אתגר אבטחת הסייבר בסביבת ענן

הענן עלול להוות חלון הזדמנות לפגיעתם של גורמים זדוניים ובכך לחשוף את הארגון לסיכוני אבטחה וסוגיות הנוגעות לפרטיות וסודיות. כיצד לנהל את מפת איומי הסייבר בענן מבלי לעצור ארגונים בדרכם לקידמה הדיגיטלית? | עופר לוינגר

החלטה המתקבלת בארגון להעביר חלק מנכסיו, או את כל נכסיו, לתשתית ענן ציבורי, היא אחת ההחלטות הקשות לארגון שאינו cloud-native. ארגונים גדולים אשר נדרשים לסוגייה זו - ואין כמעט ארגון שאינו נדרש לכך בשנים האחרונות - מוצאים את עצמם מתמודדים, בין היתר, עם אתגר שמירת הפרטיות והסודיות של המידע הקריטי, היוצא מגבולות הארגון אל הענן.

אין גבולות רשת ברורים

הארגון המודרני נדרש לרענן את תשתיות ה-IT שלו ולמכן עד כמה שניתן תהליכים עסקיים, שגוזלים ממנו משאבים יקרים הניתנים להחלפה באוטומציה ו/או מעבר לשירותים מנוהלים. מעל לכל, הארגון המודרני נדרש לספק ללקוחותיו שירות מהיר ויעיל, ובמילים אחרות: שירות דיגיטלי מלא במידת האפשר. כדי לעמוד ביעדים הללו, הצורך לעבור לענן - בין אם פרטי, ציבורי או היברידי - הופך להכרחי ויפה שעה אחת קודם.

הנהירה לענן, אשר בעבר הלא רחוק זכתה לכינוי "המסע לענן", מה שמרמז על הקשיים והאתגרים שארגונים ראו במהלך זה, הוכחה במציאות כאסטרטגיה שהעניקה לארגון גמישות לצד יעילות כלכלית. יחד עם זאת, ברור לכל העוסקים בתחום, כי עדיין מדובר בפלטפורמה שדורשת שליטה ופיקוח קפדניים על כל השירותים והיישומים המושמים בה, מאחר והענן עלול להוות חלון הזדמנות לפגיעתם של גורמים זדוניים ובכך לחשוף את הארגון לסיכוני אבטחה וסוגיות הנוגעות לפרטיות וסודיות.

צריך לזכור שבענן אין גבולות רשת ברורים וחלקים ממנו הינם קופסה שחורה, שאינה בשליטה מלאה של המשתמש. מכאן שפעילות הניטור והשליטה במאגרי המידע, הכוללת ניהול זהויות וגישות לרשת, היא מאתגרת במיוחד. צוות האבטחה בארגון חייב, לאור זאת, להיות חשוף 24/7 לסביבת ה- IT של הארגון וכאשר הארגון מקים כמה סביבות ענן, שמירה על שקיפות ונירואות הופכת לבעייתית ומגבילה את היכולת לאתר ולנתר איומי סייבר. סוגיית אבטחת הענן היא ללא ספק סוגייה מרכזית שעולה לדיון בהנהלות ארגונים השוקלות מעבר לענן, בעיקר ארגונים הפועלים במגזרים רגישים, בהם לחשיפה של המידע המאוחסן בענן יש משמעויות קשות.

"בסופו של דבר, אין פלטפורמה שלא ניתן לפרוץ אליה, אולם ככל שנערמים הקשיים בדרך למטרה וככל שהתהליך גוזל יותר זמן, פוחת הסיכוי והסיכון להפוך למטרה לגורמים זדוניים"

ארכיטקטורה לפני הכול

אז איך בכל זאת מתגברים על אתגר אבטחת הסייבר בענן ולא נותנים לסוגייה זו לעצור ארגונים בדרכם לקידמה הדיגיטלית? על כך ניסו לענות ב-RSA, עם כמה טיפים שמנסים לספק מעין סט של חוקים ל-Ciso הארגוני. יישומם, אני חייב לציין כמי שמייצג חברה העוסקת ב white hacking, עדיין אינו מבטיח סגירה הרמטית של הענן שלכם בפני black hackers, אבל בהחלט מאפשר לישון קצת יותר בשקט.

מניסיוני, העצה הטובה ביותר היא - ארכיטקטורה לפני הכול. הצעד הראשון וההכרחי בהליכה לענן הוא תכנון ארכיטקטוני נכון של הפתרון, תוך שילוב אסטרטגיית אבטחת מידע משלב התכנון. תכנון ארכיטקטוני נכון ביציאה לדרך, יאפשר לארגון למצות את יכולות הענן ולהימנע מרה-תכנון מאוחר ויקר ושגיאות אבטחה שיהיה קשה לתקן בעתיד.

יחד עם זאת, העצה הראשונה של RSA נוגעת לבקרת הרשת ולצורך להטמיע בקרי גישה מבוססי-סיכון. הרעיון הוא לספק את הגישה הנכונה, למשתמשים הנכונים, בזמנים הנכונים. ידוע שככל שסביבת הענן מגוונת ומפוזרת יותר, כך קשה יותר לאבטח את מגוון הגישות אליה, וכפועל יוצא לספק לארגון אבטחה ראויה ומקסימלית. לכן, פתרון המאזן בין זמינות, אמינות ואבטחה, בצורה של בקר שליטה, אמור על-פי RSA, לספק לפחות ארבע יכולות מפתח:

שקיפות בכל רחבי הרשת והיישומים הארגוניים בצורה אחידה, כך שניתן יהיה לנהל בצורה הוליסטית את המשתמשים והגישה ממקור אחד. הרעיון הוא להפחית "שטחים מתים" ובאופן כללי את רמת הסיכון הכללי על המערכת ;

יכולת לנהל בו-זמנית מספר סביבות ענן, תשתית מקומית ומחשבים/ טלפונים אישיים, מבלי להתפשר על האבטחה ונוחות השימוש ;

תמיכה באסטרטגית אבטחת הזהויות של הארגון - מתן גישה למשתמשים, בדגש על גישה ליישומים במהירות ובקלות ;

הטמעת מנוע מודרני, מבוסס סיכונים, העושה שימוש בתהליכי אימות בעלי שני שלבים לפחות, אשר רק על בסיס זיהוי התנהגות חשודה, דורש אימות. המטרה היא לאפשר למשתמשים גישה חלקה לנתונים, שירותים ויישומים מכל מכשיר, בכל זמן.

העצה השנייה מדברת על הרחבה בשקיפות הרשת, על בסיס ההנחה המוכרת בעולם האבטחה, כי לא ניתן לשלוט במה שלא ניתן לראות. כדי לנהל את מפת איומי הסייבר בענן, יש צורך בשקיפות גדולה ככל הניתן, וניטור בלבד אינו מספיק. כאן עולה הצורך בכלים ותהליכים לתיאום מהיר בעת אירוע סייבר. ב-RSA ממליצים על רשת שקופה ומנוהלת היטב, אשר מאפשרת מיפוי יעיל של סיכונים וכוללת:

ארכיטקטורה מודולרית ומבוזרת, אשר אוספת נתונים בכל נקודות "האחיזה" על פני כל פלטפורמות המחשוב (פיזי, וירטואלי והענן) ומייד מתרגמת את הנתונים לתובנות ופעולות ליישום ;

תהליך מואץ של איתור איומים וחקירה שלהם, באמצעות העשרת נתוני לוג, רשת וקצה בזמן אמת, על בסיס מודיעין איומים וביצוע הקשר עסקי ; אוטומציה של תגובות אבטחה, תוך מתן דגש על עקביות, שקיפות ותיעוד תהליכים.

פעולות הערכה ופיקוח שוטפות

העצה האחרונה של RSA נוגעת לניהול פעיל ויעיל של ספקיות הענן. העברת נכסים דיגיטליים - ופעמים רבות קריטיים - לסביבת ענן חיצונית, כרוכה במתן אמון חסר תקדים בספקית הענן הנבחרת. תהליך זה דורש משני הצדדים התנהלות רגישה, מתוכננת, המשלבת פעולות הערכה ופיקוח שוטפות. על מנת להקטין סיכונים הנובעים מניהול ענן באמצעות צד ג', יש להתייחס לכמה נקודות חשובות:

ביצוע ניטור וניהול פעיל של שירותי הענן, לרבות הערכת ביצועים ומעקב שוטף אחר יעילות הענן. החדשות הטובות הן, כי מרבית פתרונות הענן מספקים כלי ניטור ותיעוד מתקדמים, המאפשרים עושר מידע רב, בדרך כלל יותר מהקיים בעולם ה-On-Prem ; ביצוע סקר שוק, בכללו ניטור חוזים וזיהוי הפונקציות העסקיות הקריטיות שכל ספקית יכולה לתמוך בהן בצורה הטובה ביותר. מומלץ לבסס קשרים טובים עם הספקית ולמסד תהליכי עבודה רשמיים, כדי למנוע הפתעות בהמשך הדרך ; זיהוי פערים בבקרי האבטחה ופיתוח גישה דינאמית למדידה וניהול של סיכונים הרלוונטיים לכל ספקית ענן, וזאת כמובן תוך התייחסות לרמת החיוניות של היישום הנתמך.

עופר לוינגר | צילום: יח"צ

ללא ספק, עננים היברידיים מביאים לסביבות המחשוב החדשות עוצמה רבה, אבל יחד עם עוצמה זו באה גם אחריות גדולה לניהול חכם ובטוח. בסופו של דבר, אין פלטפורמה שלא ניתן לפרוץ אליה, אולם ככל שנערמים הקשיים בדרך למטרה וככל שהתהליך גוזל יותר זמן, פוחת הסיכוי והסיכון להפוך למטרה לגורמים זדוניים. לצד הטכנולוגיות המתקדמות שתוארו כאן ומיועדות לבצע את עבודת הניטור, הבקרה והשליטה, יש משקל רב מאוד להון האנושי, שחי ומכיר את הסיכונים בסביבת הארגון, יודע לזהות אותם מבעוד מועד ולהבטיח שהתשתית תהיה ערוכה לבלימה בצורה פרו-אקטיבית.

הכותב הוא מנכ"ל חברת הסייבר White-Hat