

"חשוב לדמות ולתרגל מתקפת DDoS"

נמרוד קרביקס, מהנדס מערכות בכיר באזור EMEA (אירופה, המזרח התיכון ואפריקה) באיקסיה, אמר כי "הדמיה של מתקפות קיברנטיות היא מרכיב מהותי ומשמעותי במסגרת היערכות ההגנה של ארגונים מפני מתקפות אלה. חשוב לדמות ולתרגל מתקפת מניעת שירות מבוזרת (DDoS) כי התרגול הוא חלק מההגנה. אנחנו מציעים מוצר לבדיקות ביצועים ומתקפות, שבמסגרתו בודקים את שני הצדדים: שרת וקליינט."

נמרוד קרביקס: "ארגונים רבים ונותני שירותים, שמשתמשים בכלים של פורטינט, מסתמכים על היישום שמספקת מערכת Ixia BreakingPoint ופתרונות בדיקת אבטחה כדי לוודא לפני הרכישה שהציוד אכן מתאים ומתפקד בצורה הטובה ביותר עבור הרשת, תמהיל השירותים והתנאים שקיימים ברשת שלהם"

"איכסיה מאפשרת עולם מאוחד", הוסיף. "היא מספקת פתרונות לבדיקת ולבחינת רשתות IP מאוחדות, שמבצעים אמולציה מנקודות הקצה האלחוטיות ועד לליבת רשת האינטרנט". לדברי קרביקס, "הפתרונות שלנו יוצרים תנאים המדמים את העולם האמיתי על ידי ביצוע אמולציה של כל טווח הפרוטוקולים, בעומסים משתנים ותוך יצירה של תעבורה שבאה מיישומי מדיה עשירה. זאת, כדי לאמת ולהעמיד למבחן את הביצועים והאבטחה של רשתות מיחשוב ענן, ליבת הרשת, מרכזי נתונים, רשתות אלחוטיות ורשתות משולבות".

הוא סיים בצינון כי "ארגונים רבים ונותני שירותים, שמשתמשים בכלים של פורטינט, מסתמכים על היישום שמספקת מערכת Ixia BreakingPoint ופתרונות בדיקת אבטחה כדי לוודא לפני הרכישה שהציוד אכן מתאים ומתפקד בצורה הטובה ביותר עבור הרשת, תמהיל השירותים והתנאים שקיימים ברשת שלהם. זאת כדי ליעל הטמעות NGFW ולהבטיח לאורך זמן שהוא אכן מספק הגנה מרבית למתקפות סייבר חדשות וישנות, שעלולות לפגוע ברשת שלהם."



אלי פרנס



אמיר אדד



נמרוד קרביקס

ואף תתחזק בהתחלת השנה הבאה, בייחוד בארגונים במגזרים הביטחוני, הפיננסי, ההיי-טק והתעשייה", כך אמר **אלי פרנס**, מנהל מכירות אזורי פורטינט.

לדברי פרנס, "ארגונים מבינים כי נדרשת הגנה מוכללת, שתספק מענה למגוון רחב של איומים. יש גידול במגמת ה-BYOD. הלוקחות מגיעים עם יישומים מהבית ונדרש להגן על כל הרכיבים. בנוסף, יש צורך לטפל ב-Big Data. נדרש לענות ולהגן על סביבות רשת עתירות מידע ולזהות סיכונים מבעוד מועד, לרבות מתקפות מתקדמות על מרכזי הנתונים עתירי המידע. עוד יש להיערך לקראת איומי הסייבר, ובראשן מתקפות ממוקדות ומתמשכות - APT. נדרש להגן על מערכות ה-IT בארגונים מפני מתקפות מרובות, שבאות לפגוע גם בארגונים פיננסיים, וכיום גם במדינות ובאתרי ממשלות. יש לתת מענה מקוון למקרה תקיפה שהצליח לחדור למערך ה-IT הארגוני. הוא סיכם בצינון כי "ארגונים מפנימים יותר ויותר את הצורך בפתרונות מוכללים, שיספקו מענה למגוון רחב של איומים".

הטמעת מוצרי פורטינט בבזק בינלאומי

אמיר אדד, מנהל מחלקת ההנדסה של בזק בינלאומי, ציין כי החברה היא שותפה של פורטינט ומטמיעה אצל לקוחותיה מגוון טכנולוגיות שלה, מפתרונות הדור הבא של הפירוד, NGFW, דרך פתרונות Secure Web Gateway וכלה בפתרונות להגנה מפני מתקפות קיברנטיות. הוא אמר כי "מגוון המוצרים של פורטינט מאפשר הגנה מקצה לקצה ומתאים

אמיר אדד: "מגוון המוצרים של פורטינט מאפשר הגנה מקצה לקצה ומתאים לכל סוגי הלוקחות, מכל מגזרי התעשייה ומכל הגדלים"

לכל סוגי הלוקחות, מכל מגזרי התעשייה ומכל הגדלים".

אדד הוסיף שבזק בינלאומי הטמיעה בתוכה שני פתרונות של פורטינט: החלפת מוצר של צ'ק פוינט בזה של פורטינט בשכבת הגנה 2 ומוצר שהצורך בהטמעתו נבע מהרגולציה, שחייבה כל ספק אינטרנט להעניק ללקוחות הפרטיים שירות אבטחת מידע. "הבאנו בחשבון גם שירותים מקבילים של סימנטק וצ'ק פוינט, ובחרנו בזה של פורטינט בשל יכולות הגמישות, הביצועים והתפעול".