שרשרת האספקה- הבטן הרכה של ארגונים וחברות

שרשרת האספקה היא מרכיב קריטי בכל ארגון,
אך בנוסף היא גם מהווה כיום נקודת תורפה ביטחונית מרכזית.
סיכוני הביטחון בשרשרת האספקה כוללים מתקפות סייבר,
דליפת מידע, ופעילות שיטוי והונאה.

הנה כמה מהסיכונים המרכזיים:

- ניצול חולשות אצל ספקים כדי לחדור למערכות ותשתיות החברה לפגיעה בהן. מתקפות אלו כוללות חדירה דרך גורמי צד ג', מתקפות כופרה, ודלף מידע רגיש.
- תקיפת ספקים על מנת להדליף או לחשוף מידע רגיש ביטחונית או עסקית, מידע פיננסי ו – IP (גם של אלביט וגם של לקוחותיה).
- פגיעה ברכיבי שרשרת אספקה, אשר עלולה לגרור פגיעה באמינות ובזמינות המערכות והמוצרים, שמיוצרים ומסופקים ללקוחות, על ידי החברה או דלף של מידע ממערכות אלו בעת פעילותן.

עקרונות ביטחון להתמודדות עם סיכוני שרשרת האספקה

הקפדה ו-וידוא כי לספקים וקבלני משנה יועבר רק מידע הנדרש לצורך תפקידם ושאיננו עלול לשמש "משטח תקיפה" של החברה ופעילותיה.

מיפוי וסיווג ספקים וקבלני משנה בהתאם לרמת הסיכון שהם מציבים לחברה ולפעילותה.

ביצוע סקרי ביטחון והערכות סיכונים לספקים וקבלני משנה ובדיקת הבקרות הקיימות אצלם. יש לוודא עמידה בסטנדרטים גבוהים של אבטחת מידע, וקיום נהלים להתמודדות עם איומי ביטחון וסייבר.

מידע ופריטים של מדינות / לקוחות חו"ל המוגדרים כ"מידע רגיש" יועברו רק לספקים וקבלני משנה מאושרים, העומדים בהגדרות הביטחון והציות.

הטמעת טכנולוגיות לניטור פעילות ספקים וזיהוי חריגות בזמן אמת.

חתימה על הסכמי ביטחון וסייבר הכוללים דרישות ברורות לאבטחת מידע ונהלים לדיווח על אירועי סייבר. הסכמים אלו צריכים לכלול סעיפים המאפשרים לארגון לבצע ביקורות תקופתיות אצל קבלני משנה הספקים.

אלביט מערכות
מטה החברה • ביטחון

Elbit Systems
ESOC