

להיות ערות לשינויים שבין עולמות אבטחת המידע והסייבר ולוודא שבנוסף למענה מיטבי עבור אבטחת המידע המסורתית, הוא ערוך עם כלי הגנה גם לתחום הסייבר."

**"ליותר ממחצית הארגונים שמטמיעים רכיבים ניידים אין מדיניות ניהול ואבטחה לתחום"**

"מחקרים מצביעים שהרוב המכריע של הארגונים הטמיעו או יטמיעו במערכת ה-IT רכיבים ניידים - טאבלטים או טלפונים חכמים - השנה, אלא שהם לא עשו פעילות משלימה: ליותר ממחצית מהם אין מדיניות ניהול ואבטחה לעולם הנייד", כך אמר **איאן אוונס**, מנהל המכירות הראשי של איירווטש לאזור EMEA (אירופה, המזרח התיכון ואפריקה).

בדבריו ציין אוונס שאירווטש, שמוצגת בישראל על ידי מוביסק, פועלת בעולם ניהול המכשירים הניידים, MDM (Mobile Device Management) ואבטחתם.

לדבריו, "יש למנמ"רים מספר מצוקות שרלוונטיות לעולם הנייד: ריבוי של מכשירים ניידים, מהארגון ומהבית, פריצות למכשירים - מגמה שמצויה בעלייה, החיבור לרשת של מגוון המכשירים מאפשר פוטנציאל לאובדן מידע ואין שליטה מה קורה למידע בעת שהוא נשלח מנייד אחד למשנהו. בסופו של דבר, למנמ"ר או למנהל התקשורת תחתיו אין מושג מה קורה למידע הארגוני בעולם הנייד."

**"ניהול חכם, פשוט ומאובטח של הניידים"**

הוא ציין נתון מחקרי, שלפיו "יותר משלושה רבעים מהארגונים ברחבי העולם (78%) מאפשרים גישה לסביבת העסקים ממכשירים ניידים שמצויים בבעלות העובדים. מצב זה דורש ניהול חכם, פשוט ומאובטח של רכיבים אלה."

"על מנהל אבטחת המידע הארגוני ליישם מדיניות אבטחת מידע בכל השכבות, לרבות שכבת הפעילות ב-IT הנייד, לממש ולאכוף אותה, תוך הגנה על המידע הארגוני לכל תווך ומקום אליו הוא משוען", אמר אוונס. "יש למנוע DLP - זליגת ודליפת מידע, ולצד זה נדרש להגן על פרטיות המשתמשים. כמו כן, צריך לוודא שהגישה לרשת הארגונית מהמכשירים הניידים נעשית תוך בקרה ורק על ידי מורשים. יש לקבוע מדיניות למקרים של אובדן רכיבים ולעשות בקרת נזקים אם זה כבר קרה. נדרש גם לתמוך בצידוד חדש ולא ידוע."

אוונס אמר שהצורך בפיתרון מקיף לניהול הניידות בארגון עלה גם בישראל. הוא ציין שיש למוביסק 70 לקוחות ארגוניים מכלל המגזרים בישראל, ביניהם בנקאות, ביטוח, תשתיות, תקשורת, שרשרת אספקה, תעשייה, אקדמיה, שירותים ורכב. הוא הוסיף ש-"בכוונתנו להכפיל השנה את טביעת האצבע שלנו בישראל". "מתוך 20 המדינות החשובות שבתחום אחריותי, ישראל מדורגת במקום השלישי ביחס המכירות של מוצרנו לגודל האוכלוסייה ולכמות הארגונים", ציין. "ישראל היא מאמצת מוקדמת של טכנולוגיה ובעלת נוכחות טכנולוגית גבוהה. אנחנו דוחפים כאן חזק פתרונות של ניהול רכיבים בעולם



גלעד מיניקס



אופיר זילביגר



איאן אוונס

**איאן אוונס: "יותר משלושה רבעים מהארגונים ברחבי העולם (78%) מאפשרים גישה לסביבת העסקים ממכשירים ניידים שמצויים בבעלות העובדים. מצב זה דורש ניהול חכם, פשוט ומאובטח של רכיבים אלה"**

חלה עלייה בכמות הרגולציות וגדלה התחרותיות. לאור זאת, על מנת לשמור על רווחיות, קיימת בקרה צמודה והדוקה אחר תקציבים, ובכלל זה גם אחר תקציב ה-IT, כך אמר **גלעד מיניקס**, מנהל ת"פ (תכנון וניהול פרויקטים) ומנמ"ר גלובל פקטורניג בישראל. לדבריו, "בישראל הודקה הבקרה על התקציבים, בשל הצורך בהתייעלות תפעולית. הדרך היחידה שלנו לממש מטרה זו היא על ידי תעדוף של פרויקטי IT, וזה מה שאנחנו עושים."

מיניקס אמר, כי במסגרת הפעילויות המיחשוביות אותן הוא והחברה בה הוא עובד מקדמים נמצאים כניסה עמוקה יותר ויותר לעולם הסלולר ופרויקטי דיגיטליזציה. "בדרך זו אנחנו מנסים לחסוך בעלויות ובמשאבים ולהביא ליעול תהליכים", אמר. לדבריו, דרך נוספת לחיסכון בעלויות המיחשוב תהיה צמצום פלטפורמות ה-IT הקיימות והאחדתן, כמו גם בניית הסכמי תחזוקה, תפעול ורמות שירות מול הספקיות, שייעשו לתקופה של כמה שנים.

**"אירועי אבטחה וסייבר שבעבר נחשבו מדע בדיוני - הם מציאות כיום"**

"ריבוי המתקפות ועוצמתן, כמו גם המורכבות הטכנולוגית שלהן, יצרו מצב שבו אירועי אבטחת מידע ומתקפות סייבר שהיו בעבר בבחינת מדע בדיוני הפכו למציאות", כך אמר **אופיר זילביגר**, מנכ"ל SECOZ. זילביגר דיבר בפתח המפגש שנערך בפראג. לדברי זילביגר, "מי היה חושב בעבר על אירוע מורכב, שמשלב את מערכות ה-IT ומערכות האבטחה של RSA, EMC ולוקהי-מרטין, כדי לגנוב מסמכים של מטוסי קרב עתידיים? כיום, הנחת העבודה היא שאירועים כאלה רלוונטיים לכלל הארגונים, לאור מגוון האירועים והמנעד שלהם."

"מצב חדש זה מביא לכך שארגונים נדרשים לבנות את מעטפת אבטחת המידע שלהם עם כמה שכבות: בניית והכשרת צוות תגובה, ניטור מהיר של זליגת מידע ומניעת המשך הזליגה, ניהול זהויות ו-IDM - כל מרחב בקרות אבטחת המידע ובתוספת להן בקרות סייבר ייעודיות", ציין זילביגר. "הפתרונות הקלסיים מקבלים פתאום משמעות אחרת. למשל, בעבר לא היו בארגונים צוותי תגובה וכיום ארגונים מעסיקים צוותי תגובה שכאלה - אם בתוך הבית ואם כשירות חיצוני על ידי מומחים."

הוא עמד על ההבדלים בין תחום אבטחת המידע לתחום הסייבר ואמר ש-"אף על פי הם מעטים, הפתרונות הנדרשים עדיין שונים. אם לעולם אבטחת המידע, למשל, יש משהו הייחודי לו, דוגמת גריסת מסמכים, הרי שעולם הסייבר דורש פתרונות רחבים יותר, לדוגמה הגנה על מערכות SCADA או איסוף מודיעין סייבר על התוקפים וסוגי המתקפות העתידיות". זילביגר ציין, כי בהתאם, "השנה אנחנו רואים ארגונים עורכים תרגילי היערכות לסייבר. אלה בתרגילים מורכבים, שכוללים הדמיה של מתקפות ממושכות וממוקדות (APT), חזירה רב ממדיית לארגון, התקפות משובכות. התרגילים מתבצעים בהיקפים גדולים וזו דוגמה לכך שאנחנו מצויים בפתחו של עידן חדש". בסיכום דבריו אמר, כי "המתקפות שינו את האופן בו ארגונים מגנים על עצמם. הנהלות הארגונים נדרשות