

18.57x24.83	1/2	26 עמוד	new-tech magazine	28/02/2020	72329383-7
20663 - סקיי - TERASK חברות טרה סקיי					



לצלוח את אתגר המיקרו-סגמנטציה

◀ דן כהן, מנהל תחום ענן ואוטומציות, חברת TeraSky

נראה כי המונח מיקרו-סגמנטציה מרחף באופן תמידי מעל ראשם של אנשי אבטחת מידע, תקשורת ו-IT בכלל. לאחר שמקבלי ההחלטות למדו את המתודולוגיה והבינו את היתרונות, נותר "רק" ליישם. בפשטות, מיקרו-סגמנטציה הינה חלוקת רשת לאזורים מאובטחים המכילים שרת אחד או יותר, כאשר בין אותם אזורים נאכפת חוקה המאפשרת תקשורת חיונית בלבד. עבור יישום מוצלח נודקק לטכנולוגיה המאפשרת שלושה דברים: יצירת קבוצות לוגיות של שרתים, שיוך שרתים לאותן קבוצות לוגיות ויצירת פוליסת אבטחה והחלטה.

למרות ששחקניות רבות בשוק מציעות מגוון פתרונות עם פחות או יותר אותן יכולות, כגון מודולים המותקנים ישירות על Hypervisor בסביבות וירטואליות או יכולות מובנות במערכת ההפעלה, חברות רבות המעוניינות ביישום של המתודולוגיה, ממאנות ליישם או שנתקלות בקשיים גדולים ביישום כבר בתחילת הדרך.

הסיבה העיקרית טמונה בקושי שבמיפוי האפליקציות והשירותים בנוסף ליצירת החוקה עצמה. כהתחלה נתמקד בסביבה וירטואלית קטנה המכילה כמה עשרות מכונות

וירטואליות. בהמשך נתייחס בקצרה גם ל-Containers. בסביבה כזו לא תהיה בעיה לאתר את אנשי האפליקציה או התשתיות שהשרתים בבעלותם, וביחד להבין באילו אפליקציות ושירותים מדובר ולתשאל לגבי אופי התעבורה. גם במקרה שאנשי האפליקציה לא יידעו לומר איזה פורטים (Ports) חיוניים עבור האפליקציה, נוכל לבצע את הניתוח באמצעות כלים מקומיים על מערכת ההפעלה כיוון שסביבת השרתים קטנה.

מה קורה בסביבות גדולות יותר, עם מאות מכונות וירטואליות וכמה עשרות אפליקציות? מיפוי דיני של האפליקציות הוא מעט סזיפי, אך עדיין אפשרי. אך מה עם עניין החוקה? ניתוח דיני של התעבורה הופך להיות במקרה הטוב פרויקט מאתגר וממושך וברוב המקרים בלתי ישים. לשם כך נולדו טכנולוגיות שונות המאפשרות ניתוח תעבורה בזמן אמת, ויתרה מכך מאפשרות בניה אוטומטית של חוקה.

בסביבות גדולות, כמתואר לעיל, האתגר גדול אף יותר. סביר מאוד שהטכניקות הקודמות שהשתמשנו בהן לטובת המיפוי כבר לא יהיו רלוונטיות. במחלקות IT לעיתים ניתן למצוא CMDB (בסיס נתונים לניהולי תצורה) מתוחזק היטב כאשר כל שרת פעיל מתועד לפרטים.

במקרה הזה ניתן לבנות אוטומציות די פשוטות שייצרו את הקבוצות ויבצעו את השייכים על בסיס המידע הטמון ב-CMDB.

בסביבות גדולות ומסועפות, ללא אמצעי תיעוד הסביבה, הסיכויים למימוש מוצלח של מיקרו-סגמנטציה פוחתים. האמיצים יתקלו במהרה באתגר מהותי נוסף - תוספת תמידי של שרתים ואפליקציות חדשות, כך שהמיפוי הופך לעבודה בלתי נגמרת.

לצד אתגרים מרכזיים אלו, נשאלת השאלה מה עושים עם סביבות Containers. על פניו, נראה שסיבכנו פרויקט שהיה כבר מסובך מלכתחילה, אך מסתבר שסביבות אלו ידידותיות יותר ליישום מיקרו-סגמנטציה. הסיבה היא ש-containers מתוייגים מלכתחילה, ובנוסף בקובץ המניפסט שלהם נקבע הפורט שלו הם מאזינים. את העובדה הזו כאמור ניתן לנצל לטובתנו.

למרות שהטכנולוגיה בשלה, יישום של מיקרו-סגמנטציה בסביבות וירטואליות הנו מאתגר מאוד, בעיקר עבור ארגונים גדולים. יחד עם זאת ישנם ארגונים שהצלחו ליישם בהצלחה פרויקטים מסוג זה גם בחברות גדולות. ההצלחה טמונה בבניית אסטרטגיה חכמה ויצירתית.

18.54x24.69	2/2	27	new-tech magazine	28/02/2020	72329382-6
20663 TERASK חברת טרה סקיי -					

ביעילות קטנה בהרבה. ישנן אפשרויות רבות, אך העיקרון הוא שאותו תהליך חייב להיקבע מראש כחלק מתוכנית הפרויקט.

תשומת לב ארגונית

לכאורה זהו האלמנט הפשוט והמוכן ביותר. בהתבוננות לאחור על פרויקטים של מיקרו-סגמנטציה, ניתן לראות שברוב המקרים הסיבה המכרעת לכישלון היא בהתגייסות של הארגון ליישום הפרויקט. פרויקט מיקרו-סגמנטציה הוא חוצה חטיבות/מחלקות/צוותים ומחייב שיתוף פעולה רוחבי.

ניקח לדוגמה חברת טלקום גדולה ומסועפת, שבה מנהל אגף הטכנולוגיות החליט להטיל על מחלקת ה-IT את משימת מימוש הפתרון. באותה חברה אין CMDB מנוהל, אין קונבנציית שמות שימושית או כל כלי תיעוד אחר.

בלית ברירה, אנשי ה-IT התחילו לפנות לאנשי האפליקציה. אנשי האפליקציה, שלא היו מחויבים לפרויקט, סיפקו היענות מוגבלת מאוד, והטריחו את אנשי ה-IT בהוצאת אינספור זימונים לפגישות ותעבורת מיילים מיותרת. בהיעדר נקודות מיקוד, המשיכים לפרויקט בכל הגופים הרלוונטיים – תקשורת, System, אבטחת מידע, R&D, DevOps, וכדומה, נוצרים צווארי בקבוק בפרויקט שמסכנים את הצלחתו.

לסיכום, יש אתגרים רבים במימוש מיקרו-סגמנטציה בהם אתגרים טכנולוגיים ואתגרים פרויקטים. על מנת להבטיח מימוש מוצלח, יש להכיר את האתגרים ולתת עליהם את הדעת. תכנון קפדני של אסטרטגיית המימוש תבטיח את הצלחת הפרויקט.



דן כהן, מנהל תחום ענן ואוטומציות, חברת TeraSky. צילום: אסף רונן

אכיפה בשלוש שכבות בלבד, כאשר תעבורה עוזבת סגמנט אחד ומנותבת לאחר. עם מיקרו סגמנטציה אנחנו יכולים לבצע חציצה על בסיס סביבה, אפליקציה, קבוצת שרתים, שרת בודד ועד כרטיס רשת. ככל שהחלוקה שלנו תהיה גרעינית יותר, כך גם תעלה רמת המורכבות של הפרויקט. אם נתייחס למשל למקרה הפשוט של אפליקציה בעלת שלוש שכבות (Web, Application, DB), אז באופן אידיאלי נרצה ליצור קבוצת אבטחה עבור כל שכבה והשרתים שלה. נוכל להחיל חוקה כך שלא רק כל שכבה תתקשר עם האחרת בפורטים חיוניים בלבד, אלא גם שלא תהיה שום תקשורת בין שרתים באותה שכבה. הבעיה היא שלא כל אפליקציה מופרדת לשכבות בצורה פשוטה כל כך. ישנן אפליקציות, במיוחד ישנות, המורכבות ממספר גדול של שרתים שכל אחד מהם מחזיק רכיב אחר של המערכת. אם ניצור קבוצה עבור כל רכיב, תהייה לנו כמות גדולה מאוד של קבוצות. שוב, במקרה של סביבה גדולה, מיפוי של קבוצות ותתי קבוצות של אפליקציות ושכבותיהן יכול להפוך למטלה ארוכה מאוד. במקרה זה יכול להיות שנעדיף לבצע את החציצה ברזולוציה של אפליקציה ולא של שירות. אמנם אנחנו מתפשרים כאן על רמת האבטחה, אבל ייתכן וזה יהיה ההבדל בין פרויקט ישים לבלתי ישים.

פריסת שרתים

בסביבה שבה מיושמת מיקרו-סגמנטציה, כל שרת צריך להיות חבר בקבוצת אבטחה. לשם כך למעשה נעשית עבודת המיפוי הראשונית אשר אחריה נבנות הקבוצות שאליהן משויכים השרתים. כאמור, אחת הבעיות היא שבמהלך הפרויקט, מתווספים שרתים נוספים לתוך המערכת, ובהיעדר תהליך שיוך מסודר, שרתים חדשים לא יקבלו חוקה מתאימה. בסביבות קטנות סביר שאנשי ה-IT הם היחידים שיוצרים שרתים חדשים במערכת, ואת הבעיה אפשר לפתור באמצעות נוהל והרבה משמעת, כלומר בעצם היצירה, איש ה-IT מוסיף את השרת באופן ידני לקבוצה המתאימה. הפתרון הזה לא מאוד ישים כאשר מדובר בסביבה בינונית-גדולה שכמות גדולה של אנשים פורסים אליה שרתים. פריסת השרתים חייבת לעבור דרך תהליך אחד מבוקר אשר במהלכו יתבצע השיוך. אפשרות אחת היא שימוש בפורטל web שדרכו יתקזזו כל הבקשות לשרתים חדשים. אידיאלית - מאחורי הקלעים ירוץ תהליך אוטומטי שידאג לשייך את השרת לקבוצה המתאימה, אך גם תהליך ידני יביא לאותה תוצאה אם כי

אלה כמה מהנקודות שיש לתת עליהן את הדעת:

טכנולוגיה

מעבר לפונקציונליות בסיסית, שתאפשר יצירות קבוצות אבטחה דינאמיות, שיוך ובניית חוקה, נרצה להשתמש בכלים נוספים שיאפשר לנו לקבל תמונת מצב של תעבורת השרת בתוך הסביבה. לכלים בשוק יש יתרונות וחסרונות, וצריך להבין היטב איך להתאים את הטכנולוגיה למקרה הספציפי. ניקח למשל מערכות ניתוח תעבורה באמצעות סוכן המותקן על גבי מערכת ההפעלה. מערכות אלו באות לעיתים עם יכולות זיהוי תעבורה ברמת התהליך. היתרון הוא שבסביבה שבה אין אמצעי תיעוד ומיפוי סבירים, נוכל להיעזר במאפייני התהליך כדי לסווג את האפליקציה. החיסרון הוא התקורה הגדולה בניהול סוכנים, והעובדה שבסביבות מסוימות קיימות מערכות הפעלה לא נתמכות.

מרחב מימוש

במילים פשוטות, על איזה חלק מהסביבה ימומש הפתרון. כאמור, שלב המיפוי בפרויקט מיקרו-סגמנטציה יכול להיות ארוך מאוד ואנו רואים פרויקטים רבים אשר כאלה נזנחים ומוכרזים ככישלון. מסיבה זו, במיוחד בסביבות גדולות, כדאי לשקול לתחום את הפרויקט לחלק קטן מהסביבה, אך בעל משמעות אסטרטגית. ניתן למשל לבחור באפליקציה גדולה בארגון כיעד לשלב הראשון. בחירה של יעד ריאלי לביצוע בזמן סביר, תסייע בהשגת והצגת הישגים לאורך הפרויקט. מלבד האפליקציה, ניתן לתחום את הסביבה לרשת, תשתית, מיקום פיזי וכדומה. לא תמיד גישה זו עדיפה. ניח שבחרנו להתחיל מאפליקציה אחת, סיימנו את המיפוי וכעת אנחנו בשלב בניית החוקה. לצורך בניית החוקה, לאחר שימוש בכלי ניתוח תעבורה, גילינו שכמו רוב האפליקציות, גם זו תלויה בשירותים של אפליקציות אחרות. על מנת לבנות חוקה אופטימלית, נהיה חייבים למפות גם את אותן אפליקציות. תלות זו יוצרת לא מעט כאב ראש, ולכן, כאשר מדובר בסביבות קטנות ואף בינוניות עם יכולת מיפוי בזמן סביר, אולי דווקא נרצה ללכת על מיפוי כולל.

רזולוציית מימוש

סגמנטציה בעולם "הקלאסי" של אבטחת מידע מתייחסת לחציצה על בסיס סגמנט IP. כלומר