

ינואר 2020 //

מגזין הסייבר



עובדי הראל, נתקלתם בהודעת דוא"ל חשודה? זיהיתם התנהגות חריגה במחשב?

פנו בכל יום ושעה למוקד דיווח וטיפול בארועי סייבר בטל: 03-7473999 או בדוא"ל "מוקד סייבר" soc-mail@harel-ins.co.il

תוכן עניינים

- 3 התקפות הסייבר הגדולות ביותר לשנת 2019
- 5 אני זה הארגון שלי: הכללים שיעזרו לכם בהגנה על הארגון
- 7 מי רוצה לערער את המשטר באיראן? פרטים של מיליוני כרטיסי אשראי דלפו לרשת...
- 8 תביעת ענק נגד אפליקציית הילדים Tiktok
- 9 מטעמי אבטחה: סין מחרימה את דל, מיקרוסופט ו-HP
- 10 מידע אישי של 1.2 מיליארד אנשים התגלה בהדלפת נתונים מאסיבית
- 11 ארגון בריאות בארה"ב שילם מיליונים בעקבות מתקפת כופר
- 12 יצרנית הרכבים הגרמנית BMW נפלה קורבן למתקפת סייבר מתוחכמת
- 13 עשור של נתוני ממשלה הוצפנו בארגנטינה בעקבות מתקפת כופר

מאמר מערכת

התקפות הסייבר הגדולות ביותר לשנת 2019

מסתבר כי למרות המאמצים הרבים שמשקיעות חברות במערך אבטחת מידע ובתוכניות מודעות לעובדים, גם השנה חווה העולם מתקפות סייבר גדולות, אפילו גדולות מאד. נכון לסוף ספטמבר האחרון, אירעו השנה לפחות 5,183 מתקפות סייבר שחשפו 7.9 מיליארד רשומות מסוגים שונים. מדובר במיליארדי רשומות של אנשים פרטיים, עסקים וממשלות שיכולים לשמש תוקפים לצורך גניבת חשבונות מקוונים, סחיטה, ביצוע מתקפות ⁸ **פישנינג**, ⁸ **כופר** ועוד.

מכיוון שאין דרך לרכז את כל אלפי המתקפות במאמר אחד, בחרנו מספר התקפות גדולות שהתרחשו בשנה האחרונה על מנת לתת לכם טעימה קטנה. למעוניינים, ניתן להיכנס לאתר בשם [haveibeenpwned](https://haveibeenpwned.com/) שאוסף רשומות ממגוון מתקפות וכן באתר [informationisbeautiful](https://informationisbeautiful.net/) המרכז בצורה ויזואלית חלק נכבד ממתקפות הסייבר הגדולות שאירעו לאחרונה. אז שנתחיל?

בסינגפור דיווח משרד הבריאות שבעקבות התקפת סייבר דלפו נתונים שחשפו את הרשומות הסודיות והרגישות ביותר של מעל 14,000 אנשים שאובחנו כחולי איידס.

[לכתבה המלאה](#)

באג בתוכנת FaceTime של חברת אפל איפשר למשתמשים לצותת לסביבה של האייפון באמצעות שיחה שלא נענתה. חוקרים טענו כי יתכן וגם ניתן היה להציג עדכוני וידאו בשידור חי מאותו מכשיר.

[לכתבה המלאה](#)

620 מיליון סיסמאות ופרטי חשבונות משתמשים שנאספו מ- 16 אתרי אינטרנט הועמדו למכירה ברשת האפלה בחנות בשם Dream Market.

[לכתבה המלאה](#)

קמפיין תקיפה בשם Operation ShadowHammer התמקד במחשבי חברת

אסוס. התקיפה זיהמה את כלי עדכוני התוכנה של החברה בשם ASUS Live Update ופגעה באלפי מחשבים אישיים.

[לכתבה המלאה](#)

בפייסבוק נחשפו נתונים של מאות מיליוני משתמשים ברשת החברתית. הנתונים כללו את השירותים Facebook, Facebook Lite ו-Instagram, כולם תחת ניהול של פייסבוק. כל זה קרה בגלל שפייסבוק ניהלה את הסיסמאות לשרתיה ללא הצפנה.

[לכתבה המלאה](#)

540 מיליון רשומות הקשורות לפייסבוק, שנאספו על ידי שתי חברות צד ג', נמצאו חשופות ופתוחות לעולם בשרתי אחסון ענן של אמזון. הנתונים כללו שמות, תעודות זהות, סיסמאות, לייקים, תמונות, שמות קבוצות ועוד.

[לכתבה המלאה](#)

מאמר מערכת

יצרנית הרכב היפנית טויוטה חשפה דלף נתונים באפריל האחרון שהתרחשה בחברות הבת וסוכנויות החברה באוסטרליה, תאילנד, וייטנאם ויפן. סה"כ הועמדו בסיכון 3.1 מיליוני רשומות של לקוחות החברה.

[לכתבה המלאה](#)

מעל 12.5 מיליון רשומות של נשים בהיריון דלפו מרשות הבריאות של ממשלת הודו. הרשומות כללו מידע רפואי מפורט עבור נשים שעברו סריקת אולטרסאונד, בדיקת מי שפיר או בדיקות גנטיות אחרות.

[לכתבה המלאה](#)

דליפה של 85 ג'יגה-בייט מרשת מלונות Pyramid Hotel Group התרחשה בגלל ספק ניהול צד שלישי. בסיס הנתונים הלא מאובטח חשף מערך עצום של נתונים רגישים השייכים למערכות האבטחה של נכסי הרשת.

[לכתבה המלאה](#)

אין ספק כי שנת 2019 הייתה עמוסה באירועי סייבר, עובדה המלמדת אותנו כי גם בשנה הקרובה איננו יכולים לנוח על זרי הדפנה. עדיין נצטרך להקפיד על כללי התנהגות בסיסיים שיגנו עלינו מפני הסכנות ברשת. זכרו, לבדוק כל הודעת דוא"ל לא צפויה שקיבלתם ולהחליט האם היא חשודה, הימנעו מלחיצה על קישורים חשודים, בדקו אילו הרשאות אתם נותנים ליישומים בטלפון החכם והימנעו ככל הניתן משיתוף נתונים שיכולים לפגוע בכם. ככל שתצליחו לקיים שגרת הגנה בסייבר טובה יותר, כך תהיו פחות חשופים למתקפות.

שתהיה לכם שנה אזרחית טובה ובטוחה יותר.

מחלקת הגנת הסייבר //

טיפ מודעות

אני זה הארגון שלי: הכללים שיעזרו לכם בהגנה על הארגון



חשבתם פעם מה היה קורה אילו היו פורצים לכם למחשב האישי, ובעזרת הסיסמא הפרטית שלכם היו מצליחים לפרוץ גם למקום עבודתכם? ובכן, שאלה זו מטרידה את עולם אבטחת המידע בשנים האחרונות לאור היטשטשות הגבולות בין החיים האישיים לעסקיים. במציאות של ימינו אותם התקני מחשב משמשים לצורך פעילות פרטית ועסקית גם יחד.

בנוסף לכך, רוב המכשירים המשמשים אותנו לעבודה ולחיינו הפרטיים כוללים גם נתוני מיקום. אם זה השעון, הטלפון החכם, המחשב או הטאבלט. תוקפים פוטנציאלים

יכולים להשתמש בנתונים אלו לצורך מעקב אחרי היעד ואיסוף מידע אודות זהות הארגון שלו. הצלבה בין שם הארגון למידע המוחזק על ההתקנים של היעד, מספק לתוקפים רמז לגבי מי משתמש ברשת הארגונית. בעזרת שימוש במידע זה, העובד הופך להיות יעד לתקיפה ודלת הכניסה לארגון. כמו גם, המידע שהוא מחזיק בהתקנים האישיים שלו הופך להיות מטרה לגיטימית.

אם עד עכשיו הופתעתם מכמות המידע שאפשר לאסוף עליכם בשביל לחדור לארגון, נוסיף נדבך נוסף של פעילות ברשתות חברתיות. אותו עובד, שעלה על

הכוונת של ההאקרים, כנראה משתף מידע ברשתות החברתיות, ואם לא הוא, אולי חבריו לעבודה. תמונות הסלפי שצילמתם ביום ההולדת שערכו לכם במשרד, או הטיול המאורגן האחרון שהיה במסגרת העבודה עלולות להכיל ברקע גם סימנים מזהים של זהות הארגון. ברגע שאלו עלו לרשת, התוקף שעוקב אחריכם יודע איפה אתם עובדים ויכול להשתמש בכך כדי לתקוף את מקום עבודתכם.

אז איך אפשר בכל זאת להקטין את הסיכון לארגון? ריכזנו עבורכם מספר עצות שיעזרו לכם בכך.

שם משתמש וסיסמא

אל תשמשו באותן סיסמאות לחשבונות פרטיים ולחשבונות המשמשים אתכם בעבודה. העדיפו סיסמא ארוכה של לפחות 8 תווים, כזו המורכבת מאותיות ומספרים ותחליפו אותה כל שלושה חודשים לכל היותר.

הוצאת מידע מהארגון

הקפידו לא להוציא חומרים עסקיים הביתה - פחות מידע, פחות חשיפה. בדקו כל שבוע את המחשב והטלפון החכם לראות אילו חומרים של הארגון שמורים בהם ומחקו אותם.

שיתוף מידע באחריות

שתפו מידע עם מחשבה. צילמתם סלפי? הקפידו לחתוך מהתמונה סממנים מזהים של הארגון. עדכנתם פרופיל בלינקאדין? אין צורך לרשום אילו פרויקטים או לקוחות שירתם. בנוסף, מומלץ לא להזכיר שמות של תוכנות ומערכות IT הקשורות למקום העבודה איתם עבדתם או פרטים אודות תפקידכם.

תוכנות מסרים מיידים

קבוצות וואטסאפ או פייסבוק יכולות להיות פעילות ממכרת, אנחנו יודעים. הקפידו לא לחשוף בהן מידע רגיש אודות פעילות הארגון או לקוחותיו.

טיפ מודעות

אחריות אישית

כל עובד בארגון עלול להיחשף במהלך ביצוע תפקידו למידע חסוי הכולל בין היתר: עובדים, לקוחות, מידע עסקי וכו'. על העובד להיות אחראי באופן אישי לאבטחת המידע אליו הוא נחשף במהלך עבודתו השוטפת.

שמירת סודיות

לאחרונה נכנסו חוקי ה- **GDPR** וחוקים חדשים בהגנה על הפרטיות ועל כן כל עובד מחויב לשמור על סודיות המידע והנתונים אליהם הוא נחשף, כולל שמירה על סודיות מול עמיתים לעבודה.

התקנת תוכנות

כל תוכנה תותקן על המחשב ע"י מחלקת מערכות מידע או הגורם המורשה לכך בלבד.

עזיבת עמדת העבודה

בתום יום עבודה חשוב להקפיד לבצע יציאה מסודרת מכל מערכות המחשב או לנעול זמנית את המחשב. בנוסף, חשוב לנקות את שולחן העבודה מכל ניירת או מדיה עם מידע רגיש כולל גריסת מסמכים.

שימוש באינטרנט

יש להקפיד לא להעביר מידע רגיש באמצעות היישומים השונים באינטרנט, רק על פי הנחיות הממונה לאבטחת מידע בחברה בכל האמור להורדת קבצים באינטרנט, מסירת פרטים אישיים, מסירת כתובת האימייל של מקום העבודה בעת רישום לאתרי אינטרנט וכו'.



מי רוצה לערער את המשטר באיראן? פרטים של מיליוני כרטיסי אשראי דלפו לרשת

פרטים של כ-15 מיליון כרטיסי אשראי איראניים פורסמו ברשת בעקבות הפגנות נגד הממשלה במדינה בחודש שעבר. מומחים חושדים כי מדובר בהתקפת סייבר מצד גורם מדינתי אשר מטרתו הינה לתרום לערעור הממשל. מדובר בחשיפת נתוני אשראי הגדולה ביותר בהיסטוריה של איראן, כך על פי התקשורת האיראנית ומשרד עורכי דין המייצג חלק מהקורבנות. הפריצה כוונה ללקוחות שלושת הבנקים הגדולים באיראן - Sarmayeh, Mellat, Tejarat. סה"כ מספר החשבונות המושפעים מייצג קרוב ל-20% מאוכלוסיית איראן.

שר ההסברה והתקשורת של איראן, מוחמד ג'ואד אזרי ג'הרומי, תיאר את הפריצה כגניבת נתונים של קבלן ממורמר שסיפק

שירותים לממשלה ולכן הייתה לו גישה לחשבונות והוא חשף אותם כחלק מניסיון סחיטה. השר הכחיש שהמחשבים של מערכת הבנקים נפרצו. הבנקים שלחו הודעה לקורבנות בזו הלשון: "חשבון הבנק שלך בסכנה לשימוש לא חוקי", וביקשו מהלקוחות לבקר בסניף הבנק ולהחליף את הכרטיסים שלהם, כך על פי עותק של המייל שפורסם בתקשורת האיראנית.

עד עתה לא ברור מי עומד מאחורי ההדלפה, האם באמת גורם מדיני / גורמי פשע עלומי שם או שמא טענת שר ההסברה של איראן נכונה. בכל מקרה, המלצתנו לנושא האשראי היא: עשו סדר בכרטיסי האשראי ובטלו כאלו שאינכם משתמשים בהם. פחות כרטיסים, פחות חשיפה.



תביעת ענק נגד אפליקציית הילדים Tiktok

בחודש דצמבר האחרון, הוגשה תביעת ענק נגד הרשת החברתית TikTok ע"י סטודנטית מקליפורניה בשם מיסטי הונג בגין חשש כי האפליקציה מעבירה מידע אישי על משתמשים לממשלת סין. מדובר באפליקציית רשת חברתית מובילה בתחום שיתוף הוידאו עם מעל לחצי מיליארד משתמשים רשומים. האפליקציה שנקראה בעבר Musical.ly וכיום ידועה בכינויה TikTok נתבעת בטענה שאספה וחשפה נתונים המאפשרים זיהוי אישי של ילדים מתחת לגיל 13 בניגוד לחוקי הגנת הפרטיות של ילדים. על מנת ליצור חשבון, האפליקציה דרשה זיהוי אישי של משתמשים כולל כתובת הדוא"ל שלהם, מספר הטלפון, שם המשתמש, שם מלא, תמונת פרופיל ונתונים נוספים בהם הם עשויים לחשוף את גילם.

יתרה מזאת, בתביעה נטען כי בין דצמבר 2015 לאוקטובר 2016, האפליקציה אספה גם נתוני מיקום על משתמשים, תכונה ש"אפשרה לנתבעים ומשתמשים אחרים באפליקציה לזהות היכן נמצא המשתמש". פגיעה נוספת בפרטיות התבצעה לאור העובדה שהאפליקציה הגדירה חשבונות משתמש כציבוריים כברירת מחדל - יחד עם כל המידע המזהה אותם באופן אישי: תמונות, סרטונים והודעות. המשמעות היא כי המידע האישי של המשתמש חשוף לכל המשמשים האחרים ביישום ללא ידיעתו.

זכרו: האחריות על הילדים היא שלכם – היו מודעים לאפליקציות שילדכם משתמשים בהן. שימו לב שילדכם נמצאים בגיל המתאים כדי להשתמש ביישום הזה או אחר. עודדו אותם לשתף אתכם בכל חוויה לא נעימה שנחשפו אליה ברשתות חברתיות.



מטעמי אבטחה: סין מחרימה את דל, מיקרוסופט ו-HP



היבט נוסף למהלך הוא סביב הרצון לשלוט טוב יותר במרחב האינטרנט כדי שסין תוכל לשמור על הנתונים שלה בגבולותיה, בעקבות חוק אבטחת האינטרנט הסיני לשנת 2017. אחת מתכונות המפתח בחוק הוא להבטיח שכל הטכנולוגיה "מאובטחת" ו"ניתנת לשליטה". בעבר, סין ניסתה להחליף תוכנות מערביות, ולפני חמש שנים היו מאמצים לגמול את המדינה מאנדרואיד ומ-Windows, אך בסופו של דבר מאמצים אלו כשלו. אחת השאלות הפתוחות בהקשר זה היא האם ממשלת סין תצליח להחליף מוצרים אמריקאים. בעבר, ממשלות אחרות, ביניהן גרמניה, ניסו וכשלו בכך.

הממשל בבייג'ינג, סין, הנחה את כל משרדי הממשלה ומוסדות הציבור להחליף את כל ציוד המחשוב והתוכנה הזרים בפרק זמן של שלוש שנים, מהלך המאיים על עסקים של חברות כמו דל, מיקרוסופט ו-HP. סין פועלת נגד חברות אמריקאיות כחלק ממלחמת הסחר בין המדינות המתנהלת בחודשים האחרונים סביב טענת ארה"ב להעדר איזון בנתוני הייבוא – ייצוא בין השווקים. עימות זה הוביל להעלאת מיסים על מוצרים סיניים בארה"ב וכן להדרת חברות טכנולוגיה סיניות מהשוק האמריקאי באמצעות חקיקה. בעקבות כך, החליטה ממשלת סין להסתמך רק על טכנולוגיה מקומית במטרה להקטין תלות בספקים אמריקאים, וכן לפגוע כלכלית בחברות אמריקאיות.

מידע אישי של 1.2 מיליארד אנשים התגלה בהדלפת נתונים מאסיבית

ב- 16 באוקטובר 2019 גילו ויני טרויה ובוב דיאצ'נקו, מאגר נתונים פתוח לרווחה ברשת ובו חשבונות משתמש וסיסמאות של יותר מ- 1.2 מיליארד איש, מה שהופך את המאגר לאחת מדליפות הנתונים הגדולות ביותר ממקור יחיד בהיסטוריה. הנתונים שהודלפו הכילו שמות, כתובות דוא"ל, מספרי טלפון, קישור ל- LinkedIn ופרופיל פייסבוק.

מה שמייחד את דליפת הנתונים הזו, הוא שהמאגר מכיל מערכי נתונים שכביכול נגנבו משתי חברות שונות העוסקות בסחר מידע שיווקי (העשרת נתונים). תמורת מחיר נמוך מאוד, חברות העשרת נתונים מאפשרות

לארגון מסחרי לקבל מידע בודד על אדם (כגון שם או כתובת דוא"ל), ולהרחיב (או להעשיר) את פרופיל המשתמש כך שיכלול מאות נקודות מידע חדשות נוספות. זוהי עוד דוגמה לכך שהמידע עלינו נסחר ועובר כמטבע מיד ליד בין חברות רבות, עד שלצערנו הוא דולף לרשת בעקבות טעויות אנוש/העדר אבטחת מידע או עקב תקיפת סייבר. כולנו יודעים שאין דרך לדאוג ל- 100% פרטיות אבל כהמלצה: סיגרו חשבונות מקוונים ללא שימוש, המעיטו בחשיפת פרטים אישיים ברשת והפעילו אימות דו שלבי בחשבונות מקוונים.

ארגון בריאות בארה"ב שילם מיליונים בעקבות מתקפת כופר

ביוני 2016, Banner Health, ספק בריאות אמריקאי המפעיל עשרות בתי חולים במספר מדינות, דיווח על מתקפת סייבר אשר בעקבותיה דלף מידע בריאותי של 2.9 מיליון לקוחות. במתקפה נגנבו רשומות רפואיות, מידע על ביטוח בריאות, נתוני כרטיסי אשראי, נתוני רופאים ופרטים על לקוחות שהשתמשו במזנון הארגון. בעקבות האירוע הוגשה תביעה ייצוגית נגד החברה על ידי הנפגעים. במסגרת התביעה, הושג הסדר במסגרתו החברה הסכימה לשלם לכל קורבנות ההתקפה סכום כולל שעומד על 6 מיליון דולר. כך עולה ממסמכים שהוגשו בבית המשפט המחוזי בארה"ב באריזונה ב-5 בדצמבר 2019.

כאמור, סוגי המידע שנגנבו על ידי ההאקרים כללו שמות, כתובות, תאריכי לידה, מספרי ביטוח לאומי, מידע אודות מרשמים, היסטוריה רפואית וכ- 30,000 פרטי כרטיס אשראי. על פי דיווחים בתקשורת, להאקרים הייתה גישה למערכות Banner Health במשך כשבועיים. זכרו: מידע רפואי יכול לשמש את התוקפים לצורך סחיטה עתידית של קורבנות או גניבת מרשמים לתרופות מצילות חיים. כמו גם, בחלק מהמתקפות על ארגוני בריאות נגנבים גם כרטיסי אשראי אשר גם אותם ניתן לנצל לצורך גניבת כספים והונאת קורבנות.

יצרנית הרכבים הגרמנית BMW נפלה קורבן למתקפת סייבר מתוחכמת

לאחרונה דווח כי קבוצת תקיפה, ככל הנראה כזו הפועלת מווייטנאם, הצליחה לחדור לרשתות יצרני רכב מובילים בעולם, ביניהם BMW וחברת יונדאי. על פי הדיווחים, החדירה כוונה לגניבת סודות מסחריים. על פי פרסומים בתקשורת הגרמנית, צוות המחשוב של חברת BMW עקב אחרי המתקפה במשך חודשים על מנת להבין מה מטרתה.

לאחר חודשים בהם התוקפים ניסו לעבור ממחשב למחשב ברשת, החליטו ב-BMW לכבות את המחשבים הנגועים ולסיים את ההתקפה. התוקפים לא הצליחו לחלץ מידע רגיש, וגם הניסיון להגיע לרשת הנהלת החברה במינכן כשל. אותה קבוצה ניסתה

לפרוץ בעבר גם לסניפים בעולם של חברת טויוטה. במקרה זה, במסגרת משחקי החתול והעכבר בין תוקפים למגנים, הצליחו אנשי אבטחת המידע של BMW לזהות את התקיפה בשלב מוקדם יחסית אך הם אפשרו לתקיפה להמשיך על מנת לנסות ולגלות מה הייתה מטרת הפורצים. זכרו: אם תוקף פרץ למחשב אחד, כל המחשבים האחרים המחוברים אליו בבית או בעסק נמצאים תחת סכנה. האפשרות הזו מכונה בשפה מקצועית "תנועה רוחבית" – כלומר, באמצעות השתלטות על מחשב אחד, ניתן לעבור למחשב אחר בתנאי ששניהם מחוברים לאותה רשת תקשורת.



עשור של נתוני ממשלה הוצפנו בארגנטינה בעקבות מתקפת כופר

מסתבר כי גם לממשלות אין חסינות בפני **מתקפות כופר**, למרות כל ההשקעה והמאמצים מפניהן. באירוע שהתרחש לאחרונה בארגנטינה, מתקפת כופר נגד חוות שרתים ממשלתית גרמה לכך שמידע ממשלתי שנאסף במשך עשור הוצפן, ולא היה נגיש. מדובר על נפח מידע עצום בגודל 7700 גיגה בייט. בדיווח לא ברור איזה מידע הוצפן, אך ככל הנראה מדובר במידע אישי של אזרחי המדינה שנשמר כגיבוי. התוקפים ביקשו מהממשלה כופר בהיקף עשרות אלפי דולרים בתמורה לפענוח הקבצים.

על פי הפרסומים סביב המקרה, הממשלה סירבה לשלם את הכופר ואנשי המחשוב של הממשלה הצליחו לשחזר את מרביתו

בהליך מורכב שארך מספר שבועות. נזכיר כי מתקפות כופר הפכו להיות נפוצות מאד בשנה האחרונה, כאשר התוקפים פוגעים בלקוחות ממשלתיים, עסקיים וגם באנשים פרטיים. תשלום הכופר לרוב נע בין מאות לאלפי דולרים למחשב, ומתבצע במטבעות וירטואליים כמו **ביטקוין**. תשומת לב: הקפידו לגבות את הנתונים החשובים לכם לפחות פעם בשבוע, ולשמור אותם בענן וגם בדיסק קשיח חיצוני מנותק מהמחשב. במידה ותחוו התקפת כופר או אפילו שהטלפון או המחשב שלכם ייהרסו מסיבות אחרות, תוכלו לשחזר בקלות את הקבצים מהגיבוי.





קבלת הודעת דוא"ל חשודה?! זיהית התנהגות חריגה במחשב?

דווחו למוקד סייבר (לרשותכם 24/7)
במייל: "מוקד סייבר" | בטלפון: 03-7473999

כיצד נזהה משהו חשוד?

שימו לב למיילים / הודעות SMS / WhatsApp:

- ⚠ שאינו מוכר לכם
- ⚠ עם תוכן או קישור חשוד
- ⚠ כאשר מבקשים מכם לבצע פעולה חריגה

