

# העולם הנייד מאיים על מערכי האבטחה בארגונים

"מגמת ה-BYOD דורשת מארגונים לעבור לשלב הבא באבטחה. 75% מהארגונים צופים גידול במספר המכשירים שיהיו בבעלות עובדיהם ו-41% מהארגונים מציינים, כי מרבית הטלפונים החכמים המתחברים לרשת הארגונית נמצאים בבעלות פרטית של העובד", התריע אלי פרנס - מנהל פעילות אזורי בפורטינט, בכנס הלקוחות השנתי שערך הסניף המקומי של החברה

יוסי הטוני < צילום: ניב קנטור

## להשיב על שאלות רבות

כל מנהל תשתיות ומנהל אבטחת מידע בארגון, אמר פרנס, "צריך לשאול את עצמו: מי אתה, לאן אתה רוצה לפנות ואיזה מידע אתה צריך? איך תוכל לאפשר לעובד לעבוד מכל מקום, לדעת מה הוא עושה ולתמוך בטלפונים שהוא מביא מהבית? האם העובד נמצא ברשת ה-LAN או ה-WAN?" הוא ציין, כי פורטינט יודעת לתת מענה לשאלות אלה על ידי יצירת הזדהות קשיחה למכשירים והוסיף, כי כל נושא ניהול המכשירים הניידים בארגון (MDM) לא טומן בחובו היבטי אבטחת מידע.

לדבריו, ככל שיש יותר מכשירים מתחברים הדורשים הזדהות, כך נדרש להגדיל את רמת היתירות והשרידות של הרשת - ויש לעשות זאת בלא להוריד את רמת אבטחת המידע. היבט נוסף, ציין פרנס, הוא לברר איזה מידע נשאב מתוך הארגון, האם הוא מאובטח ולאן הוא הולך. "נדרשת שליטה על תעבורת המידע ויש לנהל את כל התראות אבטחת המידע, על מנת לבדוק מי מהן חשובות ויש להיערך לקראתן". הוא הוסיף, כי "נדרש לתת חיווי חכם. הרשת הופכת להיות חכמה יותר והאיומים נהיים קשים ומומקדים מבעבר. אנו נותנים ציון לכל מכשיר בהיבט האבטחה שלו ובהמשך דואגים לאכוף מדיניות

חכמה על המכשיר. iPhone, למשל, רק עם דפדפן מסוים. ניתן להקשיח מכשירים בצורות שונות, על בסיס חוקים ספציפיים. כדי למנוע זליגות מידע, אני רוצה שהמשתמש יוכל לגשת רק ליישומים שנקבעים מראש.

המדיניות הממומשת צריכה להיות מבוססת מכשירים". "האיום האלחוטי הוא מאוד מורכב", קבע מנהל הפעילות האזורי בפורטינט. "עלינו להתמודד מול איומים פנימיים, כמו גם אלה החיצוניים - כמו האקרים, למשל. יש לפורטינט מענה מלא למגמת ה-BYOD, תוך קבלת שליטה מלאה בדואר האלקטרוני, אכיפת מדיניות, מניעת דליפת מידע, בקרת גישה על המשתמשים, סינון URL, מניעת פישוג וספאם ומניעת מתקפות זדוניות".

הסניף הישראלי של פורטינט, סיכם פרנס, החל לפעול בשנת 2005, "יש לנו עשרת אלפים התקנים בקרב מאות לקוחות ארגוניים. זכינו בפרויקטים במגזרי הפיננסים והביטחון. על אף המשבר, גם 2012 תהיה שנה מוצלחת עבורנו".

מגמת ה-BYOD (Bring Your Own Device), הבא את מכשירך הפרטי מהבית' הולכת ומתרחבת בכלל מגזרי התעשייה, והיא טומנת בחובה אתגרי אבטחה רבים. ארגונים נדרשים להיערך לקראת המגמה ולעבור לשלב הבא באבטחה, הכולל ניהול איומים אחוד", כך אמר **אלי פרנס**, מנהל פעילות אזורי בפורטינט. פרנס פתח את כנס הלקוחות השנתי של הסניף הישראלי של החברה. לכנס, שנערך בהפקת אנשים ומחשבים באולם East שבתל אביב, הגיעו מאות מלקוחות החברה ושותפיה העסקיים.



אלי פרנס

אלי פרנס: "ככל שיש יותר מכשירים מתחברים הדורשים הזדהות, כך נדרש להגדיל את רמת היתירות והשרידות של הרשת - ויש לעשות זאת בלא להוריד את רמת אבטחת המידע"

לדברי פרנס, בעוד שבשנה החולפת

פעלו בעולם כ-5 מיליארד מכשירים מקושרים, הרי שחברות המחקר צופות, כי בשנת 2016 כמות המכשירים תעמוד על 14 מיליארד. חלק ניכר מהם, אמר, צפויים להגיע לסביבות העבודה הארגוניות. "כבר כיום, 62% מהארגונים משלמים עבור המכשירים הסלולריים של עובדיהם ועבור השימוש בהם. 75% מהארגונים צופים גידול במספר המכשירים שיהיו בבעלות עובדיהם ו-41% מהארגונים מציינים, כי נכון להיום מרבית הטלפונים החכמים אשר מתחברים לרשת הארגונית נמצאים בבעלות פרטית של העובד".

בשל הצפי לגידול במגמת BYOD, הסביר פרנס, גדלים גם הסיכונים ואיומי אבטחת המידע. כך, ציין, כי "70% מבעלי הטלפונים החכמים עושים שימוש במכשיר האישי שלהם על מנת לגשת למידע ארגוני, אבל 80% מהמכשירים כלל לא מנוהלים על ידי מחלקות ה-IT, ובכך הם חושפים את הארגונים בפני סיכונים לאובדן מידע וזליגתו בלא אמצעי הגנה ואבטחה סבירים".