מאוחסן המידע (דיסק קשיח, CD, דיסקט, דואר אלקטרוני רגיל ולא מאובטח שמאוחסן על שרת דואר וכו') לא תהיה לו יכולת להגיע למידע עצמו ואף כלי קיים בשוק לא יצליח לאתר את המידע.

◀ המידע יהפוך לנגיש חזרה רק באמצעות תהליך UnVIPER ייחודי אשר יהיה נגיש רק לך.

◀ מערכת VIPER כוללת מודול התקנה והסרה עצמית (מנגנון "השמדה עצמית").

מודול זה מאפשר לך להתקין את VIPER על מחשב, להעלים את המידע הרגיש שלך, ומייד לאחר מכן להסיר את המערכת מהמחשב וזאת בלי להשאיר עקבות או הוכחות להתקנה כלשהי וקיום המידע על המחשב שלך.

יכולת זו הנה יכולת ייחודית – במיוחד בסביבת Windows מערכות שונות משאירות "חתימות" ו"עקבות", אשר יכולות לפעול לרעתך ומורידות את כל אבטחת המידע לטמיון.

◀ ובשורה התחתונה :

מערכת VIPER יכולה לחסוך לך נזקים שייגרמו כתוצאה מחשיפת המידע הרגיש שלך (החל מחסכון נזק כספי של מיליוני דולרים וכלה בכל נזק אחר שיכול להיגרם לך כתוצאה מחשיפת מידע). הגנה זו ניתנת בין אם מדובר בסודות מסחריים או בסודות אחרים, בין אם מדובר במידע המאוחסן על מחשבים מוגנים באמצעים אחרים, מחשבים לא מוגנים כלל, מידע המועבר על מדיה ניידת על-ידי בלדר או נשלח בדואר אלקטרוני רגיל. הגנה זו טובה למגוון איומים רחב, ויכולה לשמש לצרכים רבים.

מדיה (דיסק קשיח) המכיל מידע ש"הועלם" ע"י מערכת VIPER נבדק ע"י מספר מהטובים שבמומחי אבטחת המידע בישראל. מומחים אלו עשו שימוש הן בידע הנרחב שלהם והן במגוון כלים הקיימים בשוק וכלים ייחודיים שלהם אשר אינם קיימים בשוק. בנוסף, כולם היו מיוודעים מראש על כך שקיים משהו לא טריוויאלי על דיסק קשיח זה (יתרון שלא יהיה קיים בהכרח ברוב המקרים בהם VIPER תגן על מידע), ובכל זאת לא הצליחו לשחזר את המידע הרגיש.