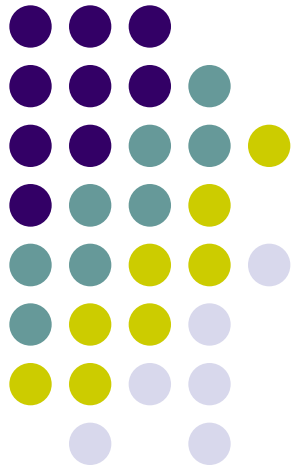
# אבטחת מערכות מידע

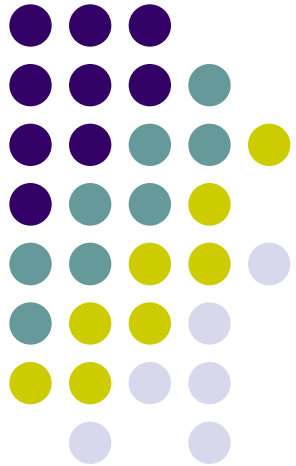


מרצה: שי שקרוב

# נושאי השיעור

- גורמי הסיכון למערכות מידע
- תהליך ניהול הסיכונים
- מודל טבעת האבטחה

# גורמי הסיכון למערכות מידע



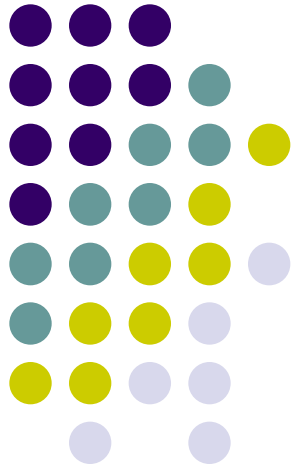
# גורמי הסיכון למערכות מידע

- הגדרה:
  - מכלול הפעולות שעל הארגון לנקוט ע"מ להבטיח את תקינות פעולתה של מ"מ בארגון.
- הבעיה:
  - יישוב הקונפליקט בין הרצון לאפשר נגישות ושימוש מרבי במשאבי המערכת לבין הרצון להגן עליהם.
- גורמי סיכון:
  - נזקי טבע (שטפון, רעידת אדמה)
  - בני אדם (בשוגג או במזיד)
  - גורמים תפעוליים (הפסקת חשמל, נפילת מתח)

# גורמי הסיכון למערכות מידע

- סיכונים פנימיים וחיצוניים
  - סיכון פנימי: נגרם ע"י גורם בתוך החברה
  - סיכון חיצוני: ע"י גורם זר
- סיכונים מוחשיים ולא-מוחשיים
  - סיכון מוחשי: למשל נזקים למחשבים, נזקים לקבצים
  - נזק לא מוחשי: לדוגמא פגיעה במוניטין

# תהליך ניהול הסיכונים



# תהליך ניהול הסיכונים

1. זיהוי הסיכונים
2. הערכת חומרת הסיכון וההסתברות לסיכון
3. בחירת שיטת הטיפול בסיכון
4. ניהול שוטף של פונקצית ניהול הסיכונים של מערכות המידע

# תהליך ניהול הסיכונים
# 1. זיהוי הסיכונים

- סקר מקיף המתייחס לכל תחומי הסיכון האפשריים:
  - סביבה פיסית: מיקום האתרים, שכנים, מזג אויר, אספקת חשמל, כניסות למבנים
  - תקשורת: אמינות, גיבוי, אבטחה ונוהלי בקרה
  - תוכנה וחומרה: הסכמי אחזקה, אמינות, תמיכת ספקים, תיעוד וגיבוי
  - תפעול: נהלי גיבוי, אבטחת נתונים, בקרת קלט פלט, בקרה מינהלית
  - כ"א: נהלי הכשרה, קידום, פיטורין
  - חוזים: עם ספקים ולקוחות
  - חוקים ותקנות: צנעת הפרט, חבות מוצרים, פרטיות, לשון הרע

# תהליך ניהול הסיכונים
# 2. הערכת חומרת הסיכון

- הערכת חומרת הסיכון:
  - כימות הנזקים
    - סיכון מוחשי
    - סיכון לא מוחשי
- הערכת ההסתברות להתרחשות הנזק
- תוחלת הנזק: מכפלת ההסתברות לנזק בחומרת הסיכון

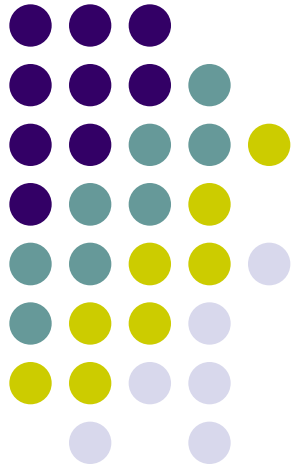
# תהליך ניהול הסיכונים
# 3. בחירת שיטת הטיפול בסיכון

- **חמיקה מסיכון**. המנעות מפעילות יוצרת סיכון
  - העברת הפעילות לקבלן משנה
- **אימוץ הסיכון.** לקחת סיכון ולשלם אם יתרחש
  - לא לעשות ביטוח
- **הקטנת הסיכון.** פעולות להקטנת חומרת הנזק לאחר התרחשותו (לא על ההסתברות)
  - התקנת דלתות חסינות אש
- **העברת הסיכון.**
  - ביטוח; חכירה

# תהליך ניהול הסיכונים
# 4. ניהול שוטף של הסיכונים

- ניהול שוטף של פונקצית ניהול הסיכונים של מערכות המידע
  - מינוי אדם או יח' לטיפול שוטף בנושא
  - מכין תכנית אבטחה ומיישם אותה

# מודל טבעת האבטחה



# מודל טבעת האבטחה

- מתאר 6 תחומים המקיפים את התחומים השונים בהם יש לטפל כדי ליצור הגנה שלמה של מ"מ:

1. אבטחה פיסית
2. בקרת גישה
3. אבטחת נתונים
4. אבטחת תוכנה
5. אבטחת תקשורת ואבטחת האינטרנט
6. נהלי אבטחה ואמצעי הגנה בלתי ישירים

# מודל טבעת האבטחה

- רמת האבטחה של מ"מ בארגון נקבעת עפ"י החוליה החלשה בטבעת.
- האבטחה צריכה לענות על שני צרכים סותרים:
  - שמירה על פעילות תקינה של המערכת
  - אי התערבות בפעילות השוטפת של המערכת
- עלות האבטחה צריכה להיות קטנה מהנזקים

# מודל טבעת האבטחה
# 1. אבטחה פיסית

- כנגד סיכונים המאיימים על התקינות הפיסית של מערכות המידע
- סיכונים אפשריים:
  - פגעי טבע (ברק, שיטפון, שרפה, רעידת אדמה, ...)
  - גורמים תפעוליים (הפסקת חשמל, נפילת מתח, פיצוץ, ...)
  - גורמי אנוש (גניבה, השחתה, חבלה, ...) ע"י גורמים חיצוניים או פנימיים.

# מודל טבעת האבטחה
# 1. אבטחה פיסית

- ההתמודדות היא ע"י בחירת אתר מתאים, מיגונו והפעלת ציוד התרעה נגד הסיכונים האפשריים.
- דוגמאות:
  - פגעי טבע – שריפה
    - מניעה: בניית חדר מחשבים חסין אש
    - הקטנת נזק: התקנת גלאי אש
  - פגעי טבע - שיטפון
    - מניעה: בחירת אתר גבוה ולא במקום מועד לשטפונות
    - הקטנת נזק: איטום קירות וגגות של חדרי מחשב

# מודל טבעת האבטחה
# 2. בקרת גישה

- בקרת הגישה למידע, לתכניות ולמשאבי הרשת
- בקרת הגישה מתבצעת ע"י:
  - וידוא זהות
  - הרשאות

# מודל טבעת האבטחה
# 2. בקרת גישה – וידוא זהות

- וידוא זהות מתבצע ע"י אחד מהאמצעים הבאים, או שילובים שלהם:
  - דבר שהמשתמש יודע
    - סיסמאות (ראשונית- מערכת הפעלה; שניונית- מסד נתונים ויישומים);
  - דבר שברשות המשתמש
    - כרטיס מגנטי, כרטיס חכם, Secure ID
  - זיהוי פיזי של המשתמש
    - טביעת אצבע, קול, חתימה, מבנה קשתית העין, ...

# מודל טבעת האבטחה
# 2. בקרת גישה – הרשאות

- המערכת צריכה להיות מסוגלת לדעת מי רשאי לגשת לאיזה מידע. נעשה ע"י:
  - רשימת בקרת גישה - רשימה המפרטת את רשימת המורשים לכל משאב (דומה לעץ)
  - מטריצת בקרת גישה (גישה טבלאית. ציר אחד מתאר משאבים השני משתמשים)

# מודל טבעת האבטחה
# 3. אבטחת נתונים

- אבטחת נתונים (באחסון ובהעברה)
  - גיבויים ומניעת עומס יתר
  - הצפנה ופענוח: (מפתחות פרטיים; מפתחות ציבוריים)
  - אבטחת מסדי נתונים:
    - שלמות מסד הנתונים; שלמות פריטי המידע; מעקב; בקרת גישה; זיהוי משתמשים; זמינות נתונים (התאוששות).

# מודל טבעת האבטחה
# 4. אבטחת תוכנה

- חשיפה לפגיעה לא מכוונת
  - שגיאות תכנות (באגים)
  - הגנה בתהליך התכנות
- חשיפה לפגיעה מכוונת
  - וירוס, סוס טרויאני, דלתות נסתרות
  - ההגנה הנפוצה היא באמצעות תוכנות אנטי וירוס.
  - מניעת הדבקה, אבחון הדבקה, ואחזור (טיפול בהדבקה)

# מודל טבעת האבטחה
# 5. אבטחת תקשורת

- אבטחת קוי התקשורת והנתונים המועברים
- הסיכונים:
  - זליגה- גורם לא מורשה מגיע לנתונים
  - הפסקה- הפרעה לקו התקשורת הגורמת לאובדן נתונים או לאי זמינותם
  - שינוי- שיבוש או שינוי נתונים ע"י גורם לא מורשה
  - זיוף- השתלת נתונים ע"י גורם לא מורשה
- פתרונות טכניים/ פיסיים (שימוש בקוי תקשורת בטוחים יותר, איתור מכשירי ציטוט)
- אמצעי זיהוי ואימות (בין הלקוח לשרת).

# מודל טבעת האבטחה
# 5. אבטחת תקשורת

- אבטחת האינטרנט - אבטחת מ"מ של הארגון; אבטחת נתוני המשתמש
- 5 מנגנוני אבטחה:
  - אישור זיהוי המשתמש ואימותו, או שימוש בחומות מגן firewall
  - הרשאה (פרוטוקול שירות החיוג למשתמש לזיהוי מרחוק), או firewall
  - הגנה על הנתונים - סודיות להגנה מפני חשיפה לא מורשית (הצפנה. פרוטוקולים: SSL; SET)

# מודל טבעת האבטחה
# 5. אבטחת תקשורת

- 5 מנגנוני אבטחה (המשך):
  - הגנה על נתונים- שלמות לצורך איתור שינויים בלתי מורשים (הצפנה דומה לזיהוי)
  - בקרה דיווחים בלתי תלויים על פעילויות תקשורת, מסייעים לבדיקת יעילות האבטחה ולאתר פעולות חשודות
    - ע"י ניטור הפעילויות ומתן התראות על חריגים;
    - אפשר להשתמש במלכודות

# מודל טבעת האבטחה
# 6. נהלי אבטחה

- אמצעי אבטחה לא ישירים, להתאוששות לאחר שקו ההגנה הראשון נפרץ:
  - ביטוח
  - גיבוי
  - תכנית מותנית לשעת חירום

# מודל טבעת האבטחה
# 6. נהלי אבטחה

- ביטוח
- השקעה באבטחת מ"מ תקטין את הפרמיות
- גיבוי
- צריך לקחת בחשבון: עלות הגיבוי, התועלת מהגיבוי, את הצורך בהתאוששות מהירה (תלוי בסביבת הפירמה)
- כוללת גיבוי: לחומרה, לתוכנה, לקווי תקשורת, לנתונים (קבצים), ולנושאי תפעול.

# מודל טבעת האבטחה
# 6. נהלי אבטחה

- גיבוי לחומרה
- מחשבים כפולים (באותו אתר)
- אתר קר (תשתית חליפית מוכנה ללא המחשב. במקרה אסון מביאים מחשב ואת הגיבויים)
- אתר חם (תשתית חליפית מלאה. באסון מביאים את הגיבויים)
- אתר לוהט (אתר חליפי זהה למקורי. הפעילויות מתבצעות בשני האתרים במקביל)

# מודל טבעת האבטחה
# 6. נהלי אבטחה

- גיבוי לתוכנה ולנתונים
- שומרים את הגיבויים באתר נפרד.
- 4 חלקי לגיבוי:
  - גיבוי מקיף (תקופתי);
  - גיבוי סלקטיבי (של קבצים שעודכנו לאחרונה, יומי);
  - אחסון דורות של גיבויים;
  - קובץ יומי המתעד את כל הפעולות מאז הגיבוי הסלקטיבי האחרון.

# מודל טבעת האבטחה
# 6. נהלי אבטחה

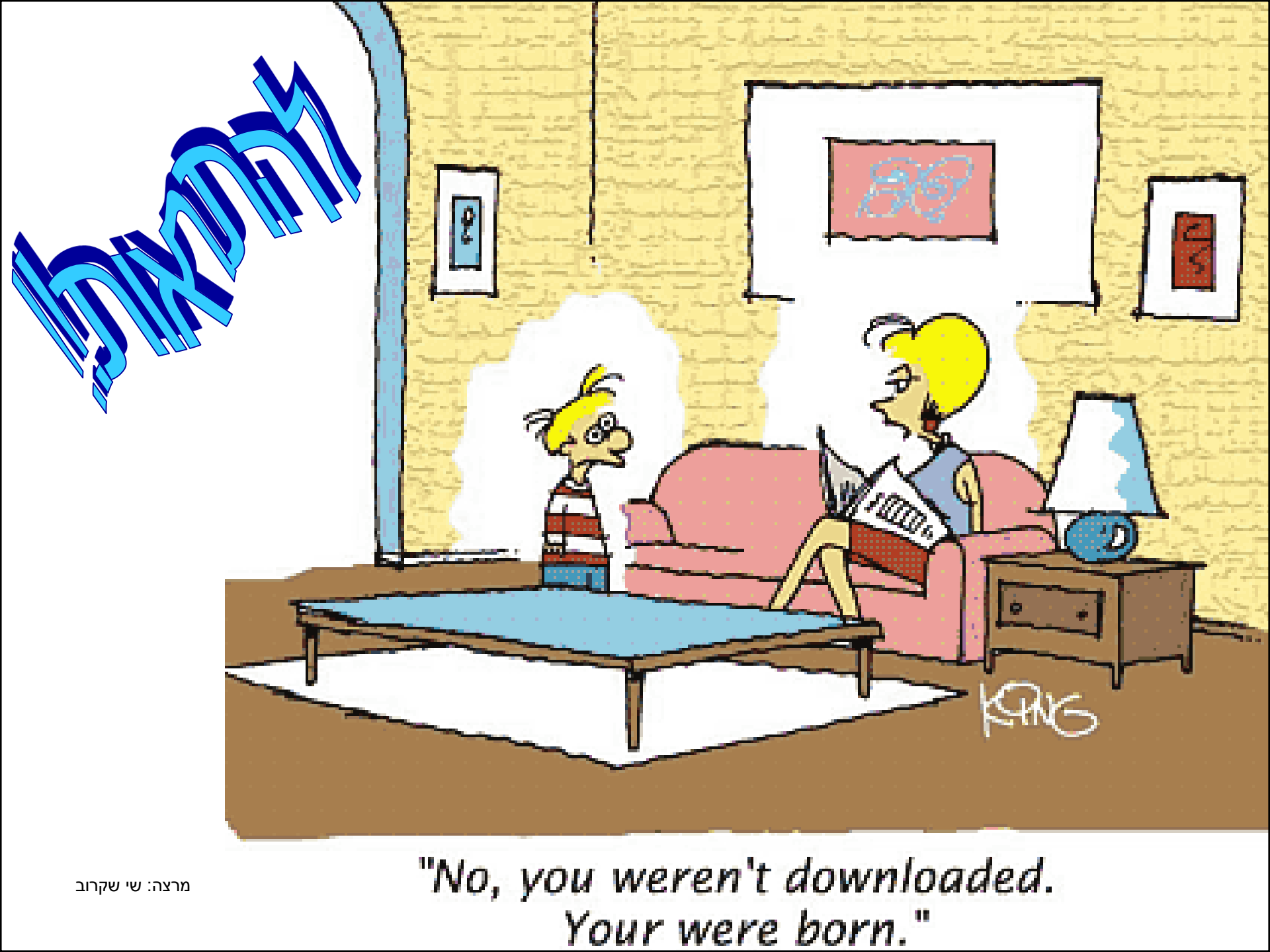
- גיבוי לקווי תקשורת
- קו תקשורת חלופי
- רשת תקשורת בה שני מסלולים לפחות בין כל שתי נקודות
- שימוש ברשת ציבורית

# מודל טבעת האבטחה
# 6. נהלי אבטחה

- גיבוי לנושאי תפעול
- גיבוי למערכות התומכות במחשוב
  - גילוי אש
  - גילוי מים
  - מזגן
  - וכו'

# מודל טבעת האבטחה
# 6. נהלי אבטחה

- תכנית מותנית לשעת חירום. התכנית כוללת:
  - תכנית חירום
    - מהן הפעולות אותן יש לבצע בעת אסון (למשל מה לעשות בשרפה)
  - תכנית התאוששות
    - מהן הפעולות שיש לבצע לאחר האסון כדי להחזיר את יכולת עיבוד הנתונים מהר
    - מהן הפעולות הדרושות לשיקום אתר המחשבים והציוד שנפגע




מרצה: שי שקרוב