



מייק דנינג

כיום רוצים לראות אימוץ נרחב של יותר פתרונות אימות בעלי גורמים כפולים, וזהו תחום שצומח מאוד עבורנו. שם משתמש וסיסמה אינם מספיקים כיום, אולם הצורך בפתרונות מורכבים יותר לא יכול להאט את האימוץ של פתרונות חדשים.

שירותי אבטחה חדשים

הוא סיפר על שני שירותי אבטחה חדשים שהשיקה CA בכנס, לניהול הזהירות והגישה (IAM) בענן. לדברי דנינג, השירותים הללו מייצגים צעד נוסף באסטרטגיה של החברה אשר מבקשת לסייע ללקוחות להשתמש בשירותי ענן ובשירותים מסורתיים, על מנת להגביר את גמישות המיחשוב ולפעול בקצב שהולם את הדרישות העסקיות.

"הפתרונות החדשים, CA IdentityMinder as-a-Service ו-CA FedMinder, מציעים את כל היתרונות של מודל היישום בענן", אמר דנינג, "ובכלל זה גמישות שמאפשרת להרחיב או לצמצם את התמיכה בשירותים לפי הצורך, מחזורי התקנה קצרים יותר וחיסכון בהוצאות, שמתאפשר בזכות העובדה שנדרשת כחות עבודת ניהול".

לדבריו, "במקביל למעבר של סביבות המיחשוב ליישומי ענן ושירותים, לצד יישומים מקומיים מסורתיים, חייבים להעביר גם את הניהול של הזהירות והגישה. סביבת היישומים ההיברידיים מוסיפה עוד רמה של מורכבות ועל אנשי המיחשוב לנהל ולאבטח אותה תוך שמירה על האיזון בין הסיכונים לתועלת. איזון זה חייב להישמר - הן בהתקנה מקומית של פתרונות IAM והן בשירותי IAM שמסופקים בענן".

הוא הסביר, כי השירותים החדשים מציעים מספר יכולות חשובות לשיפור האבטחה והגברת יעילות התפעול. כך, פירט דנינג, "הם משתלבים בשירות CA AuthMinder as-a-Service, שמאפשר ללקוחותינו ליהנות מאימות רב עוצמה של הדהות, בנוסף לאמצעים הסטנדרטיים של שם משתמש וסיסמה. עוד תומכים השירותים בהתאמה אישית של ממשק המשתמש באינטרנט, על מנת לסייע לארגונים לעמוד בדרישות העסק, להקל על ההדרכה ולהגביר את האימוץ מצד משתמשי הקצה".

* הכותב הוא שליח אנשים ומחשבים לארצות הברית

האחראי על קבוצת הפתרונות ללקוחות. "הפער הזה אמנם קיים יותר מ-40 שנה, מאז תחילת עידן ה-IT, אולם אנחנו מאמינים שהוא לא יכול להימשך יותר. הופעתו של מיחשוב הענן מהווה את ההזדמנות הטכנולוגית לשינוי המציאות הזאת".

לדברי דובסון, שבמשך 19 שנים מילא שורה של תפקידי ניהול ביבמ, "הענן הוא קונספט שמדברים עליו 12 שנים לפחות, אולם במהלך 2008 משהו השתנה. כך, בשנים האחרונות אנו עדים לנסיקה של התחום, שהולכת וגדלה מיום ליום. עם זאת, למרות שחרתנו על דגלנו להיות החברה שתוביל את המעבר למיחשוב ענן, אנחנו לא מאמינים שהדרך לעשות זאת היא לשכוח מהקיים ולזנוח את ההשקעות שבוצעו בעבר. יותר מ-20% היצע מלקוחותינו, למשל, עושים שימוש בפתרונות שלנו למיינפריים. לכן, היצע המוצרים החדש שלנו מתמקד בשימור מקסימלי של ההשקעה שביצעתם בתשתיות המיחשוב שלכם, וניצול מרבי של הקיים תוך התבוננות קדימה". "אנו חיים בעולם מבוסס רשת, שבו ה-IT חייב לעבוד במהירות שהעסק מכתוב", אמר דובסון. "זו עובדה קיימת - בדיוק כמו מיחשוב ענן. אולם, ארגונים רבים נותרו עדיין מאחור. אנו, ב-CA, סבורים שהגיע הזמן לעבוד לפי מודל ניהול חדש שיסייע ליצור עולם מונחה שירותים עסקיים, ולא עולם מונחה IT. הטכנולוגיה לא יכולה להכתיב את האופן שבו העסק יפעל, אלא בדיוק להיפך".

הוא הציג את פלטפורמת CA Cloud 360 והסביר, כי מדובר בפתרון חדש שנועד לסייע לארגונים לבדוק יישומים ושירותים עסקיים ולקבוע איזה מביניהם מתאימים בצורה הטובה ביותר לענני מיחשוב פרטיים, ציבוריים או היברידיים - או למודלים מסורתיים של אספקה. הפתרון, אמר דובסון, מציע למנהלי מיחשוב בארגונים תובנות ותחזיות להקמה בפועל של שירותי ענן חדשים תוך שלושה חודשים בלבד. כך, ציין, יכולים הלקוחות לגבש אסטרטגיית ענן מקיפה ובת קיימא שמאפשרת להסב שירותי מיחשוב ברמות צפויות מראש של עלויות, סיכונים ותמורה.

Cloud 360, הוסיף דובסון, מהווה חלק ממפת הדרכים של CA Technologies לחדשנות בתחום השירותים העסקיים והוא עתיד לסייע למחלקות המיחשוב ליצור שירותים עסקיים שמספקים את התוצאות העסקיות הנדרשות ובכלל זה שיפור הגמישות, הביצועים והחדשנות, וצמצום ההוצאות והסיכונים. "פתרון Cloud 360 CA מסייע למנהלי המיחשוב לאמץ מודלים של שירותים היברידיים ולממש אסטרטגיות להעברה של שירותי המיחשוב לענן", אמר דובסון. "כך יכולים מנהלי המיחשוב להפיק את מירב היתרונות מענני המיחשוב, ליהנות מהר יותר משירותים עסקיים גמישים ולספק חדשנות, תמורה עסקית ויתרונות תחרותיים".

אבטחת המידע בענן - קריטית

"אין ספק שאבטחת המידע בענן היא קריטית, אבל היא אינה יכולה לבוא על חשבון חוויית המשתמש", אמר מייק דנינג, מנכ"ל חטיבת האבטחה של CA. "אינך יכול לחלק אסימון (טוקן) חומרה לכל משתמש ולכל לקוח, ולומר להם 'נהנה, אני הולך לשנות לחלוטין את חוויית המשתמש שלכם'. לא לשם התחום הולך. אם תוכל לספק להם אסימון מבוסס תוכנה עם יכולות אימות זהות מוכחות, שיעמוד בסטנדרט האבטחה שהצבת, תוכל ליהנות משני העולמות".

דנינג אמר את הדברים בראיון לאנשים ומחשבים, במסגרת הכנס. דנינג הבהיר שלמרות שהמטרה ברורה, הדרך אינה בהכרח פשוטה. "אבטחת מידע עדיין מהווה חסם בדרך לאימוץ מיחשוב הענן. הסוגיה המרכזית היא שליטה: כשאתה מאחסן נתונים בדיסק-סנטר שלך, אתה יכול להגן עליו במיירוול, אנטי וירוס, אנטי נזקה, אנטי רשעה ואנטי מה-שאתה-רוצה. הכל נמצא קרוב לבית, מתחת לעיניך השומרות - ואתה יכול לבנות מבצר סביב המידע. בענן, לעומת זאת, אתה מאבד שליטה וזו סוגיה מורכבת שמנמ"רים ומנהלי אבטחת מידע רבים מתמודדים איתה".

"אני רואה עניין מתחדש בסוגיות כמו הצפנה וניהול גישה - שני תחומים שאנו מתמחים בהם באופן מסורתי", הוסיף דנינג. "כמו כן, אנשי אבטחה