24 מרץ, 2020

כ״ח אדר, תש״פ

דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית

מנהלים ועובדים יקרים,

אלו ימים מורכבים אשר עוברים על כולנו. הניסיון לבלום את התפשטות נגיף הקורונה, משפיע באופן משמעותי על ההתנהלות המקצועית ועל וחיי היומיום של כולנו.

ארגונים רבים במשק נקטו בצעדים מהירים וחריגים בכדי לבודד מחד את העובדים ומאידך לאפשר רציפות תפקודית, ופעלו במהירות על מנת לאפשר לעובדיהם עבודה מרוחקת לרבות ממחשבים ביתיים. במידה ופעולות אלו נעשו ללא ביצוע הערכת סיכונים מסודרת, יש בכך כדי להגדיל את הסיכוי להתרחשותו של אירוע אבטחת מידע.

על כן ולצד הצורך החיוני בהמשכיות הרצף התפקודי, יש להקפיד ולוודא כי גם במצבי קיצון ובמציאות דינמית ניתנת תשומת הלב הנדרשת לנושא ההגנה על פרטיות המידע ואבטחת המידע בעת טיפול במידע אישי של עובדים או של נושאי מידע בהם ארגונים אלה מטפלים במסגרת העבודה היומיומית.

ברצוננו להביא בפניכם- מנהלים ועובדים- מידע נוסף ולתת דגשים חשובים בהתנהלות הטכנולוגית של ארגונים ובהתנהלותו של כל אחד ואחת מכם מחוץ לכותלי הארגון.

סט הנחיות למעסיק בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית

המציאות החדשה אליה נקלע המשק הישראלי בדומה לעולם כולו, הכתיבה כי ארגונים רבים שינו את אופן התנהלותם ואפשרו עבודה מרחוק במכשירים זרים למערכת הארגונית, דבר שאפשר להם את המשך הרציפות התפקודית, חיסכון במשאבים ונגישות של העובדים, לעיתים במחיר של הגדלת הסיכונים לארגון ואתגר משמעותי להנהלתו.

במסגרת הסכנות הרבות שאתגר זה מציב בפני הארגון, נכללים לדוגמה- **גניבה או אבדן** של מחשב או מכשיר נייד המכיל חומר רגיש ואפשרות גישה לרשת הארגונית באמצעות אמצעי זיהוי הנשמרים עליו; **חוסר יכולת אכיפה של מדיניות אבטחה ארגונית**; גישה מרחוק דרך **מכשיר לא מאובטח** המהווה נקודת תורפה אבטחתית חמורה; **ניהול עובד שיצא לחל״ת, שחלה או שעזב** ושמכשירו האישי נשאר בידיו ובו מידע ארגוני רגיש ואפשרות גישה למשאבי הארגון ולמערכותיו;

ריבוי טכנולוגיות המייצר עומס על צוותי התמיכה והאבטחה וחוסר היכרות עם הסיכונים הגלומים במגוון רב של מערכות הפעלה וסוגי מכשירים.

לפיכך, על מנת למזער את הסיכון לדלף מידע אישי ולפגיעה בארגון, לקוחותיו או עובדיו, בעקבות חיבורם של עובדים לצורך עבודתם מן הבית באמצעות מחשב ארגוני, חשוב למלא אחר מספר כללים:

ברמת ההנהלה:

1. נושא הגישה מרחוק יתווסף מיידית לניהול הסיכונים הארגוני, תוך גיבוש מדיניות אבטחה ארגונית לטובת השימוש בגישה מרחוק ובמכשירים אישיים.
2. רצוי להשקיע במערכות ובטכנולוגיות ייעודיות להתמודדות עם הסיכונים אשר מציבים מכשירים אישיים.

ברמה הטכנולוגית:

1. יצירה של שכבות הגנה שימנעו גישה ממכשירים אישיים לא מאובטחים מספיק, לנכסים הקריטיים של הארגון.
2. הגדרת נהלי שימוש בגישה לרשת באמצעות מכשירים אישיים, ונהלי שמירה ואבטחת המכשירים בעת שלא נעשה בהם שימוש וכד'.
3. הגברת הניטור והבקרה על הגישה מרחוק בפעולות המבוצעות אל מול משאבי הארגון.
4. הגברת המודעות בקרב העובדים לשימוש בתוכנות אבטחה ולעבודה מאובטחת במכשירים הפרטיים שלהם, הדרכתם והנחייתם באשר לפעולות שעל העובד לבצע לשם הקטנת סיכוני האבטחה (כמפורט להלן).
5. הגדרת אמצעי גישה מאובטחים למערכות המשרדיות- ובכלל זה הפעלת מנגנון הזדהות חזק בכניסה לרשת (MFA\2FA), חובת הגדרת סיסמת אבטחה מוקשחת, אכיפת אפשרויות העתקה ושמירת מידע רגיש במכשיר הביתי, הגדרת חובת ניתוק חיבור לאחר פרק זמן של חוסר פעילות בגישה מרחוק, ביטול האפשרות לעבודה עם תוכנות השתלטות מרחוק כדוגמת TeamViewer, Anydesk וכד'.

<u>שימוש ב"מחשב זר" בעת גישה לרשת המשרדית</u>

המחשבים המשרדיים בהם אנו עובדים, מנוהלים על ידי אנשי אבטחת המידע ואגף מערכות המידע של הארגון בו אנו מועסקים, ועל כן הם בד"כ מוגנים. לא כך הוא המצב לגבי מחשב זר או ביתי שממנו אנו מתחברים למערכות המשרדיות, ופעמים רבות רמת מיגונו של מחשב כזה נחותה מזו שבסביבה הארגונית, למרות שהמידע שיעובד בו יהיה רגיש באותה מידה.

1. יש לוודא כי **המחשב הביתי** בו נעשה שימוש כזה כולל **מערכת הפעלה** מעודכנת **ותוכנת Antivirus** פעילה, שכן מערכת ההפעלה הינה אחד מהיעדים המבוקשים ביותר על ידי תוקפים המחפשים פרצות, ותוכנת ה- Antivirus מיועדת לנטר ולחסום פעילות חשודה על המחשב אשר עשויה להיגרם בעקבות נוזקה.
2. גם **הרשת הביתית** בה נעשה שימוש נדרשת להיות מאובטחת על ידי **תוכנת חומת אש** (Firewall) מעודכנת, **ונתב מאובטח** - בו מומלץ לשנות את שם המשתמש והסיסמא (שכן סיסמת ברירת מחדל ידועה היטב לתוקף אפשרי) ואף את שם הזיהוי של הנתב (SSID).
דאגו שעבודה על רשת ה- Wi-Fi תעשה תחת הצפנה (מומלץ לפחות WPA2) ואל תתנו את הסיסמה לרשת לכל אורח.

3. יש לוודא כי המחשב והשירותים השונים אליהם הוא פתוח מצויידים **בסיסמאות חזקות** למחשב, כדי למנוע גישה לתוקף. סיסמא חזקה היא כזו אשר תקשה על ניחושה ותכלול תווים רבים ככל האפשר (8 תווים מינימום ועדיף יותר) בשילוב של אותיות קטנות, גדולות, מספרים ותווים מיוחדים. זכרו להשתמש בסיסמאות שונות לשירותים שונים על מנת להימנע ממצב בו חשיפה של סיסמא אחת תאפשר פגיעה ביתר השירותים.
4. **תוכנות המותקנות** על המחשב יכולות להוות נקודות חולשה, בדגש על התוכנות הנפוצות אשר לרוב תוקפים מחפשים עבורן פרצות, כגון: Java, PDF Viewers, Web Browsers, Flash Microsoft Office, ועל כן יש לוודא כי גם תוכנות אלה מעודכנות בעדכוני האבטחה, וכי אין מדובר בתוכנות פרוצות אשר הורדו מהאינטרנט, אשר פעמים רבות נושאות איתם וירוסים.
5. שימוש במחשב זר שהוא ציבורי או של אדם זר, הינו אסור, ובכל מקרה אין להשאיר את סביבת העבודה המשרדית פתוחה או את המחשב עצמו פתוח ללא השגחה, גם אם הסביבה בה הוא נמצא "בטוחה". עם סיום העבודה יש לסגור את מסך ההתחברות, לסגור את הדפדפן בו נעשה שימוש ולנעול את המחשב.

<u>מערכות ארגוניות ומערכות אחרות</u>

השימוש בסביבה הביתית ותקלות טכניות במערכות הארגוניות לעיתים מאלץ אותנו לעשות שימוש בכלי דואר אלקטרוני פרטיים (כגון ג'ימייל) או מערכות מסרים מידיים (כגון וואטסאפ).

יש לזכור כי יש סיכון רב בהעברת מידע ארגוני, בוודאי מידע חסוי או רגיש, ברשתות חברתיות, במערכות למסרים מידיים או במייל פרטי, ובדרך כלל העברה כזו של מידע אישי על תשתית פומבית אסורה.

מכל מקום, בעת שימוש במערכות תקשורת אשר אינן משמשות אותנו באופן רגיל, נדרש **להגביר את תשומת הלב ולבדוק היטב את הנמענים ואת רגישות התוכן המועבר**, כדי להימנע מיצירתו של אירוע אבטחה בעקבות טעות אנוש אשר במסגרתו יישלח מידע רגיש לאנשים מחוץ לארגון אשר אינם מורשים לצפות בו.

כך לדוגמה אנו ממליצים לבדוק ב"שבע עיניים" את **כתובות הנמענים**, בסביבות עבודה שהינן פחות מוכרות לנו, על מנת להימנע מטעויות נפוצות כגון השלמה אוטומטית ולא נכונה של כתובת הנמען, אשר תגרום להעברת מידע למי שאינו מורשה בקבלתו, באופן בלתי הפיך או משלוח מענה ב- "**השב לכולם**" כשהכוונה הייתה לשלוח הודעה לגורם ספציפי.

בדומה, יש לשים לב במיוחד לפעולות של "**גיבוי**" **או העתקת מידע ממערכות ארגוניות לסביבת העבודה המקומית**, אשר יכולות לגרום - אף ללא כוונה או ידיעה - להעתקה של המידע לשרתי קבצים חיצוניים ולא מאובטחים (כגון גוגל דרייב). עם סיום העבודה על המידע המקומי והעברתו חזרה למערכת הארגונית, יש לוודא מחיקתו המלאה, מכל מקום אליו הועתק (ובכלל זה גם מפח האשפה).

<u>ניהול פגישות ושיחות חוזי מבוססות ענן</u>

במסגרת המאמץ למציאת כלים שיאפשרו את המשך פעילותם של ארגונים בעת שהעובדים אינם נמצאים בפועל במשרד תוך כדי מתיחת הגבולות הפיזיים של הארגון, הכניסו לאחרונה ארגונים רבים שימוש בכלים דוגמת זום "ZOOM cloud meetings" Webex meetings וכלים נוספים לשם קיומן של פגישות בווידאו\שמע, צ'אטים, שיחות טלפון וסמינרים מקוונים.

להלן מספר נושאים אותם יש לקחת בחשבון בעת השימוש בכלים מסוג זה:

1. יש להבין כי מדובר בסביבת עבודה ציבורית לא מאובטחת, אשר עלולה לגרום לחשיפה לא מבוקרת של מידע רגיש המונגש בה. משתמשים במערכת צריכים להיות מודעים לכך שמידע אותו הם מציגים, כולל נתונים אישיים אודות המשתתפים, עשוי להיות מצולם או מוקלט (מרצון, בזדון או בשגגה) ועשוי להיות משותף במכוון או שלא עם גורמים אחרים.
2. קישור לפגישה יכול להפוך להיות ציבורי, וזרים יכולים להיחשף או להקליט את תוכן השיחות והמידע, ולרשימת המשתתפים בפגישה והמוזמנים אליה. מידע רגיש העשוי להימצא על שולחן העבודה או ברקע יוצג לכל המשתתפים.
3. שימוש במערכת חיצונית אוסף מידע רב על המשתמשים בו, ודורש הרשאות גישה למצלמה, לקבצים על המכשיר ועוד. בשם הספקת חוויית משתמש טובה יותר - מערכות חיצוניות אלה אוספות מידע הכולל את פרטי הקשר של המשתמש, מידע על עבודתו ותפקידו, פרטי אשראי ותשלום, פרופיל מדיה חברתית (בו עושים שימוש כדי להתחבר למערכת), ומידע כללי על העדפות המוצר והשירות, על המכשיר, הרשת והחיבור לאינטרנט ועוד. המידע שנאסף או מוקלט, מועלה פעמים רבות לענן ומסופק לחברות צד שלישי המספקות לפלטפורמה שירותים נוספים, כגון אחסון, עיבוד, ניתוח ועוד. כיוון שהענן נמצא במירב המקרים מחוץ לגבולות ישראל, יש לוודא עמידה בהוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א – 2001.

הונאות וניסיונות דיוג

תזזיתיות המידע וחוסר הביטחון שכולנו חשים בימים כאלה, מהווה כר פעולה נוח לפעילותם של גופים עבריינים המבקשים לנצל את המצב, ולגזור קופון" על ידי איסוף מידע ושימוש בלתי חוקי בו. כך, בימים האחרונים אנו מקבלים דיווחים מרחבי העולם על פעילויות הונאה שונות המנצלות את מצב החרום, באמצעות ניסיונות דיוג שנועדו לאסוף פרטי מידע לצורך ביצוע הונאות והוצאת כספים במרמה.

קיימים דפוסים רבים של ניסיונות הונאה כאלה, ובין היתר **יצירת קשר באמצעות שימוש בהודעות מייל או יצירת קשר טלפוני** המתבססות על צורך בהול (אדם המתחזה להיות רופא הנוקב בשמו של קרוב משפחה אשר לכאורה מאושפז בבית חולים בעקבות הנגיף ומצביע על צורך בהול בהעברת תשלום או באיסוף מידע אישי) היצע מוגבל (הצעה לרכישת מסכות וציוד רפואי למול ביקוש עצום), מידע רפואי (התחזות לאתר רפואי המספק המלצות לדרכי התגוננות מהנגיף ומפנה לדוגמא למפת התפשטות עולמית, כדי לפתות הקורבן ללחוץ על קישור שישתיל נוזקה במכשיר לשם השתלטות וגניבת פרטים אישיים).

נספח א' – סט הנחיות למשתמש לעבודה מרחוק

1. **הגנה על המחשב המרוחק -**
   א. איסור שימוש במחשב ציבורי.
   ב. עדכון גרסת מערכת ההפעלה ועדכוני אבטחה.
   ג. התקנה ועדכון של תוכנת אנטי- וירוס.
   ד. עדכוני אבטחה של תוכנות מותקנות.
   ה. שימוש בסיסמאות חזקות, נעילת סביבת העבודה בעת הפסקת עבודה.
2. **הגנה על הרשת המרוחקת -**
   א. התקנה ועדכון של תוכנת חומת אש.
   ב. עבודה עם נתב מאובטח.
   ג. שינוי סיסמאות ברירת המחדל של הנתב והרשת.
3. **שימוש במערכות הארגוניות מרחוק -**
   א. שימוש מושכל וזהיר במערכות שאינן מנוהלות על ידי הארגון (כגון ג'ימייל, רשתות חברתיות, מערכות למסרים מהירים וכד').
   ב. מניעת אירועי אבטחה על ידי בחינה של כל פעולת העברת מידע - מה המידע ולמי הוא מועבר בפועל.
   ג. מחיקה של מידע המועתק לסביבה המקומית.
4. **זיהוי ניסיונות דיוג והונאה -**
   א. בהודעה - שימו לב לזהות השולח ולקשר שלו לתוכן ההודעה. אם אינכם מכירים את השולח - השתדלו לא לפתוח את המייל במידת האפשר, ובוודאי אין לפתוח צרופות המצורפות להודעה או להקיש על הקישורים הכלולים בה.
   ב. חפשו סימנים חשודים -
      i. גורם המבקש מכם פרטים אישיים כאשר הוא אמור לדעת פרטים אלה;
      ii. ניסיונות להלחיץ באמצעות מצג שווא למצב חרום, סנקציה או מועד אחרון להגשה;
      iii. תוכן וסגנון ההודעה אשר נראה חובבני, כולל טעויות כתיב או תחביר רעוע או אינו מתאים לתוכן המכתב (למשל: מכתב מבנק אשר נשלח מתיבת Gmail).
   ג. קישורים לאתרים הנשלחים אליכם - פיתחו בנפרד בהקלדה יזומה בדפדפן.
   ד. אם קיבלתם הודעה חשודה המבקשת לעדכן פרטי תשלום, לפתוח חשבון שנחסם ועוד - צרו קשר ישירות מול החברה השולחת לכאורה.
   ה. זכרו כי פרטי המשתמש שלכם קבועים בד"כ עד אשר מיוזמתכם אתם מבצעים שינוי, אף מוסד פיננסי או ארגון וגם לא מערכות מידע והתמיכה לא יבקש את פרטיכם האישיים, אלא יבצעו את השינוי במסגרת אתר החברה ואחרי שביצעתם הזדהות.