Process Safety Beacon
Messages for Manufacturing Personnel
www.aiche.org/ccps/process-safety-beacon

יולי 2021

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

אבטחת סייבר ותפעול מתקנים כימיים

תמונה 1: אולדסמר, מתקן טיפול במים בפלורידה.

ב-5 בפברואר 2021 הבחין עובד במתקן לטיפול במים באולדסמר, פלורידה, כי הסמן נע באופן מוזר על מסך מחשב הבקרה, בתחילה לא היה חשש; המפעל השתמש בתוכנת גישה מרחוק כדי לאפשר לצוות לשתף מסכים ולפתור בעיות IT. המפקח התחבר לעיתים קרובות למחשב המפעיל כדי לפקח גם על מערכות המתקן. כעבור כמה שעות הבחין המפעיל בסמן נע ולוחץ על מערכת בקרת מכון הטיפול במים. תוך שניות, הפורץ ניסה לשנות את ריכוז הנתרן הידרוקסיד במערכת מ -100 חלקים למיליון (ppm) ל-11,100 חלקים למיליון. המפעיל הבחין במהירות בחדירה והחזיר את ריכוז הנתרן הידרוקסיד לרמות נורמליות. למרבה המזל, לא הייתה שום השפעה על איכות המים.

מתקפת כופר על צינור חברת "קולוניאל פייפלייין" סגרה לאחרונה את אספקת הבנזין לחוף המזרחי של ארה"ב למספר ימים.

מערכות החברה שלך כנראה מחוברות לאינטרנט וזקוקות להגנה מפני איומי סייבר. ישנן אסטרטגיות רבות בהן משתמשות חברות כדי להרתיע איומי סייבר כגון: חומות אש, תוכנות אנטי-וירוס ומדיניות להגנה מפני תוכנות זדוניות ווירוסים במחשב.

יותר אנשים עובדים מרחוק; זה מגדיל את האפשרות להתקפות סייבר.

הידעת?

- פושעי סייבר משתמשים בתוכנות זדוניות מתוחכמות כדי לנצל מספר רב של נקודות תורפה ולהגשים את יעדיהם.
- מתקפות כופר הולכות וגוברות כאשר עבריינים מאורגנים משתמשים בהן ככלי לייצור כסף.
- על פי מחקר שנערך לאחרונה, מתקפת סייבר מתרחשת כל 39 שניות.
- פישינג שולח מיילים, כביכול של חברות מכובדות, כדי לגרום לאנשים לחשוף מידע אישי. התקפות אלה הן שיטת כניסה ראשית של תוכנות זדוניות. איומי סייבר יכולים להיכנס למערכות החברה באמצעות מיילים, קבצים מצורפים וממכשירי אחסון ניידים, כמו כונני דיסק און קי או התקני אחסון ניידים אחרים.
- תשעים וחמישה אחוז מהפרות אבטחת הסייבר נגרמות על ידי טעות אנוש.

מה אפשר לעשות?

- בדוק תמיד בקשות לעדכון תוכנה עם ה-IT לפני ביצוע ההתקנה והתקן עדכונים מאושרים במועד.
- ודא שחומות האש ותוכנות הרשת האחרות שלך מעודכנות ומופעלות.
- הקפד לגבות את המערכות והנתונים שלך באופן קבוע.
- השתמש בסיסמאות חזקות לכל גישה. אל תשתף סיסמאות או חשבונות ותשנה סיסמאות באופן קבוע.
- אל תשמור סיסמאות בדפדפנים.
- אל תלחץ על קישורים או קבצים מצורפים במיילים שנשלחו ממישהו שאתה לא מכיר.
- לעולם אל תתקין תוכנה לא מאושרת בשום מחשב של החברה; ודא שמפתחות הגישה והתקני אבטחה פיזיים אחרים מאובטחים כראוי.
- אם אתה משתמש בגישה מרחוק, פעל על-פי דרישות החברה. היה ערני במיוחד אם אתה משתמש באתרי אינטרנט ציבוריים.
- אם משהו במחשב שלך נראה מוזר או שונה, בקש עזרה! זה יכול להיות האקר שמנסה להשיג גישה.

התקפות סייבר הן אמיתיות. היו אתם חלק חיוני מהאבטחה.

©AIChE 2021. All rights reserved. Reproduction for non-commercial, educational purposes is encouraged. However, reproduction for any commercial purpose without express written consent of AIChE is strictly prohibited. Contact us at ccps_beacon@aiche.org or 646-495-1371.