כיצד להתמודד עם איומי סייבר בשרשרת האספקה

› ד"ר אורן איתן, מייסד ומנכ"ל חברת הסייבר הישראלית odix

בשנים האחרונות היינו עדים למספר רב של מתקפות סייבר רחבות-היקף שפעלו בווקטור שרשרת האספקה. האחרונה ואולי הבולטת שבהן הייתה התקיפה של SolarWinds. התקפות שרשרת אספקה (או מתקפות צד-שלישי) מאפשרות להאקרים גישה למספר רב של ארגוני מטרה על ידי ניצול נקודת תורפה אחת בלבד, אשר יכולה להימצא אפילו בחברה קטנה שמשמשת רק כספקית ציוד או שירותים של ארגוני המטרה.

אבטחת סייבר לקויה אצל ספקים בשרשרת האספקה עלולה לחשוף כל ארגון לאירועי סייבר חמורים ולנזק כספי ותדמיתי. תקיפה של אחד הספקים יכולה לגרום לאפקט דומינו של מתקפות נוספות שיתפשטו בקרב כלל הגורמים הנמצאים בקשרי גומלין עם הארגון לרבות לקוחות, מפיצים ועוד.

מי חשוף לתקיפות דרך שרשרת האספקה?

למעשה, כל עסק או ארגון הוא חלק משרשרת האספקה אשר מורכבת מהספקים שלו מצד אחד ומלקוחות שלו מצד אחר. חשוב להבין כי שרשראות האספקה אינן תלויות באספקת מוצרים פיזיים בלבד, אלא כוללות מעטפת של העברת מידע ושירותים בין כלל הגורמים המעורבים, באותה מידה כמו לגבי מוצרים. רשתות אספקה גלובליות אחראיות להעברת מיליוני טונות של מטען ומאפשרות לספק מוצרים במהירות ויעילות יוצאות דופן. יחד עם זאת, רשתות אלה של ספקים ושותפים מספקות לפושעי סייבר אינספור נקודות תורפה לביצוע תקיפה אפשרית נגד מערכות קריטיות או נתונים מאובטחים של לקוחות.

בשרשרת האספקה, אתה חזק רק כמו החולייה החלשה ביותר שלך. לכן מאוד חשוב שכל "חולייה" בשרשרת תשקיע את כל מה שנדרש באבטחת סייבר, או שאחרת כל החברות יהיו חשופות לסיכון.

ספרינט או ריצה למרחקים ארוכים?

נהוג לומר על אבטחת סייבר שלא מדובר ביעד שאליו ניתן להגיע, כי אם במסע ארוך שאינו נגמר לעולם. פושעי הסייבר מפתחים ללא הרף טכניקות התקפה ואיומים חדשים, ולכן יש לבדוק ולעדכן באופן קבוע את פרוטוקולי האבטחה.

על מנת להתגונן מפני הסיכונים ההולכים וגדלים, חשוב מאוד להעביר את נטל האחריות על האבטחה גם לספקים ולשאר הארגונים בשרשרת האספקה שלכם. יש לעשות זאת תוך רגישות לתרבות הארגונית ולאמצעים הזמינים בידם, ולהביא בחשבון את נקודות התורפה הספציפיות לתעשייה. מכיוון שאף מגזר אינו מוגן מפני התקפות סייבר, חשוב לשתף את כל הארגונים בשרשרת האספקה במידע על האיומים ועל הצעדים הנחוצים להגנה מפניהם. יש להעניק לדברים את ההקשר הנכון, כדי שכל הצדדים יבינו את רמת החשיבות של הנושא ומה עליהם לעשות, בהתאם למגזר התעשייה שלהם.

צעדים למניעה והתמודדות עם איומי סייבר בשרשרת האספקה:

- להקפיד ולעדכן באופן שוטף את הדרכת העובדים לגבי אבטחת סייבר.
- לאמץ השקפה הוליסטית על שרשרת האספקה ולבחון את מצב האבטחה של שותפים וספקים.
- ליצור תרבות של אבטחת סייבר ברחבי הארגון.

- להכניס את אבטחת הסייבר כשיקול מרכזי בפיתוח יישומים טכנולוגיים מראשיתו (by design) ולא רק בדיעבד.
- להכין מראש תוכניות המשכיות עסקית שיסייעו לבלום ולהגביל את הנזק במקרה של מתקפת סייבר עתידית.
- כדאי לנצל משאבים זמינים, ציבוריים או פרטיים, ולמנף הזדמנויות לשותפות בנושא אבטחת הארגון.
- ניתן לרכוש ביטוח סייבר תוך הקפדה שנוסח הפוליסה תואם את טיב החשיפה של הארגון לאיומי סייבר.

שרשרת האספקה של ארגונים הופכת לדיגיטלית יותר ויותר. מגמה זאת מאפשרת שימוש בשיטות ניהול חסכוניות וממוקדת נתונים, שלעתים מספקות גם יכולות הגנה לעסקים. יחד עם זאת, תהליך הדיגיטציה פותח בפני האקרים מגוון רחב של הזדמנויות חדשות לפריצה או גניבה של נתונים 'מאובטחים', ולכן קריטי שכל הגורמים בשרשרת האספקה יהיו מודעים היטב לסיכוני הסייבר וינקטו בכל צעד אפשרי לצמצום החשיפה בכל מחיר.

ד"ר אורן איתן, מייסד ומנכ"ל חברת הסייבר הישראלית odix

אבטחת סייבר– הופכים מילים למעשים

בכל הנוגע לאיומי סייבר בשרשרת האספקה, אין תחליף לשמירה על ערנות והקפדה על כך שכל השותפים והספקים יהיו מודעים היטב ומוכנים לקראת אירוע סייבר. יש לעבוד בשיתוף פעולה הדוק עם כל הגורמים בשרשרת האספקה, שותפים וספקים כאחד, ליצור מחויבות משותפת לקידום המודעות לאבטחת סייבר, ולדרוש מכל העובדים להפנים ולתרגל סיכוני אבטחה מדי יום. מנהלים שייצמדו לכללים אלה יהיו בעמדה טובה יותר להגן על הארגון באופן פעיל מפני איומי סייבר, ובמקרה של אירוע תקיפה - לבלום את הפגיעה ולצמצם את הנזק שהארגון יצטרך לספוג.

המחבר הוא ד"ר אורן איתן, מנכ"ל חברת odix המפתחת פתרונות אבטחה לנטרול וירוסים ונוזקות מקבצים ארגוניים. ד"ר איתן הוא אל"מ (במיל.) ולשעבר מפקד יחידת מצו"ב בצה"ל.