מיתוס אבטחת הסייבר

מָבוֹא

למרות שהאינטרנט עשה התקדמות פנומנלית במהלך העשורים האחרונים, הוא נותר שברירי ופגיע להתקפות גדולות כקטנות עד היום. משתמשים מבולבלים לגבי פעולתו המורכבת ולעתים קרובות אינם מסוגלים להבחין בין פריצה על ידי פורץ לבין פריצה לתוכנת ההגנה.

אירוע אחד כזה התרחש לאחרונה ב-18 בנובמבר 2025, כאשר Cloudflare סבלה מהפסקת הפעלה עולמית שגרמה לרגע לפגוע ברשת האינטרנט.
זה לא היה מקרה בודד. הקודם התרחש רק שמונה חודשים קודם לכן, והיו עוד כאלה לפני כן. באופן דומה, שירותי האינטרנט של אמזון (AWS) חוו שיבושים תכופים.
הפסקות אינטרנט מסוג זה הפכו לכמעט שבשגרה ואמינותם של שירותים אלה שנועדו להגן מפני חדירות סייבר הועמדה בספק.

הבעיה

הפגיעות של האינטרנט הייתה בעיה מזה עשרות שנים. בשנה שעברה פרסמה ועדת התקשורת הפדרלית (FCC) הודעה על קביעת כללים מוצעים (NPRM) שזיהתה את פרוטוקול שער הגבול (BGP) כיעד להפחתת הסיכון. מועצת ארכיטקטורת האינטרנט (IAB), המייצגת את קהילת האינטרנט, הגיבה בתגובה והביעה חששות. אף על פי כן, הבית הלבן פרסם מפת דרכים שהתמקדה בשלמות ה-BGP כאמצעי לשיפור אבטחת ניתוב האינטרנט.

בהקשר זה, חשוב לזכור כי ה-BGP נדרש להעברת חבילות בין מערכות אוטונומיות (ASes) שנבחרו על ידי שרת שמות המתחם (DNS), בהתבסס על כתובות IPv4 שהוקצו למנויים על ידי פרוטוקול בקרת מארח דינמי (DHCP), אשר נוצר כדי להתמודד עם מחסור בכתובות IPv4. מחסנית [9]רוטוקול זו הביאה לארכיטקטורת מערכת מורכבת הפגיעה להתקפה מכיוונים רבים, שכל אחת מהן דורשת תיקון נוסף בתגובה.

הפתרון

מערכת פגומה מזמינה סדרה בלתי נגמרת של פריצות ותיקונים. אינטרנט חזק הרבה יותר יכול לנבוע מארכיטקטורה פשוטה ויעילה שמבטלת את שורש הבעיה של מחסור בכתובות IPv4, ובכך מבטלת את הצורך בכל אחד מארבעת הפרוטוקולים שהוזכרו לעיל. זוהי תוצאה של מערכת דטרמיניסטית המכונה EzIP.

(לטקסט מלא. https://avinta.com/gallery/CyberSecurityMyth-IL.pdf אנא בקר)