דגשים בהגנת פרטיות ואבטחת המידע בפעילות עמותה

כידוע, עמותות ממלאות תפקידים רבים במציאות החברתית, הכלכלית והפוליטית במדינת ישראל. עמותות פועלות לשם תמיכה בעת מלחמה ומסייעות לציבור הרחב, לוחמים ואזרחים, ולאוכלוסיות שנפגעו. במסגרת פעילותן, עמותות מבקשות סיוע מהציבור, ומגייסות תרומות, ציוד, ספקים, שירותים, מתנדבים ועוד. אחד היתרונות במתן תמיכה באמצעות עמותות הוא בכך, שבעמותות קיים מערך לוגיסטי משוכלל, היכול להבטיח את הגעת הכספים, הציוד והשירותים ליעדם.
לשם פעילותן, עמותות אוגרות מידע רב ומגוון. הרשות להגנת הפרטיות (להלן: **הרשות**) שבה ומזכירה כי יש להקפיד על אופן שמירת המידע ואבטחתו. זאת, במיוחד לאור העלייה במספר אירועי אבטחת-מידע מאז פרוץ מלחמת "חרבות ברזל". יותר מתמיד, קיימת חשיבות לצמצום המידע ולמזעור המידע הנדרש.

מספר דגשים לאבטחת מאגרי המידע הללו:

עיצוב לפרטיות: איזה מידע ניתן לאסוף?

עם תחילת פעילות העמותה **וטרם** איסוף נתוני המידע הנדרשים לעבודת העמותה (הקמת מאגר המידע או כל קובץ מידע), חשוב להגדיר מהו **המידע** הנחוץ לעבודת העמותה, שבלעדיו לא ניתן לקיים את הפעילות באופן תקין. כל מידע אחר יחשב כמידע עודף ולכן אין לדורשו, לאוספו או לאחסנו.

האם יש לעמותה אתר אינטרנט?

- יש לוודא קיומם של מנגנוני הגנה מפני "הזרקת SQL"*.
- יש לוודא כי קיים ניתוק התקשורת בין השרת* למשתמש בסיום פעילותו באתר.
- יש לוודא קיומו של מנגנון המוודא שמידע לא נשמר בדפדפן של המשתמש.
- חשוב לבדוק ולוודא שהאתר אינו חושף מידע מן השרת לגולשים, ופועל באופן מאובטח.

מה הם אמצעי האבטחה שצריך להטמיע במערך המחשוב של העמותה?

- חומת אש*- יש לוודא תקינותה ופעולתה של חומת האש במערכת ההפעלה בכל מחשבי העמותה.
- יש לוודא כי קיים כלי מעקב וניטור אחר הפעילות של חומת האש.
- מערכת *EDR– יש לוודא כי על מחשבי העמותה מותקנת מערכת EDR עדכנית.
- מדיניות סיסמאות – יש לוודא קיומם של כללים ליצירת סיסמאות מוקשחות* למשתמשים, סיסמאות גישה לקבצים וסיסמאות גישה לרשת.

כיצד מוודאים אבטחה נאותה לאורך הזמן?

יש לוודא כי על מחשבי העמותה מותקנת מערכת הפעלה בגרסה אחרונה ומעודכנת, ולהקפיד על התקנה סדירה של כל עדכוני האבטחה המפורסמים על ידי היצרן.
כמו כן, יש לוודא עדכונם של כל אמצעי האבטחה הקיימים בעמותה.

מדיניות סיסמאות - כיצד נעצב סיסמאות?

יש לוודא כי כל המחשבים ברשת העמותה מוגנים לגישה באמצעות סיסמה מוקשחת – המכילה 8 תווים לפחות, אותיות גדולות, אותיות קטנות, מספרים ותווים מיוחדים.

כיצד ננהל את הרשאות הגישה למידע בעמותה?

- יש לוודא כי רק לאנשים **המורשים** ניתנת גישה למידע ולקבצים המכילים מידע. במידה וישנם מספר גורמים עם הרשאת גישה, יש להקפיד על ניהול רשימה מסודרת של המורשים והמידע המותר להם לגשת אליו, ובאיזה היקף.
- ביטול גישה בעת סיום עבודה – חשוב לנהל את הרשאות הגישה **ולבטל גישה** למשתמשים שסיימו את עבודתם בעמותה.
- בעת שימוש בקבצים משותפים (דוגמת קבצי Google Drive כגון docs ו-sheets, קבצי Dropbox ועוד), יש לוודא כי מוגדרת הרשאת פרטיות לקבצים, והם משותפים רק עם קבוצת אנשים מורשים, שהוגדרה מלכתחילה.

מה לגבי העובדים?

חשוב לבצע הדרכת אבטחת מידע ושמירה על הפרטיות לכלל העובדים בעמותה (כולל מתנדבים) בעת תחילת עבודתם ואחת למספר חודשים.

דגשים בהגנת פרטיות ואבטחת המידע בפעילות עמותה

איך נבטיח שימוש בטוח ברשת?

- **חובה** לאבטח את שרת האינטרנט ואת בסיס הנתונים המקושר באמצעות **חומות אש** עדכניות, על מנת להגן על אתרי אינטרנט ובסיסי נתונים.
- יש להקפיד **לא** להתחבר ולא להשתמש ברשתות אלחוטיות ציבוריות (כגון רשת wi-fi ציבורית). יש להעדיף תמיד עבודה ברשת מאובטחת ומוגנת בחומת אש, ולאפשר גישה מרחוק בתווך מאובטח VPN (רשת פרטית וירטואלית), עם זיהוי רב-שלבי.

הצפנת מידע – איך נמנע פגיעה בפרטיות המידע?

- בעבודה עם קבצי Office (וורד/אקסל) או PDF חשוב לאבטח את הקבצים ולנעול אותם באמצעות סיסמה מוקשחת, בפרט בעת שיתופם או העברתם.
- במידה ונדרש להעביר קובץ נתונים המכיל מידע רגיש, בדוא"ל או על גבי מדיה נשלפת (דיסק און קי), יש לוודא כי הקובץ נעול ומוגן בסיסמה טרם העתקתו להתקן או שליחתו בדוא"ל.

מחיקת מידע – מה עושים לאחר סיום הפעילות?

בסיום הפעילות (או המשימה, המטלה וכדומה), כאשר המאגר אינו דרוש יותר לפעילות/משימה שהוגדרה, **יש לוודא** ביעורו על ידי **<u>מחיקתו המוחלטת</u>**, על כל העתקיו.

מה עושים עם גיבויים?

יש לוודא את אבטחת הגיבויים שעושה העמותה למידע, בכל אמצעי שהוא, מפני גישה פיזית או לוגית.

מיקור-חוץ – כיצד מתנהלים בעבודה עם גורם חיצוני?

- במקרה שהעמותה נדרשת לעבוד עם ספק או גורם חיצוני לעמותה, לעיבוד המידע או הקמת אתר, **יש להתקשר בהסכם המגדיר את חובות הספק/הגורם – בענייני אבטחת המידע, הגנת הפרטיות, שמירת סודיות וכן ביעור (מחיקת) המידע בתום ההתקשרות.**
- יש לוודא כי התקשורת מול הספק או הגורם החיצוני מאובטחת וכוללת **זיהוי רב שלבי.**

הרשות מוצאת לנכון להבהיר כי מטרת הדגשים המובאים לעיל הינה לסייע בלבד; הדגשים משקפים דרך פעילות מומלצת (Best Practice), והם אינם מחליפים את הוראות החוק והתקנות או ממצים את דרישותיהם. על כל בעל מאגר לוודא, כי הוא ממלא אחר כל היבטי אבטחת המידע בהתאם לדרישות החוק והתקנות.

באתר הרשות ניתן למצוא פרסומים הכוללים הסברים ודוגמאות לדרישות החוק והתקנות ביחס לאבטחת מידע, לרבות מיקור חוץ הכרוך בגישה למידע אישי ועוד.

<u>מילון מונחים:</u>

- **שרת (server)** – תוכנת מחשב או מכשיר פיזי המשמש להעברת נתונים בין תוכנות מחשב והמשתמשים שלהן (תוכנת המחשב והמשתמש מכונים יחדיו "לקוח").
- **הזרקת SQL (SQLi)** – מתקפת סייבר המתבצעת באמצעות הזנת טקסט (קוד) לשדות התוכן באתר, באופן המאפשר לחשוף מידע שאינו חשוף למשתמש בדרך כלל. ניתן להתגונן ממתקפות אלו באמצעות מנגנוני אימות שדות תוכן, הצפנה וניהול הרשאות משתמשים.
- **מערכת EDR** – מערכת לזיהוי ומענה מהיר על איומי אבטחה במכשירים השונים עליהם מותקנת המערכת.
- **חומת אש (Firewall)** – מנגנון לאבטחת רשתות. חומת אש מנטרת את הפעילות ברשת, ומחליטה לחסום פעילות מסוימת בהתאם לכללי אבטחה מוגדרים מראש.
- **הקשחת סיסמאות** – מגוון טכניקות המקשות על פריצה, ניחוש וניצול של סיסמאות המשתמשים (דוגמת כללי סיסמא מחייבים, אימות דו-שלבי וכו').
- **הצפנת מידע** - מקשה על גורם חיצוני לפענח מידע שהשיג מהמאגר, האתר, השרת וכיו"ב, וכך מונעת שימוש פוגעני במידע.