Newsletter #4

לקוח נכבד,

תחום שירותי האבטחה המנוהלים (MSS) הפך לאחד הנושאים החמים בעולם אבטחת המידע. שוק האבטחה הגיע להבנה כי קיים צורך בניטור ומעקב אחר מכלול מערכות המחשוב של הלקוח על מנת לאתר את סיכוני האבטחה המאיימים על המערכות בזמן אמת.

חברת סקיוריטרי, בשיתוף עם חברת סימנטק, מספקת שירותי ניהול וניטור מרוחקים בארץ ובעולם. מוקד האבטחה שלנו מתממשק אל מרכזי האבטחה (SOC) של סימנטק בעולם ויחד אנו מנטרים ומנתחים את מערכות המחשוב וכן מספקים שירותים בזמן אמת 24X7 של התראות על סיכוני אבטחה אצל הלקוח ע"י איסוף ההתראות ממערכות ה- FIREWALL, ANTIVIRUS, VPN, ו-IDS ועוד .

ב- 18 באוקטובר נקיים יום עיון בנושא שירותי ניהול מרוחקים אשר במהלכו יתקיים סיור מודרך (VIDEO CONNFERENCE) באתר המרכזי של סימנטק בעולם.

ההרשמה מתקיימת דרך האתר :

http://securitree.co.il/seminar/registration.html

בהמשך, מצורף המאמר " שירותי אבטחה מנוהלים (MSS) בעולם" להעשרת הידע בנושא.
לקבלת פרטים נוספים ופניות בנושא, ניתן ליצור עימנו קשר בכתובת Info@securitree.co.il .

אביאת בר
מהנדסת אבטחת מידע

שירותי אבטחה מנוהלים (MSS) בעולם

מאת: אביאת בר, מהנדסת אבטחת מידע ואחראית תחום שירותי ניהול מרוחקים בחברת סקיוריטרי.

שירותי אבטחה מנוהלים (MSS) , מהם?

התקפות רבות קיימות בעולם האינטרנט בימינו. וירוסים, קוד זדוני וסוסים טרויאנים הפכו להיות המושגים השגורים בפי מנהלי ה-IT, המתמודדים עימם כחלק מהעבודה היומיומית השוטפת. חשיבות האבטחה הופכת להיות קריטית יותר ויותר עבור אירגונים שבאמתחתם מידע עסקי רגיש וכל מידע רגיש אחר הקיים במערכות המחשוב של האירגון. כאן למעשה מתעורר הצורך בביצוע הערכה מחודשת של מצב האבטחה במערכות הפנים אירגוניות במטרה לתפור תשתית מאובטחת על התשתית הקיימת. הכנת תשתית מאובטחת זו, שתענה על צרכי הארגון, גוררת עימה שיקולי ציוד חומרה, תוכנה ורישיונות תוכנה, צוות ניהול, פיקוח ותחזוק מקצועי בזמן ומחוץ לשעות העבודה ומיקום מתאים עבור אלו האחרונים, על מנת לנהל את המערך שנבנה.

כל הצרכים שנמנו, כרוכים בהשקעת עלויות גבוהות וקושי בניהול מקצועי ושוטף של התשתית האבטחתית, דבר שהניע אירגונים לחפש מקורות חיצוניים על מנת לקבל שירותי אבטחה מתאימים. כך נולד המושג Managed Security Services -MSS: הקמת מוקדי אבטחה של ניהול ובקרה חיצוניים הנותנים פיקוח שוטפים למערכות המחשבו של האירגון. ה- MSS-ים הקיימים בעולם מציעים ניהול וניטור שוטף של 24X7 בזמן אמת (real time) וכוללים בתוכם מס' שירותים עיקריים:

1. Managed Firewall - הכולל ניהול וניתוח לוגים של סוגי FW-ים שונים ומתן תגובה או חסימה בהתאם לאיומים מאותרים.
2. Managed VPN- המשלב ניהול ובקרה אחר VPN-ים הקיימים ברשת הלקוח ומאפשר טיפול בהגדרות כניסה מרוחקת לרשת דרכם.
3. Managed IDS (Intrusion Detection) - המבצע מעקב, ניהול ומתן התראות על הרשת, תוך כוונון עדין של מערכות ה-IDS על מנת לסנן התקפות שגויות (false positive) ולאתר התקפות קיימות.

4. Managed Vulnerabilities - מספק ניתוח והגנה מפני פוגענים, ונדלים וכל דרך לניצול פרצות במערכות הלקוח. שירות זה כולל בתוכו שירותים כדוגמאת ניהול Antivirus-ים וContent Filtering.

שוק ה-MSS, לאן פניו מועדות?

שירותי האבטחה המנוהלים נמצאים כיום במגמת עליה בשוק אבטחת המידע. דוח גרטנר מציג גידול של שוק ה- MSS בשנת 2003 וצופה כי ב- 2005, 60% מחברות ה-Enterprise ירכשו שירותי ניהול אבטחה מרוחקים לפחות לחלק מהרשת בארגון שלהם. חברת Yankee Group מדווחת כי שוק ה- MSS צפוי לעלות לשווי של כ-4 ביליוני דולרים ב-2008.

שחקני השוק המובילים

שוק ה-MSS החל דרכו עוד בשנת 1999, כאשר אופיין בעיקר בחברות קטנות (בוטיקים כפי שהגדירו האנלסיטים),אשר הציעו שירותי ניהול מרוחקים העטופים בתחום יחודי מתוך מכלול שירותי האבטחה. מומחים רבים טענו שמגמה זו לא תמשך זמן רב וריבוי הפתרונות מחד ומגוון רחב של חברות קטנות מאידך, לא יחזיק מעמד זמן רב . הצפי היה שחברות אבטחת מידע גדולות ירכשו את הבוטיקים ויוסיפו את שירותי ה MSS כחלק מסל השירותים המוצע שלהן . היתרון, כמובן, עומק פיננסי, חוסן כללי שהלקוחות חיפשו ומגוון עשיר של פתרונות ושירותים . ואכן נבואה זו הגשימה את עצמן . מספר מוביל של הבוטיקים בתחום ה MSS נרכשו ע"י חברות גדולות (ראה פירוט בהמשך) . היום ההבדל נעוץ במגוון השירותים וחלוקה קטגורית בין חברות המציעות שירותי ניטור בלבד (Managed Security Monitoring -MSM) לבין המציעות שירותי ניטור וניהול :

- Counterpane - חברת אבטחת מידע באינטרנט אשר מרבית משאביה מושקעים בשירותי אבטחה מנוטרים (MSM). חברה זו פיתחה את שירותיה ללא

קניית חברה שמציעה את שירותי האבטחה אלו. Counter מונה שני מרכזי אבטחה (Security Operation Center – SOC) , האחד ב-Mountain view והשני ב Cantlly. לקוחותיה נמנים בין חברות ממשלתיות , e-commerce, גופים פיננסים בריאותיים ועוד. שירותי הניהול המרוחקים של החברה מושתתים על טכנולוגיות שהיא פיתחה: האחת ה"שומר" (Sentry) המותקן ברשת הלקוח ותפקדו לאסוף למיין ולנתח נתונים מהתקנים שונים ברשת כגון:FW, נתבים וכו'. המידע עובר אל ה"מעריך" הנמצא ב-SOC (Socrate) לבדיקת איומים פוטנציאלים ברשת ולייצור אתראות ללקוח בהתאם.

- Verisign - החברה מספקת פתרונות טלקומיוניקציה חכמים ומאובטחים. בפברואר 2004 קנתה Verisign את חברת Guardent, שסיפקה שירותי ניהול מרוחקים בשנים האחרונות, והחלה מוכרת שירותים אלו. שירותים אלו מבוססים על ארכיטקטורה בשם Teraguard, האוספת מידע ממקורות שונים והופכת אותם לרצף אחיד של אירועי אבטחה הקשורים זה בזה. בשלב הבא מתבצעים קורלציה וניתוח של המידע ב-SOC.

- Symantec - החברה מספקת מוצרים והתקנים (Appliances) בתחום אבטחת המידע לחברות שונות ולשימוש ביתי. ביולי 2002 קנתה Symantec את חברת Riptech שפיתחה את שירותי ה-MSS. שירותי הניהול המרוחקים ניתנים בכשישה SOC-ים בארצות שונות בעולם ביניהם: אנגליה, גרמניה וארה"ב. שירותי הניטור והניתוח שמציעה סימנטק מקיפים מוצרי אבטחת מידע מבית סימנטק ומוצרים של ספקים שונים כאחד, דבר המאפשר התאמה אישית של השירות לצרכי הלקוח. הנתונים שמגיעים אל ה- SOC-ים, עוברים ניתוח מעמיק לשם מציאת איומים פוטנציאלים. הממצאים שנגלו מדווחים ללקוח דרך שערי מידע מאובטחים באינטרנט.

- ISS - Internet Security Systems (ISS) מספקת גם כן מוצרים ושירותים בתחום אבטחת המידע. לחברה שישה SOC-ים בעולם הנתמכים ע"י צוות מומחים המכונה X-Force, המבצעים ניתוח ומחקר של המידע המנותר.

- TruSecure - חברת שירותי אבטחה זו מספקת גם כן את רוב שירותי הניהול המרוחקים ומאפשרת ניטור וניתוח מעמיק של אפליקציות שונות הנמצאות באתר הלקוח. ה-SOC של החברה נמצא באטלנטה, ג'ורג'יה.

Company	Managed FireWall	Managed IDS	Managed VPN	Managed Vulnerabilities	שירותי ניטור וניהול
Counterpane	+	+		+	ניטור בלבד
Verisign	+	+	+	+	ניטור וניהול
Symantec	+	+	+	+	ניטור וניהול
ISS	+	+	+	+	ניטור וניהול
Trusecure	+	+		+	ניטור וניהול