מדריך עולם הסייבר

תוכן עניינים

מה זה לוחם סייבר?

דמיינו חדר אפל ובו דמות לבושה מסכה שיושבת מול מחשב ומקלידה... תווים ירוקים מופיעים על מסך שחור, ובמקום כלשהו אחר בעולם, משהו שלא היה אמור לקרות - קורה. במציאות, הדמות שלנו לא תלבש מסכה ולא יהיו סביבה קטעי קוד מטריקס...היא פשוט תשב במשרד, וכנראה תשתמש בתוכנה נוחה לעריכת טקסט. אבל כל השאר נכון. במקום כלשהו, קורה משהו שלא היה אמור לקרות. כי בעולם הדיגיטלי שלנו, יש מגוון מקורות שאינם מאובטחים ויש פושעים שירצו לגנוב סודות, לזייף חוזים, לגרום לתאונות רכב, לשגר טילים. אבל גם להתגונן מפני דברים כאלה.

צריך להבין שבעבר, בעל המאה היה האדם שברשותו שטח חקלאי. עם פרוץ המהפכה התעשייתית, בעל המאה היה האדם שברשותו תעשייה. כיום, בעל המאה הוא האדם שברשותו מאגרי מידע עצומים ונתונים בסדרי גודל מטורפים, בהם הוא שולט ויכול לעשות משהו שרוצה. כמו למשל, מארק צוקרברג בפייסבוק או כמו למשל חברות ביטוח ענק ששולטות בכמויות מידע בסדר גודל אטומי ורק אם הן לא יהיו מאובטחות, כל המידע על המובטחים עלול להיפרץ... (ראו ערך: אירוע שירביט, 2020)

מהי אבטחת מידע?

רשת המידע האלקטרונית המחוברת הפכה לחלק אינטגרלי מחיי היומיום שלנו. ארגונים מכל סוג, כגון מוסדות רפואיים, פיננסיים וחינוכיים, משתמשים ברשת זו כדי לפעול באופן אפקטיבי. הם מנצלים את הרשת לאיסוף, לעיבוד, לאחסון ולשיתוף של כמויות אדירות של מידע דיגיטלי. ככל שיותר מידע דיגיטלי נאסף ומשותף, כך הופכת ההגנה על מידע זה לחיונית יותר לביטחון המדינה וליציבות הכלכלה.

אבטחת סייבר היא המאמץ המתמשך להגן על מערכות מרושתות אלה ועל כל הנתונים מפני שימוש בלתי מורשה או נזק. במישור האישי, עליך להגן על זהותך ועל הנתונים והתקני המחשוב שלך. במישור הארגוני, כל אחד אחראי להגן על המוניטין, הנתונים והלקוחות של הארגון. במישור המדיני, עומדים על הפרק בטחון המדינה והבטיחות והרווחה של האזרחים.

מהי פרצת אבטחה?

ממבט עיני המפתח - ניתן להגדירה כפגם בעיצוב של מערכת, מימוש או פעולה, שאותו ניתן לנצל על מנת להפר את מדיניות האבטחה של המערכת.

ובאשר לצד המשתמש - כל מידע לגביך יכול להיחשב לנתונים שלך. מידע אישי זה יכול לזהות אותך באופן ייחודי כמי שאתה. נתונים אלה כוללים את התמונות וההודעות שאתה מחליף עם בני משפחה וחברים באינטרנט. פרטים אחרים, כגון שם, מספר ביטוח לאומי או תעודת זהות, תאריך ומקום לידה ושם הנעורים של אמך ידוע לך ומשמש לזיהוי שלך. פרטים כגון מידע רפואי, פרטי השכלה, נתונים פיננסיים ותעסוקתיים יכולים גם הם לזהות אותך באינטרנט.

התקני המחשוב שלך

בהמשך לתיאורייה שגורסת בכך שבעל המאה כיום הוא האדם השולט במידע של אנשים אחרים, למשל באינסטגרם יש מעל מיליארד משתמשים קבועים. נתון בסדר גודל פסיכי. כמה פסיכי? מדובר במידע שמוחזק אל צוקרברג, כאילו הוא שולט במידע כמו של כל אוכלוסיית כל אוכלוסיית דרום אמריקה יחד.

חייבים להבין - אם יש לך דברים בעלי ערך, פושעים רוצים אותם. והיום, התקני המחשוב שלך לא רק מאחסנים את הנתונים שלך. התקנים אלה הפכו לשער לנתונים שלך והם מייצרים מידע לגביך.

אם לא בחרת לקבל חשבונות בנק מודפסים, אתה משתמש בהתקני המחשוב שלך כדי לגשת לנתונים אלה. אם אתה מעוניין בעותק דיגיטלי של חשבון האשראי האחרון שלך, תשתמש

בהתקני המחשוב שלך כדי לגשת לאתר חברת האשראי. אם ברצונך לשלם את חשבון כרטיס האשראי שלך באינטרנט, תיגש לאתר האינטרנט של הבנק כדי להעביר כספים באמצעות התקני המחשוב שלך. מעבר לגישה למידע שלך, יכולים התקני המחשוב לייצר מידע לגביך.

כשכל המידע הזה לגביך זמין באינטרנט, הנתונים האישיים שלך נעשים רווחיים עבור האקרים.

בפרק הבא נדון בנושא אבטחת התקני מחשוב והגנה על התקני מחשוב - חומות אש ואבטחת סייבר.

הגנה על התקני מחשוב – חומות אש ואבטחת סייבר

לאחר שהבנו את חשיבות ההגנה על המחשב שלנו, על רשת האינטרנט שלנו או על הארגון בו אנו מאחסנים את המידע שלנו - נסביר בשיעור זה מושגים בסיסיים באבטחת סייבר וכיצד נוכל להילחם בתוקפים (מה שמוגדר 'לוחמת סייבר').

מהי חומת אש?

חומת אש היא חומה או מחיצה שנועדה למנוע מאש להתפשט מחלק אחד בבניין לחלקים אחרים. בתחום המחשבים, חומת אש מיועדת לבקר, או לסנן, את התקשורת המורשית להיכנס להתקן או לרשת או לצאת מהם, כמוצג באיור. ניתן להתקין את חומת האש במחשב יחיד כדי להגן על מחשב זה (חומת אש מבוססת מארח), או להתקין אותה בהתקן רשת עצמאי המגן על רשת מחשבים שלמה וכל ההתקנים המארחים באותה רשת (חומת אש מבוססת רשת).

המונח שאול מקיר עמיד לאש בבניין, שמטרתו לשמור על השריפה מחוץ למתחם המוגן.

חשוב לציין כי כיום אין התקן אבטחה אחד או טכנולוגיה אחת שיכולים לפתור את כל הצרכים של אבטחת הרשת. כיוון שיש מגוון של התקני אבטחה וכלי אבטחה שיש להטמיע, חשוב שהם יעבדו יחד. התקני אבטחה יעילים ביותר כשהם חלק ממערכת. התקני אבטחה יכולים להיות

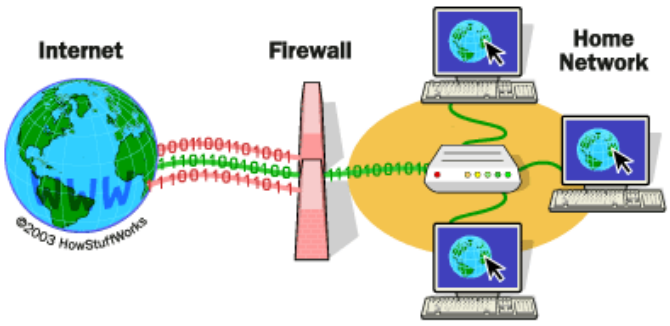
התקנים עצמאיים, ולא רק תוכנות המופעלות בהתקני הרשת כמו חומות אש. למשל, ישנם כלים מוחשיים של סיסקו כמו נתבים, IPS, VPN אשר ארגוניים חייבים להצטייד בהן. כלים אלו מוגדרים כנתבים והם מצפינים ומונעים חדירות לרשת. בקורס זה, נתעמק יותר בכלים חינמיים שאנו מכירים וחייבים להיות מותקנים בכלל המחשבים כמו אנטי-וירוס, חומות אש, התקני אבטחה הבאים בצורה אוטומטית ('האתר מאובטח https' או אבטחה על הדואר האלקטרוני שמגיע אוטומטית עם התוכנה עצמה).

כיצד פועלות חומות אש?

חומות האש הראשונות ביצעו בדיקות תנאי פשוטות ויצרו סינון (מה שהוגדר כ'מסננות פאקטות') תוך כדי השוואה בין רשימה מוגדרת של כללים לבין כניסות לא תקינות לרשת האינטרנט שיוכלו להיות מוגדרות כזדוניות. לאחר מכן, בדור השני, חומות האש הוסיפו פרמטר נוסף לסינון בשם 'מצב החיבור' והוא כלל טכנולוגיה שידעה לקבוע האם הפאקטה הייתה זו שהחלה את ההתחברות, הייתה חלק מהתחברות קיימת או שלא הייתה מעורבת כלל באותה ההתחברות. כיום, חומות האש מוגדרות כדור השלישי, והן בנויות כך שיכולות לסנן מידע מכל השכבות של מודל השכבות (מודל הOSI) שמיד נסביר עליו. באמצעות שימוש במידע זה, חומת האש יכלה לזהות התקפות המנסות להסתוות באמצעות שימוש בפורט מורשה או באמצעות ניצול לרעה של פרוטוקול לגיטימי.

מודל ה-OSI

מדובר במודל המציג את שבעת הפעולות השונות הנדרשות על-מנת להעביר נתונים ברשת תקשורת, ואת הסדר בין הפעולות השונות. התפקיד של כל שכבה הוא לטפל בנתונים שנוצרו על ידי השכבה הקודמת (והשכבות שלפניה), על מנת שיהיה ניתן להעביר אותו לצד השני של ההתקשרות. הטיפול בכל שכבה כולל ניתוח וסיווג הנתונים שהוסיפה השכבה הקודמת, והוספת נתונים טכניים חדשים, אשר יסייעו לשכבה הבאה להמשיך לטפל בהעברת הנתונים אל היעד. לאחר שהנתונים הגיעו לצד השני, יש צורך לפענח את התוספות של השכבות הקודמות על מנת להגיע חזרה למידע המקורי. על מנת ששני הצדדים יוכלו לתקשר ביניהם - הם עובדים בדרך כלל על פי פרוטוקול מוסכם. השכבות המכילות את המודל הן שכבת היישום, הייצוג, השיחה, התעבורה, הרשת, הקו והפיזית וכאמור לכל שכבה יש את המשמעות שלה בטיפול בנתונים שנוצרו על ידי השכבה הקודמת ועל מנת שיהיה אפשר להעביר אותו לצד השני של ההתקשרות. אנו נתעמק במדריך זה, בשכבת היישום המכילה את הפרוטוקולים של HTTPS, SMTP, FTP ועוד...



שכבת היישום

השכבה השביעית והעליונה של מודל ה-OSI והרביעית במודל TCP/IP.

היא ממונה על אספקת שירותי הרשת לתוכנות בהן משתמש משתמש הקצה. שכבת היישום משתמשת בשירותיה של שכבת הייצוג של מודל ה-OSI ואינה מספקת שירותים לאף שכבה אחרת במודל ה-OSI. שכבת היישום היא זו הקובעת את סוג התקשורת בין מחשבים. למשל, היא קובעת האם מדובר בתקשורת 'שרת–לקוח' (client-server) שבה מחשב אחד (השרת) מספק נתונים לאחר (הלקוח) - כמו בגלישה באינטרנט, או שמדובר בתקשורת 'קצה לקצה' (peer to peer), שבה כל אחד מהמחשבים הוא גם שרת וגם לקוח - כמו ברשתות שיתוף קבצים.

הפרוטוקולים הקיימים בשכבה זו הם HTTP, FTP, SSL, SMTP, POP3, TFTP, NFS, RSP. פרוטוקולים הכוונה היא לאופן בקשת וקבלת נתונים ברשת האינטרנט. בפרוטוקולים בשכבה זו יש גם שיטות דחיסה והצפנה גלומות בתוכן. המוכרת ביותר היא HTTP - שנועד להעברת דפי HTML ואובייקטים שהם מכילים (כמו תמונות, קובצי קול, סרטוני פלאש וכו') ברשת האינטרנט וברשתות אינטרנט. אנו מבינים שישנם פקודות שונות שרצות על גבי הפרוטוקולים של אתרי האינטרנט שלנו. פקודות כמו get (קבלת מידע מהשרת), post (שליחת מידע לשרת), connect (התחברות לשרת)... מה יקרה אם משהו בפקודות הללו לא ירוץ כשורה? אם גורם זדוני ינסה לאתר את הרשת בה אנו גולשים, את הIP הספציפי או את החברת תקשורת, וינסה

דרך הפרוטוקול להשתיל מידע כלשהו? מידע שלא רצינו בו וכאשר קיבלנו מידע, קיבלנו איתו גם וירוסים או הענקנו גישה בטעות לכלל המערכת שברשותינו... מכאן באה החשיבות הרבה לחומות אש, להגנה על פרוטוקולים, לנתבים, להצפנות ועוד...

תוכנת Packet Tracer

Packet Tracer היא תוכנת סימולציה הנועדה לתרגל בנייה וחקירה של רשתות בסביבה נוחה ויפה לעין.

באמצעות התוכנה, תיצרו את רשת המחשבים הראשונה שלכם, תוכלו לנסות להעביר מידע בין מחשבים, להגן עליהם ועוד... אם אין לכם חשבון באקדמיה של סיסקו - ליחצו על הקישור הבא בצעו רישום והיכנסו פנימה. במידה ומשהו לא עובד בתהליך ההרשמה, תוכלו לאתר את התוכנה ברחבי האינטרנט בצורה פרוצה.

יש ברחבי האינטרנט, מגוון רחב של מדריכים על תוכנה זו, פקודות שונות, מגוון רשתות מובנות ומוכנות מראש. במדריך זה, אלמד אתכם כיצד ניתן ליצור בעצמינו שני מחשבים, לקבוע להם IP, לחבר ביניהם או לחבר אותם לראוטר או לרשת תקשורת. דבר זה חשוב כצעד התחלתי בהיכרות עם הגנה על סביבת רשת התקשורת שלנו, בין אם בארגון ובין אם בבית.

אנא צפו בסרטון הקרוב, בוא אני מדגים כיצד ניתן לגרור שני מחשבים אל תוך הרשת שלנו, ללחוץ עליהם ולהגדיר אותם בIP אקראי שמעניק המחשב. לאחר שהגדרנו את הIP לכל מחשב, נגרור פנימה גם ראוטר המוגדר כhome router. כעת, נילחץ על הברק ויוצגו לפנינו

רצועת כבלים רבה. על מנת לא לסבך ולעשות חיים קלים יותר, אנא ליחצו תמיד על הברק, שהרי הוא תפקידו תמיד להגדיר את הכבל הרצוי והאידיאלי לסיטואציה אותה אנו מנסים לבצע.

נסו לגרור, בדומה לסרטון, את הברק בין המחשבים או בין כל מחשב לראוטר שהגדרתם.

נתקדם - נניח והמחשבים מדברים ביניהם (שוב, באמצעות כבל הברק) נרצה לראות זאת. נרצה לראות האם הכבל עובד והמחשבים אכן יכולים לשוחח זה עם זה.על מנת לבצע זאת, נזכור את הIP של מחשב אחד מבין השניים ונלחץ על המחשב השני. באותו מחשב שני, ניכנס לאיזור של command הנמצא תחת desktop כמו בסרטון.

ננסה להזין את הפקודה הבאה – `ping 126.17.33.1` כשמספרים אלו שכתבתי, אנא החליפו אותם במספרי הIP שזכרתם מראש של המחשב הראשון. האם ישנן שורות קוד שמופיעות על המסך? האם יש תקשורת בין המחשבים?

נסו לשנות את שם הIP הפעם תחת שורת הקריאה ping לאיזשהו IP שאינו קיים...הבחינו בכך שהפעם הוא מנסה לאתר ולחפש, אך ללא הצלחה...