מבקר המועצה האזורית הגלבוע

ביקורת

אבטחת המידע במועצה האזורית הגלבוע

דוח ביקורת לשנת 2014 – תוכן מסמך זה אסור לפרסום ללא אישור מבקר מ.א הגלבוע

כללי

אבטחת מערכות מידע

זוהי פעילות שמטרתה להגן על מערכות המחשב מפני איומים וסיכונים.

האבטחה על מערכות המידע כוללת אבטחה פיזית של המבנה בו נמצאות מערכות המחשב , אבטחה של מערכות החומרה והתוכנה ואבטחה של המידע שנאגר בהן.

ישנם מאגרי מידע רבים הנמצאים על גבי מחשבים עם גישה לאינטרנט , מאגרים אלו משמשים בין השאר מדינות , תאגידים.

אך גם למאגרי מידע שאינם יכולים להתחבר לאינטרנט , ניתן לגרום נזק באמצעות גישה ישירה שאינה באמצעות הרשת.

במציאות של היום מתחייב השימוש במערכות מידע , בארגון כמו רשות מקומית. לא ניתן לתפעל כמעט את המועצה האזורית , החולשת על 34 יישובים , בלעדיהן.

התפתחות המערך הטכנולוגי המסייע לפעילות הארגונית , כולל בתוכו את מערכות המידע אשר תומכות , והמערך הטכנולוגי מאפשר באמצעותן , התייעלות בפעילות הכוללת של המועצה האזורית.

עם זאת יש לקחת בחשבון את הסיכונים והאיומים על פעילותה של המועצה האזורית , והמידע האגור במערכות המידע שלה , בכפוף לשימוש במערכות המידע.

בין הסיכונים ניתן לצפות שיבוש הפעילות השוטפת , מניעת הצגת התוצאות להן המועצה האזורית מחויבת , וחדירות למערכות המידע אשר עשויות לחשוף את המועצה האזורית לתביעות משפטיות .

כמו כן יתכן שיתוק חלקי או מלא של מאגר המידע עד כדי התמוטטותו.

פעולות הביקורת

מפאת חשיבות הנושא, מבקר המועצה השתתף במהלך החודשים נובמבר 2014 – מרץ 2015 , בקורס הכשרה מטעם משרד הפנים – ביקורת מערכות מידע.

התקיימו מספר ישיבות עבודה עם מנהל מערכות המידע במועצה הן במסגרת הסקר המקדים לביקורת וכן במהלך הביקורת , בזמן אמת.

בנוסף התקיימו פגישות עם מומחים חיצוניים בתחום על מנת שניתן להעריך את הסיכונים בתחום בצורה אובייקטיבית וכן לבצע בקרה לתהליך הביקורת.

המסגרת הנורמטיבית

אסטרטגיית אבטחת המידע בארגון , איננה פעולה חד פעמית של כתיבת מסמך ודיווחו לכל המשתמשים במערכות המידע בארגון.

מדובר בתהליך מתמשך המתחדש בהתאם לסיכונים ולאיומים המשתנים.

האסטרטגיה המפורטת למדיניות , מכילה :

קווי מדיניות , סטנדרטים , נהלים , הנחיות , כליי הרשאות וגישה וסיווג המידע לפי רגישותו.

הוראות חוק להגנת הפרטיות ותקני ISO

1. **החוק להגנת הפרטיות מחייב את הרשויות המקומיות לעמוד בדרישותיו , בנושא אבטחת המידע.**
2. **תקן ISO 17799 איננו מחייב את המועצה האזורית , אך עמידה ב- 10 הקריטריונים שפורטו בו יש בהם כדי להצביע ולשמש בסיס להשוואה למידת איכות אבטחת המידע בין הארגונים השונים (וגם בין הרשויות המקומיות השונות).**
3. **התקן מפרט כאמור 10 קריטריונים :**

א. מדיניות אבטחת מידע.
ב. ארגון אבטחת מידע.
ג. בקרת המידע וסיווגו.
ד. אבטחת הסגל.
ה. אבטחת סביבת העבודה ואבטחה במישור הפיזי.
ו. ניהול וכללי עבודה עם המידע.
ז. בקרת הגישה.
ח. יצירת מערכות ותמיכה.
ט. אבטחת פעילות תקינה של המערכות.
י. תיאום.

תכנית הביקורת ומטרותיה :

הביקורת נערכת כתוצאה מהערכת סיכונים שנערכה במועצה.

תכנית הביקורת :

1. סקר מקדים לביקורת.
2. סקירת מסמכים .
3. אפיון סרגלי הביקורת בתחום.
4. פגישות וראיונות עם מומחים פנימיים וחיצוניים למערכת.
5. בדיקות מבוקרות במערכות המידע במועצה.

מטרות עריכת הביקורת בתחום אבטחת המידע במועצה האזורית הן :

1. בחינת מידת הסיכון לו נחשפת המועצה האזורית , בשימוש מנגנוני הבקרה המיושמים באופן שוטף בתחום.

2. בחינת אסטרטגיית ההגנה על מערכות המידע במועצה האזורית , באמצעות אפקטיביות הבקרות המיושמות במערכות המידע , במועצה האזורית.
3. ניסוח המלצות אפקטיביות לתיקון הממצאים (בתוכם הליקויים) , אשר יאותרו.

טיוטת ממצאים

להלן הממצאים שנאספו לגבי אבטחת מערכות מידע במועצה

האזורית הגלבוע :

1. **עמדות מחשבי המועצה חשופים לסיכונים הנובעים , כתוצאת היותן פתוחות לאורך זמן , מבלי ששומר מסך הופעל תוך זמן סביר.**
2. **המחשבים אשר ממוקמים בעמדות רגישות , אינם מאובטחים כראוי , והסיכון בעמדות רגישות אלו , מוגבר.**
3. **הסיכונים הללו מגבירים את ההסתברות לחדירות פיזיות עוינות למחשבי המועצה ועלולים לגרום לתביעות משפטיות , נגד המועצה.**
4. **סיכוני החדירות הפיזיות לעמדות המחשב , הפרוצות לכאורה , יכולות לשתק באופן חלקי או מלא , עד כדי פגיעה קשה בתפקוד מערכות המידע , במועצה האזורית הגלבוע.**
5. **עמדות מערכות מידע רגישות , ממוקמות אצל ראש המועצה או המוסמך מטעמו לצורך חתימות דיגיטליות (אחת משתי החתימות הנדרשות) , במחלקת הגזברות , במחלקת הרווחה ובמחלקת הארנונה.**
6. **תקן 17799ISO , בתחום מערכות המידע (אבטחת מידע) , לא מיושם במלואו.**
7. **שירותי האינטרנט האלחוטי במועצה האזורית הגלבוע, שסופקו בעבר על ידי המועצה , ניתנים כיום על ידי ספק חיצוני למערכת המועצה, שינוי שהתבצע לפני כשנתיים. השינוי המבורך הקטין בצורה משמעותי פריצות ופגיעה במערכות המידע של המועצה.**

   היות והשימוש באינטרנט האלחוטי לא מאפשר כניסה דרך

   מערכות המידע של המועצה כבעבר.

8. **השרתים של המועצה ממוקמים במקלט , אשר יש בו שימושים נוספים כמו : אחסון ארכיון , קליטת עובדים ומבקרים בעת אזעקות ובמצבי חירום ועוד.**
9. **אין כעת במועצה פרוטוקול חירום חרום מעודכן למכלול מערכות מידע החיוני ביותר למצבי חירום במועצה.**
10. **בעת הזו אין תיק מקביל להפעלת מערכות המידע במועצה.**
11. **אבטחת נתוני שעון הנוכחות , לא הוצגו על ידי מנהל מערכות המידע.**

בתגובה לטיוטת הממצאים מסר ב-20.5.15 מר רונן בגים מנהל מערכות המידע במועצה , את תגובתו :

אייל בוקר טוב,

בסעיף 1, ברצוני להבהיר כי אין חובת נעילת מחשבים ע"י שומר מסך בשום מקום ושום רשות על פי מה שאני יודע...

וכפי שציינתי בשיחתנו, במידה ויגובש נוהל כזה אין בעיה ליישמו במידי, מה גם שאני לא מוצא כל בעיה למעט אי נוחות למשתמשים שיחויבו בהכנסת סיסמה מידי כמה דקות של חוסר פעילות במחשב.

בסעיף 2, בדומה לסעיף 1 , המערכות מוגנות בסיסמת כניסה לרשת וכן במשרדים נעולים בד"כ.

ע"מ להעלות את רמת האבטחה ניתן להוסיף מס' רבדים שיסייעו בהוספת קשיים על ניסיונות פריצה למערכת , כגון קורא טביעת אצבע לכניסה למערכת.

פעולות אלו ,חייבים לציין , לעיתים מסרבלות משמעותית את העבודה ולכן צריך למצוא את שביל הזהב בין אבטחת המידע הרצויה לבין חווית העבודה במחשב.

כל החלטה ניתן ליישם די במהירות ולרוב בעלויות לא גבוהות, אך לעתים על חשבון הנוחיות של המשתמש.

במידה ויוחלט על צעדים משמעותיים יותר יש לבחון את העלויות מול התועלת שתופק מצעדים אלו.

כל מקרה, מכיוון שאנו מחוברים דרך החברה לאוטומציה בתשתיות התקשורת והאינטרנט, רמת אבטחת המידע מפגיעה חיצונית היא טובה מאוד, אך כמו כל מערכת מחשוב מעצם היותה מחוברת לעולם , חשופה לניסיונות פריצה.

מכיוון שכך, יש לבחון באופן שוטף את האמצעים להגנה מכסימלית מפני פגיעה במערכת, מה גם שמבחינה טכנולוגית מתבצעים שיפורים תמידיים

בתחום והעלויות מצטמצמות בהתאם...

אשמח לסייע בכל שאלה או בקשה נוספת...

בעקבות הוצאת טיוטת דוח סופית התקיים דיון ב-29.6.15 בראשותה של מזכיר המועצה אליו גם זומן מבקר המועצה.

להלן פרוטוקול הדיון בטיוטת דוח הביקורת :

מ.א. הגלבוע – מחלקת מחשוב

29/06/15

סיכום ישיבת אבטחת מידע והמלצות פעולה לדו"ח המבקר בשנת 2014

נוכחים:

אילנה חייט , ג'ואד זועבי, אייל פייגנבאום, רונן בגים

אייל: במסגרת קורס ביקורת מערכות מידע מטעם משרד הפנים השתתפתי , ערכתי סקר אבטחת מידע במועצה והוצאתי דוח טיוטת ממצאים שהועבר לרונן ולאילנה . את התהליך ליווה רונן ובוצע בשיתוף פעולה עם מומחה מערכות מידע.

נבדקו האפשרויות התאורטיות לחדירה למחשבי המועצה מבחוץ וכן שימוש עוין מתוך המועצה , הן ע"י עובדים לא מורשים והן ע"י אורחים.

שינוי השימוש באינטרנט האלחוטי במועצה לרשת אלחוטית חיצונית ע"י מח' מחשוב , הקטין בצורה משמעותית את הסיכון לחדירות למחשבי המועצה , מפני שהפרדת הרשתות ביטלה את האפשרות לכניסה לא מורשית דרך רשתות אלחוטיות לרשת המועצה.

בעקבות ההחלטה על השינוי , לפני כשנתיים וחצי הוסב קו בזק לחיבור אינטרנט אלחוטי ע"מ שכל אורח / עובד אשר זקוק לחיבור אינטרנט , יוכל לעשות זאת ברשת מנותקת לחלוטין מרשת המועצה.

ממליץ להוסיף רובד אבטחה פיזית לקיים , בהסכמת הגזבר ומבלי לפגוע , עד כמה שניתן בידידותיות השימוש במחשב.

יש מספר עמדות שמצריכות לפי דעתי את תוספת האבטחה הפיזית : ראש המועצה, בגזברות, ארנונה , רווחה.

בנוסף יש לאתגר את מערכות המידע במועצה , בניסיונות יזומים לחדירה מבחוץ שיפעלו כבקרה על השירותים הניתנים על ידי החברה לאוטומציה החדשה.

ג'ואד: מבחינתי אין בעיה.

רונן: ישנם כמה אמצעי הגנה כמו כרטיס מגנטי, דיסק און קי וקורא טביעת אצבע.

ממליץ על קורא טביעת אצבע כי אין בו שום אביזר שצריך להחזיק או לזכור להוציא לאחר כל שימוש. הערכת קורא טביעת אצבע לעמדה – כ 700 ₪.

אילנה : ימונה רכז לנושא אבטחת המידע מהצוות הקיים.

הנהלים בנושא יגובשו ע"י חברה חיצונית שתמונה ע"י המועצה.

בקרה וניסיונות חדירה למערכת יבוצעו ע"י החברה לאוטומציה.

מבקשת לדעת כמה עמדות רגישות ישנן במועצה ולפי זה תתקבל החלטה היכן יותקן אמצעי אבטחה נוסף.

ההמלצה המקובלת על כולם היא טביעת אצבע .

רשם: רונן בגים

<u>בעקבות הדיון התקיימו מספר פגישות עבודה נוספות עם מנהל מערכות המידע במועצה .מהפגישות עלו ממצאים נוספים ולפיכך נוספו מספר המלצות לטיוטה סופית 2 של דוח הביקורת.</u>

<u>הממצאים נוספו בפרק הממצאים וההמלצות לפרק ההמלצות.</u>

<u>חרגתי ממנהגי כאן בהוצאת גרסה נוספת לטיוטה סופית לדוח , אך מכיוון שהנושא בעל חשיבות גבוהה בהיבט הסיכונים להם המועצה נחשפת כיום , מן הראוי היה לטעמי להוסיף את הנדרש , על מנת שתיקון הליקויים יוכל להתבצע באפקטיביות הנדרשת.</u>

בעקבות קבלת טיוטה סופית 2 על ידי מנהל מערכות המידע , נוספה על ידו התגובה הבאה , במסגרת מכתב שהוציא למנהל מחלקת רישוי עסקים במועצה , בהקשר לממצאים שנוספו לטיוטה הסופית 2 :

מיקי בוקר טוב,

בשיחה שערכתי עם משה טנג'י מרמה מערכות עולה שניתן לעבוד , מעבר לצורה בה אנו עובדים כיום , בעוד מס' אפשרויות:

1. לשמור עותק של בסיס הנתונים לאמצעי אחסון כלשהו (תקליטור, דיסק נייד, דיסק און קי) ולהוציאו מחוץ למועצה כגיבוי.

2. לאחסן את בסיס הנתונים באמצעי אחסון בענן ולגשת אליו בכל הפעלה.

3. להפעיל את כל התוכנה דרך שרת בענן ע"י השכרת משתמש ושטח אחסון בשרת מחברה חיצונית.

יש לבחון את האפשרויות הרצויות והמשמעויות של כל אחת ע"מ לבחור את האפשרות המועדפת לעבודה.

אופציות 2, 3 מגדילות את התלות שלנו בקווי תקשורת ואת הסיכון להשבתת העבודה במקרה של תקלה בקווים.

למרות הנאמר, הן נותנות רובד נוסף לגיבוי הנתונים ומאפשרים במקרה של אסון את המשך התפקוד.

במידה ויוחלט לבצע מי מהאפשרויות שהועלו , נדאג להצעת מחיר מסודרת ומעודכנת.

מנהל רישוי עסקים במועצה מסר למבקר המועצה , כי הוא ממתין לקבל הצעת מחיר מסודרת לגיבוי , מסד נתוני רישוי העסקים במועצה.

המלצות

1. מדיניות אבטחת המידע , איננה פעולה חד פעמית של כתיבת מסמך , אלא תהליך מתמשך ומתחדש בהתאם לסיכונים ולאיומים , קווי מדיניות , סטנדרטים , הנחיות , נהלים , כללי גישה , הרשאות וסיווג מידע ע"פ רגישותו.
2. על הנהלת המועצה למנות רכז אבטחת מידע , מבין העובדים במועצה , אשר ייחד חלק מזמן עבודתו בין השאר , להשבחת תחום אבטחת המידע במועצה האזורית הגלבוע.
3. יש לאיגום תקציב לפעילות חשובה זו היכולה להקטין בצורה משמעותית , אם תעשה באופן שוטף , את הסיכונים למערכות המידע במועצה בתחום אבטחת מערכות המידע.
4. יש לבצע בקרות פנימיות לא מתוכננות , באמצעות ניסיונות חדירה למערכת על מנת לבדוק פרצות באבטחת המידע במועצה.
5. המלצה 4 מקבלת דגש בעקבות פריצות חיצוניות מרחוק שמתרחשות בארגונים , בשנים האחרונות. מכאן שיש להתמקד בניסיונות פריצה מרחוק , על מנת לבדוק את עמידות המערכת וחשיפת חולשותיה , אם קיימות.
6. יש לוודא כי מידע רגיש הנמצא במערכות המידע של המועצה , שחלקו אף מתייחס לצנעת הפרט , לא ייחשף כתוצאה מחדירה בלתי מורשית לעמדות מערכות המידע במועצה , או באמצעות פריצה מבחוץ. (רוב האיומים (סיכונים) בתחום כיום).
7. יש לשקול להוסיף בקרת כניסה נוספת בעמדות מערכות המידע הרגישות במועצה. כמו: עמדת ראש המועצה , עמדות במחלקת הכספים כולל עמדת הגזבר, ארנונה ורווחה.
8. עמדות אלה מאפשרות פעולות שיש לוודא כי רק בעלי ההרשאה עצמה יוכלו לבצעה. (חתימות דיגיטליות , ביצוע פעולות כספיות, צנעת הפרט).
9. בקרת הכניסה הנוספת למערכת המידע יכולה להתבצע תוך בחירה מתוך שתי האפשרויות הבאות :

א. הכנסת דיסק און קי ייעודי לפני מתן הסיסמא כתנאי כניסה לעמדה.
ב. עמדת טביעת אצבע המותאמת למורשה בלבד, בעמדת מערכת המידע.

החלופה המועדפת להקטנת הסיכון לשימוש אדם אחר מבעל ההרשאה הינה חלופת טביעת האצבע. יש לבחון הוספת הבקרות בהדרגה תוך בחינת החלופה המועדפת גם בבחינת סרבול השימוש , אך גם מנגד, מזעור הסיכונים.

10. **תקן ISO 17799 , בתחום מערכות המידע (אבטחת מידע) , לא מיושם כאמור במלואו. לפיכך יש לשאוף להשביח את התנהלות המועצה בתחום מערכות המידע , כארגון לומד ולהגדיל את העמידה ברכיבים שבתקן.**
11. **יש להכין בהקדם פרוטוקול חירום , בתחום מערכות מידע למועצה. יש לעדכן את מכלולי החירום בפרוטוקול זה.**
12. **יש להכין בהקדם תיק מקביל , שיאוחסן בכספת לשימוש בעת נבצרות מנהל מערכות המידע. יש לקבוע בנוהל אדם שיהיה אחראי לתפעול המערכות במקומו בעת נבצרות.**
13. **יש לבדוק את רמת אבטחת המידע לשעון הנוכחות לעובדים.**
14. **במידת הצורך יש לשפר את אבטחת שעון הנוכחות.**
15. **יש לשלב את מנהל מערכות המידע במועצה בכל דיון בו נדרשת חוות דעתו המקצועית בתחום , כמו גם במכרזים בתחום.**
16. **יש לוודא שכל מאגרי הנתונים , במנהלים , אגפים ויחידות הסמך במועצה מגובים כראוי , בהתאם לסטנדרטים המקובלים והעדכניים בתחום. אין ספק שהגנה כזו על הנתונים יכולה להקטין בצורה משמעותית את הסיכונים לה נחשפת המועצה בתחום מערכות המידע. מערכות המידע משמשות כיום בכל תחום בו פועלת המועצה . מערכות המידע במועצה הינן כלי בעל ערך יקר ביותר בכל הקשור לשירות לתושבי המועצה.**