ניהול אבטחת סייבר – פרוייקט גמר

מגישים – בר בנילוש, יותם פב ושמעון דסטה

איסתא | ניהול אבטחת סייבר | סמסטר ב׳ 2020

תוכן עניינים

חלק א' – תיאור הארגון

1. תיאור הארגון –

א. רקע: קבוצת איסתא נולדה בשנת 1956 היא מקבוצות התיירות הוותיקות בישראל. איסתא משווקת מוצרי תיירות, בהם טיסות, מלונות והשכרות רכב. בראש הקבוצה נמצאת החברה הציבורית איסתא ליינס בע"מ, לה מספר חברות בנות העוסקות בתחום התיירות, ובראשן איסתא ישראל, המונה 45 סניפים נכון לשנת 2014. בין החברות הבנות בקבוצת איסתא ליינס נכללות החברות אמריקן אקספרס טרוול ישראל, וואלה טורס, נופש ישיר, איסתא ספורט, אורטל, איסתא סטייל, אקדמי טרוול, איסתא נכסים ומלונות ועוד.

ב. תחום פעילות: מספר אתרי אינטרנט שנמצאים בפעילות כולל שירותים לחברות אחרות, אפלקציות מובייל, מוקד שירות טלפוני.

ג. מספר עובדים: בחברה מועסקים מעל ל-1000 עובדים שהם כ-35% מהמועסקים בענף זה.

ד. גודל: איסתא ישראל היא רשת הנסיעות הגדולה בישראל עם 45 סניפים, מתוכם 10 סניפים בתוך האוניברסיטאות והמכללות ברחבי הארץ. בנוסף, לאיסתא למעלה מ-400 יועצי נסיעות מקצועיים ומיומנים היושבים בסניפים השונים ובמוקד הטלפוני ומוכנים לתת את המענה הטוב ביותר לכל לקוח.

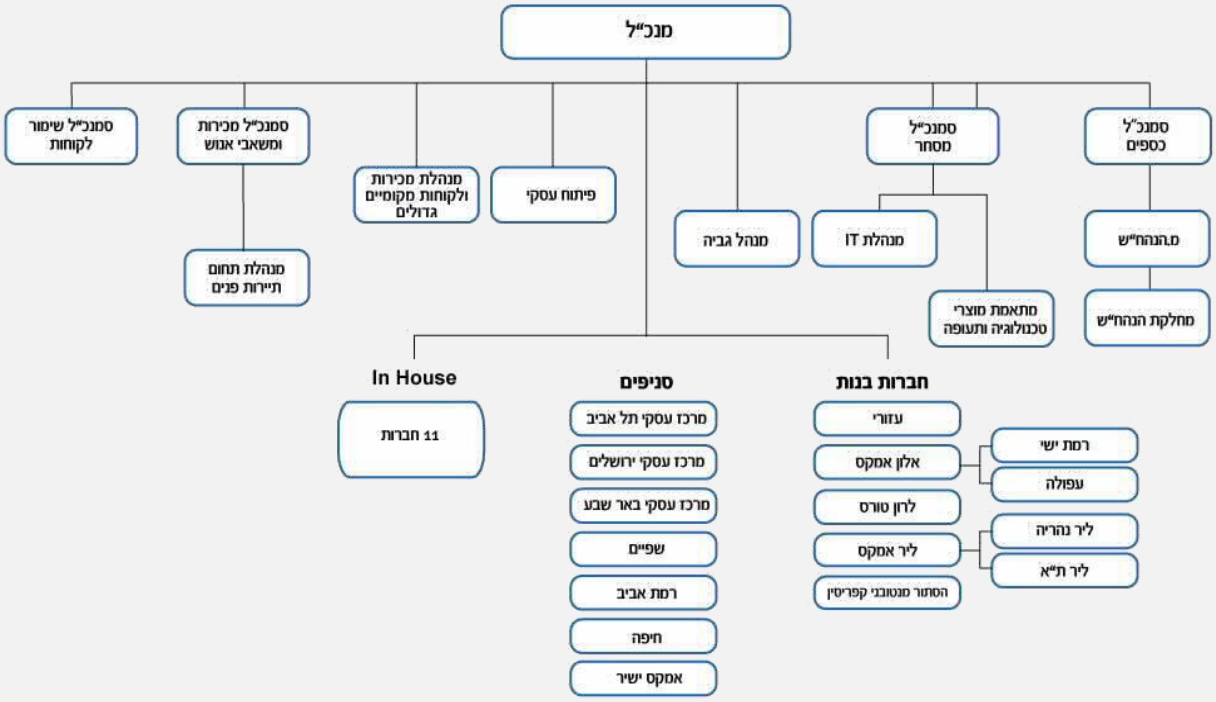
ה. מוצרים: איסתא ישראל מעניקה שירותי
תיירות יוצאת ותיירות פנים כולל טיסות סדירות, טיסות שכר, חבילות נופש, טיולים מאורגנים, חופשות סקי, ספורט ומוזיקה ובנוסף, שירותים משלימים כגון בתי מלון, השכרות רכב, ויזות, וכרטיסי סטודנט.

ו. ענף ומקום בשוק: ענף התיירות מאופיין בתחרות גבוהה וכלל מאות חברות. כיום איסתא מדורגת במקום הראשון מבין חברות התיירות הישראליות מבחינת כמות עובדים, שווי ואחוז השוק בו היא מחזיקה.

ז. מתחרים: עיקר התחרות של החברה הינה מול חברות כגון אופיר טורס, הדקה ה- 90 והשטיח המעופף.

ח. מיקום גיאוגרפי: לחברה 39 סניפים הפרוסים ברחבי ישראל ומשרדי החברה ממוקמים בבית איסתא, ברחוב מנורת המאור 8 ,תל אביב.

2. מבנה הארגון –



בראש החברה עומד המנכ"ל מר' אחישי גל ויו"ר הדיריקטוריון מר' עמיחי גרין.
תחת המנכ"ל מספר סמנכ"לים : כספים, מסחר, מכירות ומשאבי אנוש ושימור לקוחות.
מספר תפקידים בכירים בחברה כמו מנהל גביה, ראש אגף פיתוח עסקי האחראי על התפתחות החברה והרחבת המוצרים ומנהלת מכירות.
בבעלות קבוצת איסתא ליינס שורה של חברות העוסקות בצדדים שונים של ענף התיירות. כמו כן, חברות בת העוסקות בתחום הנדל"ן המניב והמלונאי.

- איסתא ישראל – רשת הנסיעות הגדולה בישראל, העוסקת הן בתיירות פנים והן בתיירות חוץ. זוהי הזרוע הראשית של הקבוצה, המפעילה 45 סניפים ומהווה את ליבת העסקים של איסתא ליינס.
- היסתור אלטיב – מחזיקת המותג "אמריקן אקספרס טרוול ישראל", כיום בשליטת איסתא ליינס, זכיינית רשמית ובלעדית בישראל של אמריקן אקספרס נסיעות. החברה מפעילה כ-16 סניפים בארץ ומתמחה בעיקר במגזר העסקי.
- מבט פלטיניום – חברת המתמחה בתיירות נכנסת. החברה מייעצת ומתאימה חבילות תיירות ליחידים ולקבוצות מחו"ל המעוניינים לבקר בישראל לכל פרק זמן ולכל מטרה.
- וואלה טורס – חברה בבעלות משותפת של "וואלה! שופס" ושל "איסתא ליינס", המתמחה בשיווק ובמכירה של שירותי תיירות באמצעות האינטרנט, על בסיס התשתית של "וואלה! שופס."
- נופש ישיר – עיקר פעילות החברה מתבצעת על ידי מוקד הזמנות טלפוני, שבו ניתן להזמין שירותי תיירות בישראל ומחוצה לה.
- אורטל – שותפות עם חברה המתמחה בתיירות פנים לקבוצות, ארגונים וועדי עובדים וכן בארגון ימי כיף, כנסים ואירועים לשוק המוסדי.
- איסתא ספורט – החברה מתמחה בחבילות תיירות סביב הופעות ואירועי ספורט בעולם, כגון משחקי NBA, פיינל פור, אולימפיאדה, מונדיאל וכדומה. לכל עובדי החברה רקע ספורטיבי.
- כנס תיירות גלובל סרוויס – חברה בת של איסתא ספורט – החברה עוסקת בתיירות נכנסת בעיקר מצפון אמריקה בסגמנטים שונים הכוללים: ארגונים יהודים, קבוצות, נוצרים, תגלית ובודדים.
- אקדמי טרוול 2013 – מתמחה בארגון משלחות נוער לפולין ומסעות שורשים למבוגרים, לצד תיירות העשרה בעולם עבור מוסדות חינוך וארגונים. בנוסף, מתמחה החברה בהטסות רפואיות.
- ממסי תיירות – מספקת שירותים ופתרונות לנוסעים לחו"ל, בדגש על השכרת רכב בחו"ל, הנפקת רישיון נהיגה בינלאומי, הסדרת ביטוחים ופתרונות תקשורת.
- איסתא נכסים ואיסתא מלונות – שתי חברות בת העוסקות בתחום הנדל"ן המניב והמלונאי. באמצעותן רוכשת הקבוצה נכסים מניבים בישראל ובתי מלון בישראל ומחוצה לה. בבעלות החברות כיום, בין היתר, מתחם מעונות הסטודנטים בנתניה, בית קליפורניה, בית קמור ובית איסתא בתל אביב, מלון ברנר תל אביב, מלון כרמים בקריית ענבים ומלון שנמצא בשלבי הקמה בהרצליה פיתוח.

3. מערכות IT ו- IS -

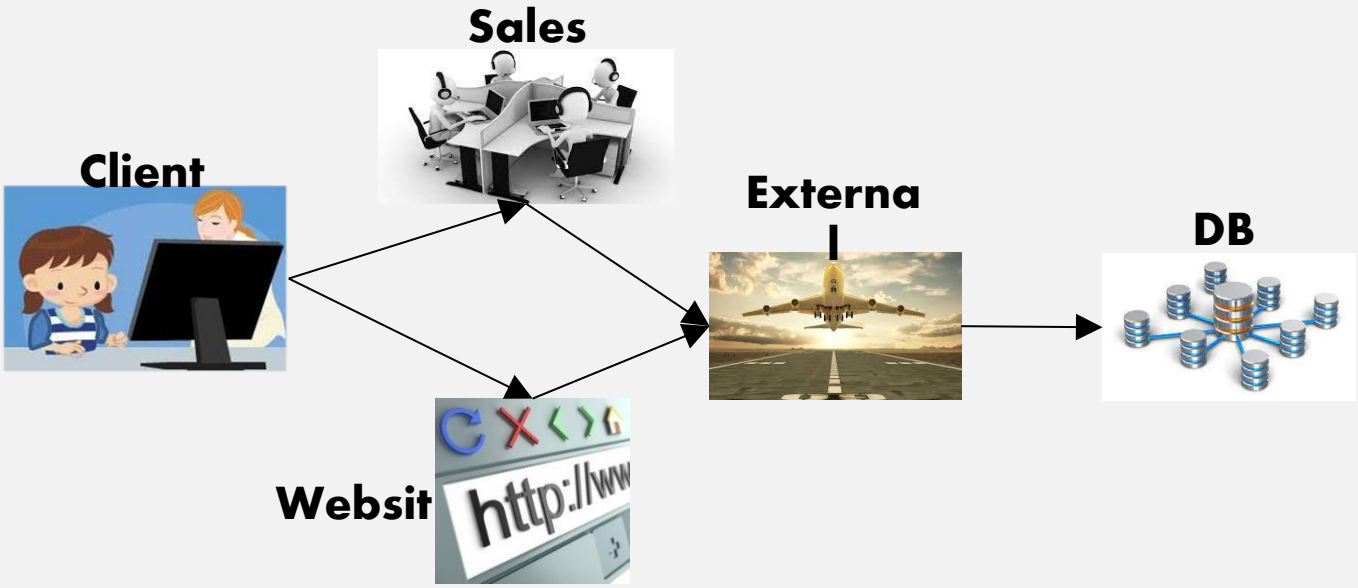
<u>Information Technology</u>

אתר איסתא מאובטח על פי התקן המקובל של פרוטוקול (Secured) SSL Sockets Layer זהו פרוטוקול להצפנת מידע באינטרנט המבטיח חסיון על הנתונים הנשלחים מהמחשב שלכם לאתר שלנו.
לסוכנויות נסיעות אין עוד גישה בלעדית לשלל לוחות הזמנים, התעריפים ופרטי היעד שנמצאים ב-GDS.
הספקים גם אימצו את האינטרנט כדרך להוזיל את עלויות הפצת מכירות הנסיעות שלהם והטכנולוגיה שוב משנה את הדרך שבה אנשים מזמינים נסיעות.
כמו כן בעידן שלנו, המדיה החברתית חשובה יותר לתכנון טיול, כמו גם לשימוש בטלפונים חכמים.

Information Systems

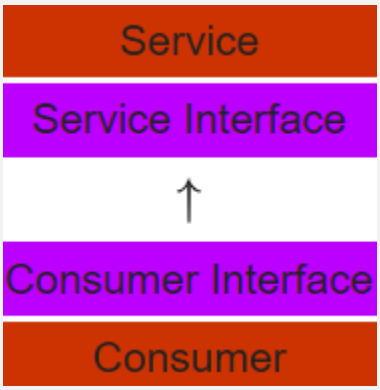
- סקירה של התפתחויות עכשוויות ונושאים מרכזיים בתחום התיירות וטכנולוגיית המידע.
- חשיבות ה-IT עבור ארגוני התיירות השונים.
- השפעת הרשת העולמית על גישות מכירה מסורתיות.
- מודלים של שימוש בטכנולוגיה. מאפיינים עדכניים של טכנולוגיות קיימות.
- מערכות בין ארגוניות בישראל.

4. ארכיטקטורה –



כפי שניתן לראות באיור הבא הלקוח מבצע הזמנה דרך האתר או דרך מוקד שירות הלקוחות. בשלב הבא מתבצע הממשק עם מערכות של ספקי התעופה והמלונאות, המידע שמגיע משרתים אלה מוצג ללקוח/נציג ובעת סגירת ההזמנה מתבצע העדכון ב-DB.

שיטה זו נקראת גם ארכיטקטורה מוכוונת שרתים או באנגלית SOA. כפי שניתן לראות באיור הבא:



בארכיטקטורת SOA השירותים הם למעשה אבני הבניין של יישומים. אנלוגיה פשטנית המתארת את מודל הרכבת היישומים מהשירותים היא בנייה באמצעות אבני לגו. בתהליך זה מתבצע חיבור קל בין אבנים שונות המאפשר הרכבת עצמים שונים באמצעות צירופים שונים של אותן אבנים. לשירות עשויים להיות מספר רב של צרכנים. המושג צרכן אינו שווה ערך למושג לקוח שמתקיים בארכיטקטורות קודמות כגון שרת-לקוח (Client-Server), זאת משום שלקוח הוא עמדת קצה מולה יושב משתמש אנושי, בעוד צרכן עשוי להיות לקוח אך יכול להיות גם שירות אחר.
ארכיטקטורה מוכוונת שירותים משמשת לאינטגרציה בין יישומים ולבניית יישומים.

חלק ב' – ניתוח סיכונים

5. סיכוני סייבר מהווים חלק משמעותי מכלל הסיכונים התפעוליים אליהם חשופות חברות ולהתממשותם עלולות להיות השלכות עסקיות שונות, לרבות :פגיעה במוניטין, אובדן הכנסות, חשיפה משפטית וכו .׳מטרות העל של תהליך ניהול סיכוני סייבר הן הפחתת הסבירות לפגיעה בתהליכים העסקיים ובמידע של הארגון כתוצאה מהתממשות סיכונים אשר מקורם במרחב הסייבר, וצמצום ההשפעה עליהם, במקרה שהתממשו סיכונים אלו.

6. רשימת נכסים –

א. אתר קניות מכירתי –
שם המערכת : כתובת אתר האינטרנט.
ייעוד המערכת : אפליקציה לרכישה מקוונת של מוצרי החברה.
רגישות : מידע לקוחות, נתוני טרנזקציה, נתוני אשראי.

ב. מערכת ניהול כספים -
ייעוד : ניהול התקציב, התזרים והתמחור של החברה.
רגישות : נתונים כספיים, נתוני חשבונאיים ופיננסים פנימיים המעידים על ביצועי החברה.

ג. מערכת ניהול רכש –
ייעוד : ניהול תהליכי הרכש בחברה.
רגישות : מידע עסקי ותפעולי על החברה.

ד. מערכת רב ערוצית –
ייעוד : ניהול התקשורת מול לקוחות החברה.
רגישות :נתונים לקוחות ונתוני עסקאות.

ה. דוא״ל –
ייעוד : שליחה וקבלת של הודעות וקבצים.
רגישות : מידע עסקי ותפעולי מסוגים שונים.

ו. שרת קבצים –
ייעוד : אחסון מידע וקבצים שונים.
רגיש : מידע הנהלה, פיתוח עסקי, נתוני לקוחות.

7. רשימת איומים וזיהוי פגיעויות –
א. גישה בלתי מורשית למחשבים אישיים של עובדים.

ב. דלף כרטיסי אשראי של לקוחות החברה.
ג. אי זמינות האתר כתוצאה מתקיפת סייבר.
ד. גישה לא מבוקרת של ספקים חיצוניים למערכת המלאי.
ה. רשת אלחוטית לא מאובטחת (נתב).
ו. דלף נתוני לקוחות אישיים משרתי החברה.
ז. דלף נתוני לקוחות ממערכת התקשורת הרב ערוצית.

8. ניתוח סיכונים (Risk Register) עפ״י טבלאות T14 –

א. נתב האינטרנט –
איומים : פריצת גורמים חיצוניים לנתב וגניבת מידע מהמחשבים.
מענה : הפקדה על גישה מינורית לנתב ע״י שינוי שם משתמש וסיסמא בתדירות גבוהה והחלפת שם הרשת.
סבירות : נמוכה
השלכות : גדולות
רמת סיכון : גבוהה

ב. פריצה לשרתי החברה -
איומים : פריצה של האקרים לשרתי החברה וגניבת מידע על לקוחות כגון כרטיסי אשראי ופרטים אישיים.
מענה : גישה מינורית לשרתי החברה לגורמים לא הכרחיים.
סבירות : אפשרי
השלכות : גדולות מאוד
רמת סיכון : גבוהה

ג. שרתי חברה ושרתי קבצים פנימיים –
איומים : התחממות של חדר השרתים והרס פיזי או הרס כתוצאה מאסון טבע.
מענה : הקפדה על מזגן קבוע בחדר השרתים ווידוא אטימות שלו.
סבירות : נמוכה
השלכות : גדולות
רמת סיכון : גבוהה

ד. מחשבים אישיים -

איומים : פריצה למחשבים של עובדים בארגון ע״י גניבה והפצת מידע של לקוחות או גניבת נתונים עסקיים על החברה והפצתם או שימוש לרעה.
מענה : הקפדה על נהלי אבטחת מידע, סיסמאות למחשבים ו-BITLOCKRER.
סבירות : אפשרי
השלכות : גדולות
רמת סיכון : גבוהה

ה. מערכת רב ערוצית -
איומים : פריצה למערכת הרב ערוצית והפצת נתונים על לקוחות או גניבת מידע על לקוחות בעת שיחתם עם נציגים.
מענה : הקפדה על שם משתמש וסיסמא לכל נציג, אי השארת מחשבים של נציגים ללא השגחה, שרתי ISOLATED.
סבירות : אפשרי
השלכות : גדולות מאוד
רמת סיכון : גבוהה

ו. חשבונות החברה ברשתות החברתיות -
איומים : פריצה לחשבונות החברה ברשתות החברתיות והצגת מידע שקרי ללקוחות + אובדן מידע קריטי.
מענה : הקפדה על שם משתמש וסיסמא למספר אנשים ספציפיים בארגון וגישה מינימלית לחשבונות.
סבירות : אפשרי
השלכות : גדולות מאוד
רמת סיכון : גבוהה

ז. חשבונות מייל של עובדי החברה -
איומים : פריצה לחשבונות אלה וגניבת מידע עסקי על לקוחות ועל החברה ונפצתו או שימוש בו לרעה כנגד החברה.
מענה : הקפדה על שם משתמש וסיסמא ונהלי אבטחת מידע כמפורט בסעיף ד׳.
סבירות : אפשרי
השלכות : גדולות
רמת סיכון : גבוהה

ח. זמינות ותקינות אתר הבית של איסתא -
איומים : פריצה של האקרים לשרתי האתר של איסתא, אי תקינות האתר למשך מספר שעות והצגת מידע כוזב ללקוחות הקצה.
מענה : גישה מינימלית לשרתי האתר ע״י מספר אנשים בארגון.
סבירות : אפשרי
השלכות : גדולות
רמת סיכון : גבוהה

9. נספח דירוג של טבלת סיכונים –

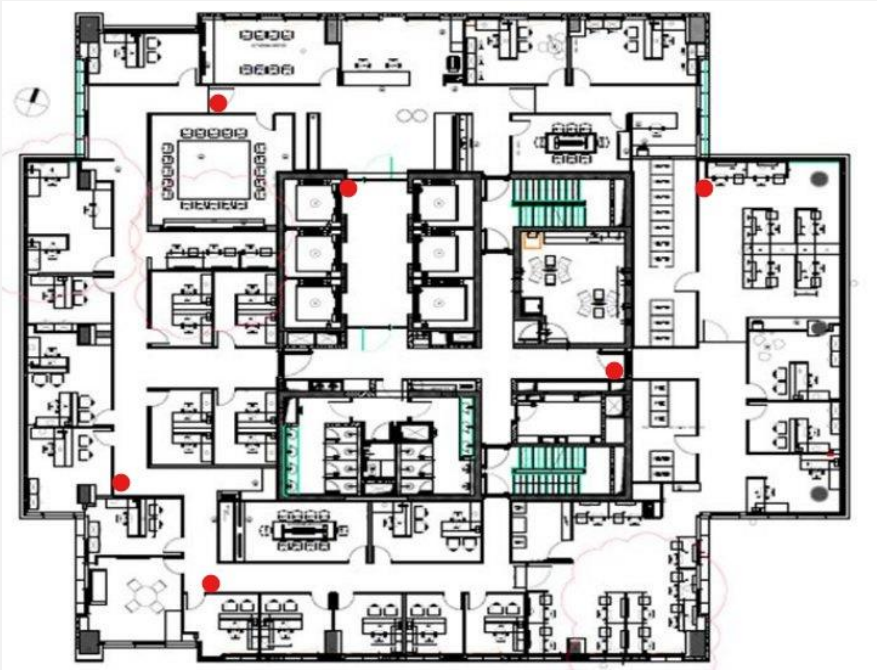
Risk priority	asset
1	שרתים
2	מאגר נתונים
3	הרס של מרכז נתונים
4	נתב אינטרנט
5	מחשבים אישיים
6	אתר הבית של איסתא
7	חשבונות של החברה ברשתות חברתיות
8	תקשורת
9	מיילים
10	ציוד משרדי

חלק ג' – אבטחת תשתיות ואבטחת הגורם האנושי

10. מודל אבטחה פיזית לארגון איסתא –

- שערים להולכי רגל , גדרות, מגרש חנייה, תאורה, שערים לכלי רכב.
- דלפק קבלה, מנעולים, שער מגנו, קוראי כרטיסים.
- שומרים בכניסה לבניין משעה 00 :07 עד שאחרון העובדים מסיים.
- מערך אבטחה בכניסה לבניין – מגנומטר, בדיקת תיקים וכד.
- כרטיס כניסה לכל עובד הארגון או אם אינו עובד אז אישור כניסה מדרג בכיר.
- מצלמות אבטחה מבוזרות בכל קומה.
- מרכז בקרה ושליטה 24/7.
- תדריך אבטחה לשומרים כל החלפת משמרת.

איור 1 - מערכת שליטה ובקרה אבטחתית



איור 2 - מיקומי מצלמות אבטחה בקומת המשרדים הראשית ***(מסומנות באדום)***

11. אבטחת הגורם האנושי –

א. סיווג קבוצות עובדים -

- דרג בכיר (מנכ״ל) – הרשאה כללית, למנכ״ל יש הרשאה להתחבר לכל מחלקה ואת סיסמאות המחשבים.
- סמנכ״לי ארגון – הרשאה לפי תחום האגף כלומר סמנכ״ל כספים צריך גישה לשכר העובדים וסמנכ״ל שימור לקוחות צריך גישה לנתוני הלקוחות (טלפונים אימליים וכד).
- מנהלי צוות – הרשאה לפי צוות ספציפי כלומר אחראי צוות פיתוח תוכנה צריך גישה למחשבי העובדים העוסקים בפיתוח.
- עובדים – הרשאה לכל מחשב אישי של העובד לפי רמת הסיווג שלו.
- מחלקת תשתיות – הרשאה כללית, מתן הרשאות לעובדים חדשים.

ב. שיטות ואמצעים ארגוניים נוספים -

- ביצוע הרצאות שמטרתן לעלות את המודעות של עובדי הארגון
- קביעת נהלים ומדיניות לתהליכים עסקיים אשר נערכים דרך המייל
- שימוש בפתרון הגנה מתקדם עד לרמה שבה הוא חוסם את דוא״ל ההונאה עוד לפני שהוא מגיע לדואר הנכנס של העובדים.
- השקעה בסיסמאות- איסור על שימוש חוזר באותה סיסמא.
- איסור מסירת נתונים רגישים בלי בירור ואישור של דרג בכיר.
- איסור על הוצאת חומר חסוי מהארגון, במידה ונדרש להוציא חומר כזה נדרש לקבל אישור מיוחד של הממונה לאבטחת מידע.
- עזיבת עמדת העבודה, כאשר עובד עוזב את עמדתו לכמה רגעים או בתום יום עבודתו חשוב להקפיד לבצע יציאה מסודרת מכל מערכות המחשבו או לנעול זמנית את המחשב.
- הקפדה על קיום מדיניות שולחן נקי הכולל שולחן עבודה נקי מכל ניירת או מדיה בסיווג חסוי כולל גריסת כל נייר השייך לארגון שאין בו עוד צורך ובפרט מידע חסוי.
- שימוש בציוד הארגון, איסור על הכנסת גורם חיצוני למחשבי החברה כמו דיסק און קי, דיסק חיצוני, חיבור טלפון סלולרי למחשב, הורדת תוכנות כגון אנטי וירוס ושינוי הגדרת המחשב.
- התקנת תוכנות הגנה והצפנת מידע על ידי מחלקת אבטחת מידע.

חלק ד' – היבטים משפטיים

12. החקיקה הרלוונטית לארגון הנבחר –

א. סיכונים משפטיים בשל אירועי סייבר בארגון –

- פגיעה ברצפיות התפקודית וכתוצאה מכך הפרת התחייבויות חוקיות או רגולטוריות.
- גניבת קניין רוחני ובפרט דליפת סודות מסחריים.
- הפרת דיני פרטיות במידע בשל דליפה של מידע על עובדים או לקוחות.
- פגיעה במיהמנות מערכות המידע של הארגון והיכולת להסתמך על המידע השמור.

ב. היערכות מקדימה לטיפול באירוע סייבר –

- נקיטת אמצעים סבירים רלוונטיים להתמודדות עם אירוע סייבר – צעדים משמעתיים כגון קנסות ואף פיטורי עובד.
- עובד אשר היה שותף ונמצא אשם באירוע סייבר יועמד לוועדת משמעת תוך ארגונית.

ג. מדיניות ארגונית בהיבטי הגנת סייבר –

- גיבוש מדיניות ארגונית ברורה המבהירה לעובדים את המותר והאסור בשימוש המערכות המידע והארגון.
- הבאת עיקרי המדיניות, לידיעת העובדים לרבות ריענון תקופתי.
- הסתמכות על כללי פעולה מקובלים בתחום.
- שימוש בהודעות על המסך/עדכונים/רענונים.

13. מקורות –

א. ספרו של Stallings, פרק 14.

ב. דוגמא לסקר סיכונים באתר הממשלה, קישור - https://www.gov.il/BlobFolder/policy/retailrisk/he/%D7%A1%D7%A7%D7%A8%20%D7%A1%D7%99%D7%9B%D7%95%D7%A0%D7%99%D7%9D%205.4.20.pdf

ג. דוגמאות לטבלאות סיכונים מאתר CyberSaint, בקישור - https://www.cybersaint.io/blog/risk-register-examples-for-cybersecurity

ד. ויקיפדיה, ארכיטקטורה מוכוונת שירותים - https://he.wikipedia.org/wiki/%D7%90%D7%A8%D7%9B%D7%99%D7%98%D7%A7%D7%98%D7%95%D7%A8%D7%94_%D7%9E%D7%95%D7%9B%D7%95%D7%95%D7%A0%D7%AA-%D7%A9%D7%99%D7%A8%D7%95%D7%AA%D7%99%D7%9D

ה. ויקיפדיה, איסתא - https://he.wikipedia.org/wiki/%D7%90%D7%99%D7%A1%D7%AA%D7%90_%D7%9C%D7%99%D7%99%D7%A0%D7%A1#%D7%94%D7%97%D7%96%D7%A7%D7%95%D7%AA