מאמר דעה

המגן עלול להפוך לתוקף

מאת: יוסי שביט, MBA, CISO, CISM, CDPSE, CC, ממחה לאבטחת מידע וסייבר במערכות בקרה תעשייתיות (ICS)

מבוא

תגובה לאירועי אבטחת סייבר בסביבות IT מסורתיות בנויה בדרך כלל סביב מטרה ברורה: לזהות את האיום, לבלום אותו, למגר אותו ולשקם את הפעילות הרגילה. פעולות כגון ניתוק מחשב פרוץ, חסימת תקשורת זדונית, השבתת חשבון או סגירת תהליך חשוד נחשבות לעתים קרובות לאמצעי הגנה סטנדרטיים.

בסביבות טכנולוגיה תפעולית (OT), לעומת זאת, המצב **שונה באופן מהותי**.

רשת OT אינה קיימת רק כדי לעבד מידע. היא שולטת ומנטרת תהליכים פיזיים. מאחורי כל בקר PLC, שרת SCADA, HMI, תחנת עבודה הנדסית, חיישן וקישור תקשורת עשויים להיות משאבות, מנועים, שסתומים, תנורי חימום, מדחסים, תהליכים כימיים וציוד פיזי אחר.

כתוצאה מכך, תגובת אבטחת סייבר שהיא נכונה מבחינה טכנית מנקודת מבט של IT עלולה ליצור תוצאה בלתי צפויה ומסוכנת בסביבה **הפיזית**.

זה מוביל לעיקרון קריטי:

ב-OT, אסור שעצירת איום הסייבר תיצור איום תפעולי או בטיחותי גדול יותר.

לכן, האתגר אינו רק לעצור את התוקף, אלא לעצור אותו מבלי לשבש את היציבות של התהליך המוגן.

1. ההבדל המהותי בין IT ל-OT

ההבדל העיקרי בין IT ל-OT אינו הטכנולוגיה עצמה, אלא ההשלכות של כשל.

בסביבת IT, כיבוי שרת פרוץ עלול לגרום לאובדן שירות, גישה לנתונים או יעילות. בסביבת OT, כיבוי בקר פרוץ עלול להשפיע על התהליך הפיזי עצמו.

לדוגמה, ניקח בקר PLC השולט במערכת שאיבה. אנליסט SOC מזהה תקשורת חריגה ומחליט לבודד את הבקר PLC מהרשת.

מנקודת מבט של אבטחת סייבר, הפעולה עשויה להיראות מוצלחת.

אך מיד עולות מספר שאלות:

- האם הבקר PLC ימשיך לשלוט בתהליך?
- מה יקרה אם הוא יאבד את התקשורת עם ה-HMI?
- האם המערכת תיכנס למצב בטוח?
- האם משאבות או שסתומים יישארו במיקומם הנוכחי?
- האם קיימת אפשרות גיבוי של הפעלה ידנית למערכת?
- האם ההפרעה עלולה ליצור מצב מסוכן? ייתכן שצוות אבטחת הסייבר הכיל את האיום הדיגיטלי ובמקביל יצר איום תפעולי.

ייתכן שצוות אבטחת הסייבר נטרל את האיום הדיגיטלי אך במקביל יצר איום תפעולי.



מאמר דעה

2. מאירוע סייבר להשלכות פיזיות

ב-OT, שרשרת ההשלכות עשויה להיראות כך:

מתקפת סייבר ← שינוי דיגיטלי ← תגובת מערכת בקרה ← שינוי בתהליך פיזי ← השפעה תפעולית/בטיחותית

התוקף אינו בהכרח זקוק לגישה פיזית ישירה לציוד. מניפולציות עם ערכים מוגדרים, שינוי לא מורשה של לוגיקת PLC או שיבוש תקשורת עשויים להספיק כדי ליזום שינוי פיזי. אותו עיקרון חל על פעולות הגנה.

מגיב עשוי לבצע:

זוהה אירוע ← בידוד רשת ← אובדן תקשורת ← אובדן שליטה/נראות ← אי יציבות בתהליך טכנולוגי

משמעות הדבר היא שגם פעולות זדוניות וגם פעולות הגנה יכולות להשפיע על התהליך הפיזי.

כתוצאה מכך, תגובת אירועי OT חייבת להעריך לא רק את ההשפעה של פעולה על אבטחת הסייבר, אלא גם את ההשלכות התפעוליות והפיזיות שלה.

3. שיטת "רדיוס התגובה"

אבטחת סייבר מסורתית מעריכה לעתים קרובות התקפה לפי **רדיוס התגובה** שלה: כמה מערכות יכולות להיות מושפעות ועד כמה התוקף יכול להתפשט.

ארגוני OT צריכים ליישם את אותה חשיבה בפעולות הגנתיות.

רדיוס התגובה

ניתן להגדיר את רדיוס התגובה כך:

ההשפעה התפעולית, הפיזית, הבטיחותית והסביבתית הפוטנציאלית הנובעת מפעולת תגובה של אבטחת סייבר.

לדוגמה: חסימת תעבורת רשת עלולה לגרום לאובדן תקשורת בין מערכות הבקרה, ניתוק HMI עלול לגרום לאובדן נראות המפעיל, אתחול מחדש של שרת SCADA עלול לגרום לאובדן פונקציות פיקוח או התרעה, ניתוק תחנת עבודה הנדסית עלול לגרום לאובדן יכולת הנדסית, עצירת PLC עלולה לגרום לאובדן שליטה על ציוד פיזי והשבתת גישה מרחוק עלולה לגרום לאובדן יכולות חירום או תחזוקה. לכן, פעולות אלו עלולות לפגוע בתהליך הפיזי במקום לעצור את התוקף.

4. השכבה החסרה בתגובה לאירועי OT

תגובה מסורתית לאירועי סייבר מתמקדת לעתים קרובות בשלוש שאלות:

מה קרה, איזה נכס נפגע וכיצד ניתן לטפל בזה?

תגובה לאירועי OT דורשת שכבה נוספת של ניתוח:

איזה תהליך פיזי נשלט על ידי משאב זה, אילו מערכות תלויות בו, מה יקרה אם התקשורת תופסק, מהו מצב הפעולה הבטוח המוגדר, האם התהליך יכול להימשך בבטחה ללא משאב זה, האם התגובה עצמה יכולה ליצור אירוע בטיחותי או סביבתי?

שכבה נוספת זו חיונית מכיוון שאותו משאב יכול להיות בעל משמעות שונה מאוד בהתאם לתפקידו בתהליך הפיזי.

תחנת עבודה המכילה מידע רגיש עשויה להיות חשובה מנקודת מבט של IT.

תחנת עבודה המשמשת לתחזוקת מערכת בקרה קריטית עשויה להיות חשובה מסיבה שונה לחלוטין.



מאמר דעה

5. מדוע ה-SOC לא יכול לעבוד לבד

אחד הלקחים החשובים ביותר מאבטחת סייבר ב-OT הוא שאף צוות יחיד אינו מחזיק בתמונה המלאה.
ה-SOC מבין את איום הסייבר.
מהנדס ה-OT מבין את ארכיטקטורת הבקרה.
מהנדס התהליך מבין את תהליך הייצור.
צוות הבטיחות מבין השלכות מסוכנות.
צוות התפעול מבין מה ניתן ומה לא ניתן לשנות במהלך ייצור חי.
לכן, תגובה יעילה לאירועי OT דורשת שיתוף פעולה בין דיסציפלינות אלו.
באופן אידיאלי, החלטת תגובה צריכה לשקול שלוש שאלות בו זמנית:

- פרספקטיבת סייבר: מה התוקף עושה?
- פרספקטיבה תפעולית: מה קורה לתהליך?
- פרספקטיבה בטיחותית: מה יכול לקרות לאנשים, לציוד או לסביבה?

ההחלטה הנכונה נובעת מהסיכון המשולב, לא מנקודת מבט של אבטחת סייבר בלבד.

6. מהירות חשובה - אך לא בכל מחיר

יש נטייה טבעית באבטחת סייבר להאמין ש**תגובה מהירה יותר היא תמיד תגובה טובה יותר**.
ב-OT, הנחה זו יכולה להיות מסוכנת.
ישנם תהליכים תעשייתיים המגיבים באופן מיידי לשינויים. לאחרים יש עיכובים משמעותיים בין פקודה דיגיטלית לבין השלכותיה הפיזיות.
ביצוע פקודה עשוי להימשך אלפיות שנייה, בעוד שההשלכות עשויות להיות גלויות מספר שניות או אפילו דקות לאחר מכן. שסתום עשוי להיסגר, לחץ עשוי לעלות, משאבה עשויה לעצור, טמפרטורה עשויה לעלות, קו ייצור עשוי להפוך לבלתי יציב.
היעדר השלכה מיידית נראית לעין אינו בהכרח אומר שפעולת התגובה הייתה בטוחה.
לכן, יש לאזן את מהירות התגובה עם מודעות לתהליך.

7. משימה חדשה עבור מגן ה-OT

אין להגדיר את מטרת אבטחת הסייבר של OTאך ורק כהגנה על:
CIA (סודיות, שלמות, זמינות)
אלה נותרים חשובים, אך סביבות OTדורשות פרספקטיבה רחבה יותר שלוקחת בחשבון גם: **SRP**(בטיחות, אמינות, יעילות) והגנת הסביבה.
לכן, למגן יש שתי משימות בו זמנית:

- לעצור את התוקף.
- להגן על התהליך הפיזי.

ברוב המקרים, מטרות אלו תומכות זו בזו. אך כאשר הן מתנגשות, על הארגון להבין איזו פעולה מייצרת את הסיכון הכולל הנמוך ביותר.



מאמר דעה

מסקנות

הטעות הגדולה ביותר שארגון יכול לעשות בתחום אבטחת הסייבר של OT היא להניח שתגובת סייבר נכונה מבחינה טכנית היא אוטומטית תגובה מבצעית בטוחה.
בסביבה תעשייתית, לכל פעולה דיגיטלית עשויה להיות השלכה פיזית.
ניתוק מערכת שנפרצה עשוי להגן על הרשת, אך במקביל לשבש תהליכי בקרה.
חסימת תקשורת עשויה לעצור תוקף, אך גם למנוע מהמפעיל לקבל תמונת מצב.

ולכן: **המגן עלול להפוך לתוקף.**



יוסי שביט,
MBA, CISO, CISM, CDPSE, CC
מומחה לאבטחת מידע וסייבר
במערכות בקרה תעשייתיות (ICS)