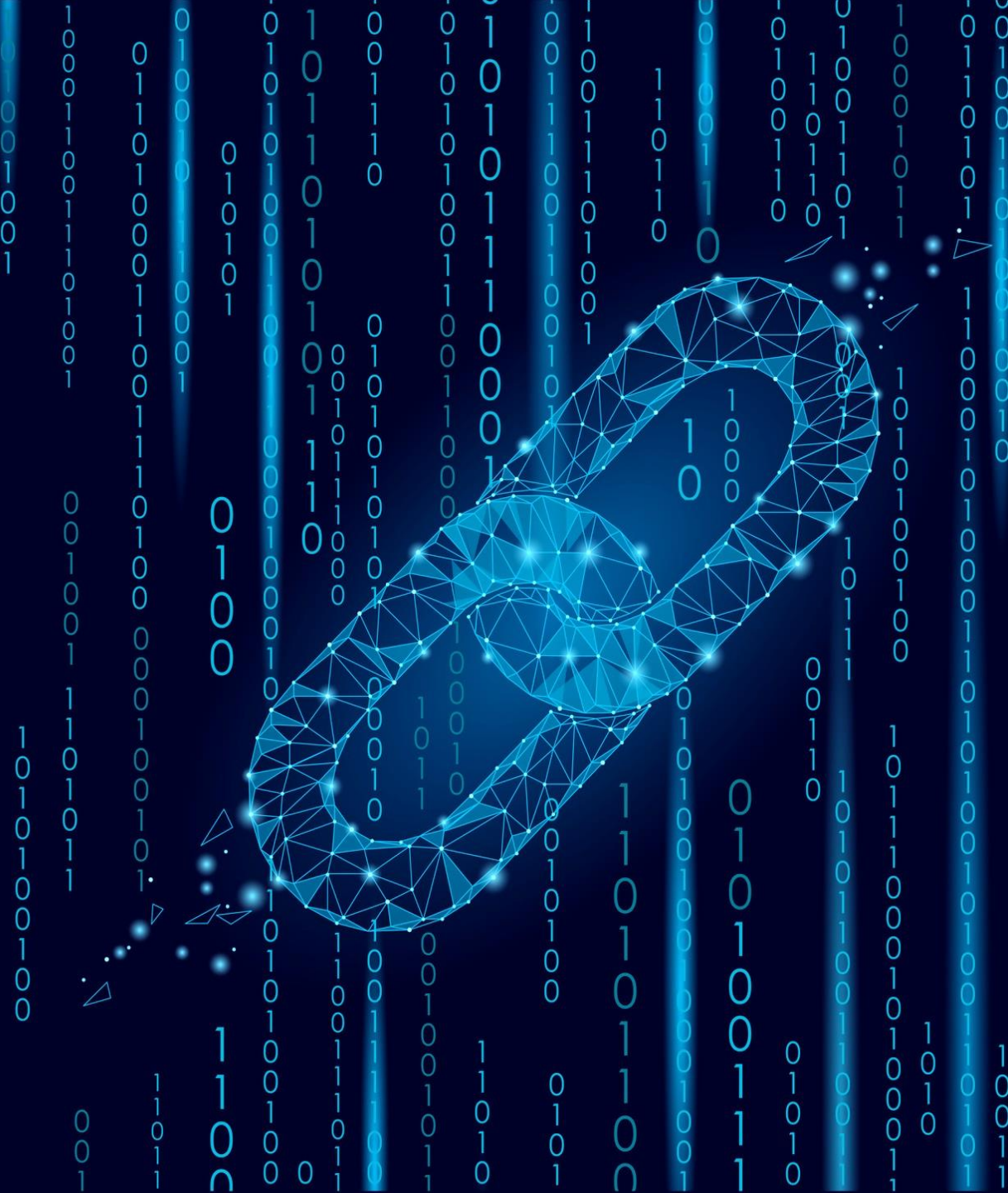


הגנת סייבר כנגד מתקפות שמקורן בשרשרת אספקה

ענת גולדיאן,
רגולציית סייבר



כיצד המעבר לעבודה מרחוק משפיע על אבטחת הארגון?

איפה זה פוגש אותנו?

עבודה מהבית במקום במשרד?

ZOOM עם לקוח מחו"ל במקום פגישה?

שיתוף והעלאת קבצים

עקיפת מנגנוני אבטחה



סייבר ישראל

מערך הסייבר הלאומי

מדוע דרישות הגנת הסייבר מתעשיות ביטחוניות הינן גבוהות יותר בהשוואה לשוק האזרחי?

- נכסי מידע
- נכסים קריטיים
- חיבוריות
- תהליכים רגישים, רכש, ייבוא, ייצוא



אירועי כופרה במספרים

היקף מתקפות הכופר וההשפעה שלהן גדלים בקצב מדאיג וארגונים אינם ערוכים לכך

50%

אחוז המקצוענים בתחום אבטחת הסייבר שאינם מאמינים שארגונם מוכן למניעת התקפת כופר (n = 582)

133,000\$

עלות ממוצעת של מתקפת כופר

14 שניות

ארגון חדש מותקף על ידי תוכנות כופר אחת ל-

97%

במהלך השנתיים האחרונות התקפות כופר עלו ב-

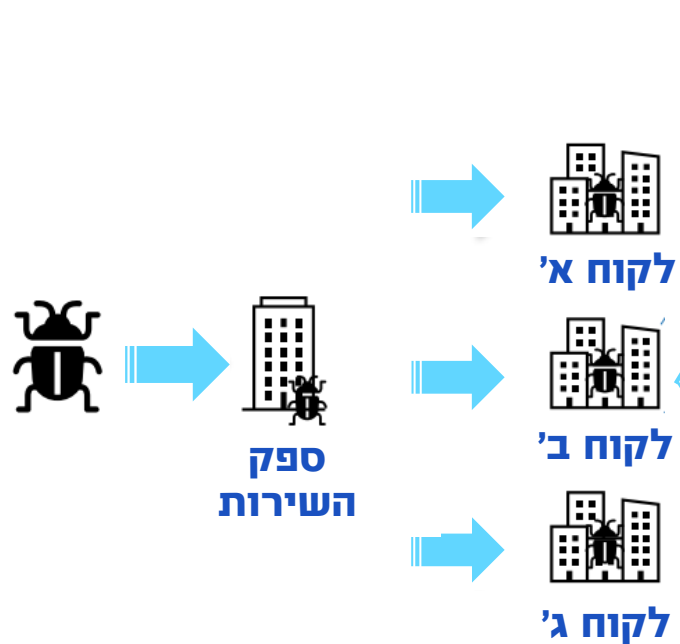


סייבר ישראל

מערך הסייבר הלאומי

עלייה בשכיחות התקפות שרשרת האספקה

משלוח מטעני כופר באמצעות ספקים מהימנים



- תוכנות זדוניות נועלות מערכות ו/או מצפינות נתונים לצורך סחיטה כספית ו/או ריגול ברשת
- תוכנות כופר מתפשטות כמו רוב התוכנות הזדוניות האחרות (לא רק באמצעות מייל דיוג): הורדה לא מכוונת של קוד זדוני למחשב או למכשיר נייד, פגיעויות באפליקציות וכו'. כתוצאה מכך, מניעה יכולה למנף שיטות עבודה מומלצות בתחום האבטחה.
- אחת מהבעיות המרכזיות היא ההפרעה העסקית הנרחבת לכן יש להתייחס לתוכנת כופר כאירוע ביטחוני והתאוששות מאסון (DR) או תקרית בתהליך המשכיות עסקית (BC)

האתגרים במשק הישראלי

כפילות מענים
על שאלונים זהים



קיים קושי לעבוד מול
מאות ואלפי ספקים



לא קיימת מתודה מוסכמת
להגדרת הדרישות
מספקי השירות והמוצרים



הכלים של המערך להתמודדות עם האתגר

על מנת לייעל את תהליך הערכת הסיכונים הארגוני במסגרת רכש שירותים, מערך הסייבר גיבש המלצות לשיטת בדיקה אחידה, המבוססת על:

1. מפרט בדיקות אחיד לספקים

2. מערכת מקוונת

3. רשימת בודקי ספקים

שם מלא	דואר אלקטרוני	טלפון נייד	אזורי פעילות
אבישי רוטשטיין	avirot@outlook.com	050-3546746	כל הארץ
אורן זיטמן	ovitman@kpmg.com		כל הארץ
אירית פוטר	irit.potter@ip-sec.co.il	054-6522550	כל הארץ
איתמר רשף	itamar.r@speant.co.il	052-3878886	כל הארץ
גבריאל פטליס	gavriel.pattis@gmail.com	052-7033888	כל הארץ
ג'ושוע גולדפרב	josh@idra.com	054-2095539	כל הארץ
דודן זילברקלנג	dotan.zilberklang@gmail.com	052-2554166	כל הארץ

4. מאגר לאומי לספקים מאושרים



סוגי התקשרויות



5. אחסון אתרים (Hosting)
נוסף בגרסה העדכנית של השאלון- 1.3



4. גישה מרחוק



3. אחסון מידע בענן



2. פיתוח תוכנה מאובטח



1. דרישות רחביות



אבטחה
פיסית

עמדות
קצה
ושרתים

פרטיות

ניהול
אירועים

גיבוי
ושחזור

ניטור
ובקרה

מיהו ספק מהותי?

ספקי שירותי תמיכה ו/או תחזוקת מערכות מידע,
אחסון נתונים רגישים מחוץ לחצרות התאגיד,
שירותי מיקוד חוץ טכנולוגיים, וכד' (נב"ת 363 ס' 7)
ו/או

ספק מסוג שפגיעה בו עלולה לגרום לנזק מהותי עבור הלקוח

החלטה על הגדרת ספק כמהותי נתונה
לשיקול דעתו של הארגון/ הרגולטור



דרגות הבדיקה וההכרה



A



פלטינה
שאלון &
ראיות &
ביקורת

B



זהב
שאלון &
ראיות

C



כסף
שאלון

תוקף - שנתיים

* בכפוף לחובת תיקוף בתום שנה

תוקף - שנה

תוקף - שנה



סייבר ישראל

מערך הסייבר הלאומי

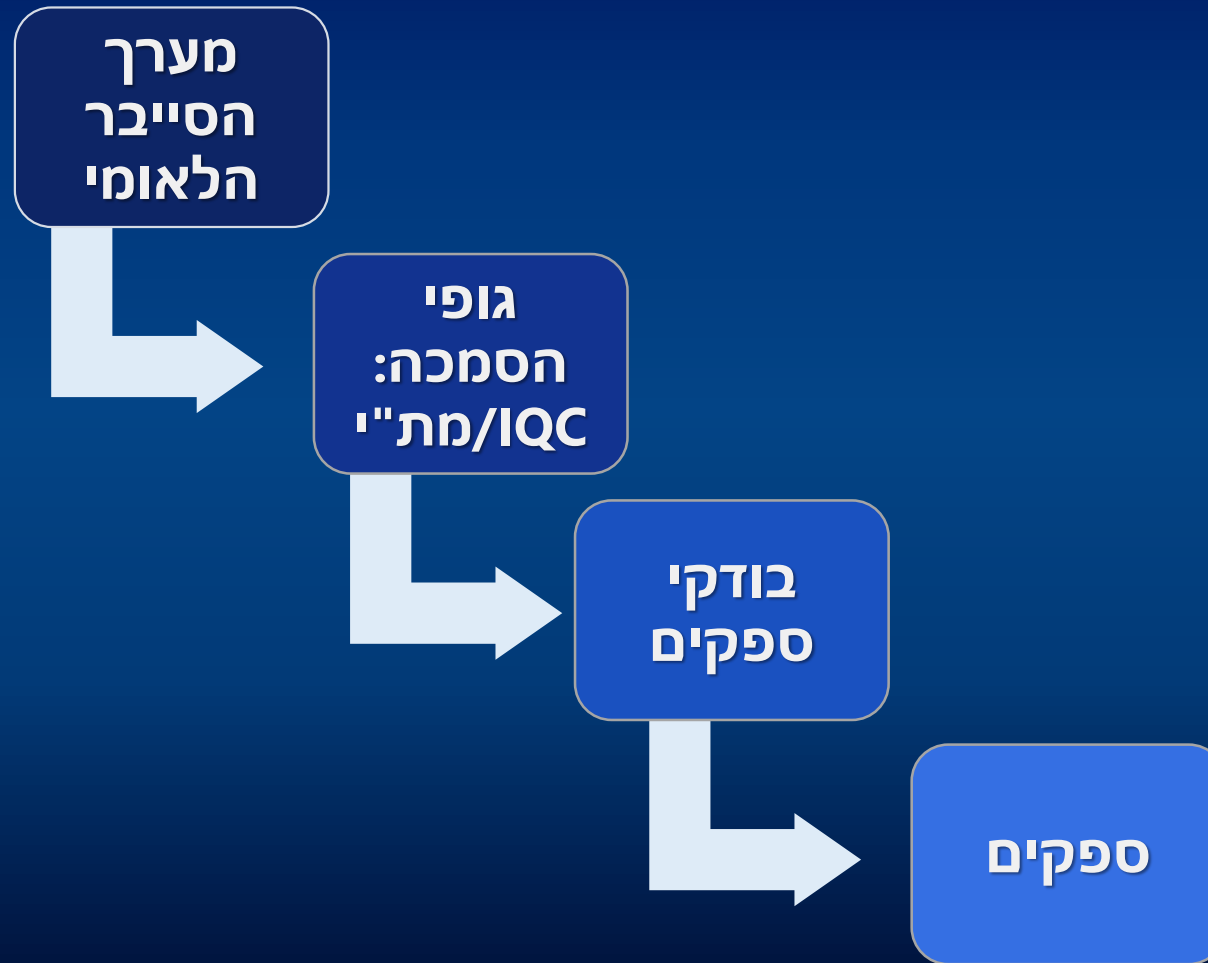
בודקי ספקים - מחזור א'



- ✓ תנאי סף
- ✓ וועדות קבלה
- ✓ תכנית הכשרה מובנית
- ✓ בחינות הסמכה
- ✓ הענקת תעודות
- ✓ פרסום באתר המערך



מודל האסדרה



תמורות עיקריות למשק יתרונות ההסמכה

- הטמעת התהליך תביא להפחתת תקורות לארגון ולספק ולניהול משאבים יעיל
- העלאת רמת המקצועיות בארגון
- מהימנות בבדיקות ההגנה באמצעות קביעת רף מקצועי

יעיל + מקצועי + כלכלי = מאובטח יותר



סטטוס נוכחי במספרים - בודקי ספקים מאושרים



סטטוס נוכחי במספרים - הטמעה בקרב ספקים





סייבר ישראל

משרד ראש הממשלה
מערך הסייבר הלאומי

ענת גולדיאן
Anatg@cyber.gov.il

Join us!

תודה על ההקשבה