

**המכללה לביטחון לאומי**

**מחזור מ"ז 2019-2020**

**שם הקורס:**

**עולם דיגיטלי לבכירים**

**מטלת סיום בנושא**

**מעבר בנק מב"ל בע"מ לבנקאות פתוחה**

ציון סופי 89

**מרצה: פרופ' דני רז**

**מגישה: רו"ח סימה שפיצר**

**תאריך הגשה:‏** **29 במרץ 2020**

**הצעת הטכנולוגיות ותיאורן**

**בנקאות פתוחה open banking**

בהתאם להוראה מס' 368[[1]](#footnote-1) של הפיקוח על הבנקים על בנק "מב"ל בע"מ" לעבור לשימוש בטכנלוגיית "בנקאות פתוחה" (open banking = Open Application Programming Interface - open API). בנקאות פתוחה מאפשרת ללקוחות הבנקים וחברות כרטיסי האשראי לשתף צדדים שלישיים במידע הפיננסי שלהם. שחקנים חדשים, שאינם בנקים, יוכלו לגשת לחשבון הבנק של לקוח, בהסכמתו, ולהציע לו שירותים בנקאיים מותאמים לצרכיו. בנק ישראל אחראי לפרסום הסטנדרט הטכנולוגי האחיד. על כל הבנקים ליצור פרוטוקול תקשורת אחיד, מסוג https תוך שימוש בשכבת תעבורה מאובטחת מסוג .mTLS התועלת מכך שישנו רק פרוטוקול אחד ויחיד הוא שכל הארגונים שיתחברו לבנקים יוכלו ליצור קשר עם כל הבנקים באותה טכנולוגיה זהה, מבלי שהבנקים יכפו על האפליקציות לעבוד מולם בטכנולוגיות שונות.

**בינה מלאכותית Artificial Intelligence**

על מנת להתמודד עם התחרות הגוברת בכוונת הבנק לעשות שימוש **בבינה מלאכותית - AI** (Artificial Intelligence = AI) [[2]](#footnote-2). בנק מב"ל יציע הצעות ערך ללקוחות של הבנקים האחרים לשיפור המוצרים ולהפחתת העלויות והריביות שהם משלמים (משכנתאות, אשראי, פקדונות, ניהול נ"ע ועוד). הבנק יעשה שימוש בבינה מלאכותית באמצעות מגוון רחב של שיטות (איתור לקוחות שעשו הקלקה על אתרי בנייה ברחבי הארץ וכן על אתרי משכנתאות בבנקים, כניסה לאתרי אינטרנט, רשתות חברתיות, שימוש בסנסורים ובמיקומים בטלפונים סלולריים ועוד).

לאחר שהבנק יאתר את האוכלוסיה הרלבנטית, הוא יציע הצעות ללקוחות תוך שמוש בטכנולוגית Open Banking.

**מהות הכנסת הטכנולוגיות וההישג המצופה לארגון**

**הכנסת הטכנולוגיה של Open API הינה משמעותית לבנק מב"ל מכמה סיבות**: ראשית, זו דרישה רגולטורית, שנית, הראשון ליישם את הטכנולוגיה באופן מיטבי משפר את מצבו מבחינה תחרותית, ושלישית – קיימת חשיפה לסיכונים משמעותית בשל הגישה של בנקים וגופים אחרים שאינם בנקים לנתונים בעלי פרטיות גבוהה, ואם הדבר לא יעשה תוך הקפדה מלאה – הדבר יביא לסיכון משמעותי לבנק – תביעות ייצוגיות, נטישת לקוחות, אובדן אמון וסיכוני מוניטין[[3]](#footnote-3). בנוסף, **הכנסת טכנולוגיית AI תאפשר** איתור לקוחות חדשים, ניצול הזדמנויות חדשות, תחומי פעילות חדשים ותבסס מקורות הכנסה חדשים בעידן של תחרות גוברת.

**סיכונים**

כיום הנתונים הבנקאיים של כל לקוח שמורים אצל הבנקים בסטנדרטים גבוהים. בנקאות פתוחה מאפשרת גישה למידע רגיש מאוד על הלקוחות לבנקים לצדדים שלישיים שאינם בנקים, אשר אינם בהכרח פועלים בסטנדרטים גבוהים.

**סיכונים תפעוליים**

סיכונים תפעוליים יכולים לנבוע **מסיכוני סייבר** – באמצעות יישום הגישות הטכנולוגיות החדשות הבנק חשוף לסיכונים של פגיעה זדונית מרחוק, בין אם על ידי משתתפים פיקטיביים שיפנו אלינו, בין אם על ידי תוכנות זדוניות (malware), גניבת פרטים וכו'[[4]](#footnote-4).

**בנוסף סיכונים תפעוליים יכולים להיגרם כתוצאה מליקויים פנימיים** בארגון, כגון: קליטה שגויה של הנתונים, אובדן נתונים, שגיאות עיבוד, שגיאות חישוב וכדומה.

**סיכוני שרידות, יתירות והמשכיות** – כיצד הארגון ממשיך לפעול במקרה של תקלה חמורה הפוגעת במערכת? האם ישנו אתר גיבוי? האם נקבעו נהלים ותהליכים במטרה לשמר את ההמשכיות של הארגון כך שיוכל להמשיך ולתפקד גם בעיתות חרום?

**סיכוני אבטחת מידע** – הסיכון של הפגיעה בבטחון המידע הרגיש השייך ללקוחות, וכן היכולת ליצור קשר עם מאגרי המידע של הבנקים מצריכים רמה גבוהה של ניהול סיכוני אבטחת מידע, כולל מבחני חדירה וסקרי סיכונים.

**סיכונים משפטיים**

על מי מוטלת האחריות במקרה של כשל משפטי. הארגון חשוף לסיכונים משפטיים בשל המרכיבים הבאים: סיכוני פרטיות, סיכוני איסור הלבנת הון ומימון טרור, ייעוץ כלכלי שגוי, תקלה בביצוע העסקה הכרוכה ביצירת נזק ללקוח וכדומה. כדי להפחית סיכונים אלו יש להתייעץ עם עורכי דין ולגבש נהלים ותהליכי עבודה ברורים להפחתת הסיכונים[[5]](#footnote-5).

**סיכונים פיננסיים**

ייעוץ שגוי, העברת נתונים למי שאינו מורשה, אירועי סייבר עלולים לגרום לסיכונים פיננסיים הן לבנק והן ללקוח באופן שיכול להביא לנטישת לקוחות הבנק, לתביעות ייצוגיות לכן יש לגבש נהלים ותהליכים וכן ללוות את כל התהליך בסקר סיכונים מקיף לבחינת יישון הטמעת המערכות החדשות, דיוקן, נכונותן, שרידותן וכו'.

**השיח עם מומחי הטכנולוגיה ואיך הוא משפיע על קבלת ההחלטות**

תאגיד בנקאי חייב לקבוע מדיניות כללית לנושא יישום טכנולוגיות חדשות. הכנסת מוצרים חדשים ומשמעותיים צריכה לידון בדירקטוריון ובהנהלת הבנק, וכן נדרש להתקיים דיון מקיף בין המשתמשים לבין הטכנולוגים המפתחים וזאת כדי לפתח את המוצר באופן מיטבי ולהימנע מחשיפה לסיכונים שפירטתי לעיל. השיח עם מומחי הטכנולוגיה צריך להתמקד בתיאור המוצר, אך גם כל אחד מהסיכונים המפורטים לעיל, וזאת על מנת שהארכיטקטורה של המוצר שיפותח ויגובש יפחיתו ככל הניתן את הסיכונים הגלומים בפעילות.

המערכת המפותחת על ידי מומחי הטכנולוגיה צריכה לתמוך בתהליכי ניהול הסיכונים. לצורך כך, בדיון עם מומחי הטכנולוגיה לערוך דיון על החשיפה לכל אחד מהסיכונים, כולל הסיכונים התפעוליים, המשפטיים והפיננסיים ועל מומחי הטכנולוגיה להציע כיצד ניתן להתמודד עם סיכונים אלו באופן מיטבי.

יודגש שקיימת חשובה לשיח פתוח אודות כל הסיכונים שכן ההחלטות הטכנולוגיות עשויות להשתנות כתוצאה מההיערכות לניהול הסיכונים.

בנוסף, מומחי הטכנולוגיה עשויים להביא לשינויים מהותיים בתהליכי העבודה ובנהלים כתוצאה מהחשיבה המשותפת ומהסקת המסקנות בתהליך.

**לקחים ונקודות לשימור מהתהליך**

בימים אלו נערכים לקראת יישום לכן אציין את הנקודות שיש להדגיש בתהליך:

* **היערכות מוקדמת**- לפני ההתארגנות לפעילות החדשה יש לקיים דיון בדירקטוריון הבנק ובהנהלה (Top down). יש לדון בעלויות, בצפי ההכנסות, בסיכונים המזוהים ובבקרות.
* **טכנולוגיות חדשות הן הזדמנות** לכניסה לתחומי פעילות חדשים ולתחומים חדשים. הבנת הטכנולוגיות החדשות תאפשר גישה לזירות פעולה חדשות ולתחומי עניין חדשים שיאפשרו הזדמנויות עסקיות חדשות בעולם משתנה ודינאמי.
* יש לערוך **סקר סיכונים** מקיף בהשתתפות הגורמים העסקיים, מומחים טכנולוגיים, גורמי הבקרה על מנת לזהות את הסיכונים המתעוררים מהטכנולוגיות החדשות.
* **אופטימיזציה בתקשורת** – המידע העובר בין התאגיד הבנקאי לצדדים שלישיים הוא רגיש ופרטי, הוא נדרש לעבור באופן מהיר והוא צריך להיות מדוייק. נדרשת אופטימזיציה בכל התהליכים לרבות - מנועי חיפוש ותקשורת נתונים.

**ביבליוגרפיה:**

Hacquebord F., McArdle R., Mercês F., Sancho D. (September 17, 2019). "Ready or Not for PSD2: The Risks of open banking". Trend Micro Research at <https://documents.trendmicro.com/assets/white_papers/wp-PSD2-The-Risks-of-Open-Banking.pdf>

Deloitte (2017). "Open banking, open risk? Managing financial crime in a disrupted world". at [file:///C:/Users/USER/Downloads/deloitte-nl-financial-crisis-open-banking-report-2017.pdf](file:///C:\Users\USER\Downloads\deloitte-nl-financial-crisis-open-banking-report-2017.pdf)

Kosoff J. (January 13, 2020). "Open banking’s three biggest pitfalls". American Bankers at <https://www.americanbanker.com/opinion/open-bankings-three-biggest-pitfalls>

הוראות הפיקוח על הבנקים, הוראת ניהול בנקאי תקין מס' 368 (פברואר 2020) "ישום תקן בנקאות פתוחה בישראל". אוחזר מהכתובת-

<https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/368.pdf>

קונפורטס י. (29 באוקטובר 2019). "מיהם המרוויחים העיקריים ממהפכת הבינה המלאכותית בבנקים?". אנשים ומחשבים אוחזר מ- <https://www.pc.co.il/featured/301937/>

רוחקס דומבה ע. (17 בדצמבר 2019). "בנקאות פתוחה דורשת חשיבה מחודשת על הגנת ממשקי העברת מידע" IsraelDefence.

אוחזר מ- <https://www.israeldefense.co.il/he/node/41297>

1. הוראה מס' 638 "ישום תקן של בנקאות פתוחה בישראל". [↑](#footnote-ref-1)
2. קונפורטס י. (29 באוקטובר 2019). "מיהם המרוויחים העיקריים ממהפכת הבינה המלאכותית בבנקים?". [↑](#footnote-ref-2)
3. Kosoff, 2020. "Open banking’s three biggest pitfalls" [↑](#footnote-ref-3)
4. Hacquebord et al, 2019. "Ready or Not for PSD2: The Risks of open banking". [↑](#footnote-ref-4)
5. Deloitte, 2017. "Open banking, open risk? Managing financial crime in a disrupted world". [↑](#footnote-ref-5)