**אבטחת סייבר:**

הרצאה מס' 1: תאריך 17/10/2018

קצת מושגים:

סגמנטציה- חלוקה, נניח אני ארגון, לחברת ביטוח יש 5000 משתשמים הרבה מאוד שרתים, האם כל המידע עכשיו הוא סופר סודי? כל המערכות שמשתמשים בהם צריך לאבטח אותם באותה רמה? התשובה היא לא. לא צריך לאבטח מידע פשוט, כמו שצריך לאבטח פרטים של חולה כזה או אחר. לכן עושים סיגמנטציה, לוקחים מידע רפואי ומידע אישי ושמים אותו במקום סופר מאובטח. ככה בעצם מבדילים בין דברים מאוד קריטיים בארגון לבין דברים פחות קריטיים.

DMZ- (\*\*\*שאלה בטוחה במבחן על מושג זה) אזור לא צבאי- אזור פחות קריטי לי. (דוגמא- יש אתר, שהמידי בו פחות רגיש- ואני יכול לשים אותו באזור הבלתי מאובטח)

הצפנות- אני עכשיו שולח מידע ואני לא רוצה שאף אחד בדרך ידע, אני אצפין אותו. יש הצפנה שמחליפה מקומות של אותיות, יש הצפנה שעושה מספריים, יש הצפנה סימטרית וא-סימטרית.

אינטרנט- האינטרנט הוא לא אנונימי- כולם יודעים עלינו הכל. הרבה מאוד טכנולוגיות- יש מעבדים בעוצמה אדירה.

CYBER- מרחב קיברנטי- כל האינטרנט- כל עולם החיבורים.

הרצאה מס' 2: תאריך 24/10/2018

מכשירים ניידים- הוסיפו לנו צורך בהגנה, כי זה אלחוטי.

מתי משלמים על אבטחת מידע? ככל שמשקיעים את הכסף באבטחת המידע מוקדם יותר זה יותר זול ויותר נכון וקל ליישום.

מחזור חיי פיתוח תוכנה – ארגון שמפתח תוכנה.

בעבר פיתחו תוכנות על ידי מפל המים- זה היה שלב אחרי שלב אחרי שלב.. אי אפשר להגדיר שלבים חדשים בלי שסיימנו שלב קודם. אפיינתי תוכנה- ראיתי מה הדרישות- תוכנה למה? מה היא הולכת לעשות? תנהל לי בית חכם? אני יושב עם יוזרים מגדיר דרישות, נגמר אפיון נכנסנו לשלב הפיתוח. לא נוגעים באיפיון, סיימתי פיתוח, עושים בדיקות שלי, סיימתי בדיקות שלי עושים בדיקות אינטגרציה. עוברים לשלב שבו עושים בדיקות משתמש, מביאים משתמשים מבקשים מהם לעשות בדיקות למערכת לראות אם היא עושה מה שביקשתי מהמערכת לעשות. זה ארוך, זה מאבד קשר עם הלקוחות, זה תהליך שאי אפשר לעשות את מהלך אחורה. ככה התנהלה תוכנה במתודולוגיה של מפל המים.

לכן מה שעושים זה ספירלה- עושים סיבוב ראשון מראים ללקוח, אולי אפילו בונים מערכת דמה, מה מכניסים? רמת סיבוכיות, מקבלים ממנו אישור עוברים לסיבוב הבא. בספירלה- הלקוח לא מחכה שנה שלמה על מנת לראות את המערכת.

אג'אי- פיתוח תוכנה מהיר, אני אפתח כמה שיותר חלקים שאין קשר בניהם, כל חלק הוא כאילו תת פרויקט שהלקוח מעורב בו. כשעושים אינטגרציה בין החלקים זה לוקח זמן. היתרון הוא שעושים את זה בחלקים קטנים, מפרקים בעיה אחת גדולה להרבה בעיות מאוד קטנות.

למה זה חשוב? כי אנחנו כאבטחת מידע לקחנו מודל SDLC, שמים איש אבטחת מידע בכל אחד משלבי הפיתוח. זה נקרא פיתוח מאובטח. זה אומר שאנשי פיתוח אין להם זמן אין להם סבלנות הם צריכים לספק סחורה מהר ולכן הם מחפשים קיצורי דרך. קיצורי דרך זה מה שהאקרים אוהבים, דוגמה: backdoor האקר נכנס לקוד ישירות, ומתחיל לעבוד. זה סוג של קיצור דרך שהאקרים מחפשים. כלל ברזל- אין backdoor.

אחד היסודות המנחים בעולם אבטחת מידע **CIA**: (\*\*\*מושג למבחן)

**Confidentiality integrity availability**

ישנה סכנת פגיעה בפרטיות במידה ומישהו חדר ואני למעשה נחשפתי לנתונים של עובדים, נתונים אישיים רפואיים, יש בעיה של סודיות, חדירה לפרטיות.

פייסבוק הייתה מאוד מוטרדת כי לקחו את פרטיהם של הלקוחות שלהם, נגעו בפרטיות של המשתמשים שלהם.

**Confidentiality –** סודיות היא מרכיב של פרטיות המיושמת כדי להגן על הנתונים שלנו מפני צופים לא מורשים. דוגמאות לסודיות של נתונים אלקטרוניים הנמצאים בסכנה כוללים גניבת מחשבים ניידים, גניבת סיסמה או הודעות דוא"ל רגישות שנשלחו לאנשים שגויים

**Integrity**- שלחתי נתון, איך המשתמש יכול לוודא שהנתון שקיבל ממני הוא באמת הנתון ששלחתי? יכול להיות שמישהו נכנס באמצע, זה יכול להיות עובד, האקר. הנתון שהעברתי הגיע שלם לצד השני.

**availability** זמינות- המערכת זמינה לשימוש, נניח והייתה התקפה, אם אני ערוך לזה שיש לי 1000 משתמשים, אם נכנסו 1500 סביר, אבל אם נכנסו לי 5000 משתמשים אני כבר לא ערוך והמערכת תקרוס.

סיכונים ובקרות:

בקרה: סוג של אמצעי שאמור לעזור לי ללהוריד את הסיכון. בקרה: דלת נעולה, אזעקה בבית.

אנחנו עוסקים בהפחתת סיכונים, איפה נשים יותר בקרות? איפה שהמידע יותר קריטי, מידע קריטי נשים הגנה בשכבות, עוד הגנה ועוד הגנה וכל הגנה כזאת תפחית את הסיכון.

בקרה שאין לה סיכון- בזבזתי את כספי הארגון. אנשים מתלהבים לשים כל מיני כלים כאלו ואחרים, אם אין סיכון לא צריך, אם צריך הגנה, אז יש צורך. צריך להפעיל שיקול לדעת, לא בהכרח יש סיכון.

אם מישהו עשה בקרה ואין סיכון- תמיד שואלים האם יש בקרה- אם יש בקרה צריך לדעת על איזה סיכון הבקרה הזאת עונה.

הרצאה מס' 3- 31/10 : גורמי הסיכון

#טכנולוגיות-מערכות חומרה ,התוכנה והתקשורת המהוות "מערכות".

#אנשים-במידה ויש עובד ממורמר בארגון הוא מהווה סכנה .ולכן לכוח אדם יש תפקיד חוב בארגון ממשום שיש להם מידע על כל עובד.

#תהליכים.(מפורט במצגת)

4 רכיבים בסיסיים באבטחת מידע

אימות זהות-נניח מישהו רוצה להיכנס למערכת. הוא צריך להזדהות באמצעות סיסמא. ז"א לוודא שזה אכן הוא.

הרשאות-מתבססת על אימות זהות כתנאי מקדים. ולאחר מכן נותנת הרשאות כגון: מחיקה כתיבה וכו .

ועכשיו לאיזה אזורים במערכת הוא מורשה להיכנס. הרשאות זה משהו שצריך לתחזק ולנהל באופן יומי.

הרשאות – 2 גישות

Need to know- מה אני מאפשר לו במערכת שהוא צריך לדעת – אני יודע מה הוא צריך לדעת ואני אתן לו את מה שהוא צריך לדעת.

List privilig- מינימום הרשאות – מדברת גם על זכויות וגם על הרשאות

שלמות ואמינות המידע-\* cia-confidently integrity ability .פרטיות/סודיות,אמינות, יכולת.

נניח שמישהו שלח מידע לאדם כלשהו(זה בעצם הפרטיות והסודיות=הגנת הפרטיות) ואיזשהו האקר התערב בשליחה.

מישהו נגע בנתונים והנתון הגיע שגוי בגלל האקר. שלמות המידה נפלה.

זמינות המידע- קשור לזמינות מערכת .אני עכשיו רוצה לבדוק אם האתר של המכללה עובד.

בתור אחראי אני רוצה להיות מסוגל לבדוק את הזמינות של האתר.\*לכל אחד מהסיכונים הללו אנו בונים בקרה. שלכול למעשה יש את הצורך להוריד את הסיכון.

אם אין סיכון אזי לא צריך בקרה. סיכונים הם משתנים ולכן הבקרה משתנה בהתאם. (למשל בישראל לא צריך לבנות בקרה למניעת הוריקן לעומת זאת בפלורידה זה טוב.

אימות זהות:

ישנם 3 אמצעים:

What you know-משהו שיש לי. למשך שם משתמש וסיסמא.

What you have-למשל תעודה ביומטרית או טלפון.

What you are-זיהוי פנים , אצבע וכו' .

אזורים קריטיים: על אזורים שהם קרטים נשים כמה שכבות של הגנה.

dmz- אזור פחות קריטי שעליו אני יגן פחות. שם אפשר לשים למשל את האתר שלי. מידע על המיילים או העובדים אני לא ישים שם.

רשימות בקרת גישה-לכל user יש רשימה אבטחות והרשאות שהוא רשאי להיכנס אליהן.

Secure by design

SDLC-מחזור החיים של פיתוח תוכנה. אני רוצה לשבת עם המפתחים ולראות שהם עושים את עבודתם כמו שצריך ולא עושים קיצורי דרך שיכולים להוות סיכונים. בגדול-מפתח משאיר לעצמו קיצורי דרך לעצמו. ז"א בסביבת הפיתוח שלו.(האקרים מחכים להזדמנויות כאלו).

איומים-threats

אין לנו השפעה על איומים חיצונים. על חולשות אפשר להשפיע. ניתן לחזק אזורים חלשים במערכת. הקושי העיקרי הוא לזהות אותם. ברגע שיש סיכונים יש לעדכן את ההנהלה. ומה המשמעות שלהם.

איך מכילים בעיית סייבר? מגדרים את אזור הבעיה. מי האוכלוסייה שנחשפה ונפגעת מהתקלה? וכמה זה חשוב לארגון. מגדרים ומפרידים בין מי שנפגע למי שלא. וכך אני מטפל במי שנפגש. מי שלא יכול להמשיך לעבוד כרגיל.

קניין רוחני-פטנטים מידע ומוניטין (כביכול לא מוחשי) שיש לי.(רוחני=לא מוחשי)

Down time-זמן שהמערכת לא זמינה. מכל מיני סיבות: הפסקת חשמל , שיפוצים וכו' .

וירוס הוא פרטני מדביק אותי. תולעת תמיד יחפש את הבא בתור.

סוס טרויאני-מפעיל את התוכנה תחת התחזות.

Contd-התוקף שולח מספר גדול של בקשות למטרה. המטרה עמוסה ולא יכולה לענות לבקשות הלגיטימיות. Ddos-ויש את השני שבו הרבה תוקפים את המטרה בו זמנית

הרצאה מס' 4: 7/11

מיישם סייבר- אדם בעל ידע ותיאוריות בסיסי ויכולת יישומית האחראי על יישום הגנת הסייבר בארגון

ישנו מסמך- אם רוצים להכשיר מיישם אבטחת סייבר.

ISO27001 תקן איכות של מכון התקנים, תקן של אבטחת מידע. חברה שעומדת בו לאורך זמן היא חברה שעובדת לאורך זמן עם אבטחת מידע

ארגון כמו ISO הוא נדיב, הכוונה שלו לייצר ידע ולייצר הבנה מה צריך לעשות ולכן בתום יומיים שלושה ניתנת הסמכה, למרות שיוכלים להיות פערים, בדקו ראו ויודעים מה הפערים, ובכל זאת קיבלו תעודה של ISO, הכוונה של הבוחנים היא לא להעניש את הארגון אלא לתת הכוונה, לאחר שנה בודקים שוב את הפערים שהיו ואם הפערים תוקנו- ממשיכים לקבל תעודה ואחרת לוקחים את התעודה.

כאנשי אבטחת מידע משתמשים בתקנים האלה כי זה עושה סדר, זה שואל שאלות ומסדר. איך אתה מגן על הנתונים איך אתה רואה שאורח שמגיע לא נכנס למערכות, אלו כלי הגנה שמוטמעים בארגון, המוטיביציה היא עסקית, איזו מסגרת כמו צ'קליסט מה יש לבדוק ומול איזה רמת סף לעשות.

מוטיביציה ראשונה- נעדיף לעבוד עם מישהו שיש לו תקן מאשר עם מישהו שלא יודע מה הוא עושה ואין לי מושג מה קורה איתו

מוטיביציה שנייה- מה אני צריך לעשות (כמו cookbook)

תקשורת, מהי?

קשה לדבר על סייבר כשלא מבינים מה זה תקשורת.

מודל 7 שכבות: OSI

בקצרה על השכבות:

אני רוצה לשלוח מייל ללאה, לאה יושבת בניו ג'רזי, אני משתמשת בג'ימייל ואני עכשיו לקוח של ג'ימייל, client server. מדובר על הלקוח שמשתמש בשרת. (השרתים נותנים לנו את האפשרות להתשמש במערכת)

אני הלקוח אני משתמשת בשירותי המכללה לצורך העניין לבדיקת נוכחות. למה זה בנוי ככה? כדי לא להעמיס על נקודות הקצה מצד אחד. נקודת קצה זה כל מחשב שיש לנו, פלאפון מחשב נייד נייח וכו'.. אני מתחברת לשרת. השרת בדרך כלל יוצא החוצה לאינטרנט, אנחנו יוצאים דרך שרת המכללה לאינטרנט.

אני נכנסת לג'ימייל כל מה שיש לי זה באקספלורר זה אפליקציית ג'ימייל, אצלי אין כלום, זה נשמר תחת השרת של גוגל, איפה נמצא השרת של גוגל? בהרבה מקומות בעולם, יצאתי לשרת של גוגל, בדרך יש ISP ספק אינטרנט, (012, אינטרנט זהב...)

אני יצאתי דרך הISP שלי שחיבר אותי לשרת של גוגל, יכול להיות שבדרך הוא עבר עוד ספק אינטרנט, כי 012 זה ישראל ויכול להיות שיש ספק אינטרנט גדול יותר שלקוח כמה מדינות. לאט לאט אני מגיעה דרך ספקים גדולים, יש ספקים מאוד גדולים שמחוברים עם פירים, ועם כבלים פיזיים שנמצאים מתחת למים.

אני כתבתי מייל ושולחת ללאה בניו ג'רזי, זה הגיע לצד השני, ולאה היא לקוחה של AOL (כמו 012 רק בארצות הברית) לאה נכנסה לשרת הISP שלה ומשכה את המייל שלי, בדרך זו או אחרת היה צריך להיות חיבור לא בהכרח פיזי, זאת אומרת היה אפשר לעשות את זה גם בויי פיי, לאה פתחה את המייל ששלחתי אליה. בדרך קרו הרבה דברים, המייל עבר כמה רשתות, רשת מכללה, רשת 012, רשת גוגל, רשת AOL, רשת בניו ג'רזי, איך זה יודע להגיע בדיוק למחשב שלו? IP ADDRESS

לכל תחנה יש IP ADDRRESS

השתמשנו באינטרנט, מה זה אינטרנט? אוסף של רשתות אוסף עצום של רשתות המחוברות בניהם.

אוסף רשתות המחוברות בניהם, מה מחבר בניהם? ראוטר.

ראוטר- זה נתב, יודע מאיפה הגיע האינפורמציה מאיזו רשת, הוא מנתב את המידע, בין רשתות. יש ראוטר של המכללה שמחבר אותה עם הראוטר של 012

ואז כשיצאתי מרשת המכללה, אני מחפשת את 012, ויעבור לראוטר של גוגל, ולראוטר של AOL וכו..

תפקידו של הראוטר- לחבר רשתות.

מה מסתתר מאחורי הראוטר? סוויטץ' או האב (hub)

אני עכשיו העברתי מסר ללאה, אמרתי לה הכובע הולם אותך, hub מודיע לאה הכובע שלך הולם אותך, זה לא מענין את כולם, היה צריך לכתוב לה באופן אישי, הhub משדר לכולם, מי שזה עבורו יודע שזה עבורו.

סוויטץ' יודע מה הכתובת שהעברתי אליה ומחבר את ההודעה אליה.

מודם: ממיר אנלוג לדיגיטל, על קווי הטלפון בשיחות אנחנו מדברים אנלוג, יש תדר. מחשב לא יודע לעבוד עם תדר, אין לו את זה בשפה, מחשב עובד BT מחשב עובד 1 0 1 0 1 0 1 עובד או לא עובד, בעוד שאנלוג עובד עם תדרים.

האינטרנט הוא אוסף של רשתות יש בניהם היררכיה וסדר, בסופו של דבר באמצעות הרשתות האלה אני מעביר מידע מנקודת קצה אחד לנקודת קצה אחר.

אני לקוחה אני ניגשת עושה שימוש ברשתות, אני ניגשת באמצעות חיבורי אינטרנט לרשת לשרתים של הספקים של פייסבוק גוגל וכו..

לאה בניו ג'רזי אני בקריות, אנחנו צריכות שפה משותפת. זה נקרא פרוטוקול- אוסף של כללים.

כללים- כשאני יעביר אינפורמציה כלשהי מהג'ימייל שלי, (כתיבת מייל) כל הדרך איפה זה עובר? מה נפתח? וכו'.. בצד השני יש שבע שכבות, שכבה מדברת עם שכבה.

תהליך N קפסולזציה- בונים את זה בצורת קפסולה- זה נוסע לצד השני- ללאה (ניו ג'רזי), והגיע לצד השני עם שישה hedear-ים, אין תחכום- יש סדר, עד לשלב שלאה פתתחה את המייל שלי נתתי את כל האינפורמציה שהייתי צריכה עד שהיא פתחה את המייל.

בכל אחת מהשכבות האלה, ניתן מענה לצורך, והצורך הזה אני עובדת מול לאה, ואנחנו מדברות באותה שפה, כי אחרת זה לא יעבור, זה הפרוטוקול לכל אחד מהכללים יש פרוטוקולים.

פרוטוקול אמרנו ששזה כללים ושפה, זה אומר שאם שלחתי לה מחרוזת זה יופיע בצורת מחרוזת.

יש מודל שנקרא TCPIP יש בו ארבע שכבות, אין שום הבדל למעט זה ש3 או ארבע שכבות אחרונות מאוחדים בניהם.

הגנת גישה: access control - אני מבקר את הגישה, מה זה גישה? אני עכשיו צריך לעבור תהליך של הזדהות, אני אומר שלום אני עכשיו נכנס למחשבים של חברת הביטוח מגדל שאני עובד איתם ואני אומר שלום אני עמי, תזדהה. יש לי תעודת זהות אולי גם סיסמא, יש תהליך עימות שאני זה אני ומותר לי להיכנס למערכת זה בקרת גישה, יש כל מיני שיטות להגן על זה, סיסמא זה אחד מהם, (אולי סיסמא זה משהו שיעלם מהעולם פעם כי זה משהו ששוכחים וכו..)

מתודולוגיה שנקראת single sign on במקום שאתחבר גם לגוגל, גם למערכת אי אר פי וגם למערכת הפיננסית ולכל המערכות שלי ואני ועובדת באותו ארגון.. וכל המשמרת אני רק אזין סיסמאות יש מערכת אחת שבודקת אם זו אני ורק אם אני מזדהה ועושה חיבור נכון זה עושה טיקט ונותן אפשרות לאפליקציות אחרות להשתמש בנתונים.

סיגמנטציה- אני רוצה להגן על מידע קריטי באופן שונה ממה שאני מגן על מידע לא קריטי.

אפשר לשים בקרות ואבטחה על כל הארגון הרבה כסף הרבה מחשבים תומכים- וזה לא נכון לעשות - על מידע לא רלוונטי של ארוחת צהריים לא צריך להגן כמו על מידע רפואי של מבוטחים, שמים הגנות בהתאם לרמת הקריטיות או רמת הרגישות שיש לה.

בקרות- מטרת הבקרה להוריד את הסיכון.

בקרה כשאין סיכון- מנהל אבטחת המידע זרק כסף לארגון. למה לשים בקרה אם אין צורך? אין פה כלום.

הגנה בשכבות- אם יש אזור קריטי אני לא אגן עליו רק עם שכבה אחת, אלא עם שנייה ושלישית ואם פרצו את האחת נגן עם שנייה ואם פרצו את השנייה נגן עם שלישית.

הקשחה- מהמילה קשוח, אני הופך אותה ליותר קשה לפריצה, אני שם לה יותר הגנות או שאני מבודד אותה מהרשת. דוגמת USB כשמישהו נכנס עם USB והעתיק את המידע. בארגונים ביטחוניים היום אי אפשר להכניס USB למחשב.

Acssess control בקרת גישה

משתמשים היום בשיטות הצפנה סימטריות וא-סימטריות. מה זה הצפנה? אני שלחתי מייל ללאה ואני לא רוצה שאף אחד יגיע לפאקט של מה ששלחתי לה, אז אני מצפינה.

שכלולים שתפקידם לערבל את המייל, כדי שאף אחד לא יוכל להגיע למייל, סייפר=הצפנה

די-סייפר= פענוח.

אם מישהו הצליח להגיע למייל לפני שלאה פתחה אותו הוא לא יוכל לקרוא אותו.

יש חסרון כי לכל זוג צריך להיות מפתח, ואז יהיו הרבה מפתחות, לכל אחד צריך להיות קוד כלשהו שבאמצעותו מצפינים, מפתח פרטי, ומפתח ציבורי, מפתח ציבורי זה משהו שכל העולם צריך לדעת, לאה תגיד לי את המפתח שלה, ואני מצפינה באמצעות המפתח הפרטי שלי והמפתח הציבורי שלי, ללאה יש את המפתח הפרטי והציבורי שלה, ככה אנחנו מצליחים למעשה להשתמש בשתי המפתחות.

אניגמה כשפענחו את הצופן של הצד השני= ככה נגמרה המלחמה.

SQL INJECTION – תהליך של פריצה מאוד ידועה בעיקר במערכות WEB

וירוס תולעת וסוס טרויאני - תוכנות זדוניות וזיהוי אנומאלי – כלי DLP קשור לדליפת מידע, אני רוצה למנוע דליפת מידע, אני רוצה למנוע הוצאת מיילים מארגון, אני יתחיל לבנות string של מילים. באמצעות string אני מציפה את כל המיילים כל מייל שמופיע בו המילים האלה, נחסם.

כל המיילים יוצאים דרך המייל שרת והמיילים נבדקים, נניח שהייתה הדלפה כלשהי כך נדע לזהות. ככה יודעים לזהות במודיעין, יודעים לזהות מילים או מחרוזות מחשידים.

קווארנטין- אזור מגודר, זה לא המייל הרגיל שיצא, אני צריך להסתכל עליו ולבדוק מהמייל של העובד, העובד מקבל הודעה נחסמת, אם יש משהו שהגיע מIP לא מוכר מאזור חשוד או לא מוכר הוא ייחסם, נכניס אותו לקווארנטין כמו מכלאה שממנה אני משחרר רק אחרי שראינו שאפשר להעביר אותה או לארגון או החוצה

אירועי אבטחת מידע- IRT – insident צוות טיפול באירוע תפקידו למעשה להתכנס ברגע שיש אירוע, יש אירוע- מה זה אירוע? בכל ארגון יש הגדרה אחרת לאירוע, כל אירוע כזה צריך לזהות ולקדם את הצוות שיטפל בו, מי קיים בצוות? אבטחת מידע, מערכות מידע, צד משפטי, לראות אם יש פה איזה שהיא חשיפה משפטית או עבירה על החוק, ואם יש צד שני שעושה לי נזק ואני צריך להפעיל נגדו צד משפטי, עובדים זה יום אחד נחמד ויום אחד סכנה ולכן הקשר שלי עם כוח אדם ואבטחת מידע הוא כל הזמן, מרגע שנתקלים בעובד לראשונה שזה החלק של כוח אדם, הגדרת תפקיד וכו.. מי שעושה את העבודה הזו זה כוח אדם, זה העובד זה תפקידו ואילו ההרשאות שמגיע לו, התפקיד של כוח אדם לוודא הרשאות- שיש הרשאות למה שהוא צריך ואין הרשאות למה שהוא לא צריך, כשנותנים כמה שפחות הרשאות אני כנראה מוכן, אם יש ספק אין ספק, לא נותן. אלה ההרשאות שקיבל וזהו. מינימום הרשאות.

דוברות- או מי שמטפל,בחוץ ביחסי ציבור, אם יש לי אירוע סייבר שצריך לדווח עליו, אנשי אבטחת מידע לא מדברים עם החוץ, יש דובר וזה תפקידו. הוא עדכן את ה"חוץ" במה שצריך.

מחשוב ענן- למה זה מסוכן יותר ומה היתרונות ומה החסרונות של הענן? אני עכשיו ניגש לענן של גוגל או מייקרוסופט אם אני בתשתיות של חברה כל כך גדולה או מבוססת מצבי טוב כי הם מספר אחת, התשובה היא לא, לא בהכרח, כשמבקשים לדעת איפה נשמר המידע, וכו' .. מקבלים חשבוניות שמנות יותר. ולכן צריך לבוא ולראות מה אני מצפה מאנשי אבטחת המידע שלי, לא לקחת את זה כמובן מאליו, יתרון- חברות גדולות מבחינת אבטחת מידע הם ליגה אחת מעלינו, שמים שם את מיטב המומחים ורוצים להגן עלינו.

מצד אחד סומכים עליהם יותר, בגלל שיש שם את מיטב המומחים מצד שני לא בהכרח כל מה שאני צריך ולא ביקשתי קיים שם אז צריך לוודא את זה.

שירותי אירוח הכוונה אווטסורסינג אם אני למעשה עושה שימוש בספקים כאלה ואחרים צריך לוודא מה רמת אבטחת המידע שלהם ואיזה שירותים קיבלתי וכו..

המשכיות עסקית- כל ארגון עושה גיבוי, אין מצב שלא מגבים.

לא מספיק- צריך גיבוי, גיבויים נעשים בשיטות שונות, ארגון גדול לפעמים לוקח 2 לילות לגבות את כל המידע. לכן המציאו דרכים לגבות את הכל, איך אני יודע שהגיבוי עובד? אני בודק אותו, עושים תרגיל, תרגילי שחזור, אם לא עשית תרגיל שחזור, גיבית- ובעזרת השם יעבוד, אתה לא רצה לסמוך על אף אחד שיעבוד.

ולכן עושים תרגילי שחזור, לקבל ביטחון ולכן מחויבים לעשות תרגילים אחת לשנה ממש לעשות שיחזור מלא לסביבת TEST, הרבה פעמים יש תקלות וחוסרים ומשלימים ועושים מה שצריך.

DRP דיזסטר = אסון- תכנון התאוששות – בונים אתר מרוחק 40 קילומטר מהאתר שלי ששם מרימים מערכת מרוחקת מהאתר שלי, לא זהה לחלוטין, כאילו אני משכפל את כל הארגון שלי. (רק מחשבים)

מדברים על תוכנית שיש לי נפילה במערכת שלי שיש לי גיבוי מרוחק למצב של אסון.

BCP- גם אסון אבל צריך לייצר המשכיות, B =ביזנס עוברים תהליך- האם זה קריטי? חברת קייטרינג, הארגון ימשיך לעבוד, אבל אם הלכה מערכת פיננסית ואני לא יודע לגבות כסף או אם זה מערכת ממושכת אז אין לי הכנסות אני חייבת שהמערכת תמשיך לעבוד מיחשובית.

אבטחה פיזית- אורח מגיע- מסתובב יחד עם מלווה, יש גדר לחברה אז יש הנחיות גובה הגדר, למה? איפה זה צריך להיות? איפה צריכים לשבת המחשבים? בד"כ במרכז לא מרתף בגלל הצפות ולא בגג, אלא קומה אמצעית.

**חוקים אתיקה תרבות ארגונית ואיך הם מתקשרים לאבטחת מידע?**

שמים הרבה מאוד בקרות- evidence דוגמה לבקרות- בתחום המחשוב, אוספים לוגים, לוג אומר איזה שהוא תיעוד של מה עשה בכל שלב אותו משתמש, אפליקציה, ואם אני אוספת לוגים כל הדרך אז אי אפשר להתכחש זה מה שהיה לאורך כל הדרך, בודקים האם המערכת שומרת לוגים, איפה היא שומרת וכו.. ואם לא יש אפליקציות שונות, יש מערכת מקליטה שמצלמת מסכים.

חוקים: דוגמה לחוק באבטחת מידע- חוק הגנת הפרטיות. נוגע בתחום שלנו, CIA – מוסבר בעמוד 2.

CIA שלושת האזורים שאנחנו למעשה אמורים להגן עליהם ולייצר מצב שהארגון קביל ועומד מאחוריהם, צריך לשמור על סודיות Confidentiality הארגון על פרטיות העובדים, החולים שאני מנהל במערכת, איזה אבטחה שמים עליו והלאה, אינטגריטי שלמות- שלחתי ללאה מידע אני רוצה לדעת שזה בדיוק מה שהיא קיבלה ולא שמישהו נכנס איפשהו בדרך. Integrity שלמות אמינות המידע, הצפנות פותחים VPN לא מעבירים בדרכים אחרות לא ברשת, יש צינור VPN כמו סיב רק ביני לבינו, availability זמינות המידע, מישהו תוקף אותי בדרך כלל עם רובוטים כתוצאה מזה שתקפו אותי מכל השרתים המערכת קורסת.

**הרצאה מס' 5 :14/11/2018**

MPA- multy factor authentiocation

פרמידת אבטחת המידע בארגון-

אסטרטגייה ברפאל- אבטחת מידע dor to dor לא מעגלים פינות אין מקום לפרצת אבטחה.

צריך לדעת מה הארגון עושה

תקן ISO 27000 אינטרס של ארגון- להגיד שאני עברתי הסמכה של ISO זה רלוונטי ללקוחות, לחברה יש מוטיבציה לבוא ולהשתמש בשם של ISO זה מכון בינלאומי ששווה להשקיע ולעשות את ההסמכה הזאת. למי שאין ISO ניגשים אליו לקוחות ורוצים לראות מה יש להם באבטחת מידע.

איך בודקים שהארגון עומד בתקן? כמה אדמיניסטרטורים יש? במערכת של 100 איש, אם יש יותר מ2/3 אדמיניסטרטורים זה בעיה למה צריך כל כך הרבה? ארגון רוצה כמה שפחות אדמיניסטרטורים.

NIST ארגון תקינה אמריקאי שמגדיר בתחום של אבטחת מידע אוסף של שאלות ותחומים כדי לעמוד באבטחת מידע, כדי לעמוד בתקן.

יש מסגרת שהיא הליבה, יש רמות שונות שצריך לעמוד בהם, יש פרופיל, אם נפתח את הNIST נמצא מסמכים של מאות עמודים שמסבירים בדיוק מה צריך לעשות על פי תקן זה. קצת יותר קשוח מהISO

ISO הוא בינלאומי.

בארץ זה נקרא מכון התקנים הישראלי (מת"י) ייצור של מוצר, צריך לבדוק שהוא לא דליק, לא מסוכן..

**Design of security architecture**

בקרות, למה צריך? זה תואם לסיכון, אם אין סיכון – לא צריך בקרה, מול סיכון שמים בקרה, תפקיד הבקרה: להוריד את הסיכון, למנוע קשה, אבל הבקרה צריכה להוריד את הסיכון.

לפני ששמים הגנות מחליטים מה קריטי ומה לא קריטי, צריך להפריד מידע על ארוחת צהריים לא קריטי לארגון, מידע של עובדים מידע של לקוחות מידע של חברות ביטוח זה חולים וכל מיני פרטים שהם מאוד אישיים וזה פגיעה בפרטיות ועליהם נבנה יותר בקרות.

הבקרות מתחלקות ל3:

בקרה ניהולית: מנהלים לא מתעסקים לא עם טכנולוגיה ולא עם תהליכים, הם מתעסקים עם אסטרטגיה, מדיניות. מדיניות זה סוג של בקרה, הנחיות.

בקרה אופרטיבית: תהליכים של עובדים וגישות פיזיות- בתהליך עצמו אורח שמגיע ילוו אותו, זה תהליך, אני אומר אין מצב שיסתובבו אצלי אורחים ללא ליווי בארגון. (כמובן שמדובר על רפאל ולא על שופרסל)

בקרה טכנית: אלמטנים טכנולוגיים.

מעגל האבטחה:

חצי מהמעגל הוא אנשים, אנשים הם מסוכנים, ספקים אורחים כל מי שנכנס, כל אדם שנכנס לתוך הארגון הוא סכנה. יש את המערכות, את המידע, את האינטרנט, על מערך זה על המעגל הזה צריך להגן עליו אז מחלקים את העולם לשתיים, את העולם של האנשים ואת העולם הטכנולוגי.

יישום של שכבות הגנה, זה דורש מהארגון לייצר רמות או שכבות של בקרה. זה דורש לעשות חלוקה של הארגון לאזורים שבהם אפשר להגן על חלקים מסוימים.

יש אפשרות לבדוק את אבטחת המידע מבחוץ מחוץ לארגון – בדיקה איך יוצאים מיילים מהארגון, איך מתנהל הדומיין.

DMZ- פה יהיה אזור שהוא לא הכי דורש אבטחה, בניגוד לאזור הארגון או אזור של רשתות נוספות שאני רוצה שהם יהיו מאובטחות יותר.

RISK MENEGMENT – אנחנו מתעסקים בעולם של סיכונים, יש סיכון של חדירה, צריך להוריד אותו.לשם כך בונים בקרות, את הבקרות האלה צריך להצדיק. מציגים את הסיכון במונחים כספיים

עושים רשימת נכסי מידע

CIA- סודיות, שלמות (שלמות הנתון) , זמינות.

**הרצאה מס' 6: 21/11/2018**

ניהול הסיכון- אני מעריך את הסיכון, בוחן את התגובה הרלוונטית. אני רוצה לשמור את הסיכון הזה תחת תאבון הסיכון שלי

לסיכון יש סבירות, נזק.

תאבון סיכון- דיי תחושתי, דוגמא: סיכון של רפאל לא דומה לסיכון של שופרסל.

ארגון בטחוני עם הרבה סודות ופטנטים שונה בהרבה מארגון כמו שופרסל.

אם ההנהלה מודעת לסיכון היא צריכה גם להבין וגם לתמוך.

צריך לזהות סיכונים צריך לסווג אותם : identification, classification, ownership

שלושה אלמנטים עיקריים בהערכת סיכון

1. לזהות
2. לנתח סיכון
3. להעריך סיכון- להבין כמותית או איכותית – לא לכל סיכון אפשר להדביק מחיר. (דוגמת ההוריקן בפלורידה- אני יודע לקמט אותו במספר כמה נזק יהיה לי)

דוגמאות לנכסי מידע:

1. Propritery -מידע שיש רק לחברה עצמה. (לדוגמה apple) שומרים את המידע שלהם כמידע סופר קריטי
2. מידע פיננסי
3. תוכניות רכישות ומיזוגים
4. תוכניות אסטרטגיות בשיווק
5. PII
6. TRENDES SECRET
7. PATENTS

מה זה איום?

איום שמסכן את הנכסים בארגון- צריך להתמודד עם זה.

אירוע תקיפה זה כל אירוע במהלכו יש פעולה כנגד הנכסים שלי ויכולים לגרום לי נזק ישיר.

מי שמחולל את ההתקפה נקרא "התוקף" הthreat actor .

איך מזהים איומים? זה שלא פגעו בי לא אומר שלא נפגעתי, עדיין לא רואים את הImpact לא אומר שהאיום לא קיים

מדברים על כמה מקורות של איומים, איומים שקרו בעבר, איומים שאני נחשף אליהם בחדשות, דוחות חיצוניים שמקבלים ממערך הסייבר הלאומי או הבינלאומי הודעות על תקיפות ככה נחשפים לאיומים, האם זה רלוונטי כן או לא, האם זה נוגע לי כן או לא, פרסומים בתעשייה.

איזה איומים רואים בתעשייה?

1. שינוי נתונים זה סוג של איום
2. סוג של טרור
3. זליגה בתשתיות
4. שריפה
5. הצפה
6. בעיה בחומרה
7. תקלות תעשייתיות
8. תקלות מכניות
9. נפילה בחשמל
10. נזק יזום

על רוב הדברים כמעט אין לי שליטה.

בניגוד להאקר שמחפש לעשות כסף או רושם על חברים פה מדובר על מתקפות ארוכות טווח,שלפעמים יושבים בתוך הרשת שלנו שנים.

מדובר על התקפות מסיביות של השקעה גדולה ועל פעילויות שהן פעילויות ברמת מדינה, דורשות הרבה כסף והרבה ידע.

מה מחזור החיים של התקפת APT? (עמוד 17 במצגת)

APT: התקפה שהיא לאוו דווקא התקפה ספציפית, זה אנשים שיושבים ברשת בעלי מטרה בד"כ מטרה אסטרטגית או מדינות או ארגוני טרור, ביון וכו'..

איומים פנימיים: בתוך הארגון- על פניו יש לי סכנות בתוך הארגון כי אני נותן אמון באנשי הארגון, לכן מה עושים? אם יש מועמדים צריך לבחון אותם. מסתכלים על עובדים וספקים על פניו זה איום כלשהו

עובד שעשה דברים בכוונה- עובד ממורמר. צריך לנסות לזהות מאיזה עובד פנימי יגיע האיום

SOD suppuration of duty

Asseseement הערכה לאיום.

יש אפשרות לבנות סיכונים TOPDOWN לפי יעדי הארגון מזהים את יעדי העסק, קשר עם לקוחות, למי מדווחים? מה מוציאים החוצה?

BOTTOMUP מחפשים סנריו של סיכון, אני עכשיו עובר תהליך מובנה, שלב שלב תקשורת חיבורים לאינטרנט כל החיבורים.

סיכון איכותי:

סיכון גדול – מיליון דולר

סיכון איכותי – בין חצי מיליון למיליון דולר

סיכון קטן- קטן מחצי מיליון דולר

ככה מקמטים סיכון.

נתוחי סיכונים:

1. נתוני עבר לראות מה הסטטיסיטיקה
2. הערכת שווי שמתבסס על נתונים שנתנו לנו
3. הסתברות שזה יקרה, נזק צפוי ואני יודע להעריך את הסיפור הזה

Risk evaluation: אם הסיכון גבוה ממה שאני מוכן לקבל אני צריך להוריד אותו. דוגמת ההוריקן, גובה הנזק כפול ההסתברות שזה יקרה, יש לי נזק צפוי או סיכון של חצי מיליון דולר, בודקים מה אומר המנכ"ל- אם הוא מוכן לספוג הוא אומר בוא נראה מה יקרה.. אם הוא לא מוכן לספוג נזק- אז הוא אומר בוא נשים על זה בקרות בוא נשים על זה הגנה – עושים תוכנית mitigation.

**איך נמנעים מהסיכון?** דוגמה בנקים: לא משתמשים בענן. כי האחראי על הבנקים בישראל החליט שלא מגבים נתוני לקוחות אלא נתונים נשמרים על שרתים של הבנקים שרתים מקומיים. אולי בעתיד הם יעברו לענן אבל נכון לכרגע זוהי דרך להימנע מהסיכון.

Risk treatment: ביטוח סייבר. (כשנגנב רכב, אנחנו יודעים לעמוד את הנזק, שווי הרכב, שווי ימי עבודה שהפסדנו, מה נעשה כדי להימנע? נעשה ביטוח)

\*\*\*רוב החברות הגדולות היום מנסות לעשות ביטוחי סייבר.

כל פונקציה בארגון- צריך לבדוק מה ייצור לה עכשיו המשכיות עסקית.

תרחישים של סיכון- בונים תרחישים ורושמים את הסיכונים ומזהים מה צריך לעשות

**שיעור מס' 7: 28/11/2018**

ניהול סיכונים:

סבירות: מה ההסבירות שזה יקרה בשנים הבאות וכו'..

נזק: הערכת הנזק

סיכון מורכב- הסיכוי שהוא יקרה והנזק הצפוי.

לפעמים לא יודעים למדוד את זה במונחים מספריים, איבוד מידע, איבוד פטנט, איבוד עובדים, זה משהו שניתן אולי לאמוד, ולקמט במספרים, אבל מוניטין זה משהו שאי אפשר לקמט, נבחן את זה במושגים של סיכון גבוה בינוני קטן.

בקרה: נועדה להוריד את גודל הסיכון

תאבון סיכון- שונה בין רפאל לשופרסל. ברפאל תאבון הסיכון שואף ל-0, לא תהיה גישה למידע לאף אחד. שופרסל- תאבון סיכון יותר גדול, ניתן לחיות עם סיכון יותר גדול.

הסיכון השיעורי- שמתי בקרה (דוגמת מפעל בפלורידה אם יש הוריקן) במרחק של 100 מטר יש אתר חלופי במידה ויש נפילת מערכות, המוקד הנוסף מתחיל לפעול.

המטרה של אבטחת מידע וסייבר להביא למעשה את הסיכון השיעורי לתאבון הסיכון שלי.

**$$$ Risk=probability (%) \* expected loss**

התמודדות עם סיכונים:

1. Risk mitigation- אבטחת מידע מתחילה לפעול. אני רוצה להפחית את הסיכון כדי להכניס אותו לתאבון הסיכון שלי.
2. Risk acceptance- נופל בתאבון הסיכון שלי ואני מקבל אותו כפי שהוא. חי עם הפסד של חצי מיליון דולר בפלורידה מוכן לקחת את הסיכון ולא עושה כלום, אם יקרה- אספוג חצי מיליון דולר.
3. Risk transfer- ביטוח, אם יש סיכון למשהו עושים ביטוח. זה מקביל לinsurance.
4. Risk avoidance - הימנעות מהסיכון- הבנקים לא עוברים לגיבוי מידע על ענן, הם נמנעים מהסיכון. (זה אולי יותר זול וכדאי אבל הם מפחדים להיכנס בכלל למצב שיש בו את הסיכון) מוותרים על הפעילות, הם לא מתמודדים עם הסיכון אבל הם נמנעים.

Justifying controls: מערכות שבדקות חיצונית את הספקים. אני רוצה להדליק את המערכת הזאת, אני צריך להודיע להנהלה שיש פה סיכון, צריך להעריך את הספקים האלה. צריך לקמט את הסיכון, הגענו למסקנה שזה שווה מיליון דולר בשנה, אז אני יכול להצדיק בקרה של עד מיליון דולר. בדקנו סבירות בדקנו מה הנזק הצפוי, (לעמוד מול המנכ"ל להסביר מה גודל הנזק)

אם יש לי סיכון שיכול לפגוע לי במוניטין- חדירה גם אם היא לא עושה נזק ואני מפרסמת אותה הלקוח יחשוב פעמיים האם לפתוח חשבון בבנק הפועלים או לא.

בנצ'מארקינג- אוספים את כל המנהלים ומתשאלים וכל אחד אומר את מה שהוא חושב ועל פי זה אני מחליט

Nist- ארגון תקינה אמריקאי

ISO- ארגון תקינה בינלאומי.

(עד כאן מצגת ניהול סיכונים)

**Access control בקרות גישה, (חשוב למבחן)**

בקרות גישה למידע, למערכות. הסיכון- גישה של מישהו לא מורשה – חדירה.

שמים סיסמאות, זה דוגמה אחת לבקרת גישה. IAAA

1. זיהוי (identify)
2. אימות (authentication)
3. הרשאות (authorization)
4. אחריותיות Accountability))

\*\*\*\*שאלה למבחן- מה הA השלישית אומר? תשובה אחריותיות Accountability))

Non repudiation- אי הכחשה- מישהו שעושה פעולות במערכת. עובד שיש לו גישה למערכת והפעולות שהוא עושה רשומות, העובד אחראי למעשיו. אוספים ראיות.

**CIA- \*\*\*חשוב מאוד למבחן**

Confidentiality **C** סודיות - היא מרכיב של פרטיות המיושמת כדי להגן על הנתונים שלנו מפני צופים לא מורשים

Integrity **I** נרצה לוודא שהמידע שהעברתי הוא שלם והוא כפי שהיה במקור ולא התערבו בו גורמים זרים.

**A** availability דוגמה הכי טובה ל availability זה מתקפה של DOS המערכת של בנק הפועלים ערוכה לכניסה של 1000 משתמשים, מהרגע שנכנסו 20000 משתמשים למערכת נוצר שימוש יתר במחשבים והמערכת קרסה.

**Access control** שיטה או דרך שבה אני מגדיר מי יכול להיכנס למערכת מי הוא משתמש שמותר לו לגשת ומי הוא משתמש שאסור לו לגשת. (בקרת גישה)

MACS- מנדטורי- אומר שאני הגדרתי דפוסים של למי מותר להיכנס למערכת ולמי תהיה גישה. מנדטורי אין גמישות.

DACS- דיסקרשינרי- אין לי שיקול דעת, אני מאפשר למשתמש לבקר או לשנות את הגישה שלו למערכת. יש גישה לשיקול הדעת של המשתמש.

Subject מי שפונה למערכת

Object המערכת שאליה אני פונה

מישהו שהוא לא מאושר רוצה גישה למערכת אני רוצה להבין

נרצה לאמת את הזהות של המשתמש- יש סיסמא, ויש גם

something you know - סיסמא

Something you have –אלמנט חיצוני (כרטיס עובד)

Something you are- ביומטרי (טביעת אצבע, קרנית, רשתית, קול, פנים וכו..) נשען על מאפיינים אישיים.

מה שבעיקר סומכים עליו זה טביעת אצבע כי היא ייחודית, קרנית ורשתית. גם ייחודיות ואי אפשר לדמות.

**ביומטרי**: (something you are)

False positove- מישהו שמותר לו, מישהו "חיובי", בטעות דחיתי מישהו שמותר לו

False negative- בטעות אפשרתי למישהו שאסור לו.

מודל בקרת גישה

BIBA INTEGRITY- אני שומר למעשה אני לא מאפשר לאף אחד, ביבה שומר על אינטגריטי

בלה לה פדולה- שומר על סודיות המידע

**הרצאה מס' 8: תאריך 05/12/2018**

Pocket filtering- דוגמה- רשת של רשימות IP שאני לא מעונין שיסתובבו ברשת שלי.

דוגמה לחוקים של הfirewalls- אם הוא הגיע מIP מסוים ומPORT מסוים, אני מוכן שיסתובב ברשת לא יותר מ3600 שניות.

Application firewalls- בנו firewalls שמונע כניסות, הוא יושב בשכבת האפליקציה, זה יושב בשכבת אפליקציה כי אני נותן לו להיכנס לרשת אבל אני לא נותן לו להשתמש באפליקציה מסוימת.

Proxy- בעברית זה מיופה כוח, כשאני בונה איזשהו שרת שהוא כביכול מיופה כוחי, הכוונה שאם הגישה עד היום הייתה לשרת שלי, אני רוצה לבנות מיופה כוח- מחשב אחר שבו אני מאפשר גישה של מחשבים אחרים.

מכיוון שהפרוקסי בדרך כלל יושב באזור שהוא פחות מאובטח הוא חשוף לסיכונים יותר גדולים. ואפשר להוסיף שם firewall נוספים.

False positive- מישהו שמותר לו, מישהו חיובי, בטעות דחיתי מישהו שמותר לו (לא אפשרתי לסטודנט שלי להיכנס לכיתה- זה טעות.)

False negative- בטעות אפשרתי למישהו שאסור לו.

**Remote access** מישהו שרוצה להתחבר מרחוק.

יש טכנולוגיה שנקראת רדיוס שזו מערכת שמאפשרת גישה מרחוק

רדיוס – אני מחבר אותו לשרת חיצוני ששם הוא מזדהה הוא אומר מי הוא, הרבה דרכים לבוא ולהגיד עכשיו תזדהה מול השרת, זה השרת שבודק אותך מותר לך או אסור לך להיכנס.

Sso- single sign on- הזדהות עבור כל כניסה לדבר אחר במחשב – הזדהות אבל אתר מסוים, הזדהות עבור תוכנה, ולא הזדהות חד פעמית המאפשרת גישה לכל האופציות במחשב.

Kerberos- במיתולוגיה היוונית זה כלב עם הרבה ראשים, קודם כל אני ניגש ל- Kerberos הזה ואז אני מתחיל להסתובב ומקבל כרטיס, עם הכרטיס הזה אני מקבל גישה ל- Kerberos נוספים לאפליקציות נוספות

Seseme- דומה מאוד ל Kerberos אבל משתמשים יותר באירופה.

VPN- virtual private networks- רשת פרטית וירטאלית – יתרון: אפשר לבקש הצפנה, ואפשר להצפין גם את הpocketים. החיבור עצמו מוצפן – חיבור מוצפן אומר שמי שאין לו את המפתח לא יכול להיכנס בכלל.

Intrusion detection and prevention system

סוג של בקרות שתפקידן להוריד את רמת הסיכון, חדירה מבוצעת כשהתוקף מנסה להשיג כניסה ומתנהג בצורה לא רגילה

אני בונה מערכות שמתחילות לחפש התנהגויות לא רגילות במערכת

התנהגות רגילה: צריך להגדיר מה זה התנהגות רגילה, וכל מה שהוא לא רגיל יזוהה.

signature - החתימה- ההתנהגות הנורמלאית.

אנומליה- בוא נראה מה אנומאלי, כל מה שאנומאלי לא ייכנס לרשת.- חשודה

אני מפעיל מערכות שצריכות לזהות חדירה למערכות. אני יכול רק לזהות אותם, ולהתריע ואני יכול למנוע מהם להיכנס.

מערכות IDPS איך אני מזהה התנהגות לא נורמאלית ומחזיר את המערכת להתנהגות נורמאלית

Detection- רק מתריע, לא זרקתי אותו מהרשת אני רק נותן התראה פנימית ואז אפשר לעקוב אחריו, אני מפתה את ההאקר להיכנס לאיזה חדר ואני "מטפל" בו שם, לפעמים לא נעים לטפל בהאקר והוא מתחיל להפעיל שיטות אחרות, ולכן בד"כ לא רוצים להתעסק עם האקרים מעדיפים לדווח על זה. אני רק רוצה שלא יחדרו ולא ייכנסו.

למה להשתמש בIDPS

כשאני מגיב לאירוע, זיהיתי שיש לי אירוע המשימה הראשונה היא להכיל את האירוע, אני מוכל, אני מבין מה גבולות הגזרה שלו אני מבין איפה הוא פוגע ואיפה לא, אני יכול לעשות פעולות שמתאימות להיקפי הנזק הצפוי ולא מעבר לכך.

אני מתריע, התראה, יש מצב של סכנה, יש מצב של חדירה ואז אני מסוגל להתריע באמצעות המערכת הזאת על חדירה לתוך המערכת. שיפורים אני רוצה לבוא ולהגדיר להנהלה, אני עושה בדיקת איכות ושיפורים אני רוצה להיות יותר טוב מבחינת אבטחת איכות או אבטחת מידע ולכן אני רוצה להוסיף מערכות כדי שזה לא יקרה בפעם הבאה.

יש סוגים שונים של IPS IDS –אני יכול לשים אותם בכניסה לרשת, כמו FIREWALL-ואז כל התנהגות חריגה בכניסה לרשת אני יאתר אותה, אני גם יכול לשים את זה באמת השרת, ברמת המחשב, במרמת הPOST (תחנת קצה)

חסרון HOST IPS- הרבה מאוד התקנות, עדכונים, צריך לחזק לשדרג לראות שזה עובד, אם יש לי אלף מחשבים ואני רוצה לשים אלף IPS IDS אני צריך לשים אלף התקנות ואני צריך גם לשדרג. בנוסף לפעמים זה לוקח הרבה מקום בזיכרון,

signature - הגדרנו חתימה, אני מחפש חתימה ברשת שמתנהגת כמו חתימות שהגדרתי, למה זה נפוץ יותר? כי אני זיהיתי פעילות מסוימת שיהיא אסורה ואני רוצה לחפש התנהגויות דומות לזה, זה החתימה, איפה הבעיה? אם יש סוג חדש של מתקפה, החתימה לא מכירה אותו, כי החתימה זה מה שהיה. – רק מתריע

ANOMALY BASES- בגישה שאני בונה מה נורמאלי לא נורמאלי, א-נורמאליה- התנהגות לא תקינה אני מתחיל לאסוף סטטיסיטיקות שמזהות התנהגות לא תקינה ברשת, סוכם (סכום מספרי) כמה פאקטים עברו, כמה פאקטים מיועדים לIP מסוים. כשיש התנהגות חריגה מבחינתי זה א-נומאליה. (מזהה גם התקפות חדשות)

למי אני צריך לתת התראה? למנהל אבטחת מידע אני אתן התראה.

מה הוא לא יכול לעשות- אם יש בעיה באבטחה הוא לא פותר לי את הבעיה, הוא רק מתריע.

שלב פורנזיקה- אני מתחיל לאסוף מידע, (להבין איך זה קרה, מה קרה – כמו חוקר במשטרה)

יישום IPS IDS אני יכול ליישם באופן מרכזי ואז יותר קל לי לבקר את זה ולתחזק את זה יותר קל לניהול ולתחזוקה, זה קיים באיזה מחשב מרכזי.

**הרצאה מס' 9: תאריך 12/12/2018**

הרעיון של firewall-

כשדורון אמרה שטלפונים לא סורקים את כל האצבע למה הם לא סורקים את כל האצבע? כי זה:

False positove- מישהו שמותר לו, מישהו חיובי, בטעות דחיתי מישהו שמותר לו

False negative- בטעות אפשרתי למישהו שאסור לו.

ביציאה מהארץ זה לא תמיד עובד, כי אתה מכניס את כל כף היד, ואתה צריך דיוק מושלם.

שמים firewall בכניסה, בDMZ. אפשר לשים firewall גם על השרת עצמו.

Proxy אני שם מחשב או שרת ואני קורא לו פרוקסי (מיופה כוח- נציג שלי) הוא מרוחק ממני, (כמו ש.ג. במכללה, אבל אם אני ישים אותו מרוחק אז יגיעו למכללה רק כאלה שעברו אותו).

לשרת שאחרי הפרוקסי מגיעים כ50% מהמבקשים, מה שלמעשה מבטל לי חצי מהבקשות.

IPS IDS

אני מחפש תנועה לא רגילה ברשת זאת אומרת אני רוצה לזהות התנהגות לא רגילה ברשת, ואז אני מתקין תוכנה שלמעשה מזהה התנהגות לא רגילה ברשת מישהו שנכנס בשעות לא נורמאליות, זאת אומרת אני מזהה תנועה חשודה, אם אני בids אני מעביר אותו לבדיקה, אם זה האקר אני מכניס אותו לבדיקה

Honeypot מלכודת דבש, יש לי יכולת לזהות מישהו עם תנועה חריגה מישהו שנכנס בשעה לא סבירה אני עוד לא מאשים אותו אני רק רוצה לבדוק אז אני מנתב אותו, איך אני מפתה אותו? אני בונה מלכודת דבש, ההאקרים כשנכנסים הם מחפשים לאסוף מידע, מי היוזר העיקרי, מי מנהל אז אני מפתה אותו לכיוון איזה אדמינסטרטור, למעשה ליקטתי אותו והכנסתי אותו לחדר סגור, הרעיון לא להתעמת איתו. הרעיון לערב את רשויות החוק שיפתרו את זה. אם ההאקר לא זיהה שהוא נתפס, זה מעולה אני מחפש לראות את ההתנהגות שלו, כדי למנוע איום.

DLP – DATA LEAKAGE PROTACTION – מערכות שמתקינים אותם בדרך כלל לטיפול במיילים - אני רוצה לראות אוסף של מחרוזות, ורוצה לראות אם זה הגיע מגורם שאני לא מכיר ממדינה שאני לא מכיר. קווארנטין זה אזור מבודד, אזור מבודד ששם המייל מחכה אותו אחד שאמור לקבל אותו. אותו אחד ששלח אותו אמור לקבל הודעה, וההודעה אומרת כזה דבר: אתה מכיר את מי ששלח לך? אתה יודע שאתה צריך לקבל? אם זה חמור כלומר יש לי מחרוזות שמצביעות על התנהגות לא תקינה

קריפטוגרפיה=הצפנה: בקרה הצפנה זה שילוב של מתמטיקה גבוה, הרעיון לבנות אלגוריתם שמערבל מידע באמצות מפתחות חיצוניים באמצעות כלים חיצונייים אני מערבל מידע כדי שהוא לא יהיה קריא.

Confidentiality- יש לי מידע מסויים כמו סודות אישיים תיק רפואי של אזרח מסוים צריך להצפין אותו.

Integrity-רוצה לוודא בצורה מוחלטת שהמידע ששלחתי לו לא השתנה מהרגע ששלחתי לו אותו ועד שהוא קיבל.

Non repudiation- אני למעשה לא יכול להתכחש למידע ששלחתי או לפעולה שעשיתי, הוכחה בלתי ניתנת לערעור לשולח, נתתי אישור לזה אני הצפנתי את המידע שלי, אני לא יכול להתכחש ששלחתי את המידע. ואז יש לי אחריותיות- אני אחראי למעשי. מדובר בעיקר על התוכן לא רק על השליחה והקבלה.

מונחים בעולם קריפטוגרפיה

לטקסט לפני שהצפנתי אותו קוראים plain Text -הטקסט לפני ההצפנה.

עושים הצפנה cipher Text הטקסט מוצפן

אם ניתן לי מייל מוצפן ואין לי דרך לפענח אותו אני לא יוכל לקרוא אותו אני אראה משהו כמו ג'יבריש.

הצפנה בסיסית-

1. תציב מספרים או מערכים, איך אני יציב מספרים? המפתח תורגם למספרים לי סדר הabc
2. האותיות נרשמים לפי מפתח של 6 אותיות, כי המפתח הוא שש אותיות.

אפשר להשתמש גם בקודים. קודים הם אלטרנטיבה אף אחד לא חייב לדעת מה הקוד הזה, בצבא יש גלגלים גפרורים וקודים כאלו, קוד זה לא הצפנה, קוד זה משהו שמוסכן על שני הצדדים ושני הצדדים מכירים אותו.

סוגים של הצפנות: אנחנו מכירים כמה סוגים של הצפנות- טרנספוזישן – אני לוקח טקסט ומשנה מיקום יש לוגיקה כלשהי.

סבסטיטיושן—אני מחליף אותיות, i הפך להיות n , B הפך להיות E, כשמבינים את השפה מתחילים בהחלפה זה הופך להיות פשוט.

בלוק סייפר- מחלקים את הטקסט לבלוקים ומטפלים ברמת הבלוק עם המפתח.

וואן טיים פל- לסיסמא או מפתח שמחולק פעם אחת ומושמד המפתח הזה מיוצר באופן רנדומאלי לשני הצדדים צריך להיות אותו מפתח, אורך המפתח כגודל הטקסט.

המחיר- קשה לייצר אותו הוא מאוד ארוך, צריך לשמור אותו כדי ששני הצדדים ידעו אותו – ההפצה בעייתית. אני רוצה לשלוח את המפתח שאני עושה בו שימוש. אז צריםך להצפין גם את המפתח

ZERO KNOWLEDGE- אני עכשיו צריך לשכנע משתמש באיזה שהיא טענה בלי שאני העברתי לו מידע בכלל.

**הרצאה מס' 9: 19/12/2018**

חזרה על שיעור קודם:

קריפטוגרפיה= תורת ההצפנה- תחום מתפתח, הצפנות עיקריות שאנחנו מכירים הם סימטריים ואסימטריים,

סימטריים לשני הצדדים יש את אותו מפתח, מפתח זהה אחד.

איך מעבירים את המפתח ככה שלא ייחשף? עם המפתח אנחנו מצפינים, ועם אותו מפתח פותחים.

זוהי שיטת ההצפנה הסימטרית

א-סימטרית- לכל אחד שני מפתחות- מפתח ציבורי (קוראים לו ציבורי כי אני רוצה שכולם יידעו אותו) אני מצפין באמצעות הציבורי של הצד השני, הצד השני פותח באמצעות הציבורי והפרטי שלו.

המפתחוות הם קריטיים כי עם האקר שם את היד על המפתח אז הוא יודע לפענח את ההצפנה.

המפתח הפרטי צריך להיות משהו לא חשוף- שמור והוא קריטי. נכנסס האלמנט של גודל המפתח- מינימום 128 ביטים, יש מפתחות גם של 512 ביטים יכול לקחת שנים לפצח אותם.

מטרת ההצפנה- משיגים שלושה אלמנטים:

**ענן.**

IAAS – Infrastructure as a service – תשתית בסיס לשירותי ענן – מקבילה לשרתים הקיימים

PAAS – Platform as a service – פלטפורמה שלמה כשירות

SAAS – Software as a service – תוכנה שלמה ומוכנה כשירות. אני לא שם את האפליקציה שלי אני קונה זכות שימוש (אני לא מפתח אותה, היא אפילו לא שלי) עבור אפליקציה שיושבת בענן.

PRIVATE – חלק שלי בענן

PUBLIC- כל האזור (לא רק שלי)

HYBRID- שילוב של שניהם

כשצריך לנהל סיכונים אם אני שם אפליקציה בענן למה אני חשוף? לדליפת מידע, לפריצות שיכולות להיות בענן כי זה לא בשליטה שלי, קריה של גוגל קריסה של אמזון. עדיין צריך לנהל את הסיכון לראות אם צריך לשים עוד בקרות.

אסטרטגיית אבטחת מידע צריכה להיות קשורה לאסטרטגיית הארגון. היא כוללת בתוכה גם את האסטרטגיה של הענן ואני כמנהל אבטחת מידע צריך לבוא ולהמליץ לחברה מה לעשות. איומים וסיכונים שצריך לקחת בחשבון, (איומים כמו פריצות חדירות מתחרים כניסה של מתחרים למערכות שלי)

ב- PUBLIC CLOUD אני אוודא שלמות נתונים וזמינות

ON PREMISE (של המשרד) – confidentiality מי משתמש וכך הלאה אני אקבע

הענן הוא חשוף- יש בקרה שאפשר להיכנס דרכה, אוטומציה, ספקים-מי הספקים (יכול להיות לי ספק ענן מעולה אבל גם לו יש ספקים)

הסבר סוף המצגת (תרגום מאנגלית לעברית)

הענן נותן הזדמנות למנהל אבטחת מידע.

תנו אמון בספקים שלכם אבל לא בתורה עיוורת

תוודאו שאתם מנטרים אותם בזהירות

לא מצליח, יש לך ספקות תעבור, למרות שהמעבר לא פשוט.

**הרצאה מס' 10: 26/12/2018**

שכבת היישומים: שכבת אפליקציה – מה שיושב על המחשב, מה שאתה כמשתמש רואה. אפליקציות web- שכבה מספר 7.

דוגמאות לשכבת אפליקציה- מיילים, web, מערכת הפעלה, (כל מה שרואים בפרונט ועושים בו שימוש)

בשכבה הפיזית עוברים ביטים.

**רכיבים בסיסיים באבטחת מידע:**

אימות זהות

הרשאות

שלמות ואמינות מידע- אני רוצה לוודא שמה שאני שולח זה מה שאני מקבל.

זמינות מידע – זמינות של מידע זמינות של מערכות.

שכבת האפליקציה נוגעת בכל הרכיבים האלו.

מודל OSI

שכבת יישום- HTTP – אינטרנט- כל גישה שלי לאינטרנט עובדת בHTTP.

SMTP – פרוטוקול בשכבת היישום שמתעסק עם דואר, יש משתמש בג'ימייל לדוגמה, זה היוזר אייג'נט.

הכי חשוב לשים דגש על אבטחה -- בשכבה הפיזית. \*\* חשוב למבחן

שכבת השיחה- דוגמה להתקפה אני פותח שיחה, למה היא חשובה? כי רוב היישומים נעשים דרך שיחה. מספר השיחות שפתוחים בו זמנית- צריך להגביל אותם.

דיברנו על 3 גורמי סיכון עד כה.

טכנולוגי- כל מה שקשור בחומרה תקשורת תוכנה. בקרות כמו firewall נועדו למנוע או למנוע חלק מהגישה לאנשים שלא מיודעים להיכנס.

תהליכים- מידת הנזק משגיאת אנוש או נקודות תורפה טכנולוגית עשויה לפחות מאוד במידה ומבוצע תכנון נכון של התהליכים בארגון. הגדרת תהליכים בסדר נכון ובדוק מראש מאפשרת זיהוי מוקדם של פגיעה או ניסיון פגיעה במערכות.

אנשים- המשתמשים בטכנולוגיות ולכן מהווים חוליה חלשה מאוד מכיוון שהם מפעילים או משתמשים בטכנלוגיות ונוטים לעשות שגיאות המייצרות פרצות במערך ההגנה אשר מאפשרות לתוקף לנצלן.

אנשים זה החולייה החלשה- עובדים ממורמרים וטעויות שתבמצעות- האקרים רק מחפשים את הטעויות האלו.

בפועל צריך להסתכל על תהליכים עסקיים ולראות האם הם מאובטחים מההתחלה עד הסוף ואם יש סיכון על הדרך.

הנדסה חברתית-

מושג מתחום האבטחה ובפרט בתחוום אבטחת המידע, שמשמעותו ניצול של תכונות פסיכולוגיות של האדם אשר עשויות להביא אותו לציית לבקשותיו של הפורץ.

התמודדות עם הנדסה חברתית- מודעות. אני צריך ליידע את כל הגורמים החברה שבאים במגע עם גורמי חוץ, לא לתת מידע גם אם נשמע לי סופר נחוץ. העלאתי את המודעות אנשים פחות חשופים ופחות נותנים מידע.

דוגמה: אפליקציה של חברת תעופה יש בה באג, (בכל המערכות יש באגים) הבאג הזה מאפשר בחמש שורות של קוד לקבל מידע על נוסעים ב24 שעות. חסר לו רק כרטיס אשראי, פה נכנסת ההנדסה החברתית- גם זה עושים על ידי שליחת הודעה למספר הטלפון של הלקוח בהודעה כתוב שדרג טיסה ב20 דולר, מי לא ישדרג ואז הלקוח שולח את מספר כרטיס האשראי בקישור שצורף בהודעה חוזרת.

איך ממשמים פישינג טוב? להסתיר URL , לקנות URL ממש קרוב לחברה נניח לגוגל זה GOO.GL אז גוגל תקנה את הכתובות הכי קרובות אליה כדי למנוע מהאקרים לפגוע במשתמשי גוגל.

וירוס כופר- RANSOMWARE

תוכנת סריקה, מתקינים קוד זדוני בדרך כלל כתוצאה מפתיחת לינק, סריקת קבצים במחשב והצפנתם. אם אתה רוצה גישה מחדש לחומר אתה צריך לשלם את הכופר של כמה אלפי שקלים.

ארגון שהצפינו לו את הDATA זה לא פשוט. איך מזהים? מוודאים שכתובת השולח נכונה ועדכנית.

מיילים עם הגבלת זמן – משהו שיוצא אלמנט דחיפות לחץ אמור להתריע לנו.

איך מתגוננים מוירוס חומר- גיבוי לא מקוון- מקוון נעשה לא און ליין. גיבוי לא מקוון אפשר לחזור אליו הוא עוד לפני הצפנה.

BUFFER OVERFLOW

שטח אחסון זמני ואם אניי מנסה לאחסן בה יותר ממה שהיא תוכננה, מה השדה שאני מצפה לו ומה החסימה כדי לא להגיע למצב שאני מכניס מיליון במקום של עשרת אלפים.

SQL injection

יש מתקפות שמתבססות על SQL תוקף מכניס מידע נוסף בשאילתא רגילה.ניתן למנוע את זה בפיתוח כל הפרצות

ZERO DAY – פעם ראשונה נחשפתי – תיעד באפליקציה שלא נכתב לה תיקון.

סוס טרויאני- מחדירים תוכנה שמתחזה לתוכנה רגילה ובאמצעותה חודרת למחשב. הגנה מכל אנטי וירוס וfirewall

STUXNET

תולעת מחשב – וירוס תולעת שהשתילו אצל האיראנים. SCADA צרה צרורה מבחינת אבטחת המידע. לתולעת יש יכולת לתכנת מחדש את הבקרים.. תולעת ראשונה שהתגלתה והראשונה שנועדה לפגוע במערכות בקרה תעשייתיות. לתולעת חתימה דיגיטלית – זה אישור שכביכול זה מגיע מגורם מוסמך. החתימה הדיגיטלית נגנבה משני מפיצים של חתימה דיגיטלית. צעד שאפשר לתולעת לא להתגלות תקופה ארוכה.

Secure facility

תשתית של החברה אני צריך להגן עליה מבחינה פיזית, להוריד סיכון של איומים פיזיים. נעזרים באלמנטים טבעיים – זרימה של מידע של תעבורה

גדרות, שערים- צריך להכניס אלמנטים אמינים של אבטחה פיזית. שומרים, כלבים, מנעולים, מפתחות, כניסה סגירה ורק אז כניסה, מונטורים אלקטרוניים. מערכות אזעקה חדרי מחשב חדרי תקשורת כרטיס עובד- אלמנט פיזי שבאמצעותו נכנסים

וכו'..

איפה שמים חדר מחשב לפי אבטחת מידע? במרכז.

כוח אדם-

אחריות כוללת של המנכל הוא צריך למנות CISO, CISO מי שעושה את זה בפועל. כדי לקחת את זה לעולם המציאות, מוצאים היום את CISO ברוב המקרים כפוף לcio

מגיע CISO וכל מה שהוא עושה זה שם ברקס – פה תשים עוד firewall

CIO רוצה להביא מערכות חדשות וכו.. מנהל אבטחת המידע תפקידו שהמערכות יהיו מאובטחות ולכן הרבה פעמים הוא עוצר את הCIO

בהרבה מקרים מוצאים שCIO מנהל את הCISO ולפעמים זה טוב.

תחת CISO יש שני גורמים צלע אחת: שמטפל בכל האיומים- כל הבקרות שדיברנו עליהם – הוא מוודא שחומת אש מותקנים כמו שצריך ואם לא איפה צריך לשפר. (תקלות ומערכות בקרה וכל מה שקשור בתפקוד היום יומי)

הצלע השנייה היא צלע פרוייקטלית (פרויקט זה בקרה כל בקרה זה פרויקט. אני מכניס חומת אש חדשה צריך לבדוק אותו) ניהול פרויקט מההתחלה עד הסוף.

הסמכות:

2 הסמכות משמעותיות:

CISSP – הסמכה בפרטים- להבין תשתיות לבוא מעולם תשתיות. ההסמכה הכי יוקרתית. ציון עובר 70

CISM- הסכמה קלה יותר מהראשונה – ציון עובר 56 מי שבא מאוריינטציה ניהולית ההסמכה הזאת יותר קלה לו.

**הרצאה מס' 11 : 2/1/2019**

**הצפנות** יש שני סוגים שצריך להכיר: סימטרית וא-סימטרית.

**Access control**

I זיהוי

A אימות

A הרשאות

A אחריותיות

**ACL: ACCESS CONTROL LIST**

רשימה של למי מותר להיכנס ולמה. טבלת הרשאות שמתעדכנת כל הזמן.

**אימות רגיל –** לקוח מתחבר לשרת מזין את הזהות שלו את האימות שלו, האימות שלו נעשה כבר בשרת עצמו ואז הוא עושה את הפפעולות שהוא צריך לבצע מול השרת שלו.

**תהליך קרברוס –** כולל שלושה רכיבים: לקוח, שרת (שירות היעד), ושרת הקרברוס.

יתרונות-

1. סטנדרט
2. סיסמאות לא עוברות ברשת
3. אימות הדדי של client ו- service
4. שימוש חכם במפתחות הצפנה.

תקנים:

**PCI DSS**

תקן שאנחנו נותנים לחברות שמתעסקות עם כרטיסי אשראי, תקן שיצרו חברות אשראי כדי שיבטיחו סליקת אשראי לצורך אבטחת מידע על מנת להגן על המידע בעסקאות.

**מטרות:**

1.הפחתת סיכון להונאות כרטיס אשראי

2.הגברת שליטה בכטיס אשראי

3.אימות זהות משופר של בעל הכרטיס

לתקן יש 12 דרישות (לא צריך לדעת אותם אחד אחד)

* הקמה ותחזוקה של רשתות מאובטחות:

דרישה 1- יש להתקין ותחזק באופן שוטף firewall להגנת נתוני כרטיסי אשראי

דרישה 2- אין להשתמש בהגדרות ברירת מחדל של כל התקנים והטכנולוגיות שסופקו ע"י ספקים חיצוניים.

* שמירה על נתוני כרטיס אשראי

דרישה 3- יש לשמור ולהגן על נתוני האשראי

דרישה 4- לוודא הצפנה של כל נתוני כרטיסי האשראי שנמצאים בתנועה

* תחזוקה לניהול פגיעויות/חשיפות:

דרישה 5- יש להשתמש ולעדכן באופן שוטף תוכנת אנטי וירוס

דרישה 6- נדרש לפתח ולתחזק מערכות ואפליקציות באופן מאובטח.

* יישום ובקרות מנגנוני גישה חזקים

דרישה 7- הגבלת גישה לנתוני כ"א רק לאותם אנשים נרשים מתוקף תפקידם

דרישה 8- כל עובד נדרש לגישה לנתוני כ"א נדרש בזיהוי ייחודי חד חד ערכי וייחודי בכניסה למערכות ואפליקציות המטפלות בכ"א.

דרישה 9- יש להגביל את הגישה הפיזית לכ"א.

* ניטור שוטף ובחינה של רשתות מחשוב:

דרישה 10- באופן שוטף נדרש לבדקות מערכות ומנגנוני אבטחת מידע ותהליכים נלווים

דרישה 11- נדרש לבצע מעקב וניטור שוטף לכל הגישות למשאבי רשתות המחשוב

* מדיניות אבטחת מידע:

דרישה 12- יש ליישם בארגון מדיניות אבטחת מידע לכל העובדים וקבלני המשנה של הארגון

(נמצא בארגונים יותר ביטחוניים)

SDLC – (דיברנו על זה בשיעור ראשון) - יש תהליכי פיתוח עשרות שנים, כל תהליך שאני אכנס אליו מוקדם יותר זה יהיה לי יותר זול ואני יוכל להימנע מכל מיני פגיעויות מיותרות.

**תקן ISO27002 :**

תקן בינלאומי המספק כללים ברורים לניהול אבטחת מידע בארגון.

הוא בסיס לתקנים נוספים שפותחו.

התקן דורש מדיניות אבטחה, נכסי מידע, היבטי אבטחה לעובדים קיימים וחדשיםף הגנת על סביבת ומתקני מחשוב, הקמת מערכות בקרה וניהולן הטכני, הגבלת זכויות גישה לרשתות, צפיית אירועי פריצה וניהול תגובה הולמת, אמצעי הגנה שמירה וניהול שחזור בעת קריסה של המידע.

**תקן ISO 27799**

תקן בינלאומי לאבטחת מידע בתחום הבריאות:

מבוסס על תקן כללי (27002) מטרתו לתת הגנה על מידע רפואי אישי שברשותם.

התקן עוסק בשמירת כל המידע הבריאותי, בריאות אישי הנוגע לאדם שניתן לזהותו וקשור למצבו הפיזי או הנפשי לשרותי בריאות המסופקים לו.

GDPR – מחויבות של כל ארגון שעובד עם האיחוד כולל צד שלישי של חברות כאלו.

המטרה של superation of duty זה למנוע מעילות כמו בסיפור של אתי אלון

Accountability – אחריותיות יעילה נשענת על היכולת להוכיח שגורם מסוים עשה פעולה מסוימת, אני עוקב אחר הפעילויות שלו, אני יודע שX עשה אתמול משהו ולכן הוא לא יכול להתכחש.

סוגי בקרות גישה:

Preventive- (מונע) אני רוצה לעצור כל פעילות שהיא לא רצויה או לא מורשית. (מישהו ניסה להיכנס, מנעתי ממנו להיכנס, לדוגמה firewall מונע כניסה

Detective- (רק מזהה) זיהיתי פעילות חריגה ברשת- מישהו נכנס בשתיים בלילה על בסיס כקבוע כבר כמה ימים, לא קרה בעבר אני רוצה לדעת למה. תזוזות לא רגילות ברשת אני רוצה לדעת – האיתור של החריגה לא בהכרח מנע את ההאקר להינכס

Corrective -(מזהה ומתקן/מונע) משחזר את האזור שהיה בו בעיה, מזהה ומתקן.

הרצאה מס' 12 9/1/2019

הרשאות – 2 גישות

Need to know- מה אני מאפשר לו במערכת שהוא צריך לדעת – אני יודע מה הוא צריך לדעת ואני אתן לו את מה שהוא צריך לדעת.

List privilig- מינימום הרשאות – מדברת גם על זכויות וגם על הרשאות

ב2 מקרים אלו נותנים למשתמש מה שהוא צריך.

שאלה למבחן- למשתמש האדמינסטרטור פותח יוזר ומגדיר הרשאות לאחת ממהרשאות הוא נותן לו גישה לקרוא לשנות – האדמינסטרטור לא נותן הרשאה

Separation of duty- חלוקת תפקידים – החלפת עובדים. בשאלות מדברים על collusion- קנוניה – שניים שחברו והחליטו לעשות פעולה זדונית לשם כך עושים Separation of duty. כשאני מדבר על fraud – מעילה.

ניטור של הפריווילגיות – אני מנטר אחת לכמה זמן את כל הפריווילגיות שנתתי ואני עושה את זה כי אנשים לפעמים מחליפים תפקידים.

מחזור חיים של המידע בתור התחלה אני מסווג את המידע מסמן את המידע, למה אני מסווג ומסמן? כדי לראות מה רמת ההגנה שאני רוצה לתת, ואם אני מסוגל לעשות סגמנטציה אז אני יכול לעשות הגנה בשכבות (defense in depth) והגנות נוספות על איזורים שאני רוצה יותר. השמדת מידע פתורה בפני עצמה – כי אם אני עכשיו מקבל מחשב של מישהו אחר, והוא מחק הכל הוא רק חושב שהוא רק מחק הכל, נשארים הרבה מאוד טביעות אצבעות. צריך לבער מידע, אם לא עשו תהליך נכון של השמדת מידע – המידע עדיין זמין וקיים גם עבור משתמש אחר במחשב.

2 סביבות:

Virtual machine - מכונות וירטואליות.

Cloud base- כל מה שקשור בענן אני מאחסן מידע בענן זה מעלה את הסיכון אני צריך לראות מי אחראי ועל מה.

(חייו של איש אבטחת מידע – מנהל סיכונים ובקרות)

Configuration management – אם התצורה משתנה אני צריך לבוא לעדכן ולראות בדיוק באיזה תצוגה אני משתמש. אני רוצה להיות כמה שיותר מעודכן ולעדכן כמה שיותר עדכונים.

Patch management – פץ' תיקון תוכנה – היו אוסף של תקלות – חברת התוכנה אוספת באגים פותרת אותם ונותנת לך פץ' שמתקן את הבעיות שהיו. הפץ' הזה מתקן את התיקונים ולפעמים מכניס בעיות חדשות.

Vulnerability management - יש כלים שמרצים היום במערכות – scanner - אני יכול לבוא באמצעות כלי מבוקר לראות איפה יש חולשות, סביבה של תשתיות שאני יודע שיש בהם תשתיות- וגם אני רוצה לראות דברים שחוזרים על עצמם.

Cloud- אני העברתי פעילות לcloud אני צריך לראות מה אני צריך לתחזק, זה הולך ומשתנה – הולך וגדל מבחינת אבטחת מידע ככל שאני עולה לכיוון הsaas

Google drive – נחשב saas – אחראי על אבטחת מידע של התשתית. בענן יש תשתית. בsaas האחריות היא על הגוף שנותן לך שירותים.

Incident response- דיברנו על חיי היום יום של אבטחת מידע, אני רוצה להגיב לאירוע, אני רוצה לזהות את האירוע, אני רוצה להגיב לאירוע, מכילים את האירוע יודעים איפה הוא נוגע ואני יודע איפה הוא לא נוגע.

botnet

רשתות של רובוטים- אני עושה שימוש ברשת של רובוטים. מחשבים שיש בהם שימוש, וכביכול הם נקראים לפעמים גם זומבים – מארגנים אותם ברשת והרשת הזאת עושים בה שימוש ההאקרים.

Men in the middle attack - התקפה שבה ההאקר נכנס באמצע ביני לבין השרת. מאותו רגע שהוא השתלט על התקשורת והוא מציג את עצמו כשרת אני מתקשר מול הההאקר, השרת כבר לא יודע שאני מבקש ממנו דברים.

אני רוצה לזהות התנהגות לא רגילה לא נורמאלית – א-נומליה ברשת- פאקטים גדולים כמויות משתמשים גדולות התנהגות לא סבירה של משתמשים – בניתי התנהגות נורמאלית ואני משווה מול המידע, אני יודע שככה זה נורמאלי – כל מה שלא- לא נוראמלי.

HIDS – אינטרוז'יין דיטקשיין

NIDS – אני מנטר את הרשת לפעילויות שהם לא רגילות

מלכודת דבש- honeypots מישהו רוצה להיכנס לרשת שלי אני מזהה בעיה זה לא רגיל אני מפתה אותו עם משהו- ההאקר מתפתה ללכת לזה ונלכד.

Penetration testing – האקר מולבן – תפקידך לקבל אפליקציה או לקבל סביבה, ולנסות לחדור אליה.

Drp סוגים:

Hot site – אתר ש"מחכה לאסון" – מוכן לגמרי למקרה של אבטחה שריפה וכו'.. מוכן לגמרי לשימוש. (דומה מאוד לmirror רק בלי כל המידע שנמצא בmirror- זאת אומרת פחות מעודכן מהmirror.

Mirror site- אתר ש"מחכה לאסון" - אני משכפל את הנתונים – אותם מחשבים אותו מידע אותו גיבוי אני צריך גם לתחזק את זה- זה מיידי לא מרגישים אפילו שאחד השרתים הלך. – הכי יקר.

Warm site- חמים- בו יש כמעט הכל בתוך שתיים עשרה שעות מפעילים את החדר מחשב הזה. כי יש בו פחות אלמנטים וצריך להעביר את המידע או לשחזר אותו ואז הוא יתחיל לעבוד.

Cold site- אתר עם מיזור רצפה הכל – רק צריך למלא אותו במחשבים כל מה שקשור בתקשורת ומערכות, ואז אוכל לעשות בו שימוש זה ייקח הרבה יותר זמן אבל הוא הרבה יותר זול.

שאלות דוגמה מהמבחן:

מה מהבאים אינו נחשב הפרה של סודיות?

1.גניבת סיסמא

2. האזנת סתר

3**. פרס חומרה**

4. הנדסה חברתית

אילו מהבאים הוא עיקרון CIA המתכוון שלsubject עם הרשאות ניתנתגישה ללא הפרעה עם אובג'קט

1.זיהוי

**2.זמינות**

3. הצפנה

4. שכבות

בקרה שאין לה סיכון- בזבזתי את כספי הארגון. אנשים מתלהבים לשים כל מיני כלים כאלו ואחרים, אם אין סיכון לא צריך, אם צריך הגנה, אז יש צורך. צריך להפעיל שיקול לדעת, לא בהכרח יש סיכון. (שאלה על חברת ביטוח שבוודאות תהיה התשובה היא בזבוז כסף של החברה)

איזה מהמשפטים הבאים הוא אחת הסיבות העיקריות שארגון אוכף חופשה כפויה

1. כדי לבצע סבב תפקידים

**2.כדי לאתר הונאה**

3.כדי להוריד את רמת הלחץ של העובדים

מהי המטרה העיקרית של קרברוס

1.סודיות

2.אינטגריטי

3**.אימות**

4.אחריותיות

הגנה בשכבות היא?

1. שיטת הגנה ממלחמת העולם השנייה
2. מתודולוגיה מאפשרת להגן על כל נכסי המידע באופן זהה
3. **הגנה על נכסי הגנה קריטיים באופן מאטובטח יותר מנכסי מידע קריטי**
4. מתודולוגיה מאפשרת

סיכון שיעורי- residual risk - הינו

1.תאבון הסיכון

2.העברת הסיכון לגורם חיצוני

3**.הסיכון שנשאר לאחר יישום הבקרות להפחתת הסיכון**

4.סיכון מחושב

Firewall- מתתבסס על:

**1.חוקים**

2.אש ועשן

3.קוד פתוח

4.קירות גבס

מי מהבאים אינו דוגמה לסגמנטיציה של הרשת

1. אינטרנט (פנימי)
2. אקסטרנט (חיצוני)
3. DMZ
4. **VPN**

רשת מסוג BOOTNET

**תשובה: משתמשת במחשבי זומבי ללא ידיעת בעליהם.**

איזה **לא** יתרון של א-סימטרי

**תשובה: מהירות**

מתקפות מסוג סחיטה- רנסמוי

**תשובה: מצפינות את קבצי המשתמש באמצעות מפתח סימטרי**

מה זה סייבר?

**תשובה: חיבור בין עולם ותוכנה וחומרה למארג אחד**

3 גורמי סיכון עיקריים הם:

**תשובה: טכנולוגיה אנשים תהליכים people process technology**

שאלות בטוחות במבחן שלא הספקתי להקליד:

\*\*\* מהו תקן ISO27002

\*\*\*מהו ? DMZ

\*\*\*שאלה על false positive