

להקשיח את מערכות ה-DNS

"נדרש להקשיח את מערכות ה-DNS. הקשה שכזו תצמצם משמעותית את הנזקים הנגרמים ממתקפות מניעת שירות מבזורות, DDoS", כך אמר **סטפן לאגרהולם**, סגן נשיא למכירות ב-Secure64. לדבריו, רוב המתקפות מסוג DDos נועדו לפגוע במערכות ה-DNS הארגוניות, לכן, ארגוני אנטרפרייז שיש להם נוכחות רחבה באינטרנט נדרשים להקשיח את מערכות ה-DNS שלהם.



סטפן לאגרהולם

Secure64 מיוצגת בישראל על ידי ConnectIT. לדברי לאגרהולם, החברה קמה ב-2002 ופיתחה טכנולוגיות לאבטחת מערכות ארגוניות קריטיות לניהול הדומיינים (DNS) מפני כמה סוגי מתקפות: DDos, חטיפות דומיין ו-IP, פשיג ותיקפות המנצלות את חולשת מערכות

ה-DNS. "אנחנו מספקים פתרונות משולבי חומרה ותוכנה להגנה על מערכות ה-DNS, כך שניתן למנוע חדירה של האקרים לארגון ולמנוע נפילה של מערכות זו ארגוניות קריטיות", אמר. הוא ציין שבין לקוחות החברה נמנות רשויות ממשל אמריקניות וספקיות טלקום בינלאומיות. "מערכות ה-DNS מהוות נקודות כניסה ויציאה מהארגון לאינטרנט", סיכם לאגרהולם. "נקודות אלה משמשות האקרים כדי לפגוע בארגון או בלקוחותיו, ולכן ההגנה עליהן כה חשובה".

"ארגונים לא מאמינים שהם יכולים להיפגע ממתקפת סייבר"

"הדור הדיגיטלי החדש נמצא בבעיה, שכן כלל הפעילויות, הפרטיות והארגוניות, נעשות כיום במרחב הווירטואלי. לכן, ארגונים נדרשים להגנה של



יואנון גד

360 מעלות מפני מתקפות סייבר", כך אמר **יואנון גד**, יו"ר ומנכ"ל משותף של אינוקום מקבוצת אמן. הוא אמר, כי "לא פעם, אנחנו נתקלים בחוסר הבנה מצד הארגונים - הם לא מאמינים שהם יכולים להיפגע ממתקפת סייבר, אף שסביר שהם חוו או חווים ממש באותם רגעים מתקפה שכזו". כך, הם לא

לוקחים בחשבון שהמדיה החברתית יכולה להיות כר פורה למתקפות מעין אלה: "הרשתות החברתיות מאפשרות להאקרים להשיג מודיעין איכותי, שמשכלל את המתקפה", אמר, "נתקלנו במתקפות מוצלחות שניצלו מידע פרטי של אחד העובדים בארגון כדי להציג מצג אונטני כביכול ולהשיג גישה למערכות ה-IT הארגוניות".

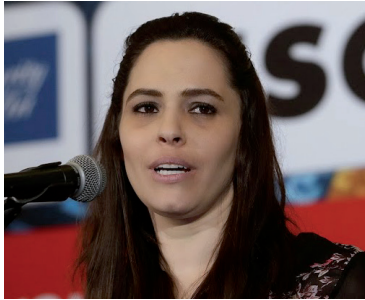
"ההגנה של הארגון נמדדת בחוליה החלשה ביותר, ולמרבה הצער אין פתרון קסם", ציין גד. "ההאקרים נמצאים צעד אחד קדימה ולכן צריך להיערך בכל החזיתות, כדי לתת פתרון שיכסה את כלל הארגון. אינוקום עושה זאת - היא מייצגת חברות אבטחה מובילות בתחומן כמו פאלו אלטו, המספקת את הדור הבא של פיירוול (NGFW), גוד, שמציעה אבטחה לפלטפורמות הניידות בארגונים, AirTight Networks-1, שמתמחה בהגנה על רשתות Wi-Fi".

"המתקפות כיום מתוחכמות וממוקדות"

"פעם, המתקפות על ארגונים התאפיינו באקראיות. כיום, רוב מתקפות

הסייבר הן חכמות, מתוחכמות ומכירות את הארגון המותקף", כך אמרה **עדי רוזה**, מנהלת תחום הכשרות סייבר באבנת אבטחת מידע.

לדברי רוזה, "מתקפות הסייבר מהוות איומים משמעותיים על ארגונים. כוח האדם שמתמודד איתם וטיב ההכשרה שיש לו משפיעים על הארגון ועל יכולתו להתמודד מול המתקפות". היא ציינה כי מאחר שהמתקפות כיום מתוחכמות, "נוצרת דילמה איך להכשיר את הארגון מול מגוון והמשימות והמתקפות".



עדי רוזה

"על מנת לענות לאתגר של עלות ההכשרות הגבוהה להתמודדות מול איומי הסייבר, חיפשנו דרך אחרת להתמודד עם האיומים והבנו שעבודה של ארגונים עם סימולטור היא הדרך היחידה", ציינה

רוזה. "אנחנו מנגישים את הסימולטור ללקוחות ובכך עונים לצרכי הארגונים". אבנת, אמרה, עובדת עם הסימולטור של התעשייה האווירית, שלתוך מנוע התרחישים שלו הוכנסו תרחישי מתקפות סייבר והדרכים להתמודדות ולהתגוננות מולם. "בדרך זו אנחנו מציעים הכשרה חדשנית וייחודית לארגונים לטובת התמודדות עם מתקפות סייבר", סיכמה.

"חשוב ללמוד ולחשוב כמו התוקפים"



רוני בכר

רוני בכר, מנהל תחום סייבר ותיקפה באבנת אבטחת מידע, הציג כיום שונים לתקיפה של ארגונים, מנוע אירועים ומוצר המאפשר לדמות רשת חיה ותקינה, שלכאורה הכול רץ עליה. בכר אמר, כי "על מנת להתמודד באופן מושכל ויעיל עם מתקפות הסייבר המגוונות והמתוחכמות, חשוב ללמוד ולחשוב כמו התוקפים".

"אנחנו מחפשים נמרים קטנים"

"ד"ר **נמרוד קוזלובסקי**, שותף לחממת הסייבר של קרן JVP, אמר כי "עכשיו זה הזמן לייצר בארץ את הדור הבא של מוצרי הסייבר".

הוא ציין כי קרן JVP הכריזה על תחרות הסייבר סטארט-אפ, שתזכה את המנצח בה בהשקעה של מיליון דולר ובהצטרפות לחממת הסייבר של הקרן בבאר שבע. כמו כן, שלושת המועמדים הסופיים יוזמנו לכנס RSA שייערך בסוף פברואר. בסוף פברואר.



ד"ר נמרוד קוזלובסקי

"JVP היא המשקיעה הגדולה ביותר בתחום הסייבר בישראל. JVP Cyber Labs היא זרוע

ההשקעות שלה בשלב המוקדם בתחומי אבטחת המידע וה-Big Data, שהוקמה בשנה האחרונה במטרה לגלות, לבנות ולהוביל את הגל הבא של חברות הישראליות שפועלות בתחומים אלה", הוסיף ד"ר קוזלובסקי.