אגף משאבי אנוש, ניהול סיכונים ורגולציה
מחלקת ניהול סיכונים ורגולציה

הנחיות ראשוניות לאבטחת מידע*

*שים לב- מסמך זה אינו מהווה חלופה לחלק או כלל תקן PCI DSS .הוא בגדר BEST PRACTICE בלבד.

1. קישוריות

רשת ציבורית
כל רשת המאפשרת התחברות של מחשבים שאינם בשליטה מלאה של בית העסק.

רוב דליפות המידע נגרמות עקב כשל או הגדרה לא נכונה של קישוריות לרשת ציבורית.

1.1. כללי

באם לצורך קישוריות נעשה שימוש בנתב (router) או במתג (Switch) יש לפעול כדלקמן:

- ☑ יש לשנות את סיסמת ברירת המחדל של הנתב(ים) ו/או המתגים.
- ☑ על הסיסמה להיות ייחודית לכל בית עסק.
- ☑ אורך הסיסמה יהיה לפחות 8 תווים.

2.1. הפרדה תקשורתית

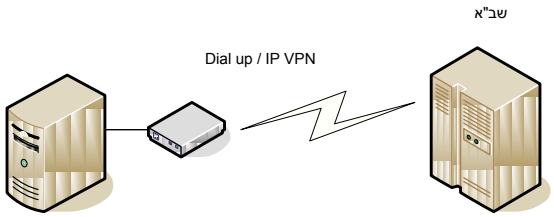
מרבית הפריצות מתבצעות דרך האינטרנט או רשת ציבורית אחרת (כגון רשת אלחוטית).

מחשבי אשראי
מחשבים בהם משודרים, נקלטים, מעובדים או מאוחסנים נתוני האשראי הבאים (חלקם או כולם): פס מגנטי, מספר כרטיס, תוקף, CVV2.

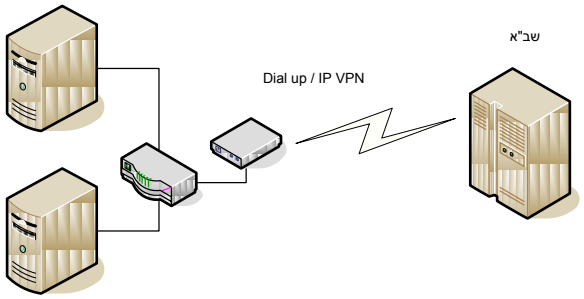
1.2.1. ניתוק מרשת ציבורית

הפתרון "הפשוט והבטוח ביותר" הוא לנתק את כל מחשבי האשראי מהרשת:

- ☑ כל מחשבי האשראי ינותקו מהרשת וסליקת האשראי תתבצע בחיוג או באמצעות קו יעודי (כגון VPN)



הערה: ניתן ליצור רשת פנימית הכוללת מספר מחשבים (קופות/עמדות/שרתים) ובתנאי שכל הרשת הנ"ל תהיה מנותקת מכל רשת אחרת, אם המחשבים ברשת זו מחוברים באמצעות תקשורת אלחוטית ראה הנחיות בסעיף 0.



1.2.2. **רשת אלחוטית**

חל איסור לחבר רשת אלחוטית (WIFI) למחשבי האשראי

2. נתונים רגישים

הגדרה: נתוני הפס המגנטי במלואם ו/או ה- CVV2 (שלוש הספרות בגב הכרטיס).

1.2. חל איסור מוחלט לשמור נתונים רגישים לאחר אישור העסקה על ידי חברת האשראי.עליך לוודא כי:

- ☑ אתה עושה שימוש בגרסא של תוכנת אשראית אשר אינה שומרת נתונים אלו(גרסא 589 ומעלה)
- ☑ אינך שומר נתונים אלו במקביל לתוכנת אשראית

2.2. אם הנך משדרג עמדה קיימת אשר עלולים להיות בה נתונים "היסטוריים", עליך לוודא כי:

- ☑ הינך מוחק את כל הקבצים, והטבלאות במסדי הנתונים המכילים מידע היסטורי
- ☑ הינך מוחק גם את הנתונים האלה מכל כונן גיבוי או מחיצה בה מגובים נתונים אלה

3. השתלטות מרחוק

שימוש לא נכון ולא בטוח בתוכנת השתלטות מרחוק מהווה "כרטיס כניסה" קל ופשוט לפורצים.

1.3. אם בחרת להתקין תוכנה כזו כדי לתמוך בלקוחותיך יש לפעול כדלקמן:

- ☑ בכל בית עסק תותקן רק תוכנה אחת מסוג אחד **כאשר היא הגרסה האחרונה והמעודכנת ביותר של תכנה זו .**
- ☑ התחברות לבית העסק תחייב אישור של משתמש מקומי. ללא אישור לא תוכל להתבצע השתלטות.
- ☑ יש להתחבר למערכות בית העסק אך ורק מ-IP קבוע ומוגדר מראש. (טכנאים אשר עובדים מהבית וכ"ו יתחברו קודם כל למחשב המרכזי עם ה-IP הקבוע ומוגדר מראש ומשם יתחברו למערכות בית העסק)
- ☑ התחברות לתוכנה תחייב סיסמה בת 8 תווים לפחות שתכלול גם סימנים מיוחדים אותיות (גדולות וקטנות) ומספרים.
- ☑ הסיסמה תהיה ייחודית לכל בית עסק.
- ☑ שם משתמש והסיסמה לא יהיו זהים.
- ☑ על התוכנה להינעל לאחר חמש הקלדות של סיסמה שגויה.
- ☑ על התוכנה להצפין את התווך בין המחשב הנשלט לבין המחשב השולט.

4. אנטי וירוס

מניתוח מקרי פריצה וזליגת הנתונים עולה כי בחלק ניכר מהמקרים מושתל בבית העסק "סוס טרויאני" אשר גונב קבצים או מעתיק לחיצות מקלדת (כולל קורא פס מגנטי) ושולח אותם אל התוקף.

1.4. יש להתקין בבית העסק תוכנת אנטי וירוס על פי הכללים הבאים:

- ☑ האנטי וירוס יהיה של חברה ידועה ומוכרת.
- ☑ אם רישיון האנטי וירוס כרוך בתשלום, על בית העסק להיות מיודע בנוגע לחובתו לחדש את הרישיון מידי שנה.
- ☑ אין לבטל אפשרויות ברירת מחדל או להגדיר החרגות באנטי וירוס.

5. שירותי רשת

במקרים מסוימים נדרשים לצורך אדמיניסטרציה ו/או עדכונים, שירותי רשת. שירותים אלה, אם הם לא מאובטחים כראוי עלולים לשמש פורצים כדלת אחורית לגישה למחשב.

1.5. השירותים היחידים המותרים להתקנה במחשבי הלקוח הם שירותי Telnet, SSH ו FTP.

☑ יש לבטל כל שירות רשת אחר המותקן במחשבי האשראי.

2.5. אם מותקן שירות Telnet/SSH או FTP יש לפעול כדלקמן:

☑ התחברות לתוכנה תחייב סיסמה בת 10 תווים לפחות שתכלול גם אותיות ומספרים ותהיה ייחודית לכל בית עסק.
☑ שם משתמש והסיסמה לא יהיו זהים.

3.5. אם מותקן שירות FTP, הכרחי שלשרת ה FTP לא תתאפשר גישה למחיצה בה נשמרים פרטי כרטיס האשראי.

6. מערכת הפעלה

מערכת הפעלה לא מעודכנת חשופה יותר בפני פורצים ותוכנות מזיקות

1.6. יש לבצע הקשחה של מערכת ההפעלה כדלקמן:

☑ יש להפעיל את מנגנון חומת אש (Firewall) של מערכת ההפעלה
☑ יש לבטל את חשבון האורח (Guest)
☑ יש לשנות את שם חשבון ה Administrator לשם אחר – על פי בחירתך.
☑ יש לקבוע סיסמה לחשבון Administrator אשר תכלול לפחות 8 תווים (אותיות ומספרים) ותהיה ייחודית לכל בית עסק.

2.6. עדכוני מערכת ההפעלה

☑ וודא כי מותקנת ערכת השירות (service pack) העדכנית ביותר עבור מערכת ההפעלה בבית העסק.
☑ עליך להתקין ידנית (או לוודא כי בית העסק עושה זאת) את עדכוני האבטחה לפחות אחת לחצי שנה.