



ירושלים, י"ז באב תש"ע
28 ביולי 2010
10LM0752
m10101P

לכבוד

התאגידים הבנקאיים וחברות כרטיסי האשראי – לידי המנכ"ל

הנדון: רשתות חברתיות

1. מבוא

בשנים האחרונות, גובר השימוש ברשתות חברתיות באינטרנט, וביניהן - Facebook, Twitter, MySpace, LinkedIn, YouTube, בלוגים ופורומים. רשתות אלו מספקות אמצעי קשר זמין ותשתית להפצת מידע נוחה וקלה בין יחידים, קבוצות בעלי אינטרסים משותפים ואף חברות מסחריות. הרשתות החברתיות עשויות לשמש את התאגיד הבנקאי ולקוחותיו לשימושים כגון: מסירת הודעות שיווקיות, תקשורת אקטיבית לטיפול בתלונות ופניות לקוחות, מתן מידע כללי, נתיב לביצוע פעולות בחשבון הלקוח, אסוף מידע ועוד.

2. סיכונים פוטנציאליים

בצד היתרונות של הרשתות החברתיות, השימוש ברשתות אלה טומן בחובו סיכונים פוטנציאליים לתאגיד הבנקאי וללקוחותיו, לרבות סיכונים תפעוליים, משפטיים, רגולטוריים וסיכוני מוניטין. סיכונים אלה עלולים לנבוע מגורמים שונים, כמוצג בדוגמאות להלן:

2.1. **זיהוי לקוח:** רישום פרטי לקוח עלול לחשוף את הלקוח ואת התאגיד הבנקאי לאירועי Social Engineering ולגניבת זהות לקוח, ולפגוע במערך הזיהוי של התאגיד הבנקאי. לדוגמא, במצב בו התאגיד הבנקאי מסתמך על נתוני האישיים של הלקוח לצורך שחרור חסימת סיסמא.

2.2. **פרסום מידע:** קלות הפרסום והתפוצה הרחבה של מידע המועבר באמצעות רשתות אלה, עלולים להגביר תפוצתו של מידע מטעה, עוין, שקרי או שגוי, ע"י עובד, לקוח או גורם שאין לו זיקה לתאגיד הבנקאי ומעוניין לפגוע בפעילותו. בנוסף, נוכח קלות ההפצה, יתכן שעובד בתאגיד הבנקאי יפרסם מידע מבלי שנבדק או אושר ע"י הגורמים הרלוונטיים, ומבלי שהופעלו הליכי הבקרה הנדרשים.

2.3. **אבטחת מידע:** האתרים והכלים הקשורים לרשתות החברתיות לא בהכרח נבנו מתוך תפיסת אבטחת מידע. השימוש בהם עלול לחשוף את התאגיד הבנקאי, את עובדיו ולקוחותיו לסיכונים כגון, וירוסים וסוסים טרויאניים, התחזות, וחדירה למחשב.


2.4. **שליטה ובקרה:** מרבית הכלים המשמשים את הרשתות החברתיות מופעלים מחוץ לחצרי התאגיד הבנקאי ואינם בשליטתו. לפיכך, אין ודאות כי הוערכו הסיכונים ויושמו בקרות נאותות לטיפול בהם.

3. ניהול סיכונים

בנוסף לאמור בהוראת ניהול בנקאי תקין 357 בנושא ניהול טכנולוגיית המידע, על התאגיד הבנקאי לפעול לצמצום את הסיכונים הנגזרים משימוש ברשתות חברתיות, בין היתר, על ידי נקיטת הצעדים הבאים:

- 3.1 ביצוע הערכה של הסיכונים הנגזרים משימוש ברשתות חברתיות ע"י התאגיד הבנקאי, עובדיו, לקוחותיו וכן, ע"י הציבור הרחב. מומלץ להיעזר, לפי הצורך, בגורם חיצוני מקצועי המתמחה בתחום זה.
- 3.2 ע"פ תוצאות הערכת הסיכונים, לקבוע מדיניות בדבר השימושים ברשתות חברתיות, לרבות סוגי המידע, סוגי הרשתות החברתיות המותרים והגורמים בתאגיד הבנקאי האחראים לפרסום ברשתות החברתיות, תהליכי עבודה ומנגנוני בקרה, ולעגן זאת בנהלים.
- 3.3 למפות את השימושים של התאגיד הבנקאי, תוך בחינתם אל מול תוצאות הערכת הסיכונים והמדיניות, ולבצע שינויים, ככל שנדרש.
- 3.4 לקחת בחשבון שימושים פרטיים אפשריים של עובדי התאגיד הבנקאי ולקוחותיו ברשתות חברתיות ואת השלכותיהם על מערך האבטחה והבקרה של התאגיד הבנקאי.
- 3.5 להטמיע אמצעי בקרה לוודא קיום המדיניות והנהלים (מנגנוני ניטור, כגון, בקרת השימוש, Logs וכד') ולהכין מערך תגובת למקרה של התממשות סיכונים.
- 3.6 לפרסם הנחיות ואזהרות לעובדים וללקוחות.
- 3.7 לעקוב באופן שוטף אחר מגמות, שימושים, סיכונים ושינויים ברשתות החברתיות במטרה לעדכן, לפי הצורך, את המדיניות, הנהלים ואופן הטיפול בנושא.

בכבוד רב,


רוני חזקיהו

המפקח על הבנקים