לקוחות נכבדים,
בשבוע שעבר קיימנו מפגש בנושא "השלכות המעבר לענן על תחום הגנת הסייבר".
תודה לנותני החסות – חברת CISCO וחברת Commvault-Metallic על ההרצאות המעניינות ועל הפרספקטיבה החשובה.
תחום אבטחת המידע הנו תחום שמאתגר את הארגונים באופן מהותי וגם בסביבת ה- DC המסורתית ארגונים מציינים את הקושי הגדול לגייס ולשמר אנשים ובנוסף לשמור על רמת ידע מספיקה של הצוות.
אולם בענן האתגרים גדלים ומקבלים מאפיינים חדשים שלא היו קיימים קודם – מיעוטם משפרים את רמת אבטחת המידע אך רובם מאתרים הרבה יותר.
העובדה שבענן יש לוג מרכזי של "מי נגע בקונפיגורציה ואיפה שינה" משפרת את היכולת לגלות בעיות בקונפיגורציה ולנהל בעיות כבר בזמן ההתקנה ולא בדיעבד.
השליטה על התשלום בענן – כלומר ה- FinOps – גם היא יכולה להוות אינדיקציה לבעיית אבטחת מידע כי על פעילות מזיקה תחת החשבון של הארגון תתבטא גם בחשבון שהלקוח יצטרך לשלם ולכן ישנו קשר בין FinOps לבין נושא אבטחת המידע.
אולם מן הצד השני בענן יש יותר החלטות בזמן קצת יותר, הדברים משתנים באופן מהיר יותר, יש הרבה יותר שירותים בענן אליהם מתחברים (בד"כ ב- SSO)– וכל נקודת חיבור היא נקודת תורפה. באופן כללי יש בענן יותר הרבה יותר "שערים" והגורמים הטכנולוגיים לא תמיד מודעים להם. גם ה- Shadow IT מרים את ראשו בענן כי באמצעות כרטיס אשראי כל מחלקה עשויה להשתמש בענן – לדוגמה ארגון ציין שבמחלקת "רכב" החלו להשתמש ב- draw.io לציור תרשימים כשה-IT גילו את הדבר במקרה.
בענן לאנשי הסיסטם ולאנשי הפיתוח יש הרבה יותר עצמאות ולכן קשה יותר לשלוט בפעולות שלהם.

דילמה בסיסת ביישום אבטחת מידע בענן היא האם להשתמש בפתרון אבטחת מידע שקיים ב- DC של הארגון גם בסביבת הענן או להשתמש בפתרון ענני חדש.
בבחירה בין האלטרנטיבות מדובר במשולש שיקולים שמשפיע על הבחירה הסופית.
המשולש כולל שלוש צלעות שמחייבות את ה- CISO להתפשר. מדובר על היכולת הטכנולוגית של המוצר, Time to market ליישום הפתרון, וההתאמה של הפתרון לארגון.
מבחינת **היכולת הטכנולוגית** ישנם פתרונות ענן שעונים על צרכים שלא היו קיימים ב- DC ולכן מוצרי ה-DC הקיימים לא יכולים לעמוד בדרישות. ארגון ציין שה-SIEM שמותקן אצלו לא מסוגל להתמודד עם ה- LOGS וההתראות שמגיעות מהענן ולכן יש נטייה לבנות SIEM ענני נפרד.
ישנם גם מקרים הפוכים שבהם פתרונות הענן לא מספיק בשלים ולא יכולים לספק את התכונות הרובסטיות של המוצרים הקיימים – דוגמה אופיינית למקרה זה היא ה- FW שסיפקו יצרניות הענן שלא סיפק את אותן התכונות המתקדמות של ה- FW ב- DC.
ה- **Time to market** הנו שיקול חשוב כי במקרים רבים לפרוייקטי ענן לו"ז צפוף. ברוב המקרים השימוש בפתרונות הענן יהיה מהיר יותר גם כי כבר "מותקן וזמין" בענן וגם האינטגרציה שלו לשאר רכיבי הפרויקט בענן תהיה מהירה יותר. ארגונים ציינו שלעיתים כאשר יש פרוייקט בלו"ז סופר דחוף תהיה בחירה במוצרי הענן מקצה אל קצה – לפחות בשלב הראשון.
השיקול האחרון – לייתר דיוק משפחה של שיקולים – היא **ההתאמה של הפתרון לארגון** באופן הוליסטי. במשפחה זו נכניס את הנראות (visibility) – עד כמה הפתרון החדש משתלב בתמונה ההוליסטית שה- CISO רואה – חיבור ל- SIEM הארגוני, שילוב בתהליכי העבודה הקיימים וכד'. בנוסף יש להכניס את השיקול של ה- governance – מי משתמש במוצר, האם אין

חשיפות לרגולציות השונות על ידי השימוש במוצר, שדרוג המוצר לגרסאות החדשות, יעילות השימוש במוצר– ובתוך זה ניתן להכניס את עלות המוצר מבחינת המחיר ואת נושא ה-FINOPS. לבסוף בנושא של "התאמה לארגון" יש להכניס את השיקול של ידע. האם אנשי האבטחה בארגון יכולים להשתלט על המוצר החדש מבחינת ידע וזמן תפעול.
כפי שעלה בדיון, באופן כללי, משקלו של השיקול הטכנולוגי הנו קטן יותר ממשקלם של שתי הצלעות האחרות במשולש ואם אין אילוץ מהותי של לו"ז השיקול האחרון של התאמה ארגונית יקבל את המשקל הגבוה ביותר.
לדוגמה בתחום ה- FW רובם המכריע של הארגונים בחרו בסופו של דבר להשתמש ב- FW הארגוני ולהרחיב אותו לענן.

עם זאת עלתה הנקודה שככל שעולים בשכבות בענן – כלומר מ- IaaS ל- PaaS ל- SaaS כך יותר קשה להשתמש בפתרונות אבטחת המידע הותיקים ולכן הבחירה תהיה בפתרון אבטחה עניים – אם קיימים.

תודה למשתתפים על תרומתם למפגש,

בברכה

פיני כהן
STKI