אתן חוקרות פרטיות
אנליסטיות מומחיות, בעלות שם עולמי

נבחרתן
למשימה סודית

מתחילים

מבוסס על לומדה שפותחה ע"י נעמה מרוז עבור מגמת מידע ונתונים- Data Analysis

פותח מחדש עבור המגזר החרדי בידי דבורה פינסקי

שלום, אני משה ארבל,
מנכ"ל חברת סטרטאפ

אנחנו בבעיה רצינית, גילינו שאחד העובדים גנב מאגר כרטיסי אשראי של לקוחות שלנו.

הוא שלח לנו הודעה בו הוא מבקש סכום כסף גדול מאוד, בתמורה לאי שימוש במאגר.

אנחנו חייבים את עזרתכן!

המשימה שלכן

לאסוף נתונים,
למצוא את העובד שביצע את הגניבה

ולחזור למקבלי ההחלטות
עם תובנות מהמידע שאספתן

צאו לדרך

היכנסו לכל אחת מהמשימות

חיקרו ומצאו פרטים חשובים

חיזרו לכאן עם הנתונים שאספתן

העובדים החשודים

יהודה רוזנס - תאילנד
נועם סגל – ארצות הברית
ראובן גולדברג - קנדה
שלמה בר - ספרד

המיילים החשודים

איטליה, תאילנד,
מקסיקו, רוסיה,
בריטניה, ספרד

השיחות החשודות

יהודה רוזנס
נועם סגל

חיפוש נתונים בקובץ אקסל

גילינו שההודעה נשלחה מחו"ל...
אבל איך נדע איזה מהעובדים היו בחו"ל בשבוע האחרון בוצעה הגנבה?

לצורך כך, קיבלנו את קובץ נתוני העובדים שביקשו חופש
ניכנס לקובץ ונבדוק מי מהעובדים ביקש ימי חופשה בשבוע זה.

מתחילים לחפש

יש פה הרבה עובדים שלקחו חופש!

אבל חלק מהם לקחו חופש ממש קצר, של יום או יומיים.

ניכנס לטבלה ונסמן רק את מי שלקח 3 ימי חופשה ומעלה.

אבל רגע... לעבור על הרשימה אחד אחד ייקח המון זמן!

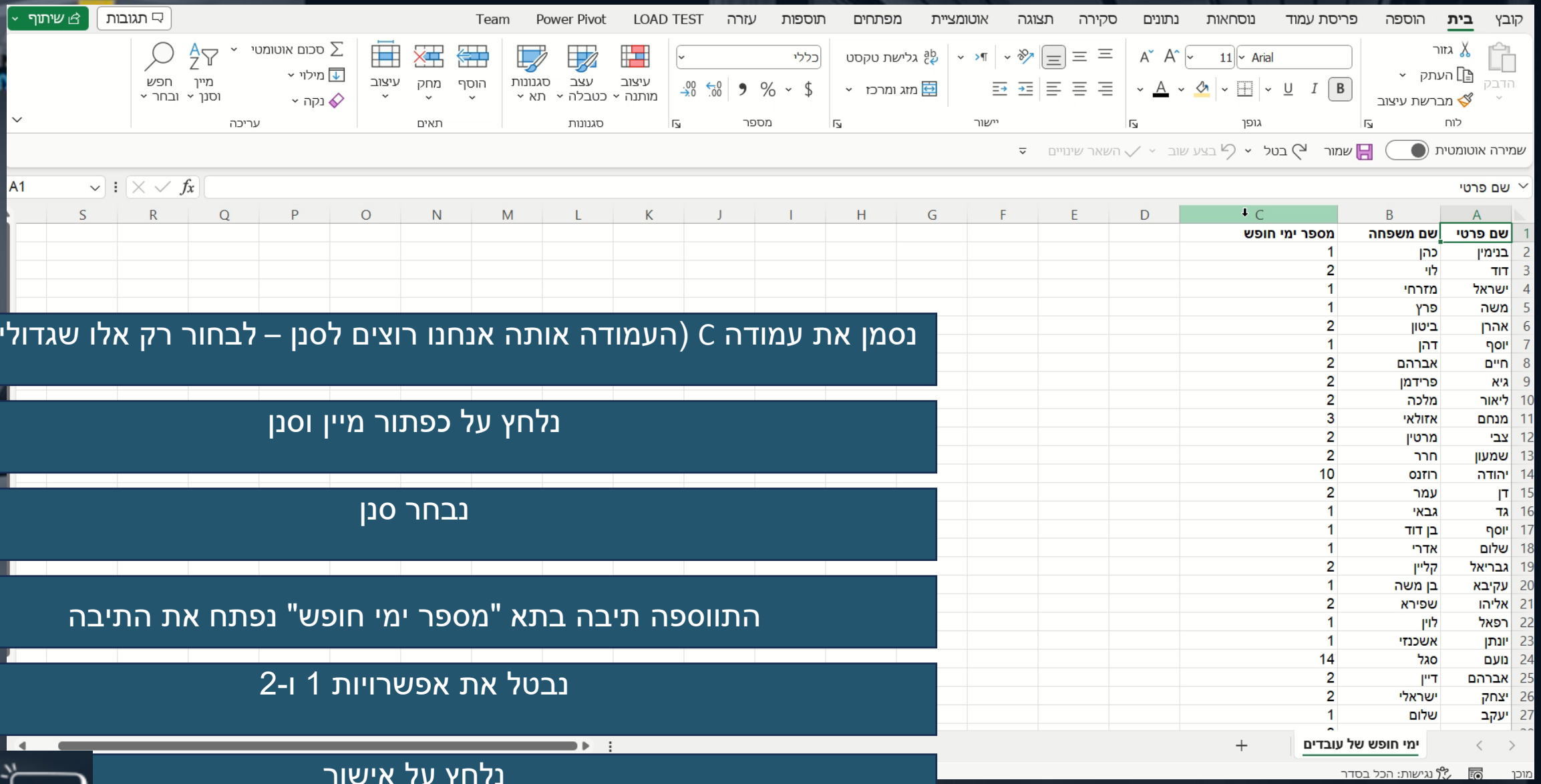
יש דרך לעשות את הסינון בלחיצת כפתור.

יודעות איך לעשות את זה?

	A	B	C
1	שם פרטי	שם משפחה	מספר ימי חופש
2	בנימין	כהן	1
3	דוד	לוי	2
4	ישראל	מזרחי	1
5	משה	פרץ	1
6	אהרן	ביטון	2
7	יוסף	דהן	1
8	חיים	אברהם	2
9	גיא	פרידמן	2
10	ליאור	מלכה	2
11	מנחם	אזולאי	3
12	צבי	מרטין	2
13	שמעון	חרר	2
14	יהודה	רוזנס	10
15	דן	עמר	2
16	גד	גבאי	1
17	יוסף	בן דוד	1
18	שלום	אדרי	1
19	גבריאל	קליין	2
20	עקיבא	בן משה	1
21	אליהו		
22	רפאל		
23	יונתן		
24	נועם		
25	אברהם		
26	יצחק		
27	יעקב	שלום	1

אין לי מושג!
מה זה בכלל סינון באקסל?

בטח!
לעשות סינון באקסל זה שגרתי אצלי



נסמן את עמודה C (העמודה אותה אנחנו רוצים לסנן – לבחור רק אלו שגדולים מ-3)

נלחץ על כפתור מיין וסנן

נבחר סנן

התווספה תיבה בתא "מספר ימי חופש" נפתח את התיבה

נבטל את אפשרויות 1 ו-2

נלחץ על אישור

נסמן את עמודה C (העמודה אותה אנחנו רוצים לסנן – לבחור רק אלו שגדולים מ-3)

נלחץ על כפתור מיין וסנן

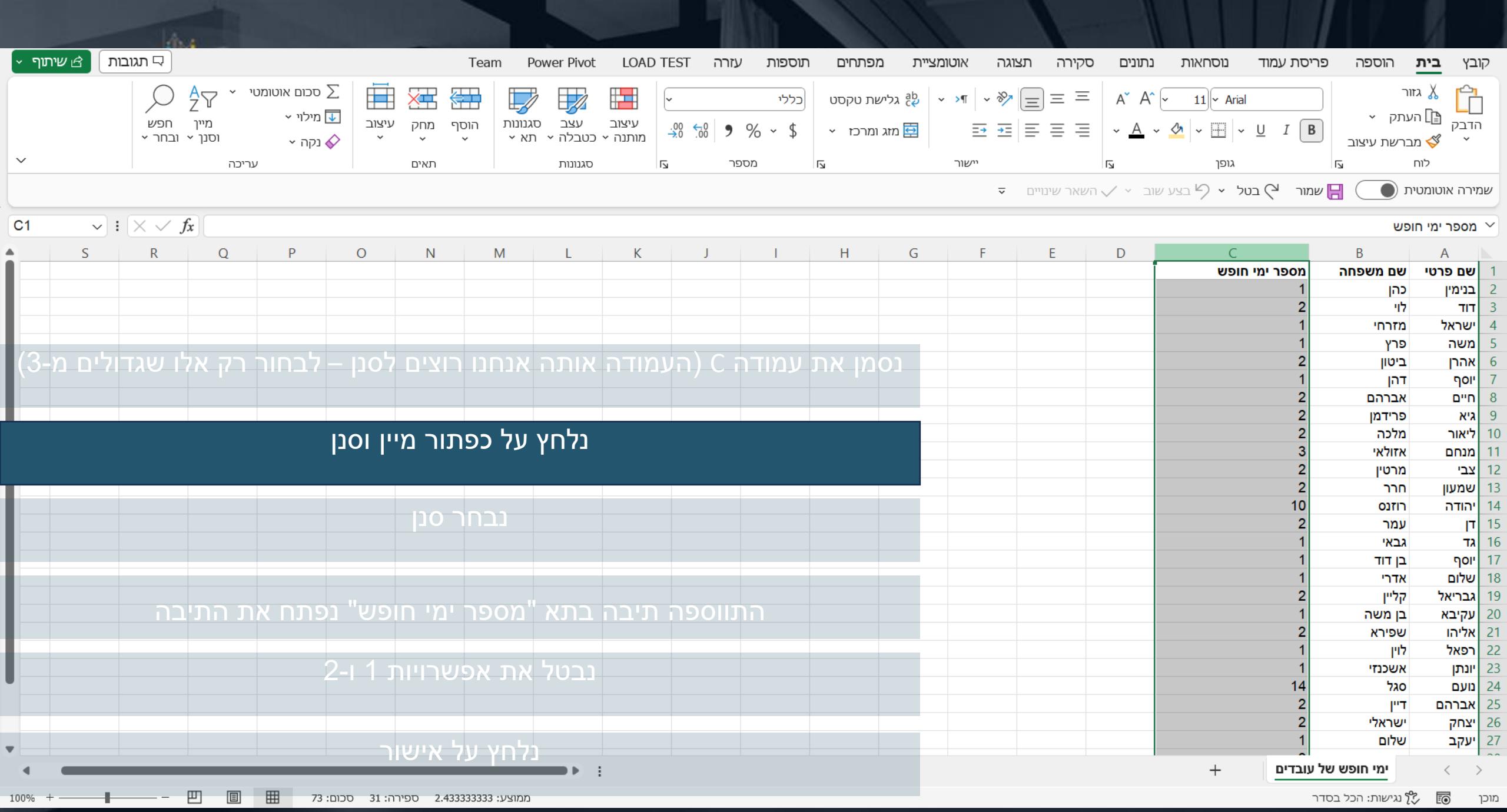
נבחר סנן

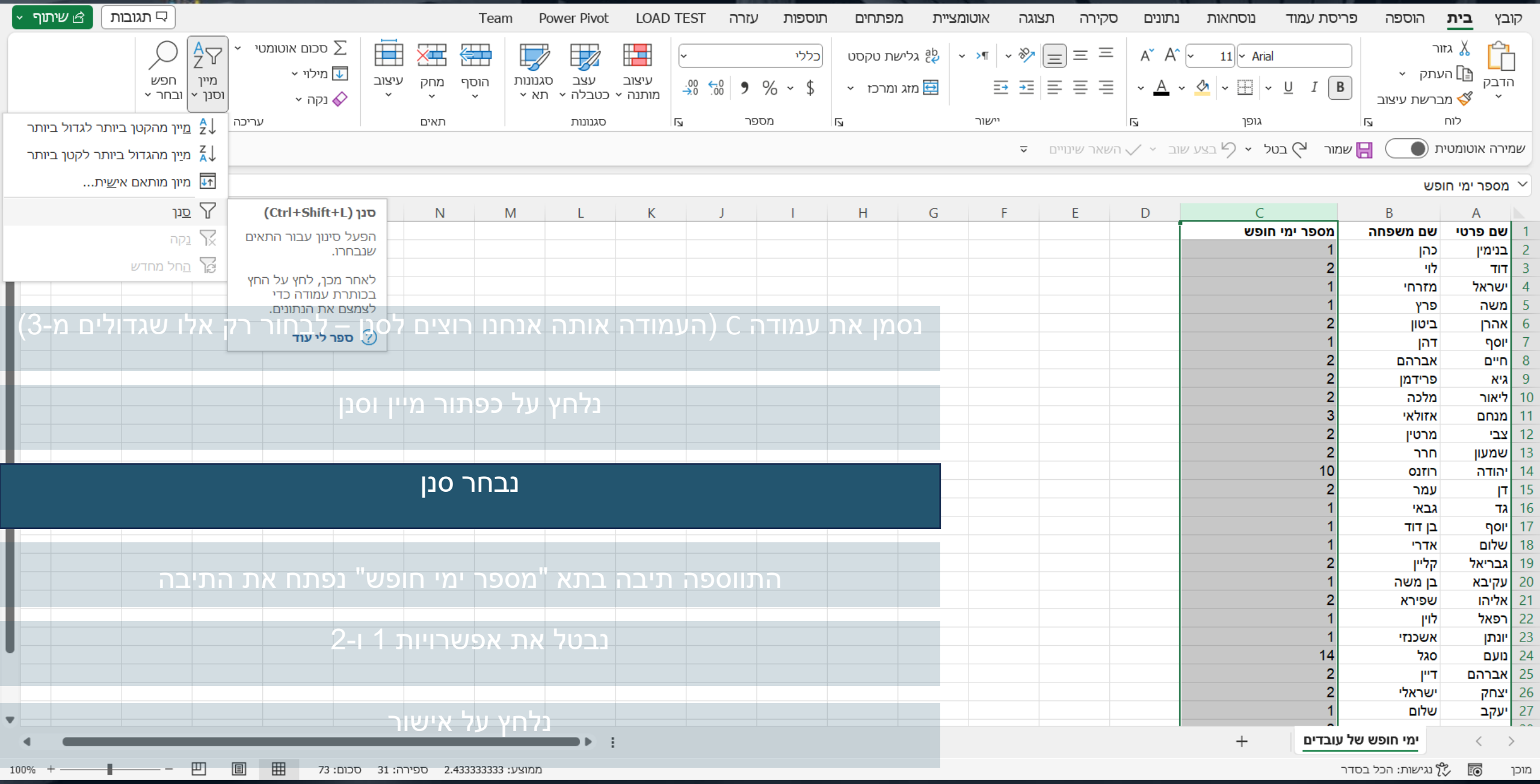
התווספה תיבה בתא "מספר ימי חופש" נפתח את התיבה

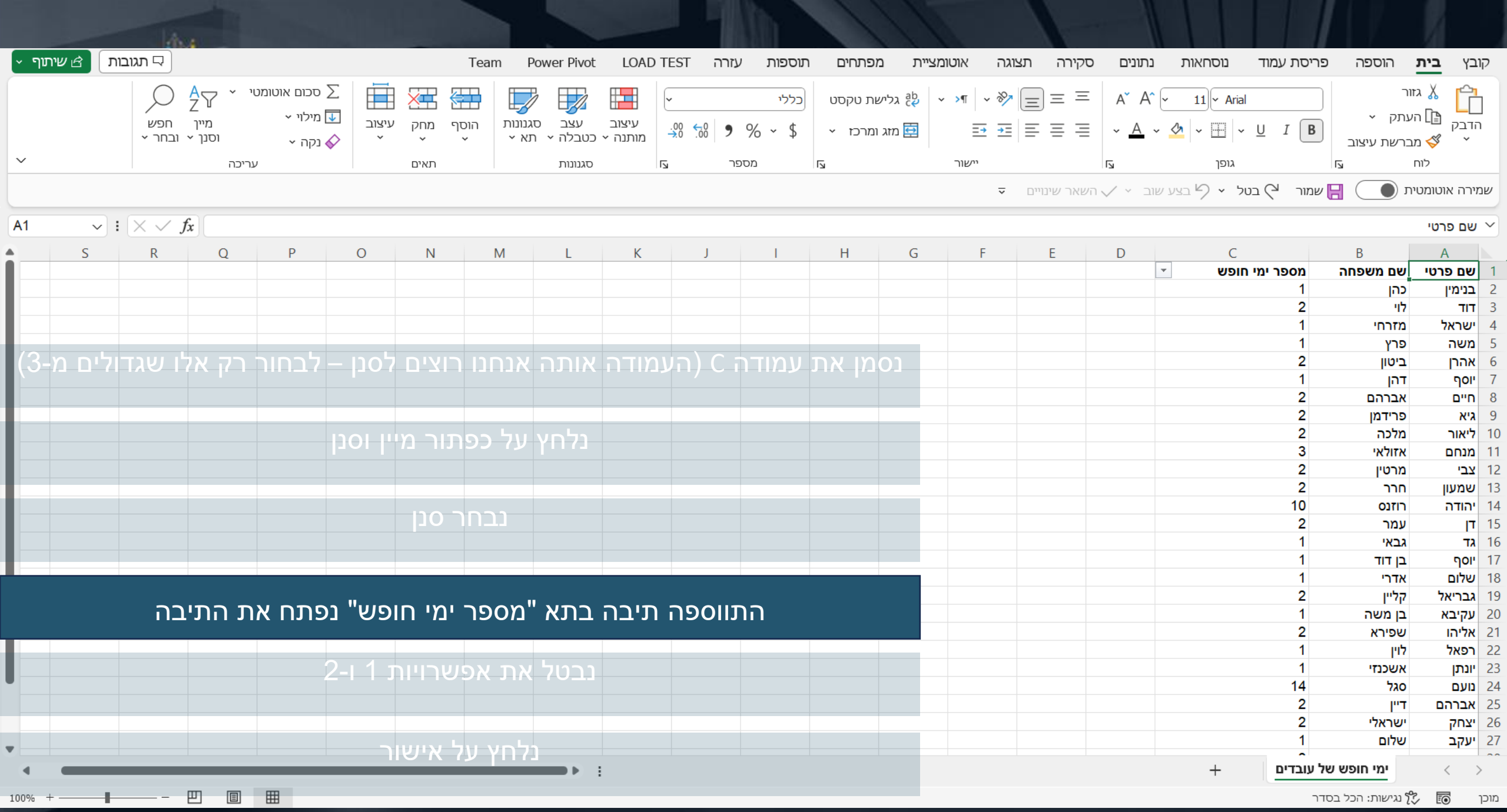
נבטל את אפשרויות 1 ו-2

נלחץ על אישור

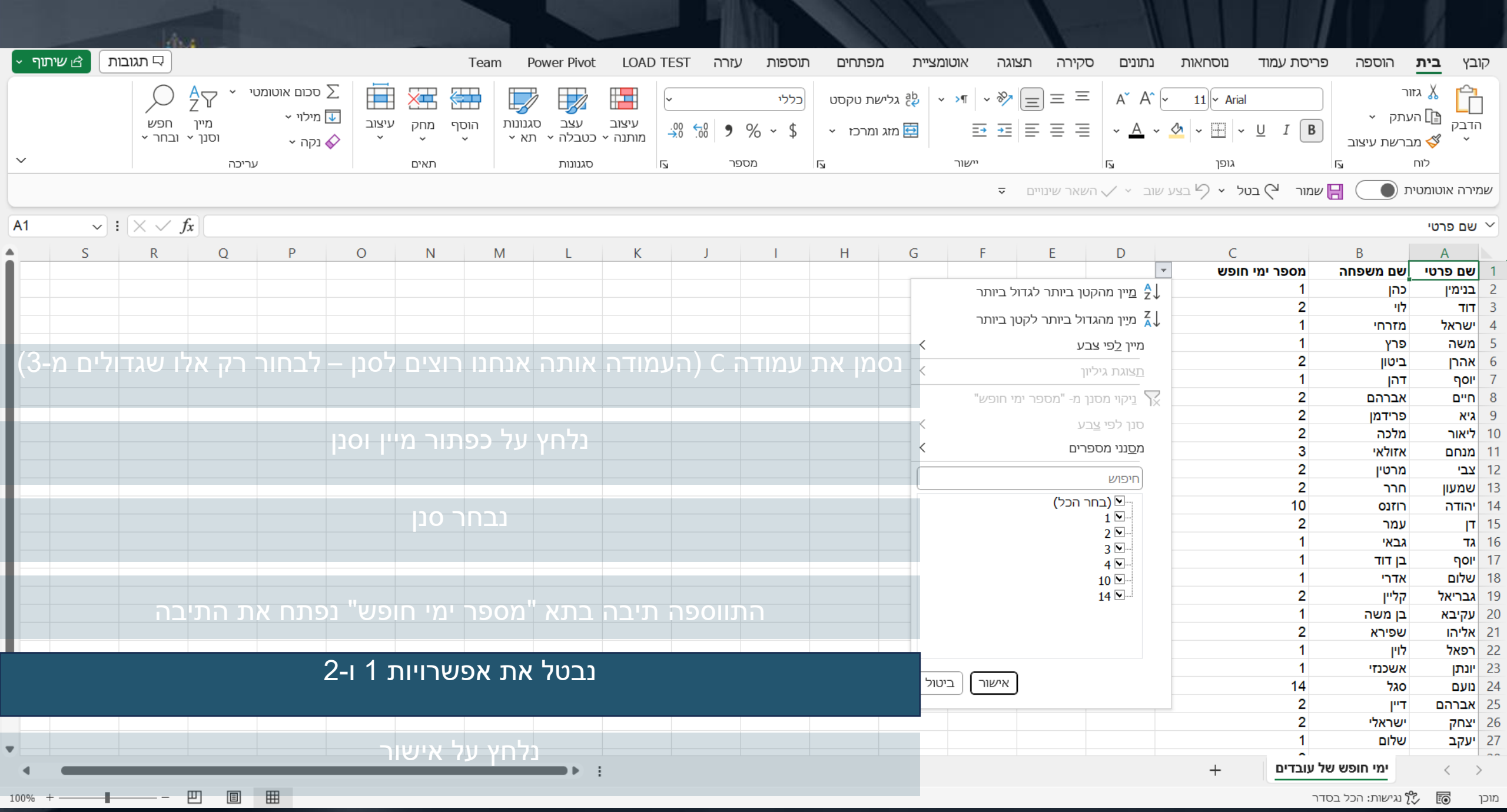
שם פרטי	שם משפחה	מספר ימי חופש
בנימין	כהן	1
דוד	לוי	2
ישראל	מזרחי	1
משה	פרץ	1
אהרן	ביטון	2
יוסף	דהן	1
חיים	אברהם	2
גיא	פרידמן	2
ליאור	מלכה	2
מנחם	אזולאי	3
צבי	מרטין	2
שמעון	חרר	2
יהודה	רוזנס	10
דן	עמר	2
גד	גבאי	1
יוסף	בן דוד	1
שלום	אדרי	1
גבריאל	קליין	2
עקיבא	בן משה	1
אליהו	שפירא	2
רפאל	לוין	1
יונתן	אשכנזי	1
נועם	סגל	14
אברהם	דיין	2
יצחק	ישראלי	2
יעקב		1

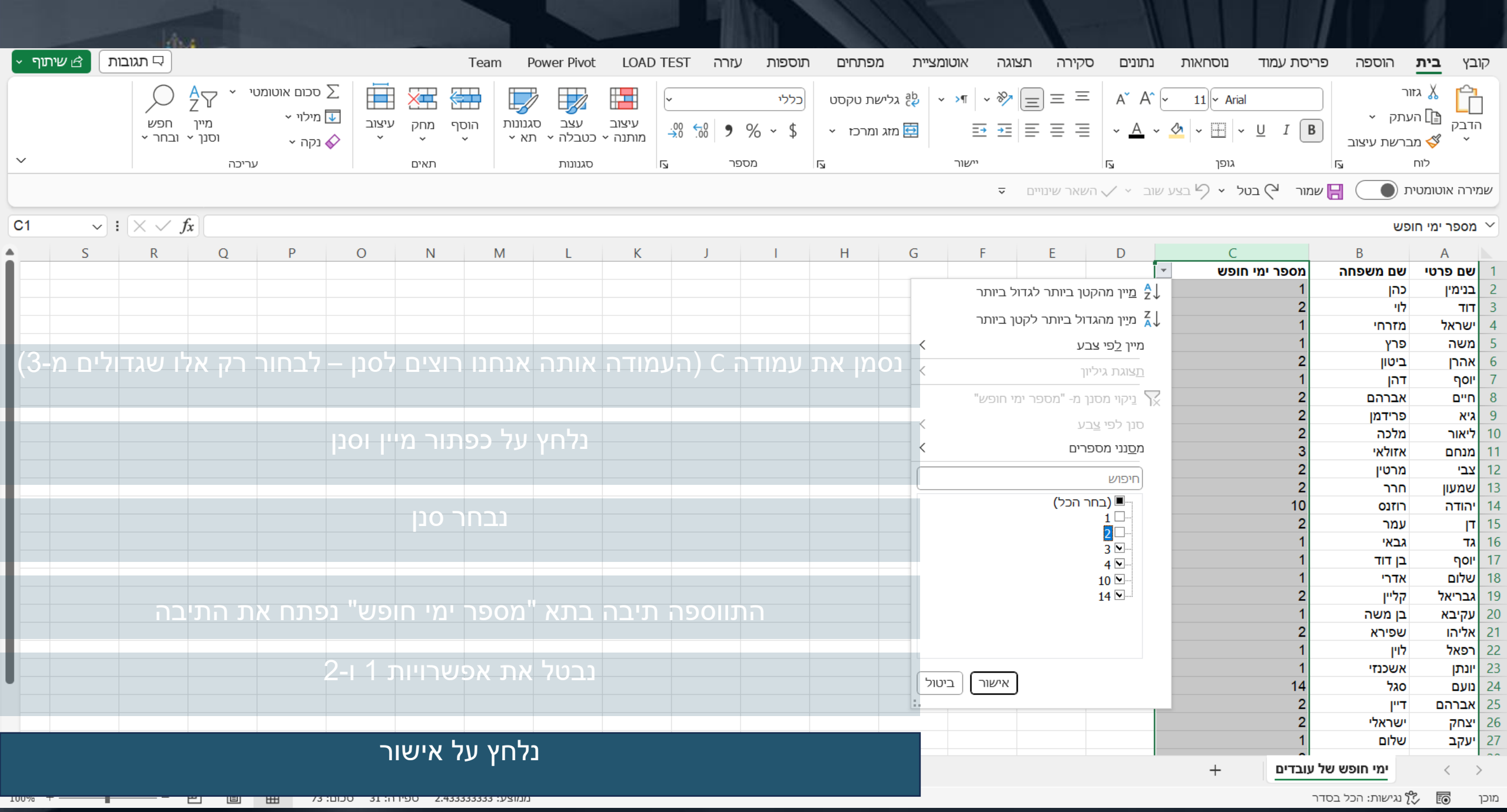

נסמן את עמודה C (העמודה אותה אנחנו רוצים לסנן – לבחור רק אלו שגדולים מ-3)
נלחץ על כפתור מיין וסנן
נבחר סנן
התווספה תיבה בתא "מספר ימי חופש" נפתח את התיבה
נבטל את אפשרויות 1 ו-2
נלחץ על אישור
מספר ימי חופש
שם פרטי
שם משפחה
בנימין כהן 1
דוד לוי 2
ישראל מזרחי 1
משה פרץ 1
אהרן ביטון 2
יוסף דהן 1
חיים אברהם 2
גיא פרידמן 2
ליאור מלכה 2
מנחם אזולאי 3
צבי מרטין 2
שמעון חרר 2
יהודה רוזנס 10
דן עמר 2
גד גבאי 1
יוסף בן דוד 1
שלום אדרי 1
גבריאל קליין 2
עקיבא בן משה 1
אליהו שפירא 2
רפאל לוין 1
יונתן אשכנזי 1
נועם סגל 14
אברהם דיין 2
יצחק ישראלי 2
יעקב שלום 1
ימי חופש של עובדים


נסמן את עמודה C (העמודה אותה אנחנו רוצים לסנן – לבחור רק אלו שגדולים מ-3)
נלחץ על כפתור מיין וסנן
נבחר סנן
התווספה תיבה בתא "מספר ימי חופש" נפתח את התיבה
נבטל את אפשרויות 1 ו-2
נלחץ על אישור
מיין וסנן
מיין מהקטן ביותר לגדול ביותר
מיין מהגדול ביותר לקטן ביותר
מיון מותאם אישית...
סנן
נקה
החל מחדש
סנן (Ctrl+Shift+L)
הפעל סינון עבור התאים שנבחרו.
לאחר מכן, לחץ על החץ בכותרת עמודה כדי לצמצם את הנתונים.
ספר לי עוד
מספר ימי חופש
שם פרטי
שם משפחה
מספר ימי חופש
בנימין כהן 1
דוד לוי 2
ישראל מזרחי 1
משה פרץ 1
אהרן ביטון 2
יוסף דהן 1
חיים אברהם 2
גיא פרידמן 2
ליאור מלכה 2
מנחם אזולאי 3
צבי מרטין 2
שמעון חרר 2
יהודה רוזנס 10
דן עמר 2
גד גבאי 1
יוסף בן דוד 1
שלום אדרי 1
גבריאל קליין 2
עקיבא בן משה 1
אליהו שפירא 2
רפאל לוין 1
יונתן אשכנזי 1
נועם סגל 14
אברהם דיין 2
יצחק ישראלי 2
יעקב שלום 1
ימי חופש של עובדים



שם פרטי	שם משפחה	מספר ימי חופש
בנימין	כהן	1
דוד	לוי	2
ישראל	מזרחי	1
משה	פרץ	1
אהרן	ביטון	2
יוסף	דהן	1
חיים	אברהם	2
גיא	פרידמן	2
ליאור	מלכה	2
מנחם	אזולאי	3
צבי	מרטין	2
שמעון	חרר	2
יהודה	רוזנס	10
דן	עמר	2
גד	גבאי	1
יוסף	בן דוד	1
שלום	אדרי	1
גבריאל	קליין	2
עקיבא	בן משה	1
אליהו	שפירא	2
רפאל	לוין	1
יונתן	אשכנזי	1
נועם	סגל	14
אברהם	דיין	2
יצחק	ישראלי	2
יעקב	שלום	1


נסמן את עמודה C (העמודה אותה אנחנו רוצים לסנן – לבחור רק אלו שגדולים מ-3)
נלחץ על כפתור מיין וסנן
נבחר סנן
התווספה תיבה בתא "מספר ימי חופש" נפתח את התיבה
נבטל את אפשרויות 1 ו-2
נלחץ על אישור
מיין מהקטן ביותר לגדול ביותר
מיין מהגדול ביותר לקטן ביותר
מיין לפי צבע
תצוגת גיליון
ניקוי מסנן מ- "מספר ימי חופש"
סנן לפי צבע
מסנני מספרים
חיפוש
(בחר הכל)
1
2
3
4
10
14
אישור
ביטול
שם פרטי
שם משפחה
מספר ימי חופש
בנימין כהן 1
דוד לוי 2
ישראל מזרחי 1
משה פרץ 1
אהרן ביטון 2
יוסף דהן 1
חיים אברהם 2
גיא פרידמן 2
ליאור מלכה 2
מנחם אזולאי 3
צבי מרטין 2
שמעון חרר 2
יהודה רוזנס 10
דן עמר 2
גד גבאי 1
יוסף בן דוד 1
שלום אדרי 1
גבריאל קליין 2
עקיבא בן משה 1
אליהו שפירא 2
רפאל לוין 1
יונתן אשכנזי 1
נועם סגל 14
אברהם דיין 2
יצחק ישראלי 2
יעקב שלום 1
ימי חופש של עובדים


נסמן את עמודה C (העמודה אותה אנחנו רוצים לסנן – לבחור רק אלו שגדולים מ-3)
נלחץ על כפתור מיין וסנן
נבחר סנן
התווספה תיבה בתא "מספר ימי חופש" נפתח את התיבה
נבטל את אפשרויות 1 ו-2
נלחץ על אישור
מיין מהקטן ביותר לגדול ביותר
מיין מהגדול ביותר לקטן ביותר
מיין לפי צבע
תצוגת גיליון
ניקוי מסנן מ- "מספר ימי חופש"
סנן לפי צבע
מסנני מספרים
חיפוש
(בחר הכל)
1
2
3
4
10
14
אישור
ביטול
מספר ימי חופש
ימי חופש של עובדים

שם פרטי	שם משפחה	מספר ימי חופש
מנחם	אזולאי	3
יהודה	רוזנס	10
נועם	סגל	14
ראובן	גולדברג	4
שלמה	בר	3

ימי חופש של עובדים

אז מה למדנו?

בעולם נצבר המון מידע: בחברות על העובדים, בביה"ס על התלמידים, בעירייה על תושבים, בממשלה על אזרחים וכדו'.

כדי להשתמש בכמויות האדירות של המידע, צריך להשתמש בכלי לניתוח נתונים.

אתן השתמשתן ב**אקסל** וביצעתן פעולת סינון.

הפעולה הזאת צמצמה את החיפוש ואפשרה להגיע ל-5 תוצאות מתוך 267

יעיל, לא?

סיימנו את משימה 1

נשארנו עם 5 שמות חשודים שלקחו 3 ימי חופשה ומעלה.

אבל איך נדע אם הם טסו או לאן?

בואו נתקדם לשלב הבא ונגלה

משימה 2

נשארנו עם 5 עובדים חשודים, **שייתכן** שטסו לחו"ל בזמן החופשה וביצעו את המעילה.
אבל...
איך נוכל לדעת האם אכן טסו לחו"ל ואם כן, לאן?

סמני איפה כדאי לבדוק כדי לוודאי אם אכן טסו לחו"ל

- שיחות אחרונות שביצעו מהעמדה במשרד ✓
- המחשב במשרד ✓
- מצלמת אבטחה ✓

הבדיקה העלתה את הסימנים הבאים:

מנחם אזולאי – בדיקה במחשב במשרד גילתה הרבה מסמכים רפואיים, השיחות האחרונות היו לרופאים מומחים.
מצלמת האבטחה גילתה שהסתובב בימים האחרונים בפנים מודאגות במיוחד.
בדיקה מעמיקה יותר גילתה שיש לו בת חולה שמתחילה עכשיו אשפוז ארוך, בבי"ח בארץ.

יהודה רוזנס – התקשר בימים האחרונים, למספרי טלפון בקידומת של תאילנד.
בנוסף, התקשר לסוכני נסיעות שמתמחים בטיולים למזרח הרחוק.

נועם סגל – התקשר בימים האחרונים למספרי טלפון בקידומת ארצות הברית.
מצלמת האבטחה ראתה אותו מעיין במשרד בהזמנה לחתונה של קרובי משפחה בארה"ב.

ראובן גולדברג – התקשר בימים האחרונים למספרי טלפון בקידומת קנדה
במחשב במשרד גילו קובץ עם טיולים אפשריים בקנדה ובסביבה

שלמה בר – התקשר בימים האחרונים למספרי טלפון בקידומת ספרד.

"עין רואה ואוזן שומעת **וכל מעשיך בספר נכתבים**"

אז מה למדנו?

כיום, אנחנו משאירים עקבות בכל מקום.

שרתים ומאגרי מידע מתוכננים לשמור כמויות עתק של נתונים

כל פעולה דיגיטלית נשמרת.

התקשרת לברר מתי מגיע האוטובוס? המידע הזה נשמר.

תמונות ממצלמות אבטחה, תיעוד שיחות יוצאות ונכנסות.

ועוד ועוד...

כל הכבוד! סיימנו את השלב עם מידע חשוב ביותר!

גילינו ש:

יהודה רוזנס היה בתאילנד

נועם סגל היה בארצות הברית

ראובן גולדברג היה בקנדה

שלמה בר היה בספרד

המשך

איתור כתובות מייל חשודות

מייל מהגנב התקבל מכתובת עם סיומת לא מוכרת,
יש לנו פה את רשימת המיילים החריגים שהתקבלו בחברה בשבוע הסחיטה

בואו נבדוק מהיכן הגיעו המיילים עם הסיומות החריגות

קדימה למשימה

איתור כתובות מייל חשודות

היכנסו לטבלת סיומות, בדקו מאלו מדינות הגיעו המיילים החשודים
העבירו קו בין כל מייל למדינה ממנה הוא הגיע.

יש ללחוץ על הנקודה שליד כתובת המייל, ואח"כ על הנקודה שליד המדינה.

ארצות הברית	agadaultc@dell.es
מקסיקו	dolos@goo.ne.mx
יפן	egera1@rambler.uk
ספרד	ipinso@rambler.ru
בריטניה	ckeevers1g@goo.th
טורקיה	bblestr@thetimes.it
איטליה	
רוסיה	
תאילנד	

טעות, נסי שנית

סיומת	מדינה / ארץ / אזור
.ae	איחוד האמירויות הערביות
.ar	ארגנטינה
.at	אוסטריה
.au	אוסטרליה
.be	בלגיה
.bg	בולגריה
.br	ברזיל
.ca	קנדה
.ch	שווייץ
.cy	קפריסין
.cz	צ'כיה
.de	גרמניה
.dk	דנמרק
.eg	מצרים
.es	ספרד
.et	אתיופיה
.eu	האיחוד האירופי
.fi	פינלנד
.fr	צרפת

סיומת	מדינה / ארץ / אזור
.ge	גאורגיה
.gr	יוון
.hk	הונג קונג
.il	ישראל
.in	הודו
.iq	עיראק
.ir	איראן
.is	איסלנד
.it	איטליה
.jo	ירדן
.jp	יפן
.lb	לבנון
.ly	לוב
.ma	מרוקו
.mx	מקסיקו
.nl	הולנד
.no	נורווגיה
.pa	פנמה
.pk	פקיסטן

סיומת	מדינה / ארץ / אזור
.ps	הרשות הפלסטינית
.pt	פורטוגל
.ro	רומניה
.ru	רוסיה
.sa	ערב הסעודית
.sd	סודאן
.se	שוודיה
.sk	סלובקיה
.su	ברית המועצות
.sy	סוריה
.sz	שווייץ
.th	תאילנד
.tr	טורקיה
.ua	אוקראינה
.ug	אוגנדה
.uk	בריטניה
.us	ארצות הברית
.ye	תימן
.za	דרום אפריקה

איתור כתובות מייל חשודות

עשיתן עבודה מעולה!

איתרתן את המדינות מהן נשלחו המיילים החשודים:

איטליה	תאילנד	מקסיקו	רוסיה	בריטניה	ספרד

אז מה למדנו?

העולם שלנו מוצף במידע.

הרבה פעמים כל מה שצריך זה להגיע למידע הרלוונטי,

לבדוק אם הוא אמין ולהשתמש בו בצורה מושכלת.

כל הכבוד! סיימנו את השלב עם מידע חשוב ביותר!

גילינו שהמיילים החשודים נשלחו מהמדינות:

איטליה, תאילנד, מקסיקו, רוסיה, אנגליה וספרד.

המשך

הצלבת מידע ממפות המשרד

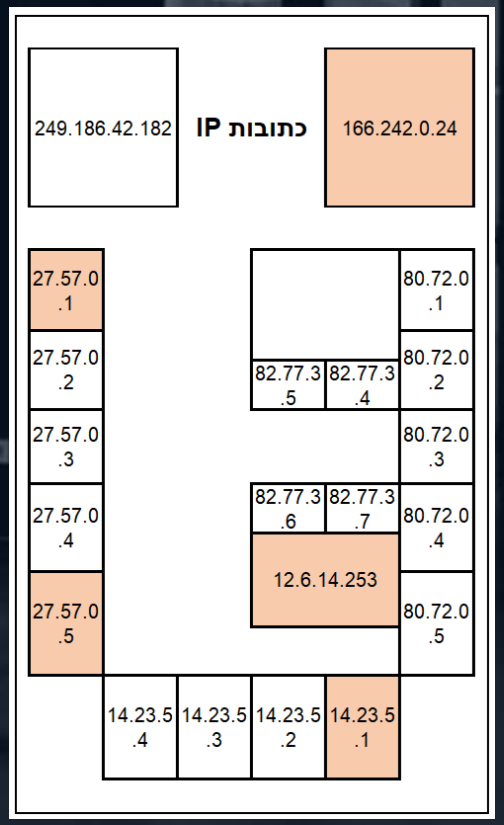
בחקירה גילינו שכדי לגנוב את כרטיסי האשראי, האזין הסוחט לשיחות בין נציגי שירות לבין לקוחות שמסרו את פרטי כרטיס האשראי.

קיבלנו את כתובות ה-IP שמהן בוצעה ההאזנה לשיחות ואת מפת המשרד שעליה מסומנים המחשבים החשודים.

בואו נצליב את המידע הזה עם מידע נוסף ונראה מי ביצע האזנות לא חוקיות לשיחות.

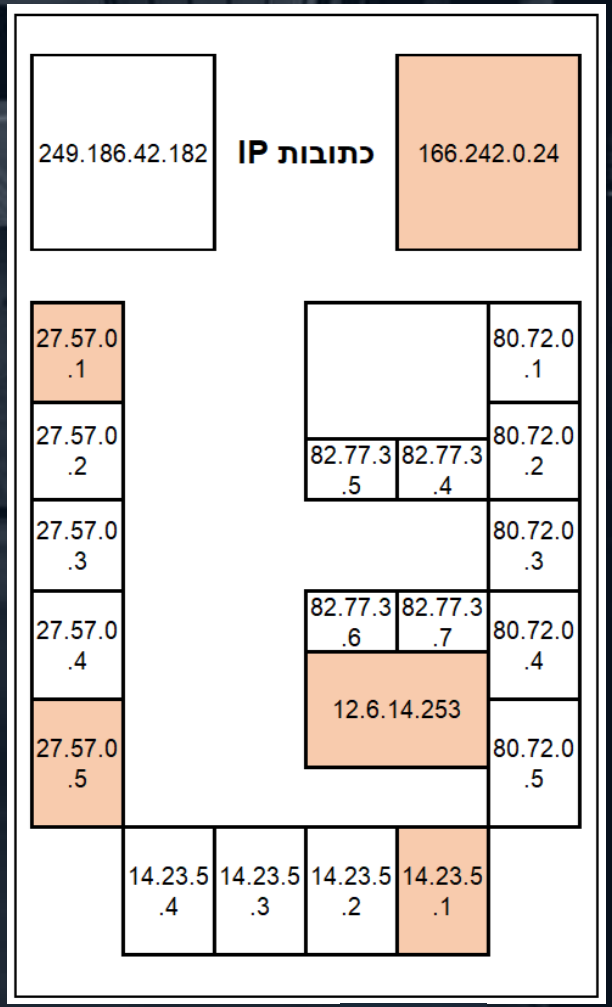
קדימה למשימה

הצלבת מידע ממפות המשרד

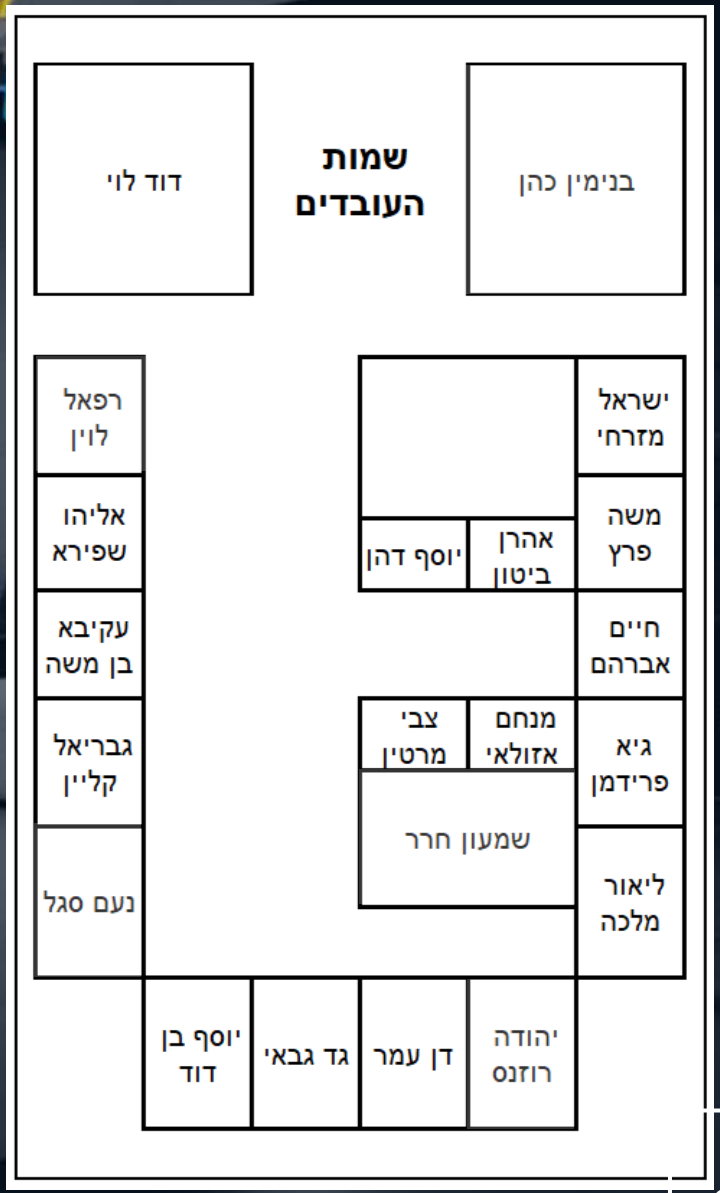


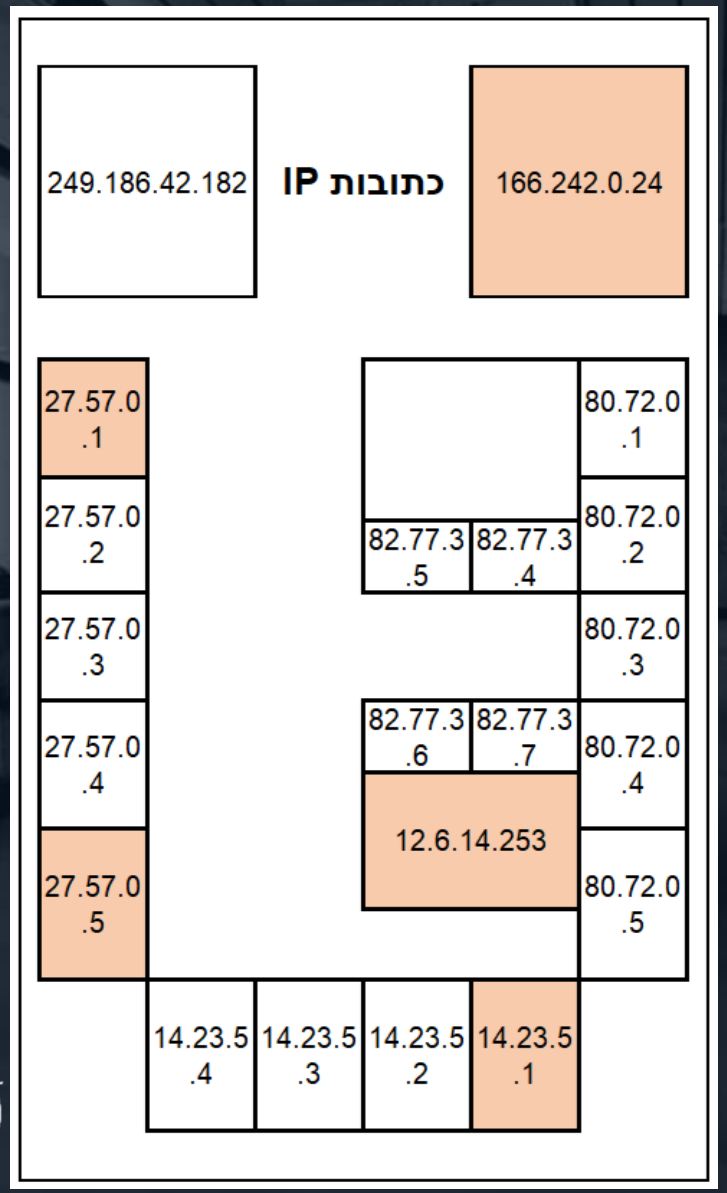
זו המפה עם כתובות ה-IP (המחשבים) שמהם בוצעו ההאזנות לשיחות.
מייד תקבלו מפות משרד נוספות עם פרטי מידע שונים.

הצליבו בין מפת ה-IP לבין המפה המתאימה ביותר כדי לקבל את המידע למציאת החשוד
איזו מפה כדאי לבדוק?



לחצו על שמות העובדים החשודים.





מדוע העובד חשוד בהאזנה?

עבודה מעולה!

נשארנו עם 5 שמות חשודים שהאזינו לשיחות

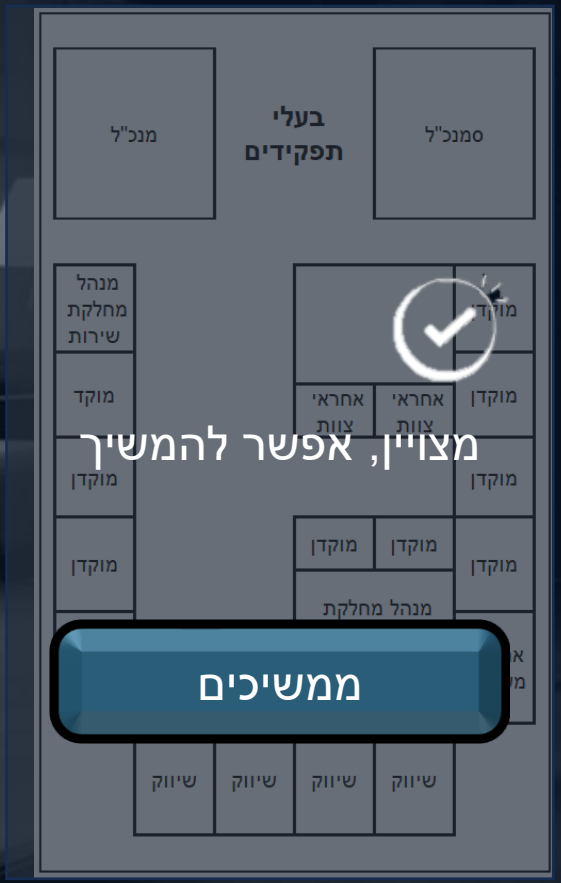
איך נדע למי מהם מותר להאזין לשיחות במסגרת התפקיד ולמי אסור?
נשאל את משה המנכ"ל.

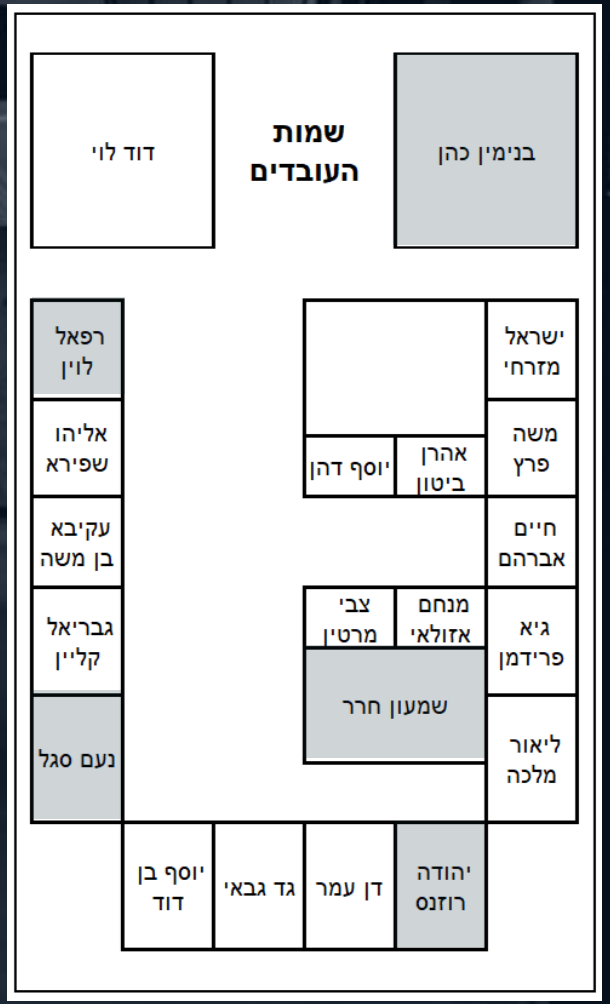
על פי נהלי החברה
רק מנהלים
רשאים להאזין לשיחות של
מחלקות השירות.

תוכלו לחשוב על מפה נוספת שבעזרתה נדע מי לא היה אמור להאזין לשיחות?

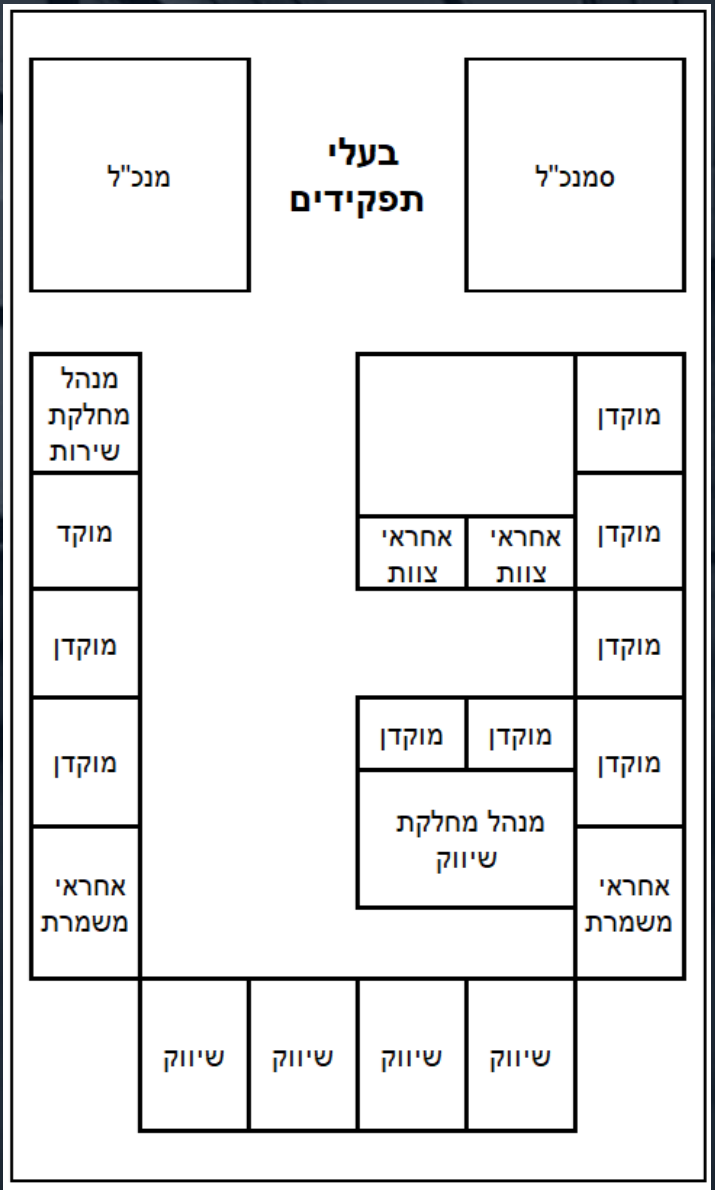
נעבור לרשימה ונבחר מפה נוספת.

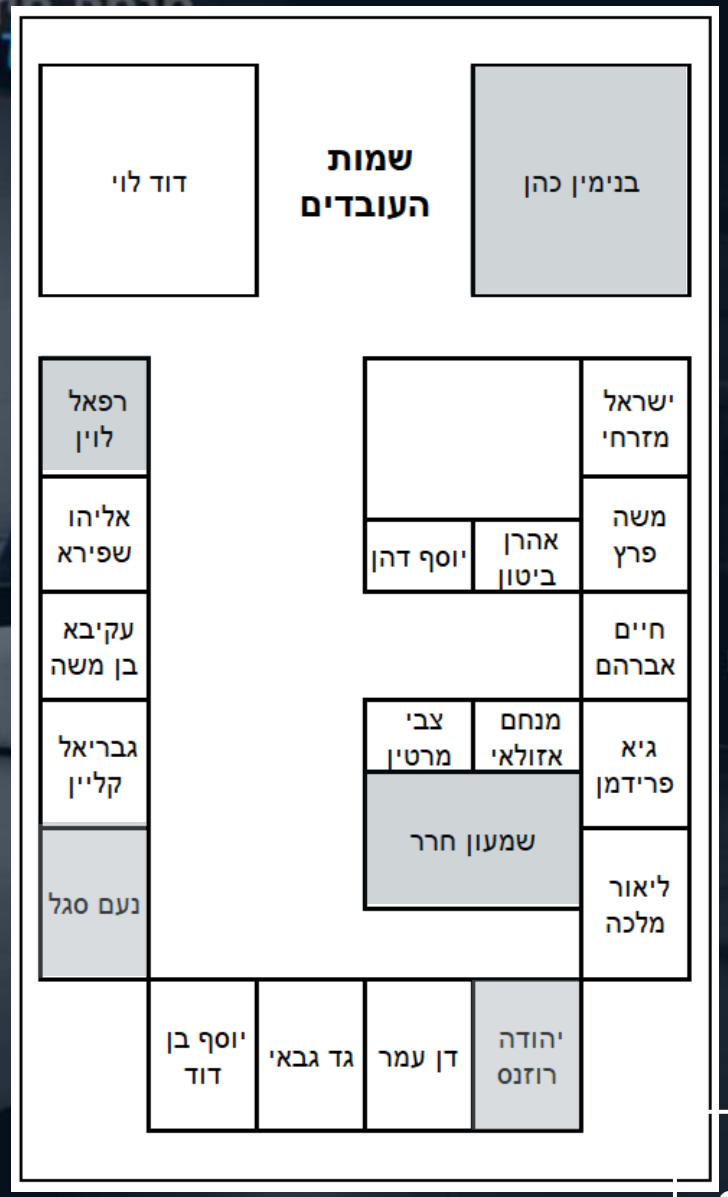
לחצו על שם המפה הנוספת שבעזרתה נדע מי לא היה אמור להאזין לשיחות.





זכרו, רק מנהלים רשאים להאזין לשיחות
לחצו על שמות העובדים שהאזינו לשיחות למרות שאינם רשאים לכך.





מדוע העובד חשוד בהאזנה?

אז מה למדנו?

כשמחפשים מידע לפעמים מוצאים כל מיני פריטי מידע

שכל אחד מהם לבד לא מספר כלום.

אך מהצלבת פרטי המידע השונים ניתן להגיע לתובנות חשובות.

כל הכבוד! סיימנו את השלב עם מידע חשוב ביותר!

גילינו שהעובדים שהאזינו לשיחות באופן לא חוקי הם:

יהודה רוזנס

נועם סגל

המשך

כל הכבוד!!!

החשוד הוא:

יהודה רוזנס

שלח את המייל מתאילנד

סיום