זהירות - הנדסה חברתית

לאחר שהתברר שהנדסה חברתית היא "הבטן הרכה" של הגנת סייבר, הוקם באיחוד האירופי קונסורציום מחקרי, שנועד לפתח שיטות וכלי מיגון כנגד תקיפות המבוססות על הנדסה חברתית, בו שותפה גם התעשייה האווירית לצד חברות, אקדמיה ומשתמשי קצה. המטרה - למזער סיכוני סייבר שמקורם בהנדסה חברתית | ד"ר נתן וייס

1 ש הטוענים שהמקצוע העתיק ביותר בעולם הינו "הנדסה חברתית" - שכנוע אנשים לבצע פעולות שבמצב רגיל לא היו מבצעים. השכנוע יכול להיות למטרת שיווק, או לחילופין למטרת הונאה. כבר בסיפור המקראי של אדם וחוה אנו מוצאים דוגמה קלאסית להנדסה חברתית: "ויאמר האדם: האישה אשר נתתה עמדי, היא נתנה לי מן העץ ואוכל ... ותאמר האישה, הנחש השיאני ואכל".

לא מפתיע שמאז המצאת המחשב ורשתות תקשורת, הנדסה חברתית מהווה נדבך חשוב, ואפילו קריטי, בשרשרת תקיפת הסייבר. לדוגמא, כשתוקף רוצה לעקוף את חומות האבטחה הטכנולוגיים סביב מערכות מידע של ארגון מסויים, הוא ישכנע אחד מהעובדים בחברה "לפתוח לו דלת" לתוך המערכת, תוך ניצול "חולשות אנוש". על-פי הדיווחים, הנדסה חברתית שימשה כחוליה העיקרית בדילוג בין הרשת המנהלתית לרשת התפעולית, המנותקת מהאינטרנט, במתקפת Stuxnet.

בעבר, הנדסה חברתית במתקפת סייבר התבצעה בעיקר באמצעות פריסת רשת רחבה. היום, עולם המחשוב המודרני מאפשר עליית מדרגה בתחכום וביעילות של מתקפות. לדוגמא, בשיטת ה"פישינג" המסורתית, נשלח דוא"ל לקהל רחב בכוונה שחלק קטן ממקבלי הדוא"ל ילחצו על לינק מסוכן וכך יוזרק פוגען סייבר לתוך המחשב של הקורבן, ומשם יודבקו מחשבים ורכיבי מחשוב אחרים בתוך הארגון.

מהנדסים מתקפות באמצעות מידע אישי

בעשור האחרון השיטה השתנתה באופן מהותי, כאשר השינוי הדרמטי ביותר הוא הכמות הבלתי נתפסת של מידע הנמצאת בכל רמות התקשוב: בענן, ברשתות חברתיות, במחשבים האישיים של משתמשים, ובמחשבים ובשרתים של ארגונים. אם לתוקף יש גישה, אפילו חלקית, למידע על ארגונים ו/או אנשים שמעניינים אותו (למשל, מנהל תקשוב בבנק, קצין בכיר בצבא, שר בממשלה וכדומה), הוא יכול להשתמש במידע כדי ל"הנדס" מתקפה ממוקדת כנגד אישיות מסויימת.

השיטה הנפוצה ביותר הינה שיטת "פישינג ממוקד", "spear phishing" (האמור להזכיר את המונח "דייג חנית") באמצעות שימוש רחב במידע המופיע ברשתות החברתיות לצורך ביצוע התקיפה. בשיטה הזו, לדוגמה, תוקף שולח דוא"ל, מסרון, או הודעה ברשת חברתית, כגון פייסבוק או ווטסאפ, למנהל IT בחברה המציע אביזר חדש ליאכטה החדשה שקנה אותו מנהל לאחרונה, מסרון הכולל פרטים אישיים נוספים כך שהקורבן ירגיש שהמסרון אותנטי ורלוונטי. לכן הוא עלול להקליק על הלינק ו... הפוגען כבר בפנים.

עולם המחשוב המודרני גם מקנה לתוקף כלים להשיג את המידע שהוא צריך כדי לבצע את משימתו. מידע אישי ואינטימי על כל אחד מאיתנו נמצא ברשתות החברתיות, בענן, במחשבים האישיים שלנו, ובאפליקציות בהן אנחנו עושים שימוש. בנוסף, השימוש ההולך ומתרחב במוצרי IOT - אינטרנט של דברים - מוסיף ערוץ איכותי ביותר לאיסוף מידע בכמות ובאיכות שלא היה כמותה בעבר!

לא צריך להיות האקר מתוחכם כדי למצוא מידע איכותי על אנשים ברשת. מידע רב נמצא ברשתות החברתיות כגון פייסבוק וטוויטר. תחום ה OSINT - Open Source Intelligence - איסוף מידע ממקורות פתוחים, הינו תחום מפותח במיוחד וקיימים מוצרים, תוכנות ושיטות ידועות להשגת מידע ממקורות פתוחים, בין אם מחפשים מידע על אנשים מסוימים או, לחילופין מחפשים אנשים עם מאפיינים מסויימים (כגון עובדי חברה מסויימת).

בנוסף, קל עד כדי גיחוך, לייצר דמויות בדויות ברשתות החברתיות ולעשות בהן שימוש על מנת ליצור קשרים עם גורמי ענין. לראייה, מומחי הסייבר של התעשייה האווירית ערכו ניסוי מעניין לפני כשנתיים וחצי, במסגרתו הקימו דמות בדויה ברשת חברתית. הקמת הדמות ארכה פחות משבע דקות. מדובר היה בבחורה אנגליה, ילידת צרפת, אשר למדה בקולג' לאומניות ליד לונדון. בתוך 48 שעות, לדמות הבידיונית היו כבר 100 חברים, והיא ניהלה שיחות משמעותיות עם מגוון אנשים מסביבתה החברתית החדשה.

נדבך קריטי בפתרון הוליסטי

האיחוד האירופאי, בתוכנית מו"פ הדגל "הורייזון 2020", הצביע על נושא הנדסה חברתית בתחום הסייבר כנושא מחקר מרכזי, במטרה לפתח שיטות וכלי מיגון כנגד תקיפות המבוססות על הנדסה חברתית. התעשייה האווירית הינה חלק מקונסורציום של חברות, אקדמיה ומשתמשי קצה אשר זכה בפרויקט DOGANA. השם DOGANA הוא קיצור של: aDvanced sOcial enGineering And vulNerability Assesment framework - "הקמת מסגרת להערכת פגיעויות של הנדסה חברתית מתקדמת". זהו פרויקט הממומן במסגרת הורייזון 2020 שנועד לבצע מו"פ בנושא הנדסה חברתית בתחום הסייבר.

> פרויקט דוגנה משלב מומחי סייבר עם פסיכולוגים ומשפטנים וכולל ניסויים בשטח לבדיקת הכלים המפותחים. כלים אלה יהוו נדבך קריטי בפתרון הוליסטי עתידי לניהול סיכוני סייבר בארגון

בפרויקט דוגנה שותפים חברות, אקדמיה ומשתמשי קצה ממגוון מדינות כולל בלגיה, צרפת, פורטוגל, אנגליה, איטליה, אוסטריה, שוויץ, רומניה, יוון וישראל.

פרויקט דוגנה מפתח כלים וטכנולוגיות בשלושה כיוונים:

1. שרשרת כלים לביצוע הערכת פגיעות בארגון למתקפת סייבר המבוססת על הנדסה חברתית - SDVA (Socially Driven Vulnerability Assessment). הכלים המפותחים יהוו נדבך קריטי בפתרון הוליסטי עתידי לניהול סיכוני סייבר בארגון.

2. מסגרת חינוכית המבוססת על ניתוח פסיכולוגי במטרה למזער סיכוני סייבר שתחילתם בהנדסה חברתית.

3. פיתוח טכנולוגית ה-SDVA במסגרת חוקית ומוסרית על-פי הקריטריונים של האיחוד האירופאי.

פרויקט דוגנה משלב מומחי סייבר עם פסיכולוגים ומשפטנים וכולל ניסויים בשטח לבדיקת הכלים המפותחים.

אנו מצפים ששילוב תעשייה, אקדמיה ומשתמשי קצה ושילוב בין ההיבט הטכנולוגי, המשפטי והחינוכי, כמו גם השילוב עם ניסויי שדה וגישה מבוססת ניהול סיכוני סייבר בארגון, יובילו לפיתוח גישה חדשה ויעילה כדי להפחית נזק הנובע מהנדסה חברתית בתקיפות סייבר.

הכותב הינו מדען בכיר במינהל מערכות סייבר של התעשייה האווירית