

## ממ"ר"ם הקים ענף חדש שיתמקד בסייבר

הענף עוסק בהבנה, ייצור תפיסות מבצעיות וזמינות מבצעית לגבי עולם הסייבר - חשף מפקד ממ"ר"ם, אלוף משנה חנן א', בכנס DRP לאומי ♦ "סייבר זה אירוע אחר לגמרי, אשר מתנהג אחרת לגמרי. המטרה שלנו היא לשמר תהליכים מבצעיים של צה"ל - בחירום ובשגרה", אמר מפקד ממ"ר"ם

מבוססי מידע, חשיבות המידע והשקלול שבין שניהם. עלי לבחון מהו חלון הזמן שהמשתמש יכול לפעול בלא לסבול בלי זמינות המערכות או בלי המידע. מכאן עלינו להגדיר את הארכיטקטורה הנדרשת, תוך מתן מענה לכל אחת מהתשובות השונות."

הרציונל לתמונת מצב אחודה, אמר מפקד ממ"ר"ם, "נובע מהקשר בין שכבות המיחשוב השונות ושינוע המידע בין השכבות: תשתיות רשת ותמסורת, תשתיות מיחשוב, יישומים, תהליכים מבצעיים, ומאמצי לחימה בעולם הפיסי".

אל"מ חנן סיכם באומרו, כי "השקענו המון מאמץ בתחום. אנו נעזרים בתעשייה ובגורמים שונים על מנת להבין לאן ללכת אנו ניצבים בפני אירוע גדול, של העתקת המתקנים דרומה, לנגב. אנו משקיעים המון מחשבה איך לעשות זאת נכון, ומעריכים את כספו של משלם המסים, על מנת שהמעבר ייתן זמינות גבוהה יותר של המערכות".

**יוסי הטוני**



לכן, זו סוגיה בעייתית - להבין מה גודל הסיכון ומה פוטנציאל הנזק". במקביל, אמר מפקד ממ"ר"ם, "עלינו לבחון מה קורה בשגרה. עלינו לחשוב על ההבדלים במענה - כי אנו לא יכולים לענות על הכל. יש לראות מה קורה: מה גורם הרבה נזק, להבין את חשיבות המידע ועל קריטיות השירות. יש אזורים של מידע קריטי, אבל לא נורא אם הוא לא יהיה זמין כמה שעות. יש לשקלל בין זמינות המידע והשירותים

ענף חדש שקם בימים אלה ממ"ר"ם עוסק בהבנה, ייצור תפיסות מבצעיות וזמינות מבצעית לגבי עולם הסייבר - כך חשף מפקד ממ"ר"ם, אלוף משנה חנן א', בכנס.

"סייבר זה אירוע אחר לגמרי, אשר מתנהג אחרת לגמרי", אמר מפקד ממ"ר"ם. "המטרה שלנו היא לשמר תהליכים מבצעיים של צה"ל - בחירום ובשגרה". הוא ציין מהם האתגרים בעת אירוע אותו כינה "שבר": "שמירה על פעילויות העסק, תוך ניהול סיכונים כולל ויעיל; שמירה על שרשרת אספקה רציפה ופתוחה לשותפים ולקוחות; מניעת השלכות כלכליות כתוצאה מההפרעה לעסק; הימנעות מאיבוד זמן בגישה למקורות מידע קריטי".

בעת תכנון פתרון רציפות והמשכיות עסקית והתאוששות מאסון, אמר אל"מ חנן, "עלי לשקלל בין אירועים שהשכיחות שלהם לא גבוהה, אבל מבחינה סטטיסטית יכולים לקרות במשמרת שלי, לבין אירועים בעלי שכיחות נמוכה עם פוטנציאל גבוה לנזק.

שירותים קריטיים בהם, ואפילו מדינות".

### לצפות את הבלתי צפוי

לדברי מנכ"ל SECOZ, "על מנהלי אבטחת המידע בעידן הסייבר לצפות את הבלתי צפוי: מתקפות ממוקדות, 'מוענות' ארגון, כאלה שלא ניתן לזהותן בכלים הסטנדרטיים. טכנולוגיות מבוססות חתימה אינן מספיקות. יש צורך בכלים טכנולוגיים מבוססי זיהוי, כלים המזהים מגמות, מבינים את ההקשר ומספקים התרעה ממוקדת".

"מנהלי אבטחת המידע צריכים למלא את תפקידם תוך הבנה לרוחב ולעומק", הוסיף. לדבריו, "תפקיד מנהל האבטחה התמקד תחילה בעולם הטכנולוגי ובחלוף השנים הוא התחבר להיבטים העסקיים בארגון, למשל בהיבט ניהול הסיכונים. הופעת הסייבר מצריכה שוב העמקה טכנולוגית, לצד זו העסקית, למשל, לטובת עמידה ברגולציות".

זילביגר סיכם באומרו, כי "עמידה בפני מתקפות סייבר הופכת להיות קריטית וחיונית עבור מנהלי אבטחת המידע והארגונים שלהם. גודל הנזק ייקבע על פי היכולת, המקצועיות וההיערכות המוקדמת של צוות התגובות. זה יצטרך להכיל את הפגיעה ולצמצם את הנזקים וההשפעות שלה. יהיה עליו לנהל את איומי הסייבר, כחלק מניהול הסיכונים התפעוליים. עליו לוודא שהנהלת הארגון מבינה את הסיכון ומתעדפת ומתקצבת אותו. הוא צריך לבנות תוכנית עבודה ישימה, עם הקצאת משאבים וצוות".

### "לא כל גוף צריך BCP"

"על המדינה לסווג את הגופים העסקיים השונים שבתחומה ולהגדיר 'תקינה', משמע - מהן הדרישות העקרוניות שצריך כל גוף שכזה. בסופו של

### "בימים אלה, לאחר

הופעת איומי הסייבר,

על מנהלי אבטחת מידע

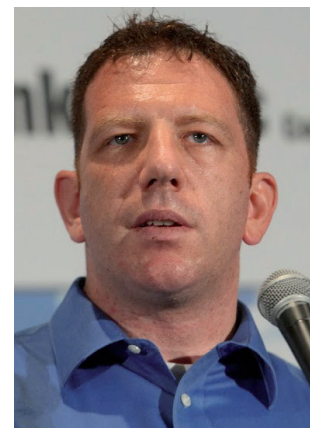
להיות ערוכים בשני

כיוונים - פנים וחוץ?

של אבטחת המידע, שמתאפיינת ביותר מורכבות טכנולוגית, יותר יצירתיות, יותר כיסוי מערכתי ויותר מוטיבציה ורלוונטיות.

הוא הביא כמה דוגמאות לנזקים פוטנציאליים העלולים להיגרם כתוצאה ממתקפות סייבר. אחת מהן היא פגיעה קריטית בהיבטים העסקיים והכספיים בארגון, בשל גניבת מידע שנבעה מניצול הפגיעות של פרוטוקול מערכת בקרת הגישה הארגונית. דוגמה נוספת אותה הוא הביא היא מתקפת סייבר על מערכת SCADA, המבקרת את פעילות סכר או סכרים - דבר שיביא להצפת הסכר, פגיעה במי השתייה של תושבי האזור, הפסקות חשמל ועוד.

על פי זילביגר, "נדרש להבין את העוצמה הגלומה במתקפות קיברנטיות: אלה מתקפות ממוקדות, מופעלות לזמן קצר, שבמאמץ קטן יחסית יכולות לגרום לנזק רב - נזק שעלול להשביט ארגונים, או



אופיר זילביגר