דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית

מזכר לקוחות – מרץ 2020

לקוחות יקרים,

הרשות להגנת הפרטיות ("**הרשות**") פרסמה ביום 24.3.2020, מסמך דגשים למנהלים ועובדים בהפעלת מדיניות עבודה מרחוק אל מול הרשת הארגונית ("**המסמך**"), שמטרתו לספק דגשים ביחס להתנהלות של ארגונים המאפשרים עבודה מרחוק אל מול הרשת הארגונית - ושל פרטים מחוץ לכותלי הארגון. הדגשים האמורים מקבלים משנה תוקף בעת הזו, שעה שארגונים רבים במשק פעלו במהירות על מנת לאפשר לעובדיהם עבודה מרוחקת לרבות ממחשבים ביתיים.

להלן סקירה תמציתית של מספר כללים שהרשות מציינת שחשוב לקיים, וכן תובנות שלנו בקשר אליהם.

1. <u>ברמה הארגונית</u>

- יש להוסיף את נושא הגישה מרחוק לניהול הסיכונים הארגוני, תוך גיבוש מדיניות אבטחה ארגונית לטובת השימוש בגישה מרחוק ובמכשירים אישיים ורצוי להשקיע במערכות ובטכנולוגיות ייעודיות להתמודדות עם הסיכונים אשר מציבים מכשירים אישיים.
- בהקשר זה נזכיר כי לפי תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, יש לעדכן במסמכים שונים הנוגעים למאגרי המידע שברשות הארגון כאשר מתרחש שינוי בסיכונים העיקריים לפגיעה באבטחת המידע. בנוסף נזכיר שכאמור במזכרנו הקודם בנושא ("מזכרנו הקודם"), ישנן הוראות דין שונות המקימות חובה לארגונים להיערך טכנולוגית ביחס לגישה מרחוק למאגרי המידע שלהם ולמערכותיהם.

- יש להגדיר נהלי שימוש בגישה לרשת באמצעות מכשירים אישיים, ונהלי שמירה ואבטחת מכשירים אלה בעת שלא נעשה בהם שימוש וכד'. הן בהקשר זה והן ברמה הטכנולוגית אנו ממליצים למשל להנחות עובדים לעבוד ממחשביהם האישיים (לא ממחשבים ציבוריים/מחשבים שאינם של העובד עצמו), להימנע מלשמור קבצים על המכשירים האישיים שלהם ולהיות עירנים לתוכנות ויישומונים המותקנים על גבי מכשיריהם (ולהימנע למשל משימוש בתוכנות חינמיות/פרוצות).

WWW.AGMON-LAW.CO.IL
ירושלים הגן הטכנולוגי מלחה, בניין 1
טלפון: 02-5607607 | פקס: 02-5639948
תל אביב מגדל אלקטרה, יגאל אלון 98
טלפון: 03-6078607 | פקס: 03-6078666

2. ברמה הטכנולוגית

- יש ליצור שכבות הגנה שימנעו גישה ממכשירים אישיים לא מאובטחים מספיק, לנכסים הקריטיים של הארגון.
- יש להגביר הניטור והבקרה על הגישה מרחוק בפעולות המבוצעות אל מול משאבי הארגון (בהקשר זה ראו גם את מזכרנו הקודם).
- יש להגביר את המודעות בקרב העובדים לשימוש בתוכנות אבטחה ולעבודה מאובטחת במכשירים הפרטיים שלהם. כפי שהמלצנו במזכרנו הקודם, במסמך הרשות מנחה ליזום הדרכות באשר לפעולות שעל העובד לבצע לשם הקטנת סיכוני האבטחה.
- יש להגדיר אמצעי גישה מאובטחים למערכות המשרדיות ובכלל זה הפעלת מנגנון הזדהות חזק בכניסה לרשת (Multi Factor Authentication/Two Factor Authentication), הגדרת סיסמת אבטחה מוקשחת (ראו את מזכרנו הקודם בנושא זה).
- יש להגדיר וליישם ניתוק לאחר פרק זמן קצר יחסית של היעדר פעילות מצד המשתמש, ולהסיר תוכנות השתלטות מרחוק.

3. שימוש "במחשב זר" בעת גישה לרשת ארגונית

- יש לוודא שבמחשבים מרוחקים מותקנות מערכות הפעלה ותוכנות Antivirus, מעודכנות. בהקשר זה אנו ממליצים שאלה תוספנה להתעדכן באופן תדיר.
- יש לוודא שמותקנים עדכוני אבטחה בתוכנות המותקנות במחשבים המרוחקים.
- יש לוודא כי ברשתות בהן נעשה שימוש מותקנת חומת אש ונעשה שימוש בנתב מאובטח (בו מומלץ לשנות את שם המשתמש, הסיסמא ואת שם הזיהוי של הנתב (SSID))
- יש לוודא כי המחשב והשירותים השונים אליהם הוא פתוח מצויידים בסיסמאות חזקות למחשב וכי סביבת העבודה ננעלת לאחר תקופת היעדר פעילות קצרה ככל הניתן. ביחס לדגשים בנוגע לאפיון וחוזק סיסמאות, ראו את מזכרנו הקודם.

4. מערכות ארגוניות ומערכות אחרות

- השימוש בסביבה הביתית ותקלות טכניות במערכות הארגוניות לעיתים מאלץ עובדים לעשות שימוש בדואר אלקטרוני פרטי ו/או מערכות (IM) Instant messaging. יש לעשות שימוש זהיר באמצעים אלה. יש סיכון רב בהעברת מידע ארגוני, בוודאי מידע חסוי או רגיש, ברשתות חברתיות, מערכות (IM) Instant messaging או בדואר אלקטרוני פרטי, ובדרך כלל העברה כזו של מידע אישי על תשתית פומבית אסורה.
- 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.

WWW.AGMON-LAW.CO.IL
ירושלים הגן הטכנולוגי מלחה, בניין 1
טלפון: 02-5607607 | פקס: 02-5639948
תל אביב מגדל אלקטרה, יגאל אלון 98
טלפון: 03-6078607 | פקס: 03-6078666

5. **<u>ניהול פגישות ושיחות חוזי מבוססות ענן</u>**

- שימוש בכלים מקוונים לשם קיומן של פגישות ווידאו\שמע, צ'אטים, שיחות טלפון וסמינרים מקוונים, עלול לגרום לחשיפה לא מבוקרת של מידע המונגש בהם. חשוב לזכור שמידע המוצג בכלים אלה יכול להיות משותף, מצולם ומוקלט שלא ביוזמת כל המשתמשים, ולהפוך לציבורי במקרים מסוימים.
- כן רצוי לזכור שרשימות המוזמנים לפגישות אלה אינן חסויות בכל המקרים, שמידע על שולחן העבודה עלול להיות חשוף ליתר המשתתפים בחלק מהמקרים, וכי כלים אלה מבקשים לא אחת הרשאות הרשאות גישה לרכיבים/קבצים המצויים במכשיר המשתמש באמצעותם נאסף מידע רב אודות המשתמשים.
- ברב המקרים שרתי הענן נמצאים מחוץ לישראל ויש לזכור שהעברת מידע בתווך זה עלולה להביא את המעביר למצב בו אינו עומד בהוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות ישראל) תשס"א – 2001.

6. **<u>נסיונות דיוג (Phishing).</u>**

- כאמור במזכרנו הקודם, בהתאם להודעת מערך הסייבר הלאומי בעניין זה, מבקשת גם הרשות להגנת הפרטיות להעלות את המודעות לכך שלאחרונה נרשמה עלייה במספר הניסיונות לביצוע מתקפות סייבר על גופים שונים. במסמך הרשות שמה דגש על תרמיות מסוג דיוג (Phishing), במסגרתן נעשים נסיונות לאסוף פרטי מידע לצורך ביצוע הונאות, הוצאת כספים במרמה ושתילת רוגלות.
- הרשות מציינת שקיימים 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), והצעה לקבל מידע רפואי (התחזות לאתר המכיל מידע רפואי המספק המלצות לדרכי התגוננות מהנגיף ומפנה לדוגמא למפת התפשטות עולמית, כדי לפתות הקורבן ללחוץ על קישור שישתיל נוזקה במכשיר הקצה שלו).

לקישור למסמך שאלות ותשובות בנושא הגנת הפרטיות בעקבות התפשטות נגיף הקורונה, *ראו* https://www.gov.il/BlobFolder/reports/corona_work/he/CORONA_%D6%B9WORK_%D6%B9PRIVACY.pdf

WWW.AGMON-LAW.CO.IL
ירושלים הגן הטכנולוגי מלחה, בניין 1
טלפון: 02-5607607 | פקס: 02-5639948
תל אביב מגדל אלקטרה, יגאל אלון 98
טלפון: 03-6078607 | פקס: 03-6078666

אנו, במשרד אגמון ושות' רוזנברג הכהן ושות', ממשיכים לעמוד לצדכם ולספק את מלוא השירותים המשפטיים ברמה המקצועית הגבוהה ביותר. נמשיך לעקוב אחרי התקנות והמצב המשפטי המתפתח, ולעדכן את לקוחותינו.

אנו מאחלים לכולם בריאות שלמה וחזרה מהירה לשגרה.

נשמח לעמוד לרשותכם בכל שאלה

עו"ד אסנת סרוסי פירסטטר, ראש מחלקת טכנולוגיה והייטק
osnat@agmon-law.co.il

עו"ד סער רוסמן, שותף, מחלקת טכנולוגיה והייטק
saar@agmon-law.co.il