

מה שהיה לא יהיה (באבטחה)

הנק ון דר היידן, CA: "אי אפשר לאבטח כל שכבות המיחשוב; נדרש לשנות את התפיסה ולטפל בליבה" ♦ "מה שהיה לא יהיה - ומנהלי אבטחת מידע בארגונים נדרשים להבין את זה", אמר ון דר היידן, סגן נשיא CA לאזור EMEA לתחום אבטחת המידע ♦ לדבריו, "פעם הכול היה פשוט מאוד, אולם לא זה המצב כיום: העולם מתפוצץ מעודף נתונים ומידע, הקישוריות והחיבוריות חובקות כל מכשיר נייד, ואנחנו בתחילת עידן 'האינטרנט של הדברים'. מצב זה לא מאפשר לאבטח כל רכיב ורכיב, כבעבר", ציין

יוסי הטוני

בין השאר, את ארקוט, שהטכנולוגיה שלה מספקת אבטחה בענן ודואגת לכך שתעבורת התקשורת תהיה מאובטחת לכל אורך הדרך שהיא עוברת, בין אם בענן ובין אם מחוצה לו. ארקוט אחראית לאבטחת המידע בעשרות רבות של גופי בנקאות גדולים בעולם.

מנהלי אבטחת מידע בארגונים נדרשים להבין שמה שהיה לא יהיה. כבעבר ניתן היה לאבטח הכול, כיום לא. לכן, נדרש להתמקד ולטפל בליבה - ניהול ובקרת גישה לזהויות ואבטחת הנתונים והמידע, כך אמר **הנק ון דר היידן**, סגן נשיא CA לאזור EMEA (אירופה, המזרח התיכון ואפריקה) לתחום אבטחת המידע.

"יש לנו מתחרות בשלוש שכבות: ההגנה על המידע, ניהול הזהויות ובקרת הגישה, ושכבה שממזגת ביניהן. בתחום ההגנה על המידע, המתחרות העיקריות שלנו הן סימנטק, מק'אפי וובסנס. בעולם ניהול הזהויות ובאיחוד שתי השכבות המתחרות העיקריות שלנו הן אורקל ויבמ."



הנק ון דר היידן

"כלי CA IdentityMinder מטפל בבקרת גישה למערכות וז' ליישומים במערכות הארגוניות הטמעות מביאה לשיפור היעילות התפעולית ולהפחתת הסיכון הביטחוני הכרוך בהכנסת משתמשים חדשים למערכות ה-IT השונות שבארגון. השימוש בכלי גורם לכך שארגונים מקבלים גישה מאוחדת לניהול הזהויות של המשתמשים לאורך כל מחזור החיים שלהם, והפלטפורמה מספקת בקרת גישה בזמן היאות וליישומים ולנתונים שמותר להם להגיע אליהם. הפלטפורמה מאפשרת למכן את תהליך הוספת והורדת המשתמשים, תוך מענה לנהלי אבטחת מידע ובקרת זהויות".

מי המתחרות שלכם?

"יש לנו מתחרות בשלוש שכבות: ההגנה על המידע, ניהול הזהויות ובקרת הגישה, ושכבה שממזגת ביניהן. בתחום ההגנה על המידע, המתחרות העיקריות שלנו הן סימנטק, מק'אפי וובסנס. בעולם ניהול הזהויות ובאיחוד שתי השכבות המתחרות העיקריות שלנו הן אורקל ויבמ. היתרון שלנו מול המתחרות הוא בכך שאנחנו החברה היחידה שמצויה בשלוש השכבות".

לסיום, התייחס ון דר היידן לשוק הישראלי. לדבריו, "זה שוק חשוב עבורנו. ישראל היא מדינה מרובת חברות מוטות טכנולוגיה וככזו - היא עבורנו מקום לפעילות עסקית. בנוסף, השוק הישראלי הוא מאמץ מוקדם של טכנולוגיה". הוא ציין, כי CA רכשה בארץ כמה סטארט-אפים, בהם אובליקור ויריקופאי.

הוא ציין בראיון לאנשים ומחשבים, כי "פעם הכול היה פשוט מאוד. היה מיינפריים, הייתה קונסולה אחת, והסיכון הגדול ביותר היה שמישהו בטעות יכבה את המחשב מבלי שישים לב. לא זה המצב כיום: העולם מתפוצץ מעודף נתונים ומידע, הקישוריות והחיבוריות חובקות כל מכשיר נייד, ואנחנו בתחילת עידן 'האינטרנט של הדברים'. מצב זה לא מאפשר לאבטח כל רכיב ורכיב, כבעבר".

מה נדרש לעשות?

"מנהלי אבטחת מידע נדרשים 'לשנות דיסק', להחליף את התפיסה בה הם אוחזים לגבי האופן בו מערכי אבטחת המידע נדרשים לפעול. יש לעבור מתפיסת אבטחת מידע כוללת, של אבטחה מהתשתיות אל היישומים, לאבטחת מידע ממוקדת בליבת הפעילות הארגונית. המיקוד יתבסס על שני שדות פעולה עיקריים, בהיותם קריטיים להשגת מירב האבטחה: ניהול ובקרת הגישה לזהויות, והגנה על הנתונים והמידע. כך ניתן לגשר על הפער בין הצורך באבטחה כוללת, שכאמור, היא בלתי אפשרית, להשגת מרב האבטחה במגבלות כוח אדם ותקציבים".

כיצד זה מבוצע הלכה למעשה?

"ארגונים בכלל ומנהלי אבטחת מידע בפרט נדרשים להבין שכאשר העובדים פועלים בעולם העסקי, מול שותפים, ספקים ולקוחות, עליהם להיות בטוחים בזהות של מי שמולם. כך הם יכולים לנהל את הסיכונים באופן המטבי, תוך צמצומם משמעותית. "נדרש להשיג את מרב המידע על כל משתמש, פנימי או חיצוני, שמנסה לעשות משהו עם הנתונים או ביישומים. יש לנהל את הקונטקסט של המשתמש: לאיפה מותר לו לגשת, מאיזה רכיב מיחשוב, לקבוע כללים לפעילות שלו ברשת הארגונית כשהוא בעבודה וכללים שונים, מחמירים יותר, כשהוא גולש ברשת הארגונית מאינטרנט קפה בטלפון החכם שלו. "איסוף הנתונים על אודות המשתמש והתנהגותו מביא לידי ניהול סיכונים יעיל יותר ומשפר את קבלת החלטות בתחום".

מה לגבי אבטחה בענן?

"לאבטחה יש גם היבטים חשובים בעת הגירה למיחשוב ענן. רכשנו,