המלצות הגנה - עבודה מרחוק - מהבית

מסמך המלצות הגנה לארגונים ועסקים - עבודה מרחוק - מהבית בעקבות התפשטות נגיף הקורונה

תוכן עניינים

הקדמה

התפשטות נגיף הקורונה בארץ ובעולם מעודדת ואף מחייבת ארגונים רבים לשנות את שיטת העבודה ולאפשר לעובדיהם לעבוד מהבית.

אמנם לא כל הארגונים ערוכים לעבודה מרחוק מהבית, אך בעידן של היום הדבר מתאפשר וכל אחד מאיתנו יכול להתחבר לעבודה מרחוק, מכל מקום ובכל זמן, באמצעות אמצעי המחשוב האישיים והארגוניים שברשותו.

עבודה מרחוק מאפשרת לעובדים לקבל גישה למערכות הארגוניות מה שעלול לחשוף את הארגון לפגיעות. המחשבים ניידים ומכשירים חכמים מאחסנים בתוכם מידע רב ועלולים להוות "שער כניסה" פוטנציאלי עבור תוקפים אשר מטרתם לנצל ולאתר הזדמנויות וחולשות , במיוחד במצבים כאלו. לפיכך, קיימת חשיבות גבוהה להגן על העובדים , על אמצעי המחשוב הארגוניים והאישיים ועל המידע המאוחסן בהם.

מסמך זה, הינו מסמך המלצות להגנה עבור בעלי העסקים והעובדים המאפשרים עבודה מרחוק. מטרת ההמלצות היא לצמצם במספר צעדים פשוטים ומהירים את סיכוני הסייבר כתוצאה מעבודה מהבית של עובדים.

המסמך מבוסס על המלצות מערך הסייבר הלאומי, המלצות אתרי מודעות סייבר בעולם וכן המלצות אבטחה של החברות המפעילות.

קהל יעד

מסמך זה נכתב עבור מנהלי ארגון, בעלי עסקים, עובדים, אנשי IT, מנהלי מערכות מידע (מנמ"ר), מנהלי הגנת מידע וסייבר (CISO).
כמו כן, אנשי IT וביקורת פנים בעולם ה-IT והסייבר עשויים אף הם לקבל ערך מוסף מקריאת מסמך זה.

← המלצות להגנה על רשת הארגון

מה העובד ומה הארגון נדרשים לעשות על מנת להגן על הארגון?

- רצוי כי הגישה מרחוק תתבצע מאמצעי **קבוע** אשר מוכר לאיש/אשת המחשוב של הארגון.
- יש לבחון הענקת **הרשאות גישה מרחוק לתיקיות** מחשוב. מומלץ להתיר גישה לתיקיות חיוניות בלבד.
- מומלץ **להפריד גישה לדוא"ל לבין גישה לשרת/תיקיות/נכסים רגישים**. לאחר בחינה ארגונית ובמידה והמסקנה היא כי הדבר הכרחי, מומלץ לפתוח את הגישה לפרק הזמן הנדרש בלבד באמצעות איש המחשוב הארגוני.
- הסרת **הרשאות גישה של העובד/ת למערכות ארגוניות/ממשקים שאינם חיוניים** - הגדירו הרשאות גישה עבור תוכנות הרלוונטיות לממשקי העבודה בלבד (לדוגמה: במידה ומנהל/ת הכספים נדרש/ת לעבוד מהבית, אפשרו גישה למערכת השכר לפרק הזמן הנדרש בלבד). אחת לתקופה, בדקו האם ההרשאות אשר הוקנו עדיין רלוונטיות ואם לא, הסירו את ההרשאות שאינן נדרשות.
- ביצוע **גיבויים** לכל המכשירים ולמידע האגור בהם. במקרה של פריצה או השבתה של המכשיר, ניתן יהיה לשחזר את המידע. עדיף לבצע את הגיבוי להתקן חיצוני נייד וכן גיבוי בענן.
- הגדרת **מדיניות אכיפת הגדרת סיסמאות מורכבות/קשות לניחוש** באמצעות מנגנון ניהול המשתמשים (כגון GPO במיקרוסופט), ואילוץ המשתמש **להחליף סיסמה באופן עיתי**, במידת האפשר גם הגדרת **OTP** (one time password) כאמצעי זיהוי נוסף.
- יש להגדיר כי חיבור המשתמש (Session) יהיה לפרק זמן מוגבל (X דקות/שעות).
- יש לוודא בחוקת ה-Fire-Wall (הארגוני והמקומי) **טיוב חוקים** אשר מאפשרים גישה מרחוק, כך שגישה זו תצומצם למינימום וכן כי מתקבלים **לוגים** לתיעוד ההתחברות. בנוסף, מומלץ להגדיר מדינות/אזורים אשר מורשים להתחבר לארגון. לטיוב החוקה ב-FW המקומי מבוסס מערכת ההפעלה של Microsoft, היכנסו ל-

https://support.microsoft.com/he-il/help/4026516/windows-use-remote-assistance-to-let-someone-fix-your-pc

לארגונים להם יש בנוסף Fire-Wall ארגוני של יצרן אחר, יש לפנות ליצרן לטובת הנחיות לטיוב החוקה.

- למתקדמים:
  - במחשב נייח/נייד, יש **להגביל את הגישה לשורת פקודה** (דוגמת PowerShell) כך שלא יהיה ניתן להריץ סקריפטים שמקורם לא ידוע, או שמקורם ממחשב אחר.
  - מומלץ לאפשר לעובד.ת התחברות דרך **ממשק מאובטח** (כגון Terminal Services).
  - הקלטת ה-session ושמירת ההקלטה לפרק זמן קבוע (חודשים/שבועות).

← מודעות עובדים

בעת מתן אישור לעובד לעבודה מרחוק, חשוב לבצע הדרכת מודעות קצרה, שתכלול את הנקודות הבאות:

- חשיבות **נעילת המכשיר** באמצעות סיסמה חזקה, אמצעי ביומטרי, קוד, או נעילת דפוס וכן הגדרת **נעילה אוטומטית לאחר אי-שימוש במשך זמן קצוב** (רצוי לבחור כהגדרת מחדל את המינימום האפשרי).
- הפעלת **אימות דו שלבי** (2FA) **בכל מכשיר וכל חשבון** המאפשר זאת.
- ניהול **שתי תיבות דוא"ל נפרדות** - אחת לעבודה ואחת לפעילות פרטית, יצירת סיסמה שונה עבור כל חשבון וכן וידוא הפעלת אימות דו-שלבי.
- **הימנעות** ככל האפשר **מלהתחבר לרשת Wi-Fi מזדמנת** (של השכנים לדוגמה) שאינה מאובטחת ולהעדיף להתחבר באמצעות VPN או רשת סלולרית. במידה וניתן להתחבר רק מרשת ה-Wi-Fi הביתית יש לוודא כי הרשת פרטית וכי מוגדרת סיסמת כניסה מורכבת שאינה ברירת המחדל של היצרן ואשר לא בוצע בה שימוש בחשבון אחר שברשותו.
- לרוב, **הנתב הביתי** בעל אבטחה לקויה וקל לפרוץ אותו ולכן חשוב לבצע מספר צעדים פשוטים כדי לאבטחו. להרחבה קראו: https://www.gov.il/he/departments/publications/reports/homenetwork
- מומלץ כאמור כי יוגדר שעדכוני תוכנה יבוצעו אוטומטית, אולם אם לא בוצעה הגדרה זו אז טרם מסירת המחשב לעובד.ת, יש להדריך אותו.אותה כיצד לבצע עדכוני תוכנה וכן אודות תדירות העדכון הנדרשת.
- יש לחדד ערנות מפני **ניסיונות דיוג** (פישינג על כל סוגיו) המתקבלים בערוצי התקשורת השונים (פרטי וארגוני) וכן חובת עדכון העובד.ת את ה-IT או מנהל.ת בכל חשד לניסיון שכזה.

← המלצות הגנה עבור העובד (ציוד מחשוב/מידע)

מומלץ לוודא כי על אמצעי המחשוב בבית (מחשב נייח/נייד/טאבלט/סמארטפון:

- כלל המכשירים ברשות העובד, הארגוניים והאישיים - נעולים בסיסמה (PIN, נעילת דפוס, ביומטרי, כרטיס חכם וכד').
- מותקנת **תוכנת אנטי וירוס** (Anti-Virus) **מעודכנת**. התוכנה מבצעת סריקה בניסיון לאתר וירוסים ואיומי מחשב שונים.
- מותקנת במכשיר **תוכנת חומת אש** (Fire-Wall) מעודכנת.
- במחשבי נייח/נייד בהן מותקנת מערכת Microsoft חשוב לוודא כי Windows Defender אכן מופעל (ע"י התחלה -> הגדרות -> אבטחה)
- מותקן **VPN** (רשת וירטואלית פרטית) להתחברות מאובטחת ופרטית בין העובד למשאבי הארגון וכן הפעלת **אימות דו שלבי/רב גורמי** (MFA/2FA) בשימוש בדרך זו - בעדיפות אימות זיהוי שאינו מבוסס מסרון (SMS).
- הגדרת ביצוע **עדכוני תוכנה אוטומטית לכלל התוכנות** במכשיר (מומלץ להגדיר עדכונים לשעות הלילה), כולל דפדפנים. בנוסף, חשוב לבצע עדכון יזום במכשירים החכמים למערכת ההפעלה מיד עם פרסומם.

במידה ותוכנה מסוימת אינה מאפשרת עדכונים אוטומטיים, מומלץ לשים תזכורת לבחון באופן חודשי את עדכניות התוכנה מול אתר האינטרנט של היצרן, ולבצע עדכון ידני בעת הצורך.

ביבליוגרפיה

1. https://www.techrepublic.com/article/how-to-maintain-safe-cybersecurity-practices-while-transitioning-workers-from-the-office-to-remote-workstations/
2. https://www.inc.com/neill-feather/how-to-protect-your-remote-employees-from-cyber-threats.html
3. https://www.securityplanner.org/#/action-plan/1JoW1HICfgDMc6FO
4. https://www.gov.il/he/departments/policies/endstation
5. https://www.gov.il/BlobFolder/policy/small_bussines/he/cyber_booklet_small-bussines-Hangasha.pdf
6. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-46r1.pdf
7. https://www.gov.il/he/departments/publications/reports/homenetwork