

## מיכה וייס, בנק מזרחי טפחות: "במתקפות סייבר אנחנו כמו ברווזים במטווח"

"המתקפות האחרונות על האתרים הישראליים, כולל מוסדות ממשלה, הדגישו את העובדה שכדי הגורמים בענף צריכים עזרה להתמודד איתן, הוגרמים בענף צריכים עזרה מהמטה הקיברנטי הלאומי, מרא"ם שבשב"כ ועוד", אמר מיכה וייס, מנהל אבטחת מידע בבנק ♦ לדבריו, "ישראל מגנה על תושביה בכל היבט - למעט הסייבר"

יש כוונות, הרבה גורמים הם יותר ממוקדים ואנחנו יותר מותקפים. כמו כן, בשנה האחרונה רמת העצימות של המתקפות צמחה. יש יותר תקיפות, ההסתברות לתקיפות עלתה ועימה עלה הסיכון."

"מה שנדרש ממנהלי אבטחת המידע הוא לפעול בכמה מישורים", ציין וייס. "צריך לראות מה מחובר למה, מאיפה מגיעות התקיפות, לחבר נתונים ולדווח לדרגים השונים. יש המון מידע, נדרש לסנן אותו ולמצות ממנו מידע מדויק, על מנת לדעת מה לעשות עימו. צריך להתמחות ולמצות את העיקר מכל המערכות. מערך הדיווח הוא נושא מאוד חשוב. יש להקים מערכת להתוויית מדיניות ולוודא שהיא מגיעה לכל הפינות בארגון. צריך לבצע הערכת סיכונים דינמית ושוטפת. יש להדק את שיתופי הפעולה, ברמה הפנים ארגונית, ברמת מגזר התעשייה וברמה הלאומית כאחד. ככל ששיתופי הפעולה יעמיקו, כך ההצלחה תהיה טובה יותר."

טכנולוגית גם בעבר, אלא שכעת היא צצה מעל פני השטח. מנהלי אבטחת המידע בארגונים חווים בפועל, באירועים האחרונים שקורים, את מה שדיברנו עליו בעבר באופן תיאורטי, כפוטנציאל של סכנה."



מיכה וייס

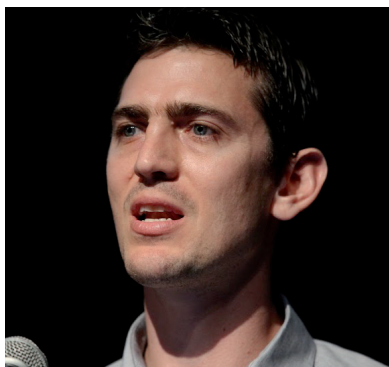
הוא אמר, כי "מספר מימדים השתנו לרעת מנהלי אבטחת המידע בארגונים: התוקפים הם בעלי טכנולוגיה ההולכת ומתפתחת,

"במהלך אפריל היו תקיפות של אלפי אתרים במדינה, כולל מוסדות ממשלה, והן חיזקו את העובדה שכאשר התקיפות באות מבחוץ, אנחנו כמו ברווזים במטווח. לשם כך, הגורמים בענף צריכים עזרה ממוסדות המדינה", כך אמר מיכה וייס, מנהל אבטחת מידע בבנק מזרחי טפחות. לדבריו, "ישראל מגנה על תושביה בכל היבט - למעט הסייבר. יש משמר הגבול, משטרה, צבא, הגנה על הדואר ועל נמל התעופה בן גוריון. התחום היחיד מפניו אין הגנה הוא הסייבר." "אנחנו יודעים להתמודד עם שלל האתגרים הקיימים בעולם אבטחת המידע ובעולם הסייבר, אבל זקוקים לסיוע מהרשויות: מהמטה הקיברנטי הלאומי, מרא"ם שבשב"כ ועוד", הוסיף וייס. "יש למצות את העיקר משלל המידע האבטחתי הקיים". וייס דיבר בכנס במסגרת פאנל שנערך באירוע, אותו הנחה אופיר זילביגר, מנכ"ל SECOZ. לדבריו וייס, "לתוקפים הייתה יכולת

מאפשר זיהוי ממשי של המשתמש, כדי לשלוט בגישה שלו למידע. בשכבה השנייה נמצא התקן ה-IPS, שמספק ניהול טלאים לפי פרופילים מומלצים. ה-IPS מוודא שהחולשות של היישומים לא ינוצלו ומגן גם על משתמשי הקצה. השכבה השלישית היא האנטי וירוס, שלמעשה

מנקה 'רעשים' אבל לא לוכד את כל האימונים על המידע."

"מעליה נמצא האנטי בוט. בעת מתקפות בוט, הבוט מחכה להוראות ממרכז השליטה והבקרה של התוקפים ומפיץ את עצמו ברשת. בין היתר, בוטים מסוגלים לגנוב סיסמאות מהמחשב, להריץ דואר זבל בכמויות גדולות וליצור Anti-Bot.click fraud. ה- Anti-Bot מבין את התנהגות



צור תדהר

הבוט ומסוגל להתמודד עם כל האימונים הללו. הוא עושה זאת, בין היתר, על ידי יצירת חתימות התנהגות של משתמש ולא של קובץ. ניתן לחסום

תוכנות וחומרה, שמאפשרים הגנה מפני חדירות לרשתות מחשבים ותקשורת, מערכות מידע ורשתות פנים ארגוניות. מוצרי החברה מספקים פתרונות הגנה מפני מתקפות Zero Day, מתקפות ממושכות וממוקדות (APT) ופתרונות להגנה מפני רוגלות."

לדבריו, "הפתרונות פותחו במטרה לתת מענה מלא לרגולציות שונות בעולם אבטחת המידע במגזרים השונים, והם מספקים יכולת ללמוד בזמן אמת את הרשת ולהתאים את מדיניות ההגנה לכל מערכת. יתרונה של SOURCEfire הוא בהיותה בעלת יכולת הזיהוי הכי גבוהה בשוק של רוגלות - גם בתחנות הקצה וגם בשרתים. אנחנו מחוללים שינוי באופן שבו ארגונים וגופים ציבוריים בינוניים עד גדולים מנהלים סיכוני אבטחה, ומפחיתים אותם למינימום."

הוא סיים בצינון, כי החברה פתחה באחרונה סניף ישראלי ואמר, כי "אנחנו מקווים שהשוק הישראלי ירתח."

### בחמש שנים האחרונות קפצה כמות הנוזקות ב-700%

"בחמש השנים האחרונות קפצה כמות הנוזקות ב-700%, בכל יום יש אירוע סייבר וכל יישום מגיע כיום עם פגיעויות. המענה למציאות הזו הוא הגנה רב שכבתית", כך אמר צור תדהר, מהנדס מכירות בצ'ק פוינט.

לדברי תדהר, יש בהגנה הרב שכבתית שבע שכבות. "בשכבה הראשונה נמצא הפירודול, שיוצר סגמנטציה ברשת, לא רק של כתובות IP, אבל