מדנס SM

סוכנות לביטוח בע"מ

בריאות | חיים | חבויות | רכוש | פנסיוני

מדנס סוכנות לביטוח בע"מ | רח' השלושה 2 תל אביב | טל: 03-6380000 | פקס: 03-6380385 | www.madanes.com

ביטוח סייבר
מאת: בן ברק, עו"ד
חטיבת עסקים

על מה נדבר

1. מהו סיכון סייבר?
2. מהו הנזק הפוטנציאלי?
3. האיומים המרכזיים
4. למי רלוונטי ביטוח סייבר?
5. פוליסת סייבר
6. סיכום

מהו סיכון סייבר:

- ✓ סיכונים הנובעים מחשיפת המחשב לרשת אינטרנט
- ✓ לדוגמא: מתקפה זדונית, חדירת האקרים, טעות אנוש (שליחת מייל לכתובת שגויה)
- ✓ **החשש - שימוש במידע ללא אישור ולא למטרה שלשמה הוא נאסף.**

מהו סיכון סייבר:

- ✓ רוב המידע של תאגידים - שמור באופן דיגיטאלי - "מאגר מידע"
- ✓ למידע (פרטי/מסחרי) - ערך רב כלכלי/אישי

קיים אינטרס ברור באיסוף ובשמירת מאגרי מידע.

- ✓ **המטרה במתקפת סייבר:** שיבוש, השבתה, הרס, שליטה על סביבת מחשוב ותשתיות – פגיעה בחיסיון או בשלמות המידע

מהו הנזק הפוטנציאלי ?

נזקים לצד א'

- אובדן הכנסה
- שחזור מידע
- פגיעה במוניטין
- דמי כופר
- הוצאות משפטיות
- הוצאות בגין תיקון נזקים
- אבדן מידע/גניבת זהות
- עלויות הודעה לצדדים ג'+ משרד יחסי ציבור

נזקים לצד ג'

- פגיעה במוניטין
- נזקים פיננסיים
- הוצאות משפטיות
- הוצאות בגין תיקון נזקים
- שחזור ואבדן מידע- כתוצאה מזליגת המידע
- פגיעה בקניין רוחני

האיומים המרכזיים:

כשל אבטחת מידע

כשל מערכות/ פריצת אבטחה למערכות המחשב של החברה

- סייבר טרור / חדירה זדונים
- השבתת תשתיות מחשב
- סחיטת סייבר

כשל מערכות

טעות, השמטה של עובד חברה - הפעלה של מערכות מחשב

- עדכון גרסאות
- שדרוג מערכות
- כשל במרכיבי חומרה

ספקים

- שירותי ענן
- מרכזי נתונים – Data Center
- קבלני משנה

- כשל מערכתי
- אובדן מידע

למי הביטוח רלוונטי? קצת נתונים...

8 מכל 10 חברות חוו מתקפת סייבר בשנתיים האחרונות

34% מהעסקים שנשענים על "שירותי אירוח תוכנות", נפרצו

נכון לשנת 2016 – מתקפת סייבר נחשבת לאחד מ- 10 הסיכונים המשמעותיים ביותר

80% מהעסקים הקטנים שמשתמשים ברשתות החברתיות ככלי שיווק, נפגעו

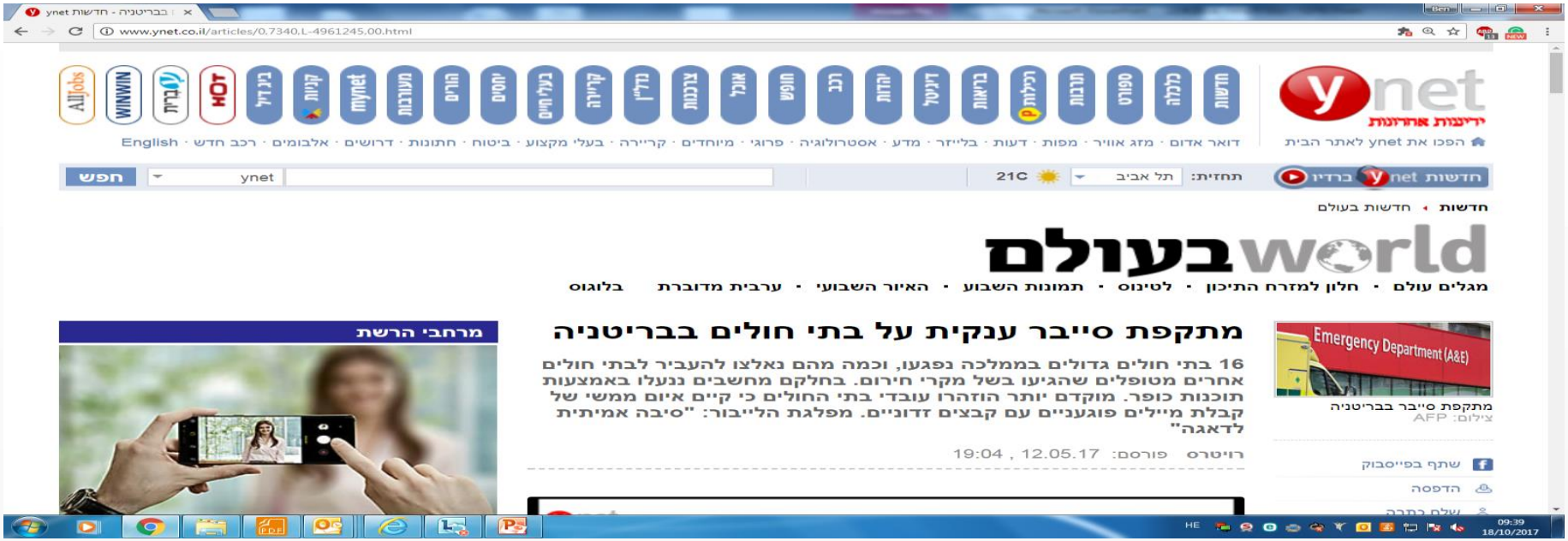
כ- 60% ממתקפות הסייבר בעולם היו על עסקים עם פחות מ- 250 עובדים

למי הביטוח רלוונטי?

1. חברות טלקום
2. חברות עם פעילות בחו"ל
3. חברות תשתיות
4. מוסדות אקדמאיים
5. מוסדות רפואיים
6. מוסדות פיננסיים
7. מלונות תיירות ונופש

כל עסק המחובר לאינטרנט – המחזיק נתונים ומידע

בכותרות לאחרונה:



ביוני 2017 – מתקפת סייבר עולמית – משרדי ממשלה, נמל תעופה וחברות הותקפו מרכז ההתקפה באוקראינה

המודיעין הרוסי פרץ למיילים של ועידת המפלגה הדמוקרטית – הילארי קלינטון

אתר הבגידות לאשלי מדיסון נפרץ – האקרים סוחטים את מנויי האתר

פוליסת סייבר

2 המטרות העיקריות של הפוליסה-

1. לכסות תביעות של צד ג׳ בשל אובדן או הפרת מידע/קניין רוחני
2. לשלם הוצאות ונזקים **<u>של המבוטח (צד א׳)</u>** כתוצאה מאירוע סייבר.

במסגרת הפוליסה ניתנים - שירותי ייעוץ למבוטח לפני האירוע, תוך כדי האירוע ולאחריו

המטרה לנהל את המשבר (חס וחלילה) בהצלחה ולמזער נזקים.

<u>בפוליסת סייבר יש 3 שלבים עיקריים :</u>

התנהלות לפני האירוע, התנהלות בעת אירוע, חזרה לשגרה

שלב 1: התנהלות לפני האירוע – בחינה והערכת סיכון המבוטח (מערכות ההגנה הקיימות, מדיניות הסיסמאות, סוג הפעילות והמידע שקיים בעסק וכו').

פוליסת סייבר

שלב 1: כהתנהלות מונעת מומלץ לבצע (לפני אירוע) :

- הדרכות תקופתיות לעובדים בנושא סייבר ואבטחת מידע
- מבחני חדירות לרשת הארגונית
- התקנת מערכת לניטור כתובות IP חשודות
- ביצוע סקרי סיכונים בנושא אבטחת מידע

פוליסת סייבר המשך

שלב 2: התנהלות בעת אירוע סייבר- אירוע חירום וניהול המשבר - המטרה להבין **מה קרה?**

- **<u>בתחום הטכנולוגי</u>**: המטרה - להשיב את החברה לפעילות שוטפת כמה שיותר מהר; תוך מזעור נזקים.

- **<u>בתחום המשפטי</u>**: **המטרה- דיווח הנכון לגורמי חוץ בדגש על לקוחות, רגולטור וצד ג' אחר**

- **<u>בתחום השיווק:</u>** התמודדות עם התקשורת ולקוחות- יחסי ציבור.

שלב 2: התנהלות בעת אירוע סייבר- מה הפוליסה מכסה?

שירותים מיידים בזמן אמת לטיפול באירוע:

- כיסוי הוצאות ועלויות לתמיכה וייעוץ משפטי ראשוני
-
- ייעוץ וליווי טכנולוגי ראשוני ומידי
- ייעוץ תקשורתי לניהול המשבר התדמיתי

שלב 2: התנהלות בעת אירוע סייבר- מה הפוליסה מכסה?

<u>שירותים מתמשכים</u> לאחר תחילת האירוע:

- בדיקת החשיפה המשפטית
- שיקום טכנולוגי – השבת המצב לקדמותו

פוליסת סייבר המשך

שלב 3: חזרה לשגרה - לאחר שהחברה חזרה לעבוד באופן תקין יש לבצע:

- הסקת מסקנות
- קבלה וביצוע של תשלומים לנותני השירות השונים
- כימות הנזק שנגרם (מוחשי ולא מוחשי)

שלב 3: חזרה לשגרה – מה הפוליסה מכסה?

אספקת שירותי IT שירותי ייעוץ טכנולוגי, הכוללים:

- חקירת האירוע והנזק שנגרם למידע
- הסרת התוכנה הזדונית
- טיפול במניעת גישה וההפרעה לרשת הארגונית
- תשלום הוצאות שיחזור מידע ועלויות המידע שאבד

שלב 3: חזרה לשגרה – מה הפוליסה מכסה?

הגנה על מוניטין:

- תשלום הוצאות ייעוץ תדמיתי ושירותי יחסי ציבור
- תשלום הוצאות בקרת אשראי לניטור ומניעת שימוש בכרטיסי אשראי או בזהות גנובה

שלב 3: חזרה לשגרה – מה הפוליסה מכסה?

- תשלום קנסות ברי ביטוח אשר הוטלו בעקבות חקירה

תשלום תביעות של צד ג':

- תשלום תביעות והוצאות הגנה
- תביעה של צד ג' בגין אי עמידה בחובת דיווח (הרגולטור/בעל המידע)

מה הביטוח לא מכסה?

- ✓ הפרת חוקי הגבלים עסקיים
- ✓ התחייבות חוזית
- ✓ הפרת פטנטים
- ✓ נזק פיזי לגוף או לרכוש

הרחבות חשובות בפוליסה

- Network Interruption - אובדן הכנסות בעקבות פגיעה עד מקסימום של 120 ימים

- כיסוי בגין סחיטת סייבר- פיצוי בגין כספים ששולמו בעקבות איום וסחיטה

- כיסוי לסייבר טרור

- כיסוי לפעילות Outsourcing -שירותי חוץ (**שירותי ענן, טאבלטים, סמארטפונים**)

לסיכום

<u>"אל תגידו לי זה לא יקרה" סיכוי גבוה להתממשות לאירוע סייבר</u>

מגוון גדול של נזקים ישירים – גניבת מידע, שיבוש מידע וכו'...

נזקים עקיפים- פגיעה במוניטין, פגיעה בשווי התאגיד, אבדן הכנסות

דרכי התמודדות – תכניות הגנה לפני אירוע, גיבויים ורכישת ביטוח כאמצעי להעברת הסיכון.

לסיכום

בראש רשימת המגזרים הנפרצים ביותר:

המגזר הרפואי עם כ-21%

המגזר הפיננסי עם כ- 17%

המגזר הקמעונאי עם כ-13%

לסיכום

<u>הסיבות העיקריות לפריצה או פגיעה במאגרי מידע הן</u>:

1. פעולות של האקרים - מטעמים אידאולוגיים או כופר כ- 31%.
2. תוכנות מזיקות - וירוסים כ- 14%.
3. טעויות של עובדים, או רצון שלהם להתנקם במעסיק כ- 11%.

תודה על ההקשבה