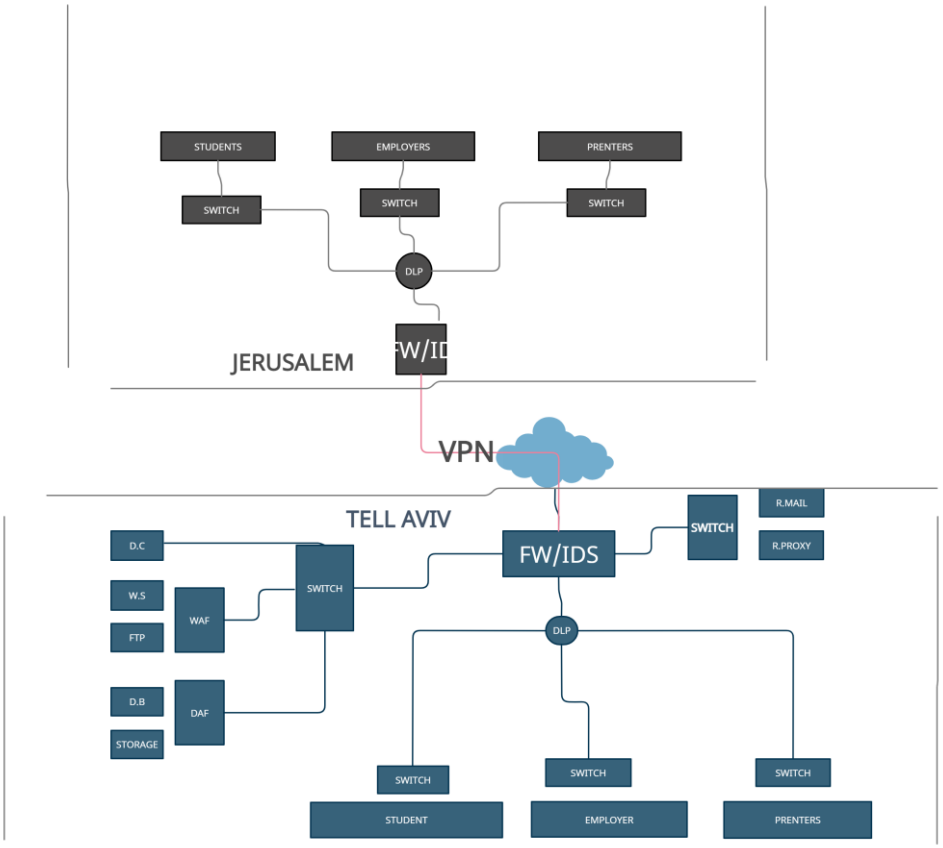
# NITS-Cyber Security Framework




1. Identify - שלב זיהוי נכסים והסקת פוטנציאל הנזקים
2. Protect - הגנה על ארגון באמצעות כלים טכנולוגים
3. Detect - זיהו וניטור של איומים שונים
4. Respond - שלב תגובה לאירועים
5. Recovery - שלב שיקום וחיזוק הארגון לאחר אירוע

## ----------Identify----------

**)שלב זה שלב מאוד קריטי בשביל לעשות עבודה מאוד טובה בעולם אבטחת מידע**

**בשלב זה אנו מרכזים את הנכסים של הארגון, מחשבים את פוטנציאל הנזקים שיכולים להיות**

**לטובת עבודה הזו בלבד אני לוקח כ4 אסטים מרכזים בשביל להדגים כל שלב ושלב במודל הזה(**

### Assets

- עובדים ולקוחות - יועצי לימוד, מזכירות, מאבטחים, מנהלי סניפים, מרצים, איש אבטחת מידע, סיסטם, סטודנטים
- קבצים- חומרי לימוד, פרטים אישים של הלקוחות
- שרתים וכלי הגנה - **computers, web server,storage, telephones, ,fax,ftp,active directory,daf,waf,nac.dlp,switchs,prenters,cameras**

### Busines enviroment

Domain busines

- לימוד קורסים מקצועים בכיתה או באונליין - מכללה שמעבריה קורסים מקצועים ברמה הכי טובה שאפשר

Assets inpuct on the busines

- השפעת עובדים ולקוחות -במסגרת עבודה של כל עובד ועובד ניתנת גישה לנכסים שונים של המכללה, כל עובד משפיע על הארגון בתחום העסק שלו לדוגמא מרצים מעברים את החומר לימוד לתלמידים, ומאבטחים מוודאים כל כניסה למכללה, התלמידים משתמשים בקבצים שונים של המכללה, מנהל סניף אחראי על סדר וארגון של אותו סניף
- השפעת קבצים - כל התכנים והקבצים הם אלה שהופכים את המכללה לארגון שנותן שירות כזה.
- השפעת שרתים -למכללה יש שרתים שונים.חלק מהשרתים מחזיק את התכנים שמכללה מציעה וחלק מגון על המכללה.

*Governace*

***רגולציות חיצוניות***

- רגולציה מצד הבנקים בעקבות שימוש כרטיסי אשראי של התלמידים, בעקבות רגולציה זו הוחלט שהמכללה תעשה מבד חדירות כל שנה על מנת לשמור על הכרטיס אשראי של הלקוחות שלה
- פיקוח ובקרה מטעם משרדי הממשלה

***תקני מכללה***

- לא מכניסים מחשבים אישים, דיסקים
- איסור כניסה לחדרים אסורים
- שינוי סיסמא כל כמה חודשים

*Risk management*

- הפסד כספי - בעקבות נזק כלשהו על השרתים של המכללה או גניבה פיזית של אחד השרתים היוקרתיים המכללה עשויה להגיע להפסד כספי
- איבוד לקוחות - בעקבות פריצה כלשהי למערכת של המכללה הרבה תלמידים מחליטים לעזוב את המכללה
- טביעה משפטית - בעקבות גניבה פרטים אישים של התלמידים, התלמידים עשויים לטבוע את המכללה
- איבוד מוניטין של המכללה - בעקבות פריצה כלשהי המכללה עשוי לאבד את התדמית שלה

*Risk management startegy*

- קניה מוצרים מתאים- על מנת לשמור על גניבה או פגיע הפיזית על השרתים המכללה צריכה לרכוש מוצרים שיכוטלים למנוע נגיעה יד אדם לדוגמא קודים בכניסה לחדרי שרתים, מצלמות אבטחה
- קניית מוצרי אבטחת מידע - על המכללה לקנות מוצרים מתקדמים ביותר בכדי לעשות את מירב המאמצים בכדי למנוע פריצה כלשהי לאתר המכללה
- הקצאת תקציב מסוים לטובת שיווק ופרסום - במידה הצורך המכללה עשויה לעשות פרסומים אגרסיביים בכדי למשוך לקוחות חדשים

**סיכום : בשלב זה בחנו את כל הנכסים השונים שיש למכללה ומה הרמת השפעה של כל נכס על המכללה, הבנו מה רגולציות ותקנים שיש על הארגון, הסקנו מה הפוטנציאל הנזק שיכול להיות על כל נכס ותכננו תכנית ברור איך להתכונן לכל נזק אפשרי**

## ----------Protect----------

**)שלב זה מדבר על ההגנה על ארגון עצמו ועל הנכסים שלו**

**על מנת לתת את הביצוע הכי טוב בשלב הזה חשוב מאוד להכיר את כל**

**הנכסים של הארגון רק לצורך הדוגמה בלבד נשתמש רב4 נכסים(**

## *Accsess control*

- שומר בכניסה לבניין - המכללה שמה מאבטח בכניסה לבניין כדי למנוע כניסה של אנשים זרים
- מצלמות בתוך הבניין - המכללה שמה מצלמות אבטחה על מנת לבקר את כל מה שקורה בתוך המכללה ומחוץ לה
- המכללה משתמשת בטכנולוגיות מתקדמים ביותר על מנת למנוע כניסה של אנשים לא בעלי מקצוע לחדרי שרתים ולמקומות שונים
- המכללה משתמשת בטכנולוגיות מתקדמות על מנת לשמור על אתר אינטרנט של המכלה, על מאגר נתונים, ועל שרתי אחסוnfirewall, daf, waf-
- כדי למנוע הדלפת מידע מצד העובדים או מצד התלמידים המכללה משתמשת בטכנולוגיה מתאימהnac, dlp-
- המכללה משתמשת בשרת active directory בשביל לנהל את העובדים והתלמידים שלה באופן מסודר

## *Awareness and trainig*

- מרצה במכללה מעבירה הדרכה קצרה לתלמידים חדשים בנושא הכנסת רכיבים חיצונים למכללה
- המכללה דורש מעובדים שלה רקע טכנולוגי כלשהו
- תלמיד במכללה נדרש להחליף סיסמא חדשה כל כמה חודשים
- פעם בכמה חודשים מייסד המכללה מעביר הדרכה קצר לעובדים ולתלמידים בנושא אבטחת מידע

## *Data security*

- המכללה משתמשת בכלי טכנולוגים על מנת להגן על מידע שהוא אינו בעל ערך
- על המאגר נתונים של המכללה נמצאים נתונים אישים של התלמידים, בשביל שתלמיד לומד מהבית או עטבד כלשהו שנמצא לסניף אחר של המכללה יוכל לעדכן או לעשות כל שינוי כלשהו בפרטים האישים שלו המכללה מאפשרת מוצר טכנולוגי מתקדמת כדי לשמור על הפרטיות של התלמיד
- אחד הכלים שהמכללה משתמשת בו הוא.vpn

## *Info protectio*

- בכמה שרתים של המכללה נמצאים תכנים חשובים של הארגון (כל החומרים לימוד,פרטים אישים של תלמיד,כל מה שקשור לעולם השיווק והפיננסי) לכן על המכללה להשתמש בטכנולוגים שונים על מנת לשמור על הדברים הללו
- מוצרים טכנולוגים למשל daf,waf,

## *Maintenance*

- המכללה נעזרת באיש סיסטם על מנת לשמור על המערכת שלה מעודכנים וניהול הרשאות קבצים
- במכללה יש עובד שמתחזק את כל מה שקשור לעולם החוקים- חוקים gpo, firewall,active directory ומשנה אותם לפי הצורך ובנוסף לכך עובד זה מקשיח את כל החוקים שנמצאים בשרתים שונים על מנת לצמצם את מרחב התקיפה על שרתים שונים
- בעקבות הרגולציה שחלה על המכללה מצד הבנקים המכללה מביאה כל שנה בעלי מקצוע חיצונים על מנת לבדוק את רמת ההגנה שלה

## *Protective technolegy*

**<u>שימוש במוצר אבטחת מידע</u>**

- **Network firewall-**קביעת חוקים ומדיניות על הרשתות השונות

- **Dlp** - על מנת למנוע הדלפת מידע
- **Daf** - מוצר אבטחת מידע על אתר אינטרנט
- **Waf** - מוצר אבטחת מידע על מאגר נתונים
- **Active directorey** - ניהול משתמשים
- **Nac** - בשביל למנוע התחברות לא מוכרת של רכיב חיצוני
- Vpn - טכנולוגיה המאפשרת התחברות מרחוק לשרת המכללה מבלי לבדוק רמה ערכי של התוכן המכללה משתמש בכלי זה על מנת שעובד או תלמיד כשהו יוכל לעדכן או לעשות שינוי כל שהוא בפרטים האישים שלו

**סיכום: בשלב זה בחנו את כל העקרונות ההגנה שמכללה מתכננת ליישם ולבסוף ציינו את כל הכילים הטכנולוגים על מנת להגן על המכללה בצורה הכי טובה שאפשר**

## ----------Detect----------

***)שלב זה הוא ניטר וזיהו איומים, שלב זה משתמש בכל התכנים שמעביר לו כל השרתים שנמצאים בהגנה על הארגון(***

### Anomalls and events

- למכללה יש מערכת זיהוי וניטור איומים,מערכת זו מקבלת את האירועים ותיעודים מהשרתים השונים ויוצר לעצמה דפוס או תבנית התנהגות התחלחלתית , אם בשלב כלשהו תהייה איזה שהיא חריגה מהתבנית הראשוני המערכת צריכה לתת התראה
- דגש חשוב: בזמן יצירת הדפוס צריך להביא בחשבון עד כמה התבנית הראשונית נקיה.

### Security continuous monitoring

- זהו שלב שבו עוקבים אחרי האירועים במערכת כלשהי בצורה ממושכת-אחד הדוגמאות שיכול להמחיש את השלב הזה הוא לעשות מעקבים של כל כניסה של תלמידים או עובדים למערכת-תהליך מסוג כזה נותן לנו בקר מי מתחבר למערכת

### Detection processes

- לאחר קבלת מידע מהתלכים השונים שעשינו אנחנו מתחילים כל אירוע ואירוע מחליטים את הערך או את המשמעות של האירוע דוגמא:אם במכלה החלטנו שעושים ניטור על הרשת בשלב הזה מסתכלים על האירועים שקיבלנו ומחליטים מה כל אירוע ואירוע אומר
- **<u>גישה ראשונה :</u>** גישה זו אומרת ליצור רישמה של חוקים שרוצים לאפשר ומה שלא נמצא על הרשימה זו הוא אסור(white list)
- **<u>גישה שנייה :</u>** גישה זו היא הפוכה מגישה הקודמת,בגישה הזו יוצרים רשימה של חוקים אסורים וכל מה שלא נמצא על הרישמה הוא מותר(black list)

**סיכום: בחלק זה אספנו את כל האירועים משרתים שונים ויצרנו דפוס ראשוני ועשינו ניטור לטובת ניתוח מעמיק ולבסוף הגדרנו מהי שיטת עבודה שלנו**

## ----------Respond----------

***)בשלב זה עושים תגובה כלשהי לאיזה אירוע שקרה, על מנת לעשות את התגובה הכי טובה והכי מהירה שאפשר חשוב מאוד להגדיר את הגדרות הזיהו והניטור בצורה הכי מקצועית שאפשר(***

### Response planing

בשלב זה מכינים את תכנית התגובה שלנו. תכנית תגובה צריכה להיבנות בשלב של אסטרטגית ניהול סיכונים בשביל להביא בחשבון איזה רכיבים שיכולים לעשות תגובה לרכוש בזמן ההגנה

דוגמה לתכנית תגובה:

- אחד הסיכונים על המכללה הוא גניבת אחד השרתים במקרה כזה התכנית תגובה היא לתקשר עם אנשי התחזוקה של המכללה ולהשתמש בשרת הגיבוי.

### Communications

זה השלב של התנהלות תקשורת פנימית וחיצונית

- תקשורת פנימית - תקשורת שעושים בארגון בזמן תגובה על אירוע כלשהו, תקשורת זהו מתבצעת בין העובדים -בהמשך לדוגמה בקודמת בשלב הזה אנו מעדכנים את אנשי התחזוקה את מנהלי הסניף וכל מי שרלוונטי לאירוע
- תקשורת חיצונית - המכללה מחליט להוציא לתקשורת ארצית את מה שקרה -מנהל סניף מחליט אם להוציא לתקשורת את האירוע

### Analysis

אחרי שהכנו תכנית תגובה ברור זה השלב בו שבוחנים בודקים את כל התלכים שגרמו בצורה היקפית

- אי ערנות של המאבטח בכניסה הוא הגורם הראשוני לגניבה, חוסר ערנות מצד העובדים והתלמידים הובילו להגעתו אל חדר שרתים, תקלה במערכת התראה בכניסה לחדר שרתים אפשרו להיכנס פנימה ולקחת ציוד

### Mtigation

לאחר חקירה ואבחון מעמיק מה קרה לאירוע בשלב הזה עושים את המעשה הראשון בדרך לפתרון ובכדי לעצור את האירוע הכי מוקדם שאפשר.

### Improvments

שלב ניתוח ולימדה על האירועים שקרו

- בהמשך לדוגמא הקודם של גניבת ציוד והבנו את ההשתלשלות של האירוע ושלב הזה עושים לתיקונים לפעם הבא
- מגדילים את הערנות של המאבטחים התלמידים והעובדים
- תיקון על מערכת התראה

***סיכום: בחלק הזה הגדרנו תוכנית תוגבה ברורה ודרך ההתקשרות פנימית וחיצונית ויישמנו המלצות ושיפורים על מנת להגן על הארגון בצורה הכי טובה שאפשר***

## ----------Recover----------

### Recoreyplaning

זהי תכנית שיקום האגון לאחר אירוע - בתכנית הזו אנו מפרטים את שיטת השיקום שלנו בכדי להחזיר את הארגון למצב הקודם והתקין שלו. תכנית השיקום צריכה להיות ברורה. אם לדוגמא התרחשה איזה שהיא פריצה לארגון שלנו וחלק מהקבצים הוצפנו בשלב השיקום אנו נקח מהשרת הגיבוי שלנו בשביל לשקם את הרגון

### Improvement

זהו תהליך שיפור ולימד על התהליך השיקום-הדרך שבה אנו בוחנים את עצמנו על השיטה העבודה שלנו בזמן השיקום

### Communication

תקשורת פנימית: התקשורת שמתבצעת במכללה בין הצוותים על מנת לעשות שיקום מהיר וחזק

תקשורת חיצונית:לאחר מאמצים רבים של הצוותים השונים להחזיר את המכללה למצב התקין שלה המכללה מחליטה לצאת לתקשורת ארצית לעדכן את תמונת המצב

***לסיכום:בחלק הזה הגדרנו תוכנית ברורה על החזרת המכללה לאחר פגיעה כלשי ועל שיטה ותקשורת הצוותים ולמדנו לקחיום ושיפורים.***