

KISS - Keep information security simple

”מורכבות היא האויב הנורא ביותר של אבטחת מידע” Bruce Schneier - מומחה אבטחת מידע

מאת: אורן שניצר

4. האם הפתרון מוסיף או גורע מהעומס של העבודה השוטפת?
 5. האם הפתרון מאפשר לי, מחלקת אבטחת המידע, שליטה, אכיפה וניתוח המידע בהתאם לצרכי היחודיים?
 בחינת השאלות הללו בשלב סקירת המוצר, תאפשר קבלת החלטה נכונה יותר על אופן השילוב, אם בכלל, של הפתרון בארגון. על כולנו החובה להקטין את פגיעות הארגון ולשפר את אבטחת המידע מפני איומי הסייבר השונים. כעת רק נותר להתאים את הפתרון הנכון ביותר והפשוט ביותר לארגון ולצרכיו.



אורן שניצר

חברת רי-סק טכנולוגיות מפתחת את פלטפורמת הגנת התוכנה הארגונית ReZone. המערכת מספקת הגנה מפני התקפות סייבר באופן רב שכבתי ובין היתר בפני איומים מודרניים כדוגמת APT, Zero-Day והתקפות ממוקדות. המערכת מודלרית וניתנת להתאמה פשוטה ומדויקת לצרכי הלקוח. המערכת כוללת רכיבי אבטחה מתקדמים המאפשרים שליטה על המידע הזורם לארגון ואת זיהויים המוקדם של האיומים. בין יתרונות המערכת נמנים השקיפות למשתמש הקצה, נוחות הניהול והתחזוקה המינימאלית. ReZone מציעה התממשקות פשוטה לגלישה בטוחה, מיילי, חוסם התקנים על תחנת הקצה, כספות וכו'. היא מאפשרת הגדרת ואכיפת פרופילי משתמשים שונים באופן אחוד ובהתאם לסוגי הקבצים (True Type) שמוכנסים לארגון.

***הכתוב הינו מומחה אבטחת מידע ושותף מייסד בחברת רי-סק טכנולוגיות**

מלחמת הסייבר מתנהלת סביבנו בכל עת כשדיווחים על אירועים חמורים כקלים עושים כותרות על בסיס יומי. כבר בשנת 2010 כארבעים אחוזים מהארגונים דיווחו על: malware related breaches (Source: Deloitte-NASCIO Cyber Security Study 2010) ובמעל שישים אחוזים נמצאו BOT. אין כמובן סיבה להרים גבה ולהתפלא, כיום ניתן לרכוש ב-\$500 BOT TOOLKIT המאפשר התאמה דינאמית לסוג ההתקפה שרוצים לחולל ולארגון היעד הספציפי אותו מעוניינים לתקוף. התקיפה כאמור מתרחשת על בסיס קבוע. הנזקים נאמדים במאות מיליוני דולרים והמירוץ אחר פתרונות הולך ומתעצם מיום ליום. הארגונים מודעים היטב לחולשה שלהם - מידע הנשלח ו/או מוכנס מחוץ לארגון פנימה. בידי מנהלי אבטחת המידע הופקדה משימה בלתי אפשרית, הם נדרשים להפטר מחולשה זו במינימום תקציב ותחת מגבלות קשות. הוטל עליהם למצוא את ה-silver bullet שיגן על הארגון באופן מושלם ויסגור את כל הפרצות וכל זה מבלי לפגוע בעבודה השוטפת, כמובן.

מלאכת האיזון הינה האתגר המרכזי בניסיון לתת מענה לבעיה המדוברת. הארגון נדרש לשמר שגרת עבודה שוטפת מחד, ולעמוד בסדרה של מגבלות שיעודן להגן על הארגון מאידך. אופי המגבלות ומורכבותן תלוי ברמת הסיכון אליה חשוף הארגון ואותה הוא מוכן לספוג. הממשקים להם נדרש לתת מענה נעים על קשת רחבה, כאשר הבולטים מביניהם הם קבלת מיילים מחוץ לארגון, גלישה מאובטחת וקבלת מדידת נתיקות לתוך הרשת הפנימית.

מנהלי אבטחת המידע עסוקים היום בחלק הולך וגדל מזמנם בבחינת שלל פתרונות המתמקדים בהגנה על ממשק כזה או אחר מתהליכי העבודה בארגון. הפתרונות השונים בארגון הופכים לנטל ניהולי מורכב הדורש שעות עבודה רבות, קשב ותחזוקה יומיומית. בנוסף, כל מערכת חדשה שמוטמעת דורשת התאמה של תהליכי הניהול הקיימים ו"חינוך" של כוח האדם תוך ניסיון לשמור על פגיעה מינימלית בנהלי העבודה שהיו נוהגים עד כה. דמיינו את הפליאה והמרמור של העובדים כאשר ביום בהיר אחד הם נדרשים לפתע לעמוד בתור מול עמדה יעודית על מנת להכניס קובץ ממדיה נתיקה למחשב שלהם או כשפתאום חלות עליהן מגבלות קשות בעת גלישה.

בתור מול עמדה יעודית על מנת להכניס קובץ ממדיה נתיקה למחשב שלהם או כשפתאום חלות עליהן מגבלות קשות בעת גלישה.

נשאלתי לאחרונה בייאוש ע"י מנהל אבטחת מידע בארגון פיננסי - מה היא דרך המלך?

התשובה כמובן אינה פשוטה, אך כשבוחנים פתרון כדאי להקפיד על מספר קווים מנחים:

1. כמה מורכב הפתרון וכמה מורכב יהיה ניהולו (בשעות עבודה) או שאולי הוא בכלל חוסך עבודה?
2. האם הפתרון יודע להתאים את עצמו בקלות להתרחבות הארגון או המערכות הקיימות/עתידיות?
3. עד כמה הפתרון שקוף למשתמשים והאם נדרשת הדרכה בארגון?

