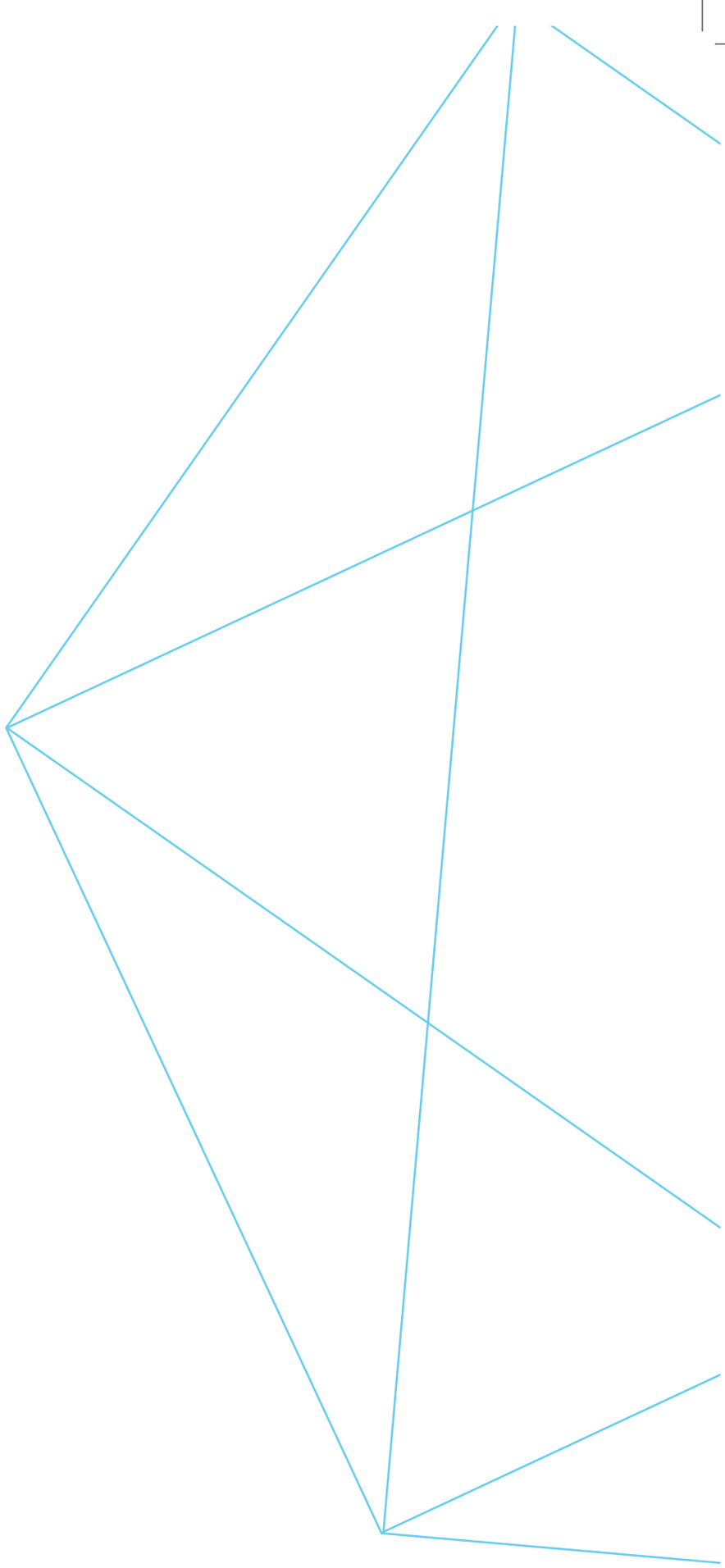
משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

מסמך הרחבה לתורת ההגנה בסייבר בארגון

שימוש בשירותי ענן

גרסה 1.0

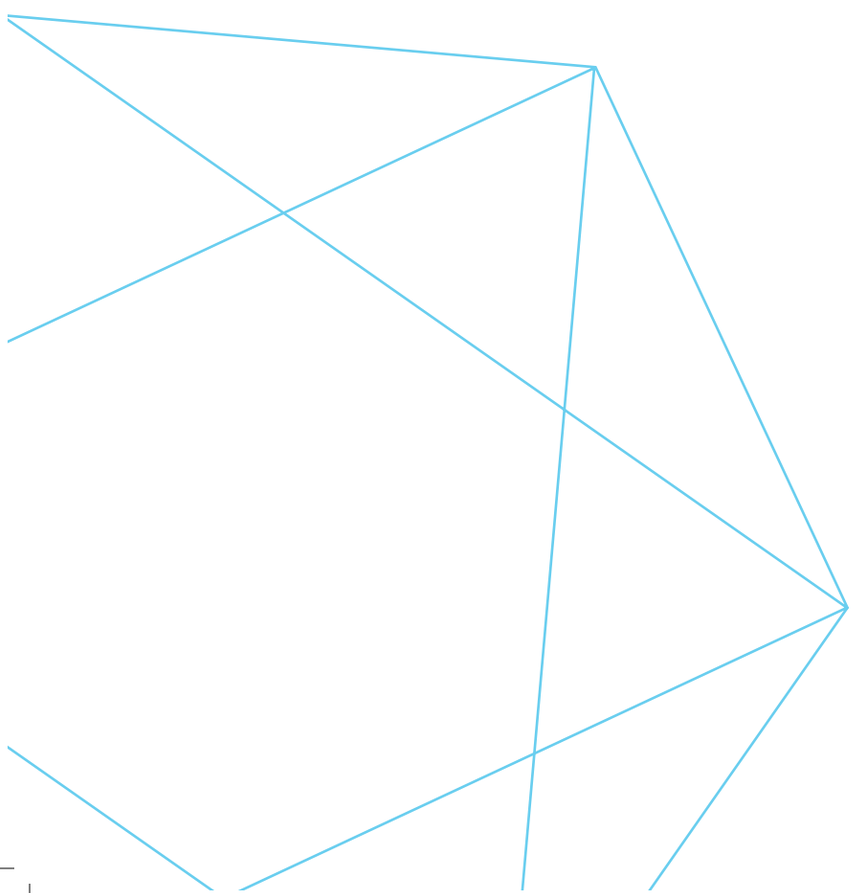


משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

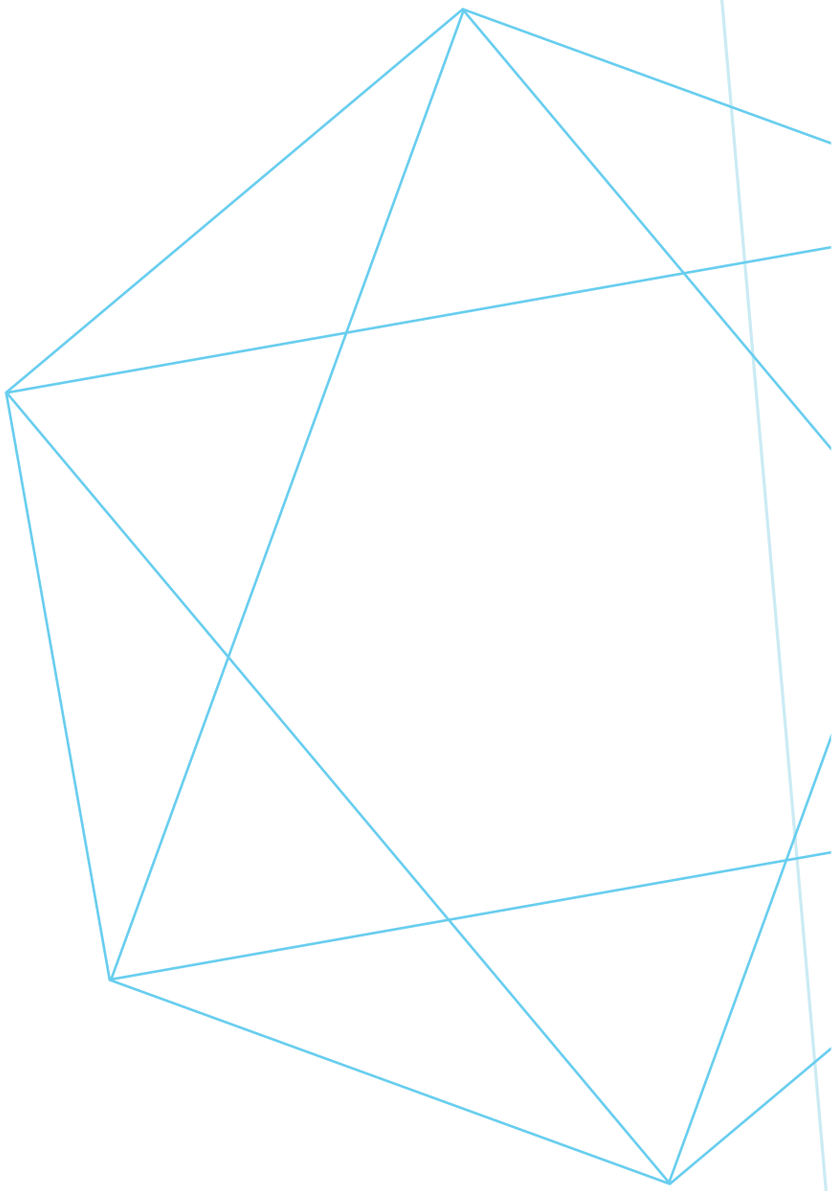
מסמך הרחבה לתורת ההגנה בסייבר בארגון

שימוש בשירותי ענן

גרסה 1.0



תוכן העניינים



הקדמה

מסמך זה הינו **מסמך הרחבה** ל**תורת ההגנה בסייבר לארגון** של הרשות הלאומית להגנת הסייבר.

מסמך ההרחבה מביא תוכן מקצועי מפורט ומשלים בנושא מסוים בתחום הגנת הסייבר.

במסמך זה יפורטו הרקע לנושא והקשרו לתחום בהיבטי הגנת סייבר. כמו כן יפורטו שיטות עבודה נכונות ליישום והרלוונטיות לנושא הנדון, לטובת החיזוק של הגנת סייבר ושיפורה.

המסמך מיועד למנהל האבטחה הארגוני (CISO) ככלי עזר מסדר ומכוון במסגרת בניית תכנית ההגנה הארגונית על-ידו.

ככלל, במסמך זה אין התייחסות ליצרנים של מוצרי אבטחה, או לשיטות מומלצות (BP) מפורטות להקשחה ולחיזוק ההגנה על-ידי הגדרות טכניות. לטובת אלה, יש לעשות שימוש במסמכי היצרן או במסמך BP רלוונטי, אשר יפורסם על-ידי הרשות הלאומית להגנת הסייבר בנפרד.

רקע

בעולם התקשוב (IT) מתחזקת המגמה של ארגונים ומשתמשי קצה לצרוך שירותי ענן, המתבטאת באימוץ טכנולוגיות, המיושמות כשירותי ענן הן באמצעות שימוש ביישומים חדשים שמסופקים על-ידי יצרני ענן והן באימוץ חשיבה עסקית להסבה או להעברה של פעילות מחשובית קיימת להפעלה מתוך יישום או תשתית ענן.

על-פי סקר שפורסם בפברואר 2017 על-ידי חברת גרטנר (Gartner), המובילה בסקרי שוק בעולם ה-ICT, בשנת 2017 צפויה עלייה של 18% בצריכת שירותי ענן (ההוצאה העולמית תעמוד על כ-246.8 מיליארד דולרים). עוד צופה גרטנר, כי עד 2020 יהיו 50% מעסקאות מיקור-החוץ של שירותי ה-IT - שירותי ענן.

ארגונים רבים עוברים שינוי מהותי בצריכת שירותי ה-IT. עד עתה תוחזקו, הוטמעו ולעתים אף פותחו מרבית היישומים על-ידי מחלקת הIT- של הארגון. כיום ניכרת מגמה של יחידות עסקיות בארגון לקדם ערוצים נפרדים לבניית יישום או לצרוך שירותי IT לצורך תמיכה בפעילות העסקית במודל ענן.

שירותי הענן המסופקים הם מגוונים ורבים ומתחדשים בקצב מהיר. המשמעויות והדגשים שה-CISO (מנהל אבטחת המידע הארגוני) נדרש לתת עליהם את הדעת בבואו לקבוע וליישם הגנה נאותה - גם הם מגוונים ורבים.

מסמך זה מיועד ל-CISO, כהרחבה לתורת ההגנה בסייבר לארגון, שהופצה על-ידי הרשות הלאומית להגנת הסייבר במהלך 2017.

מטרת מסמך זה להציג שיטת עבודה נכונה עבור מנהלי אבטחה ארגוניים, הנדרשים לבנות תכנית הגנה תוך התייחסות לשירותי הענן שהארגון מקבל וצורך.

מונחים המתייחסים לשירותי הענן

1. מחשוב ענן (Cloud computing) מתייחס למצב שבו נעשה שימוש במשאבי חומרה ו/או תוכנה מרוחקים מהמשתמש על-גבי רשת ציבורית או פרטית.

מונח	הסבר
CSP	Cloud Service Provider - ספק שירותי ענן.
CSC	Cloud Service Customer - לקוח שירותי ענן.
CSN	Cloud Service Partner - שותף לשירותי ענן.
Cloud portability	האפשרות להעביר יישום מידע מספק ענן אחד לספק ענן אחר.
Elastic computing	צריכת משאבים ואפשרות הרחבה וצמצום לפי צורך.
Cloud Middleware	תוכנה המתווכת בין ספקי ענן שונים.
Openstack	תוכנת קוד פתוח, המאפשרת אוטומטיזציה ביצירת סביבת ענן, הכוללת מערך אחסון, מערך תקשורת ותוכניות ניהול.
PPU	Pay Per Use - תשלום לפי צריכה.
RTO	Recovery Time Objective - בהתייחס לזמינות שאליה מתחייב ספק הענן.
SLA	Service Level Agreement - אמנת שירות, בהתייחס לרמת השירות שאליה מתחייב ספק הענן.
Vendor lock-in	משמעות ההתקשרות עם ספק ענן ואפשרות סיום ההתקשרות.

2. קיימים כמה מודלים של **שירותי ענן**, הבולטים שבהם הם:

2.1 **Colocation** - חברה שמעדיפה לחסוך בבניית חדר שרתים משלה, העומד בתקנים מחמירים, כגון מבנה תת-קרקעי מוגן, הכרוך בהשקעות גדולות בהקמת תשתיות חשמל, קירור, כיבוי אש ורכיבים נוספים, תעדיף לאחסן את ציוד המחשוב במתקן מסודר של ספק ידוע במודל הנקרא **שטח/מתח** - הלקוח מקבל את השטח שבו יאוחסן ציוד המחשוב, את החשמל והמיזוג וכן הגנה בפני שריפה ושמירה 24X7, וירכוש, יתקין ויתחזק את החומרה באופן עצמאי.

2.2 **תשתית כשירות** (Infrastructure as a Service - **IaaS**) - המודל הבסיסי והנפוץ ביותר כשירות לחברות ולארגונים. מטרתו העיקרית היא להימנע מבניית חדרי מחשב ומרכישה ותחזוקה של רכיבי חומרה, הכוללים מערכי אחסון, שרתים, רכיבי תקשורת ורכיבי אבטחת מידע וקבלת שירותים תמורת תשלום לפי צריכה במודל של אובייקטים וירטואליים הניתנים לשליטה באמצעות ממשק שירות.

2.3 **פלטפורמה כשירות** (Platform as a Service - **PaaS**) - במודל זה, נוסף על רכיבי החומרה והתשתית, ספק הענן מספק ללקוח פלטפורמה של תוכנות בסיס, המשמשות לשם סביבת פיתוח יישומים, ביצוע בדיקות מוצרים של הלקוח ואספקת שירותי מחשוב מתוך הפלטפורמה.

2.4 **תוכנה כשירות** (**SaaS** - Software as a Service) - במודל זה ספק הענן מספק הן את החומרה והתשתית והן את יישומי הקצה של הלקוח, כשהיישום נרכש מחברה המתמחה בתחום יישומי מסוים.

2.5 **מידע כשירות** (**DaaS** - Data as a Service) - במודל זה הארגון צורך מידע מתוך בסיס נתונים בענן וקולט אותו לתוך מערך המידע שלו. לדוגמה, חברת חשמל, המתכננת את תפוקות הייצור העתידי, תצרוך מידע לגבי מזג האוויר הצפוי בימים הקרובים. החברה תתחבר לבסיס נתונים שיכול להיות מאוחסן בענן ותשלוף מידע רלוונטי כשירות מגוף המוכר אותו. במקרה זה הארגון יצטרך לאמת את המידע כדי לוודא שהמידע מהימן.

3. **אבטחה כשירות** (**SecaaS** - Security as a Service) - מודל עסקי של צריכת שירותי הגנה באמצעות שירותי ענן על-מנת לחסוך בעלויות של משאבי כוח אדם, חומרה, תוכנה ורישיונות. השירותים הניתנים הם לרוב הזדהות, מניעת נוזקות, מניעת חדירה לרשת, ניטור ותגובה לאירועים.

4. נהוג להתייחס ל-4 **פריסות** של סוגי ענן:

1.4 **"ענן ציבורי"** - מצב שבו שירותי הענן ניתנים באמצעות תשתית (חומרה, תוכנה ויישומים) משותפת ופתוחה **לכול**, לעתים אף ללא תשלום. אמנם, קיימת חלוקה והפרדה לוגית ולעתים פיזית בין הלקוחות והחשבונות, אך כאמור, מדובר בשיתוף משאבים.

4.2 **"ענן פרטי"** - מצב שבו שירותי הענן ניתנים באמצעות תשתית (חומרה, תוכנה ויישומים), הנגישה רק ללקוח המסוים. לעתים תשתית זו נמצאת באתר הלקוח ולעתים היא נמצאת באתר של ספק הענן. התקשורת והגישה לתשתית ניתנות בלעדית ללקוח הייעודי, ומעורבותו בניהולה עשויה להיות גבוהה.

4.3 **"ענן קהילתי" -** מצב שבו מגזר מסוים או כמה ארגונים בעלי אינטרס משותף מתאגדים לקבלת שירותי ענן ייעודיים עבורם.

4.4 **"ענן היברידי" -** מצב שבו לקוח משתמש בענן פרטי לצורך יישומים מסוימים, ובתוך כך גם בענן ציבורי לצורך קישור המידע או היישום עם יישומים או מידע.

5. במחשוב ענן מתקיימת חלוקה ל-2 אפשרויות של מימוש ארכיטקטורה**:**

5.1 **דייר-יחיד** (Single-Tenant) **-** בהתאם לסוג שירות הענן ולפריסה, השימוש של הלקוח הינו בלעדי, ללא חלוקה ושיתוף עם משתמשים אחרים בתוך ומחוץ לארגון. הנ"ל עשוי להתבטא החל משימוש במשאב חומרה וכלה ביישום אפליקטיבי, אשר פותח באופן ייעודי עבור הלקוח (לרוב בפריסה של ענן פרטי).

5.2 **ריבוי-דיירים** (Multi-Tenants) **-** במקרה זה, בהתאם לסוג שירות הענן והפריסה, הלקוח חולק משאב עם משתמשים נוספים, לעתים בתוך הארגון ולעתים בארגונים אחרים.

6. על-מנת לממש בצורה מיטבית את פעילותו של ארגון מול ספק הענן, ראוי כי הארגון יקצה לכך משאבי כוח אדם מקצועיים. להלן הגדרת התפקידים ותכולתם. מימושם ייקבע בכל ארגון על-פי המשאבים העומדים לרשותו ובהתאם לנפח הפעילות של הארגון בקבלת שירותי ענן.

תפקיד	אחריות ותכולה
CCO Chief Cloud Officer	מנהל פעילות ענן ארגוני, אחראי על מפת המידע והשירותים ומיקומם במערך העננים, על ההתקשרות העסקית עם ספקי הענן (בליווי מנהל רכש בארגון) ועל אפיון הצרכים מול ספקי הענן בהיבטי הממדים: • ממד המידע - צורת האיחסון. • ממד השירות והזמינות הנדרשת, כפי שהוגדרו על-ידי הגורם העסקי. • איפיון תעבורת המידע אל הענן ומן הענן.
מנהל יישומי ענן	אחראי על איסוף הדרישות הארגוניות של היחידות העסקיות ליישומי ענן ועל העברת המידע לאחראי אבטחת מידע בענן ול-CISO.
אחראי אינטגרציה בין ספקי ענן	אחראי על אבטחת מידע של נתיבי העברת המידע, על הצפנת המידע ועל תכנון לאבטחתו של מעבר המידע בשלמותו בין ענן לארגון או בין ענן אחד לאחר.
אחראי אבטחת מידע בענן	אחראי על אבטחת התשתית במודל IaaS ועל הטמעה של רכיבי אבטחת מידע: • אבטחת מידע מאוחסן - אחראי על הצפנת נתונים או התממתם. • אחראי אבטחת גישה למידע, למערכת הפעלה, לבסיסי נתונים. • אחראי על מתן הרשאות לפי צורך לגישה למידע ולביצוע פעולות על מידע בענן. PaaS/- SaaS אחריות על בקרת קוד מאובטח.
מנהל בקרות מידע בענן	IaaS : בקרה על טופולגיית הרשת בענן ועל הגדרתם של אמצעי אבטחת המידע. PaaS: בקרה על פיתוח קוד/יישום מאובטח.
אחראי BCP	כתיבת נוהלי המשכיות עסקית ליישומים ולמידע המאוחסנים בענן.

פרק א׳: בניית תכנית הגנה לשירותי ענן

הצורך בשירותי ענן מונע לרוב על-ידי היחידות העסקיות בארגון. לעתים התהליך אינו משלב את ה-CISO ואף לא את ה-CIO בשיקולים לצרוך שירות ענן וכן בתהליך היישום.

פרק זה יסקור את השיקולים שה-CISO , וגם ה-CCO - אם קיים בארגון - נדרשים לקחת בחשבון בפעילויות ההכנה של בניית תכנית ההגנה כאשר הארגון מתעתד לרכוש שירותי ענן.

הפרק יתייחס למודל חלוקת האחריות בין ספק הענן לארגון (לקוח) בהתאם למודלי השירות, הפריסות ומימוש הארכיטקטורה.

שלב א.1 – מיפוי נכסים ואיסוף מידע

בשלב זה ה-CISO נדרש ללמוד ולנתח את הנתונים הרלוונטיים לשירותי הענן בארגון.

1. על ה-CISO להכיר מהו הצורך העסקי של הארגון שבגינו הוא מתכנן לרכוש שירותי ענן (למעט מקרים שבהם השיקול לרכישת שירותי ענן הוא דווקא הרצון להגביר את ההגנה והאבטחה של הארגון).
2. ראשית, נכון יהיה לבחון את הנושא הנדון בהתייחס להגנה על **המידע** מזווית של ארגון הפועל בישראל. על ה-CISO לבחון את מהות המידע שאותו הארגון מבקש לפתח, להשתמש ו/או לאחסן במסגרת שירותי הענן בהיבטים האלה:

2.1 **חוק** או **רגולציה**, המחייבים את הארגון (למשל, **רשות מידע ומשפט** - תקנות הגנת הפרטיות) ואשר עשויים לאסור או להגביל את את השימוש במידע במסגרת שירותי ענן בכלל (למשל, בשל סיווגו הביטחוני, רגישותו העסקית או הגנה על פרטיות) ובדגש של אחסון המידע מחוץ לגבולות ישראל.

2.2 **הקריטיות של זמינות** המידע לתפקוד הארגון, כולל לקוחות וספקים שלו, בייחוד במקרה של מערכת **שפעילותה חיונית** למשק הישראלי, בהתייחס לפגיעה בתשתית התקשורת בין ישראל לחו"ל.

2.3 האם **חשיפת** המידע למי שאינו מורשה **תשפיע** על תפקוד הארגון, ובכלל זאת לקוחות וספקים של הארגון?

2.4 האם **פגיעה באמינות** המידע **תשפיע** על תפקוד הארגון, ובכלל זאת לקוחות וספקים של הארגון?

2.5 האם קיים **שיפור**, או לכל הפחות השוואה **לרמת ההגנה** על המידע במסגרת שירותי הענן לעומת זו הקיימת בארגון?

3. אם אפשר, רצוי לפלח ולהגדיר מהו **החלק** במידע שהוא בעל **רגישות** (למשל: מספר כרטיס אשראי, מספר תעודת זהות).
4. על ה-CISO לבחון האם השימוש בשירותי ענן הינו פן **תפעולי**, אשר פגיעה בו תשליך באופן מיידי ו/או מתמשך על פעילות הליבה של הארגון (Core business). (לדוגמה: **ארגון שעיסוקו המרכזי הוא מכירה באמצעות אתר אינטרנטי, המאוחסן במסגרת שירותי ענן, שפגיעה בזמינותו תהווה פגיעה בתפקודו השוטף של הארגון**.)

5. ה-CISO נדרש להכיר מהו **שירות** הענן שאותו הארגון מתכנן לרכוש (IaaS, PaaS, SaaS).
6. ה-CISO נדרש להכיר את **פרטי ספק הענן** בהיבטים האלה:
   6.1 האם מדובר בספק מוכר ומובילי?
   6.2 האם הספק עומד בתקינה מוכרת, הנוגעת לאבטחת שירותי ענן של ארגונים, כמו, לדוגמה CSA, Nist, FedRAMP, PCI, ISO, HIPPA וכדומה?
7. נדרש לקיים **מודל אחריות משותפת** (Shared Responsibility Model) בהתאם לסוג שירות הענן ופריסתו. מודל האחריות עשוי להיות שונה בין ספק לספק.
8. חשוב כי הגדרת האחריות לתפעול, להתקנה, לתחזוקה ולהגנה של כל שכבה תהיה ברורה ומתועדת **במסמך חוזי** במהלך ההתקשרות.
9. **השכבות** שאליהן יש להתייחס בהסכם החוזי בין ספק הענן ללקוח, **תוך ציון מי מבין הצדדים נושא באחריות בנושאי התפעול וההגנה**, הן:

השכבה	הסבר
מידע	הסוג והתוכן של הנתונים אשר ייעשה בהם שימוש ותהיה אליהם גישה בשירות הנדון.
ממשק המשתמש	האופן שבו הלקוח או מי שיידרש לכך יהיה נגיש למידע.
יישומים	היישומים שבאמצעותם יתבצעו הגישה והשימוש במידע על-ידי המשתמשים.
בסיס נתונים	בסיס הנתונים לשימוש אחסון הנתונים והיישום.
תוכנה	שפות הקוד שנעשה בהן שימוש לפיתוח ולהרצת היישומים.
מערכות הפעלה	הפלטפורמה המנהלת את משאבי החומרה והתוכנה.
מכונות וירטואליות	סביבת האמולציה שהלקוח יעשה בה שימוש.
ממשקי רשת וירטואלית	האופן וההגדרות לתקשורת בין המכונות הווירטואליות בסביבת האמולציה.
Hypervisor	התוכנה והממשק לניהול סביבת האמולציה והמכונות הווירטואליות.
חומרה	המשאבים הפיזיים, כגון כוח עיבוד וזיכרון, המוקצים לשימוש הלקוח.
אחסון	המשאבים הפיזיים המוקצים ללקוח לטובת שמירת המידע ואחסונו.
תקשורת	התווך והאופן שבו מתקיימת גישה בין סביבת הלקוח לסביבת ספק הענן.
מתחם פיזי	המקום שבו נמצאים המשאבים הפיזיים של ספק הענן עבור הלקוח.

10. פירוט האחריות המשותפת בחלוקה למודל השירות:

10.1 **IaaS** - לרוב, ללקוח יש שליטה ואחריות על שכבות רבות - מרמת ממשקי הרשת הווירטואליים ועד המידע.

אחריות הספק במודל IaaS	אחריות הארגון במודל IaaS
• הספק אחראי לספק כוח מחשוב בהתאם לנדרש ולנרכש. • הספק אחראי על זמינותם של משאבי המחשוב לאורך זמן ההתקשרות.	• הקמת מערך התשתית, הכולל: מערך אחסון, מערך שרתים, הגדרות תקשורת פנים-ארגונית. • הגדרת משתמשים. • אחריות על היישום ועל זמינותו למשתמשים. • אחריות על פיתוח היישום, על תפעולו ועל רישוי התוכנה. • אחריות על הגנת המידע המאוחסן (הצפנה, התממה וכו'). • אחריות על המשכיות עסקית.

10.2 **PaaS** - לרוב, ללקוח יש שליטה ואחריות על השכבות של היישומים והאפליקציות.

אחריות הספק במודל PaaS	אחריות הארגון במודל PaaS
• הספק אחראי לספק כוח מחשוב בהתאם לנדרש ולנרכש. • הספק אחראי על זמינותם של משאבי המחשוב לאורך זמן ההתקשרות. • הספק יספק פלטפורמה לפיתוח יישומים ויהיה אחראי לתחזק אותה הן ברמת גירסאות והן מבחינת עדכונים (Patches).	• הגדרות תקשורת פנים-ארגונית. • הגדרת משתמשים. • אחריות על היישום ועל זמינותו למשתמשים. • אחריות על פיתוח היישום, על תפעולו ועל רישוי התוכנה. • אחריות על הגנת המידע המאוחסן (הצפנה, התממה וכו'). • אחריות על המשכיות עסקית.

10.3 **SaaS** - לרוב, ללקוח אין יכולת שליטה ואחריות, למעט על סוג ותוכן המידע ועל הגדרות ממשק המשתמש, והאחריות הינה מלאה של הספק.

אחריות הספק במודל SaaS	אחריות הארגון במודל SaaS
• הקמת מערך התשתית, הכולל: מערך אחסון, מערך שרתים, הגדרות תקשורת פנים-ארגונית. • אחריות על היישום ועל זמינותו למשתמשים. • אחריות על פיתוח היישום, על תפעולו ועל רישוי התוכנה. • אחריות על הגנת המידע המאוחסן. • אחריות על הצפנת המידע, אם צריך. • אחריות על המשכיות עסקית.	• אחריות על נכונות המידע. • הגדרת משתמשים. • אחריות על התממת המידע.

11. **דוגמה** למודל חלוקת האחריות בין ספק הענן ללקוח בחלוקה לשכבות **(כפי שמוצג בתקן PCI)**.

ספק ענן לקוח

שכבה	מודל שירות		
	IaaS	PaaS	SaaS
מידע			
ממשק המשתמש			
יישומים			
בסיס נתונים			
תוכנה			
מערכות הפעלה			
מכונות וירטואליות			
ממשקי רשת וירטואלית			
Hypervisor			
חומרה			
אחסון			
תקשורת			
מתחם פיזי			

12. כאמור, הכרחי לקבוע **מודל אחריות** בין הארגון (לקוח) לבין ספק הענן, אך אין הדבר פוטר את ה-CISO מהיכרות עם הפרטים והמאפיינים התהליכיים והטכניים של כל שכבה המצוינים בסעיף הקודם.

גם בשכבות שבהן סוכם כי האחריות המלאה מוטלת על ספק הענן**,** בבואו להתייחס לפעילות והשירותים שהארגון צורך במסגרת הענן בבניית תכנית ההגנה הארגונית - על ה-CISO להכיר ולהתייחס לכל אחת מהשכבות ולשאול את השאלות האלה**:**

12.1 **מה הן הבקרות הנדרשות והמתאימות לכל שכבה?**

12.2 **האם הבקרות מתקיימות?**

12.3 **האם אפשרי לקיימן כדרישה מהספק או על-ידי הארגון בהתאם למודל האחריות?**

12.4 **במידה ולא - האם קיימות בקרות מפצות שאפשר לקיימן?**

12.5 **במידה ולא - האם הסיכון שלא לקיים את הבקרות הנ"ל הינו מידתי?**

12.6 מהו המיקום הגיאוגרפי של השכבה, **"מתחם פיזי"**? בהיבט הנגישות של הארגון, סמכויות משפטיות, פוטנציאל לסנקציות על רקע פוליטי בגין העובדה שהארגון (לקוח) הוא ישראלי.

12.7 אילו מבין שירותי "הענן" הינם של הספק (In House) ואילו הוא רוכש מספק משנה, ומיהו ספק המשנה?

12.8 רצוי לפלח גם במקרה זה את שירותי הענן **לשכבות**. הדבר יסייע ל-CISO לדעת מה הם המוצרים שאותם רוכש הארגון במסגרת שירותי הענן בהיבט חומרה, תקשורת, תוכנה ויישומים, לנתח את הסיכונים והחולשות המוכרים לכל אחד מהמוצרים בשלב התכנון ולאחר מכן לאורך מתן השירות, ובהתאם לכך לבחור בקרות ומענים תואמים.

12.9 ראוי שה-CISO יכיר אירועי עבר, כגון תקיפות, הנוגעים לספק שירותי הענן ו/או לספקי המשנה שלו, במסגרת השירותים הניתנים לארגון.

שלב א.2 - ניתוח הסיכון

בשלב זה נדרש ה-CISO לגזור את האיומים של שירות הענן על הארגון על סמך המידע שאסף וניתח.

13. ה-CISO נדרש לרכז תרחישים רלוונטיים של פגיעה בארגון במסגרת שירות הענן.

14. ה-CISO צריך להכיר ולהתייחס לפריסה ולארכיטקטורת המימוש בענן המתוכנן ו/או הקיים במודל השירות שהוא רוכש.

15. במסגרת בניית התרחיש, נכון יהיה לבחור, ראשית, את **האיום** - הנזק הסופי הרלוונטי, זאת בהתאמה למודל השירות והפריסה של הענן.

לדוגמה**:** ה-CISO ניתח כי "**במידע המאוחסן ב-DB במסגרת שירותי ענן קיימת רשומה המכילה כתובת למשלוח של לקוחות, ששינוי שדות בה ופגיעה באמינותה עשויים לגרום לארגון נזק תפעולי וכספי רב, ומכאן על ה-CISO לנתח מה הם התרחישים אשר בגינם ייגרם שינוי השדות".**

16. בשלב הבא עליו **להעריך** מהי סבירות המימוש של כל תרחיש, תוך התייחסות לבקרות הקיימות, על-מנת לבחון בקרות נוספות נדרשות, בהתייחס לפרמטרים האלה:

16.1 רמת המומחיות והמשאבים הנדרשים למימוש התרחיש.

16.2 רמת הפגיעות של הרכיבים הרלוונטיים למימוש התרחיש.

16.3 רמת הנגישות הלוגית לנכס, בהתייחס למודל השירות, הפריסה וארכיטקטורת מימוש הענן.

16.4 רמת הנגישות הפיזית לנכס, בהתייחס למודל השירות, הפריסה וארכיטקטורת מימוש הענן.

17. לאחר בחירת התרחישים לכל נזק סופי רלוונטי, על ה-CISO לשקול בסדר עדיפות יורד - מהתרחיש הסביר ביותר ומטה - אילו בקרות נדרש ליישם? האם ניתן ליישמן? במידה ולא - מה הן החלופות התפעוליות עסקית המתייחסות למודל השירות, הפריסה וארכיטקטורת המימוש בענן אשר ייתנו מענה העומד בניהול סיכונים סביר?

18. אם נחזור לדוגמה של **"שינוי פרטי רשומה, המתייחסת לכתובת לקוח המאוחסנת בשרת DB בענן, אשר שינויה יגרום נזקים תפעוליים וכספיים לארגון",** אזי דוגמה לשיטה של ניתוח הסיכון תיראה כך:

האיום	פגיעה באמינות המידע - שינוי פרטי רשומה, המתייחסת לכתובת לקוח המאוחסנת בשרת DB
מודל שירות הענן	IaaS
פריסת הענן	Public
ארכיטקטורת מימוש הענן	Multi-Tenants

התרחיש	ניתוח הסבירות	הערכת הסבירות	בקרות שיש לשקול
גישה של "דייר" אחר לרשומה.	• רמת מומחיות ומשאבים - נמוכה. • רמת הפגיעות של שרת ה-DB - בינונית. • רמת הנגישות הלוגית של "דייר" אחר - בינונית. • רמת נגישות פיזית - נמוכה.	בינונית	• הצפנה - הפרדה על-ידי הצפנה חזקה עם ניהול מפתחות נפרד, בניהולו של הארגון ולא של הספק. • VPC - התפלגות וירטואלית של סביבות, יצירת ענן פרטי בתוך הענן הציבורי. • הפרדת דיירים - הפרדה על-ידי שימוש ברכיבים פיזיים נפרדים.

פרק ב': בקרות הגנה לשירותי ענן

פרק זה יפרט ויביא דוגמאות לדגשים לבקרות הגנה הרלוונטיות ליישום בבניית תכנית הגנה על-ידי ה-CISO לשירותי ענן בארגון.

ב.1 – מתווכי אבטחת גישה בשירותי ענן (Cloud access security brokers – CASBs)

CASBs הן מערכות אבטחה ובקרה, אשר חלקן נמכרות על-ידי ספקי ענן וחלק על-ידי חברות צד שלישי. המערכות ממוקמות בתווך שבין הלקוח לספק הענן לטובת שילוב והפרדה בהתאם להגדרות האבטחה של הארגון (לקוח) בעת שימוש וגישה של הלקוח ליישומים ולשירותים במסגרת שירותי הענן. זאת לטובת מתן מענה לסיכונים בשירותי ענן, לאכוף מדיניות אבטחה ולעמוד בדרישות רגולציה, גם כאשר שירותי הענן חיצוניים לאתר הלקוח ומחוץ לשליטה ישירה של הלקוח.

מאפיינים ויכולות של מערכות CASBs הן:

1. **חשיפה** - מתן יכולת ללקוח לראות ולשלוט בשירותים מורשים ולא מורשים, לאפשר בקרה של הגנת הסייבר ו/או ה-IT של הלקוח במקום לחסום לחלוטין שירותי ענן מסוימים, לנהל ולהגביל בתוך השירותים גישה לפעילות ולמידע בחלוקה להרשאות משתמשים ו/או מכשירים.

   חשיפת פעילות IT שאינה גלויה (Shadow IT) - בדמות יישומים, שימוש, משתמשים, מידע וקבצים בסביבת הענן וביישומי צד שלישי המחוברים לענן כולל מכשירים ניידים ולקוחות מסונכרנים.

2. **ציות** - מתן אפשרות לבדיקת עמידה בדרישות רגולציה החלות על הארגון לצורך שמירה והבטחה של ההגנה ופרטיות המידע של הלקוח, בדיקת יישומים ושימוש בהם אל מול הרגולציה הרלוונטית החלה על הארגון, ובעת זיהוי פערים - מתן יכולת לבצע פעולות שינוי ו/או מניעה על-מנת לעמוד בדרישות.

3. **הגנה על המידע** - שימוש ביישום אבטחה בענן של מכניזם לזיהוי ומניעת דלף מידע (DLP), כגון קביעת "טביעת אצבע" למסמכים בשילוב הקשרים (משתמש, מיקום, פעילות וכדומה). ניהול הרשאות ושיתוף מידע ויצירת דו"חות והתראות מתואמים אישית, כמו גם שימוש בהצפנה להעברת המידע.

4. **הגנה מפני איומים** - יכולת לסרוק, לאתר, לטפל ולחסום פעילות זדונית ו/או לא מורשית בשירותי ענן מאושרים ולא מאושרים על-ידי שימוש בניתוח נוזקות באופן סטאטי או דינמי, זיהוי אנומליות משתמש ותעדוף טיפול באירועים בהתאם לחומרה.

ב.2 – קבלת שירות ממספר ספקי ענן במקביל

1. לעתים ארגונים בוחרים או נאלצים לצרוך שירותי ענן מספקים שונים - אם בשל שיקולי עלות, שוני ביישומים הנדרשים ולעתים אף כתפיסת הגנה של הפרדה ופיזור של הסיכון.

2. קיימים אתגרים בסנכרון בין הספקים אשר חלקם מספקים שירותים בתחום של תפעול ה-IT וחלקם בתחום של הגנת המידע.

3. קיים חוסר במערכת בקרה תקנית, אשר תשמש כ-API בין שירותי הענן של הספקים השונים, על כן ניתן לבצע שימוש במערכות קוד פתוח או בשירות של ניהול שירותי ענן של ספק צד שלישי לניהול בקרה מרוכזת בעלת יכולת ניטור יישומים ושרתים, בקרת גישה ואכיפת מדיניות.

4. לא כל ספקי הענן מציעים אותם שירותים בדגש על כלי הודעות, זרימת עבודה וניהול ועובדה זו לעתים כופה עבודה ברמה הנמוכה של המכנה המשותף. מענה לכך הוא שימוש בתוכנה מצד שלישי, לרוב קוד פתוח, המאפשרת שירות חלופי אשר יתאים בסביבות של כל ספקי הענן.
5. גם בשימוש בשירותים דומים ומקובלים בין ספקי הענן תיתכן שונות באופן שבו מבוצע ניהולו של אותו שירות. גם במקרים אלה קיימים ספקי צד שלישי, המספקים API, שהותאמו לשימוש מול ספקי הענן השונים.

ב.3 – בקרות הגנה לארגון בשימוש בשירותי ענן

הבקרות מתייחסות ספציפית לשירותי הענן והן הרחבה לפרק הבקרות, שה-CISO נדרש ליישם בתכנית ההגנה המלאה של הארגון לפי **תורת ההגנה בסייבר לארגון** של הרשות הלאומית להגנת הסייבר.

(עמודת ה"זיהוי" מתייחסת לזיהוי הבקרה בתורת ההגנה בסייבר לארגון בהקשר הקרוב ביותר במידה שקיים.)

זיהוי IDENTIFY			
משפחה	**זיהוי**	**הבקרה**	**דוגמה ליישום הבקרה**
אחריות דירקטוריון והנהלה תאימות	3.1 3.2	וידוא כי קיימים תהליכים אפקטיביים של מדיניות ניהול סיכונים וציות לתקן	1. מדיניות אבטחת מידע והגנת סייבר ארגונית בהיבט שירותי הענן של הארגון, כתובה ומאושרת על-ידי הנהלת הארגון וספק הענן, איומים, תרחישים ובקרות למניעתם, נוהלי DR &BC ונוהלי זיהוי אירועים ותגובה. 2. אישורים לכך, שספק הענן עומד בתקינה מתאימה להגנה על שירותיו, כגון: א. אבני התווך הן **ISO27001** - תקן של מכון התקנים הבינלאומי, המגדיר את עקרונות ההקמה, הניהול והתחזוקה של מערכת אבטחת מידע המתאימה לארגון, או **SOC2** - תקן של AICPA, ארגון רואי החשבון האמריקני, אשר בודק בקרות אבטחה לשמירה על זמינות, אמינות וסודיות המידע בארגון. ב. **CSA STAR** - הסמכה הנחשבת מובילה בתחום, המגיעה בשלוש רמות הסמכה. הרמה השנייה מתבססת על קיום ISO 27001 ומטריצה של Best-practice, הנקראת CCM. ג. **ISO 27017/27018** - תקנים של מכון התקנים הבינלאומי, המגדירים בקרות הגנה ופרטיות בשירותי ענן. ד. **PCI-DSS** - תקן של חברות האשראי להגנה על נתוני ועסקאות אשראי. בתקן קיים מסמך בשם Cloud Computing Guidelines. ה. **NIST** - SP 144-800 - בקרות הגנה על שירותי ענן לפי הארגון לתקינה טכנולוגית, שארגונים פדראליים בארה"ב נדרשים לו במסגרת FISMA (Federal Information Security Modernization Act) לשם רישיון הפעלה. ו. **FedRAMP** - תכנית אמריקנית פדרלית להערכת סיכונים, הרשאות ובקרה לשירותי ענן (רלוונטית לפעילות חברה בארצות הברית, בייחוד מול גופי ממשל). ז. **רשות מידע ומשפט** - תקנות הגנת הפרטיות 7809, המגדירות הגנה על מאגרי מידע. ח. EU General Data Protection Regulation **(GDPR)** - תקנות הגנת הפרטיות של האיחוד האירופי. ט. **HIPAA** - חוק החל בארצות הברית ועיקרו שמירה על הפרטיות והאבטחה של מידע רפואי חסוי.

זיהוי IDENTIFY			
משפחה	**זיהוי**	**הבקרה**	**דוגמה ליישום הבקרה**
תאימות		אכיפת מדיניות פרטיות	3. הסכם משפטי במעורבות היועץ המשפטי של הלקוח, המגדיר באופן ברור את האחריות של ספק הענן בנוגע להגנה על מידע המאפשר זיהוי אישי, והכולל התייחסות לשיפוי במקרים של נזק או אובדן. 4. החתמת ספק הענן על הסכמים של רגולטורים רלוונטיים להגנה על פרטיות. 5. הפרדה בין מאגרי מידע - מידע המאוחסן בשירותי הענן ומכיל רשומות אנונימיות ומידע החושף זיהוי אישי בחיבור לרשומות האנונימיות, יאוחסן באתר הלקוח או באופן מאובטח יותר אצל ספק הענן.
בקרה וביקורת	3.4	ביקורת לתהליכים תפעוליים ועסקיים	6. קבלת דו"חות ביקורת מספק הענן, שבוצעו על-ידי גורם ביקורת צד שלישי עצמאי, לגבי התהליכים התפעוליים והעסקיים הקיימים במסגרת השירותים, להבנת בקרות ההגנה שספק הענן מיישם במסגרת שירותיו, בדגש על הנושאים האלה: א. בקרות הגנה המוודאות הפרדה בין יישומים ומידע של הלקוח ללקוחות אחרים בסביבה של "ריבוי דיירים". ב. בקרות הגנה המוודאות מניעת גישה לא מורשית של עובדי ספק הענן למידע וליישומים של הלקוח (לדוגמה, SOC2). 7. וידוא כי מבוצעות גם ביקורות לקיום הגנה על האמצעים לשירות עצמי, הנוספים לשירותים שניתנים על-ידי ספק הענן, כגון אמצעי רישום לשירות, או תהליכים לביצוע תשלום. אמצעים אלו, אשר מצויים, כאמור, בשימוש עצמי של הלקוח, לרוב פגיעים יותר לסיכון מאשר השירות עצמו, ועל כן נדרש לוודא, כי הביקורות שמבוצעות כוללות גם אותם.

הגנה PROTECTION			
משפחה	**זיהוי**	**הבקרה**	**דוגמה ליישום הבקרה**
שרשרת אספקה ומיקור חוץ	16.2	שימוש בכלים משפטיים וחוזיים להגדרת האחריות של ספק הענן והלקוח	8. חוזה שירות מחייב, המפרט את חלוקת האחריות בין הספק לארגון. ניתן לפרט לרמת השכבות. האחריות צריכה להתייחס להגנה על השכבה, לתפעול ולטיפול בתקלות. 9. חוזה השירות צריך לכלול את מיקום המידע (פיזית - באילו מדינות), את החוקים החלים עליו והתחייבות, כי המידע לא יעבור לתחום שיפוט אחר ללא הסכמת הלקוח. 10. בחוזה נדרש לכלול התייחסות גם לכל ספק משנה, שספק הענן הראשי משתמש בו במסגרת שירות הענן. 11. בחוזה השירות צריכה להיות התייחסות לגבי חובת הדיווח של ספק הענן ללקוח בנוגע לאירועים של חדירה לרשת, גילוי נוזקות, תקלות וכשלים וכל אירוע אשר סיכן או השפיע על המידע והתפקוד של הלקוח במסגרת שירות הענן. 12. בנושא הדיווח, בחוזה נדרש לפרט לוחות זמנים, את אופן הדיווח, ציון גורם האחראי לאירוע כחלק מקביעת מדדים לשיפוי ופיצוי הלקוח במידת הצורך. 13. דוגמה לחוזה שירות המוצג על-ידי ארגון ה-CSA (Cloud Security Alliance): "Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union"

הגנה PROTECTION			
משפחה	זיהוי	הבקרה	דוגמה ליישום הבקרה
בקרת גישה משאבי אנוש	4.6 4.7 4.29 4.34 19.10	ניהול אנשים, תפקידים וזהויות	14. בקרב לקוחות אשר בארגונם קיימת מערכת לניהול זהויות והרשאות מומלץ להרחיב את השימוש בה במסגרת הגישה לשירותי הענן הן בהביטי יעילות והן בהיבטי בקרה על שינוי תפקיד של עובד וסיומו. 15. הלקוח צריך להיות בעל הרשאות לניהול הזהויות וההרשאות של המשתמשים. 16. על הלקוח לאפיין כיצד מתבצע הסנכרון בעת הקמת משתמש חדש, בדגש על משרות זמניות, שינוי משתמש קיים וסגירת משתמש שעזב, כשלים בסנכרון זה יכולים להותיר סיכון לחשיפת מידע. 17. יכולת לביצוע כניסה והתנתקות של המשתמש בתהליך יחיד (AD federation) על-מנת לוודא, כי תהליך החיבור לכל שירותי הענן הסתיים, רכישת שירות IDentity as a Service (IDaaS). 18. ביקורת (Audit) ולוגים על גישה ושימוש של משתמשים בשירותי הענן, הכוללים זיהוי משתמש בהתחברות (שם משתמש, תחנה שממנה בוצע החיבור, כשלים בהתחברות, גישה או כישלון גישה לאזורים ממודרים), שליפה או הוצאה של מידע כגון הדפסה ועוד. 19. תמיכה במנגנוני הזדהות מורכבים וחזקים, כגון הזדהות דו/רב-שלבית, ביומטרי וכדומה. 20. מתן יכולת ללקוח להגדיר ולאכוף במסגרת הגישה לשירותי הענן את ניהול התפקידים והקבוצות בארגונו בהתאם למדיניות ההגנה שבה הוא פועל. 21. הגבלת גישה לפי סוג ההתקנים, כתובות רשת ו-MAC ומיקום גיאוגרפי.

הגנה PROTECTION			
משפחה	**זיהוי**	**הבקרה**	**דוגמה ליישום הבקרה**
הגנה על המידע	5.2 5.3 5.4 5.5	פילוח המידע וסיווגו לטובת יישומה של הגנה נאותה	22. יצירת רשימה של נכסי המידע - זיהוי הנכסים, סיווגם בהיבט חשיבותם ללקוח ו/או רגולציה החלה עליהם, הגדרת הבעלים והנושאים באחריות על המידע, מיקום המידע והנגישות אליו. 23. התייחסות לכל סוגי המידע: א. מידע מובנה (ERP, CRM) שמאוחסן במאגרי מידע בסביבה מרובת דיירים - הגנה על-ידי הפרדה ובידוד **או** ערבוב בתוך מאגר המידע, שימוש בהצפנה כהגנה על המאגר. ב. מידע לא מובנה (תמונות, סריקות מסמכים וקובצי מולטימדיה) - יכול להיות רגיש ונדרש ליישם עריכה או מיסוך של מידע, כגון חתימות, כתובות מגורים ופרטים אישיים אחרים. 24. התייחסות לפרטיות המידע - לפי המוגדר בחוק וברגולציה על נגישות, אחסון ושימוש במידע המאפשר זיהוי אישי. יצירת הגבלות בגישה ובשימוש במידע הנדון, סימון המידע ככזה, אחסון באופן מאובטח בהתייחס, למשל, למיקום גיאוגרפי, ומתן גישה רק למשתמשים מורשים. 25. יישום סודיות, אמינות וזמינות של המידע - שימוש ביישומים שניתן לבצע בהם סיווג של המידע, הצפנה של מידע רגיש באחסון ובהעברה והתייחסות לאחסון מפתחות ההצפנה בנפרד, שימוש בטכניקות של אימות המידע, כגון גיבוב (Hashing), שימוש בגיבוי וביישומי התאוששות מהירה. 26. יישום מנגנוני זיהוי והרשאות גישה למידע ואיסוף היסטוריה ולוגים של גישה ושימוש לטובת ביקורת וחקירה. 27. ניטור פעולות של העברת המידע בין הלקוח וספק הענן לצורך הפחתה/מניעה של העברת מידע לא מורשה באמצעות: א. Database Activity Monitoring (DAM) ב. File Activity Monitiroing (FAM) ג. Url Filtering ד. Data loss Prevention (DLP) 28. שימוש במנגנון IDA, שבאמצעותו מפוצל המידע לכמה חלקים, כאשר כל חלק מאוחסן בשרת אחסון שונה. 29. במודל IaaS - הצפנת הכוננים (Volumes) על-מנת להגן מפני שכפול וגישה לא מורשית.

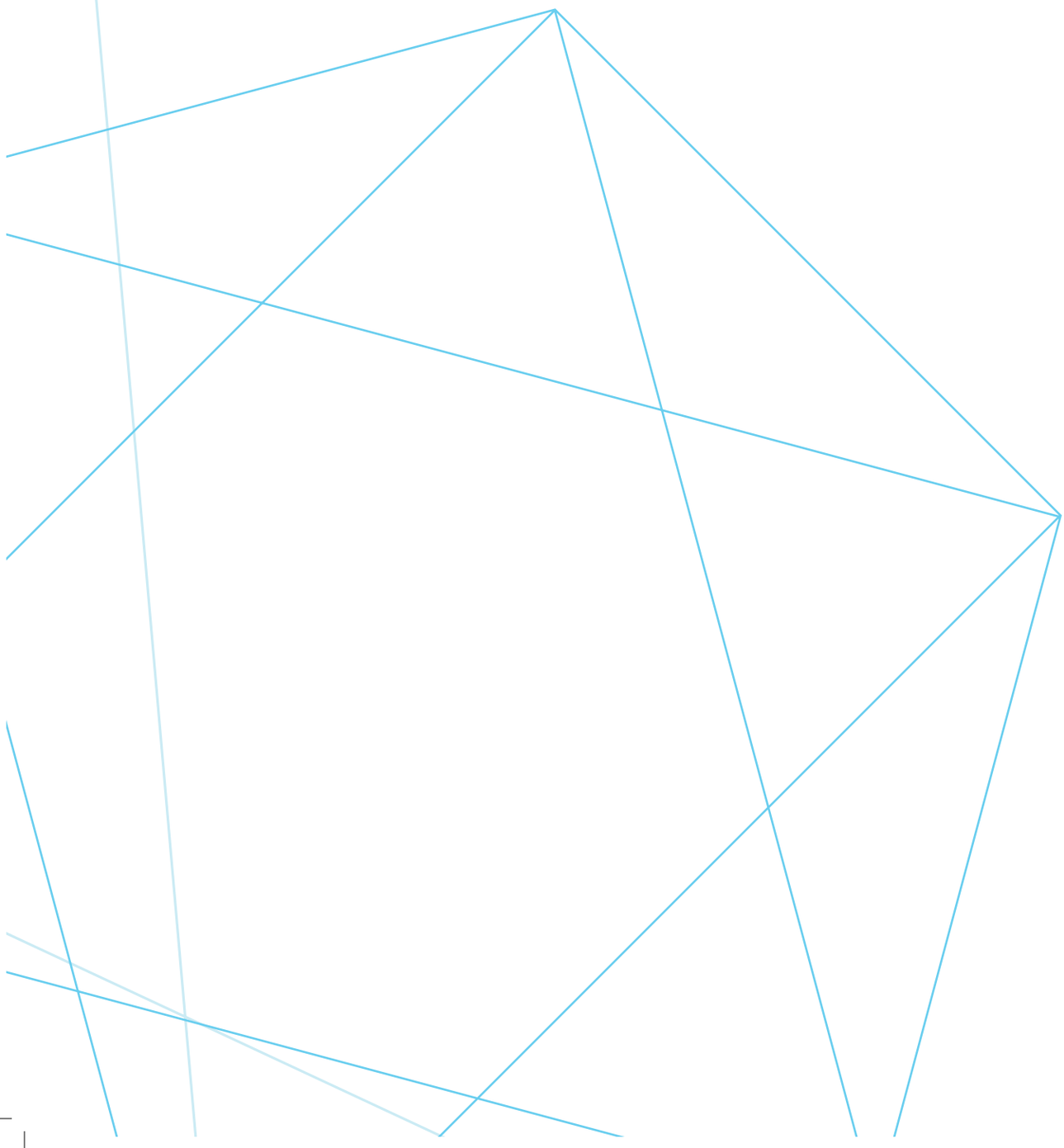
הגנה PROTECTION			
משפחה	זיהוי	הבקרה	דוגמה ליישום הבקרה
אבטחת רשת מניעת קוד זדוני הפרדת סביבות	7.1 7.6 9.3 9.9 9.24 10.2 10.8 10.9	סינון, איתור והפרדה להגנה על תעבורת הרשת	30. סינון תעבורת רשת באמצעות יישומים כגון Firewall - במידה שקיים שירות Firewall המנוהל על-ידי הספק (לרוב מנוהל על-ידי הלקוח). א. דרישה לקבל מספק הענן את רשימת הפורטים הפתוחים. ב. התייחסות לסינון תעבורת רשת גם בפרוטוקול IPv6 ולא רק IPv4. 31. הגנה מפני התקפת מניעת שירות (DDOS) - יכולת ספק הענן וספק האינטרנט שלו להתמודד עם תעבורת רשת גבוהה, כגון זיהוי מתקפה בסדר גודל גדול על הספק, זיהוי מתקפה בסדר גודל קטן הממוקדת על שרת הלקוח, התרעות אוטמטיות על מתקפה, שימוש ב-WAF, (Web Appliction Firewall) יכולת ניתוח לאחר תקיפה. 32. שימוש בתוכנות מעודכנות לסריקה והגנה מפני נוזקות (Malwares), המסופקות על-ידי ספק הענן או על-ידי תוכנת צד שלישי בעלת API מתאים לשירותי הספק: א. ברמת מערכות ההפעלה של תחנות הקצה והשרתים - Anti Virus מנוהל ומועדכן באופן שוטף, במודלים של SaaS ו-PaaS - באחריות הספק, במודל Iaas - באחריות הלקוח. ב. סינון תעבורת התקשורת - שימוש במערכות IPS/IDS, WAF, בכל המודלים - באחריות הספק. ג. סינון תעבורה וקבלת קבצים בדוא"ל ובגלישה - שימוש במערכות MailRealy ו-SandBox, במודלים SaaS ו-PaaS - באחריות הספק, במודל Iaas - באחריות הלקוח. ד. סינון גלישה על-ידי שימוש ב-URL Filtering וב-Proxy, בכל המודלים - באחריות הספק. 33. לוגים ועדכון: א. קבלת יכולת מספק הענן לחזות במצב התקינות של הרשת על-ידי מערכת או ממשק בזמן אמת. ב. הבהרה בנוגע לתרחישי טיפול באירועים (כגון תקיפה) ואופן הדיווח ללקוח - הגדרת סוג האירועים אשר ספק הענן ידווח עליהם ללקוח, כגון איתור קוד זדוני בשרת הלקוח או איתור תקשורת זדונית משרת הלקוח לשרת תקיפה (C&C), אופן הטיפול באירוע, סיוע בהערכת נזק ופעולות תיקון והגנה למניעת הישנות. ג. התייחסות למגבלות חוקיות בנוגע לאיסוף לוגים ולאחסונם בהיבט של הגנה על הפרטיות. ד. הגדרה של הלקוח מול ספק הענן אילו לוגים וכיצד הוא יכול לקבלם לטובת חקירה עצמאית של אירועים.

הגנה PROTECTION			
משפחה	זיהוי	הבקרה	דוגמה ליישום הבקרה
אבטחת רשת מניעת קוד זדוני הפרדת סביבות	7.1 7.6 9.3 9.9 9.24 10.2 10.8 10.9	סינון, איתור והפרדה להגנה על תעבורת הרשת	34. כלים ואמצעים להפרדה בין לקוחות שונים ובין לקוחות לרשת האינטרנט: א. שימוש בהתפלגות רשת (Segmentation) באמצעות שימוש בחלוקת רשת וירטואלית (Vlan's). ב. תעבורה מוצפנת - התחברות לשירות "site-to-site" או "client-to-site" באמצעות תווך רשת פרטית וירטואלית (VPN), שימוש בהצפנה, כגון IPsec, SSL/TSL. ג. Firewall לסינון תעבורה בין Vlan's. ד. סינון תעבורת רשת על-ידי הספק, למשל באמצעות ה-Hypervisor או Ebtables (תוכנה ב-Linux לסינון תעבורת רשת). 35. הקשחה של מכונות וירטואליות ושרתים, כגון חסימה וביטול של שירותים (Services), שימוש במערכת Pacth Manaegment לעדכון טלאי אבטחה - במודלים SaaS ו-PaaS - באחריות הספק, במודל IaaS - באחריות הלקוח. 36. הגנה על הרשת הפנימית של ספק הענן - הלקוח צריך לוודא, כי ספק הענן מיישם בקרות הגנה ברשת הפנימית שלו, הצגת ממצאי דו"ח ביקורת צד שלישי או הסמכת תקינה רלוונטית.
הגנה פיזית וסביבתית	18.8 18.15 18.17 18.19 18.20	בקרות הגנה על אמצעים ואתרים פיזיים.	37. בחינת הסיכונים הקיימים לגבי המיקום הפיזי הגיאוגרפי של מקום אחסון המידע על-ידי ספק הענן, בהיבט של אסונות טבע, רמת פשיעה ואי-סדר חברתי/פוליטי. 38. יישום בקרות סינון ומניעה של גישה פיזית למי שאינו מורשה לאתרים של ספק הענן ולמתחמים אשר מאחסנים אמצעים ותשתיות, המשמשים את הלקוח במסגרת שירותי הענן - מתחם מגודר, שומרים, בקרת כניסה אלקטרונית, ניטור מצלמות, אזעקה אלקטרונית וכו'. 39. יישום בקרות מניעה וצמצום נזק כתוצאה מאירועים חיצונים וסביבתיים, כגון: מזג אוויר, הצפה, שריפה, רעידת אדמה, קצר חשמלי ואחרים - לדוגמה: הוכחת עמידה בתקן הישראלי 1243 "בטיחות אש של מחשבים וציודם ההיקפי", או ב-ISO 27001, המגדיר, למשל, כיבוי בגז בחדר שרתים וארונות חשמל, חיישני טמפרטורה, פתרונות ניקוז מים, אלפסק (UPS) ו/או גנרטור ועוד. 40. יישום בקרות כנגד גניבה, אובדן פגיעה בזדון וונדליזם של אמצעים ותשתיות, הרלוונטיים לשירות הענן - בקרת כניסה אלקטרונית, שומרים, ניטור מצלמות, אזעקה אלקטרונית, נעילות וכו'. 41. בקרות מניעה כנגד אובדן מידע ו/או זליגתו במקרה של זריקה/סילוק או שימוש מחדש בציוד המאחסן מידע - ניהול רישום מצאי, שימוש בחברות לגריטה וגריסה של ציוד אלקטרוני ומדיה מגנטית, ביצוע מחיקה עמוקה WIPE לזיכרונות שאינם נדיפים.

איתור DETECT			
משפחה	**זיהוי**	**הבקרה**	**דוגמה ליישום הבקרה**
תיעוד וניטור	21.4 21.5 21.12	קבלת התראות ודיווחים מספק הענן	42. גישה של הלקוח להתראות של מערכות בקרת האבטחה של ספק הענן, כגון SEIM, המתייחסות לזיהוי חשד לאירוע זדוני. 43. קבלת דיווחים מספק הענן על כל אירוע שהיווה סיכון או פגיעה לנכסי הלקוח, הכוללים לוגים המאפשרים ניתוח פורנזי של האירוע- • זהות המערכת שהסנסור שלה דיווח ל-SEIM, החוק ב-SIEM שבגינו נוצרה ההתרעה. • פעולות בדיקה וחקירה שבוצעו לאימות או לאישוש ההתרעה. • פעולות תיקון למניעת הישנות וכדומה. 44. קבלת דו"חות ניתוח מספק הענן, המתייחסים לאימות, להרשאות ולניהול המידע, הנוגעים ליישומים ולמידע שבשימוש הלקוח אל מול בקרות ההגנה שספק הענן מיישם.

תגובה RESPOND			
משפחה	**זיהוי**	**הבקרה**	**דוגמה ליישום הבקרה**
ניהול אירועים ודיווח	24.3	קביעת תכנית מול הספק ל"תגובה לאירועים"	45. וידוא כי לספק השירות יש שירות "תגובה לאירוע" (incident response), אשר נוגע בנושאים אלה: א. זיהוי אירוע - כיצד מזוהה, האם מבוצע ניטור 24/7, האם קיים ניתוח של הזיהוי על-ידי אנליסט או באופן טכנולוגי אוטומטי. ב. כוח אדם מומחה לטיפול באירוע - הצהרת הספק לגבי רמת הידע המקצועי של כוח האדם, יחס כוח אדם אל מול כמות האירועים ולקוחות הספק. ג. תהליך ניתוח ובחינה עמוקה לאיתור הגורם לאירוע ויישום פעולות למניעת הישנות - האם קיימת מתודלוגיה סדורה, התרשמות מדו"חות סיכום של אירועים קודמים שטופלו על-ידי הספק. 46. קביעה בכתב של אופן, לוחות הזמנים וסוג האירועים לדיווח ללקוח על האירוע, למשל: קבלת דיווח על אירוע שנגרמו בו אחד או יותר מה-CIA, דליפה, שיבוש או זמינות של מידע ושירותים הרלוונטיים ללקוח, טיפול הספק בחשד לאירוע שלא הוזם תוך 24 שעות וכדומה. 47. קביעה בכתב של אופן, שלב וסוג האירועים לשיתוף צוות תגובה מטעם הלקוח בטיפול באירוע - בהתאם ליכולת הלקוח לספק צוות תגובה ונכונות הספק לאפשר זאת. הנ"ל רלוונטי במודל IaaS בעיקר.

התאוששות RECOVER			
משפחה	**זיהוי**	**הבקרה**	**דוגמא ליישום הבקרה**
המשכיות עסקית	25.1 25.10 25.14 25.17 25.19	יישום תכניות גיבוי והתאוששות של ספק הענן במקרה של תקלה או נזק.	48. וידוא כי לספק הענן יש תכנית כתובה להמשכיות עסקית (BCP) ולהיערכות החברה להתאוששות מאסון (DRP) והאם היא תורגלה. 49. וידוא כי לספק יש אתר DR, אשר אליו מבוצעים גיבויים "חמים" (בזמן אמת) ו/או "קרים" (במועדים קבועים) בהתאם להגדרת הנחיצות והקריטיות של המידע עבור הלקוח. 50. בדיקה מהו המיקום הגיאוגרפי של אתר ה-DR ובחינה האם קיימות מגבלות רגולטוריות או סיכונים מצד השלטון או המצב הפוליטי-ביטחוני במדינה שבה נמצא האתר, שיכולים להשפיע על זמינות האתר ועל תפעולו. 51. קביעת SLA לקבלת שירות, ל"עלייה לאוויר", לשחזור גיבויים - בהתאם לניתוח הלקוח של קריטיות הזמינות של השירות או של המידע עבורו (דקות/שעות/ימים) - הלקוח יתעדף את ה-SLA מול הספק בהתאם לתעריף התשלום והיכולת הטכנית של הספק.
	11.2	הגדרת תהליך סיום השירות	52. הגדרת זמן הודעה מראש משני הצדדים על הפסקת התקשרות - נהוג 30 יום תוך ציון בחוזה ההתקשרות. 53. הלקוח צריך להכין מראש תוכנית מפורטת להעברת המידע או השירות (אם נדרש המשך פעילותו) לספק ענן אחר, בטווח זמן ההודעה מראש. 54. נדרש להגדיר מראש מול ספק הענן דרך מאובטחת להעברת המידע של הלקוח שאחוסן אצל ספק הענן בסיום ההתקשרות, בהתאם לצורכי הלקוח ולדרישותיו - למשל, העברה פיזית של אמצעי אחסון או בתקשורת מוצפנת, בהתאם לכמות ולסוג המידע. 55. הגדרה בחוזה ההתקשרות, כי ספק הענן מחויב לשמור לטווח זמן של בין 1-3 חודשים את המידע של הלקוח על-מנת לוודא כי העותק שהועבר ללקוח שמיש וללא ליקויים. 56. יש להגדיר, כי מחיקת המידע תבוצע באישור כתוב של הלקוח ולא באופן חד-צדדי על-ידי הספק. 57. נדרש להגדיר מראש מול ספק הענן את אופן מחיקת המידע בעת סיום ההתקשרות מולו, ובמסגרת זאת גיבויים, לוגים ודו"חות ביקורת, בצורה שתבטיח ללקוח כי לא יהיה אפשר לשחזר את המידע וכי אין חשש שידלוף לגורם שאינו מורשה, שימוש במחיקה עמוקה (Wipe) ורישום מחדש של נתונים על דיסק האחסון. 58. קבלת הצהרה כתובה רשמית מהספק, כי המידע נמחק בהתאם למנגנון שעליו סוכם עם הלקוח.



משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

לפמ