בנק הפועלים

בעל עסק יקר,

מדינת ישראל נמצאת תחת איום מתמשך של מתקפות סייבר,
מצד גורמי פשיעת סייבר ותוקפים מדינתיים.
תקיפות סייבר רבות מכוונות כנגד ארגונים וחברות, במטרה לגנוב מידע וכסף או בכדי לפגוע בתשתיות הארגון ובפעילותו.
עלון זה מכיל הסברים והמלצות לשיפור רמת ההגנה על בית העסק.

לתשומת לבך:

- אבטחת מידע הינו נושא מורכב ומשתנה, וכפוף להוראות דין שונות.
- המידע הכלול בעלון זה הינו כללי, ולא הותאם למטרות או דרישות ספציפיות. אין לראות בו כייעוץ מקצועי, משפטי או אחר.
- זכויות היוצרים והקניין הרוחני במידע הכלול שייכות לבנק הפועלים בע"מ.
  אין להעתיק, להקליט, להפיץ, לבצע, למכור, לתרגם או לעשות כל שימוש אחר בתוכן ללא אישור הבנק.

2025

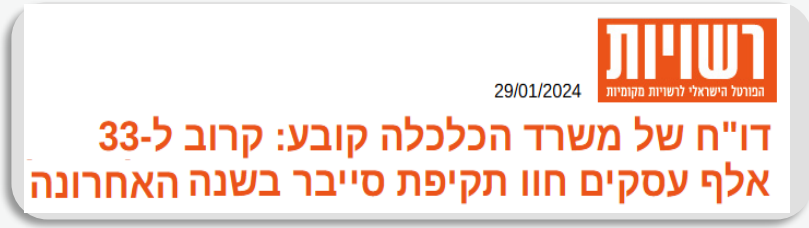
01 פתיח

בשנים האחרונות ניכרת התגברות משמעותית בהיקף ובחומרת מתקפות הסייבר כנגד אנשים פרטיים, עסקים וארגונים בישראל.

מתקפת סייבר עלולה לגרום לנזקים משמעותיים הפוגעים בפעילות העסקית, במוניטין, ברווח הפיננסי ועד לכדי השבתת פעילות העסק.

בנק הפועלים פועל רבות בתחום הגנת הסייבר תוך שימוש בטכנולוגיה ושיטות אבטחה מתקדמות.
על מנת שגם אתם תוכלו ליהנות מהתובנות שאספנו, ריכזנו בעבורכם הסברים והמלצות שיסייעו לכם בהגנה על בית העסק מפני איומי סייבר.

בעלון זה נסביר מספר מונחים בסיסיים, נסקור סוגי מתקפות שכיחות ונמנה דרכים להתגוננות בבית העסק.


רשויות
הפורטל הישראלי לרשויות מקומיות
29/01/2024
דו"ח של משרד הכלכלה קובע: קרוב ל-33 אלף עסקים חוו תקיפת סייבר בשנה האחרונה

גלובס
מפרוץ המלחמה: עלייה של עשרות אחוזים בתקיפות סייבר וכופר נגד חברות ישראליות
נבו טרבלסי 08.2024

02 מיהם תוקפי הסייבר, כיצד הם פועלים ומה יוצא להם מזה?

ישנן מספר מוטיבציות עיקריות לביצוע מתקפות סייבר:

- **מניע אידאולוגי** - גורמים אנטי-ישראליים הפועלים לפגוע בעסקים ובחברות במטרה לייצר נזק והפחדה.
- **מניע מדינתי** – מדינות התוקפות עסקים וארגונים במטרה לגנוב סודות מסחריים, צבאיים, קניין רוחני או כספים.
- **מניע כלכלי** – ארגוני פשיעת סייבר שמטרתם גניבת כספים.

אחת הדרכים הנפוצות להתחזות מול עובדים בהודעה או בשיחה מתחזה, נעשית באמצעות "הנדסה חברתית".
התוקפים אוספים מידע על עובדי החברה באמצעות מקורות מידע גלויים (כמו אתר החברה ומאמרים שפורסמו) וברשתות החברתיות על מנת להכיר את העובד, תפקידו בחברה ותחומי עניין אישיים. מידע זה מאפשר התחזות לעובד ומול העובד.

<u>סוגי מתקפות נפוצות</u>:

וירוס כופר (Ransomware) – נוזקת סייבר המצפינה קבצים במחשבי בית העסק ומונעת גישה אליהם ובכך פוגעת בפעילות העסקית.
התוקפים דורשים תשלום לשחרור הקבצים המוצפנים.

סחיטה – תוקפי הסייבר המצליחים לשים את ידם על מידע רגיש דורשים דמי סחיטה על מנת שהמידע לא יופץ.

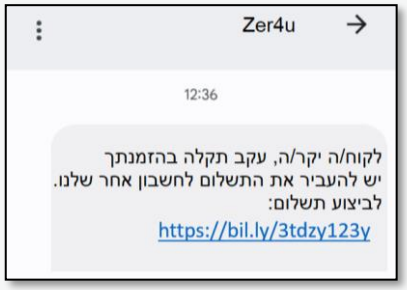
התחזות דיגיטלית – השתלטות על תיבות מייל וחשבונות WhatsApp של לקוחות או ספקים לצורך התחזות ושינוי פרטי חשבון בנק,
כך שהכספים יועברו לחשבונות של התוקפים במקום ללקוחות או לספקים. פעולת ההתחזות יכולה להתבצע גם בשיחת טלפון.

גניבה ממערכות כספים – נוזקת סייבר המנתבת העברות כספיות לגיטימיות לחשבונות התקופים וכן גניבת מידע רגיש מבית העסק לצורך מכירתו.

02 המשך - מיהם תוקפי הסייבר, כיצד הם פועלים ומה יוצא להם מזה?

הודעות ושיחות מתחזות

אחת מהונאות הדיגיטל הנפוצות ביותר היא שליחת הודעות מתחזות (המוכרת גם כ'פישינג') באמצעות מסרון SMS, במייל, ב-WhatsApp וברשתות חברתיות. הודעות אלו כוללות לרוב בקשה לביצוע פעולה דחופה או הצעת הטבה מפתה, בלחיצה על קישור או בהפעלת קובץ מצורף.
הונאה נוספת כנגד בתי עסק היא התחזות בהודעה או בשיחת טלפון לגורם בכיר בחברה או ללקוח / ספק של העסק, במטרה לגרום לבית העסק להעביר תשלום למספר חשבון חלופי של התוקפים.



לחיצה על הקישור בהודעה מפנה לאתר אינטרנט מתחזה בו מתבקשים להקליד פרטי זיהוי רגישים (לצורך השתלטות על חשבון דיגיטלי), או אמצעי תשלום המועברים לתוקפים.

כיצד ניתן להתמודד עם הונאה זו?

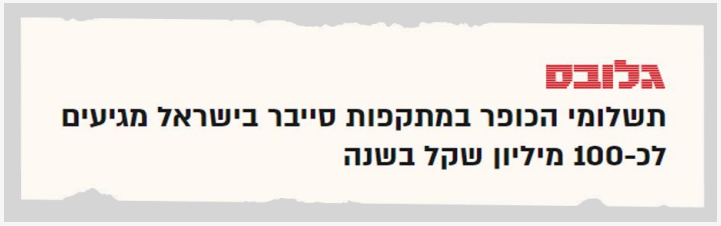
- הימנעו מלחיצה על הקישור או מפתיחת קובץ המצורפים להודעה. **הגיעו לאתר ביוזמתכם, באמצעות חיפוש האתר בגוגל או דרך האפליקציה.**
- בכל הודעה המכילה בקשה רגישה לשינוי פרטי תשלום, רצוי לבצע אימות נוסף בערוץ תקשורת אחר, מול גורם מוכר לכם בחברה.
- בקבלת שיחת טלפון שלא אתם יזמתם, הימנעו ממסירת פרטים אישיים, בדגש על פרטי זיהוי לחשבונות דיגיטליים או קודי אימות. נתקו את השיחה וצרו קשר ביוזמתכם לפי המספר הרשמי של החברה המפורסם באתר החברה הרשמי.
- בחשש למתקפת סייבר או חשיפת מידע רגיש, דווחו למערך הסייבר הלאומי בחיוג 119 או ב-team@cyber.gov.il ולאיש הקשר בבנק הפועלים.
- הפעילו אימות דו-שלבי בחשבונות הדיגיטליים של בית העסק.
- קבעו סיסמה חזקה וייחודית לכל אחד מחשבונותיכם הדיגיטליים. מומלץ להשתמש בתוכנה לניהול סיסמאות (Password Manager).

03 כיצד ניתן לצמצם את סיכון הסייבר לבית העסק?

מוכנות למתקפת כופר (Ransomware)

נוזקות כופר מצפינות קבצים במחשבי בית העסק ופוגעות בפעילות העסקית השוטפת. לרוב נוזקת כופר נכנסת למחשבי בית העסק באמצעות קבצים זדוניים המצורפים למיילים, קישורים המובילים לאתרים זדוניים או בעת חיבור רכיבי USB המכילים את הנוזקה.
נוזקות אלו מוכרות כ'נוזקות כופר' מכיוון שהתוקף מציע לקורבן לשלם דמי כופר על מנת לקבל מפתח ייחודי לשחרור הקבצים המוצפנים.

ynet
חברות ישראליות שילמו כופר של יותר ממיליארד דולר ב-2020
19.08.21 | טל שחף


גלובס
תשלומי הכופר במתקפות סייבר בישראל מגיעים לכ-100 מיליון שקל בשנה

כיצד ניתן להתמודד עם וירוס כופר?

- גיבוי מידע - הקפידו לגבות את המידע החשוב לבית העסקת על גבי כונני אחסון חיצוניים או בחברות המספקות שירותי גיבוי.
- דווחו בהקדם לגורם האחראי בבית העסק. ניתן לפנות למערך הסייבר הלאומי לדיווח על האירוע וקבלת הנחיות.
- נתקו את המחשבים בבית העסק מרשת המחשוב, על מנת למנוע המשך התפשטות של הווירוס לשאר המחשבים ברשת.
- הימנעו מתשלום דמי הכופר לתוקפים מכיוון שאין וודאות שתקבלו את מפתח ההצפנה ומכיוון שייתכן שמתקפה זו תוביל לניסיונות תקיפה נוספים.
- היעזרו בשירותים המציעים מענה בחינם לנפגעי מתקפות כופר כדוגמת אתר https://www.nomoreransom.org, המספק מפתחות הצפנה שפורסמו בעבר.
- אם אין בידיכם את מפתח ההצפנה לפתיחת הקבצים, עומדת בידיכם האפשרות למחוק ולהתקין מחדש את המחשבים בבית העסק ולהשתמש בגיבוי המידע שהכנתם מבעוד מועד.

03 המשך - כיצד ניתן לצמצם את סיכון הסייבר לבית העסק?

מניעת סיכון אבטחתי של התחברות מרחוק לבית העסק

בתי עסק וארגונים רבים מאפשרים לעובדיהם להתחבר למערכות בית העסק מביתם באמצעות מחשבם האישי או מחשב שסופק להם ע"י בית העסק. תוקפי סייבר רבים מחפשים חולשות אבטחה שיאפשרו ניצול של יכולת ההתחברות מרחוק לפגיעה בבית העסק.

המלצות להגנה על רשת בית העסק

- **הגדרת מדיניות מאובטחת להתחברות מרחוק** - ניתן לקבל ייעוץ מחברות סייבר או בהנחיות של מערך הסייבר בקישור הבא – https://www.gov.il/he/pages/cybersecuritymethodology_2?chapterIndex=2.
- **שימוש בתווך תקשורת מאובטח ומוצפן** כדוגמת שירותי VPN.
- **התחברות באמצעות מחשב של בית העסק** הכולל מדיניות אבטחה, לרבות הקשחה של Group Policy ומערכות הגנה.
- **יישום מדיניות סיסמאות מורכבות** ושימוש באימות דו-שלבי.
- **טיוב ה-Firewall הארגוני** לצמצום הגישה מרחוק למינימום, להגדרת מדינות המורשות להתחבר ולתיעוד ההתחברות.

04 המלצות בסיסיות להגברת המוכנות לסיכוני סייבר

פרק זה מפרט המלצות פשוטות ליישום או בעלות נמוכה יחסית, אשר יישומן ישפר את רמת ההגנה על בית העסק.

- **הגברת מודעות עובדי בית העסק לסיכוני הסייבר** – הקפידו לקיים הדרכות תקופתיות הסוקרות את איומי הסייבר הרלוונטיים לבית העסק ואת דרכי ההתמודדות.
- **ניהול משתמשים** – הקפידו לטייב מעת לעת את ההרשאות הניתנות לעובדים בבית העסק, כך שכל עובד יקבל את ההרשאות הנדרשות לביצוע תפקידו ולא יותר מכך.
- **ניהול סיסמאות** – הגדירו מדיניות סיסמאות כך שהעובדים יידרשו להחליף את סיסמתם מעת לעת ולקבוע סיסמה חזקה שלא קל לנחש.
- **הגנה על חשבונות דיגיטליים** – הפעילו שכבת הגנה נוספת על חשבונות הדיגיטליים של בית העסק באמצעות הפעלת אימות דו-שלבי.
  אימות דו-שלבי הוא אמצעי הגנה חינמי שיישלח לכם קוד אימות ב-SMS בכל מקרה שתזוהה כניסה ממכשיר חדש לחשבונכם.
- **עדכוני מערכות הפעלה ותוכנות** – הקפידו להשתמש במערכות הפעלה עדכניות ונתמכות במחשבי בית העסק, לדוגמה מערכת ההפעלה Windows 7 אינה נתמכת עוד ע"י מיקרוסופט ואינה מקבלת עדכוני אבטחה תדירים ועל כן שימוש בה מהווה סיכון לבית העסק.
  הקפידו לעדכן מעת לעת את מערכות ההפעלה במכשירים השונים, את התוכנות ואת האפליקציות.
- **אנטי-וירוס להגנה על מחשבי בית העסק** – תוכנות אנטי-וירוס מגינות על מחשבי בית העסק מפני וירוסים מוכרים. מומלץ לרכוש ולהתקין תוכנת אנטי-וירוס, המספקת יכולות Internet Security ומגינה מפני סוגים נוספים של מתקפות.
  במערכת ההפעלה Windows 10 ומעלה קיים אנטי-וירוס מובנה הנקרא Windows Defender המספק הגנה בסיסית.
  יש להקפיד ולעדכן את תוכנת האנטי-וירוס באופן תדיר ולבצע סריקת וירוסים בכל מחשבי בית העסק מעת לעת.

04 המשך - המלצות בסיסיות להגברת המוכנות לסיכוני סייבר

- **גיבוי הקבצים החשובים של בית העסק** – גיבוי המידע הקריטי של בית העסק, באופן המופרד ממערכות בית העסק, יאפשר לחזור לפעילות במהירות יחסית לאחר מקרה של נזק תפעולי או מתקפת סייבר. מומלץ לייצר תהליכי גיבוי אוטומטיים ככל שניתן.
- **אבטחת רשת ה-Wi-Fi של בית העסק** – הגדירו סיסמת כניסה לרשת האלחוטית של בית העסק, כך תמנעו כניסה מ'אורחים לא רצויים'. מומלץ לבחור סיסמה חזקה ולהימנע משימוש במספר טלפון כסיסמה.
- **שמירה על מידע המוגן עפ"י תקנות הגנת הפרטיות** – חשיפת מידע אישי אודות לקוחות ועובדי בית העסק עלולה להוביל לצעדי אכיפה מצד הרשות להגנת הפרטיות ולתביעות אזרחיות. במידה ובית העסק מחזיק מידע אישי רגיש בהתאם להנחיות הרשות, יש לפעול למניעת חשיפה של המידע לגורמים בלתי מורשים.

  למידע נוסף בנושא תקנות הגנת הפרטיות ניתן ללחוץ על קישור זה: https://www.nevo.co.il/law_html/law00/144811.htm
  או חפשו ב'גוגל' "תקנות הגנת הפרטיות".

05 המלצות מתקדמות להגברת המוכנות לסיכוני סייבר

פרק זה מפרט המלצות המיועדות לעסקים בינוניים וגדולים. יישום ההמלצות כרוך בהשקעה תקציבית, אך ישפר באופן משמעותי את רמת ההגנה.

- **הגדרת אחראי אבטחת מידע בבית העסק** - איוש התפקיד ע"י גורם מקצועי יגביר במידה ניכרת את מוכנות בית העסק לאיומי סייבר.
  מנהל אבטחת מידע מקצועי יפעל להתאמת מדיניות ובקרות לבית העסק.
- **הפעלת מערכות להגנה על רשת המחשבים הארגונית** –
  - **התקנת Firewall** - רכיב המשמש כ'שער הכניסה' לבית העסק ומבצע הפרדה בין רשת האינטרנט הציבורית לרשת בית העסק.
    מומלץ להיעזר בשירותי גורם מקצועי להפעלת והגדרת הרכיב.
  - **פתרון IPS (Intrusion Prevention System)** - מערכת לניטור התקשורת הנכנסת לרשת העסק ומסייעת במניעת מתקפות סייבר נפוצות.
  - **מערכת לסינון דוא"ל** – מיילים הנשלחים לעובדי בית העסק הם הסיכון הנפוץ ביותר להכנסת נוזקות למערכות המחשוב של בית העסק.
    מערכת הסינון סורקת את המיילים הנשלחים לבית העסק וחוסמת תוכן זדוני, לפני שהוא מגיע לתיבת המייל של העובד.
  - **מערכת סינון גלישה** – מערכת הסינון מסייעת במניעת גישה לאתרים באינטרנט ברמת סיכון גבוהה ובהורדת קבצים מסוכנים.
  - **שמירה על מידע לפי תקנות הגנת הפרטיות** – חשיפת מידע אישי אודות לקוחות ועובדי בית העסק עלול להוביל לצעדי אכיפה מצד הרשות להגנת הפרטיות ולתביעות אזרחיות. במידה ובית העסק מחזיק מידע אישי מזהה, יש לפעול למניעת חשיפה של המידע לגורמים בלתי מורשים. ניתן לעשות שימוש בפתרונות לניטור ומניעת דלף המידע שיוצא מרשת בית העסק, למשל באמצעות הדואר האלקטרוני.
  - **ביצוע סקרי אבטחת מידע ומבדקי חדירה תקופתיים** – באופן זה, בית העסק יוכל לקבל תמונה על המצב הקיים במערכות השונות.
    ככל שהסקר יהיה רחב יותר, ניתן לבצע מבדקי חדירה למערכות ו/או שרתים ע"י תרחישים שונים שיוגדרו מראש. תוצאת המבדק יתנו לבית העסק תמונת מצב עדכנית, לרבות שינויים ועדכונים שיומלצו לביצוע על מנת להגביר את רמת האבטחה למערכת הנבדקת.