| חידושים בתעשייה החכמה בישראל - 2020 |

מגזין ההייטק הישראלי

דצמבר 2020

דוח ההייטק של IVC ומיתר: פעילות המשקיעים הזרים בישראל גדלה משמעותית ב-2020, והביאה לזינוק בהיקפי ההון שהגיע לחברות צעירות ובשלות

"האקרים מבינים איפה מרוחה החמאה - ולכן תוקפים כיום את ההתחברות מרחוק"

הקורונה האיצה את המעבר לעבודה מהבית או ממקומות מרוחקים מהמשרד, והגדילה מאוד את החשיפה של ארגונים למתקפות סייבר בנקודה הפגיעה ביותר - החיבור מרחוק למערכות המחשוב. סייפ-טי הישראלית מציעה פתרון בגישה חדשה, ללא צורך להחליף את ה-VPN הקיים (המשך בעמ' 10)

- האם אתם מוגנים מהתקפת סייבר? הפתרון של Guardicore יגן עליכם ממתקפת כופר (עמ' 7)
- הסכם הנורמליזציה מול האמירויות פותח דלתות חדשות להייטק הישראלי (עמ' 19)
- לדבר למכשירים: בחברת Onvego רוצים שתשוחחו עם מכשירים כמו שמדברים עם חבר (עמ' 11)

המגזין הופק בשיתוף:

כלכליסט המחלקה המסחרית תוכן שיווקי

IVC DATA AND INSIGHTS

איגוד ההיי-טק הישראלי

להגן על הפיירוול של הארגון - ולעצור סוסים טרויאנים

מתקפות האקרים על מפעלים, ארגונים ואפילו מדינות - מתרבות והולכות, ולעתים דווקא הפיירוול שאמור להגן על המערכת הוא החוליה החלשה. חברת אמבדד סולושנס הישראלית היתה אחת הראשונות בעולם להציג פתרון לבעיה

לאחרונה היינו עדים למתקפות רבות של האקרים, בין אם מדובר בחברות במגזר התעשייתי, במגזר הביטוח, תשתיות חיוניות ועוד. "במקרים רבים מדובר במתקפת כופר, כמו במקרים של חברת ביטוח גדולה ויצרן שבבים בצפון", אומר ירון מינצקר מחברת אמבדד סולושנס, המספקת פתרונות אבטחת מידע.

לדבריו, "מתקפות כאלה נועלות את כל החברה או המפעל, שמושבתים עד לשחזור המידע או תשלום הכופר; ובנוסף, ההאקרים משיגים גישה למידע הרגיש ביותר של החברה, לאחר שהצליחו לעקוף את כל שכבות ההגנה".

חברת פורטינט, ספקית פתרונות פיירוול מהמובילות בעולם, פרסמה לא מזמן כי 49 אלף ססמאות VPN של לקוחותיה (ביניהם ארגוני ממשלה ובנקים) זלגו החוצה, וייתכן שהגיעו לגורמים עוינים. בעיה דומה קיימת גם במערכות תעשייתיות (SCADA), המותקנות בתשתיות רגישות, כגון מפעלים, מתקני חשמל, מים ועוד.

המוצר שפיתחה אמבדד סולושנס משלב טכנולוגיות White Box Cryptography (WBC), סינון ב-Layer 2, אי תלות בפרוטוקולים ואי-נראות רשתית המיועדות להתמודד עם מקרים מסוג זה ומספקות אפשרות לתקשורת דו-כיוונית מאובטחת, תוך מניעת מתקפות על הפיירוול שמבקשות לפתוח בו "דלת אחורית".

Embedded Solutions 3000
TOP
Cyber Security
Companies in Middle East
2020
Recognized by
ENTERPRISE SECURITY

אמבדד סולושנס נבחרה לאחת מ-TOP10 חברות הסייבר המובילות במזרח התיכון, ע"י מגזין Enterprise Cybersecurity

התמונה באדיבות חברת אמבדד סולושנס

לדברי מינצקר, "כלי ההגנה הקיימים כיום חדירים בפני עצמם למתקפות. ברוב המקרים, מדובר בפישינג - מישהו שהצליח להשיג גישה לתוך הארגון ואפשר לעשות את זה בקלות. מספיק שאחד העובדים לוחץ על לינק או פותח קובץ, או שילמו לו קצת כסף כדי לספק גישה להאקרים. כך נכנס למערכת סוס טרויאני שתוקף בין היתר את כלי ההגנה עצמו ופורץ אותו, כך שההאקרים יכולים 'לחגוג' על המידע של החברה ובמקרה של תשתיות קריטיות לבצע פיגוע טרור.

"הפתרון שלנו מגן בין היתר גם על כלי ההגנה עצמם מהתקפות חיצוניות. לו עצמו אין כתובות IP ו-MAC כך שהוא שקוף, אי אפשר לראות אותו ולתקוף אותו. הוא מספק הגנה חיצונית ופנימית, וכך במקרה של מתקפת פישינג שהצליחה להיכנס לארגון, הוא סוגר את הפרצה ועוצר את ההאקרים".

בנוסף, אומר מינצקר, "אנחנו נותנים מענה לבעיה של ארגונים רבים שהתקשורת בין הסניפים שלהם מתבססת על SSL ו-VPN, כלומר, עושים שימוש בסמה חיצונית שקל לתוקפים מבחוץ להשיג אותה, ואז הם יכולים לעשות כבשלהם במערכות המחשוב. בטכנולוגיית WBC, אין כלל מפתחות חיצוניים שמהווים נקודת תורפה".

אמבדד סולושנס פועלת בשוק זה 18 שנה, כשעיקר לקוחותיה בשנים הראשונות היו גופים ביטחוניים. "למעשה, פיתחנו פתרונות WBC עוד לפני שקראו להם כך, כלומר, רק עכשיו השוק מגיע למקום שבו אנחנו נמצאים כבר זמן רב".

לפרטים נוספים: www.embedded-solutions.co.il

03 / הדרך של סאסא סופטוור להגן על תשתיות קריטיות מפני מתקפת סייבר

04 / דברי פתיחה - איגוד ההייטק

05 / אמדוקס - הענקית הישראלית שממשיכה להוביל את השוק ולהתחדש

06 / סיכום שנה בהייטק הישראלי

07 / Guardicore מציעה תוכנה חכמה המספקת אבטחה רשתית מהירה ויעילה

08 / נא להכיר: הבניין הירוק - ששומר על בריאות העובדים

10 / לאבטח התחברות מרחוק בלי להחליף את ה-VPN: הפתרון של סייפ-טי

11 / דברו אל מכונת המשקאות ואל המעלית - עם המערכת של Onvego

12 / קבוצת מ.ת.א.ל מעדכנת את הטכנולוגיה של מוצרי גילוי האש

13 / לומניס הישראלית מציגה פריצת דרך נוספת ברפואת עיניים

14 / הפתרון הייחודי של IMNA מעלה את סיכויי ההצלחה בניסויים רפואיים

15 / אפשר לרשום פטנט על תוכנה - ובפירמת עורכי הדין פינגן יודעים כיצד

16 / מה צריכים לדעת יזמים ישראליים שיוצאים לחפש משקיעים?

17 / חזק נטוורקס סוגרת את פרצת האבטחה שיוצרים הסמארטפונים של העובדים

17 / רובוטיקה ברחפנים וברכב אוטונומי: החדשנות של Thirdeye systems

18 / באקווה סקיוריטי מפתחים פתרונות אבטחה שנולדו לענן - ומנצלים את כל היתרונות שלו

19 / בהייטק הישראלי מתכוננים להזדמנויות חדשות מול משקיעים מהאמירויות

ניהול והפקה:
חברת פפריקה www.paprikapro.com
PAPRIKA
Spicy Marketing Relations

עורכת: חוה טרטנר

עיצוב: נעה כהן

מנהלת המגזין: ענבל פלג
inbal@paprikap.com | 052-3232130

זכויות היוצרים על התצלומים המופיעים בעיתון שייכות למפרסמים ולאתר depositphotos.com

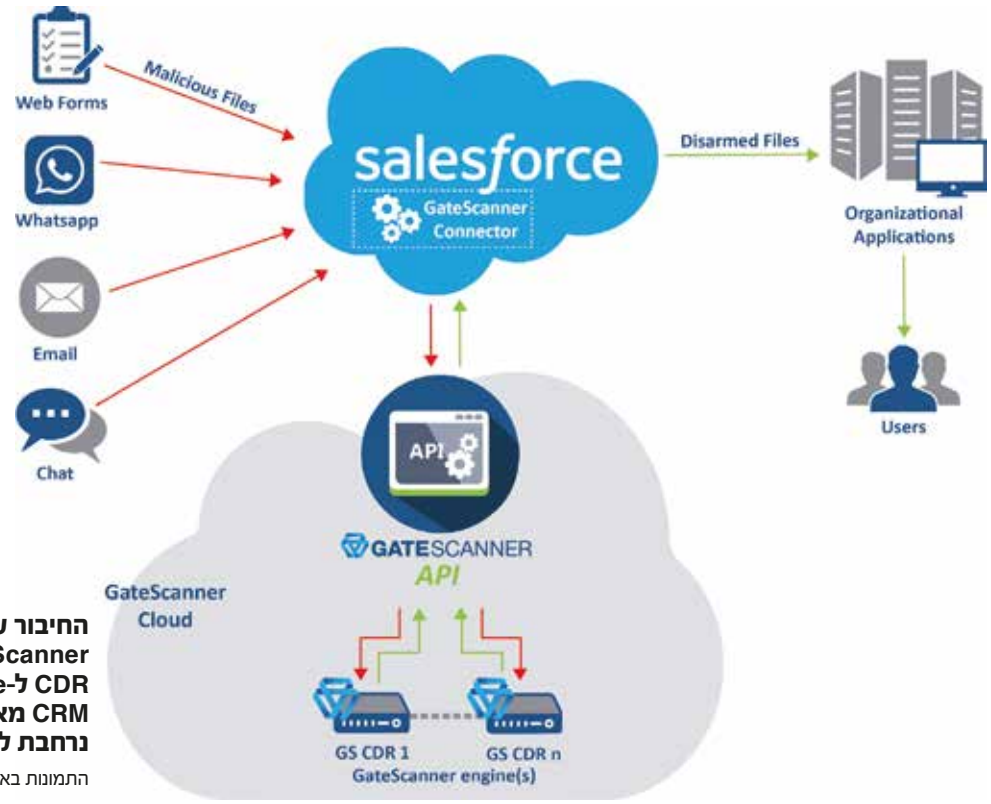
גילוי נאות: המוסף הינו בהפקת חברת פפריקה הפקות בשיתוף עם המחלקה המסחרית של כלכליסט, מערכת עיתון כלכליסט ו/או חברת פפריקה אינן אחראיות לתוכן המודעות וכן מבקשות להבהיר כי המוסף הינו פרסומי ואין לראות במאמרים ו/או במודעות משום המלצה מכל סוג שהוא.

המגזין הופק בשיתוף
עם IVC ואיגוד ההיי-טק הישראלי

כלכליסט
המחלקה המסחרית
תוכן שיווקי

האנטומיה של מתקפות סייבר

כללי המשחק של המתקפות השתנו. מה אנו יכולים ללמוד מהאירועים האחרונים? / יעקב ירוסלב



החיבור של GateScanner CDR ל-Salesforce CRM מאפשר הגנה נרחבת לארגון

התמונות באדיבות סאסא סופטוור

מתקפת הסייבר על "שירביט" מצטרפת לגל מתקפות על ארגונים בארץ ובעולם המצביעות על שינוי מהותי בדפוסי הפעולה של התוקפים. אם בעבר מתקפות היו "שקטות" ונועדו בעיקר עבור גניבת מידע, הדפוס שרואים כיום הוא התבססות של התוקפים ותכנון שעת "שין" ליצירת נזק רוחבי, תוך התמקדות בפגיעה תפעולית ותדמיתית. דוגמה לכך היא המגמה של מתקפות הכופרה מסוג Wiper ransomware.

כולנו שמענו על ארגון שנפגע או שחווינו זאת אישית - פותחים צרופת אימייל (Attachment) ולפני שיודעים זאת, מתקפה משתלטת על המחשב ומצפינה את הקבצים. במציאות הנוכחית, התרחיש חמור הרבה יותר, כשהאקרים מתמקדים ב"מחיקה" רוחבית של הארגון.

הפריצה הראשונית מושגת במגוון דרכים - הורדת קובץ מאתר לגיטימי שנפגע, מתקפות "דיוג" (פישינג) בדואר, קבלת קבצים משרשרת האספקה וחדירה דרך חולשות נוספות במערך האבטחה. במקרים רבים נעשה "מיחזור" ואריזה מחדש של פוגען ידוע כדי שיוכל להתגבר על מערכות לזיהוי איומים. ברגע שהושגה האחיזה הראשונית מתחיל רצף של אירועים. התוקפים מאתרים חולשות ברשת הארגונית, לעתים עם כלי פריצה (pentest) מסחריים. החולשות מאפשרות השגת שליטה מרבית על נקודות הקצה, השרתים, הגיבויים ואחסון הענן של יעד התקיפה. הפצת המתקפה מתבצעת על ידי רכיב "תולעת" (worm) למעבר מרשתות מנהלתיות אל הרשתות התפעוליות והרגישות של הארגון. שלב זה עשוי להימשך מספר שבועות תוך מעורבות פעילה וממוקדת מצד התוקפים. חלק משמעותי בשלב זה הוא גניבת מידע רגיש כדי שישמש כמנוף להפעלת לחצים בהמשך.

לאחר שהשליטה על הארגון הושגה, תוכנת הצפנה מופעלת בצורה מסונכרנת כדי להשיג שיבוש ארגוני נרחב ומהיר, כך שהארגון לא יוכל לעצור את התפשטות הנזק. לאחרונה ישנה גם מגמה של הצפנה בלתי הפיכה למחשבים שנפגעו, כך שמטרת התקיפה היא השבתת היעד ולאו דווקא תשלום כופר.

ראיונות עם האקרים שמאחורי התקיפות מגלים כי הדפוס אינו מקרי. התקיפה הרוחבית יוצרת מנגנון שמפעיל על המותקף לחץ לשלם את הכופר, הן כדי לשחרר את ההצפנה והן כדי למנוע נזק תדמיתי וכספי עקב הדלפת המידע.

אז מה ניתן לעשות?

במציאות של האיומים הנוכחיים חשוב מתמיד שארגונים יפרסו מערך הגנה מבוסס שכבות ממגוון טכנולוגיות, ויוודאו שהתשתית הקיימת מיושמת באופן מיטבי. במקביל, יש לבחון אילו פערי הגנה קיימים. על פי דו"ח מחקר של חברת Verizon, קרוב ל-50% מהמתקפות מגיעות דרך קבצים. מסמכי "עבודה" ובמיוחד קבצי PDF ו-MS-Office מהווים ווקטור תקיפה מרכזי, עקב קלות ההטמעה של נוזקות כך שיוכלו להתגבר על סריקת AV סטטית וניתוח דינמי באמצעות Sandbox או באמצעות כלי זיהוי בנקודת הקצה. מערכות "הלבנה" או Content Disarm and Reconstruction (CDR) הן כלי מוכח למניעה מראש של השלב הראשוני של החדרת קבצים פוגעניים לארגון, ובכך עצירת שרשרת התקיפה. המערכות המובילות, כגון GateScanner מבית Sasa Software משלבות את מיטב כלי הזיהוי, לרבות מערכות NextGen AV, כדי לנפות מראש קבצים נגועים, אשר "עברו" שכבות הגנה קודמות. אך מערכות הלבנה יוצאות מנקודת הנחה שזיהוי איומים עשוי להיכשל ולכן מפעילות תהליך נטרול איומים שהופך כל קובץ שנכנס להעתק בלתי מזיק, ובכך מונעות איומים מתקדמים ובלתי ניתנים לזיהוי, לרבות מתקפות אשר מעולם לא נראו לפני כן.

יענקלה ירוסלב, מנכ"ל סאסא סופטוור

שימוש במערכות הלבנה נפוץ מזה שנים רבות בישראל, וכעת רואים אימוץ בינלאומי נרחב, לרבות המלצה של חברת האנליסטים גרטנר לשילוב CDR כשכבת הגנה חיונית לכלל האוכלוסייה. את החשיבות של השימוש בהן ניתן לראות בכך שסאסא סופטוור הוכרזה על ידי גרטנר כ-"Cool Vendor" להגנה על תשתיות קריטיות Cyber - Physical Security.

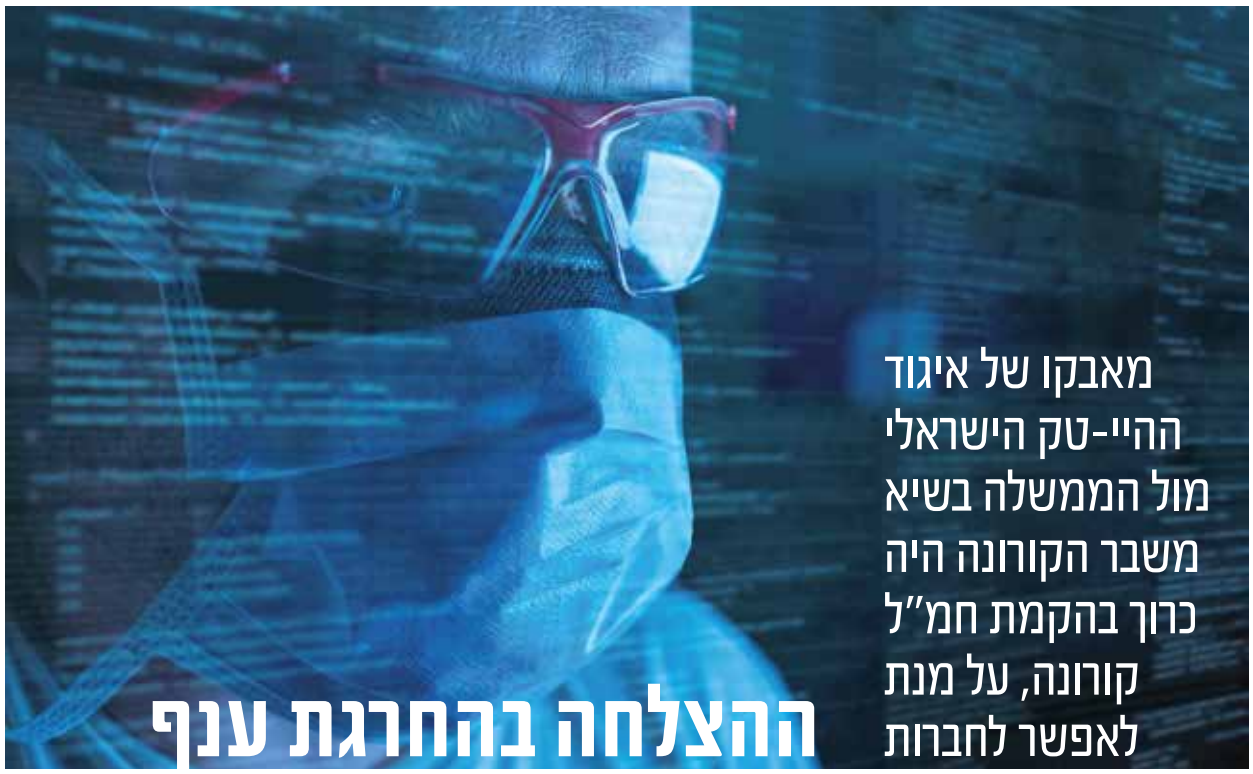
אם בעבר השימוש במערכות "הלבנה" היה בעיקר בכדי להגן על רשתות רגישות, הרי שכיום גוברת ההבנה שיש לחבר את המערכות אל מכלול הדרכים להעברת קבצים לתוך וגם אל מחוץ לארגון. ערוצי תקשורת קריטיים הם דואר אלקטרוני, הורדות קבצים מגלישה, שיתוף קבצים, כספות ומגוון רחב של אפליקציות ומערכות צד שלישי. תקופת הקורונה והעבודה מהבית מייצרות אתגרים נוספים. עובדים רבים נמצאים בסביבה שאינה מבוקרת אבטחתית, ואף משתמשים במחשבים אישיים שאינם מותקנים עם כלי ההגנה הארגוניים. לכן, המציאות מייצרת חשיפה מוגברת כיוון שעובדים ולקוחות עשויים לשלוח קבצים ממחשבים אישיים שנפגעו.

לדוגמה, במגזר הבריאות נדרשו המטופלים לצמצם הגעה למרפאות, ולכן חל גידול ניכר בתקשורת מרחוק עם הצוות הרפואי. כדי לשפר את רמת האבטחה, אסותא מרכזים רפואיים, במסגרת פרויקט שביצעה Deloitte, מפעילה כיום את GateScanner CDR על כל הקבצים שמטופלים שולחים לתוך ה-Salesforce CRM הארגוני. כדי לתת מענה נרחב, סאסא סופטוור השיקה מגוון מוצרים כשירות, SaaS. בשיתוף פעולה עם MedOne, לקוחות בישראל יכולים כעת להגן על מגוון ערוצים, לרבות הדואר הארגוני כולל חיבור ישיר ל-Office 365, להשתמש במערכת ייעודית לניהול תוכן, ולחבר מגוון רחב של אפליקציות באמצעות מנגנון REST API.

לסיכום,

נקודת מפנה חלה השנה גם באיומי סייבר מדינתיים. במתקפה שיוחסה לאיראן, נפגעה חברת התוכנה "עמיטל" כמו גם עשרות מלקוחותיה בתחום השינוע והלוגיסטיקה. האם מטרת מתקפה זו הינה גם שיבוש מערך הפצת חיסוני הקורונה? הרי איראן כבר ניסתה לפגוע במערכות המים בישראל. דפוסי ההגנה שנועדו למנוע את המתקפות ה"שקטות" מהעבר רלוונטיים גם כיום, אך רמת הסיכון עלתה ברמה ניכרת. להגנה מיטבית הכרחי ליישם מנגנוני הגנה המתבססים על מניעה מראש. מערכות הלבנה הן רכיב חיוני בגישה זו, וכעת זמינות גם לקהל הרחב.

הכותב הוא מנכ"ל סאסא סופטוור, yeroslav@sasa-software.com, אתר: www.sasa-software.com



מאבקו של איגוד ההיי-טק הישראלי מול הממשלה בשיא משבר הקורונה היה כרוך בהקמת חמ"ל קורונה, על מנת לאפשר לחברות הטכנולוגיה להמשיך ולייצר במרץ

מירב קינן, מנכ"לית איגוד ההיי-טק הישראלי

ההצלחה בהחרגת ענף ההיי-טק בעת משבר הקורונה אפשרה לתעשייה בישראל להמשיך להוביל את המשק

השנה החולפת, שנת 2020, הייתה מהשנים המאתגרות והקשות שחווה המשק הישראלי ומאתגרת מכולן לחברות ההיי-טק במדינה. בחודש מרץ מצאה עצמה תעשיית ההיי-טק מושבתת בהינף יד, כאשר המגיפה משליכה על פעילות החברות ועל המשך פיתוח החדשנות בהן. עם זאת, כאשר ענפי מסחר רבים במשק נפגעו קשות כתוצאה ממשבר הקורונה, מגזר ההיי-טק ספג את הפגיעה הכי מועטה ביחס לשאר ענפי המשק ממשבר הקורונה. בזמן שענפים רבים רחוקים מהתאוששות וחלקם עדיין מושבתים, אנחנו רואים כיום כי הביקוש לעובדים בהיי-טק בענפי המידע והתקשורת מתקרב לרמתו לפני המשבר, הון ממשיך לזרום לענף ותהליכים טכנולוגיים הואצו בשל הקורונה כך שנוצר פוטנציאל שוק חדש לחברות ההיי-טק בעיקר בתחומי הרפואה, דיגיטל, סייבר ותעשייה מתקדמת.

זה לא קרה מעצמו. חברות ההיי-טק אמנם יודעות להתאים עצמן למצבים משתנים ורבות מהן מבססות את היכולת העסקית על היכולת להגיב במהירות, אבל במשבר הקורונה זה לא מספיק. מיד כשהתחיל משבר הקורונה אנו, ראשי איגוד ההיי-טק בהתאחדות התעשיינים, פנינו לראש הממשלה, בנימין נתניהו, בדרישה להחריג את ענף ההיי-טק ולאפשר לו להמשיך לפעול תוך ציות מלא להוראות משרד הבריאות. זה לא היה פשוט. זה היה קרב שניהלנו עד הרגע האחרון כשבכל צומת מופעלים לחצים להשבית לחלוטין את הענף. לחצים שהצלחנו להדוף. ההצלחה בהחרגת הענף ואספקת תעודות המשך עבודה, אפשרה לחברות ההיי-טק בישראל להמשיך להוביל את המשק ובהתאם הצטרפו לאיגוד עשרות חברות חדשות.

מירב קינן, מנכ"לית איגוד ההיי-טק הישראלי | באדיבות איגוד ההיי-טק הישראלי

כחלק מהפעילות הקמנו חמ"ל קורונה, שנתן מענה מיידי לחברות התעשייה והשקנו, במסגרת פעילות התאחדות התעשיינים, את תוכנית "מגן תעשייה" לקטיעת שרשראות ההדבקה בתעשייה. כיום אנו מפעילים מערך של הכשרות לחוקרים אפידמיולוגיים, מצליחים לשחרר מבידוד עובדים רבים, ובעיקר - מאפשרים לחברות להמשיך ולייצר בכל הכוח גם תחת מגיפה של פעם במאה שנים. בזכות המאבק של התאחדות התעשיינים, בג"צ הורה להפסיק להכיר בימי הבידוד כימי מחלה והבאנו לכך שהמדינה תשתתף במימון עלות ימי הבידוד. לאחרונה מאבק נוסף שלנו נשא פרי כשמשך הבידוד קוצר ל-10 ימים.

שמירה על הישגי תעשיית ההיי-טק תוביל להתאוששות המשק

המאבק המוצלח להחרגת ההיי-טק לא התרחש בוואקום. בשנים האחרונות הפך איגוד ההיי-טק לאיגוד המוביל והמשפיע על מקבלי החלטות וקובעי המדיניות בממשלה. האיגוד פועל במטרה לפתח משק יצרני ויצירתי בתעשיית ההיי-טק הישראלית - לחפש כיוונים טכנולוגים חדשניים וליצור את החיבור בין החדשנות של החברות באיגוד לחברות התעשייתיות במשק. האיגוד טיפל במאות פניות של חברות לקבלת סיוע במימון ומענקים. הנפקנו תעודות אישור שיוך לענפים מוחרגים, קידמנו פעילות מול הרשות לחדשנות בנושא מימון חברות שלמות, קידמנו פעילות מול הגופים המוסדיים להשקעה בחברות היי-טק, פתחנו פורומים מקצועיים חדשים, ביצענו פעילות מול משרדי הממשלה השונים וקידמנו מגוון פעילויות שסייעו לתעשייה לשמור על מקומה כקטר הצמיחה של המשק הישראלי.

כעת ברור ביתר שאת כי הערוץ המשמעותי ביותר להתאוששות המשק יהיה באמצעות שמירה על הישגי תעשיית הטכנולוגיה העילית. תעשייה אשר יצרה בשנים האחרונות כ-12% מהתמ"ג ותרמה לייצוא בשנת 2019 מעל 46 מיליארד דולר. זה הזמן לקחת את תעשיית הטכנולוגיה העילית, ואיתה את המשק כולו, צעד משמעותי קדימה, כלכלית וחברתית. המדינה חייבת ליצור תנאים המעודדים חברות טכנולוגיה ישראליות להתאגד, לצמוח ולהתבסס בישראל. המשימה הדחופה ביותר של הממשלה הינה להתמקד בהצמחה של חברות ישראליות שלמות (חברות גדולות המנוהלות בשלמותן מישראל).

עם הדיווחים על חיסון, אנחנו מתחילים לראות אווירה אופטימית יותר ואנו מקווים כי בחודשים הקרובים ניתן יהיה לחזור לפעילות בינלאומית ולשגרה עסקית מלאה. למרות שנת הקורונה הקשה, ענף ההיי-טק המשיך להיות הקטר של המשק, אך כדי שימשיך להיות כזה, האתגרים העומדים לפתחו רבים. גם האיגוד מתחדש והחברים בו בחרו הנהלה חדשה, בראשות איש ההיי-טק מריאן כהן, נשיא קבוצת מר. הנהלת האיגוד הנבחרת תקדם חשיבה יצירתית ומחוץ לקופסה על חיבורים בין עסקים לתעשייה, ותפעל מול הממשלה לסיוע ממשלתי בתשתיות טכנולוגיות, הקלת רגולציה ומיסוי ועידוד פעילות החברות השלמות. בין הנושאים שאנו מקדמים כחלק מפעילות האיגוד: הקטנת הנטל הרגולטורי והבירוקרטי, הורדת מס חברות, טיפול בחוסר בכוח אדם ובעלות העסקה גבוהה בהשוואה בינלאומית על ידי הרחבת מסלולי התעסוקה, הכשרת כ"א איכותי על פי צורכי המעסיקים ומשיכת כ"א מקצועי מוביל מאוניברסיטאות מובילות בעולם.

האיגוד שקד בשנה הקרובה על הגדלת ההשקעה והתקציבים הממשלתיים לפיתוח חדשנות ותעשיית ההיי-טק. אנו עוסקים באופן תדיר בהרחבת סל השירותים לחברות האיגוד, בהקמת פורומים מקצועיים חדשים ומפגשים דיגיטליים ופרונטליים בין חברי האיגוד, בניית שיתופי פעולה ויצירת הזדמנויות עסקיות בארץ ובעולם. בתוקף פעילותינו בהתאחדות התעשיינים אנחנו מהווים גשר בין חברות היי-טק לחברות התעשייה השונות. אנו מתכוונים להגדיל את שיתוף הפעולה בתחומים המשפיעים ישירות על התעשייה בתחום הסייבר, AI, רפואה דיגיטלית, Industry 4.0 ועוד. אנחנו מאמינים שהשקעה בתחומים אלו יכולה להביא את ישראל למובילות בינלאומית, והחיבורים בין התעשיות יאפשרו לחברות ישראליות לשגשג ולצמוח להפעיל את השירותים שלהן בחברות.

כמנכ"לית איגוד ההיי-טק אני קוראת לחברות ההיי-טק להצטרף לעוצמה שייצרנו ומזמינה את השותפים שלנו להיות חלק ביצירת השינוי לטובת התעשייה כולה.

אמדוקס: לא מה שחשבתם

פיתוח בענן, מיקרו סרביסס וזמני תגובה של שניות גם במערכות שתומכות במיליארדי טרנזאקציות ביום. אמדוקס, מהחברות הגדולות ביותר שקמו בישראל, ממשיכה להוביל בחזית הטכנולוגיה ולאפשר לעובדים שלה להתנסות באתגרים מורכבים מאי פעם

אמדוקס, מענקיות ההייטק הישראליות, עוברת בשנים האחרונות מהפך של ממש. אם בעבר זוהתה החברה עם תחום הבילינג, כיום הוא רק אחד מתוך עשרות תחומי הפעולה של החברה, שבין לקוחותיה ענקיות גלובליות כמו Sprint, Vodafone, AT&T ו-T-Mobile.

"אוכלוסיית היעד העיקרית שלנו נותרה חברות הטלקום והמדיה ברחבי העולם, אבל אנחנו מפתחים עבורן את כל הפתרונות שהן צריכות - מיצירת לקוחות חדשים, ניהול קשרי לקוחות, טיפול ברכישה ברשת, ועד אקטיבציה ותפעול המערך שלהן", מספר אבישי שרלין, מנהל חטיבת הטכנולוגיה באמדוקס.

"כך למשל, חברות טלקום מתמודדות היום עם אתגר חדש - למשתמשים יש מגוון מכשירי קצה, מסמארטפונים משלל סוגים ועד טאבלטים ומחשבים. האינטראקציה עם משתמשי הקצה דורשת פיתוח שונה לחלוטין לעומת המערכות שפועלות מאחורי הקלעים (בקאנד), ואני שמח לומר שאנחנו עומדים בחזית הטכנולוגיה של פיתוח ממשק משתמש מודרני.

"יש לנו יחידות המטפלות בפיתוחים מורכבים למערכות מסחר אלקטרוני, שירותי דיגיטל מתקדמים וניהול מערכות מקוונות. יחידה המונה יותר מ-100 עובדי אמדוקס עוסקת כיום בפיתוח ממשק משתמש ואיפיון תהליכים באזורי הדיגיטל קומרס ושירות לקוחות - ולא כל העובדים הם מפתחים, מהנדסי תוכנה או מנהלי מוצר. על מנת לפצח את ממשק המשתמש ואת התהליכים האינטואיטיביים שבסופו של דבר יביאו את התוצאות העסקיות ללקוחות שלנו, אנחנו מעסיקים גם פסיכולוגים וסוציולוגים, ופועלים במתודה של Design Thinking שפותחה באוניברסיטת סטנפורד", אומר שרלין.

מאז ומתמיד, בכל שנות פעילותה, נדרשה אמדוקס להתמודד עם סדר גודל אדיר של לקוחות קצה - מה שרק גבר עם השנים. "אנחנו מטפלים במאות מיליונים, מיליארדים ואפילו עשרות מיליארדים של טרנזאקציות", אומר שרלין. "חשוב להבין שמשתמש היום נמצא כל הזמן באינטראקציה עם היישומים שלו, ואנחנו רוצים שהקשרים יהיו מותאמים אליו אישית. לכן, המערכות שלנו משלבות אנליטיקה ומנועים לומדים. התוצאה היא יכולות טיפול והתאמה ברמה פרסונלית מחד, ומאידך, התמודדות עם נפחי עבודה גבוהים בכמה סדרי גודל ממערכות שתוכננו לאלפי משתמשים.

"נסענו לעמק הסיליקון וישבנו במעבדות של גוגל, אמזון ומיקרוסופט, כדי ללמוד מחברות שמתמחות בסביבות של פיתוח ענן בסדרי גודל אדירים. כיום אנחנו משתמשים בשיטות ובכלים המתקדמים ביותר, מה ששינה את אופי העובדה וגם את אופי העובדים. כיום, קרוב ל-50% מהעובדים שלנו, ובחלק מהחטיבות אף יותר מכך, הם בני 26-27 לכל היותר".

אבישי שרלין, מנהל חטיבת הטכנולוגיה באמדוקס

כדי להפוך את החדשנות לחלק מהדנ"א של החברה, "הקמנו מעבדות חדשנות כדי לטפח רעיונות שהם לאו דווקא מסחריים", מסביר שרלין. "אנחנו מציגים אותם ללקוחות שלנו ובוחנים אותם גם בתוך החברה, כדי לראות אם הם יכולים להתאים לנו - מרעיונות דמיוניים לגמרי ועד אלגוריתמים חדשים שמפותחים פה. "אנחנו נדרשים לספק הרבה גמישות ללקוחות שלנו, כדי שיוכלו כל הזמן להמציא ולשנות תוכניות ורעיונות חדשים. הכל מתבסס על מנועים שלנו, שעברו לזמני תגובה של שניות, לעומת ימים ושבועות בעבר. עכשיו הכל בריל טיים, גם במערכות המורכבות ביותר".

בימים אלה, מוסיפה אמדוקס לגייס עובדים, ושרלין מדגיש כי "אנחנו מחפשים יצירתיות, ורוצים עובדים שמבקשים ללמוד את הכלים הכי מתקדמים בתעשייה ולהיות מעורבים בפרויקטים פורצי דרך. במקרים רבים, אנחנו נכנסים לתחומים שאיש עוד לא דרך בהם לפנינו. אנחנו החלוצים בפתרונות דור 5 בעולם, ומריצים פתרונות תוכנה לעולמות האלה שבמקומות רבים מאוד הם עדיין רק בשלב הניסוי. רבים מהעובדים שלנו מגיעים לכאן ללמוד ולהתפתח, ואז ממשיכים את הקריירה במרכזי הפיתוח שלנו בעולם, כמו באירופה וארה"ב".

לפרטים נוספים: www.amdocs.com

בוגרי תכנית ה-Greenhouse לגיוס סטודנטים 2019, ב-Web Summit בליסבון

התמונות באדיבות חברת אמדוקס

מעורבות גבוהה בקהילה

"כחברה עסקית מובילה בתחומנו, יש לנו תפקיד משמעותי בהתמודדות עם האתגרים החברתיים והסביבתיים הגדולים ביותר בעולם - הדבר נכון לגבי ההון האנושי שאנו מגייסים לאמדוקס, לטכנולוגיות שאנו מפתחים, וכמובן לעשייה החברתית והסביבתית הענפה שלנו ברחבי העולם", אומר שרלין.

"עולמות האחריות שלנו מגוונים וכוללים צמצום פערים דיגיטליים, הנעת תעסוקה עתידית, עידוד יזמות וחדשנות, תמיכה בחינוך, בפיתוח מוצרים בני קיימא ועוד, כל זאת תוך הטמעת גיוון והכלה ושמירה על הסביבה. "כך למשל, עובדים שלנו ממקסיקו פיתחו בהתנדבות פלטפורמה טכנולוגית שמחברת בין עודפי מזון לבין אנשים נזקקים, ובשנה וחצי הראשונה להשקה, למעלה מ-400 אלף אנשים כבר קיבלו מזון בזכות הטכנולוגיה שפיתחנו. דוגמה נוספת היא ממשק טכנולוגי שיצרנו עבור אחת הלקוחות שלנו, חברת סלולר, שאיפשר ללקוחות שלה לתרום חלק מחבילת הגלישה שלהם לטובת נערים בסיכון. כמו כן, אני גאה מאוד במיזם 'חברים דיגיטליים' שאמדוקס יזמה בתקופת הקורונה, המאפשר לעובדים שלנו לתת תמיכה דיגיטלית באזרחים ותיקים במטרה לסייע להם להשתמש באפליקציות שיחות וידאו על הטלפון".

"סביבת עבודה גמישה ומאפשרת"

ערין סלמן מטר, מנהלת צוות באמדוקס, עובדת בחברה כבר 14 שנה, ומילאה שורה של תפקידים מגוונים. לדבריה, "הודות לכך שהחברה גדולה מאוד ועוסקת בהמון דברים, בכל שלב בקריירה שלי, מצאתי תפקידים ותחומים שעניינו אותי, כולם בעולמות הטכנולוגיה והפיתוח.

"סביבת העבודה מוכוונת תוצאות ועל כן יש גמישות ואפשרויות לא רק להורים שרוצים לשלב קריירה ומשפחה, אלא לכל מי שרוצה לשמור על איזון מול החיים הפרטיים שלו. אני למשל, כאם לשתי ילדות קטנות, לא מרגישה שאני צריכה להתפשר בקריירה או בחיים הפרטיים. גם האמהות מעולם לא הפריעה לי להתקדם בקריירה, ניהולית או מקצועית, ולא בכדי, יש לא מעט עובדים עם ותק דומה לשלי ויותר, שמתפתחים לאורך השנים".

דוח ההייטק של IVC ומיתר קובע:
2020 - שנת שיא בגיוסים ושפל באקזיטים

לפי נתוני החברות, ב-2020 נרשמו 578 עסקאות בסכום השקעה כולל של כ-9.9 מיליארד דולר; מספר העסקאות עלה ב-14%, וההון המושקע צמח ב-27%. עם זאת, נרשמה ירידה חדה בעסקאות המיזוגים והרכישות

שנת 2020 פותחת עשור עם צמיחה מואצת בגיוסי ההון בהייטק הישראלי, כך עולה מנתוני דוח ההייטק ל-2020 של חברת המחקר IVC ופירמת עורכי הדין מיתר. מהדוח עולה כי ב-2020 רשמו החברות הישראליות 578 גיוסי הון בסכום השקעה כולל של כ-9.9 מיליארד דולר. מדובר בגידול של 14% במספר העסקאות מהשנה שעברה, ובצמיחה של 27% בהון המושקע. כמו כן, נרשם שיא בגיוסי ההון בזירת חברות ההייטק הנסחרות בבורסות תל-אביב ובעולם. 121 חברות גייסו 6.55 מיליארד דולר ב-2020, לעומת 68 חברות שגייסו 1.95 מיליארד דולר ב-2019. מבחינת המשקיעים, המגמה הבולטת ב-2020 היתה התמקדות בחברות הפורטפוליו הקיים וגידול בהיקפי השקעות ההמשך.

גיא הולצמן, מנכ"ל IVC, אמר כי "אנחנו מעריכים כי לאחר שנה מאתגרת אך מוצלחת עבור חברות סטארטאפ ישראליות, ההייטק הישראלי ימשיך להוות מקור משיכה לשחקנים בינלאומיים מובילים, פיננסיים ואסטרטגיים. בשנה החולפת פעילות המשקיעים הזרים בישראל גדלה משמעותית, והביאה לזינוק בהיקפי ההון שהגיע לחברות צעירות ובשלות. אל מול האתגרים הפיננסיים בתעשייה, נראה בשנה הקרובה את המשקיעים המוסדיים הישראלים מגדילים את המעורבות בתחום".

מקור גרפים: IVC-Meitar The Israeli Tech Review 2020

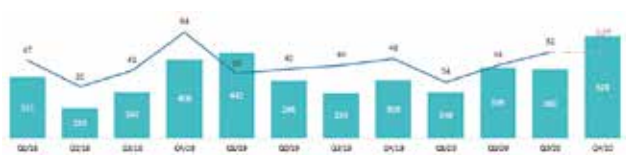
ההייטק הישראלי, 2015-2020

העלייה בהשקעות בהייטק הישראלי

קרנות הון סיכון: התחזקות במחצית השנייה של השנה

ב-2020 השתתפו קרנות הון סיכון ב-371 עסקאות בסך השקעה כולל של 8.74 מיליארד דולר. מדובר בעלייה במספר העסקאות ובסך ההשקעה של קרנות הון סיכון לעומת השנה החולפת. השקעות בסבבים מוקדמים (Seed + A Rounds) חוו ירידה במהלך הרבעון הראשון והשני של 2020, בגלל חוסר הוודאות בשוק לאור משבר הקורונה, אך ברבעונים השלישי והרביעי נרשם זינוק בהשקעות הקרנות מבחינת הסכומים ומספר העסקאות.

השקעות של קרנות הון סיכון בסבבי Seed + A Rounds, לפי רבעונים



המיזוגים והרכישות ירדו - ההנפקות הראשונות עלו

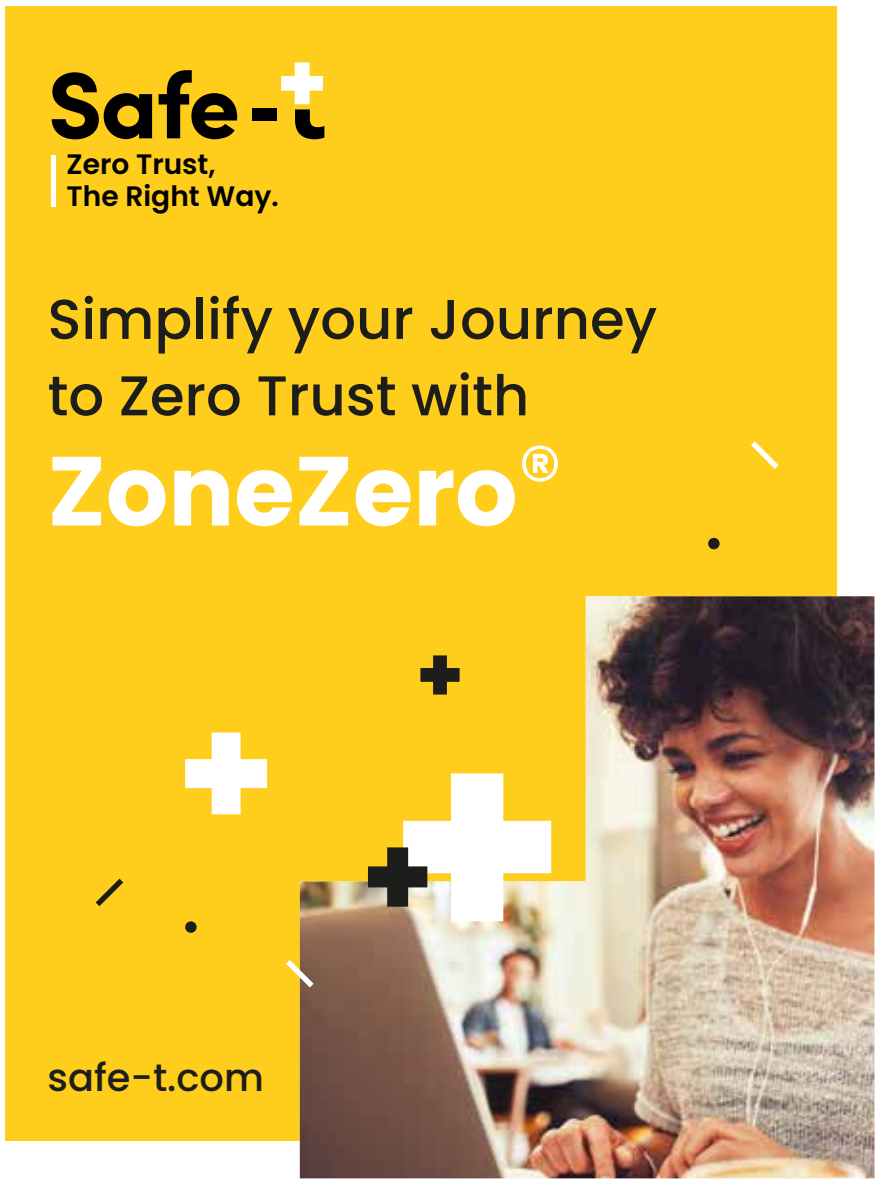
בכל הנוגע למיזוגים ורכישות, 2020 מסתיימת עם ירידה חדה - 93 עסקאות בהיקף כולל של 7.8 מיליארד דולר, בהשוואה ל-14.24 מיליארד דולר ב-143עסקאות ב-2019 (בנטרול עסקאות של 5 מיליארד דולר ומעלה).

במהלך 2020 התבצעו 18 הנפקות ראשונות (IPO) של חברות ישראליות בשווקי ההון בארץ ובעולם, בסך כולל של כ-1.6 מיליארד דולר. בסך הכל הגיעה פעילות החברות הציבוריות הישראליות בשווקי ההון לכ-6.55 מיליארד דולר ב-2020 (כולל הנפקות ציבוריות ופרטיות וגיוסי חוב) ב-121 עסקאות לעומת 1.95 מיליארד דולר שגויסו ב-68 עסקאות ב-2019.

מחברי הדו"ח, שירה עזרן, מייק רימון ואיתי פרישמן, שותפים במשרד מיתר, מסבירים כי "בעוד שב-2020, בעיקר לאור מגפת הקורונה, ראינו ירידה משמעותית בפעילות המיזוגים והרכישות של חברות ישראליות, הרי שבמקביל חלה עלייה משמעותית בגיוסי ההון על ידי משקיעים ישראלים וזרים. 2020, שהיתה לאורך חודשים ארוכים תחת עננת הקורונה, מסתיימת באופן חזק ועם תקווה להמשך הפעילות המשמעותית בגיוסי ההון ובהנפקות ולצמיחה מחודשת במיזוגים ורכישות".

אקזיטים בהייטק הישראלי לפי סוג העסקה

מקרא משמאל לימין: רכישות (buyouts) במיליוני דולרים | הנפקות ראשונות במיליוני דולרים | מיזוגים ורכישות במיליוני דולרים | מספר רכישות | מספר הנפקות | מספר מיזוגים ורכישות



הגנת סייבר בארגונים - סגמנטציה רשתית, קו ההגנה החיוני ברשת הארגונית

Guardicore מספקת אבטחה רשתית במהירות רבה וביעילות גדולה בהרבה מאשר השימוש בשיטות המסורתיות

במציאות של היום ולאור ריבוי התקפות מסוג כופרה לאחרונה, הגנת סייבר בתוך חוות השרתים והרשת הארגונית בכלל היא תחום מאתגר מאוד עבור מנהלי תשתיות ואנשי אבטחת המידע. הגדילה המתמדת בכמות השרתים, המעבר לענן והצורך בגמישות עצומה במערכות ובתקשורת בין השרתים ובין המשתמשים בארגון, מביאים איתם כפועל יוצא אתגר אדיר בשמירה ובתחזוקת הקשרים הנכונים בין השרתים בכל סביבה.

החשיפה לפריצות אבטחת מידע

גם מי שלא מגיע מתחום אבטחת המידע בפרט או מתחום מערכות המידע בכלל, יכול להבין את המונח "פילוח" או סגמנטציה. בדומה למה שאנו חווים מאז הגיעה הקורונה לעולם - הדרך להפחית את הסיכון בהדבקה (או פירצה ברשת בהקבלה) היא לייצר סגמנטים; מעין קפסולות ברשת בהתאם לצורך העסקי, ובעגה המקצועית Network Segmentation.

לא מעט ארגונים בארץ ובעולם ביצעו סוג של סגמנטציה רשתית כבר לפני שנים, בדמות סגמנטציה קשיחה המבוססת על VLAN ו/או Firewall רשתי. אלו הם פתרונות מהדור הקודם וכיום קשה מאוד, עד כדי בלתי אפשרי, להקים ולתחזק רשתות בצורה קשיחה ולא נוחה מסוג זה - פרויקטים כאלו הם על פי רוב מייגעים ומורכבים.

כיוון שכך, רוב הארגונים נשארו עם רשת שטוחה, שנחשבת כיום פצצת זמן מתקתקת המחכה לפורץ שיחדור לרשת הארגונית. ברשתות שטוחות תמיד אפשר למצוא חוליה חלשה ברשת שדרכה ניתן לבצע חדירה, באמצעותה התוקף יכול לנוע לרוחבה של הרשת, משרת לשרת, ויהיה כמעט בלתי אפשרי לבלימה.

ברוב המקרים, הארגון גם לא ירגיש בחדירה, במידע שידלוף החוצה או במערכות שיוצפנו עד שיהיה מאוחר מדי! הסיכון לחדירה אף הולך וגדל ככל שהארגון גדל ומספר השרתים ומשתמשי הקצה עולה וכן ככל שהארגון משתמש ביותר יישומים וגורמי צד שלישי המתחברים לרשת, למשל כאלה העוסקים בתמיכה.

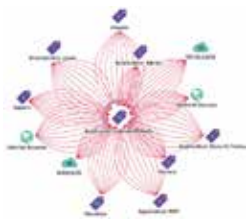
הפתרון האופטימלי: סגמנטציה מנוהלת תוכנה

ההבנה כיום בארגונים היא שסגמנטציה קשיחה אינה נותנת מענה לצרכים העסקיים מכיוון שהיא מורכבת ומסורבלת ליישום ולתחזוקה. הפתרון המודרני כיום לביצוע פילוח חכם ברשת (Network Segmentation) הוא באמצעות תוכנה.

Guardicore, חברה דינמית בעלת שילוב מנצח של מומחי סייבר מקהילת המודיעין עם בכירים מתעשיית הסקיוריטי בישראל, מאפשרת לארגונים להפחית את הסיכון לחדירה. המימוש מהיר, גמיש ומאפשר יישום חוקה בתוכנה בכל רמה אפשרית. על ידי כך, הפתרון מספק באופן אופטימלי אבטחה רשתית במהירות רבה וביעילות גדולה בהרבה מאשר השימוש בשיטות המסורתיות. המפתח ליישום סגמנטציה חכמה בתוכנה הוא לספק נראות גבוהה וממוקדת עד כדי רמת ה-Process לכל רוחב הרשת, כפי ש-Guardicore מסוגלת לספק.

תמונה מצב ברורה ועדכנית של משטח ההתקפה הפוטנציאלי

דמיינו לכם שמישהו או משהו היה יכול להראות לכם את כל הדרכים שבהן תוקף פוטנציאלי יכול להשתמש על מנת לגשת לשרתים והשירותים הקריטיים של הארגון, כולל, כמובן, דרכים שאפילו לא ידעתם על קיומן. הרי ברור שמיד תתקבל תמונה מאירת עיניים והעיוורון שקיים היום בנראות התעבורה בתוך הרשת הארגונית - יעלם. Guardicore מספקת כלי חכם הנפרס ברשת תוך שעות ספורות. הכלי מספק מפות מפורטות המאפשרות לראות בבירור - את כל היישומים שלכם כולל נתיבי התקשורת, לפני ואחרי מדיניות סגמנטציה. במילים אחרות, אתם מקבלים תמונה מצב ברורה ובזמן אמת של משטח ההתקפה הפוטנציאלי על האפליקציות הארגוניות, מאגר הנתונים, מאגר הקבצים וכדומה, עוד לפני ביצוע הפילוח וגם לאחריו.



Guardicore מספקת מפות מפורטות המאפשרות לראות את כל היישומים שלכם כולל נתיבי התקשורת, לפני ואחרי מדיניות סגמנטציה

איך מונעים תנועת תוקף ברשת?

כאמור, עם כל הוספה של שרת, שירות מסוג מנוי, או חיבור גורם צד שלישי העוסק בתמיכה ביישום ספציפי לדוגמה, משטח ההתקפה והסיכוי לחדירה לארגון גדלים. באופן דומה גם באמצעות כל יציאת רשת פתוחה (Port), נפתחת דרך חדשה לתוקפים לחדור לרשת.

חלק מפרוטוקולי התקשורת (Network Ports) מועדים יותר לשימוש לרעה במהלך תנועה רוחבית של התוקף ברשת ולמעשה מאפשרים לתוקף דילוג חשאי וקל משרת לשרת בתוך הרשת. דוגמה לפרוטוקולים מועדים לפורענות הם כאלו המאפשרים הרצת קוד (למשל: SSH), יציאות רשת מסוג SMB, או יציאות רשת בלתי מאובטחות דוגמת Telnet. מצב זה יוצר חשיפה גבוהה יותר ובאופן טבעי מהווה סיכון גדול יותר לפריצה לרשת מיציאות אחרות.

כחלק מהנתונים הנאספים, המערכת של Guardicore מספקת פירוט של כלל תעבורת הרשת ובפרט על פרוטוקולי התקשורת, כך שגם במקרים כאלו ניתן לקבל תובנות חזקות כאשר מיישמים סגמנטציה בתוכנה באמצעות המערכת של Guardicore.

Guardicore מביאה לתוצאות בשטח

ארגונים רבים בארץ ובעולם, ממגזרים שונים כמו פיננסים, טלקום, בריאות ותעשייה כבר בחרו ליישם סגמנטציה בתוכנה של Guardicore המצטיינת בתפיסת עולם זו. אחד מהם הוא ארגון המוכר לכולנו מתעשיית המזון והמשקאות, טמפו תעשיות. האתגר שעמד בפני מערכות המידע של הארגון בביצוע סגמנטציה ברשת הלך וגדל עקב הצמיחה של החברה, שהגדילה באופן טבעי את כמות השרתים.

אהוד הומינר, מנהל התשתיות הגלובלי של טמפו תעשיות, מסביר: "יש לנו בארגון מספר סביבות מחשוב ולכן חיפשנו פתרון אבטחת מידע בתפיסת ארכיטקטורה אלסטית שבנויה לענן, ומצד שני לא תלויה בתשתית ספציפית", הוא אומר. "ארכיטקטורה שתאפשר ותיישם החלת אבטחה באופן דינמי, ותתאים לטפל בטבע האלסטי של יישומי הענן בהם אנחנו משתמשים, במקביל לסביבת המחשוב ברצפת הייצור. Guardicore נתנה לנו מענה על כך ובנוסף תומכת באופן גמיש בעומסי עבודה גבוהים. הפלטפורמה מאפשרת לנו כוח אכיפה לחציצה בין שרתים ו/או תחנות באמצעות מיקרו-סגמנטציה ללא תלות בתשתית התקשורת עצמה וללא צורך ב-Firewall פנים ארגוני".

פאבל גורביץ', מנכ"ל ומייסד משותף של Guardicore, מוסיף ומציין: "על בסיס יכולת הנראות של הפלטפורמה שלנו, אנחנו עוזרים לארגונים לאכוף את מדיניות האבטחה שלהם עד רמת ה-process והשרת הבודד באופן ייחודי, תוך חסימת תקשורת שאינה לגיטימית וללא תלות בתשתית וטופולוגיה, בין אם השרתים בענן, באתר מקומי, או בכל שילוב אחר, ובכך ליישם סגמנטציה מלאה לכל הרשת בצורה פשוטה, והכל מנקודת ניהול מרכזית אחת".

לפרטים נוספים: 09-7880090 ● www.dna-it.co.il

"במציאות בה החברות מתחרות על הטאלנטים, סביבת העבודה היא שובר שוויון"

"ההצלחה של חברות טכנולוגיה מובילות נובעת מיכולתן לגייס את העובדים הטובים ביותר", אומר האדריכל חן שליטא, מנכ"ל אלפא פרויקטים ירוקים. "התחרות על תואר החברה שהכי כדאי לעבוד בה ממחישה את החשיבות של סביבת עבודה טובה ואיכותית, שגם מצמצמת למינימום פגיעה סביבתית"

"**אנחנו** מבלים את רוב שעות הערות שלנו באותם חללי תעסוקה, שם אנחנו יוצרים ומייצרים", אומר חן שליטא, מנכ"ל אלפא פרויקטים ירוקים. "ההפרש בין העלות שלנו כעובדים, לבין המחיר בו ניתן למכור את התוצרת שלנו, הוא זה שמספק רווח לחברות, ותורם לשגשוג הכלכלה. עם זאת, כדי שנהיה במיטבנו ונממש את הפוטנציאל היצירתי שלנו, המבנה שבו אנו שוהים שעות רבות כל כך מדי יום, צריך להיות מתוכנן כך שישמור על בריאותנו.

"כאן בא לביטוי החזון של חברת אמות, שאימצה אסטרגיית פיתוח בת-קיימא, החותרת לאיזון בין השיקולים הכלכליים, החברתיים והסביבתיים, וכפועל יוצא מקימה את מגדלי המשרדים לא רק במיקומים מרכזיים ובעיצוב אדריכלי מרשים - אלא גם תוך יצירת סביבות עבודה בריאות ונוחות, המצמצמות שימוש במשאבים סביבתיים".

הקשר בין אוויר צח לתפקוד קוגניטיבי

קבוצת חוקרים מבית הספר לבריאות של הרווארד, בראשות ד"ר ג'וזף אלן, הגדירה תשעה יסודות לבניין בריא ובדקה איך ניתן להגיע לשיפור תפקוד עובדים בחללי עבודה. "תוצאות המחקר הן מדהימות", אומר שליטא. "אצל מי שעבדו בחללי עבודה בריאים יותר, נרשמה עלייה של מאות אחוזים בתפקוד הקוגניטיבי. בין היתר, הם מצאו פתרונות יצירתיים יותר, הצליחו לעמוד בלוחות זמנים וגם דיווחו על מתח ועומס נמוכים יותר".

שליטא מציין את המאפיינים העיקריים של סביבת עבודה בריאה יותר: "העיקרון הראשון הוא נוחות ויזואלית. מעטפת בניין מתקדמת צריכה להחדיר אור יום שהוא הבריא ביותר לאדם, אך במקביל עליה למנוע סינוור והארת יתר, בלי לחסום את האפשרות להתבונן בנוף.

"העיקרון השני עוסק בנוחות תרמית. בניינים שאינם מתוכננים נכון, גורמים לקרינת חום מהמעטפת פנימה לעבר חללי העבודה. מעטפות תרמיות מתקדמות מקטינות את חדירת החום פנימה.

"עקרונות נוספים כוללים הכנסת אוויר צח לבניין ושמירה על איכות האוויר בתוך הבניין, כך שדייריו לא יסבלו מרעלים ומריחות לא נעימים, מניעת עובש, שמירה על איכות המים ולבסוף, הגברת תחושת הביטחון של דיירי הבניין.

באדיבות חברת אלפא פרויקטים

האדריכל חן שליטא, מנכ"ל אלפא פרויקטים ירוקים

"מעטפת הדאבל סקין שקיימת, בין השאר, בקמפוס אמות, מהווה חזית טכנולוגית חדשנית שמקיימת את כל העקרונות הללו, והופכת את אמות לאחת החברות היחידות בישראל שפועלות ברוח זו", מוסיף האדריכל שליטא. "קיר המסך מורכב מחלון פנימי וחלון חיצוני עם וילון ביניהם, שנשלט על ידי מערכת בקרה וכך עוקב אחרי זווית השמש, במטרה לספק אור טבעי מקסימלי ולמנוע סינוור. כמו כן, קמפוס אמות מתוכנן לעמידה בתקן LEED Platinum מה שמביא לחיסכון של כ-40% מאנרגיית החימום והקירור של הבניין וטביעת הרגל הפחמנית שלו תהיה מהנמוכות ביותר בישראל. אמות, בהובלת המנכ"ל, שמעון אבודרהם, היתה חלוצה ביישום טכנולוגיה זו, והיא חברה מובילה בתחום עד היום".

המעסיק מרוויח עוד כ-6,000 שקל בחודש לעובד

"חשוב להדגיש, שלעקרונות הללו יש משמעות כלכלית של ממש", מציין שליטא. כך למשל, מחקר שנערך בחיל האוויר האמריקאי מצא, שהקפדה על סביבת עבודה שקטה ואיכות אוויר, מעלה את הפריון של העובד ב-15% - בין היתר באמצעות צמצום מספר ימי המחלה והעלאת כמות החמצן באוויר, שמשפרת את היכולת לשמור על ערנות לזמן ארוך יותר.

"נניח שכיום עובד הייטק ממוצע יוצר למעסיק רווח של פי 1.5 מעלות ההעסקה שלו. כלומר, אם השכר הממוצע בהייטק ב-2019 היה כ-24 אלף שקל, ובתוספת עלויות נלוות של רכב, דלק וכו', עלות ההעסקה הכוללת היא 30 אלף שקל - עלייה של 15% בפריון, משמעה תוספת של 6,000 שקל עבור המעסיק, לכל עובד ועובד.

"בנוסף, בחברות הייטק יש סטטיסטיקות שמראות כי בחישוב כולל, עלויות שכר ונלוות הן 82% - ועלות שכירות המשרדים היא 9% בלבד. לכן, השקעה בבניין שנבנה לפי עקרונות הבניין הבריא ותורם לרווחת העובדים, ליצירתיות ולפריון שלהם, היא עסקה משתלמת מאוד".

שלושה מגדלים של החברה - מגדל אמות אטריום שאוכלס לפני חמש שנים, מגדל ToHa שבנייתו הסתיימה לפני שנתיים, וקמפוס אמות חולון הנבנה בימים אלה, הם פרויקטי המשרדים היחידים בישראל שזכו להסמכה הגבוהה בעולם לבנייה ירוקה - LEED Platinum, הקובע קריטריונים מחמירים לשמירה על נוחות ובריאות העובד תוך הקטנת עלויות תפעול ושמירה על הסביבה.

בבניין LEED Platinum, דמי השכירות גבוהים בכ-10 ₪ למ"ר. "בהנחה שהיחס הוא 10 מ"ר לעובד, מדובר על תוספת של 100 ₪ לעובד לחודש לעומת בניין רגיל. שוב, השקעה זו מחזירה לחברה 6,000 ₪ לחודש - פי 60!", אומר שליטא. "מכאן, שהפער בדמי שכירות בין בניין ירוק בתקן LEED לבין בניין 'רגיל', שווה לשוכר רווח של אלפי ₪ לחודש לעובד".

פארק ירוק גדול

קמפוס אמות חולון, הנבנה באזור התעסוקה של העיר ואכלוסו צפוי במחצית השנייה של 2021, כולל משרדים להשכרה בהיקף של 60 אלף מ"ר, כאשר שטחי הקומות נעים בין 2,600-3,600 מ"ר. בפרויקט זה, אמות ניצלה את חטיבת הקרקע הגדולה שבבעלותה וריכזה את כל הבינוי על 4 דונם מתוך 11, כדי ליצור פארק ירוק גדול . כחלק מהאסטרטגיה התכנונית, בנייני אמות ממוקמים בסמוך לקווי הסעת המונים, וקמפוס אמות בחולון נמצא במרחק מטרים ספורים מהתחנות העתידיות של הקו הירוק של הרכבת הקלה, וקו המטרו. במקום גם חניון אופניים מאובטח עם אפשרות לטעינת סוללות, חניה לקורקינטים ומלתחות בסטנדרט מלונאי גבוה. אמות מעודדת את העובדים להגיע בתחבורה אלטרנטיבית, אך כמובן שהקמפוס כולל גם חניון בן חמש קומות עבור כלי רכב פרטיים.

מגדל אמות אטריום | צילום: שרון צרפתי

מגדל ToHa | צילום: איתי סיקולסקי

קמפוס אמות חולון | הדמיה: ויו פוינט

CAMPUS AMOT

IT'S ABOUT TIME!

תנאים משתלמים במיוחד בקמפוס העסקים החדשני בישראל בהזדמנות שאסור לפספס

זה הזמן להצטרף לפרויקט המשרדים המוביל של אמות, הנבנה בתקן LEED Platinum – ההסמכה הגבוהה בעולם לבנייה ירוקה, הכולל בתוכו כל חלום שאי פעם היה לכם על המשרד הבא שלכם: תקרות גבוהות, חללי עבודה רחבים, חדרי כושר, מקלחות, מרפסת יוגה, פארק ירוק רחב ידיים ועוד.

אכלוס: חציון 2, 2021. **אזור התעסוקה חולון.**

amotcampus.co.il

אמות | *6744

"האקרים מבינים איפה מרוחה החמאה - ולכן תוקפים כיום את ההתחברות מרחוק"

הקורונה האיצה את המעבר לעבודה מהבית או ממקומות מרוחקים מהמשרד, והגדילה מאוד את החשיפה של ארגונים למתקפות סייבר בנקודה הפגיעה ביותר - החיבור מרחוק למערכות המחשוב. סייפ-טי הישראלית מציעה פתרון בגישה חדשה, ללא צורך להחליף את ה-VPN הקיים

האם אתם בודקים אם הדלת נעולה לפני שאתם הולכים לישון? סביר להניח שכן. אחרי הכל, יש לכם בבית חפצים יקרים, בין אם כספית או ללבכם, ואתם רוצים לשמור על ביטחונם. אך מה עם מערכות המחשוב של הארגון שלכם? האם לפני שאתם מכבים את האור ונכנסים למיטה, אתם מוודאים שאיש לא יוכל לפרוץ אליהן? סביר להניח שלא - גם אם תכולת המערכות הללו יכולה להגיע לשווי של מיליוני דולרים ויותר.

"אני אוהב להשוות את העולם הווירטואלי לעולם הפיזי", אומר שחר דניאל, מנכ"ל חברת אבטחת המידע סייפ-טי המפתחת טכנולוגיות גישה מרוחקת מאובטחת המבוססות על מודול ה-Zero Trust ו-Identity Awareness. "ברור לכולנו מה הנזק שעלול להיגרם מפריצה לבית שלנו, או לשדה תעופה - נזק רב מערכתי שיכול להתחיל מפגיעות קטנות אבל להגיע גם למצב שבו חיי אדם מצויים בסכנה. בעולם הווירטואלי, אנחנו לא מרגישים את הסכנה על בשרנו, אז קשה יותר להבין אותה, אבל היא קיימת. תשאל את מי שחווה כבר פריצה במשמרת שלו, התגובה שלו תהיה 'זר לא יבין זאת'.

"עסק או ארגון אחר שנתון למתקפת סייבר, חשוף לנזקים בכמה רמות. ראשית, קיימת סכנה של עצירה מוחלטת של הפעילות בגלל המתקפה. זו פגיעה שיכולה להגיע להיקף של מיליוני דולרים ואפילו יותר, בהתאם לסדר הגודל של העסק. מעל כ-30 שנה ארגונים מסתמכים בעיקר על שיטות גישה מיושנות מבוססות רשת, VPN ופיירוול והזדהות באמצעות OTP הנשלח למשתמש באמצעות הטלפון הנייד לאישור חיבור מרחוק. רק שחלפו הימים בהם השיטות הללו החזיקו מים. נתונים מראים שמעל 80% הפרות אבטחה קשורות בגניבת זהות וסיסמה. המטרה של התוקפים השתנתה ולכן גם המטרה של הארגון צריכה להשתנות ולהתמקד יותר באבטחה סביב המשתמשים ובמניעה של גניבת הזהויות שלהם.

"אבל מעבר לכך, קיימת סכנה גדולה יותר, של פגיעה במוניטין החברה. במקרים מסוימים, זה יכול לחסל עסק לחלוטין, או לעלות לו מיליארדי דולרים. אפשר להביא כאן את הדוגמה של יאהו, שלאחר שהדאטה בייס שלה נגנב בידי האקרים, הצעת הרכישה שהיא קיבלה צנחה במיליארדי דולרים. בנוסף, חברה שמחזיקה מידע פרטי וסובלת מפריצה, חשופה לתביעות ענק מצד הלקוחות".

מהן נקודות הכשל של הארגונים בתחום אבטחת המידע?

"אנחנו עוסקים בתחום כבר כמה שנים, והניסיון שלנו מראה שארגונים רבים מסתכלים רק על ה'ביזנס', ומבחינתם, כל השקעה שאינה בליבה העסקית, לא מניבה ROI ולכן הם מצמצמים אותה ככל האפשר. יש ארגונים ידועים ומכובדים, שמנהל אבטחת המידע שלהם הוא סטודנט בחצי משרה - מה שהם לא יעשו לעולם בתחום המכירות, למשל, מאחר שעל זה המנכ"ל נמדד בסוף השנה. זה מוביל לכך שכל עולם הסיכונים לא מנוהל כמו שצריך.

שחר דניאל, מנכ"ל חברת אבטחת המידע סייפ-טי

"וזו בעיה אמיתית - מאחר שעולם הסייבר הוא מטורף. גנב שמנסה לפרוץ לבית שלך הוא לא תמיד הכי מתוחכם, אבל יש בעולם אין סוף האקרים שהם מתוחכמים מאוד וממציאים את עצמם מחדש כל הזמן עם איומים חדשים. לאף עסק או ארגון אסור שיהיה רגע של נחת כל עוד הסיכונים קיימים והעסק לא מוגן מספיק. ארגון שלא פתוח לחדשנות ונצמד לפתרונות ישנים כי מבחינתו זה מעודכן מספיק או שאינו מעוניין 'לגעת' כי זה עובד, חושף עצמו למתקפות חדשות. מה שהגן עליו אתמול, כבר לא יגן עליו מחר.

"בעיה נוספת היא אי הבנה או היעדר משמעת מצד העובדים, שלא מודעים לבעיית אבטחת המידע. מתקפות רבות החלו לאחר שעובד לא פעל לפי הנוהל, ואיפשר לגורמים עוינים לחדור לארגון. ומעבר לכל אלה, ארגונים, במיוחד גדולים, משתמשים במערכות מידע רבות, ובמערכות הגנה - שכולן צריכות לדבר עם כולן. לפעמים, יש חורים בין המערכות הללו, וההאקרים יודעים למצוא אותם כדי לחדור למערכת".

הקורונה האיצה את המעבר לעבודה מהבית והחריפה גם את בעיית האבטחה. מה הגישה שלכם לפתרון הבעיה?

"עוד לפני הקורונה זיהינו שהעולם משתנה, וגם אחרי המגפה, הוא לא יחזור להיות כשהיה. הגבולות נפרצים. פעם אנשים קמו בבוקר, נסעו לעבודה, התחברו לקיר והתחילו לעבוד. כיום הם עובדים מכל מקום - משדות תעופה, מבתי קפה, ממקומות מרוחקים. הפתרונות הנוכחיים לאבטחת גישה מרחוק לא נותנים מענה לאיומי הסייבר הרבים שקיימים כיום. ההאקרים הבינו איפה מרוחה החמאה, ואכן רוב המתקפות הן על התחברות מרחוק.

"יש חברות שמציעות לארגונים להחליף את כל מערך ה-VPN בפתרון מעודכן ומאובטח יותר, וגם לנו יש מוצר כזה. אבל אנחנו מבינים שזה לא פשוט, בוודאי לא בארגון גדול שמשתמש במערכת מסוימת כבר 20 שנה וכל האפליקציות שלו רצות עליה. לכן, הפתרון שלנו הוא אחר: לא צריך להחליף כלום. תשתית ה-VPN הקיימת נשארת על כנה, ואנחנו מאבטחים אותה באמצעות עיקרון פשוט: הפרדה בין המקום שבו העובד מזדהה (Authentication) לבין הגישה לארגון עצמו (Access) ומאפשרים לזהות ולאשר את המשתמש באמצעות מה שאנחנו מכנים "Multi-factor Continuous Authentication" - כלומר, אם כיום המשתמש מזדהה פעם אחת בלבד בעת חיבור לארגון באמצעות סיסמא חד פעמית (OTP) אשר נשלחת אליו לטלפון הנייד ולאחר מכן מותר לו להתחבר באופן חופשי לאן שמוגדר לו מראש בתוך המרחב הארגוני, באמצעות הטכנולוגיה ™ZONEZERO של סייפ-טי, המשתמש ידרש לאשר הזדהות חזקה (MFA) מתוך הטלפון הנייד שלו או באמצעות התקן ביומטרי בכל פעם מחדש כאשר הוא ינסה להתחבר לשירות כלשהו בתוך הארגון.

דוגמה מהמערכת של סייפ-טי

"אם נחזור לעולם הפיזי - נאמר שמישהו צריך להגיע למתקן ביטחוני רגיש מאוד. אני לא אתן לו את הכתובת מיד, אלא אשלח אותו למקום אחר, ורק אחרי שאזהה אותו בוודאות, אתן לו הסבר כיצד להגיע - אבל אך ורק לחדר שבו הוא צריך להיות, ולא למתקן כולו. במקרה שלנו, הגישה תהיה רק לאפליקציה הספציפית שהעובד צריך להשתמש בה, במקום לתת לו מפתחות למערכת כולה, כולל אזורים עם מידע מסווג או רגיש.

"יש לנו גם פתרון ייחודי שהוטמע כבר ביחידות מודיעין מובחרות, והייחוד שלו הוא שגם לאחר שהעובד נכנס פנימה, מבחינתנו עדיין קיים סיכון, ולכן אנחנו ממשיכים לוודא שמדובר באדם בעל הרשאות מתאימות - בכל פעם שהוא מנסה לגשת למידע רגיש. פתרון של הזדהות רב שלבית, מול אפליקציות ומול השירותים ומאגרי המידע הקיימים, מספק חלופה מלאה להתחברות מאובטחת מרחוק - גם על גבי VPN קיים. זה מאפשר לנו להמשיך למנוע איומים פנימיים לכל אורך הדרך, ולצמצם את כמות הפגיעות שנובעת מחולשתו של הגורם האנושי בארגון", מסכם דניאל.

לפרטים נוספים: www.safe-t.com

כשהמעלית תתחיל לדבר

התמונה באדיבות חברת Onvego

החזון של חברת Onvego הוא לבסס את התקשורת שלנו עם מכשירים ביתיים ותעשייתיים על דיבור טבעי ככל האפשר, ללא לחיצה על כפתורים או הקפדה על הגייה מסוימת באוצר מילים מצומצם. "בעולם התעשייה, זה פתרון שחוסך הרבה מאוד זמן וכסף", מסבירים המייסדים

ב-2015, אז נוסד הסטראטאפ הישראלי Onvego, החזון של הבאת יכולות דיבור למכשירים עם מעט כוח מיחשוב וללא חיבור לאינטרנט היה נראה מאתגר. "שמנו לנו למטרה להביא יכולות דיבור לעולמות של מכונות, אפליקציות וטלפונים", מתאר רועי גוריון, מנכ"ל החברה ואחד משלושת המייסדים. "רצינו שאפשר יהיה לשוחח עם מכשירים כמו שמדברים עם חבר, בלי להשתמש רק באוצר מילים מוגבל, או להקפיד על היגוי מסוים. למשל, נאמר למכונת הקפה 'אני רוצה אמריקנו בלי סוכר ועם מעט חלב' והיא תבין מיד למה התכוונו.

"בזמנו, לא כולם הבינו שזה אכן עומד לקרות. אבל עם כניסת העוזרות הקוליות של אמזון, גוגל ואפל לשוק ה-B2C, ואימוץ הטכנולוגיה על ידי המשתמשים הביתיים, כיום כולם מבינים שזה הכיוון אליו השוק צועד". על פי חברת המחקר גרטנר, בתוך שנתיים בלבד, יותר מ-60% מהאינטראקציות שלנו עם מכשירים יהיו מבוססות דיבור. "גם אם זו תחזית אופטימית מדי, מדובר בשוק בהיקף אדיר", אומר גוריון.

הייחוד של הפתרון שפיתחה Onvego הוא ביכולת העבודה באופליין (על המכשיר עצמו) ובגמישות הרבה של הפלטפורמה, המבוססת על יכולות AI. "פרט לכך שאפשר להפעיל את המערכות בין אם יש חיבור לאינטרנט או אין, הרעיון המרכזי הוא שניתן לתקשר עם המכונה בשפה חופשית, או לפי פקודות מוגדרות מראש - הכל כתלות בעולם בו פועלים, והיא תגיב בהתאם", מסביר גוריון.

"במקרה של מעלית למשל, שיתוף פעולה שלנו עם חברת שינדלר, די באוצר מילים מוגבל מאוד. היא צריכה להבין פקודות כמו 'קומה 5' או 'למחלקה האונקולוגית'. היא לא צריכה להכיר את כל המילון. לעומת זאת, מערכת שעוסקת בהזמנה לאירועים צריכה להחזיק באוצר מילים גדול יותר ולדעת לפעול בקונטקסט רחב, מה שמתקרב לשפה חופשית". עבור כל לקוח, Onvego מתאימה את הפתרון לצרכים הייחודיים שלו. "אנחנו בונים את העולם שאיתו המשתמשים הולכים לעבוד, ומגיעים לרמות דיוק גבוהות מאוד", מסביר גוריון.

"אנחנו מלמדים את המערכת לפעול גם באופליין, כשאין חיבור לרשת וגם באונליין. אם את נוסעת ברכב בכביש הערבה, ואומרת 'פתח חלון אחורי' - זה יתבצע גם אם אין חיבור רשת באותו רגע. אם את שואלת איזו מסעדה איטלקית יש בסביבה וצריך חיבור לאינטרנט, המערכת תתחבר לרשת ותחזיר את המידע הרצוי".

להגיע במהירות ל-ROI

"החוזקה שאנחנו מביאים היא היכולת לזהות ברמת דיוק גבוהה מאוד את כוונת המשתמש, ולהפוך את המענה לפונקציונלי ביותר", אומר גוריון. "קחי לדוגמה מכשיר רפואי. הידיים של הרופא תפוסות בביצוע פעולה כלשהי, ובמקום לתפעל את המכשיר באמצעות מסך מגע, כל מה שהוא צריך זה לדבר אל המכשיר והבקשה שלו תתבצע.

"דוגמה נוספת היא המערכת שבנינו עבור כביש 6 צפון, שעוסקת בסליקה. לכל לקוח שמתקשר לשלם חשבון על נסיעה בכביש עונה המערכת שלנו, והיא יכולה לקחת פרטי אשראי, מספר רכב וכו', עד להשלמת תהליך התשלום - ללא מעורבות של נציג אנושי, אלא אם הלקוח מעוניין בכך". ואכן, בהאזנה לשיחה שהגיעה למוקד, ניכר כי המערכת מתורגלת בהתמודדות עם מצבים שונים. גם כאשר הלקוחה החלה להקריא מספר כרטיס אשראי, התבלבלה באמצע וביקשה להתחיל מחדש - המערכת הבינה את כוונתה, והתשלום בוצע בהצלחה.

כיום, מתמקדת Onvego בעולמות התעשייה. "במקומות הללו, אפשר להגיע למצב שבו השימוש בקול הוא אפקטיבי מאוד ומקצר תהליכים באופן ניכר, מה שמאפשר להגיע ל-ROI במהירות", מסביר גוריון. "ניקח לדוגמה עובד בסופרמרקט שעובר ידנית על כל המוצרים ומעדכן להם את המחיר, באמצעות מסופון. אם נאפשר לו לעשות את זה באמצעות דיבור - כלומר, לסרוק את קוד המוצר ולומר את המחיר בקול, במקום להקיש אותו - העבודה תתייעל במידה ניכרת".

אף אחד כבר לא רוצה ללחוץ על הכפתור

את החברה הקים גוריון יחד עם אלון בוכניק ומארק חפץ, כולם בעלי עבר עשיר בתעשיית ההייטק. "שלושתנו כבר לא ילדים", הוא צוחק. "עבור מארק זה הסטארטאפ הרביעי. Onvego הוקמה אחרי שמארק ואלון יזמו חברה בשם וויסי, שפיתחה פתרונות בדיבור לעיוורים. הם קיבלו תגובות חיוביות מאוד, והרבה אנשים שאלו אותם למה בעצם הפתרונות הם לעיוורים בלבד. הם הגיעו לתובנה שיש כאן שוק גדול הרבה יותר, שפונה ל-B2B, וכך נוסדה Onvego".

בתקופה הנוכחית, הצורך במוצר של החברה גדול מתמיד. "הקורונה העלתה את המודעות לזיהומים שיש על משטחים במקומות ציבוריים", מסביר גוריון. "עכשיו, כולם מעדיפים להפעיל את המעלית בדיבור או לדבר למכונות השתייה ולהגיד 'אני רוצה בקבוק קולה חצי ליטר', במקום ללחוץ פיזית על הכפתורים. דיבור הוא גם פתרון מצוין לכל מי שמסתבך עם ממשק ההפעלה של המכונות השונות".

רועי גוריון, מנכ"ל Onvego: "אנחנו מלמדים את המערכת לפעול גם באופליין, כשאין חיבור לרשת וגם באונליין. אם את נוסעת ברכב בכביש הערבה, ואומרת 'פתח חלון אחורי' - זה יתבצע גם אם אין חיבור רשת באותו רגע. אם את שואלת איזו מסעדה איטלקית יש בסביבה וצריך חיבור לאינטרנט, המערכת תתחבר לרשת ותחזיר את המידע הרצוי"

Onvego שוכנת כיום ביקנעם. בתחילה פעלה החברה במימון עצמי (בוטסטראפ) ובהמשך השקיעה בה Terra Venture partners שבבעלותם חממת טרהאב ביוקנעם העוסקת בהשקעות אימפקט. כמו כן החברה מקבלת תמיכה מרשות החדשנות במסלול מימד.

"יש לנו לקוחות אזרחיים וביטחוניים, במגוון שפות", אומר גוריון. "בין אם מדובר בארגון ביטחוני או בחברה תעשייתית, אנחנו לומדים את הצרכים הספציפיים ועולם התוכן שלהם, כדי להתאים להם את הפתרון המושלם".

לפרטים נוספים:
www.onvego.com ● info@onvego.com

להגן על רכוש וחיי אדם - בטכנולוגיה המתקדמת ביותר

תחום גילוי וכיבוי האש קפא על שמריו שנים רבות, בין היתר לאור ההשקעה הגבוהה שדורשת התקינה המודרנית. קבוצת מתאל הישראלית הצליחה להביא לענף טכנולוגיות פורצות דרך, המאפשרות שליטה מלאה באירועי בטיחות אש, החל מסניפי בנקים ועד קומפלקסים מורכבים של מאות אלפי מטרים

בימינו, רוב החברות והארגונים כבר מכירים את נושא אבטחת המידע, ודואגים להגן על מערכות המחשוב של החברה מפני סכנות כגון מתקפות האקרים, פישינג, כופר, וירוסים וכן הלאה. עם זאת, חשוב לזכור גם את הבטיחות הפיזית ובמיוחד את הצורך בהגנה מנזקי אש, בדגש על משרדים המצויים במגדלים רבי קומות. קבוצת מתאל שייסד חיים קפלן, מורכבת מחברת מ.ת.א.ל שהוקמה ב-1996 ועוסקת באינטגרציית מערכות בטיחות האש, וחברת MTECH (R&D) שהוקמה ב-2011 ומתמקדת בפיתוח מערכות גילוי אש משולבות כריזה, בקרה ושליטה לשווקים הבינלאומיים (תקנים אמריקאים UL ו-NFPA).

בשנים האחרונות, עם העלייה המשמעותית בתקינה הבינלאומית בנושאי בטיחות וכיבוי אש, נמצאת הקבוצה בתהליך התפתחות מואץ בישראל וגם בחו"ל, כשהיא פונה בעיקר לשווקים הפועלים על פי תקני בטיחות אמריקאים, ובהם ארה"ב, הודו, גיאורגיה, אוזבקיסטן והשוק הרוסי.

"מערכות גילוי האש שנפוצות כיום הן לרוב מיושנות מאוד", מסביר קפלן, שהוא גם מנכ"ל הקבוצה. "מדובר במערכות שיש להן כמה תפקידים: הן מגלות שריפות בבניינים, ואז מתחילות בתהליך ניהול אינטגרטיבי שמפעיל את כל מערכות הבטיחות בבניין בכדי לאפשר פינוי אנשים באופן בטוח, על ידי יצירת מסדרונות בטוחים מאש ועשן, הפניית האנשים בהתראות ויזואליות וקוליות, הפעלת מערכות פינוי עשן ייעודיות, שליטה בדלתות ממודרות ושלל מערכות החירום.

"עלייה במספרם של גורדי השחקים וקומפלקסים יצרה גידול אקספוננציאלי בכמות אביזרי הגילוי, אשר הפכו את המערכות למורכבות הרבה יותר לתפעול, לבקרה ולשליטה. בנוסף, זמני התגובה של המערכות התארכו ויצרו סכנה לחיי אדם", מסביר קפלן.

בקבוצת מתאל רותמים את החידושים הטכנולוגיים המתקדמים ביותר בתחום, ביניהם תקשורת נתונים, חומרה וחויית משתמש, לטובת שיפור בטיחות האש. "הטכנולוגיה שאנו משלבים במערכות מאפשרת עיבוד וניהול מספר תרחישים בלתי מוגבלים ובהתאמה לתקנים המחמירים ביותר בעולם", אומר קפלן. "פיתחנו פלטפורמת תוכנה לניהול כל המערך, שמאפשרת לצוותי החרום בכל רגע נתון לראות ON-LINE את הסטטוס של כל מערכות החירום בבניין, ואף מספקת אפשרויות בקרה על מערכות נוספות.

חיים קפלן (ראשון משמאל) עם נציגי משרד הכבאות של אוזבקיסטן במשרד הכבאות הארצי של ישראל

"פלטפורמה זו מאפשרת לצוותי החרום והצוותים הניהוליים בבניינים לשלוט באופן מלא בכל מערכות הבטיחות, כגון מערכות ניהול עשן ומערכות ניהול סיכונים, ומספקת אפשרויות 'טייס אוטומטי'. כוחות הצלה וביטחון שמגיעים לטפל באירוע, מקבלים ממשק מידע מלא בזמן אמת על היקף האירוע והאופי שלו, דרכי הפעולה האפשריות וכן שליטה מלאה על כל מערכות הבניין.

"התוכנה היא פיתוח יחודי שלנו. המספקת לכוחות ההצלה את כל המידע הנדרש בהתאם לתיעדוף המידע הרלוונטי. לאחר נסיון רב שנים ובשילוב עם כוחות ההצלה, פיתחנו ארונות שליטה ובקרה FSCS מאושרים תקן UL864 10th edition UUKL שבהם הנגשנו את כל מערכות החירום בבניין. בנוסף, המערכת מתממשקת באופן מלא לטאבלטים ייעודים לכוחות ההצלה והכבאות. כמו כן, הקבוצה מפתחת מוצרים בהסכמי שיתוף פעולה בלעדיים עם קונצרן EATON וקונצרן HALMA - APOLLO".

ביקוש גדול באיחוד האמירויות

הניסיון הרב והמוניטין שזכתה בהם קבוצת מתאל, פתחו בפניה שווקים בינלאומיים נרחבים, והיא לקחה חלק משמעותי בלא מעט פרויקטים בקנה מידה עולמי. "כך למשל, במונדיאל 2018 התקנו מערכות בשני אצטדיוני כדורגל ברוסיה (מעל 14,000 גלאים ויחידות קצה). ביצענו התקנות במלון מריוט Paragraph בבאטומי; החודש נמסר מלון מריוט בטשקנט אוזבקיסטאן; וחתמנו הסכם עם מרכז הבנקאות העולמית בטשקנט, המתפרס על פני 269,000 מ"ר. בכל המקומות הללו, יהיו מערכות מתוצרת ישראל", מתגאה קפלן.

לאחר החתימה על "הסכמי אברהם" בבית הלבן, הצפויים להביא לנורמליזציה של היחסים בין ישראל לאיחוד האמירויות, בחריין ומדינות נוספות, מאגר הלקוחות הפוטנציאליים של מתאל גדל באופן משמעותי. "איחוד האמירויות הרי ידועה בשלל גורדי השחקים המרשימים שלה, ואנחנו כבר מנהלים מגעים אינטנסיביים עם גורמים משמעותיים בדובאי. המטרה שלנו היא שעד סוף 2021, תהיה לנו נציגות באמירויות, ואנחנו נמצאים במגעים גם עם גורמים מערב הסעודית", מגלה קפלן.

הובלת הטכנולוגיה העתידית של כיבוי האש

חברת מתאל מעסיקה, נכון להיום, כ-60 עובדים ויש לה סניפים קיימים ובהקמה בארה"ב, רוסיה, אוזבקיסטן, הודו וגאורגיה.

בישראל, החברה מבצעת פרויקטים רבים, ביניהם מיגון אש בכלא 10 ובקריה המשפטית החדשה של צה"ל; קמפוס ארגמן ברמת גן; מגדלי אקרו נדל"ן בתל אביב ורבי קומות וגורדי שחקים נוספים.

מערכת גילוי אש היברידית כחול לבן

מוצרי גילוי האש והבקרה אושרו לתקן UL864 10th EDITION וכמובן לתקן הישראלי. "העובדה שהמוצרים שלנו בעלי תקינה UL האמריקאית, הופכת אותנו לאחת החברות המובילות בעולם מבחינת טכנולוגית ומהמובילות בתחום הגילוי, הכיבוי והשליטה בניהול העשן באתרים", מסביר קפלן.

"בישראל אנחנו כבר די דומיננטיים בנישות מסוימות, ורואים את עצמנו כקבוצה מוטת ייצוא בכל הקשור לטכנולוגיה המתקדמת שלנו. המערכות שלנו מאפשרות גמישות מלאה בבניית ארכיטקטורת מגוונות, מה שמאפשר תוספות, שינויים והרחבות, ללא צורך בשינוי התמהיל המרכזי", מוסיף קפלן. "כך למשל, ניתן לשלוט במספר מוקדים מנקודה אחת, ואף לאפשר עדיפות למוקד ספציפי. למעשה, אנו מסוגלים לשלוט על ערים שלמות במתכונת של 'סייף סיטי'. תוכנת המוקד שלנו מאפשרת הקמת מוקד שליטה ובקרה מקומי, עירוני ואף ארצי, כך שלקוחות בעלי סניפים בכל העולם יכולים לשלוט בכל המערכות ממוקד מקומי שלהם", מסכם קפלן.

מעל 14,000 גלאים ויח' קצה הותקנו באיצטדיון כדורגל ברוסיה | התמונות באדיבות חברת מתאל

לפרטים נוספים:
www.mtech-fire.com ● www.matael.co.il

טכנולוגיית הלייזר לטיפול בגלאוקומה עולה כיתה

הפיתוח החדש של לומניס, מהמובילות העולמיות בתחום רפואת העיניים, יוצר תיעוד ויזואלי ומחבר בין מכשיר הטיפול בלייזר המיועד לחולי גלאוקומה, לבין מערכות המחשוב של המרפאה. כך מתאפשרת הנגשה מלאה של המידע עבור המטופלים, הרופאים ובני המשפחה, לצד ייעול אופרטיבי של המרפאה

לומניס היא אחת החברות הישראליות המוכרות ביותר בעולם. עם מאות עובדים המועסקים במטה החברה ביקנעם, החברה מפתחת ומייצרת מוצרים המבוססים על טכנולוגיית לייזר וגלי רדיו, הנמכרים ברחבי העולם ומיועדים לשימושים רפואיים, פרא-רפואיים וקוסמטיים. לפני כשנה, נרכשה החברה בידי קרן השקעות אסייתית גדולה תמורת למעלה ממיליארד דולר.

פעילות החברה נחלקת בין שלוש חטיבות - חטיבה כירורגית, עם מוצרים לטיפול באבנים בכליות, בעיות ערמונית ועוד; חטיבה אסתטית, עם מוצרים לטיפול בצלקות, קמטים, הסרת שיער וכדומה; וחטיבה אופטלמית, הכוללת מוצרים מובילים לטיפול במחלות עיניים כגון גלאוקומה, מחלות רשתית ועין יבשה.

כבר לפני 20 שנה, היתה לומניס חלוצה בתחום רפואת העיניים העולמי, כשהציגה את טכנולוגיית ה-SLT לטיפול בגלאוקומה. "גלאוקומה היא מחלת עיניים נפוצה מאוד, שמתחילה לרוב בגילאי ה-40, ושכיחותה עולה עם הגיל", מסביר איתי מאייר, מנהל החטיבה האופטלמית בלומניס. "בקרב בני 70, יש כבר כ-10% הסובלים מהמחלה, שהיא הגורם מס' 2 בעולם לעיוורון.

"הגלאוקומה יוצרת מצב של לחץ תוך עיני, כאשר הנוזל בתוך העין לא מתנקז באופן אפקטיבי וגורם ללחץ על עצב הראייה, מה שהורס אותו לאט לאט. מאחר שעצב הראייה הוא זה שמעביר מידע מהעין למוח, כשהוא נהרס - שדה הראייה מתכווץ והולך, עד למצב של עיוורון". האתגר הגדול שמציבה הגלאוקומה בפני הרפואה הוא ההתקדמות האיטית שלה, באופן כמעט בלתי מורגש. "הגלאוקומה מכונה 'הגנב השקט של הראייה', מאחר שהיא א-סימפטומטית. אצל מי שסובל ממנה, שדה הראייה מצטמצם לאט לאט, וכשהוא כבר מבין שיש בעיה והולך להיבדק, אפשר אולי לשמר את המצב הקיים באמצעות טיפול, אבל לא לתקן את הנזק שכבר נגרם ולהחזיר את מלוא שדה הראייה".

טכנולוגית ה-SLT (Selective Laser Trabeculoplasty) שהשיקה לומניס לפני שני עשורים מיועדת לטיפול כבר מהשלב הראשוני של גלאוקומה, ומורידה את הלחץ התוך-עיני באמצעות לייזר הנורה לשכבת הניקוז בעין, המפעיל תגובה ביולוגית שמשפרת את תהליך הניקוז - בדומה לפתיחת סתימה בצינורות מים.

"באמצעות לייזר, אפשר לפתוח את ה'סתימה' הזו בקלות ובמהירות, בתוך דקות ספורות, ללא כאבים כלל", מסביר מאייר. השקת ה-SLT אפשרה ללומניס להמשיך לבסס את מעמדה כשחקנית דומיננטית ומובילת שוק בתחום רפואת העיניים העולמי, וזה 20 שנה היא מרחיבה את פורטפוליו המוצרים העושים שימוש בטכנולוגיה זו.

מגזין Lancet היוקרתי אף הכתיר לאחרונה את ה-SLT כטיפול קו ראשון המומלץ לגלאוקומה על פני טיפות, לאחר מחקר בהשתתפות מאות חולים שמצא שהטיפול אפקטיבי באותה מידה כמו טיפות, ובטווח הארוך גם מצמצם את הצורך בניתוח ומוביל לחסכונות ענק למערכות הבריאות ולמטופלים.

"הזדמנות לשפר באופן משמעותי את הקשר עם המטופל"

בימים אלה, משיקה החברה פיתוח נוסף, המעביר את הטכנולוגיה שיצרה מהעולם האנלוגי אל הדיגיטלי, כפי שמגדיר זאת מאייר. "עד היום, מכשיר הלייזר עמד בפני עצמו במרפאה. ניתן היה לבצע בו את הפעולה הרפואית, אך לא יותר מכך. הוא לא יכול היה להתחבר למחשבים של המרפאה או למחשבים של רופאים אחרים, ובזמן שרופא או רופאה ביצעו את הטיפול, נדרשה נוכחותו של איש צוות נוסף כדי לתעד את הפעולות והממצאים.

"המוצר החדש שפיתחנו, 'דיגיטל דואט', מחבר בין כל הקצוות. הוא מאפשר צילום של סרטים ותמונות לפני, במהלך ואחרי הטיפול וכמו כן מתממשק למערכת המידע במרפאה, ומעביר אליה את כל הפרמטרים, התמונות וסיכום של הטיפול שבוצע".

צוות הפיתוח של הדיגיטל דואט עם המכונה | צילום: אילן מור

מכונת הדיגיטל דואט: מאפשרת צילום של סרטים ותמונות לפני, במהלך ואחרי הטיפול | צילום: אילן מור

לדברי מאייר, לא מדובר בשדרוג טכני בלבד. "יש לנו כאן הזדמנות לשפר באופן משמעותי את הקשר עם הפציינט, גם עם בני המשפחה שלו, עם רופאים אחרים ועם כלל המערכת הרפואית. אנחנו יכולים להראות לפציינט בדיוק מה היה מצב העיניים שלו בטיפול ואחריו, במקום לתאר לו במילים; לשלוח לרופא המשפחה את המידע באופן אוטומטי; וכמו כן ללמד סטודנטים איך מתבצע התהליך באמצעות סרטים שמראים את הפעולה בזמן אמת.

היכולות הדיגיטליות מנגישות את הטיפול לפציינט מצד אחד, ומצד שני מאפשרות למרפאות את היעילות הנדרשת לתמיכה בביצוע נרחב של טיפולי SLT ביעילות ובמהירות, תוך שיפור איכות הטיפול והשגת חיסכון אדיר למערכת הבריאות.

"העובדה שהכל מתועד ושמור, גם בצורה ויזואלית, מאפשרת לרופא המשפחה, למשל, לראות במהירות אילו טיפולים בוצעו. העולם שלנו כיום ויזואלי מאוד, וגם הרופאים כבר מעדיפים לחלוק מידע באמצעות תמונות וסרטים, ולא רק באמצעות תיאורי מקרה".

בעתיד, מתוכננת המערכת להציע אפשרויות נוספות, כגון שליחת המידע לענן, ליצירת דאטה בייס שיכלול מיליוני טיפולים, ויאפשר לבצע אופטימיזציה של הטיפול על פי נתוניו של המטופל.

תהליך הפיתוח של המערכת הושלם לאחר פרוץ מגפת הקורונה, ולדברי מאייר, הצוות עמד בפני אתגרים לא פשוטים. "ביצענו ניסויים גם בישראל וגם בניו יורק, והכל בפיקוח של מומחי גלאוקומה מהמובילים בעולם. לאחר שפרצה המגפה והוטלו סגרים בישראל ובארה"ב, לא יכולנו להגיע אל הרופא שעובד בניו יורק - עניין קריטי כשמדובר בפיתוח מערכת חומרה המשלבת תוכנה. עם זאת, בהרבה מאמץ, הצלחנו לעמוד בלוח הזמנים". הקורונה, אומר מאייר, הדגישה את היתרונות הטמונים במערכת. "בזמן מגפה, המטרה היא לקצר את השהות של המטופל במרפאה ככל האפשר", הוא מסביר. "באמצעות המערכת, הוא נכנס, עובר את הטיפול ויוצא תוך 10 דקות לכל היותר, בלי הצורך להמתין עד שכל הנתונים והממצאים יוקלדו ידנית לתוך המחשב במרפאה. לפי המשוב שקיבלנו ממרפאות בארה"ב, זה משפר מאוד את היעילות התפעולית במרפאה".

לפרטים נוספים: www.lumenis.com

IMNA פיתחה פלטפורמה דיגיטלית לניסויים קליניים המאפשרת ליווי אישי ומדויק של הנסיין

פלטפורמת TrialME מאפשרת לחברות פארמה ומרכזי מחקר לוודא המשכיות של הניסויים הקליניים גם בזמן מגיפת COVID-19 תוך מעבר חלק למבנה היברידי העוקב אחר ההנחיות החדשות של ה-FDA במהלך המגיפה, ומאפשרת ליווי אישי ותקשורת עם הנסיינים בכל מקום וזמן

במהלך התפרצות COVID-19 מסייעת IMNA Solutions לחברות פארמה ולצוותי מחקר להעביר ולנהל את הניסויים אשר עד כה נוהלו במרכזי המחקר לפורמט היברידי דיגיטלי, מה שמאפשר את המשך הניסויים תוך התמודדות עם האתגרים התפעוליים אשר צפים ועולים בעולם האמיתי. IMNA Solutions פיתחה פלטפורמה טכנולוגית חדשה שנועדה לאסוף מרחוק נתונים, לפתח מודלים סטטיסטיים חדשים ולאפשר התייעלות כלכלית טובה יותר של הניסוי הקליני.

כבר דובר רבות על חשיבות הצבת המשתתף במרכז חוויית הניסוי הקליני, אבל בפועל נראה כי חברות פארמה ומרכזי מחקר עדיין מתקשים ליישם גישה זו. הסיבה המרכזית לכך היא תקשורת לקויה עם הנסיינים והיעדר יכולת ללוותם באופן צמוד ולהבין באופן רציף את מה שעובר על המשתתף במהלך הניסוי. למרות שישנם מספר גורמים המעורבים בתהליך הניסוי הקליני, אף גורם אינו אחראי באופן בלעדי על ניטור חוויית הנסיין (המשתתף).

לדברי ישראל חייקין, מייסד ומנכ"ל IMNA Solutions, אי הצבת המשתתף במרכז מעלה את שיעורי הנשירה מהניסויים הקליניים. השילוב של מידע רפואי שנאסף מהמשתתפים, עם שאלונים מתוקפים המדווחים ישירות על ידם, וכן טכנולוגיית תקשורת מרובת ערוצים המותאמת לדרישות HIPAA, מסייע לשיפור תוצאות המחקרים הקליניים ולהצלחתם.

המחיר הגבוה של נטישת הנסיינים

השלכות שיעורי הנשירה הגבוהים בקרב המשתתפים הן משמעותיות מאוד. לפי נתוני ה-FDA ל-2018, בעיית נשירת המשתתפים מהניסוי, כמו גם חוסר היכולת לקבל נתונים מדויקים מהם, הינם הגורם המרכזי לאי מעורבות המשתתפים בניסוי, דבר המוביל, בין היתר, לכישלון המחקר ולעלויות גבוהות אותן נוכל לחסוך אם נבין טוב יותר את התהליך שעובר המשתתף וננגיש לו פתרונות ומענה המתאימים לו באופן פרסונלי.

על פי חברת המחקר FORTE, חלק מהסיבות המרכזיות לכך שמשתתפים נושרים מהניסוי הן חוסר הפנמה מצד צוותי המחקר למורכבותו של התהליך אותו הם חווים, קשיים בהנגשת פרוטוקול הניסוי ודרישותיו, וקושי של הנסיינים לתקשר עם מתאמי המחקר. כל אלה תורמים לשיעור נטישה של 30%. על פי מחקר אחר, העלות החציונית לחולה עומדת כעת על 41,117$. ככל שהעלות למשתתף ממשיכה לעלות, מציאת דרכים לשימורו במחקר ולטיוב פעילותו בו, הופכת קריטית. על רקע זה, צוותי המחקר מבינים את הצורך הגובר במעורבות המטופלים בניסויים קליניים.

"באמצעות שימת דגש רב על העמדת המשתתף במרכז, מחקרים קליניים ייהנו משיעור השתתפות גבוה יותר", אומרת מירב נאור-וינשטוק, שותפה מייסדת וסמנכ"לית מוצר ואסטרטגיה בחברת IMNA Solutions. "כשהמחקרים אינם מצליחים לענות על צרכי המשתתפים, לא רק שהם מסתכנים באי אישור תוצר הניסוי הקליני על ידי ה-FDA, אלא גם מסכנים את בטיחות המשתתפים. מנהלי המחקרים הקליניים נדרשים להיות מודעים היטב לתהליכים שעוברים וחווים המשתתפים לאורך הניסוי כולו וזאת לצורך הנגשת התהליך והתאמתו למשתתפים, תוך שימת דגש על פרמטרים כגון מדד איכות חיים, תופעות לוואי, השפעות פסיכולוגיות ופיזיות, וכדומה".

עם זאת, בלב סוגיית הנשירה של המשתתפים עומדת חוסר הסינרגיה הקיימת בין הגורמים השונים במחקרים הקליניים. מעורבות המשתתפים בניסוי היא תהליך המצריך הבנה נרחבת של המשתתף וסביבתו, הפיכת השתתפותו במחקר לקלה, צמצום חסמים ושיפור הידע.

פלטפורמת TrialME מאפשרת לצוות הקליני לראות כיצד הנסיין מגיב לתרופה בזמן אמת, מה מצבו הנפשי ואם הוא סובל מתופעות לוואי | התמונות באדיבות חברת IMNA Solutions

כשהוצאות המו"פ עומדות על 2.7 מיליארד דולר לאישור תרופה, הצורך לשזור את מעורבות המשתתפים בתכנון המחקר הוא קריטי לפיתוח תרופות חדשות. לצורך זה דרוש פתרון בעל שני שלבים. הראשון - היכולת לקבל, לסווג ולנתח נתונים הנאספים מהמשתתפים ועל ידם, כגון שאלונים, מדדים, מדדים ממכשירי ניטור ועוד. השני - ניתוח הדאטה המתקבלת מהמשתתפים באמצעות תהליך למידת מכונה (BI & ML) והשוואתה לנתונים הנאספים במרכזי המחקר תוך שימוש בטכנולוגית תקשורת מאובטחת.

"חשוב להבין שלכל משתתף יש צרכים שונים, והגישה 'מידה אחת מתאימה לכולם' בדרך כלל אינה עובדת כשמדובר בניסויים קליניים", אומר חייקין. לדברי נאור-וינשטוק, "יצרנו ב-IMNA Solutions את לוח המחוונים האידיאלי להבנת המטופלים במהלך הניסוי, שיעזור לכל חוקר לשפר את המדדים הנוכחיים שלו. אנו יוצרים מצב שבו מרכזי מחקר מחוברים למאגר המשתתפים ומעורבים טוב יותר בתהליך הניסוי. לוח המחוונים הקל לשימוש שפיתחנו הוא הראשון מסוגו בשוק והוא מספק לחוקרים תובנה ייחודית על רצונותיהם וצרכיהם של משתתפי המחקר באמצעות טכנולוגיה מובילה בתעשייה".

מנגישים את תגובת הנסיין בזמן אמת

היכולת לעקוב באופן דיגיטלי אחר מצבם של נסיינים באמצעות לוח המחוונים מועילה ביותר למרכזי המחקר, שכן "הצוות הקליני יכול לראות כיצד הנסיין מגיב לתרופה בזמן אמת, מה מצבו הנפשי והאם הוא סובל מתופעות לוואי המשפיעות על יכולתו התפקודית. בהמשך לכך יכולים הצוותים להגיב ולהתערב בזמן אמת ולא בדיעבד. באמצעות לוח מחוונים מרכזי המנגיש את נתוני המטופלים בצורה מהירה ומרוכזת, אתרי המחקר אף מפחיתים מעומס העבודה שלהם", אומרת נאור וינשטוק.

כיום יכולים נסיינים המשתתפים בניסויים קליניים המנוהלים באמצעות פלטפורמת IMNA Solutions להשתמש באפליקציה ייעודית לניסוי. זו מאפשרת להם לעקוב אחר דרישות המחקר ואחר בריאותם האישית בזמן אמת, מה שמשפר את ההיצמדות לפרוטוקול הניסוי ומעלה את אחוזי ההצלחה. נותני חסות לניסויים קליניים, CRO ואתרי מחקר בכל מקום מכירים כעת ביתרונות של שילוב המשתתף בניסוי תוך חיבורו לאפליקציה ייעודית ומכשירים רפואיים דיגיטליים. פתרון זה, המוצע על ידי IMNA Solutions וממוקד בנסיין, מאפשר לחברות פארמה, מרכזי מחקר ו-CROs לערוך ניסויים ביתיים (וירטואליים) כדי לשפר את היענות המשתתפים והצלחת המחקר גם בתקופה מאתגרת כמו COVID-19.

לפרטים נוספים: www.imnasol.com

למה כולם רושמים פטנטים על המצאות תוכנה?

פטנטים מוסיפים ערך לכל חברה, ובמיוחד לחברות תוכנה שמתבססות בעיקר על קניין רוחני שיחסית קל להעתיק. לפניכם 3 עצות שיעזרו לכם לקבל פטנטים חזקים במהירות / גרשון פניטש, שותף בפניגן

אם מישהו יגיד לכם שאי אפשר לרשום פטנט על תוכנה, הוא טועה. למיקרוסופט יש מעל 40,000 פטנטים פעילים בארה"ב לבדה (ועוד אלפים בדרך). היא הוסיפה 3,144 פטנטים אמריקאיים חדשים ב-2019, 32% יותר מאשר ב-2018. בשנה שעברה, סיילספורס הגדילה את הפטנטים האמריקאיים שלה לעומת השנה שקדמה לה ב-64%; פייסבוק ב-78%; אורקל ב-20%; SAP ב-50%; אדובי ב-40%, בנק אמריקה ב-30%, עליבאבא ב-96%; אקסנצ'ר ב-36% וקפיטל וואן ב-232% (!). מגמות דומות ניתן לראות גם בחברות תוכנה ואינטרנט קטנות הרבה יותר. מדוע חברות ממהרות לרשום את המצאות התוכנה שלהן? יש לכך סיבות רבות, שכולן נובעות מהעובדה שפטנטים מוסיפים ערך. לפני 50 שנה, ערכה של חברה התבסס בעיקרו על נכסיה הפיזיים. היום, נכסים לא מוחשיים מהווים את חלק הארי מערך החברה. בחברות ממוקדות תוכנה, שבהן מתחרים יכולים להעתיק המצאות במהירות, הפטנטים חיוניים במיוחד כדי להגן על ערך החברה. למעשה, הפטנטים הם לעיתים קרובות הנכס המשמעותי ביותר שניתן להעברה, שחברות תוכנה ומסחר אלקטרוני מחזיקות ברשותן.

ניתן להשתמש בפטנטים באופן אסטרטגי בדרכים רבות. כשהמתחרים מתקרבים יותר מדי, ניתן להשתמש בפטנטים כדי לעצור אותם. כשיש צורך בתזרים כספי, אפשר להעניק רישיון בפטנטים כדי להוסיף הכנסות. כשחברה זקוקה לגישה לטכנולוגיה של מתחרה, ניתן להעניק רישיונות צולבים בפטנטים. בנוסף, תיק פטנטים חזק עוזר להגן על בעליו מתביעות מאחר שהמתחרים פוחדים מתביעת הפרה כתגובה.

בשל כל אלה, חברות תוכנה מבוססות משקיעות הרבה בפטנטים וחברות תוכנה צומחות הולכות בעקבותיהן. אפילו בחברות סטארט-אפ, ככל שרמת ההשקעה בחברה עולה, משקיעים מתוחכמים מתעקשים על תיק פטנטים איכותי שישמש למעשה כבטוחה כנגד השקעתם. פטנטים מעניקים למשקיעים לא רק בלעדיות בשווקים תחרותיים, אלא גם נכס שניתן להפיק ממנו רווח במקרה שהחברה תיכשל.

על חברות תוכנה לנקוט זהירות ולא לחכות יותר מדי כדי לרשום פטנטים. אם החברה תמתין עד שיתבעו אותה או לסבב ב' כדי להיות רצינית לגבי פטנטים, זה יהיה לרוב מאוחר מדי. כדי למצב את החברה כך שתמקסם את ערכה בשלבים מאוחרים יותר, יש להשיג פטנטים אסטרטגיים וחוסמים בשלבים המוקדמים יותר. לפניכם שלוש עצות שיגדילו את סיכויי החברה שלכם להשיג פטנטים חזקים במהירות:

פיליפ ליבקין, Getty Images

ראשית, אל תשאפו ליותר מדי. חברות רבות מנסחות פטנטים על תוכנה בצורה רחבה מדי כשהן משאירות לבוחן את הרושם שהן שואפות ליותר מהמגיע להן. כשזה קורה, בקשת הפטנט נלכדת בשרשרת אינסופית ויקרה של דחיות. מצד אחר, שאיפה למעט מדי עלולה להוביל לפטנטים חסרי ערך שהמתחרים יעקפו בקלות. כדי למצוא את האיזון הנכון כדאי להיעזר באסטרטג פטנטים שיודע מה סביר להניח שבוחן הפטנטים יקבל, ויכול לנסח את הפטנט בדרך שמכסה את מה שהמתחרים יזדקקו לו כדי להתחרות.

שנית, בחרו מילים בקפידה. לכל ניואנס בבקשת פטנט יש השפעה אדירה על השאלה אם הוא יתקבל, ובאיזו מהירות. לדוגמה, יש קבוצות בחינה במשרד הפטנטים וסימני המסחר האמריקאי שמעניקות פטנטים בפחות מ-40% מהמקרים, בעוד קבוצות אחרות מעניקות פטנטים בלמעלה מ-80% מהמקרים. כשבקשות הפטנטים מגיעות, פקידים מעבירים אותן לקבוצות בחינה בהתבסס על תיאורים מסוימים בבקשות. במילים אחרות, הדקויות בשפה יקבעו לעיתים לאיזו קבוצת בחינה תוקצה הבקשה. אם תוכלו לכוון את בקשת הפטנט לקבוצה הנכונה, תגדילו את הסיכויים לקבלתו. יש לוודא שאסטרטג הפטנטים בקיא ומנוסה בכך.

שלישית, השתמשו במסלול המהיר. כמעט כל הלקוחות שלי משתמשים כעת במסלול המהיר במשרד הפטנטים האמריקאי. בהתחלה זה עולה קצת יותר, אבל לטווח הרחוק זה חוסך כסף ולעיתים קרובות מוביל לקבלת פטנט תוך שנה או פחות. המסלול המהיר עובד ביעילות רק אם שתי הנקודות הראשונות מכוסות בהצלחה. כלומר, אם תשאפו ליותר מדי או לא תצליחו להסיט את הבקשה שלכם מקבוצת בחינה קשה, ייתכן שהמסלול המהיר לא יהיה יעיל.

לסיכום, פיראטיות תוכנה, הן כהעתקה ישירה והן כהעתקה רעיונית, נמצאת במגמת עלייה, ולכן פטנטים על תוכנה הופכים חשובים יותר ויותר לחברות סטארט-אפ ולחברות בוגרות כאחד. תוך שימוש בשיטות ובכלים הנכונים חברות יכולות להשיג פטנטים על תוכנה שיעלו את ערכן.

• • •

גרשון פניטש, שותף בפניגן

המחבר הוא שותף בחברת פניגן, אחת הפירמות הגדולות בעולם בתחום הקניין הרוחני ובעלת 10 משרדים ברחבי העולם. פניטש משמש כראש קבוצת תכנון קניין רוחני אסטרטגי וראש הסניף הישראלי של החברה, המייצגת מעל 160 מהחברות המובילות והמתוחכמות ביותר בישראל. פניטש, בעל ניסיון של מעל 30 שנה בחוקי פטנטים ומרצה אורח בבית הספר לעסקים של אוניברסיטת תל אביב שם, במשך שלוש השנים האחרונות, קיבל את פרס המרצה המצטיין עבור הקורס שלו במנהל עסקים על פיתוח ושימוש בפטנטים ככלים עסקיים אסטרטגיים. בנוסף להתדיינות בסכסוכים מורכבים הקשורים להפרות פטנטים בבתי המשפט המחוזיים בארצות הברית ובוועדה האמריקאית לסחר בינלאומי (ITC), פניטש מייעץ בקביעות לחברות כדי לעזור להן לפתח גישה ממוקדת עסקית לרישום פטנטים במטרה לשפר את הכנסותיהן.

ליצירת קשר:
gerson.panitch@finnegan.com

לצפיה בסרטון על פטנטים ותוכנה, סרקו את הברקוד

החלטות משקיעים בהייטק - ה"אמת" ומשמעויותיה ליזם

האם משקיעים מייחסים חשיבות רבה יותר למוצר או לצוות שמאחוריו, מדוע המצגת הראשונית היא החשובה ביותר - ומה הקריטריונים האמיתיים שלפיהם מתקבלות החלטות השקעה? / ערן פלומין

"היתה פגישה מוצלחת.. הם עומדים להשקיע בנו!" - כמה פעמים שמענו משפט דומה, ובכמה מהן נסגרה השקעה? רק 1% מהחברות שכלל נשקלו ו-3.6% מהחברות שקיימו פגישה עם VC יקבלו את ההשקעה המיוחלת בפועל (בתחומי ה-IT השיעור נמוך משמעותית לעומת תחום הבריאות). בנוסף, רק 10% מאלה שעברו לבחינה עם שותפי הקרן, 20% מאלה שעברו בדיקת נאותות וכ-60% מאלה שקיבלו Term Sheet - ייחתם עימם הסכם השקעה. לפיכך, עד שלא נחתם, יש להמשיך ולפעול לגיוס הון מול משקיעים נוספים, אך יזמים רבים נכשלו עקב אופטימיות יתרה בנושא.

יזמי הייטק רבים לוקים בתפישות מוטעות רבות נוספות לגבי משקיעים ואתגרי גיוס ההון. מאמר זה מדגים את מקצתן, משתי זוויות הסתכלות על המציאות: האחת, מחקר שניתח תשובות סקר בקרב 885 משקיעי הון סיכון, מרביתם שותפים בקרנות אמריקאיות ("כיצד משקיעי הון סיכון מקבלים החלטות השקעה?", גומפרס מאוני' הרווארד ואח'). השנייה, פרקטית לישראל, מבוססת על שיחות עם 150 משקיעים בחברות הייטק ישראליות בתחומי B2B בתעשייה ובבריאות; ניסיון במחקרי שוק ייעודיים ו-Equity Research לתמיכה בקבלת החלטות השקעה; וכן כמי שמאמץ בעצמו Best Practices לצורך השקעותי הנקודתיות בתחום. נקודת המוצא היא, כאמור, התפישות המוטעות של חברות רבות הפונות לסיוע בגיוס הון ובתכנון הצמיחה.

איך מגיעים למשקיע המתאים?

משקיעי הון הסיכון דיווחו כי כשליש מהשקעות שביצעו נבע מהרשת המקצועית שלהם. גם בישראל, מייחסים משקיעים חשיבות לטיפוח הקשר עם רשת יועצים, עו"ד ורו"ח, המסננים עבורם הזדמנויות איכותיות הנמצאות מתחת לרדאר. שיעור נמוך יותר מההשקעות נבע מפעולה יזומה של המשקיע עצמו או מהפנייה שקיבלו ממשקיעים אחרים (שמרו על יחסים טובים גם עם מי שדחה אתכם!).

מהי חשיבות המוצר/ השוק/ התעשייה לעומת צוות החברה?

כמחצית ממשקיעי הון הסיכון, במיוחד בשלבי השקעות מוקדמים ובתחומי IT, מתייחסים לצוות המייסדים/ ההנהלה כפרמטר החשוב ביותר לבחירת השקעה. לכאורה, יותר (בסדר חשיבות יורד) מהמוצר, המודל העסקי, השוק, התעשייה ומשווי החברה. "לכאורה", שכן הצוות נמדד גם על יכולתו לשכנע בתיאור הזדמנות ההשקעה במוצר/ השוק/ התעשייה. חברות רבות נפסלות אפילו טרם פגישה ראשונית, כאשר תוכנית הצמיחה לא שכנעה באמצעות מחקר וניתוח מעמיקים, לרבות קיומם של הצרכים הבלתי מסופקים בגינם מוכנים לקוחות פוטנציאליים לשלם מחיר רווחי על יתרונות הפתרון של החברה; או לגבי היקף פוטנציאל ההצלחה של יישומי הטכנולוגיה בוורטיקלים ובשווקים גדולים ומוכחים.

ערן פלומין | צילום: עופר לוי

משקיעים מייחסים חשיבות לצוות גם מתוך הבנה שהם יוצאים עימו למסע שבמהלכו יידרש שינוי המוצר/ שוק היעד/ PIVOT, ושעליו להוכיח יכולת להצליח גם בשינוי. אולם, תוכנית צמיחה איכותית הבוחנת את פוטנציאל ומגמות השוק, תעיד על צוות איכותי המקטין מלכתחילה את הסיכון שיידרש שינוי.

יזמים רבים מתקשים בתהליכי גיוס ההון, גם כי לא הפנימו את הפערים בהתאמת צוות המייסדים והנהלת החברה לכלל הדרישות להצלחתה. לפיכך, חשוב לשמוע בפתיחות דעות חיצוניות לגבי פערים אלה, אשר ניתן לצמצם גם באמצעות הגדלת משקלם של מומחים, יועצים וחברי Advisory Board פעילים המתאימים ל"פאזל" הנדרש להצלחת החברה בטווח הקרוב - באמצעות השלמת הבשלות העסקית, יכולת הניתוח והתכנון האסטרטגי, ההיכרות עם שוק היעד, או המומחיות הרב-תחומית הנדרשת לזיהויו.

מארק טווין אמר כי "סוסים חכמים יותר מבני אדם: עוד לא היה סוס שהימר על האדם הלא נכון". למשקיעים ותיקים ניסיון מצטבר בכל הקשור לפן האישיותי של הצוות, אולם מרביתם לא הגיעו לתחום ההשקעות בזכות כישרון מולד (המיוחס יותר לנשים, שחשיבותן בקרנות גוברת - כנראה גם מטעם זה) או הכשרה פורמלית בנושא. היזם יכול לשפר את ה"כימיה" שהוא מייצר עם משקיעים, במטרה להצליח בפרמטר חשוב זה.

כיצד העמקה לפני ה-Due Diligence ובמהלכו תגדיל את סיכויי ההצלחה?

אחד ההסברים לשיעור הגבוה של השקעות כושלות בהייטק קשור לתהליכי Due Diligence חסרים. המחקר העלה שמשקיעים מדברים במהלכו רק עם כ-10 בעלי דיעה הרלוונטיים לחברה. היות שההזדמנויות והסיכונים של סטארטאפים קשורים למגוון שווקי ומדינות מטרה, סוגי לקוחות, שותפים וכיו"ב, הרי שכל אחד ממרכיבים אלה מקבל תיקוף מועט, אם בכלל. ממילא, סטארטאפים רבים מסתפקים בפידבק ישיר מועט מהשוק לעומת הנדרש לתוכנית צמיחה מבוססת.

לפיכך, גם כשנסגרה ההשקעה, עדיין חסר לצדדים ביסוס לתוכנית הצמיחה הנכונה. כשמסתבר בהמשך כי הציפיות לא התממשו ו/או הערכת השווי היתה שגויה, נוצרים מתחים; וכשעולה הצורך ב-PIVOT כבר לא בטוח שהמשקיע יתמוך בו. לפיכך, ליכולת להגיע לתוכנית מוסכמת ומבוססת במקביל לסגירת הסכם ההשקעה יש ערך מוסף גבוה. המשימה מוטלת בראש ובראשונה על היזם: עליו להרשים מלכתחילה בהצגת תמונה מבוססת לכלל הסוגיות המרכזיות, ואזי ה- Due Diligence יתמקד בתיקוף ובהשלמת פערים ספציפיים בלבד.

אז איך באמת משפיעים על החלטת השקעה?

מסגרת ההחלטה נמצאת בגבולות המנדט שסוכמו עם המשקיעים בקרן, כפי שנרמז מהצהרת תזת ההשקעה ומפורטפוליו ההשקעות בפועל. בפועל, החלטות השקעה בהייטק הן מורכבות ורב-מימדיות: לגבי המשקל הנכון שיש לייחס לכל קריטריון השקעה, לגבי הציון ההולם לגבי כל פרמטר, ובמיוחד לגבי אי-הוודאות ביחס לעתיד. טבען של החלטות כאלו הוא שקשה להכניס אותן למודל, ויש להישען בפועל גם על ה'אינטואיציה' והניסיון של מקבלי ההחלטות. מציאות זו מאפשרת ליזם להגדיל את סיכויי הצלחת גיוס ההון: אם ירשים ויבלוט בהצגת הזדמנות ההשקעה ותוכנית הצמיחה המבוססת, ה'מאכילה בכפית' את התשובות והפתרונות לגבי כל הקריטריונים הרלונטיים לבחינה; אם ישפיע על אלמנט ה-FOMO כשהמשקיע מבין כי לפניו הזדמנות השקעה מעניינת; ועוד. לפיכך, ליזמים דרכים רבות לשפר ולהשלים את תהליך גיוס ההון המאתגר בהצלחה. למידע נוסף לגבי Best Practices וצ'קליסט לגיוס הון ולהשקעות מוצלחות: Linkedin.com/in/eranflumin.

הכותב הוא מנכ"ל "מהלכים אסטרטגיים - תכנון, מימון ויישום מהלכים אסטרטגיים לצמיחה" ובעל 20 שנות מומחיות בינלאומית בייעוץ ובמחקר לחברות ולמשקיעים בתחומי B2B בהייטק ובתעשייה.

שומרים על הנקודה הרגישה ביותר בארגון

כשרוב העובדים משתמשים בסמארטפון הפרטי כדי להיכנס למייל של העבודה, התוקפים מזהים נקודת חולשה ומנצלים אותה. חברת חזק נטוורקס הישראלית מציגה את הפתרון

גם בתקופה שבה אבטחת המידע נמצאת במודעות של כולנו, וכמעט כל ארגון דואג להצטייד במערכות מתאימות - ישנה עדיין נקודת תורפה בולטת ומשמעותית, שבמקרים רבים אינה מטופלת. אלה הם הסמארטפונים של העובדים - המכשירים הפרטיים, מבוססי מערכות ההפעלה אנדרואיד או iOS, שאיתם מגיעים העובדים לארגון, אך אינם מוגנים כלל מפני ציתות ומתקפות סייבר. רק לאחרונה אמר גיל שויד, מייסד ענקית האבטחה צ'קפוינט בראיון ל"שבעה ימים", כי "אנחנו רואים עלייה מטורפת בכמות ההתקפות על טלפונים ניידים. הטכנולוגיה נגד ההתקפות זמינה, אבל בחלק מהמקרים ארגונים פשוט לא משתמשים בה. זה קצת כמו להגיד: 'קניתי וולוו משוכללת אבל אני לא חוגר את חגורת הבטיחות'". בחברה הישראלית חזק נטוורקס (Assac Networks) זיהו פרצה זו - ופיתחו פתרון מתאים, שהותקן בשנה האחרונה בהצלחה במספר ארגונים בעולם. "כמעט 75% מנקודות הקצה שמחוברות לארגונים ברחבי העולם הן סמארטפונים, לדברי חברת המחקר גרטנר", אומר שמעון זיגדון, מנכ"ל חזק נטוורקס. "עובדים משתמשים בהם כדי להיכנס למערכות של הארגון, כמו מייל וקבצים, וגם לאפליקציות הפרטיות שלהם - ווטסאפ, אינסטגרם, פייסבוק ואחרות.

"כיום יש ניסיון לחצוץ בין היישומים הפרטיים לארגוניים באמצעות VPN. כך למעשה התקשורת מתבצעת משרת שאמור להיות בטוח יותר, מתוך הארגון. ואולם גם ל-VPN יש נקודת תורפה. ההאקרים הולכים קודם כל לסמארטפונים של העובדים, כיוון שעליהם אין אמצעי הגנה וקל יותר לפרוץ לתוכם. ברגע שהם מצליחים להגיע למייל הארגוני, למשל, הם יכולים להרחיב את המתקפה שלהם לכלל מערכות הארגון.

התמונה באדיבות חזק נטוורקס

"תוקף שמצליח להגיע לשרת המיילים, יכול למשל לשלוח לינק פישינג, להריץ תוכנה זדונית בתוך הארגון, ואף להתחזות לעובד מן המניין ולגנוב מידע, או לבצע מתקפת DoS", אומר זיגדון. "הוא יכול לגרום נזק רב מאוד, וכל זה כשמערכת האבטחה של הארגון מאמינה שהוא עובד רגיל ולכן מאפשרת לו גישה למקומות רגישים.

"הפתרון שלנו הוא תוכנה הזמינה הן למשתמשי אנדרואיד והן למשתמשי אפל, המשלבת בין שתי מערכות. אחת מהן, ShieldiT, מספקת הגנה מפני טאפינג והאקינג - מציתות לשיחות טלפון ומפריצה של האקרים לטלפון; מערכת ManageiT משלימה אותה, ומאפשרת לנהל את כל יחידות הקצה בארגון, לצפות בכל האיומים שהארגון חשוף אליהם, להיערך למתקפות אפשריות ולזהות נקודות חולשה. זאת, תוך השתלבות מלאה ברשת הארגונית, הן ברשתות הדיבור והן ברשתות ה-IT.

"גם אם ישנם עובדים שמתנגדים להתקנת אפליקציות להגנה על הסמארטפונים שלהם, חשוב לזכור שהפתרון שלנו מגן גם על הפרטיות של העובדים. כיום הרי ניתן 'לגנוב' למישהו את הווטסאפ, להתחזות אליו או לשאוב תמונות אינטימיות מהמכשיר הפרטי שלו, ולכן הגנה על נקודות הקצה שומרת גם על מידע חיוני ופרטי של העובדים", מסכם זיגדון.

לפרטים נוספים: www.assacnetworks.com

החברה הישראלית שהפכה לשם נרדף לבינה מלאכותית לרחפנים

מערכות רחפנים לזיהוי אדם וכלי רכב, טכנולוגיה המשתלבת ברכב אוטונומי - לכל אלה אחראית החברה הישראלית Thirdeye systems, שהתחילה את דרכה בגראז' עם שני שותפים ורעיון, והפכה לאחת החברות המובילות בתחום הבינה המלאכותית לרחפנים

דרך ארוכה עברה חברת Thirdeye מאז שהוקמה ב-2010, במרתף בבית הוריו של המנכ"ל, ליאור סגל, ועד היום - כשהיא מתכוננת להנפקה בימים אלה, כחברה המתמקדת באלגוריתמיקה של בינה מלאכותית למערכות רובוטיות, עבור מגוון יישומים.

"המוצר הראשון שפיתחנו אני ויואל מוטולה, שותפי להקמת החברה, סיפק פתרון לגילוי אדם עבור שימושים ביטחוניים, ועם הזמן נוספו מגוון מוצרים המספקים מענה לתחום האבטחה ותחומים נוספים", מספר ליאור סגל, מנכ"ל החברה. "בשנת 2015 גיל ברק הצטרף כשותף שלישי. ההתעוררות בעולם הרחפנים הפכה משמעותית בשנים האחרונות ולשמחתי פגשה אותנו בשלבי פיתוח מתקדמים, כך שצמחנו תוך מתן מענה לביקוש שגדל בשוק. בחזון החברה ראינו את יכולת המערכות שלנו להפוך כלים לאוטונומיים לחלוטין. לשוק הרחפנים לקח זמן להבשיל וליהנות מהפוטנציאל הטמון בכלים אוטונומיים אלה, אבל זה הגיע וזה קורה".

באדיבות Thirdeye systems

ליאור סגל, מנכ"ל חברת Thirdeye systems

סגל סבור שמזל מגיע כשעבודה קשה פוגשת הזדמנות, וב-Thirdeye ללא ספק היתה עבודה קשה שיצרה הזדמנויות. "בעבודה קשה ועקשנות, וחרף תנאי שוק לא פשוטים, הצלחנו לגדול ולקחת חלק בפרויקטים משמעותיים, שחלקם כבר התפרסמו ואחרים לא ניתן לפרסם. השגנו דריסת רגל משמעותית בתחום הרחפנים, גילוי תנועה ואפילו בתחום הרכב האוטונומי".

"השמים הם הגבול וגם עליו אנחנו שומרים"

החברה פועלת כיום בשלושה תחומים מרכזיים - פיתוח מערכות לרחפנים אוטונומיים; מערכות לגילוי רחפנים; ועולם הרכב האוטונומי. "אנו מפתחים מערכות עבור רחפנים, המזהות אובייקטים שונים בצורה אוטומטית לחלוטין וללא מעורבות אדם. הכל קורה בתוך המצלמה, שפועלת ביום וגם בלילה באמצעים תרמיים. האנליזה מבוצעת בזמן אמת על גבי הרחפן, והממצאים משודרים תוך כדי הגילוי. מערכות אלו חיוניות למשימות אבטחת מתקנים, גבולות וכיו"ב".

מוצר נוסף הוא מערכת לגילוי רחפנים. "התאמנו את הטכנולוגיה הקיימת במערכות לרחפנים, בשינוי היישום. מדובר במערכת אלקטרו-אופטית שמגלה רחפנים, ויכולה לפעול לבדה, או כחלק ממערכת מכ"מ, כדי לעזור לטייב את הגילויים שלה. בתחום זה, יש לנו כמה מוצרים".

בעולם הרכב האוטונומי, האלגוריתמים שפיתחה החברה מסייע לרובוטים ה"נוהגים" בכלי רכב קרקעיים להתנייד בבטחה, מבלי לפגוע בהולכי רגל, במכוניות או בעצמים אחרים בכביש.

לדברי סגל, "בשלוש השנים האחרונות אנחנו בתנופה וגדילה משמעותית, כעת, כשהשוק הבשיל וזיהה את הצורך במוצרים ובפתרונות שלנו. כך למשל, בעבר, רחפנים לא היו מוצר בעל אפקט גדול, כי הם דרשו אדם שיפעיל כל אחד מהם ויביט במסך. היום אין צורך להקצות אדם לכל רחפן, בטכנולוגיה שלנו אפשר להעלות לאוויר 100 רחפנים, ואדם אחד יקבל את המידע מכולם. "בעולם מדברים על רובוטיקה כבר עשרות שנים, אבל עד כה, חוץ מפסי ייצור במפעלים, היא עדיין לא זוכה לתפוצה גדולה. הטכנולוגיה שלנו היא גורם מפתח שמאפשר להרחיב את השימוש ברובוטיקה לתחומים נוספים ללא מעורבות אדם וזה מה שמרתק בעיני", הוא מסכם.

לפרטים נוספים: www.thirdeye-systems.com

פתרונות האבטחה שנולדו אל תוך הענן

"כולם עוברים לענן, זו כבר עובדת חיים. אין ספק שהמעבר הזה מספק יתרונות טכנולוגיים רבים, ובראשם האפשרות להריץ תשתיות גדולות מאוד גם בארגון שאין לו משאבי ענק, תוך חיסכון כספי. ואולם, לא כולם עוצרים לחשוב על המשמעות של אבטחת מידע בעידן הענן, ועל כך שהפתרונות המסורתיים, כבר לא מתאימים במציאות הנוכחית", אומר דרור דווידוף, מנכ"ל חברת אבטחת המידע אקווה סקיוריטי (Aqua Security).

לדברי דווידוף, "כיום המגמה היא לא להעביר תשתיות ואפליקציות לענן - אלא לבנות אותן מראש בהתאמה מלאה לענן, כדי לנצל את מלוא היתרונות הגלומים בו. יישומי קלאוד נייטיב, קונטיינרים, קוברנטיס, Serverless - כל אלה נולדו לעבוד בענן ולספק גמישות, מהירות, חיסכון בעלויות ויכולת תגובה מיידית לשינויים בשוק.

"האפליקציות שרצות בענן פועלות בסביבת DevOps, בעוד שבעבר היתה הפרדה בין המפתחים של האפליקציות לאנשים שהריצו אותן. בעולמות ה-DevOps

דרור דווידוף (מימין) ואמיר ג'רבי, מייסדי חברת אקווה סקיוריטי

יש המון טכנולוגיות חדשות, הכל רץ בענן וזה מאפשר לעסקים גמישות, יכולת התאמה מהירה וסקיילביליות, אבל מציב אתגרי אבטחה חדשים שלא ניתן לתת להם מענה עם כלי אבטחה מיושנים שלא מותאמים לקצב המהיר של עדכון יישומים וליכולת להריץ את אותם יישומים בכל תשתית ענן פרטית או ציבורית".

אבטחת ענן כחלק מהאסטרטגיה העסקית

אקווה סקיוריטי, שנוסדה לפני חמש שנים על ידי דווידוף ואמיר ג'רבי, יצאה למסע לפיתוח כלי אבטחה חדשים, שממנפים את היתרונות הרבים של הענן כדי להעמיד פתרון מקיף ודינמי, בהתאמה מלאה לסביבות DevOps. "כיום יש קטגוריה חדשה, של DevSecOps - אנשים שאחראים על האבטחה ב-DevOps", מסביר דווידוף. "המטרה שלנו היא לספק להם פלטפורמה מלאה להגנה על האפליקציות שרצות בענן.

"קהל היעד שלנו הוא למעשה כל חברה

מגמת המעבר לענן ממשיכה להתרחב משנה לשנה, ומציבה בפני ארגונים אתגרים לא מוכרים של אבטחת מידע. באקווה סקיוריטי הישראלית הבינו שבעולם חדש זה, דרושים גם כלי אבטחה חדשניים

שרוצה לפעול בענן, מחברות גדולות בתחומי הבנקאות, הביטוח והמדיה, ועד סטארטאפים צעירים - כולם זקוקים לפתרונות אבטחה מותאמים. עבור הארגונים הגדולים, שעומדים בפני רגולציה כבדה עם דרישות אבטחה רבות, ונתונים תחת לא מעט מתקפות, בנינו את המוצר המתקדם ביותר בשוק זה.

"שישה מעשרת הבנקים הגדולים בעולם, ושלוש מחמש חברות המדיה הגדולות בעולם הם לקוחות שלנו. אנחנו עובדים עם הארגונים הגדולים בתחומם שנמצאים במעבר לענן, ומבינים שאבטחה היא לא רק כדי לסמן וי על הדרישות, אלא שבלעדיה הם לא יכולים לעבור לענן בקצב הרצוי להם ולשמור על היכולת התחרותית שלהם. האבטחה היא חלק מהאסטרטגיה העסקית שלהם, והם מבינים שכללי המשחק באבטחת הענן הם שונים.

"בעבר, אם היתה לי אפליקציה שנתנה שירות לארגון או ללקוחות, היא ישבה בחוות השרתים תחת ניהולי והיתה לי שליטה מלאה עליה. בניתי הגנה היקפית בעיקרה, דאגתי להגדיר מי יכול לגשת לאן, ממש כמו חומה פיזית. כיום, האפליקציה יכולה לרוץ בכמה עננים במקביל, וכוח העבודה או הלקוחות שלי פזורים בעולם. ההגנה ההיקפית כבר פחות מתאימה, כי הגבולות הרבה פחות מוגדרים.

"כלומר, יש צורך בשינוי גישה - לאבטחה נקודתית, גרנולרית, שיודעת לזוז יחד עם האפליקציה, מענן לענן ומסביבת עבודה אחת לשנייה. כלי ההגנה המודרניים שאנחנו מפתחים נולדו לעולם של הענן. אנחנו ניצבים כל הזמן מול אתגרים חדשים, למשל של פרטיות, גישה לנתונים והפרדה בין התשתית לאפליקציה, וממשיכים לשפר את המוצרים שלנו כדי שייתנו מענה".

דווידוף מסביר כי כיום, מקובל בקרב ספקי הענן הקונספט של אחריות משותפת - Shared Responsibility. "הספק אומר ללקוח - אנחנו יודעים לשמור על התשתיות שלך עד לנקודה מסוימת, וממנה והלאה אתה אחראי לאבטחה. אנחנו מספקים את הפלטפורמה ששומרת על האפליקציות בענן, במקומות שהם באחריותו של הלקוח. "חשוב לזכור שכיום התוקפים הפכו למתוחכמים, נועזים ומאורגנים הרבה יותר, ולא פעם מדובר בארגונים עם משאבים עצומים, אפילו מדינות. הדבר מצריך בנייה של הגנה שיודעת להתמודד עם איומים בסדר גודל עצום, שמשתנים כל הזמן. לכן בכל ארגון יש כמה שכבות של הגנה, כאשר אקווה מספקת את הכלים לשמירה על האפליקציות שרצות בענן כבר משלב הפיתוח ובזמן ההרצה".

ממשיכים להתרחב - גם בתקופת הקורונה

דווידוף מספר כי התרבות הארגונית באקווה סקיוריטי מוכוונת DevOps באופייה. "אנחנו מכירים את הטכנולוגיות הכי חדשות בענן, ועובדים במחשבה על העולמות האלה, במיוחד בפיתוח. יש לנו יותר מ-400 לקוחות בעולם, ומערכת היחסים שלנו איתם לא מסתכמת במכירה חד-פעמית של המוצר, אלא היא ארוכה ומתמשכת, כשמדובר בשיתוף פעולה אמיתי. אנחנו עוברים איתם את המסע, הם גדלים וכל הזמן יש להם צרכים חדשים.

"צוות מחקר מיוחד הפועל בתוך החברה עוסק אך ורק באיתור פגיעויות וחולשות שיש בטכנולוגיות החדשות,

פלטפורמה מלאה להגנה על האפליקציות שרצות בענן. המערכת של אקווה סקיוריטי |
התמונות באדיבות חברת אקווה סקיוריטי

והתקפות בענן, כדי שנזהה אותן לפני השוק ונפתח פתרון אבטחה לפני כל השאר. אנחנו פעילים מאוד בעולמות ה-Open Source וה-Cloud ולא פעם משתפים בקוד פתוח פרויקטים שלנו שיכולים להיטיב עם כולם - גם עם חברות שלא רוכשות את המוצר שלנו, במטרה לעזור לשפר את האבטחה".

לאקווה סקיוריטי מטה ישראלי ובו כ-120 מפתחים, לצד מרכז פיתוח בהודו ומשרד שיווק ומכירות ראשי בבוסטון. לאחר התרחבות מואצת בשנים האחרונות, החברה ממשיכה במגמה זו, ודווידוף מעריך כי "בשנה הקרובה נגייס 50-60 עובדים בישראל. אתגרי אבטחת המידע בענן לא עוצרים לרגע - וגם אנחנו לא".

דווידוף: "בעבר, אם היתה לי אפליקציה שנתנה שירות לארגון או ללקוחות, היא ישבה בחוות השרתים תחת ניהולי והיתה לי שליטה מלאה עליה. בניתי הגנה היקפית בעיקרה, דאגתי להגדיר מי יכול לגשת לאן, ממש כמו חומה פיזית. כיום, האפליקציה יכולה לרוץ בכמה עננים במקביל, וכוח העבודה או הלקוחות שלי פזורים בעולם. ההגנה ההיקפית כבר פחות מתאימה, כי הגבולות הרבה פחות מוגדרים"

לפרטים נוספים:
www.aquasec.com

הסכם הנורמליזציה מול האמירויות פותח דלתות חדשות להייטק הישראלי

באיחוד האמירויות פועלות כ-180 קרנות הון סיכון לצד אנג'לים רבים, המשקיעים סכומים ניכרים בחברות הייטק - בדגש על כמה מהענפים הבולטים גם בתעשייה הישראלית

הסכמי אברהם בין ישראל לאיחוד האמירויות, שנחתמו בספטמבר 2020 בבית הלבן בארה"ב, כוללים גם התייחסות משמעותית לשיתופי פעולה בתחומי האנרגיה והטכנולוגיה. בעוד היחסים הלא-רשמיים שנוצרו בין ישראל לבין מדינות המפרץ בשנות ה-90 לא הניבו פירות רבים, הרי שהסכם הנורמליזציה החדש מעורר תקווה לשינוי.

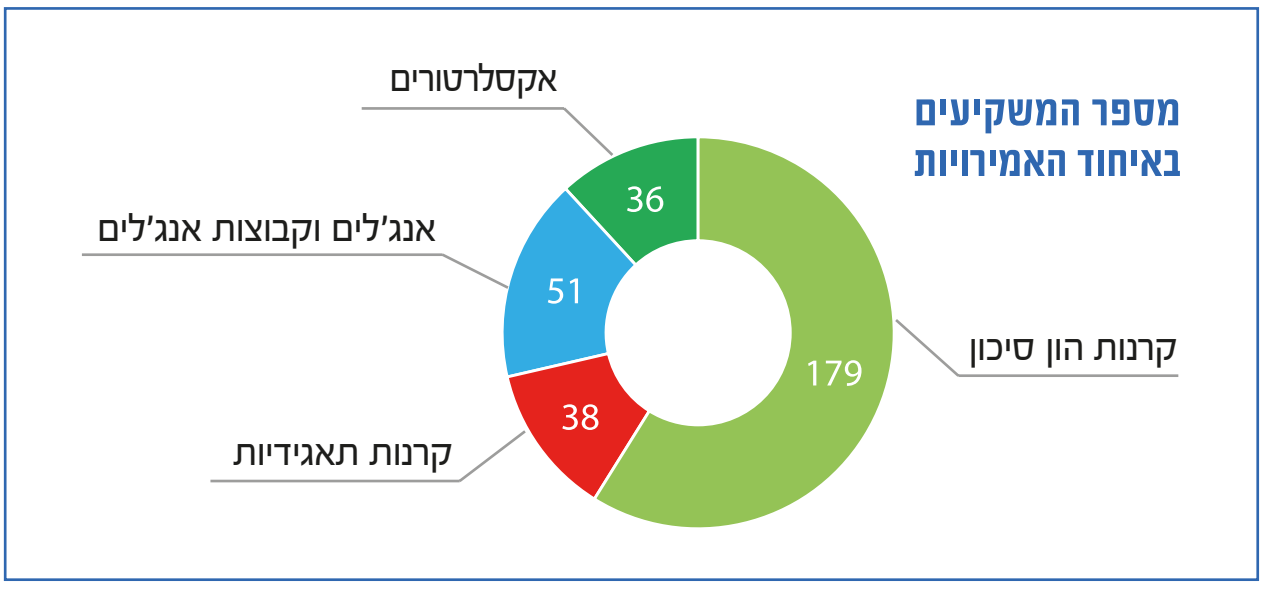
בחברת המחקר הישראלית IVC מסבירים כי בהתאם לנתוני קראנצ'בייס, בשנים 2013-2020, איחוד האמירויות היתה המדינה האקטיבית ביותר בהשקעות הייטק, כשקטאר היא השנייה בדירוג. משקיעים מאיחוד האמירויות לקחו חלק בסבבי השקעות בסכום כולל של 13 מיליארד דולר בתקופה זו. כספים אלה הוקצו לחברות הייטק בינלאומיות, כשהמשקיעים מהאמירויות האיצו את פעילותם הגלובלית ב-2017.

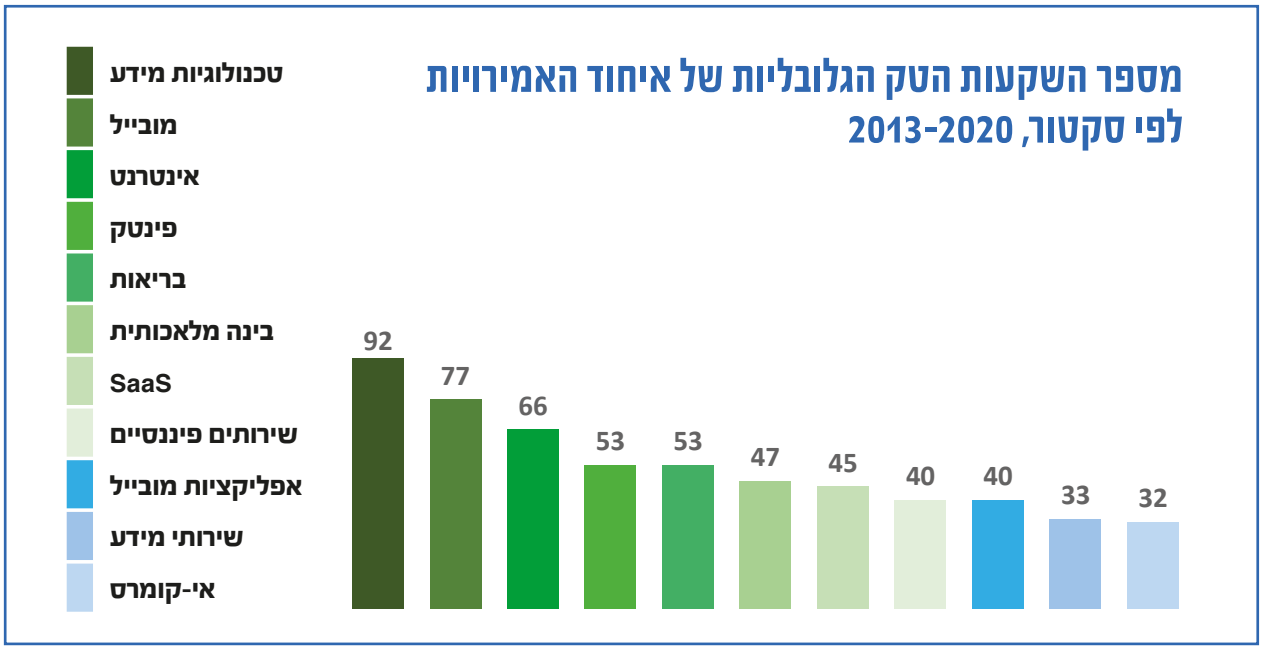
על פי IVC, בשבע השנים האחרונות, פעילות המשקיעים מהאמירויות התמקדה בארה"ב, שם ביצעו 438 עסקות, ובאירופה, עם 88 עסקות. "התנהגותם של המשקיעים מהאמירויות מייצגת אקוסיסטם שדומה לזה של ההייטק הישראלי", אומרים ב-IVC. "קיימות 179 קרנות הון סיכון באמירויות, 38 קרנות תאגידיות, 36 אקסלרטורים, 51 אנג'לים וכן קבוצות אנג'לים. חברות IT הן האטרקטיביות ביותר עבור משקיעים מהאמירויות, בדומה למתרחש בישראל, ואחריהן חברות מובייל, אינטרנט ובריאות".

בישראל, פעילותם של המשקיעים מהאמירויות היתה פחות מורגשת עד כה. חברות הייטק ישראליות משכו השקעות בהיקף של 2.8 מיליון דולר ממשקיעים אלה בספטמבר ובתחילת אוקטובר. "זהו סכום צנוע בהשוואה ל-2.74 מיליארד דולר שהחברות הישראליות גייסו ברבעון השלישי של 2020", אומרים ב-IVC. "לפי הנתונים שלנו, מאז נובמבר 2019, חמש חברות ישראליות גייסו 33.3 מיליון דולר ממשקיעים בקטאר, ערב הסעודית ואיחוד האמירויות".

קרן ההשקעות הישראלית מניב מוביליטי הודיעה בנובמבר על השקעה של 3.8 מיליון דולר בפניקס - סטארטאפ מאיחוד האמירויות. בהשקעה הגדולה ביותר עד כה, חברת Venus Concept הישראלית הנסחרת בנאסד"ק יצאה לסבב גיוס של 28 מיליון דולר, שבו השתתפה קרן הפריווט אקוויטי SEDCO, מערב הסעודית, שהשקיעה 7 מיליון דולר. ונוס קונספט מפתחת ציוד אסתטיקה רפואית.

"הקרבה הגיאוגרפית בין המדינות, והצמיחה המהירה שאפיינה את האזור עד תחילת הקורונה, יוצרות הזדמנות של Win-Win לשני הצדדים", מסכמים ב-IVC.





מקור: Crunchbase.com, IVC Global Partner

בואו להציג את עצמכם בפני המגזר העסקי באיחוד האמירויות

Israel-UAE Business Guide ייצא לאור בתחילת 2021.

המדריך יופץ למגזר העסקי
באמירויות על ידי לשכות המסחר
של אבו דאבי, דובאי וארגונים נוספים,
ויגיע לרוב החברות
ואנשי העסקים במדינה.

מוכנים להיחשף ולעבוד בשוק חדש,
מרתק ומבטיח?

צרו קשר כדי לקבל פרטים:
Inbal@paprikap.com או ב-052-3232130

PAPRIKA
Spicy Marketing Relations