



ארז קרינר

איום קיברנטי ואבטחת מידע

כאשר קוראים את התבטאויות מנהיגי העולם סביב הנושא. כולם טורחים להתבטא בעניין - מנשיאי ארה"ב, רוסיה, מדינות אירופה, ישראל ועד למנהיגי המזרח הרחוק.

איום הסייבר הוא מרחב עצום, הכולל את כל מערכות התקשוב ואת תוכנן. האיום עוטף אותנו בכל מקום: הוא נמצא במערכות הביתיות (מחשבים, ממירים דיגיטליים של שידורי טלוויזיה, וכו'); בטלפון הנייד; במערכות המכונית (הנעה, בטיחות, מולטימדיה, וכו'); ברשת החברתית שאליה אנו מתחברים; ועם התפתחות רעיון "האינטרנט של הדברים" (Internet of Things [IOT]), הוא עתיד להימצא במערכות רבות נוספות.

מובן שהאיום קיים בכל מערכות התקשוב, שאנו משתמשים בהן במקום עבודתנו. מערכות אלו מחוברות למערכות של שותפים עסקיים, של ספקים ושל לקוחות; ולמקורות מידע חיצוניים. האיום מקבל משנה מרץ, כאשר עובדי הארגון מחברים מכשירים פרטיים (כגון: סמארטפון, דיסק חיצוני, וכו') למערכות התקשוב בסביבת עבודתם. איום זה יוצר פגיעות רבה, כי הוא מובנה בתוך ה-DNA של מערכות הארגון. אמנם, חשיפת נקודות התורפה של המערכות ומימושן של האיום מחייבים ידע והבנה של עולם המחשוב, אך רף הכניסה במרחב הסייבר הולך ופוחת.

כמעט כל אדם יכול לאתר באינטרנט תוכנות לביצוע תקיפות, חדירות, ופגיעות מורכבות, ואולי אף חמור מכך - לביצוע מניפולציה על נתונים הנמצאים במערכת. המניפולציה עלולה לגרום נזק קטן ומתמשך, שממבט ראשון אינו גלוי, אך עם הזמן פגיעתו עלולה להיות הרסנית. ולדוגמה: הפגיעה בתאגיד הקמעונאי "Target Corporation", בארה"ב. חדירה מתמשכת

** "האינטרנט של הדברים" (IOT) מבוסס על הרעיון, שכל מכשיר אפשר לחבר לאינטרנט. חיבור זה מאפשר תקשורת בין מכשירים לבין בני-אדם ובין מכשירים שונים לבין עצמם. כך אפשר לשלוט עליהם מרחוק, להפיק מהם מידע, ולהפוך פעולות שונות לאוטומטיות.

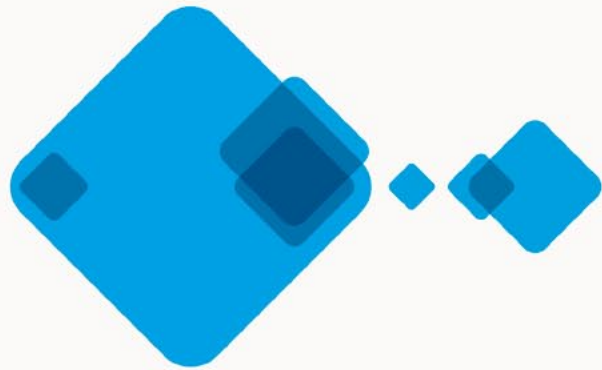
האיום במרחב הקיברנטי, המוכר כאיום הסייבר (Cyber), הוא תופעה חדשה יחסית, שעדיין אינה מגובה בכללי התנהגות, בחוקים ובדינים. האיום נוצר בידי אדם, הוא כמעט ואינו כפוף לחוקי טבע מוכרים, והוא מתפתח בקצב מהיר ביותר. איום הסייבר מסכן את פעילותו התקינה של כל ארגון (ביטחוני, ציבורי ופרטי), ופגיעתו עלולה להיות בעוצמה כה רבה, שאין לה אח ורע בהשוואה לחומרת פגיעתם של איומים אחרים. לראיה: מערכת הביטחון מגדירה את איום הסייבר כמרחב הלחימה החמישי, נוסף על מרחבי הלחימה המסורתיים: ביבשה, בים, באוויר ובחלל*.

* מתוך המאמר: הממד החמישי - היערכות ישראל למתקפת סייבר מורכבת. כתב העת מערכות, בית ההוצאה לאור של צה"ל, גיליון 452.

האיום מקבל משנה מרץ, כאשר עובדי הארגון מחברים מכשירים פרטיים (כגון: סמארטפון, דיסק חיצוני, וכו') למערכות התקשוב בסביבת עבודתם. איום זה יוצר פגיעות רבה, כי הוא מובנה בתוך ה-DNA של מערכות הארגון



slimstock



! 600 חברות כבר יודעות

התייעלות בשרשרת האספקה
זה לא רק צמצום מלאי
ושיפור רמת השירות



slimstock הינו המותג המוביל באירופה בתחום
אופטימיזציית המלאי הרכש ותכנון היצור, מותאם לצרכי
הארגון בכל גודל ובמגוון ענפים, נסיון בינלאומי עשיר
ותמיכה גלובלית ב-5 יבשות

- ◆ תהליכי הטמעה קצרים במיוחד
- ◆ קישוריות לכל מערכות ה-ERP או ניהול המלאי
- ◆ תחזיות ביקוש וחישוב מלאי ביטחון
- ◆ הקטנת ערך המלאי בכ-35%
- ◆ הקטנת החוסרים בכ-80%
- ◆ מניעת מלאי מת
- ◆ מתאים ל-S&OP, VMI, SCM, MRP

אינפולוג ישראל בע"מ

03-6418285.טל info@infolog.co.il www.infolog.co.il

INFOLOG

ב. איום פנימי, המגיע מצד עובדי הארגון, ולדוגמה: עובד ממורמר/מתוסכל, שיש לו הרשאה להשתמש בבסיס נתונים חיוני, או שהוא משיג גישה לנתונים, אשר אינם קשורים לעבודתו.

ג. שרשרת הזרימה של נתוני הארגון, כגון ממשקי מחשב עם ספקים ועם לקוחות קבועים, העלולים לשמש נשאים לתוכנות זדוניות, שמאן דהו שותל בתוך רשת הארגון. בשנים האחרונות, השימוש בגורם השלישי להעברת האיום הולך וגובר, כי יחסי האמון הנרקמים בין הארגון לבין ספקיו ולקוחותיו יוצרים פגיעות רבה.

עובדה מעניינת על כלי-הנשק במרחב הסייבר היא, שמשך פיתוחם הוא קצר ביותר, לעומת מחזור הפיתוח של כלי נשק קונבנציונליים. לראיה: פיתוחה של תוכנת תקיפה, העלולה לגרום נזק ממשי, יכול להסתיים בתוך שבועות אחדים. זאת, לעומת מחזור הפיתוח של כלי הנשק המסורתיים, שמשכו יכול להגיע לעשור שנים ואף יותר מכך. עובדה זו מציבה אתגר מורכב לאנשי המקצוע, האמונים על הגנת הארגון. יתרה מזו, המורכבות אף תלך ותגדל עם הוספת מערכות אחרות לרשת הארגון, שכיום אינן פועלות בסביבה ממוחשבת.

מכאן, שארגון שאינו נוקט תהליך מובנה ומסודר של הגנה על מערכתיו, ושאינו מקפיד לשפר תמידית את מערך הגנתו, הוא כמעט בחזקת מתאבד, כיוון שברור לחלוטין שתקיפה בוא תבוא. השאלה היחידה היא שאלה של זמן, והיא תלויה בגודל רשעותו של גורם הזדון.

ההגנה הנדרשת מפני איום הסייבר כוללת: נקיטת יוזמה וגישה פרו-אקטיבית, הגדרת מדיניות הולמת לאבטחת המידע, כתיבת נוהלי אבטחת מידע ותחזוקתם, תרבות ארגונית התואמת את צורכי האבטחה, יתירות (יכולות עודפות וגיבויים), בידוד מערכות מידע חיוניות, בידול בין המערכות, פריסת מערך אבטחת מידע קונבנציונלי בכמה שכבות, אבטחה פיזית של מערכות המידע, וכו'.

אבטחת המידע

המידע הוא נכס חשוב לארגון, שיש להגן עליו מפני איומים חיצוניים ופנימיים, העלולים לגרום נזק לארגון וללקוחותיו. מטרת אבטחת המידע (Information Security) היא לספק מענה הולם לאיומי אבטחת מידע ולמזער את השפעתם של אירועי אבטחת המידע.

מדיניות אבטחת המידע כוללת היבטים פיזיים ולוגיים, ובכלל זה: אחסון נתונים על מחשבים, העברת נתונים בין מערכות, כתיבת מסמכים והדפסתם, וכו'. המדיניות מקיפה את הנושאים הבאים: הגדרת אזורים פיזיים ותהליכים ארגוניים, המחויבים באבטחת מידע; הגדרת עקרונות אבטחה בסיסיים והנחיות ליישום; העלאת המודעות לאבטחת מידע ולנושאים רגישים באבטחת מידע, בקרב הנהלת הארגון ועובדי

למערכות התאגיד גרמה בשיאה לגניבת פרטים על כרטיסי אשראי של כ-70 מיליון לקוחות, ולנזק גדול למכירות התאגיד ולדימויו, בתקופה שלאחר גילוי הפריצה.

אם נבחן את האיום על שרשרת האספקה נמצא, שמייגון תוכנות מחשב מעורב בכל תהליכי האספקה, ולדוגמה: רכש טובין מנוהל במערכת לתכנון משאבי הארגון (Enterprise Resource Planning) [ERP], פריקת הטובין מן האונייה והעמסתם מנוהלות במערכת לתפעול הרציף (Terminal Operation System) [TOS], שינוע הטובין מנוהל במערכת לניהול הובלה קליטת הטובין במחסני הארגון וניפוקם מנוהלים במערכת לניהול מחסן (Warehouse Management) [WMS], תהליכי העיבוד של הטובין במפעל מנוהלים במודול לתכנון דרישות חומרים (Material Requirements Planning) [MRP], וכו'.

מכאן, ששרשרת האספקה נשלטת באמצעות מערכות מחשב, אשר פעולתן ונתונין מהווים מטרות לפגיעה. כל מניפולציה של גורם זדוני על קובצי המחשב בתוכנות אלו עלולה לגרום לתוהו ובוהו, לגניבת מידע עסקי*** ואף למנוע את זמינותם של הטובין בעת הצורך. עולם גורמי הזדון כולל בתוכו בני-עשרה, שפגיעתם היא לצורכי שעשוע בלבד, וארגונים עסקיים חובקי עולם, המייצרים תוכנות ייעודיות לתקיפת ארגונים במרחב הסייבר.

אפשר לסווג את מקורות התקיפה/הפגיעה בארגון על-פי הקטגוריות הבאות:

א. איום חיצוני, המגיע מרשת האינטרנט ומגורמים שאינם קשורים ישירות לפעילות היום-יומית של הארגון.

*** בשנת 2005 התפוצצה בישראל פרשיית ריגול תעשייתי חמורה, שהיו מעורבות בה חברות גדולות במשק. הריגול התבצע באמצעות השתלת תוכנת סוס טרויאני במחשבי המתחרים.



A.G.S

תכנון וייעוץ לוגיסטי

תכנון פונקציונלי למחסנים ומרכזים לוגיסטיים

- ✓ תכנון העמדת המבנה ע"ג המגרש
- ✓ תכנון שטח האתר כניסות ויציאות
- ✓ תכנון פתחים, רמפות ומשווי גובה
- ✓ תכנון גובה המבנה ושיפועי הגג
- ✓ תכנון סוג הרצפה ואיכותה - SFF
- ✓ תכנון תאורה במחסן וצרכי חשמל
- ✓ תכנון אזורי תפעול ושרותי ערך מוסף
- ✓ תכנון מערכות אחסון ושינוע
- ✓ תכנון כמויות מיקומי אחסון ותפוקות
- ✓ תכנון שיטות תפעול קבלה, אחסון, ליקוט והפצה
- ✓ תכנון זרימת המוצרים



קבוצת קאופמן ד"ר גב / נטוצ'י

תכנון וייעוץ לוגיסטי

- ✓ תכנון וייעוץ לוגיסטי אסטרטגי
- ✓ תכנון פרויקטים חדשים - ROI
- ✓ שדרוג פרויקטים קיימים
- ✓ תכנון מערכות אחסון ושינוע
- ✓ ייעוץ לוגיסטי כלכלי
- ✓ ייעוץ בנושאי עלויות ומחירים לוגיסטיים
- ✓ ייעוץ בנושאי מיקור חוץ (אאוטסורסינג)
- ✓ ייעוץ לחברות 3PL
- ✓ ייעוץ לחברות הפצה לוגיסטיות
- ✓ אופטימיזציה לוגיסטית של תהליכים
- ✓ הדרכות לוגיסטיות



קבוצת טבת

תכנון וייעוץ תוכנות לוגיסטיות

תוכנות WMS - TMS - PLANNING

- ✓ אפיון לוגיסטי לקביעת סוג התוכנה הנדרש
- ✓ אפיון התהליכים הלוגיסטיים
- ✓ כתיבת מכרזים לרכש תוכנות לוגיסטיות
- ✓ ליווי פרויקטים של תוכנות לוגיסטיות
- ✓ ייעוץ בנושאי ציוד קצה: מספונים, מדפסות

Inbound ASN, Receiving, Q/C, VAS, Putaway

Stock Manage FIFO, LIFO, FEFO, S/N, LOT, Bar-Code

Outbound Replenishment, Picking, Packing, Voice, P2L, Distribution



קבוצת גלובוס

תכנון וייעוץ מערכת אחסון ושינוע

תכנון מערכות אחסון למחסנים

- ✓ מערכות אחסון סטטיות
- ✓ מערכות אחסון דינמיות
- ✓ מערכות אחסון נעות
- ✓ מערכות אחסון אוטומטיות
- ✓ אפיון מלגזות ומערכי שינוע למחסנים
- ✓ מלקטות ועגלות "ווספות"
- ✓ מלגזות משקל נגדי, היגש וצריח
- ✓ מסועים, שאטלים, ממינות
- ✓ שירותי שרטוט מערכים לוגיסטיים LAYOUTS



קבוצת 207

Logistic *In* motion!

ככה *In* מתכננים מחסן!

ת.ד. 4357, ראש העין 4856729
T: 03- 6584040 M: 052- 3327541

פארק לב הארץ-קסם: מבנה 6, כניסה C, קומה 1
ags@ags.co.il www.ags.co.il

ואת צורכי לקוחותיו. ה. תחזוקה תדירה של התכנית ושיפורה המתמיד, כדי לתת מענה הולם לאיומים חדשים, ולטכנולוגיות חדשות הנכנסות לשימוש. דוגמה לכך היא מגמת השימוש במכשירים פרטיים, בסביבת העבודה (Bring Your Own Device) [BYOD]. העובד אוגר נתונים על מכשירו הפרטי וכאשר המכשיר מתקלקל, הוא מוסר אותו לתיקון במעבדה חיצונית. עובדי המעבדה עלולים להעתיק את הנתונים מן המכשיר, או לחלופין, להפוך את המכשיר לנשא של תוכנת תקיפה (וירוס/סוס טרויאני/תולעת), שתדביק את מערכות הארגון לאחר שהעובד יחזור להתחבר אליהן עם מכשירו הפרטי.

להלן כמה כלים חיוניים:

בהיבט האנושי

- **מהימנות עובדים.** תהליך גיוס עובדים חדשים צריך להיות מותאם להפחתת סיכוני אבטחת המידע. ולדוגמה: גיוס עובדים נאמנים, שהם בעלי מחויבות גבוהה, המלצות ראויים, וכו'; במקרים מסוימים, מנהל הביטחון של הלקוח מתחקר את המועמדים, וכו'; כל עובד נדרש לחתום על נספח אבטחת מידע, שבו הוא מתחייב לשמור על סודיות במשך תקופת העסקתו ובמשך תקופה מסוימת לאחריה; העובד חותם על ציוד מושאל; בסיום העסקתו, הוא נדרש להחזיר את הציוד, ונציג מערכות המידע מבטל את הרשאותיו; וכו'.
- **אחריות אישית.** כל עובד בארגון נדרש לאחריות אישית לאבטחת המידע באמצעות הפעולות הבאות: שמירת סודיות הסיסמאות, אבטחת עמדת העבודה האישית וסביבתה, בקרה על הדפסת מסמכים, שימוש ברשת האינטרנט לצורכי העבודה בלבד, דיווח למנהל אבטחת המידע על אירועי אבטחת מידע, וכו'.
- **הדרכה ומוודעות.** מנהל אבטחת המידע דואג להכין תכנית הדרכה שנתית בתחום אבטחת המידע ולקיים הדרכות לעובדי הארגון.
- **ספקים וקבלנים.** מנהל אבטחת המידע דואג להחתים על הסכם סודיות (Non Disclosure Agreement) [NDA] את השותפים העסקיים, את הספקים, את הקבלנים ואת עובדיהם, העלולים להיחשף למידע קריטי/רגיש.

בהיבט הטכנולוגי

- **אבטחת הסביבה הפיזית.** האבטחה כוללת: הגנה על אזורים מאובטחים באמצעות אמצעי בקרת גישה (Access Control) ואבטחת סביבת העבודה באמצעות מדיניות המבוססת על העקרונות הבאים: אחריות אישית של העובד, "שולחן נקי" (אחסון מסמכים ומדיה נתיקה באזור מוגן, בסוף כל יום עבודה) ו"מסך נקי" (הפעלה אוטומטית של שומר מסך בעמדת העבודה, לאחר זמן מוגדר ללא שימוש).
- **אבטחת נתונים ותקשורת.** מנהל מערכות המידע מאבטח את הגנת השימוש ברשת מפני כניסה לא מאושרת, באמצעות הרשאות גישה רק על-פי צורך

הארגון; הגדרת התפקידים של הגורמים הרלוונטיים באבטחת המידע ושל אחריותם; וכו'.

הגורמים המובילים באבטחת המידע הם: מנהל מערכות מידע (Chief Technology Officer) [CTO], האחראי על כל מערכות המידע בארגון, ומנהל אבטחת המידע (Chief Information Security Officer) [CISO] (בדרך-כלל, קצין/מנהל הביטחון), האחראי על אבטחת המידע הפיזי והלוגי של הארגון. כולל: הכנת תכנית לאבטחת מידע; כתיבת נהלים, הוראות והנחיות; הטמעת המדיניות; ביצוע מבדקים פנימיים; העלאת המודעות בקרב העובדים; דיווח למנהל מערכות המידע; וכו'.

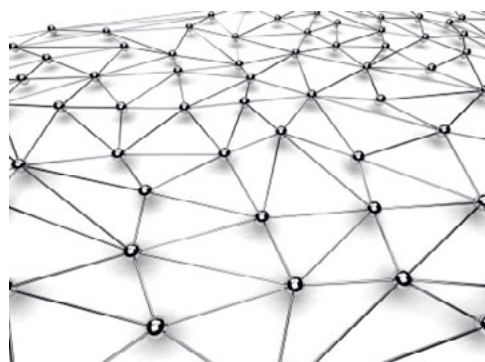
מנהל מערכות המידע אחראי לנהל את רשימת נכסי המידע בארגון ולתחזק אותה, ומנהל אבטחת המידע אחראי להגדיר את הדרישות לאבטחת המידע על-פי סיווג הנכס.

להלן קטגוריות אפשריות לסיווג:

- מידע קריטי (Critical Information), שחשיפתו עלולה לגרום נזק מהותי לארגון. ולדוגמה: מידע ביטחוני, מידע עסקי, מידע אישי על עובדים, וכו'.
- מידע רגיש (Sensitive Information), שנגיש לעובדים מסוימים, ושחשיפתו עלולה לגרום נזק לארגון. ולדוגמה: נתוני מכירות, תהליכים פנימיים, וכו'.
- מידע כללי (General Information), שנגיש לכול, ושחשיפתו אינה גורמת נזק לארגון. ולדוגמה: מחזור הפעילות של ארגון ציבורי, פרופיל הארגון (מפורסם באינטרנט), וכו'.

להלן השלבים בתכנית אבטחת המידע:

- א. מיפוי הארגון: לבחון מי נגד מי ולנתח מה קורה בארגון. כולל: סקר סיכונים, ניתוח פערים, הבנת מצב הארגון, הכרת נכסי הארגון והבנת פגיעותו.
- ב. הגדרת התהליכים, שעליהם הארגון רוצה להגן על-פי סדרי עדיפויות, החל מתהליכים קריטיים ביותר ועד לתהליכים, שאפשר להסתפק בהגנתם הבסיסית בלבד.
- ג. הכנת תכנית אבטחה על-פי מטרות הארגון, יכולותיו ואילוציו השונים (כגון: מגבלות תקציב, אילוצים תפעוליים, משאבים שאינם זמינים, וכו').
- ד. יישום התכנית. בשלב זה מתבצעת התאמה של התהליכים ושל טכנולוגיות, ואינטגרציה של תחומים נוספים. כך שבסופו של התהליך, הארגון מתפקד היטב על-פי מטרותיו ובצורה ההולמת את צרכיו



המידע הוא נכס חשוב לארגון, שיש להגן עליו מפני איומים חיצוניים ופנימיים, העלולים לגרום נזק לארגון וללקוחותיו. מטרת אבטחת המידע (Information Security) היא לספק מענה הולם לאיומי אבטחת מידע ולמצער את השפעתם של אירועי אבטחת המידע

- אישורה.
- **בקרת גישה לנתונים/למידע.** הבקרה כוללת: ניהול הרשאות, חשבונות משתמשים וסיסמאות (כולל הגדרת מבנה סיסמה מאובטחת, הקפדה על שמירת פרטי הסיסמה האישית, החלפה תדירה של סיסמאות, וכו').
- **רכש מערכות.** מנהל מערכות המידע בודק מערכת נרכשת טרם הטמעתה. המבדק מתבצע בסביבת ה"מבחן" ("Test"), ובכל מקרה, לא בסביבת ה"עבודה" ("Production").
- **מעבר לאמור לעיל יש פעולות ייחודיות,** שהארגון יכול להכין במערכתיו ואשר יהיו בבחינת הפתעה לתוקף, ידרשו ממנו מאמצים וזמן, ויסיטו אותו הלאה ממערכות הארגון.

סיכום

איום הסייבר ואיומים אחרים על מערכות המידע הם איומים ממשיים, המסכנים את קיומו של הארגון. עם זאת, נסיים את המאמר במילים אופטימיות: במדינת ישראל קיים ידע רב בתחום אבטחת המידע, שמביא לידי ביטוי יכולות הגנה ומניעה מתקדמות ביותר. הידע תורם תרומה חשובה להגנת הארגונים, ונוסף על-כך, הוא הופך להיות מקור הכנסה חשוב למדינה בייצוא פתרונות ייחודיים בנושא ללקוחות בכל העולם. ■

לפרטים נוספים, תוכלו לצפות באתר האינטרנט: www.fivec.com

(Need to have). אחראי אבטחת המידע סוקר את רשימת ההרשאות אחת לתקופה ומבקר אותה. האבטחה כוללת: הגנה בגישה מרחוק (Remote Direct Access), באמצעות הרשאות גישה רק על-פי הצורך; גישה מרחוק באמצעות חיבור לרשת פרטית (Virtual Private Network [VPN]); הזנת שם משתמש וסיסמה אישית; הגנה מפני גישת אורחים באמצעות איסור על שימוש בהתקנים חיצוניים, והקצאת אמצעים לגישה נפרדת; וכו'. נוסף על-כך, אחסון של ציוד רגיש באזור סגור לאחר שעות העבודה; השמדת מדיה מגנטית שיוצאת משימוש; וכו'.

- **פעילות אבטחה.** הפעילות כוללת: גיבוי הולם של אמצעים ושל נתונים, כדי להבטיח את המשכיות התהליכים העסקיים בעתות תקלה/אסון; מדיניות תגובה על אירועי אבטחת מידע, המפרטת כללי התנהגות בכל סוג אירוע; וכו'.
- **הגנה מפני וירוסים, סוסים טרויאנים וקוד זדוני.** זאת, באמצעים הבאים: התקנת תוכנת אנטי וירוס בכל עמדות העבודה והמחשבים הניידים, ניהול רשימת ההתקנות, תחזוקתה, עדכונה ובקרתה.
- **בקרת שינויים.** ניהול אפקטיבי של מערכת מאובטחת מחייב את מעורבותם של מנהל מערכות המידע ושל מנהל אבטחת המידע בכל שינוי, בסביבת מערכות המידע. המנהלים בוחנים את היבטי האבטחה ומנתחים סיכונים אפשריים ביישום השינוי. המנהלים אחראים, כל אחד בתחומו, לבדוק את המערכת הרלוונטית לפני

שימו את עצמכם במרכז



המרכז להשתלמויות
בר-אילן חברה למחקר ופיתוח בע"מ
אוניברסיטת בר-אילן ב"א

מסלול ↙
רכש ולוגיסטיקה

רשימת הקורסים במסלול:

- יבוא יצוא וסחר בינ"ל בשיתוף UPS
- ניהול רכש ולוגיסטיקה
- ניהול רכש ולוגיסטיקה בכיר

המרכז להשתלמויות בר-אילן מזמין אתכם ליהנות ממבחר קורסים חדשים, מעודכנים ומותאמים אישית, שיעניקו לכם את הכלים והידע הדרושים לעבודה ולהצלחה בשוק המקצועי והדינאמי.

1-800-36-10-60 | www.bih.co.il