רכבת ישראל
פשוט ליהנות מהדרך

הנדון: <u>הנחיות לעבודה מול ספק שירותי ענן</u>

סימוכין:

1. מסמך הרחבה לתורת ההגנה בסייבר בארגון – שימוש בשירותי ענן גרסה 1.0 של הרשות הלאומית להגנת הסייבר
2. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז 2017

<u>רקע</u>

4 לאחרונה קיים גידול משמעותי לדרישות לשימוש במערכות מבוססות מחשוב ענן ברכבת ישראל.

5 דרישות אלו מגיעות ממגוון מקורות, כגון פרויקטים טכנולוגיים, מערכות המפותחות בחברה, והן בדמות פתרונות/מערכות המסופקות ע"י קבלנים חיצוניים.

6 מסמך זה מכיל דרישות סף לעבודה מול רכבת ישראל.

7 <u>הנחיות לעבודה מול ספק שירותי ענן</u>

פרק זה סוקר כללי אבטחה מומלצים לעבודה מול ספקי שירות ענן במטרה לצמצם את מס' סוגיות האבטחה והאיומים עמם נדרשת רכבת ישראל להתמודד.

7.1 הנחיות כלליות טרם המעבר לענן

בעת בחירה של ספק ענן יש לפעול ע"פ ההנחיות הבאות:

- לבחון לעומק את הסכם רמת השירות (SLA) וההתחייבויות החוזיות (Contractual obligations) אליהם מתחייב ספק שירותי הענן ולוודא כי הם עומדים בדרישות רכבת ישראל ודרישות רגולטוריות שונות בהתאם למידע והשירות בו נעשה שימוש.
- לערב גורמים מטעם אבטחת המידע והאגף המשפטי בזמן תהליך המשא ומתן וכתיבת החוזים עם ספק שירותי הענן.
- לוודא כי הספק מחויב לחוזה שנחתם הן בזמן מתן השירות והן בסיומו.
- לבצע מדידה של רמת הביצועים והאפקטיביות בניהול אבטחת המידע של המערכת כפי שקיימת ברכבת ישראל טרם המעבר לענן תוך שימוש בסטנדרטי מדידה אחידים ותיעוד מלא של

הנתונים. על רכבת ישראל לבחון ולהבין כיצד ישפיע המעבר לענן על הביצועים והאפקטיביות בניהול אבטחת המידע של המערכת המיועדת להעברה לענן.

- לבחון את יכולות המעקב אשר מציע ספק שירותי הענן ולוודא כי ניתן לבצע מעקב אחר פעולות שונות הנעשות במערכת בהתאם לדרישות/צרכי רכבת ישראל.
- לוודא כי הספק מאפשר ביצוע ביקורות אבטחה הכוללות סקרי סיכונים ומבדקי חדירה למערכות רכבת ישראל בענן.
- לוודא כי הספק ערוך להתמודד עם גדילה עתידית של צריכת משאבים (נפח אחסון, כוח עיבוד, רוחב פס וכו') בהתאם לצרכי רכבת ישראל.
- לבחון ביסודיות את מסמכי המדיניות, נהלים ותהליכי העבודה על פיהם עובד הספק ולוודא כי הם תואמים לדרישות רכבת ישראל. בפרט יש לבחון את הנהלים הבאים:
  - Information Security Policy – מדיניות אבטחת המידע.
  - Physical and environmental security – נוהל אבטחה פיזית וסביבתית.
  - Human Resource Security – נוהל אבטחת מידע במשאבי אנוש.
  - User Management Procedure - נוהל בקרת גישה וניהול משתמשים.
  - Audit Policy – מדיניות תיעוד ובקרה.
  - Back-up and restore Policy – מדיניות גיבויי ושחזור נתונים.
  - Hardening Policy – מדיניות הקשחת שרתים (במידה ומנוהלים ע"י הספק).
  - External Party Management – מדיניות עבודה עם צדדים שלישיים.
  - Security Incident Response – נוהל תגובה לאירועי אבטחת מידע.
  - Risk Analysis – מסמך ניתוח סיכונים.
  - Risk Assessment – מסמך הערכת סיכונים.
  - Vulnerability Assessment – ניתוח פגיעויות.
  - Business Continuity Plans – תכניות המשכיות עסקית.
  - Disaster Recovery Plans – תכניות התאוששות מאסון.
  - User Account Termination Procedures – נהלי סגירת השבונות משתמשים
  - Background Check Reports of Security Staff - בדיקות רקע שבוצעו על סגל העובדים (יש לבחון מדי שנה).

  בעת בחינת המסמכים יש לשים דגש על הדברים הבאים:
  - לוודא כי המסמכים מעודכנים, עברו בקרה שנתית של ספק שירותי הענן וכי קיימת חתימה של הנהלת ספק השירות.
  - לוודא כי מסמכים אשר צריכים להיות נגישים לעובדי הספק, שמורים באתר פנימי שיתופי כך שגורמים מורשים יוכלו לגשת אליהם בכל עת.
  - לוודא כי הספק ערוך מפגשי העלאת מודעות לאבטחת מידע לפחות אחד לשנה לצורך חידוד הנהלים.
  - לוודא כי הספק ערוך מפגשי אבטחה לעובדים חדשים לצורך מעבר על מדיניות אבטחת המידע, נהלי אבטחה ותהליכי העבודה.

7.2 רגולציה ומשפט:

- יש ליצור תהליך מוסדר למול ספקי שירותי הענן בעת קבלת שירותים בענן תוך החתמת הספק על חוזה התקשרות אשר יכלול בין היתר התחייבויות כגון:
  - מינוי ממונה אבטחת מידע מטעם הספק אשר יהיה אחראי על אבטחת המידע הנכלל במאגרי המידע המצויים בידי הספק וכן על יישום ההנחיות של רכבת ישראל בנושאי אבטחת מידע.
  - שמירה על סודיות.
  - נשיאת אחריות המוטלת על הספק בנוגע למידע ואבטחתו.
  - תיעוד ודיווח על אירועים אשר יש בהם משום פגיעה בשלמות, סודיות וזמינות המידע.
  - ביצוע מחיקה מלאה של מידע משרתיו ומאמצעי הגיבוי השונים בעת סיום החוזה עם רכבת ישראל והצגת הוכחות למחיקתו של המידע.
- יש לבדוק מול ספק שירותי הענן היכן נשמר המידע (פיזית – באילו מדינות) בפועל ולבחון את החוקים בהם נדרש הספק לעמוד הנוגעים לשמירה על פרטיות וסודיות המידע. לדוגמא: באסיה פסיפיק מדינות רבות אימצו את חוקי OECD[1] ו-APEC[2]. יש לוודא כי דרישות אבטחת המידע בחוקים בהם נדרש הספק לעמוד אינן פוחתות מדרישות החוק במדינת ישראל. בנוסף, יש לבחון כיצד חוקים אלו משפיעים על רכבת ישראל.
- GDPR עמידה בתקן רגולציית **הגנה על פרטיות**, הספק נדרש לפרט מהן ההוראות המחייבות שהוא מקיים כדי לעמוד בתקן זה.
- יש לבחון את הסכמי הספק עם צדדים שלישיים, ולוודא שאלו אינם מאפשרים חשיפת מידע של רכבת ישראל לגורם צד שלישי ללא אישור של רכבת ישראל.

7.3 עמידה בתקני אבטחת מידע

- יש לוודא כי הספק עומד בתקני אבטחת מידע מובילים ומחמירים בתחום ה-IT ובעדיפות לתקנים ייעודיים לענן:

<u>להלן רשימת תקני אבטחת מידע מקובלים בתחום ה-IT אשר הינם ייעודיים/מותאמים לסביבות ענן:</u>

- ISO/IEC 27017[3]
- ISO/IEC 27018:2014[4]
- ISO/IEC 27036-x[5]
- AICPA SOC 2/3[6]

<u>להלן רשימת תקני אבטחת מידע בינלאומיים מקובלים נוספים אשר אינם ייעודיים לענן:</u>

- ISO/IEC 27001[7]/27002

[1] OECD - Organisation for Economic Co-operation and Development
[2] APEC - Asia-Pacific Economic Cooperation
[3] Cloud Computing Security and Privacy Management System Security Control
[4] Information technology - Security techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds
[5] Information technology - Security techniques - Information security for supplier relationships
[6] American Institute of Certified Public Accountants - Service Organization Control
[7] Information technology - Security techniques - Information security management systems - Requirements

- PCI DSS[8]
- COBIT[9]

7.4 אבטחת מידע בתנועה (Data in transit)

- יש להעביר מידע אשר נמצא בתנועה כגון מידע העובר בין רכבת ישראל לענן, בין ספקי ענן שונים או בין רכיבים שונים בתוך הענן, על גבי תווך תקשורת מוצפן (SSL/IPSEC/VPN/SSH וכו').
- יש לנטר את כל פעולות העברת המידע בין רכבת ישראל לספק ע"י אחד או יותר מהאמצעים הבאים להפחתה/מניעה של העברת מידע בלתי מורשה לענן:
  - Database Activity Monitoring (DAM) – יאפשר איתור פעולות מגרציה של נתונים.
  - File Activity Monitoring (FAM) – יאפשר איתור פעולות מגרציה של קבצים.
  - URL Filtering – יאפשר ניטור וחסימה של משתמשים המתחברים לשירותי ענן.
  - Data Loss Prevention (DLP) – יאפשר ניטור וחסימה של מידע רגיש בלתי מורשה המועבר לענן.
- יש לשקול שימוש באמצעים שפורטו לעיל גם לצורך איתור וחסימה של מידע רגיש העובר ללא אישור בתוך שירות הענן עצמו (לדוגמא בין שרתים/מופעים שונים בענן).
- במידה ולא נדרש עיבודו של המידע המיועד לאחסון אצל ספק שירותי הענן, מומלץ להעביר את המידע לשירות הענן לאחר שהוצפן תחילה בחצרות רכבת ישראל.

7.5 אבטחת נתונים נייחים (Data at rest)

- כתלות במודל השירות (IaaS/PaaS/SaaS) ויכולות ספק שירותי הענן, מומלץ לעשות שימוש במנגנון IDA[10] בו מפוצלים הקבצים למס' חלקים (Fragments) כאשר כל חלק מאוחסן בשרת אחסון שונה. שימוש במנגנון זה יקשה על תוקף להשיג את המידע היות והוא יצטרף להשיג גישה לכל התקני האחסון אליהם פוזר המידע.
- יש להצפין מידע רגיש השמור בענן תוך שימוש באלגוריתם הצפנה סטנדרטי ומוכר. יש להימנע ככל שניתן משימוש באלגוריתם קנייני (proprietary) אשר אינו מוכח ונוטה לרוב להיפרץ.
- בעת שימוש במודל שירות IaaS מומלץ להצפין את הכוננים (Volumes) על מנת למזער את חשיפתו של המידע לגורמים בלתי מורשים אם ע"י שכפול כוננים (Snapshots) ואם ע"י גישה בלתי מורשית של מנהלי המערכת מטעם ספק הענן.
- יש להבין את ארכיטקטורת אחסון הנתונים של ספק שירותי הענן כדי לזהות סיכונים אבטחתיים ובקרות זמינות להתמודדות עם סיכונים אלו.

[8] Payment Card Industry (PCI) Data Security Standard (DSS).
[9] Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance.
[10] Information Dispersions Algorithm (IDA)

7.6 בקרת גישה

7.6.1. הזדהות

- במידת האפשר יש להתחבר למערכות ושירותים של ספק שירותי הענן תוך הזדהות באמצעות השבונות משתמשים של רכבת ישראל (BYOI - Bring your own identity). לצורך כך על מערכות ושירותי הספק לספק תמיכה בסטנדרטים כגון SAML או WS-Federation.
- יש להתחבר למערכות ושירותי הספק תוך שימוש באמצעי הזדהות חזק אשר מתבסס על לפחות שניים מתוך שלושת שיטות ההזדהות הבאות:
  - Something you know: סיסמה מורכבת וארוכה.
  - Something you have: כרטיס חכם (Smart Card), RSA Token, קוד OTP (One Time Password) הנשלח באמצעות SMS או מופק דרך טלפון/התקן חכם אחר.
  - Something you are: אמצעי ביומטרי כגון טביעת אצבע, רשתית עין וכדומה.
- במידה ונעשה שימוש בסיסמה לצורך הזדהות, עליה לעמוד בדרישות הבאות:
  - מורכבות סיסמה: תהיה מורכבת מ-10 תווים או יותר הכוללים אותיות קטנות וגדולות, ספרות וסימנים מיוחדים.
  - תוקף סיסמה: תוקף הסיסמה יפוג לאחר תקופה של עד 90 יום ולאחר מכן יידרש המשתמש להחליפה.
  - היסטוריית סיסמאות: תשמר היסטוריית סיסמאות של לפחות 10 סיסמאות לאחור.
- 5 ניסיונות הזדהות שגויים באמצעות כל אחד משלושת שיטות ההזדהות שהוזכרו תוביל לנעילת המשתמש למשך 15 דקות.
- יש להגדיר פרק זמן קבוע שלאחריו יופעל מנגנון ניתוק תקשורת (session time out) המחייב זיהוי מחדש של המשתמש.

7.6.2. ניהול הרשאות וזהויות

- יש לאפשר גישה לענן רק מסוגי התקני מחשוב (מחשבים נייחים/ניידים, שרתים, טלפונים חכמים, טאבלטים וכו') ומאזורים גאוגרפים/כתובות רשת שיקבעו ע"י רכבת ישראל.
- יש להגדיר הרשאות גישה למידע באופן מדוקדק תוך הענקת הרשאות גישה רק לגורמים אשר גישתם למידע הכרחית לצורך מילוי תפקידם.
- במידת האפשר, הרשאות הגישה לשירותי הענן ינוהלו ע"י רכבת ישראל. הדבר אפשרי במידה והספק תומך בפרוטוקול OAuth 2.0[11], User Managed Access (UMA)[12], XACML[13] או באמצעות דרכים אחרות המאפשרות את ניהול ההרשאות ע"י הלקוח.

---

[11] An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications. http://oauth.net/

[12] User-Managed Access (UMA) is an OAuth-based web-based access management protocol.

[13] eXtensible Access Control Markup Language

- במידה ונתמך ע"י הספק, מומלץ לעשות שימוש במערכת ה-IDM[14] רכבת ישראל או במערכת SCIM[15] לצורך ניהול זהויות והרשאות גישה של משתמשי רכבת ישראל הניגשים לשירותי הענן.
- יש לבצע סקר/טיוב הרשאות ומשתמשים אחת לתקופה מוגדרת. במסגרת זו על רכבת ישראל לוודא כי המשתמשים וההרשאות מוגדרים על פי עיקרון "הצורך לדעת". עיקרון זה מגביל את תפוצת המידע לבעלי התפקידים הזקוקים לו בלבד.
- יש לנהל את הרשאות הגישה בכל השכבות הבאות בהתאם לדרישות האבטחה של רכבת ישראל וכתלות במודל השירות הנבחר (IaaS/PaaS/SaaS):
  - שכבת התקשורת (Network Layer): לדוגמא, הגבלת גישה לכתובות רשת ופורטים בשירות הענן למורשים בלבד תוך שימוש באמצעים כגון FW, ACL's, VLAN's וכדומה.
  - שכבת המערכת (System Layer): לדוגמא, הגדרת רשימת פרוטוקולים באמצעותם ניתן להתחבר לשרתים ולשנות הגדרות (Remote Desktop, SSH, WMI, SNMP וכדומה).
  - שכבת האפליקציה (Application Layer): לדוגמא, הגדרת הרשאות גישה לתפריטים/אפשרויות מערכת.
  - שכבת תהליכים (Process Layer): לדוגמא, הגדרת תהליכים הניתנים להרצה ע"י האפליקציה.
  - שכבת המידע (Data Layer): לדוגמא, הגבלת גישה לקבצים, תיקיות, רשומות בבסיס הנתונים וכדומה.

[14] Identity Management (IDM)
[15] Simple Cloud Identity Management (SCIM)

7.6.3. ניהול מפתחות הצפנה

- על מנת לשמור על רמת אבטחה גבוהה ועמידה בדרישות רגולטוריות, על רכבת ישראל לנהל את מפתחות ההצפנה באופן עצמאי בשטח רכבת ישראל או באמצעות ספק חיצוני אמין המתמחה בניהול מפתחות הצפנה.
- את מפתחות ההצפנה בענן יש לנהל באמצעות רכיב אחסון מפתחות מאובטח, מרכזי וייעודי לארגון.
- יש להעדיף שימוש ברכיב HSM ייעודי לאחסון מפתחות ולניהול תהליך הצפנת המידע/פענוח הצפנה, חתימה דיגיטלית ואימות חתימות.
- יש להימנע ככל שניתן משימוש בפרוטוקולי הצפנה/חתימה ישנים כגון DES, MD5 וכדומה.
- בעת עבודה מול רכיבי HSM בענן יש לוודא כי הספק עומד בתקני אבטחה מחמירים כגון FIPS 14-2, Common Criteria EAL4+ וכדומה, ותומך בפרוטוקולי הצפנה סטנדרטים ומוכרים.
- בעת העברת מפתחות הצפנה בין רכבת ישראל לשירות הענן (גם אם באמצעות רכיב HSM) יש להשתמש בתווך תקשורת מוצפן כגון SSL/IPSEC/VPN תוך ביצוע הזדהות חזקה בשני שלבים (factor authentication 2).

7.7 אבטחה פיזית

7.7.1. אבטחה סביבתית

- יש לבחון את הסיכונים הקיימים בעקבות מיקומם הפיזי של מתקני ספק שירותי הענן ומיקומם של שירותים עליהם מסתמך הספק. בין השאר יש לוודא כי האזור בו ממוקמים מתקני הספק:
  - אינו רשום כאזור בעל סיכון גבוה לרעידות אדמה.
  - אינו שייך לאזור גאוגרפי בעל סיכוי גבוה לשיטפונות, מפולות או אסונות טבע אחרים.
  - אינו חשוף לרמת פשיעה גבוהה ו/או לאי סדר חברתי/פוליטי.
  - אינו מנותק גאוגרפית מאזורים מיושבים.
- יש לבחון את נהלי האבטחה הפיזיים של ספק שירותי הענן ולוודא את קיומן של בקרות האבטחה הבאות:
  - מערכת בקרת גישה - הכניסה למתקנים מתאפשרת רק לאחר הזדהות באמצעות כרטיסים חכמים ו/או אמצעים ביומטריים (טביעת אצבע, קרנית וכו').
  - ציוד בטיחות להתמודדות עם שריפות הכולל גלאי עשן, ממטרות מים, מטפים, צינורות כיבוי אש וכדומה פרוסים ברחבי המתקנים.
  - חיישני תנועה, התקני מעקב טרמיים וגלאי שבירת חלונות.
  - בקרות אקלים (טמפרטורה ולחות) בחוות השרתים.
  - יציאות חירום.
  - מצלמות במעגל סגור (CCTV) פרוסות ברחבי המתקן (כולל שמירה של גיבויים).
  - ארונות השרתים נעולים ומפתחותיהם נגישים למורשים בלבד.
  - כספת חסינת אש משמשת לשמירת מסמכים/מדיות חשובים.
- יש לוודא כי קיים צוות אבטחה המורכב משומרים, מפקחים וקציני בטיחות השומרים על המתחם 24/7.

- יש לוודא כי קיימות הנחיות מפורשות בנוגע לנושאים הבאים:
  - הזדהות ורישום של עובדים, ספקים ואורחים בעת כניסה למתחם ולמערכות הספק.
  - הנפקה של תגי עובדים ושחזורם במידה ואבדו/הושחתו.
  - הנחיות מעקב ותגובה לאירועים.
  - שליטה בהכנסה והוצאה של חומרים לבניין.
  - צפייה בשידורי מצלמות במעגל סגור.
  - ליווי של אורחים בתוך הבניין.
  - הנחיות השמדה של מדיה תקולה (דיסקים קשיחים, קלטות גיבוי וכדומה).
- יש לוודא כי חוות השרתים מצוידות בהתקני UPS וגנרטור חירום לצורך אספקה קבועה של מתח חשמל.

7.7.2. משאבי אנוש

- יש לוודא כי כל עובדי הספק בעלי גישה למידע של רכבת ישראל:
  - עברו בדיקות רקע ומבחני אישיות טרם העסקתם.
  - חתמו על הסכם סודיות (NDA).
  - עברו הדרכות בנושא מודעות אבטחת מידע.
  - עברו תרגולי התאוששות מאסון וטיפול באירועי אבטחה.
- יש לבחון מסמכים המפרטים את רשימת עובדי הספק ותפקידיהם ולוודא כי קיימת הפרדת תפקידים (Segregation of duties), כלומר לוודא כי עובדים שונים מנהלים תשתיות קריטיות שונות. בנוסף יש לוודא כי לכל תפקיד הוגדר סט הרשאות מינימלי הנחוץ למילוי התפקיד. רשימת תפקידים זו נדרשת להירשם במסמך Organization's information security policy אשר עבר בקרה ונחתם ע"י הנהלת הספק.
- יש לוודא כי קיים נוהל פורמלי המסדיר את תהליך עזיבתם של עובדי הספק ומפרט את רשימת הפעולות שיש לנקות בעת עזיבת עובד.

7.7.3. המשכיות עסקית והתאוששות מאסון

- יש לבדוק את הסכם השירות (SLA) עם הספק לצורך בחינה של זמני השירות והתגובה לאירועים להם מתחייב הספק ולוודא כי זמני שירות ותגובה אלו עונים לצרכי רכבת ישראל.
- יש לוודא את קיומם של הצוותים הבאים בספק הענן:
  - צוות תגובת חירום (Emergency Response Team).
  - צוות ניהול משברים (Crisis Management Team).
  - צוות תגובה לאירועים (Incident Response Team).
- יש לוודא קבלת הוכחות מהספק לכך שמבוצעים באופן שוטף תרגילי BCP/DR במתקניו.
- בהתאם לרמת זמינות המערכת הנדרשת, יש לשקול הקמה של אתר DR. את האתר יש להקים במיקום גאוגרפי שונה ולהעדיף שימוש בספק שירותי ענן שונה.
- יש לבצע גיבויים אינקרמנטליים (Incremental backups) או צילומים (Snapshots) של מערכות רגישות בהתאם לדרישות רכבת ישראל.

7.8 מעקב ובקרה

- על רכבת ישראל והספק להסכים מראש על הדרך בה יאספו, יאוחסנו וישותפו ראיות לאירועי אבטחת מידע (לדוגמא רישומי מעקב – Audit Logs, דוחות פעילות – Activity Reports, הגדרות מערכת וכו').
- יש לבקש מספק השירות לספק דוחות כגון SSAE 16 SOC2 [16] או ISAE 3402 Type 2 report[17]. דוחות אלו יספקו לרכבת ישראל מידע איכותי ואמין אודות בקרות הנעשות אצל ספק הענן ע"י גופים חיצוניים אמינים הסוקרים נושאים הקשורים לאבטחת המידע, זמינותו, שלמותו וחשאיותו, וכן בקרות הקשורות להגנה על הפרטיות.
- בהתאם למודל השירות הנבחר ולסוג המערכת/המידע הנשמרים בענן, כאשר בוחנים את רישומי המערכת (Logs), יש לשאול את השאלות הבאות ולוודא כי התשובות עונות על צרכי רכבת ישראל:
  - אילו רישומי מערכת זמינים? לדוגמא: רישומים של התקני תקשורת, מערכות הפעלה, ניהול ענן, גיבוי ושחזור נתונים, תחזוקה, גישת משתמשים, שגיאות וכו'. לכל הפחות יש לוודא כי קיים רישום של אירועים במערכות/רכיבים שהוגדרו ע"י רכבת ישראל כבעלי רגישות גבוהה לתפקוד המערכת.
  - כיצד נאספים הרישומים? יש לוודא כי רישומי המערכת נאספים ע"י מערכת SIEM או SysLog ייעודית בענן או ניתנים לשליחה למערכת ה-SIEM רכבת ישראל אית לצורך ניטור והתראה על אירועי אבטחה המתרחשים בענן.
  - מתי יוכל רכבת ישראל לקבל את הרישומים מהספק? בהתאם לרגישות המערכת, יש לוודא כי רישומי המערכת ניתנים לאיסוף ע"י רכבת ישראל בזמן אמת/באופן מתוזמן.
  - האם הלוגים המופקים ע"י המערכות קונסיסטנטיים ושלמים? יש לוודא כי השעונים ואזורי הזמן (Time Zone) בכל המערכות מסונכרנים ועובדים מול אותו שרת NTP.
  - לכמה זמן נשמרים הרישומים? יש לוודא כי הספק מאפשר שמירה לאחור של רישומי מערכת לתקופה המשתנה בהתאם לרגישות המערכת ולדרישות רגולטוריות התקפות למערכת.
  - האם הרישומים עמידים בפני חבלה (מחיקה/שינוי ע"י גורמים בלתי מורשים)? יש לוודא כי רישומי המערכת נשמרים בשרת מרכזי המנוהל ע"י צוות עובדים נפרד.
  - מהו הפורמט בו נשמרים הלוגים והאם הוא נתמך ע"י מערכות רכבת ישראל? יש לוודא כי הפורמט בו נשמרים רישומי המערכת הינו סטנדרטי וניתן לקריאה/יבוא ע"י מערכות רכבת ישראל (כגון מערכת ה-SIEM).
- יש לבצע ניטור (Monitoring) שירותים ומערכות בענן ברבדים הבאים:
  - ניטור של לוגים - יבוצע לצורך מענה לדרישות רגולטוריות ולצורך איתור בזמן אמת או בדיעבד של בעיות טכניות או אירועי אבטחת מידע המתרחשים.

[16] https://www.ssae-16.com/soc-2/
[17] http://isae3402.com/ISAE3402_reports.html

- ניטור ביצועים – יבוצע לצורך מעקב אחר עומסים במשאבי המחשוב בענן (מעבד, זיכרון, אחסון וכו'). עומס חריג עלול להעיד על פעילות עוינת המתרחשת ברשת (יתכן ע"י לקוח החולק משאבים עם רכבת ישראל).
- ניטור אחר פעילות עוינת/חריגה – יש להגדיר אילו פעילויות במערכת מעידות על פעילות עוינת/חריגה ולנטרן. פעילות עוינת/חריגה יכולה להתבטא בניסיונות הזדהות כושלים, ניסיונות גישה של משתמשים למשאבים לא מורשים, כניסה כפולה של משתמש למערכת בו זמנית וכדומה. יש לעקוב אחר פעילויות אלו ולהתריע לגורם מוסמך מטעם רכבת ישראל על התרחשותן.

- טרם המעבר לספק שירותי הענן וכן כל תקופה מוגדרת בהתאם לרגישות המערכת, יש ליזום מבדקי חדירה עם דגש מיוחד על בדיקת הנושאים הבאים:
  - בדיקות אפליקטיביות אוטומטיות לזיהוי של פגיעויות מוכרות.
  - בדיקות ידניות אשר יבחנו חולשות הנובעות משימוש בפלטפורמת ריבוי לקוחות (Multi-Tenancy). בדיקות אלו יבחנו האם ניתן לבצע העלאת הרשאות ו"לקפוץ" בין מופעים (Sessions) שונים עקב היעדר אכיפה מספקת.
  - כאשר מבוצעת מיגרציה לשירותי ענן מבוססי מודל שירות PaaS או IaaS, יש לבצע בדיקות נוספות במטרה לבחון האם בקרות אבטחה ברמת התשתית (כגון VM Zoning and segregation, Virtualization Security וכדומה) הוגדרו באופן תקין.

7.9 וירטואליזציה

- יש לבדוק מהו סוג הפלטפורמה הווירטואלית אשר נמצאת בשימוש ספק הענן ולבחון את הסיכונים האבטחתיים הרלוונטיים לפלטפורמה זו.
- יש לבצע הפרדה פיזית (רכיבי חומרה נפרדים) בין הסביבות הבאות:
  - הפרדה בין סביבת הייצור לסביבות בעלות רמת אבטחה נמוכה יותר כגון סביבת הבדיקות והפיתוח.
  - הפרדה בין סביבות המכילות מידע ברמת רגישות שונה.
  - הפרדה בין סביבות המשמשות לצרכים שונים. לדוגמא, הפרדה בין סביבת תחנות קצה לסביבת שרתים.
- יש לבצע הקשחה של כלל מערכות ההפעלה במופעים (Instances) ורכיבי תקשורת המשמשים את רכבת ישראל..
- יש להתקין תוכנות אבטחה כגון אנטי-וירוס, HIPS[18], DLP ומערכות נוספות על פי הצורך בכלל מערכות ההפעלה במופעי (Instances) רכבת ישראל. מומלץ כי תוכנות אבטחה אלו יהיו מותאמות לעבודה בסביבה וירטואלית לצורך חסכון במשאבים.
- במידה וניתן, יש להקשיח את הגדרות האבטחה בפלטפורמה הווירטואלית ע"פ המלצות היצרן.
- יש להתקין עדכוני אבטחה באופן סדיר בכלל רכיבי התשתית והמופעים המשמשים את רכבת ישראל.

7.10 שימוש במערכות אבטחה מבוססי ענן (SecaaS[19])

- על פי אופי ורגישות המידע/המערכות בענן יש לשקול שימוש במערכות אבטחה נוספות המוצעות כשירות ע"י ספקי שירות ענן רבים. בין מערכות אלו ניתן למנות את המערכות הבאות:
  - Data Loss Prevention (DLP): מערכת המשמשת למניעת דלף מידע. המערכת מנטרת אחר מידע נייח או בתנועה וחוסמת העברה של מידע רגיש לגורמים/יעדים בלתי מורשים. מומלץ לעשות שימוש במערכת זו לצורך מניעת זליגתו של מידע רגיש של רכבת ישראל לידיים בלתי מורשות.
  - Intrusion Detection/Prevention (IDS/IPS): מערכת המבצעת ניטור של תעבורה ברשת לאיתור וחסימה (IPS בלבד) של אירועים חריגים המזוהים על פי חוקים, ניתוחי התנהגות, שיטות היוריסטיות ודרכים נוספות. מערכות אלו לדוגמא יכולות לאתר פעילות זדונית מאורגנת המתבצעת ע"י גורמים החולקים משאבים עם רכבת ישראל (Multi-Tenancy). מומלץ להטמיע מערכות אלו בסגמנטים ברשת המשמשים סביבות רגישות של רכבת ישראל.
  - Security Information & Event Management (SIEM): מערכת מרכזית לאיסוף רישומי מערכת ואירועים ממערכות נבחרות בענן. המערכת מבצעת קורלציה בין רישומי המערכות השונות לאיתור ודיווח על אירועי אבטחת מידע המתרחשים בזמן אמת ברשת.

[18] Host Intrusion Prevention System (HIPS)
[19] Security as a Service (SecaaS)

רכבת ישראל
פשוט ליהנות מהדרך

- בעת שימוש במערכות אבטחה מבוססי ענן יש לוודא כי תווך התקשורת בין המערכות הינו מאובטח.
- במידה והשירות ניתן ע"י ספק ענן נפרד, יש לוודא כי ספק זה עומד בכל כללי האבטחה המפורטים במסמך זה.

7.11 מעבר בין ספקי שירות ענן

- הסכמי רמת השירות (SLA) משתנים מספק לספק. יש צורך לבחון את הפערים בין הסכמי השירות ולהבין כיצד הם משפיעים על רכבת ישראל.
- ספקי ענן שונים עובדים עם פלטפורמות מחשוב שונות ועם ארכיטקטורה שונה. השוב להבין את המגבלות של השירותים והפלטפורמות החדשים אשר כוללים בין השאר מגבלות כגון ממשקי תוכנה (API's), Hypervisors ומגבלות נוספות, ולבחון כיצד אלו משפיעים על רכבת ישראל.

7.12 סיום התקשרות עם ספק

- עם סיום ההתקשרות עם ספק שירותי הענן יש לבצע את הפעולות הבאות:
  - מחיקה של כל הנתונים והמידע השמורים בשירות הענן ונמצאים תחת שליטת רכבת ישראל.
  - דרישה מהספק להשמיד עותקים של הנתונים והמידע בהם נעשה שימוש במסגרת פעילות הספק עבור רכבת ישראל.
  - דרישה מהספק להציג הוכחות לכך שהמידע הושמד (רישומים ודוחות רלוונטיים).
  - במידה והמידע הוצפן –ביטול (Revoke) מפתחות ההצפנה ומחיקתם.

8 סיכום

מסמך זה הציג הנחיות אבטחת מידע לעבודה מול ספק שירותי ענן תוך התייחסות להוראות חוק ולרגולציה בישראל. בהתאם לסוג הענן, מיקומו והשירותים אותם יספק, וכן בהתאם לסוג המידע ורגישותו, עלולים להתווסף כללי אבטחה נוספים אותם נדרש יהיה ליישם בעת מעבר לענן.

כפי שהוצג במסמך, יישום שירותי ענן בארגון מעלה סוגיות אבטחה רבות כגון: זליגת/ אובדן מידע, הצפנה, מתקפות מבפנים (Malicious Insiders), שיתוף במשאבים ושירותים (Multi Tenancy) ועוד. עבודה על פי כללי האבטחה שפורטו במסמך זה תעזור לרכבת ישראל להתמודד עם סוגיות אבטחה אלו.

יש לציין כי המעבר לשימוש בשירותי ענן מחייב אישור הרגולטור.

רכבת ישראל
פשוט ליהנות מהדרך

בברכה,

שרון בן אבי

יועץ אבטחת מידע יח' הסייבר

משרדי הנהלת הרכבת, יוספטל 1 , לוד
טלפון : 08-6533406