

נספח 3

**העתק דיוור שירביט**

**ללקוחותיה מיום 3.12.2020**

עמ' 9

3/12/2020

עדכון על אירוע סייבר בשירביט חברה לביטוח בע"מ

לקוחות שירביט היקרים,

אנחנו בשירביט ערים לפניותיכם ומבינים את הצורך שלכם בקבלת פרטים ומידע אודות אירוע הסייבר שאירע בחברתינו, אשר הולך ומתפתח. חשוב לנו בנקודת הזמן הזו לעדכן ששירביט שמה בראש סדר העדיפויות שלה את השקיפות והשיתוף המלא ובפרטים הרלוונטיים. אנחנו משקיעים את מירב המאמצים עם טובי מומחי הסייבר ומלווים על ידי גורמים שילטוניים כדי לספק לכם בטחון אישי וידיעה שאתם בידיים טובות ובטוחות שדואגות ראשית כל לכם ולמידע שלכם. שירביט פועלת ותמשיך לפעול כדי להגיע לפתרון האירוע על הצד הטוב ביותר עם מינימום נזקים ללקוחותיה. אנו יוצרים בימים אלו קשר יזום עם אנשים שפרטיהם הודלפו ונמשיך לפעול כך.

צביקה ליבושור

מנכ"ל שירביט חברה לביטוח בע"מ

מה קרה?

ב-30 בנובמבר זיהו מערכות הניטור של החברה כי היא חווה אירוע סייבר. לאחר בירור ראשוני שביצעה בנושא, החברה גיבשה מהר ככל הניתן את דפוס הפעולה הדרוש לשלב הבא בהתמודדותה עם האירוע.

בתוך כך, החברה יידעה את הרשויות הרלוונטיות, בהן מערך הסייבר הלאומי, רשות שוק ההון, ביטוח וחיסכון, משטרת ישראל, הרשות להגנת הפרטיות ומשרד האוצר.

לשם בירור מקיף ומעמיק ככל האפשר בנוגע לאירוע, ולצורך גיבוש המלצות אופרטיביות והכללתן, החברה שכרה את שירותיהם של מומחי סייבר מהמעלה הראשונה המתמחים בניהול אירועי סייבר, מחקר פורנזי, מחקר מודיעין וניהול משברים. הצוותים הללו עובדים במהלך 48 השעות האחרונות באופן רצוף במטרה לסכל את התקיפה ולהחזיר את החברה לעבודה תקינה. החוקרים מבצעים ניתוח מעמיק של היקף האירוע, הגורם המבצע, היקף הנזק ונקיטת פעולות שיחזור לשם חזרה מהירה לפעילות עסקית מלאה של חברת שירביט.

מהרגע בו התגלה האירוע חברת שירביט פועלת להגנת מערכות המידע של החברה בהתאם להנחיות הרשויות, והיא עובדת עמן בתיאום מלא. לחברה גיבוי מלא של הנתונים וכצעד שנועד למניעת נזק ולשמירה על המידע של לקוחותיה - החליטה לסגור את אתרי האינטרנט שלה ואת כל דרכי הגישה לארגון דרך רשת האינטרנט, עד לבירור האירוע על ידי מומחי הסייבר. בנוסף, החברה פועלת על מנת לבטל או למזער, ככל שניתן, את השפעת האירוע על לקוחותיה.

במהלך הלילה של ה 3/12 התקבלה דרישת כופר בסך של כמיליון דולר ואולטימטום בצידה. לצד דרישת הסחיטה, הדליפו התוקפים פרטים נוספים שמתייחסים גם לתביעות עבר של כמה מלקוחות החברה.

צוותי המומחים וגורמים נוספים בוחנים את השלכות ההודעה שפרסמו התוקפים, ובמקביל נערכים בחברה לחזרה לפעילות באופן מבוקר ומאובטח. באמצעות צוותי מומחים ממלכתיים ופרטיים בתחום הסייבר, שירביט פועלת כדי להגן על המידע ועל לקוחותיה.

אנו מבקשים מלקוחות החברה והציבור הרחב להסתמך אך ורק על ההודעות הרשמיות המתפרסמות מטעם החברה.

אילו שירותים החברה מספקת ומה נפגע?

מרבית הפעילויות של החברה פועלות באופן תקין, לרבות: מכירת פוליסות חדשות, חידוש פוליסות, דיווח על תביעות ותשלומים לספקים. כל מרכזי שירות הלקוחות הטלפוניים של החברה זמינים ופעילים 24/7. חלק מפעילויות החברה ובכלל זה חלק מפעילות הסוכנים ודואר אלקטרוני חיצוני - מושהים לעת עתה, על מנת להגן על מערכות החברה ועד לסיום עבודת מומחי הסייבר. צוותי השירות של החברה עובדים ללא הפסקה להמשך מתן שירות עבורכם, גם במהלך הטיפול באירוע. אנו מצפים לחזור לפעילות מלאה במהלך השבוע הקרוב.

מי הם התוקפים?

בשלב זה אין לנו או לגופים הרלוונטיים הרשמיים של מדינת ישראל יכולת לשייך את התקיפה לגורם מסוים. עם זאת, להערכתנו מדובר בגורם תקיפה שאינו מוכר לגורמי הסייבר והגורמים השלטוניים. ידוע לנו כי הגורם שכביכול אחראי לתקיפה פתח חשבונות Twitter ו-Telegram תחת השם "Black Shadow", ופרסם בהם מספר תמונות וקבצים של תיקי פוליסות ביטוח של כמה עשרות של לקוחות החברה. חשבון ה-Twitter של BlackShadow נחסם ואינו פעיל עוד.

מה הכמות והיקף המידע שדלף?

נכון לעת הזאת, בידי החברה אינדיקציות לדליפת מידע בהיקף מוגבל.

עשיתי בעבר ביטוח בשירביט. איך אדע אם פרטי נחשפו?  
נכון לרגע זה, איננו יכולים לדעת בביטחון מלא אם מידע אודותיך הודלף באופן ספציפי, אלא אם כן שמך כלול במידע שכבר פורסם על ידי התוקפים. שירביט נוקטת באמצעים להגנת המידע האישי של לקוחותיה. מי שיש לו חשש, יכול ליצור עמנו קשר במספר: \*2003.

האם עליי לנקוט בצעדים מיוחדים בשימוש במייל הפרטי שלי או בזה של מקום העבודה?  
אין צורך בנקיטת צעדים מיוחדים, מלבד הקפדה יתרה על התנהגות נכונה ברשת: יש להימנע מפתחת מיילים, לחיצה על לינקים או העברת פרטים אישיים או מזהים בכל מקרה בו מתעורר חשד בנוגע לזהות השולח.

האם צריך לבטל את כרטיס האשראי שלי?  
על פי מידע שבידנו, הפרטים המלאים של של כרטיסי האשראי של לקוחות החברה לא נגנבו, והם מאובטחים. אתה בטח יודע/ת שבכל מקרה, יש לך ביטוח של חברת כרטיסי האשראי על תנועות בכרטיסי אשראי שלך, ולחברות כרטיסי האשראי יש גם מנגנונים שונים למניעת שימוש לרעה. תמיד נכון לעבור על הפעולות בכרטיס האשראי שלך ובמידה ויש פעולה לא מוכרת - יש לצלצל מיד לחברת כרטיס האשראי.

מה עשתה החברה על מנת להתגונן מפני מתקפות סייבר ולשמור על פרטיות העובדים?  
חברת שירביט הינה גוף מוסדי הכפוף להוראות רשות שוק ההון, ביטוח וחסכון. ככזאת, החברה מיישמת את ההוראות הרלוונטיות החלות עליה, לרבות ניהול סיכונים סייבר בגופים מוסדיים, ניהול המשכיות עסקית בגופים מוסדיים ותקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017. החברה עורכת תרגילי סייבר והמשכיות עסקית, מתרגלת את העובדים לזהות מיילים חשודים, מבצעת סקרי סיכונים ומבדקי חדירות למערכות קריטיות, ככל הנדרש.

אנחנו מאחלים לכם ולנו שנות ביטוח רבות ומשותפות גם בעתיד!

לפרטים נוספים תוכלו ליצור קשר ב 2003\*

\*\*\*\*\*