יפעת מידע תקשורתי דרך מנחם בגין 96-98 (לשעבר דרך פ"ת) תל אביב 67138 טל. 03-5635050 פקס. 03-5617166

66162006-7	29/11/2018	הארץ - סייבר	עמוד 14	1	26.13x32.93
EM חטיבת האבטחה של - RSA - 54442					

הפוזיציה החדשה של מנהל האבטחה

משרדי White-Hat בתל אביב | צילום: עמית הרטמן

בעשור האחרון אנו עדים למהפיכה של ממש בתפקידו ובמעמדו של מנהל אבטחת המידע בארגון, המציבה אותו בעמדת מפתח כשחקן קישור בין ניהול הסיכונים לניהול העסקי של החברה. מה המשמעות של מהפיכה זו ומה צופן העתיד למקצוע?

צופית שחר, CTO **חברת הסייבר** White-Hat

בטחת מידע הייתה עד לפני כעשור בל־בד רק אחד הוורטיקלים בהם טיפל מנהל מערכות המידע. הדגש היה בעיקר על גיבוי מידע קריטי ועל מתן הרשאות גישה למידע מוצפן. בעשור האחרון אנו עדים למהפיכה ממשית בתחום, שקרתה באופן הדרגתי, כאשר עם העלייה באירועי הסייבר, עלתה המודעות ועימה ההכרה בחשיבות הנושא לשרידות העסק. בהתאם, ראינו כיצד התפקיד תופס נפח, מקבל מקום משלו ואפי־לו "זוכה" למיתוג עכשווי, כאשר אבטחת המידע התחלפה בהגנת הסייבר. בד בבד עם ההבנה בא־רגונים שלתפקיד זה נדרשות מיומנויות מוגדרות, זינק הביקוש בשוק לאנשי אבטחת מידע.

איגוד ISACA (Information Systems Audit and Control Association) התריע לאחרונה על צפי למחסור של שני מיליון אנשי מקצוע בתחום הגנת סייבר בשנת 2019. המשרד האמריקאי לסטטיסטיקה בעבודה מעדכן על גידול צפוי של 28% בדרישה לאנליסטים בתחום הגנת הסייבר בלבד, כאשר הגידול הממוצע בדרישה לכלל התפקידים בקושי מגיע ל־7%. לשם השוואה, שיעור האבטלה בשוק האמריקאי היום עומד על 4.1%, לעומת תחום הגנת הסייבר בו שיעור האבטלה הוא 0%.

המועצה לאבטחת החדשנות העסקית (SBIC – Security for Business Innovation Council) שהקימה RSA, מקבוצת דל טכנולוגיות, פרסמה לאחרונה דו"ח המתמקד במהפיכה העוברת על תפקיד מנהל אבטחת המידע. מאמר זה מביא את הממצאים העיקריים של הדו"ח, כפי שפר־סמה RSA, אשר למעשה מציב את מנהל הגנת הסייבר העכשווי, בעמדת מפתח כשחקן קישור בין ניהול הסיכונים לניהול העסקי של החברה.

לתמוך בליבה העסקית של הארגון

הגנת סייבר מהווה כיום אחד התחומים בעלי קצב הגידול הגבוה ביותר בארגון ותחומי האח־ריות של מנהל התחום משתנים בהתאם לגודל ובשלות החברה. דו"ח ISACA בשנת 2016 הראה,

צופית שחר | צילום: הדר שחר

כי ל־50% מהארגונים היה מנהל אבטחת מידע ובשנת 2017 השיעור עלה ל- 65%. למרות נחי־צותו של התפקיד, לא רבים מעוניינים בו בגלל הסביבה הטכנית המורכבת, השינויים ברגולציה וכמובן תשומת הלב המתמקדת בו כאשר קורה אירוע סייבר. על־פי דוח RSA, חברי מועצת SBIC, המייצגים אלף ארגונים ברחבי העולם, דווקא מערערים על הערכות אלה וטוענים שמנהלי אבטחת המידע נהנים מאתגרים טכניים, מע־בודה לא שגרתית שבה "אין יום הדומה לשני", ומהשפעתם הגוברת בארגון.

למרות שהפונקציה בקושי הייתה קיימת לפני 20 שנה, תפקיד מנהל אבטחת מידע הת־פתח במהירות ועבר מאבולוציה לרבולוציה. אם פעם מנהל אבטחת המידע ישב במרתף, או בחדר אחורי כלשהו בחברה, מנהל אבטחת המי־דע הנוכחי יושב בקומת ההנהלה ומוזמן לפגישות הנהלה עסקיות ולפגישות בנוכחות הדירקטוריון והמנכ"ל. ברור שהדבר דורש מגוון רחב של יכו־לות, כגון כישורי מנהיגות טכנולוגית ועסקית על מנת להישאר רלוונטיים.

הכישורים הנדרשים ממנהל אבטחת המידע כיום, כמעט זהים לאלה של מנהלים בכירים וכו־ללים כישורי תקשורת מצויינים, שיתוף פעולה, יכולת חשיבה ביקורתית וכן יכולת לנהל סיכונים. הם צריכים להכיר לעומק את תחום עיסוקם המ־קצועי, אך גם מעבר לכך על מנת שיוכלו לתמוך בליבה העסקית של הארגון.

ראייה אסטרטגית וניהול סיכונים

ממצא מעניין בדו"ח הינו כי מנהלי אבטחה נדרשים לפעול להסרת חסמים ארגוניים, אשר עומדים בדרך לאינטגרציה של האבטחה בחב־רה. הם זקוקים ליכולת שכנוע כדי לגרום ליחידה העסקית להבין ולהטמיע את הקשר ההדוק בין סיכון סייבר לסיכון עסקי. כלומר, הציפיות ליכו־לת מנהיגות גדלות, כאשר מנהל אבטחת המידע צריך להיות מסוגל לעבוד עם כל השכבות והרב־דים של הארגון על מנת ליצור תחושה של דחי־פות ולזכות בשיתוף פעולה מלא.

אחד השינויים הגדולים שמנהלי אבטחת המידע נדרשים להוביל, על־פי SBIC ו- RSA, הוא המעבר שלהם עצמם מתפקיד של "כופים" (enforcer) ל"מאפשרים" (enabler). זה לא עובד יותר לומר "לא" ליוזמה עסקית, אשר נועדה לה־גדיל הכנסות, בגלל צפי לסיכוני אבטחה. מנהלי אבטחת המידע נדרשים לראייה אסטרטגית של המטרה העסקית דרך עדשת הגנת הסייבר. בע־זרת מסגרות טכנולוגיות המחברות תהליכי אב־טחה ודאטה עם ניהול סיכונים, מנהל אבטחת המידע צריך גם להתייחס לקשר שבין פעילות עסקית לסיכוני IT.

היבט נוסף שמרחיב את מוטת האחריות של מנהל הגנת הסייבר, נובע מהעובדה שלגורמים הפנים-ארגוניים בהם הוא מטפל, מתווספים גו־רמים חיצוניים, כמו צרכנים וספקים מעבר לגבו־לות הארגון. אם נוסיף לכך את התקני המובייל, הענן והאינטרנט של הדברים, שנכנסים לכל אר־גון מתקדם, ברור כי נושא ניהול הסיכונים הופך לדאגה רב-תחומית והשאלה המופנית כיום למ־נהל אבטחת המידע היא: מה האיום הבא וכיצד ניתן להיערך אליו?

להכשיר את הדור הבא

אין ספק, כי תפקיד מנהל הגנת הסייבר, ימ־שיך לגדול ולהתפתח בזמן שחברות מתמודדות עם איומים חיצוניים חדשים והרסניים יותר. חב־רי SBIC מעלים בהקשר זה המלצה חכמה ונכונה למנהלי האבטחה של היום - לזהות ולהכשיר את הדור הבא של מנהיגי הגנת הסייבר. לדבריהם, חיוני להתחיל בהקמת תוכניות רשמיות ופחות רשמיות, במטרה לאפשר למומחי אבטחה לה־תנהל בתבניות הייחודיות של חברתם ולתמוך בתוכנית המשכיות מוצלחת. מדובר בעצה שנכו־נה לכל ארגון באשר הוא ולכל מדינה באשר היא וישראל אינה שונה בהיבט זה.

תפקיד חדש - מנהל תחום אבטחת מידע עסקי

בזכות מערך כישורים רחב יותר והשפעה הולכת וגדלה על עתיד העיסוק שלהם, למנהלי אבטחת המידע יש מגוון רב של אפשרויות קריירה. אולם, האינטגרציה של אבטחה, טכנולוגיה ועסקים תוביל ככל הנראה להופעה של תפקידים חדשים. אחד התפקידים המדוברים לאחרונה שהופיע לצד ה-CISO, ומדווח ישירות אליו או באופן מטריציוני, הינו ה-BISO (Business Information Security Officer) - מנהל תחום אבטחת מידע עסקי. ניתן לראות מינויים כאלה בחברות פיננסיות וקמעונאיות גדולות בארה"ב, ומטרתם לעזור ליחידות העסקיות לשפר את הבשלות בתהליכים ובמודלים העסקיים, בראייה של סיכוני אבטחת מידע. אין ספק כי הדור הבא של מנהל אבטחת המידע, נדרש להתחמש במגוון רחב של כישורים, דומים מאוד לאלה של מנכ"לים. מדובר אמנם באתגר משמעותי עבורם, אולם בהחלט בר השגה.