

ביטוחי סייבר

עו"ד יגאל שגיא, יועץ לעניני ביטוח
לרשויות מקומיות ולאירגונים

ביטוחי סייבר

- מה זה סייבר - CYBER
- כינוי למרחב הכולל רשתות מחשבים, מערכות תקשורת, מידע ובקרה, וכיוב'
- מונחים והגדרות:
- HACKING – קבלת גישה למחשב למטרת השמדה או גרימת נזק למחשב או תכולתו.
- MALWARE – תוכנה זדונית, שמטרתה לגרום נזק ("נוזקה")
- PHISHING – תקשורת אלקטרונית המתחזה להיות ממקור לגיטימי שמכילה קובץ זדוני או קישור לקובץ או תוכנה זדוניים ("נוזקות"), במסווה אמין.

ביטוח סייבר

"אירוע סייבר" מהו

אירוע שנגרם על ידי HACKING או MALWARE או PHISHING שגרם במערך המיחשוב ו/או מאגר הנתונים של האירגון ל:

א. שינויים בנתונים האלקטרוניים ו/או דיגיטליים באירגון ו/או

ב. מנע מהאירגון לספק שרותים .

ביטוח סייבר

שכתוצאה מהנ"ל נגרמו לאירגון נזקים ו/או הוצאות:

נזק פיזי כתוצאה מאירוע סייבר לרשת תקשורת.
הוצאות לשחזור נתונים עקב השחתה או עיוות של נתונים.

אבדן הכנסה או הוצאות נוספות
או איום בגרימת נזק לצורך סחיטה ודרישת כופר

ביטוח סייבר

מיהם הגורמים לסיכון?

צד שלישי שמטרתו:

ריגול תעשייתי

פשע, גניבה הפקת רווחים אישיים

האקרים (פצחנים) למטרות הנ"ל ו/או
למטרות "מוסריות"

עובדי האירגון הנפגע

ביטוח סייבר

חשיפה לתביעות של צדדים שלישיים בגין:

גניבת נתונים אישיים ועיסקיים של צדדים שלישיים

גניבת תמונות, סרטים, מוזיקה, ספרות וכיוב'
המוגנים על ידי זכויות קניין רוחני, זכויות יוצרים,
פטנטים. ושימוש בהם או העתקתם או הפצתם
בניגוד לזכויות היוצרים של בעליהם, כולל הוצאת
לשון הרע והשמצות

הפצת וירוסים תוכנות זדויות הגורמות לנזקים
לצדדים שלישיים

ביטוח סייבר

- התקפות סייבר נמצאות בין חמשת הסיכונים הגלובליים הגדולים ביותר. (על פי מחקר של הפורום הכלכלי העולמי)
- כ- 2 מיליון ניסיונות תקיפת סייבר ביום על תשתיות קריטיות
- כ- 1,000 התקפות סייבר בממוצע ליום

ביטוחי סייבר

מקרים ידועים בעולם

- התערבות בבחירות 2016 בארה"ב - חדירה למחשבי המפלגה הדימוקרטית - הילרי קלינטון, ושימוש במידע לצורכי תעמולת בחירות כולל הפצת FAKE NEWS

- חדירה למחשבי המודיעין האמריקאי (NSA) והפצת המידע (אדוארד סנואודן)

חדירה לאמצעי השליטה והבקרה של צנטריפוגות באיראן וגרימת נזק כבד ועיכוב בפיתוח הגרעיני.

ביטוחי סייבר

מיחשוב ברשויות מקומיות:

נתונים אישיים של תושבי הרשות המקומית :

- מספרי תעודות זהות, מצב משפחתי (נשוי/אה, רווק/ה, מספר ילדים וגיל הילדים), בתי ספר, גני ילדים, כתובות ונתוני דיור - גודל בית, גודל חלקת קרקע, מספר נפשות הגרים בבית
- נתונים על כרטיסי אשראי, שיקים, חתימות

ביטוחי סייבר

נתונים של עסקים בתחום הרשות המקומית:

- סוג העסק, כתובת העסק, שטחים, מחזורים כספיים,
- כתובות, סניפים, מספר ח.פ. של העסק
- נתונים על כרטיסי אשראי של העסק
- מספרי טלפון, כתובות דואר אלקטרוני,

ביטוחי סייבר

מערכות מיחשוב של רשויות מקומיות:

- מרכזיות טלפון, תקשורת עם תושבים וגורמי חוץ, מערכות הדפסה מרכזיות
- נתוני ארנונה, אגרות, היטלים, מסי השבחה,
- מערכת חשבונות של רשויות מקומיות כולל גביה, קופות, תשלומים ותקבולים, תשלום משכורות, תשלומי ביטוח לאומי

ביטוחי סייבר

שליטה ממוחשבת על מערכות פיזיות ברשות המקומית:

- שליטה על מערכת פינוי אשפה ונקיון
- שליטה על הדלקה וכיבוי תאורת רחוב
- שליטה על רמזורים
- שליטה על כלי רכב של הרשות
- שליטה על קבלני ביצוע
- שליטה על אספקת מים, ביוב, מתקני חימצון, בריכות

ביטוחי סייבר

- תפעול מוסדות עירוניים – בתי ספר, גני ילדים, מוסדות למען הקשיש, מפעלים לנוער, מפעלי ספורט
- רישום לבתי ספר, גני ילדים, מעונות וכיוב'
- תקשורת פנים ברשות, סיכומי ישיבות, מעקב החלטות, התכתבות פנימית, ריכוז נתונים היסטוריים .

ביטוחי סייבר

התקפות סייבר - תרחישים:

תרחיש 1

אין גישה למאגרי מידע של הרשות

מופיעה דרישה על המסך לתשלום כופר בסך
5,000,000 ש"ח

האיום: אם הכופר לא ישולם, כל המידע האצור
במחשבי הרשות יאבד

ביטוחי סייבר

תרחיש 2

הרמזורים בעיר מופעלים ומשותקים לסירוגין

מערכות התקשורת משותקות

המרכזיות יצאו מכלל פעולה

ביטוחי סייבר

תרחיש 3

**מחלקת המיחשוב מגלה כי המערכת
נפרצה**

ונתונים אישיים ועסקיים נגנבו.

ביטוחי סייבר

תרחיש 4

**מערכת התשלומים האינטרנטית חסומה
בגלל מליוני פניות, מערכת הגביה
האינטרנטית משותקת ולא מתבצעים
תשלומים על ידי משלמי ארנונות ומסים או
על ידי משלמי אגרות ומקבלי שירותים**

ביטוחי סייבר

תוצאות:

תביעות צד שלישי:

- התושבים מגישים תביעות נזיקין נגד הרשות המקומית על התרשלות בשמירה על נתונים אישיים ועל פגיעה בפרטיות
- עסקים מגישים תביעות נזיקין על דליפת נתונים עסקיים שלהם למתחרים וגורמים זרים
- מוגשות תביעות נזיקין על אבדן ימי עבודה
- מוגשות תביעות נזיקין על נפילות ופציעות בשטחים ציבוריים וברחובות היישוב המוחשכים

ביטוחי סייבר

תוצאות - המשך

תשלום כופר:

הרשות נאלצת לשלם כופר כדי לשחרר את
המידע האצור במחשביה

ביטוחי סייבר

תוצאות - המשך

גרימת הפסדים כספיים והוצאות לרשות

נגרמים לרשות הפסדים כספיים כבדים בגלל השמדת או שיבוש קובצי הגביה של הארנונה והמיסוי העירוני.

נגרמים לרשות הוצאות כבדות בגלל הפעלת כוח אדם מיוחד לתיקון הרמזורים ולהפעלה ידנית של מערכות ממוחשבות

ביטוחי סייבר

תוצאות - המשך

הוצאות נוספות עקב אירוע סייבר

נגרמות לרשות המקומית הוצאות כבדות של שכירת שירותי מומחים ויועצים לטיפול בתקלות המיחשוב והחזרת המצב לקדמותו.

נגרמות לרשות הוצאות כבדות בגלל הצורך לתת הודעות אזהרה לתושבים על הנזקים העלולים להגרם להם בגלל גניבת נתונים אישיים.

ביטוחי סייבר

הפיתרון הבטיחותי

**יצירת גיבויים מתאימים, התקנת הגנות
כנגד וירוסים וחדירות בלתי מורשות
למחשבים (Firewalls),**

**הנהגת כללי זהירות של התנהגות ברשת
והתייעצות עם מומחי אבטחת מידע.**

ביטוחי סייבר

הפיתרון הביטוחי

עריכת ביטוח סייבר המכסה את הנזקים
האפשריים בעיקבות מתקפת סייבר על
מערכות המיחשוב של הרשות המקומית:

ביטוח נזקים לרשות, וביטוח המגן מפני
תביעות של צדדים שלישיים

ביטוחי סייבר

השתתפות עצמית	סכום הביטוח	תיאור הכיסוי
20,000 ש"ח	5,000,000 ש"ח	נזקים עצמיים: <ol style="list-style-type: none">1. כיסוי בגין אבדן או נזק סייבר לרשות המקומית2. כיסוי בגין "גניבת סייבר" (כספים וטובין)3. כיסוי נזקים תוצאתיים (העדר גביה, גידול בהוצאות תפעול)4. כיסוי בגין סחיטה ותשלומי כופר5. כיסוי הוצאות טיפול בתקיפת סייבר למומחים6. כיסוי בגין הוצאות רגולטוריות

ביטוחי סייבר

השתתפות עצמית	גבול אחריות	תיאור הכיסוי
20,000 ש"ח	10,000,000 ש"ח	כיסויי חבות סייבר כלפי צד שלישי:
	כל הכיסויים נכללים בגבול האחריות הנ"ל	חבות מדיית סייבר
		חבות בגין הפרת זכות לפרטיות
	ההשתתפות העצמית חלה במשותף על כל הנזקים מאירוע סייבר אחד	חבות בגין חדירה למידע של צד שלישי
		הוצאות יחסי ציבור והוצאות הודעה לצד שלישי
		הגנה בהליכים פליליים ומנהליים

ביטוחי סייבר

תנאים לעריכת הביטוח

- מי שרוצה להיות מבוטח ידרש למלא טופס הצעה הכולל פרטים על מערך המיחשוב שלו.
- ידרש חיתום שבו יעריכו המבטחים את רמת הסיכון של האירגון.
- בין השאלות המהותיות תמצאנה השאלות הבאות:
 1. האם כל הנתונים האישיים השמורים בכל מערכות המידע שברשותך מוצפנים
 2. האם קיים גיבוי, לפחות שבועי, לכל הנתונים
 3. האם קיימת תוכנת אנטי וירוס על כל המערכות
 4. האם קיימת תוכנית מסודרת להתמודדות במקרה נפילת מערכת (DRP) (Disaster Recovery Plan) ?

ביטוחי סייבר

תודה על ההקשבה