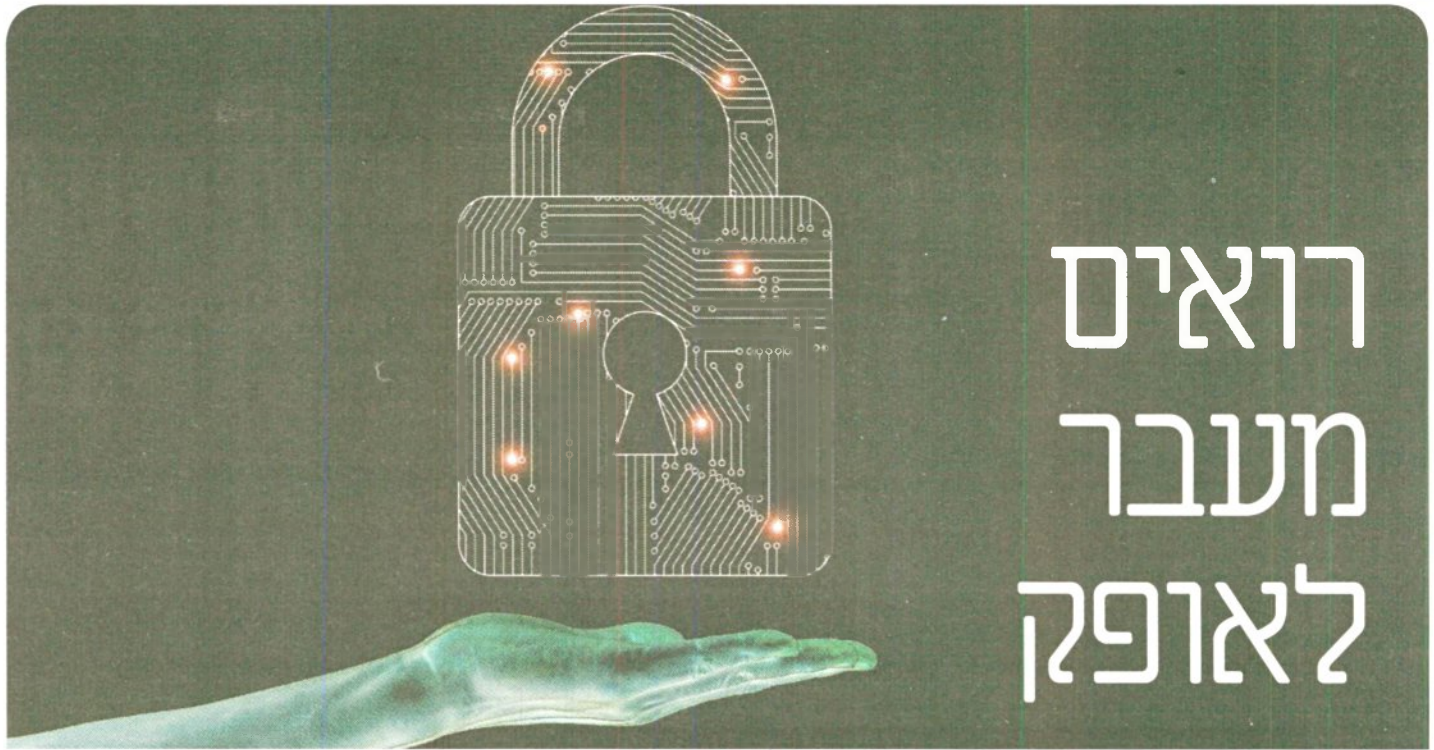


26.27x32.95	1	11	עמוד	11	סייבר - הארץ	28/01/2019	66981641-1
545568 - חברת CyberProof חברת UST Global							

ניהול סיכוני סייבר



יובל וולמן | צילום: גיאוי כהן



רואים מעבר לאופק

מה יהיו אתגרי הסייבר המרכזיים בשנה הקרובה? יובל וולמן, נשיא חברת CyberProof המכהן גם כחבר הנהלה ב-UST Global העולמית, משרטט תחזית מקיפה בתחום הסייבר סקטור, המאפשרת לחברות וארגונים להעריך את הסיכונים ולהיערך למשברים עתידיים | יואל צפרי

המניה והמוניטין ועד פגיעה בתזרים המזומנים. יתכנו גם נזקים פיננסיים ארוכי טווח, מדגיש וולמן. דירקטוריונים של ארגונים דורשים כיום תשובות ברורות מהמנהלים להערכת הנזקים ועדיין אין בנמצא מתודולוגיה סדורה ומגובשת, שתספק הערכה מושכלת על הנזקים האפשריים. קיימים אמנם מספר כלים ספציפיים של ניטור רוחבי-פנימי, שמעניקים ציון למימד זה או אחר בחברה (מודיעין, פגיעות) אבל מדובר בכלים ניי-שתיים. לאור זאת, מתקיים מרוץ לפיתוח כלים שיספקו להנהלות תובנות כמותיות ואמירה חדה וכוללת לגבי מידת החוסן של הארגון - אמירה שתבסס על איסוף וניקוז מידע מכל מוצרי האבטחה בחברה.

● המעבר לענן - חברות רבות מעבירות את בסיסי הנתונים שלהן לענן, אך המעבר הוא מסובך ודורש פתרונות אבטחה מתקדמים, הן באתר עצמו (On-premises) והן בענן. האתגר הוא מורכב, שכן לא פעם מדובר בחברות ענק שנוצרו משרשרת של מיזוגים ורכישות וכוללות שכבות רבות של נתונים. מעבר לכך, האבטחה נדרשת להתמודד עם מספר סביבות, ענניות ולא ענניות. ארגונים שונים חשופים גם לרגולציות שונות, שמשפיעות על כמות וסוג המידע שהן יכולות להעביר לענן.

● ההון האנושי - הסביבה הטכנולוגית בה פועלים חברות וארגונים נעשית מורכבת יותר ודיגיטלית יותר. גם ממשק הלקוחות הופך דיגיטלי יותר. כל זה דורש הון אנושי ברמה גבוהה בעידן בו קיים מחסור בכוח אדם טכנולוגי מיומן. חברות ענק מחזיקות חב'רות-בנות לאבטחה, אך לא כולן מסוגלות או יכולות לעשות כן. אפילו חברות בעלות שווי גבוה המעסיקות 20 אלף עובדים מתקשות להקים כוח פנימי וצורכות את הפתרונות בחוץ.

● תמחור - כמות המידע הזורמת לארגון ודורשת אבטחה, גדלה במהירות עד כדי חוסר יכולת הכלה של החברות. נדרשים עוד ועוד מנגנונים, טכנולוגיים ואנושיים, לטפל בכך. קיים חשש שכמות המידע העצומה - הנאספת כיום מכל רחבי הארגון - תייצר

לאמוד את הסיכון, לתעדף את ההשקעה
הצורך לשרטט את מפת האיומים בסייבר הוביל את וולמן, המכהן גם כחבר הנהלה ב-UST Global העולמית, להכנת תחזית מקיפה הכוללת את האתגרים המרכזיים בתחום הסייבר סקטור בשנה הקרובה:

● אמידת הסיכון - מקבלי ההחלטות בדרגים הבכירים בארגון, כולל יו"ר הדירקטוריון, הפנימו היטב בשנים האחרונות את הסיכונים הכרוכים במתקפות סייבר, אך מתקשים למדוד אותם ולהעריך את מידת הנזק שיגרמו. לעניין זה חשיבות רבה בהערכת הסיכונים הכוללת של הארגון, נושא שתובע יותר ויותר את תשומת לב הבכירים גם מתוקף הרגולציה וחובות הדיווח של חברות ציבוריות. ככל שהשנים נוקפות ומתקפות הסייבר מתגברות ומשתכללות, כך עולה הצורך להבין לעומק מהי ההשפעה שלהן ומהי מידת הסיכון שלהן לארגון. הניסיון מלמד כי למתקפות סייבר יכולה להיות השפעה רוחבית משמעותית - מהשבתה כוללת דרך פגיעה בערך

מרומי הקומה ה-41 במגדלי עזריאל אפשר לראות ביום בהיר לא רק את קו הרקיע האורבני של תל-אביב, אלא גם את קו האופק. במערב הים ובמזרח את רכסי השומרון. עבור יובל וולמן, נשיא חברת CyberProof, אשר מטה הנהלה ומרכז השירותים והפיתוח שלה שוכנים באותה קומה, קו האופק הוא לא רק עניין גיאוגרפי-מטאפורי, אלא גם יעד קונקרטי לחיזוי. זרוע הסייבר העולמית של UST Global, חברה בינ"ל מובילה בתחום הטכנולוגיה הדיגיטלית, CyberProof פועלת כל הזמן לנתח ולהעריך את איומי הסייבר ולספק ללקוחות חברת-האם מענה אבטחה באמצעות שירותי אבטחה מנוהלים. הרקע הביורגרי של וולמן מסייע לו בהערכת איומים. הוא שימש בעבר כקצין ומפקד בחיל מודיעין בצה"ל ואחר כך כמנכ"ל המשרד לענייני מודיעין. גם העובדה שצוות המומחים של CyberProof מתבסס על בוגרי יחידות טכנולוגיות מקהיליית המודיעין מסייעת לחיזוי האיומים.

מעניקים שקיפות והגנת סייבר לחברות הגדולות בעולם

יובל וולמן הוא נשיא CyberProof, זרוע הסייבר הבינלאומית של תאגיד המחשוב והטכנולוגיה האמריקאי UST Global. וולמן כיהן בתפקידים בכירים במגזר הממשלתי, הביטחוני והעסקי. הוא היה מנכ"ל המשרד לענייני מודיעין, יועץ כלכלי לשר האוצר, ולאחר מכן סמנכ"ל פיתוח עסקי ב-IDB. בעבר שירת כקצין ומפקד ביחידת מודיעין בצה"ל.

חברת CyberProof מתמחה במתן שירותים ובפיתוח פתרונות מקיפים לאבטחת סייבר, המבוססים על טכנולוגיות לימוד מכונה ובינה מלאכותית. החברה משנה את כללי המשחק בשוק המתפתח של שירותי אבטחה מנוהלים, בעזרת גישה ייחודית של אבטחת סייבר מבוססת-סיכונים. חברת המחקר Forrester Research אף דירגה לאחרונה את CyberProof כ-Leader בשוק ה-Emerging MSSP's.

CyberProof מעניקה שקיפות וביטחון לחברות המובילות בעולם, כולל לקוחות פורצ'ן 500 וכמה מתאגידי הבנקאות והקמעונאות הגדולים בעולם. מרכז הפיתוח והשירותים של CyberProof ביש"ר אל נמצא במגדלי עזריאל בתל-אביב.

התראות שווא על תקיפות סייבר ולכן היכולת לתעדף מידע הופכת קריטית. ההשקעות בטיפול במידע ובאבטחתו הן רבות ומחייבות ניהול מושכל. ניהול זה חייב להיעשות באופן רבעוני במטרה לבדוק האם החברה השקיעה נכון במוצר או בטכנולוגיה.

● התמודדות עם משברים - היערכות למשברים עתידיים ובלתי צפויים חייבת להיות חלק מארסנל הנשק של חברות כיום. הנחת העבודה היא שחברות יתקפו ללא הרף והשאלה המרכזית היא כיצד יכולה החברה לשמור על רציפות עסקית, למזער את הפגיעה ולהתאושש במהירות. לצורך כך יש לגבש מתודולוגיית תגובה סדורה, שכוללת גם התייחסות למימד הפיננסי, הציבורי והתקשורתי של המשבר, וזאת עבור מגוון תרחישי אפשריים.

איזה מענה אתם מציעים לאתגרים הללו?
"מעבר למתן פתרונות אבטחה, כספק של שירותים מתקדמים מבוססי ראייה עמוקה של מערכות ה-IT של הלקוחות, אני לעיתים יודע עליהם יותר ממה שהם יודעים על עצמם... אני גם נהנה מראייה רוחבית של כלל הלקוחות, שכן אני עובד עם חברות רבות מענפים שונים ויודע להצביע על תובנות שמשותפות לכלל התעשייה. "בכל הקשור לאמידת סיכון יש לנו יכולת להעריך את מיקומו של הלקוח ביחס לשוק, עניין קריטי עבור מנהלים. בתחום הענן אנו שואפים לספק פתרון היברידי, שיאפשר לחברות לתמרן בין סביבות עננים, טכנולוגיות, גיאוגרפיות ורגולציות שונות, תוך סנכרון בין העולמות. העורבדה שאנו מהווים מיקור-חוזק מספקת פתרון יעיל להתמודדות עם המחסור בכוח אדם מיומן. זה מאפשר לחברה לנהל בקלות רבה יותר את משאביה הפנימיים.

"בתחום ההשקעות בסייבר אנו מייצרים ערך מוסף, שמאפשר לחברות לתעדף נכון את ההשקעה ולייצר מודל תמריצים המשרת את מערך הרכש. בתחום החשוב של היערכות צופה-פני-עתידי, אנו מסייעים לארגונים בקיום סימולציות של תקיפות ובייזום תקיפות מבוקרות, לעיתים ללא ידיעת הצוות (אבל בתיאום עם המנהלים), מה שמאפשר לאתר פרצות ולסגור פערי אבטחה."

לאן אתם הולכים מכאן? מה החזון?
"לאחרונה חברת המחקר Forrester Research דירגה אותנו כ-Leader בשוק ה-Emerging MSSP's. בימים אלה אנו נמצאים בתנופת פיתוח וגיבוס עובדים למרכז הפעילות שלנו בישראל ואני מאמין שבשנים הקרובות נמשיך להוביל את תחום שירותי האבטחה המנוהלים, כשאנו מרחיבים את היקף ועומק הפתרונות וחודרים לסקטורים נוספים, בארץ ובעולם."