הענן כאן כדי להישאר, אבל הכל מתחיל ותלוי באבטחתו

מאת: דני לב-רן, מנכ"ל cloudride

על אף שסביבת הענן מביאה עימה יתרונות רבים; מהירות וגמישות, שיתופי פעולה אפקטיביים, חסכון בעלויות, ניידות ואמינות, לא חסרים בה גם אתגרים, כאשר הבולט שבהם הוא אבטחת הענן והוא ישפיע על היכולת וההצלחה שלנו לעבוד בסביבה עננית.

אבטחת ענן מתייחסת למערך רחב של סוגי מדיניות, טכנולוגיות, יישומים ואמצעי בקרה המשמשים להגנה על נתונים, יישומים, שירותים, והארכיטקטורה המשויכת לתשתיות הענן. כאשר חברות מעוניינות להעביר את כלל פעילותן או את חלקה לסביבת הענן, תחום בלתי נמנע בו הן ייתקלו בסופו של דבר, הוא אבטחה: "האם סביבת הענן הופכת את החברה שלנו לחשופה יותר להתקפות סייבר? האם ננקוט באמצעי מניעה וטיפול מול התקפות סייבר אלו? מהי הדרך הטובה ביותר ליישם אמצעי אבטחת ענן עבור הצרכים הארגוניים שלנו?" אלו רק חלק מהשאלות העומדות בפני כל מנהל מערכות מידע, מנהל IT או CTO ככל שהדבר נוגע לארכיטקטורת הענן שלהם.

כיצד סיכוני אבטחה בענן משפיעים על העסק שלך?

כאשר מתרחשת הפרת אבטחה בחברתך, יתכן שנמהר להפנות אצבע מאשימה לעבר האקרים, "פרצו אלינו!". ייתכן שפרצו, אבל גם העובדים שלך ממלאים חלק בהפרת אבטחת הנתונים. גם אם הם לא מסרו ביודעין מידע להאקרים, הם תרמו מבלי משים להפרה. מתן הרשאות באופן מתירני הינו האיום מספר 1 על עומסי העבודה הממוחשבים המתארחים בענן הציבורי. סביבות ענן ציבוריות מקלות מאוד על מתן הרשאות נרחבות, וקשה מאוד לנהל אחריהן מעקב קפדני. כתוצאה מכך, עומסי עבודה בענן חשופים להפרות נתונים, פריצה לחשבונות וניצול משאבים. ובמילים אחרות? עד שנעלה על זה, כבר יהיה מאוחר מדי. לכן, בכל הנוגע לאבטחת ענן, עליך לנהוג באופן פרואקטיבי ולא ריאקטיבי.

כיצד ניתן להישאר צעד אחד קדימה?

הדבר תלוי למעשה ביכולתך לזהות איומים ולפתח אמצעים למניעת התקפות לפני שהם בכלל מתרחשים. כאשר אבטחת הענן מתבצעת נכון, היא מבטיחה שכבות שונות של בקרות תשתית, כגון בטיחות, עקביות, המשכיות, זמינות ותאימות רגולטורית לנכסיך בענן.

האמצעים שניתן לנקוט כוללים ניטור וסינון תקשורת, ניתוח אירועים, ניהול זהויות, תכנון נכון של המשאבים ומעקב אחרי שינויים. הצבת אמצעי ההגנה הנדרשים עבורך ביעילות עשויה לגבות ממך זמן רב ואף דורשות מיומנויות וידע רב.סביבות ענן ציבוריות מקלות מאוד על מתן הרשאות נרחבות, וקשה מאוד לעקוב אחריהן. כתוצאה מכך, שירותים בענן חשופים לגניבת נתונים וניצול משאבים. על מנת להגיע לסביבת ענן מאובטחת ואופטימלית ניתן ואף מומלץ להשתמש בשירותי מומחים לארכיטקטורת ענן.

במסגרת שותפות אסטרטגית, חברה Radware לחברת מומחי הענן Cloudride אשר נותנת מענה לפתרון אבטחה מרכזי הנשען על Best practices של ספק הפלטפורמה (AWS או AZURE), בשילוב הטכנולוגיה של Radware במטרה להתמודד מול איומי אבטחת המידע שהוזכרו לעיל. היתרון המרכזי בשירות זה הוא שמתבצעת התאמה מלאה של סביבת הענן הכוללת פתרונות אבטחה המותאמים לצרכי הפעילות השוטפת של החברה כך שמנהל המערכת שלך יכול לישון בשקט.

Radware's Cloud Workload Protection הוא מוצר SaaS אשר מספק פתרון agentless ומעניק הגנה אוטומטית מפני איומים מסביב לשעון בכל הרשת. משמעות הדבר היא ניטור מתמיד בזמן אמת של התקפות ברחבי הרשת, ללא צורך בהתערבויות ידניות המועדות לטעות אנוש, וזאת בתגובה לבקשות משתמשים לגיטימיות. התקפות אלה מתפתחות, וזו הסיבה שבעזרת הגנת DDoS בענן מתקדמת תוכל לזהות במדויק את האיומים הדינאמיים ביותר בזמן הקצר ביותר ולהשתמש בהגנה יעילה ביותר מפני האיומים המתקדמים השונים.

Cloudride היא חברת שירותים מומחה בתחום הענן הציבורי, המתרכזת בשירותי אבטחת הפלטפורמה הציבורית בעזרת כלים וידע שנצבר לאורך שנים.

על מנת לקבל הערכה לייעוץ פעילות האבטחה בענן ללא התחייבות לחץ כאן>