open | solutions

The asset protection specialists

הצורך בניהול אבטחת מידע כמו יחידה עסקית

Run information security like you run your business

A White Paper

Prepared by Danny Lieberman-Open Solutions

Feb 1, 2005

נהל ע"פ יעדים. לאנשי המכירות בחברה יעדי מכירה והישגיהם נמדדים על פי מרווח גולמי וגביה בפועל. לאנשי הייצור וההפצה שלכם יעדי אספקה ומספר סבבי מלאי. האם ל CSO, CIO, אנשי אבטחת מידע ומפתחי התוכנה שלכם הוצבו יעדים ברי מדידה עם תגמול שמותנה בעמידה ביעדים או בביצועים מעבר ליעדים? רוב הסיכויים הם שבחברתך אבטחת המידע אינה מנוהלת ככל יחידה עסקית אחרת עם אסטרטגיה ברורה וממוקדת בלקוחות, מצב השוק ומתחרים. ללא מודלים סטנדרטיים ונטולי השפעות ספקים, ללא מדדי ביצועים תקניים ומוגדרים היטב, לא יתכנו התקדמות ושיפור, והתקדמות ושיפור הם בדיוק מה שהלקוחות שלנו דורשים.

הכר את היחידת העסקית של 2005. בין אם אתה קבלן החופר תעלות לספק טלוויזיה בכבלים או בין אם אתה מנכ"ל חברת הכבלים, אתה חי על מידע. נכסי מידע יקרים כגון רשומות לקוחות נאגרים בצורה דיגיטלית במחשב אישי, בשרתי חלונות, לינוקס או במיינפריים. הנייר הפך עותק בלבד ולא הנכס המקורי. החברה שלך מנהלת רכוש קבוע ומפיקה דוחות לבורסה, **אבל** האם אתה מסמן ומשערך את הנכסים *הדיגיטליים* המהווים עמוד שדרה לעסק? האם אתה יכול לחשב ROI לטכנולוגיית אבטחה או להוכיח תאימות עם Sarbanes Oxley 906 ללא שערוך כספי של הנכסים הדיגיטליים העיקריים של העסק?

בחר באסטרטגיה עסקית לאבטחת נכסי המידע שלך. היום, אבטחת מידע פועלת במעגל אכזרי של פגיעה, תגובה ורכישה. הפעילות חייבת לפעול באופן רצוף ויזום במסגרת מודל איומים סטנדרטי ומוגדר היטב שיכול לעמוד בהשוואה עם שחקנים אחרים בתעשייה שלך בדומה לפעילות benchmarking שמטרתה שיפור ניהול, תפעול ורווחיות היחידה העסקית.במאמרו הקלאסי "What is strategy?", כותב מייקל פורטר: "תמצית האסטרטגיה היא לדעת במה **לא** לבחור... עמדה תחרותית חזקה דורשת החלטות ברורות ומערכת של פעילויות משולבות המתאימות היטב לעסק ומחזקות אותו". ברור שאסטרטגיה כזאת חסרת במרבית ארגוני אבטחת המידע בישראל.

בצע מדידות על מנת לנהל, לשפר ולעמוד בדרישות החוק. ישנם מודלים עסקיים מוכרים ומקובלים המתאימים לכל יחידה עסקית. לתמחור מוצר או שירות, חברת הפצה משתמשת במרווחים, מפעל ייצור משתמש בכתב כמויות וחברת שירותים מקצועיים בתמחיר פעילויות ושעות עבודה במחירי תקן. על מנת להעריך את תזרים המזומנים כל שעליך לעשות הוא לבדוק את התזרים מתפעול העסק, או לחשב תזרים חופשי (FCF) שהוא התזרים מהתפעול בניכוי הוצאות בגין רכישת ציוד הוני. אכן, FCF לא כולל את עלות החוב, אך עדיין יש בידך מדד אובייקטיבי שניתן למדוד מדי שבוע, או רבעון במשך כל חודשי השנה. רשת סופרמרקטים גדולה הפסידה לא מזמן כחמישה מיליון דולר במכירות בגלל שעובד הדליף את מחירי הקנייה של מוצרים למתחרה באמצעות Instant Messaging. החברה הגיבה בנעילת דלתות מצלמות, אבל מנעולים ומצלמות לא יכולים לבחון בזליגת מידע ולספק מדדים למידת שמירת הסודיות של הארגון.

בחן את אסטרטגיית אבטחת המידע שלך

1. האם ההשקעה שלכם בהגנה על נכסים דיגיטליים נדחפת ע"י תקנות המחוקק?
2. האם מחקרים של גרטנר מהווים גורם מפתח בקבלת החלטות רכש?
3. האם עדיין אין לך מדדים של נצחונות מול הפסדים במלחמת אבטחת המידע היום-יומית?
4. האם ה CSO שלך נפגש עם לפחות שלושה ספקים ביום?
5. האם תהליך הרכישה של מוצר חדש בתחום אבטחת המידע אורך לפחות שישה חודשים?
6. האם יש חוסר בכוח אדם וזמן רב לא ייושמו טכנולוגיות אבטחה חדישות?
7. האם הCTO שלכם מעולם לא מכרה או התקינה בעצמה אפילו אחד ממוצרי החברה?

אם עניתם בחיוב לארבע מתוך שבעת השאלות, סימן שלחברה שלך צורך דחוף באסטרטגיה עסקית עם מדדים תפעוליים למערך אבטחת המידע.

נקוט פעולות הגנה על נכסי המידע שלך כשם שאתה מנהל את העסק שלך

1. הצב מדדים ופרסם אותם אחת לשבוע באינטראנט הארגוני כך שכל העובדים יכירו אותם. התחל עם שלושה מדדים: מספר אנומליות הרשת שנמצאו על ידי ה IDS באותו שבוע, זמן מחזור נוכחי לעדכוני תוכנה ומספר השעות הנוספות שעבד צוות האבטחה באותו שבוע.
2. בצע ביקורת אבטחה מתמשכת. רכוש כלי לביקורת רשת והפעל אותו פעם בשבוע, כל פעם בחלק אחר של הרשת. החבר׳ה במחסן שנים כבר לא עושים ספירת מלאי מלאה שנתית; הם סופרים חלק קטן מהמלאי מדי יום בעזרת קוראי ברקוד. הביאו יועץ מומחה שיעזור לך להקים את כלי הביקורת והפעיל אותו בעצמך.
3. הפעילו תוכנית מודעות עובדים. הפוך את מספר שעות ההדרכה לאחד מהמדדים שלך.
4. בנה מודל איומים ובסיס נתונים של נכסים, איומים ונקודות התורפה עיקריים. התחל בבניית מודל האיומים כבר היום.
5. הגדר את האסטרטגיה התחרותית שלך למערך אבטחת המידע:
   - האם הקוו המנחה הוא לשמור על רמת השקעה כספית נמוכה?
   - האם הכוון הוא מדיניות של ספק יחיד? או Linux desktops ?
   - האם המיקוד הוא ב end-point security לעומת perimeter security?
6. יישם מערך פעילויות **עקבי**, למשל תקן של Thin clients, Remote desktop ו Windows Terminal Server
7. חשוב כיצד פעולות שונות יכולות **לחזק** זו את זו, למשל התקנת תוכנת firewall אישית המדווחת על נסיונות חדירה לשרת ראשי כך ניתן לתכנן את התגובה להתקפות עתידיות.
8. זהה מערך פעולות **המייעל** את מאמציך בתחום. אולי שיש לכם רשת שטוחה לחלוטין הדומה לצלחת ספגטי של שרתים ותחנות. חלק את הרשת ל VLAN's, שרתי יישומים בסגמנט אחד, שרתי נתונים בסגמנט אחר, תחנות עבודה בסגמנטים מחלקתיים וכן הלאה. הביצועים והאבטחה ישתפרו ותוכל לבצע ביקורת תוכן (content monitoring) ביעילות. פחות זמן יבוזבז על כיבוי שריפות ויותר זמן יתפנה למחשבה ותכנון.
9. התקינו את המוצרי החברה בעצמכם פעם ברבעון. לאחר שתעשה זאת בחן את האופן שבו לקוח סופי מבצע את ההתקנה, ורשום הערות. עדכן את מודל האיומים על פי הממצאים.

לפרספקטיבות נוספות בנושא אסטרטגייה תחרותית ראה מאמרו המצוין של מייקל פורטר "What is Strategy" בגרסה המקוונת של Harvard Business Review.

הערות, הארות ל dannyl@software.co.il
ניתן לקבל מידע נוסף באתר www.software.co.il/extrusion

דני ליברמן, מנכ״ל של Open Solutions. החברה מתמחית בהגנה על נכסים דיגיטליים ועוזרת להנהלה הבכירה למנוע זליגת מידע בשוגג ובמזיד ולפתח מערכת תוכנה בטוחות יותר. עם לקוחות המוצרים והשירותים שלנו נמנות חברות כגון Sun ו BMC Software .