בס"ד

TOP 60 IN 60 MINUTES

אירועי אבטחת מידע וסייבר מהעולם – סיכום שנתי 2014

אירועי אבטחת מידע וסייבר מרכזיים- דצמבר:

1. נחשף מבצע של האקרים איראניים כנגד **מטרות אמריקאיות** שנמשך כבר כשנתיים ובו הצליחו לחדור **למערכות הרגישות ביותר** כגון: מערכות תעופה, יצרני מכוניות, חברות גז ויצרני מערכות צבאיות. המבצע זכה לשם **"Cleaver"** והחודש ראינו שחברה ביטחונית נוספת בשם **KeyPoint** נפרצה ונגנבו פרטיהם של **40,000** עובדים ביטחוניים.

2. שרתי ה-DNS של חברת "**Dnsimple**" סובלים ממתקפת DDOS ממושכת בנפחים גבוהים של **25 Gb/ps** וגורמים לשיבושים בהפניות רבות ברחבי האינטרנט.

3. המגזין "פורבס" מפרסם נתונים מפריצה נוספת לחברת **"סוני"** שהתרחשה בינואר ולא דווחה, בה נגנבו פרטיהם של כ- **50,000** לקוחות מהאתר sonypictures.de

4. נחשפה תקיפה בהיקף ענק שניצלה פגיעות בתוסף "Slider Revulotion" שנמצא בשימוש נרחב באתרי **"Wordpress"** ברחבי העולם **100,000** אתרים נפרצו ושימשו להפצת תוכנה זדונית שמקורה הייתה בדומיין ברוסיה בשם SoakSoak.ru.

5. תקיפה חסרת תקדים על תשתיות האינטרנט ב**צפון קוריאה** גורמת **לנפילת האינטרנט בכלל המדינה**. גורמים בממשלה האשימו את ארה"ב שביצעה זאת כנקמה על הפריצה הגדולה ל-"**סוני**" בה הודלפו סרטיים הוליוודיים שעוד לא הוקרנו באינטרנט ושם נטען שצפון קוריאה הייתה אחראית לכך. עם זאת קבוצה בשם **Gator League** שמשויכת לאנונימוס לקחה את האחריות על התקיפה.

אירועי אבטחת מידע וסייבר מרכזיים- נובמבר:

1. שרתים פרטיים של **שרות הדואר בארה"ב** (**USPS**) נפרצו ובעקבות כך נגנבו פרטיהם האישיים של כ- **800,000** עובדי החברה (כולל מספרי ביטוח לאומי) והשרתים הושבתו לזמן מה. לפי חקירת ה-FBI מקור התקיפה הוא בסין. כמו כן נפרץ גם מוקד טלפוני של החברה וממנו נגנבו פרטי לקוחות שיצרו קשר עם החברה בין ינואר לאוגוסט. לטענת החברה לא נגנב מידע שהכיל פרטי חיוב.

2. חברת הפקת הסרטים של **"סוני"** (**Sony Pictures**) נפרצה ע"י מי שנחשדים כהאקרים סיניים שהתחזו לצפון קוריאניים והביאו לקריסת מערכותיה של החברה. בשרתיה הפנימיים של סוני הופיע כיתוב ושעון עצר עם איום להפצת מידע רגיש של החברה אם ימולאו דרישות הפורצים. כמו כן הופצו סרטים חדשים של החברה ברשת והביאו להפסדי עתק המוערכים בכ- **$200,000,000** עד כה. הטענה הרווחת שהפריצה הגיעה בעקבות סרט קומדיה בו יש נסיון להתנקש במנהיג צפון קוריאה.

3. חברת ההחזקות **"HSBC"** העולמית הודיעה שהמערכות של החברה בסניף טורקיה נפרצו ונגנבו מהם פרטי האשראי ופרטים אישיים של **2.7 מליון** לקוחות. בהמשך התגלה כי גם פרטי חשבון הבנק של הלקוחות נגנבו.

4. האקרים טורקים מקבוצת "Red Hack" פרצו למערכת ניהול הלקוחות המקוונת של **רשות החשמל הטורקית** ומחקו חובות בשווי **$650,000** שהיו שייכים למחוז סומה בטורקיה.

5. **משרד המסחר והתעשייה הפיליפיני** נפרץ ע"י האקר המשייך עצמו לקבוצת "**אנונימוס**" שהצליח לגנוב יותר מ- **1900** שמות משתמשים וסיסמאות באמצעות Sql Injection . לאחר מספר ימים בוצעה תקיפה נוספת כנגד מספר אתרים ממשלתיים שהושחתו ע"י אותו גורם. התקיפות בוצעו כמחאה על אופן טיפול הממשלה ופעולות החילוץ באסון סופת "יולנדה" .

<u>אירועי אבטחת מידע וסייבר מרכזיים- אוקטובר:</u>

1. תוכנה זדונית בשם **"Tyupkin"** נחשפת ע"י מעבדות **"קספרסקי" והאינטרפול** וביכולתה להעניק שליטה מרחוק לתוקף על כספומטים. לפי ההצהרה בדו"ח המשותף נמצאו מעל ל-**50 כספומטים** ברחבי **רוסיה** ומזרח אירופה הנגועים בתוכנה הזדונית ומהם נגנב סכום העולה על **$30,000,000**

2. שירות איחסון הקבצים הפופולרי – **"Dropbox"** סופג פגיעה קשה בה **7,000,000** חשבונות משתמשים וסיסמאות נגנבים ומופצים ברשת. נציגי החברה מסרו הודעה בה הם טוענים שהנתונים נגנבו ממקור אחר ולא משרתי החברה.

3. חברת הטלוויזיה הדרום-קוריאנית **"Pandora TV"** נפרצת פעמיים ולאחר ביצוע ניתוח התקיפה הסתבר כי **7,500,000** רשומות של מידע אישי נצפו ולפחות **115,000** רשומות נגנבו.

4. מטרות **ישראליות** רבות הותקפו ובהן **50** אתרים ממשלתיים ו-**970** אתרים שונים. האתרים הותקפו ברובם במתקפות מניעת שירות והשחתת אתרים ע"י קבוצות שונות המשתייכות לאנונימוס כגון: **AnonGhost** וזאת כמחאה על הרג עוֹרְוֶוֶה חמאד ע"י כוחות הביטחון.

5. חברת "**Drupal**" המספקת פלטפורמה לניהול תוכן WEB מדווחת שקרוב ל-**1,000,000** אתרים המשתמשים במערכת שלה הותקפו תוך כמה שעות לאחר פירסום פירצת אבטחה באופן פומבי (CVE-2014-3704)

אירועי אבטחת מידע וסייבר מרכזיים- ספטמבר:

1. ארבעה גברים בגילאים 18-28 (Nathan Leroux, Sanadodeh Nesheiwat David Pokora, Austin Alcala) הורשעו בחברות באירגון פשיעה אינטרנטי ובביצוע פריצות ל**צבא ארה"ב**, **"Microsoft"** ויצרני משחקים שונים. בפריצות אלו נגנב מידע בשווי של יותר מ- **$100,000,000**

2. חברת התעופה היפנית "**Japan Airlines**" מדווחת על כך שחוותה מתקפת סייבר בה הודלפו נתוניהם האישיים של **750,000** לקוחות. המתקפה זרעה בהלה בקרב הלקוחות שחששו מגל של גניבת זהויות. החברה סירבה לדווח אם נגנבו גם פרטי אשראי במתקפה זו.

3. **הסנאט האמריקאי** פרסם דו"ח חקירה בו הוא חושף הוכחות ש**ממשלת סין** אחראית לפריצות מרובות כנגד **יצרנים ביטחוניים** אמריקאיים. נחשף למשל כי מערכותיהם של קבלנים שונים שעבדו יחד עם חיל התובלה האמריקאי נפרצו כ- **50** פעמים בתקופה של 12 חודשים בשנים 2012-2013.

4. **הבית הלבן** מדווח לעיתון ה-"**וול סטריט ג'ורנל**" שהאקר הצליח לפרוץ לאתר הממשלתי **Healthcare.gov** ולגנוב מידע אישי ורגיש של כ-**40,000,000** אזרחים אמריקאיים.

5. רשת "**Home Depot**" מאשרת שהאקרים הצליחו לחדור למערכות התשלום שלה, הפרוסה בכ-2,200 סניפים ברחבי ארה"ב וקנדה. לפי דיווחי החברה-בפריצה זו נגנבו **56,000,000** כרטיסי אשראי.

אירועי אבטחת מידע וסייבר מרכזיים- אוגוסט:

1. דליפות רבות של **תמונות אישיות של מפורסמים** כגון: ריאהנה, קים קרדשיאן, סלינה גומז, סקרלט ג'והנסן ועוד רבים נוספים מופצות ברחבי האינטרנט. את ההדלפה מייחסים לפריצה לשירותי **"iCloud"** של חברת "אפל" וניצול של מנגנון שיחזור הסיסמא להשגת שליטה מלאה על חשבונות אישיים של מפורסמים.

2. הרשויות ב**דרום קוריאה** חושפות פריצת ענק שבה קבוצת האקרים לא ידועה הצליחה לגנוב **220,000,000** רשומות המכילות מידע אישי ורגיש של **27,000,000** אזרחים בגילאי 15-65.

3. האירגון הרפואי הענק "**Community Health Care**" המתפרש על פני 29 מדינות בארה"ב מכריז שהאקרים סיניים בעלי מניע כספי הצליחו לחדור למערכותיו ולגנוב מידע אישי ורגיש של **4,500,000** מטופלים כולל מספרי ביטוח לאומי (SSN).

4. חברת "**Hold Security**" חושפת את המאגר הגדול ביותר של סיסמאות ומשתמשים גנובים שנתגלה אי פעם המכיל בתוכו **1,200,000,000** רשומות. ורשימה נוספת המכילה **500,000,000** כתובות אי-מייל שנאספו ע"י קבוצה הנקראת **CyberVor** באמצעות מתקפות SQLi שבוצעו כנגד **420,000** אתרי אינטרנט ושרתי FTP.

5. אתר הדרושים הישראלי **Zerem.co.il** נפרץ ע"י קבוצת האקרים איראניים הקוראת לעצמה **ICRG** כהמשך למבצעי #OpSaveGaza המתמשכים. כתוצאה מהתקיפה נגנבו פרטיהם האישיים של **70,000** משתמשים.

<u>אירועי אבטחת מידע וסייבר מרכזיים- יולי:</u>

1. הכתב בריאן קרבס מפרסם כתבה על פריצה מתוחכמת שבוצעה כנגד 3 חברות ביטחוניות ישראליות שאחראיות לפיתוחה של מערכת "**כיפת ברזל**". בתקיפה זו נגנבו מסמכים סודיים רבים הנוגעים למערכת ע"י קבוצת תוקפים הידועה בשם "**Comment Crew**". *** כמו כן באותו חודש אתרים ישראליים רבים כגון אתר המוסד, בנק ישראל, משרד החינוך, משטרת ישראל, MSN ישראל (השחתת האתר ע"י קבוצה טורקית) ועוד סובלים ממתקפות רבות במסגרת מבצע **#OpSaveGaza.** מספר ימים קודם לכן נפרץ חשבון הטוויטר של צה"ל ע"י קבוצה הקוראת לעצמה **Syrian Electronic Army** ש"צייצה" ל- **300,000** העוקבים כי קיימת סכנת קרינה גרעינית באזור המרכז.

2. האקר רוסי הקורא לעצמו **W0rm** פרץ לאתר החדשותי של חברת **CNET**, גנב פרטים של מעל ל- **1,000,000** משתמשים ואיים לפרסם אותם אם לא ישלמו לו כופר על סכום זעום של ביטקויין אחד (בשווי 400 $ בערך).

3. מחלקת המשפטים האמריקאית הודיעה שהיא תובעת את איש העסקים הסיני **סיו בין** על כך שפרץ למערכות המיחשוב של "**בואינג**", "**לוקהיד מרטין**" וחברות תעופה נוספות והצליח לגנוב מסמכים סודיים ו**תוכניות מפורטות של מטוסים**.

4. משטרת **ניגריה** חשפה הונאת ענק בהיקף של **$12,000,000** לאחר שהתברר שהאקרים פרצו לבנק באוגון העוסק בתחום המשכנתאות ונמצא בבעלות המדינה והצליחו לבצע העברות כספים לא חוקיות.

5. חוקרים מחברת "**RSA**" חושפים פרטים על בוטנט בהיקפים עצומים. באמצעות מתקפות Man-In-The-browser התוקפים הצליחו לגנוב סכום עצום של **$ 3,750,000,000** כשיירטו העברות בנקאיות שבוצעו באמצעות בולטו (Boleto) - שירות העברת כספים הנפוץ ביותר בברזיל (בדומה ל- Westren Union).

אירועי אבטחת מידע וסייבר מרכזיים- יוני:

1. הרשויות **במונטנה** שולחים הודעות ל- **1,300,000** אזרחים ומיידעים אותם על כך שפרטיהם האישיים נגנבו ככל הנראה, במתקפת סייבר שבוצעה כנגד שרתי משרד הבריאות.

2. קבוצת האקרים העונים לשם **Rex Mundi** מצליחה לפרוץ לשרתי רשת הפיצה **"Domino's Pizza"** בצרפת ובבלגיה ולגנוב פרטים של **592,000** לקוחות מצרפת ו- **58,000** לקוחות מבלגיה. הקבוצה ביקשה כופר בתמורה למידע.

3. הרשת החברתית **"Twitter"** סופגת מתקפת XSS קשה בה לפחות **85,000** משתמשים "צייצו" מחדש לכל העוקבים שלהם הודעה שהכילה קוד זדוני המנצל חולשה באפליקציית **TweetDeck**. הקוד הופץ במהירות עצומה כך שבתוך כמה שעות נפגעו מיליוני משתמשים. לדוגמא: חשבון טוויטר בודד כגון זה של רשת ה-BBC שלח את ההודעה ל- **10,100,000** משתמשים וכך הרשת החברתית כולה הייתה בסכנה.

4. חברת אבטחת המידע **"ESET"** מדווחת שפורום האבטחה שלה נפרץ ונגנבו פרטים אישיים וסיסמאות של **2,700** מהמשתמשים בפורום. כמה ימים קודם לכן, 4 אתרי החברה בגרסה הספרדית הושחתו ע"י האקר המכנה עצמו **Hmei7**.

5. חשבון הפייסבוק של להקת הרוק **"Linkin Park"** נפרץ ושלח הודעות ספאם עם תמונות בוטות ולינקים שונים ל- **65,000,000** המעריצים של הלהקה.

אירועי אבטחת מידע וסייבר מרכזיים- מאי:

1. **מלחמת הסייבר בין הודו לפקיסטן** נמשכת ותקיפות רבות מבוצעות משני הצדדים על מגוון מטרות למשל:
* אתר הטאג' מאהל מושחת ע"י האקר המכנה עצמו **H4$N4!N H4XOR** ובאתר הופיע דגל פקיסטן.
* האקר פקיסטני המכנה עצמו **rOOX** משחית את **47** אתרי משרד הרכבות וגורם לשיבושים בתחבורה.

2. לפי דיווחי ה**מכון למחקר המים והאטמוספירה בניו זילנד** האקר סיני ביצע מתקפה מתוחכמת וממוקדת נגד מחשב-העל שבבעלות המכון ששוויו **$12,700,000** ומצליח להשתלט עליו.

3. פורום התמיכה של חברת אבטחת המידע **"Avast"** נפרץ והפורצים מצליחים לגנוב **400,000** שמות משתמש, סיסמאות וכתובות מייל.

4. אתר המסחר האלקטרוני **"E-bay"** מדווח כי אחד ממסדי המידע שלו שהכיל פרטים אישיים של **145,000,000** משתמשים נפרץ במהלך החודשים פברואר-מרץ , למרות שלא נראה שבעקבות הפריצה בוצעו פעולות לא חוקיות באתר המסחר, החברה שלחה ללקוחותיה הודעה המחייבת שינוי סיסמא לכניסה לאתר.

5. חברת התקשורת **"Orange"** מדווחת כי שרתי החברה בצרפת נפרצו ופרטיהם של **1,300,000** לקוחות צרפתיים נגנבו ע"י פריצת למערכת השירות האישי באתר.

<u>אירועי אבטחת מידע וסייבר מרכזיים- אפריל:</u>

1. חברת האינטרנט **"AOL"** נופלת קורבן לתקיפה שבה נגנבים פרטי ההתחברות למייל של **50,000,000** משתמשים . לאחר גילוי הפריצה החברה הפצירה במשתמשים להחליף סיסמאות בהקדם האפשרי.

2. **המכון למחקר החלל בגרמניה** שנמצא בקולגן , נופל קורבן למתקפה מתוחכמת וממוקדת. מידע רב נגנב ונגרם נזק למערכות. לפי דו"ח של המגזין "**דר ספיגל**" המתקפה מומנה ובוצעה ע"י **ממשלת סין**.

3. חברת החדשות **"רוייטרס"** מדווחת שהאקרים הצליחו לגנוב **200,000** כרטיסי אשראי דרום-קוריאניים, לשכפל אותם ולגנוב **$115,000** באמצעותם.

4. מחלקת הכספים באקדמיה הבריטית על שם "**אלדהלם**" נפלה קורבן למתקפת Spear-Phishing בה גרמו לעובדים לחשוב שהמייל מגיע מהבנק של האקדמיה וכתוצאה מהמתקפה נגנבו מהם **$1,700,000.**

5. הרשויות בגרמניה מאשרות שמתבצעת חקירה בעקבות מתקפה שבה נגנבו **18,000,000** חשבונות מייל וסיסמאות של חשבונות השייכים **לספקי האינטרנט** במדינה.

<u>אירועי אבטחת מידע וסייבר מרכזיים- מרץ:</u>

1. קבוצת האקרים רוסית הקוראת לעצמה **"Rucyborg"** פורצת למחשבי השגרירות הסינית במוסקבה ומדליפה מסמכים סודיים המעידים כי **סין** סיפקה ל**רוסיה** ציוד על מנת לרגל אחר חברת התקשורת האוקראינית **"Intertelecom"**. כחלק מאותה תקיפה הקבוצה גם הדליפה את פרטיהם של **100,000** לקוחות החברה האוקראינית.

2. בעקבות חדירה של תוכנה זדונית דלפו פרטיהם האישיים של **550,000** לקוחות ועובדים מרשת המשקפיים הענקית **"Spec's"** לאחר חקירת האירוע התברר שהתקיפה נמשכה כבר משנת 2012.

3. גבר בן 31 נעצר בקוריאה לאחר שחדר לכ- **25,000,000** חשבונות בפורטל האינטרנט הגדול בקוריאה- **"Naver"**. לפי נתוני חקירת המשטרה החשוד רכש את המידע מאדם אחר ממוצא סיני-קוריאני.

4. ממשלת דרום קוריאה פתחה בחקירה לאחר שנתגלתה פריצה גדולה נוספת ופרטיהם של **12,000,000** לקוחות נגנבו מחברת התקשורת הקוריאנית **"KT Corp."**

5. צוות מחקר האינטרנט ואבטחת המידע **"Team Cymru"** חושף פרטים על תקיפת DNS Hijacking ענקית שבה **300,000** ראוטרים הותקפו וביצעו הפניות לא חוקיות לאתרים.

אירועי אבטחת מידע וסייבר מרכזיים- פברואר:

1. קבוצת ההאקרים הידועה בשם **The Syrian Electronic Army** פורצת לשרתי **"Forbes"** גונבת מידע של משתמשים ואף מפרסמת סיפורי חדשות מזויפים. ממערכת "Forbes" נמסר כי אכן בוצעה פריצה ונגנבו מידע אישי וסיסמאות של **1,000,000** משתמשים.

2. האתר הידוע **"Kickstarter"** המשמש כפלטפורמה למימון המונים, מפרסם פרטים אודות פריצה לשרתי החברה. בפריצה זו נגנבו פרטים אישיים וסיסמאות של **5,600,000** משתמשים.

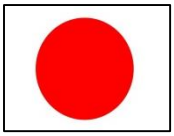
3. חברת **"CloudFlare"** המספקת שירותי DNS עולמיים נמצאת תחת מתקפת DDoS שהפכה לגדולה ביותר שתועדה אי פעם וגרמה להאטה בכלל האינטרנט בעולם! המתקפה הגיעה לנפחים עצומים של **400 GB\ בשנייה**!.

4. חברת שירותי הבריאות **"St. Joseph"** דיווחה לכ- **400,000** מטופלים ועובדים על כך שבעקבות פריצה למערכותיה נגנב מידע אישי ומידע רגיש הכולל מספרי ביטוח לאומי (SSN), חשבונות בנק, מידע רפואי ועוד.

5. קבוצת האקרים הקוראת לעצמה **NullCrew** פרצה לשרתיה של חברת התקשורת הקנדית **"Bell"**, בעקבות הפריצה הודלפו לרשת פרטיהם של **40,000** לקוחות.

אירועי אבטחת מידע וסייבר מרכזיים- ינואר:

1. קבוצת האקרים ידועה, המכנה עצמה **The Syrian Electronic Army,** פורצת את חשבונות ה**טוויטר והפייסבוק** של חברת **"Skype"** וחברת החדשות **"BBC"**. בנוסף גם האתרים של החברות נפרצים כמחאה על מדיניות הריגול של ה- **NSA**.



2. מנהל רשת מגלה שבוצעה גישה לא מורשית יותר מ-**30** פעמים בתוך חמישה ימים לאחד מתוך שמונה שרתים האחראיים על בקרה ב**כור הגרעיני** במונג'ו ביפן. באותו מחשב היו **42,000** מיילים חסויים ומידע רב. לאחר חקירה נראה שמקור הפריצה היה מדרום קוריאה.

3. האקרים מפרסמים פרטים אישיים חלקיים של **4,200,000** ממשתמשי **"Snapchat"** לאחר שהשתמשו בחולשה שפורסמה קודם לכן ומנהלי האפליקציה סירבו לייחס לה חשיבות והגדירו את הפירצה "תאורטית".

4. רשת החדשות "FOX" דיווחה כי שירותי הפרסום של חברת **"יאהו"** נפרצו ומשמשים להפצת תוכנות זדוניות. קצב ההדבקה של הגולשים היה גבוה מאוד ונדבקו בערך **300,000** משתמשים בתוך שעה בתוכנות זדוניות שונות. לאחר מכן משתמשים רבים התלוננו שנפרצו חשבונות המייל שלהם.

5. עובד לשעבר בענקית המסחר **"Alibaba"** ושני שותפים לפשע נעצרו לאחר שחקירה גילתה כי הם מכרו פרטים אישיים של לקוחות במשך מספר שנים. המידע נמכר לחברות מסחר אינטרנטיות מתחרות משנת 2010 והגיע לכמות של כ- **20 GB**.

בס"ד

תקיפות של השחתת אתרים (Deface)

תקיפות של מניעת שירות (DoS/DDoS) שנת 2014