רשות ניירות ערך

מחלקת ביקורת והערכה

רח' מונטיפיורי 39, תל אביב 6520108

טלפון: 03-7109970

דוא"ל: secinspec@isa.gov.il

www.isa.gov.il

ד' תמוז תשפ"א

14 ביוני 2021

תובנות בנושא 'סיכוני סייבר בחיבור מרחוק למערכות הארגוניות'

מיועד למנהלי קרנות נאמנות והנאמנים לקרנות, חברות לניהול תיקי השקעות, זירות סוחר לחשבון עצמי, רכזי הצעה (להלן: "הגופים המפוקחים")

רקע

ההתפתחות הטכנולוגית של השנים האחרונות אפשרה לארגונים רבים גמישות מרבית בכל הקשור למיקום העבודה של עובדיהם. חיבור מרחוק למערכות ארגוניות הפך להיות כלי שימושי ונפוץ גם אצל רוב הגופים המפוקחים על ידי רשות ניירות ערך. היקף השימוש בחיבור מרחוק עלה במיוחד בתקופה האחרונה, עקב התמודדות הגופים עם השפעת משבר הקורונה.

לצד היתרונות שטכנולוגיה זו מספקת, חשוב להכיר גם בסיכונים הטמונים בשימוש בה, כאשר בראש ובראשונה יש להתייחס לסיכוני סייבר תוך יישום בקרות נדרשות לצמצום חשיפות פוטנציאליות.

לאור האמור, ערכה מחלקת ביקורת והערכה ברשות ני"ע פגישות וראיונות עם מדגם גופים מפוקחים, במטרה לוודא כי סיכוני סייבר הכרוכים בעבודה מהבית באמצעות חיבור מרחוק, מטופלים על ידן באופן נאות.

ריכוז תובנות ופרקטיקות נפוצות

1. כאמור, מעבר גורף לעבודה מרחוק טומן בחובו הרחבה משמעותית של החשיפה לסיכוני סייבר בתוך הארגון, ואכן, רוב הגופים המפוקחים ציינו כי סיכון החשיפה של מידע רגיש וזליגתו הם הסיכונים המשמעותיים ביותר בעבודה באמצעות חיבור מרחוק.
2. מבחינה טכנולוגית, קיים מגוון פתרונות של חיבור מרחוק, כאשר כל המפוקחים עמם שוחחנו משתמשים בכלים מוכרים ומבצעים עדכונים לכלים אלו בהתאם להוראות היצרן. כעקרון, החיבור מרחוק, המוגבל אצל רוב החברות רק לגולשים מתוך ישראל, מבוצע לתחנת העבודה של העובד במשרד או לשרת הטרמינל של הארגון באמצעות פרוטוקולים מאובטחים, כאשר אימות המשתמשים מבוצע באמצעות אימות דו שלבי (אימות שדורש בנוסף לצורך בהקלדת

שם משתמש וסיסמה, גם שימוש בטוקן/ אפליקציה/ הקלדת קוד חד פעמי הנשלח לטלפון של המשתמש (OTP)).

3. רוב החברות מאפשרות חיבור של טלפונים סלולריים למייל הארגוני, כאשר המיילים מחוברים לאזור נפרד מוגן בטלפונים, ובכך נמנעת זליגת מידע עסקי לתוך המכשירים הפרטיים של העובדים וסיכון זליגת מידע רגיש מצטמצם.

4. במקרים רבים, הרחבת אפשרות העבודה מרחוק לכלל העובדים במהלך המשבר נעשתה באופן מהיר יחסית ללא ביצוע הערכת סיכוני סייבר מסודרת לפני או במהלך היישום, עקב לחץ זמן. כעת, לאחר רגיעה מסוימת, רוב החברות ביצעו או נמצאות בתהליך ביצוע סקר סייבר מקיף, שכולל גם היבטים של מעבר עובדים לעבודה באמצעות חיבור מרחוק.

5. כל הגופים המפוקחים עמם שוחחנו, שמים דגש על העלאת המודעות של עובדיהם לתחום אבטחת המידע, ומבצעים הדרכות בהקשר זה באופן תדיר. תכני ההדרכות מתייחסים, בין היתר, לנהלי עבודה, דרכי הפעולה אותן מצופה מהעובדים לנקוט, עדכונים לגבי סיכוני סייבר חדשים ודוגמאות של התקפות שהתרחשו. בנוסף, חלק מהחברות מבצעות בדיקות חדירה ותרגולי סייבר בהשתתפות העובדים, כאשר התרגול הנפוץ ביותר הוא תרגול פישינג, היינו שליחת מייל זדוני לעובדים.

<u>המלצות הסגל</u>

1. נוכח השינוי בדפוסי העבודה שהיו מקובלים טרם פרוץ המגפה והמעבר לעבודה מהבית, אשר צפוי ככל הנראה להימשך גם לאחר הסרת המגבלות, קיימת חשיבות גדולה כי כל ארגון יבצע הערכת סיכוני סייבר אשר תכלול את כל ההיבטים של מעבר עובדים לעבודה באמצעות חיבור מרחוק, ונקיטת פעולות להפחתת הסיכונים הקיימים בכך.

2. היכולת להתמודד עם סיכונים הטמונים בעבודה מהבית בכל הקשור לאבטחת מידע, נסמכת בין היתר על מודעות העובדים לסיכונים אלו. סגל הרשות מבקש לחדד את הצורך בהמשך שיפור ותחזוק מערך ההדרכות בהקשר זה, תוך מתן דגש על סיכוני סייבר חדשים וביצוע תרגולים לעובדים.

לשאלות והבהרות ניתן לפנות למרט סליוזברג, CISA, marats@isa.gov.il.