אבישי וול*

הגירה לענן - הנושא החם באבטחת הרשתות

להעברת חוות השרתים לענן יש זווית של אבטחת הרשת ♦ זהו תהליך מסובך, המערב בעלי תפקידים רבים שלא תמיד מדברים באותה שפה, וביניהם צוות אבטחת הרשת - אשר לו תפקיד מהותי בתוכנית ההגירה

הגירה לענן היא הנושא החם בעולם אבטחת הרשתות כיום. ארגונים רבים מעוניינים לנצל את היתרונות והתועלות של הענן ומתכננים להעביר את חוות השרתים שלהם אליו. מה הם השיקולים המרכזיים להעביר את חוות השרתים, או לפחות חלק מהאפליקציות החשובות ביותר. למרכז מיחשוב בענן?

יש שלושה שיקולים למעבר: חיסכון בהוצאות התפעול; שיפור יכולות ההתאוששות מאסון; תאימות לדרישות רגולטוריות לשמירה על נתונים אישיים של לקוחות מסוימים בתוך המדינה, ואיסור על הוצאתם מחוצה לה.

השרתים הישנה, כיוון שהשרתים בדרך כלל תומכים באפליקציות רבות. מעבר לכך, לא תמיד ברור אילו שרתים אחרים צריכים לתקשר עם השרת שנמצא בתהליך הגירה, ואילו פורטים ופרוטוקולים צריך לפתוח לצורך התקשורת הזאת. הסיבה לחוסר הוודאות היא, שבארגונים רבים תיעוד התלות של אפליקציות בשרתים, וערוצי תעבורת הנתונים התומכים בכל אפליקציה הוא שגוי, מיושן או לעתים פשוט לא קיים.

ואולם לא הכל שחור: כיוון שיש מקור אחד למידע אמין, שתמיד אפשר לפנות אליו, גם אם מזניחים אותו לעתים - ההרשאות בפיירוול עצמן. אחרי הכל, לפני העברת השרתים תפקדו האפליקציות כשורה.

העברת חוות שרתים לענן, מכל סיבה שהיא, היא תהליך מסובך, אשר מערב בעלי תפקידים רבים שלא תמיד מדברים באותה שפה, וביניהם צוות אבטחת הרשת, אשר יש לו תפקיד מהותי בתוכנית ההגירה. במאמר זה נבחן את תהליך המעבר לחוות שרתים וירטואלית מנקודת המבט של צוות אבטחת הרשת.

העברת חוות שרתים פיזית לענן פרטי, או משותף, דורשת ביצוע ארבעה צעדים בסיסיים: בחירת שרת בחוות השרתים הישנה; יצירת עותק (clone) של השרת בחוות השרתים החדשה; הפניית כל האפליקציות שקיבלו שירותים מהשרת הישן אל השרת החדש (זהו השלב בתהליך, שבו צוות אבטחת הרשת הכי מעורב. כדי שהאפליקציות העסקיות יוכלו להשתמש בעותק השרת החדש, יש לעדכן את המדיניות וההרשאות בפיירוולים ובנתבים הרלוונטיים וכך לאפשר זרימת מידע אל ומאת השרת החדש); סגירת השרת הישן.

צעדים אלה נראים פשוטים, אך האתגר הוא לבצע אותם מבלי לשבש שירותים קיימים ומבלי לגרום להשבתות בלתי מתוכננות. סקר שערכנו באחרונה מצא, ששני שלישים מהארגונים נתקלו בהפרעות או בהשבתות של הפעילות בשל פרויקטים להעברת חוות השרתים.

מדוע תקלות נפוצות כל כך?

לרוב לא ברור בדיוק אילו אפליקציות תלויות בשרת מסוים בחוות המסקנה ההגיונית היא, שכל ערוצי תעבורת הנתונים שהאפליקציות נזקקו להם היו, ועדיין, פתוחים בחוקי הפיירוול.

בזכות השימוש בחוקים הקיימים של פיירוול, אפשר להעביר את השרתים ללא הפתעות בלתי מתוכננות. בשלב הראשון צריך לגלות את כל חוקי הפיירוול המתייחסים לכתובת ה-IP הישנה של השרת. לאחר מכן תוכלו להוסיף את כתובת ה-IP של השרת המשוכפל לכל החוקים שחשפתם (כך שהשרת הישן והשרת החדש יוכלו לעבוד במקביל). כאשר הכתובות מעודכנות, מהנדסי היישומים יוכלו לקנפג מחדש את כל רכיבי האפליקציות ולהפנות אותם לשרת החדש מבלי שהתקשורת תיחסם. ברגע שכל האפליקציות הנזקקות לשרת החדש עודכנו ונבדקו, ניתן להוריד את השרת הישן ללא חשש ולהסיר מחוקי הפיירוול את כל ההפניות לכתובת שיצאה משימוש.

למעשה, השימוש בחוקי פיירוול כדי להכוון את העברת חוות השרתים יאפשר לצוות אבטחת הרשת להוליך את תהליך ההגירה. לא משנה כמה התיעוד בחוות השרתים לוקה בחסר - חוקי הפיירוול תמיד יוכלו לספק רמזים חשובים לשאר צוותי טכנולוגיות המידע לגבי אילו אפליקציות יושפעו מהגירה של שרת מסוים, ואילו קבוצות של שרתים עדיף להעביר כקבוצה אחת.

* פרופ' אבישי וול, יזם ומדען ראשי, אלגוסק