



אמינות ושלמות המידע במערכת שמות המתחם (DNS) באינטרנט

מבוא

מערכת שמות המתחם (DNS) היא המערכת המאפשרת למשתמשים לנווט את דרכם ברשת האינטרנט באמצעות שמות המתחם המוכרים. זהו בסיס נתונים גלובאלי, היררכי ומבוזר, שחלקיו השונים מנהלים כל אחד באופן עצמאי. מטבע הדברים, אמינות ועקביות המידע שבמערך מידע זה הן קריטיות.

מסמך זה מציג מספר דגשים חשובים בשמירה על אמינות המידע במערך ה-DNS, ובפרט, מתייחס אל תפקידם של ספקי השירות וחלקם בהבטחת אמינות זו.

פירוט

מערכת שמות המתחם (Domain Name System) היא מערכת גלובלית, שתפקידה העיקרי הוא תרגום שמות מתחם (כגון "www.isoc.org.il") לכתובת מחשב באינטרנט (IP Address). מערכת זו היא המאפשרת למשתמשי הרשת לגשת לשירותים הרצויים להם, תוך שימוש בשמות, וללא היזקקות לכתובות מספריות מסובכות. המערכת היא, למעשה, בסיס נתונים היררכי, המתחיל בשרתי השורש הגלובאליים (Root Servers), מהם לשרתי השמות ברמה העליונה (TLDs) – כגון .com או גם .il הישראלי, וכך הלאה.

איתור שם מתחם ב-DNS מתחיל, עקרונית, בשרת השורש, ומשם, לאחר שורה של הפניות, מאותר שרת השמות שבו נמצא המידע המלא על השם אותו מחפשים. שרת זה נקרא השרת המוסמך (Authoritative Server) עבור אותו שם מתחם. לדוגמה: כאשר ניגשים לאתר האינטרנט www.example.org.il, יפנה שרת השורש את המחפש לשרת המוסמך של il (במקרה זה, השרת של מרשם השמות הישראלי), משם תהיה הפנייה לשרת של org.il, ומשם לשרת המוסמך של example.org.il. שם, יימצא המידע המלא על מיקומו של האתר המבוקש. כל האמור לעיל מתבצע, כמובן, אוטומטית, ע"י התוכנה במחשב המשתמש ושרתי השמות בעולם.

המידע בשרת השמות המוסמך עבור שם מתחם, מנוהל ע"י מחזיקו הרשום של אותו שם, או נציג טכני מטעמו. לעתים קרובות, יהיה נציג זה הגוף המספק לו שירותי אירוח אתרים (Hosting).

קביעתו של שרת שמות כמוסמך עבור שם מתחם מסוים נעשית ע"י שרת השמות ברמה שמעליו – בדוגמה דלעיל, קביעתו של שרת המוסמך ל-example.org.il נעשית במרשם השמות, האחראי, בין היתר, על השרת של org.il.

כך, למשל, כאשר מחזיקו של שם-מתחם מבקש להחליף ספק שירות אירוח, הוא פונה למרשם השמות – במקרה שבדוגמה, איגוד האינטרנט הישראלי (ישירות, או באמצעות הספק החדש), ומעדכן במרשם שמות המתחם את פרטי השרת המוסמך החדש. במקביל, מתבצעות שתי פעולות חשובות נוספות:

א. ספק השירות החדש (כלומר, זה שאליו עוברים), מעדכן את שרת השמות שלו להציג מידע מוסמך עבור שם המתחם המועבר;

ב. ספק השירות הקודם מעדכן את שרת השמות שלו ע"י הסרת הגדרת ההסמכה.



Israel Internet Association (ISOC-IL)

איגוד האינטרנט הישראלי

פעולות אלה צריכות להתבצע תוך זמן קצר, כדי שאמינות ועקביות המידע במערכת ה-DNS תישמר. אי התאמה בהגדרתם של שרתים כמוסמכים הינה מקור לבעיות רבות.

לעיתים קורה, שהעדכון השני (סעיף ב' לעיל), מתעכב. העיכוב עשוי להיגרם כתוצאה מהזנחה, אך קרו גם מקרים בהם טען ספק שירות כי אינו מעדכן את השרתים בגלל אי הסכמה עסקית בינו לבין בעל האתר.

במקרה כזה, לאחר ביצוע ההעברה, פרטי השרת המוסמך החדש מתפרסמים ברשת האינטרנט, וכל המבקש מידע אודות שם המתחם המדובר יגיע לשרת החדש ולמידע המעודכן המצוי עליו – כולם, זולת לקוחותיו של ספק השירות הקודם, שלא עדכן את שרתיו. הסיבה לכך היא, שבכל פעם שלקוחותיו של אותו ספק ניגשים לאינטרנט, מחשביהם פונים בדרך כלל קודם כל לשרת השמות של אותו ספק. אם אותו ספק לא ביצע את העדכון הנדרש של שרתיו, שרתים אלה ימשיכו להתייחס לעצמם כשרתים מוסמכים (ולכן, ככאלה המחזיקים מידע מעודכן לכאורה) ויחזירו למשתמש את המידע המצוי עליהם, שהוא כעת מידע מוטעה ולא אמיתי.

כתוצאה מכך, ספק השירות שלא עדכן את שרתיו מפיץ לכל לקוחותיו, להם בלבד וללא ידיעתם, מידע מוטעה ולא מעודכן אודות שם המתחם. לדוגמא, בהנחה שאתר שאינטרנט הקשור לאותו שם מתחם שינה את מקומו, אי העדכון מביא לכך שכל לקוחותיו של הספק (והם בלבד!) יוטעו לחשוב כי אתר כזה לא קיים, וזאת בניגוד גמור למציאות בה האתר קיים ונגיש לכל שאר העולם (או גרוע מכך – יופנו לגרסה לא עדכנית של האתר שעלולה להכיל תכנים שאינם מעודכנים ואינם מורשים). דוגמא נוספת עשויה להיות שלקוחותיו של אותו ספק (והם בלבד) לא יוכלו לשלוח דואר אלקטרוני למחזיק שם המתחם, עובדיו ו/או לקוחותיו (או אפילו שדואר אלקטרוני זה יזרום לשרתיו של ספק השרות הסרבן, במקום לתעודתו).

אי עדכון שרתים וניתוק קבוצות משתמשי רשת שלמות ממידע מעודכן (וניתובם למידע מטעה), מביא לפגיעה ביציבות ובאמינות רשת האינטרנט, ועלול להיות בעל השלכות הרסניות בטווח הארוך.

חובתו של ספק שירותי אינטרנט לדאוג לכך ששרתי השמות שלו יספקו בכל עת מידע נכון ומעודכן אודות שמות המתחם באשר הם. אין לו בשום פנים ליצור מצג מוטעה ללקוחותיו, כאילו שרת ה-DNS שלו הוא השרת המוסמך, אם אין הדבר כך במציאות עפ"י המידע במערכת ה-DNS הגלובאלית, כל זאת תוך שבאופן מעשי מקבלים לקוחותיו מידע מוטעה ומטעה, מנותקים מחלק מן המידע המעודכן הקיים ברשת, ותנועותיהם ברשת מנותבות למקומות שלא התכוונו להגיע אליהם – ללא ידיעתם. למותר לציין כי טענות על חילוקי דעות עסקיים (כגון חובות כספיים) עם מאן דהוא כמניע לפרקטיקה זו, אין להן דבר עם הצגת מידע שגוי באופן מכוון ומודע, וודאי שאינן יכולות לשמש צידוק לפעולה שכזו.