



בינת יישום מערכות

הגנה על מערכות הביטחון
בפני איומי סייבר

בימים אלה הפכו מערכות תפעול ובטחון ליעד תקיפות סייבר והן החזית החדשה

תקיפות סייבר מוגדרות "טרור" המנצל חולשות אבטחה בכוונת זדון לגרום:

- נזקים ביטחוניים
- סיכון חיי אדם ונזקים בריאותיים
- השבתת המשכיות עסקית
- פגיעה במידע ושיבוש נתונים
- נזקים כלכליים
- נזקים תדמיתיים ועוד



ישראל היום

פרטיות ואבטחה

טכנולוגיה ומדע

חשש: פרטים אישיים של עובדי התאגיד דלפו

נבדק החשד שהפרטים נגנבו במתקפת סייבר על שרת באתר התאגיד • עם היוודע המתקפה, המערכות שנפרצו כובו ונותקו • לא נגרם נזק לעבודה השוטפת

יוני בן שושן //
פורסם ב: 24.12.2020 17:30 | עודכן ב: 25.12.2020 10:32 9 /



לפי גורמים בתאגיד, נבדק החשד כי התרחשה פריצה למערכת בקרת הכניסות של גוף השידור הישראלי, שבשנה האחרונה נמצאת בשלבי הסיום של הקמתה על ידי חברה חיצונית.

חדשות | מדיני ביטחון

דיווח: מתקפת הסייבר האיראנית נועדה להעלות את רמת הכלור במים בישראל

לפי העיתון פייננשל טיימס, אם התקיפה היתה יוצאת לפועל היא היתה גורמת למאות ישראלים לחלות ולנתיק עשרות אלפי בתים ממים. בחודש שעבר פורסם שישיראל ביצעה בתגובה מתקפת סייבר על נמל באיראן

24 שיתוף קריאת 1 שיתוף

✉️ 📧 📧

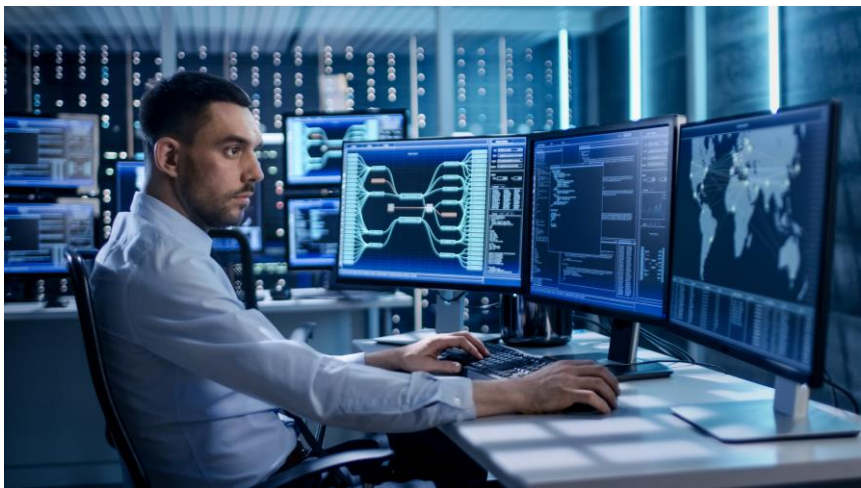
איראן ניסתה להעלות את רמת הכלור במי השתייה בישראל באמצעות מתקפת סייבר בחודש אפריל - כך פורסם אתמול (ראשון) בעיתון פייננשל טיימס. לפי הדיווח, התקיפה ביצעה באמצעות קוד איראני שעבר בין שרתי מחשב אמריקאיים ואירופיים כדי להקשות על זיהוי מקורו.



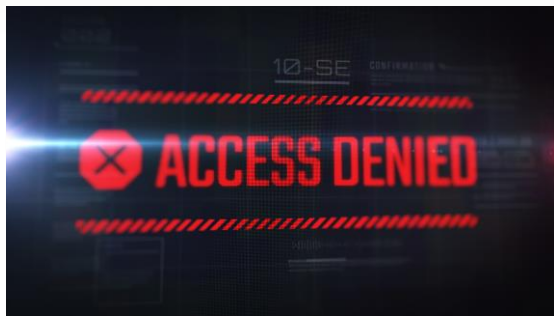
פורסם ב: 01.06.2020

בית יישום מערכות

- התחזות למורשה כניסה עם הרשאות. לדוגמה: זהות מזויפת של טכנאי מחשבים עם הרשאות כניסה למקומות רגישים.
- שיבוש הרשאות לפתיחת דלתות - חסימת הרשאות לפתיחת דלתות.
- השבתת אמצעי פריצה ושיבוש נתונים בבקרים כחלק מתוכנית חדירה.
- השבתת רציפות עסקית על ידי שיבוש נתונים ויצירת נזק לחיי אדם. לדוגמה: ניסיון מדינת אויב לשנות את מינון הכלור במי שתייה של תושבי מדינת ישראל.



- מערכת שו"ב (שליטה ובקרה)
- מערכת בקרת כניסה
- מערכת LPR
- מערכת גילוי פריצה
- מערכת טמ"ס (טלוויזיה במעגל סגור)
- מאגרי הקלטות וידאו
- מצלמות קבועות ומתנייעות (PTZ)
- מערכות כריזה
- מערכת גדר אינדוקטיבית
- מערכות רדאר לגילוי חדירות



- זיהוי וחסמת איומים חדשים
- מניעת התקפות DoS (Denial of Service)
- זיהוי והתראה על האיש שבאמצע (Man-In-The-Middle)
- חסימת תקשורת עם IP לא מורשה
- חסימת פרוטוקולים לא מורשים
- עצירת התקפות סיסמה מסוג Brute Force
- סריקת יציאות Port והשבתת יציאות עם חריגות חשודות
- זיהוי הגדרה או שינוי כתובות MAC
- זיהוי הגדרה או שינוי כתובת IP
- סריקת אלמנטים לא מקוונים
- זיהוי והתראה על תעבורה חשודה להתקן
- זיהוי והתראה על מעבר נתונים בכמות חריגה להתקן
- זיהוי חיבור התקן חיצוני לא מאושר כגון USB
- זיהוי והתראה על פעילות חריגה בנקודות קצה

- הגנה על מערכות בטחון בארגון ← יש לבסס על מפת האיומים
- הגנה טובה ניתן להשיג באמצעות ← מיפוי נכסים ורכיבים קריטיים
- בחינה מחודשת של הארכיטקטורה ← לגילוי נקודות תורפה
- שימוש בפרוטוקול OSDP מוצפן ← למימוש במקומות מאוימים
- הגבלת השימוש ב-NFC ו-BT ← בטלפונים חכמים והתקנים מתקדמים
- מעבר ל"תגים חכמים" ← והתאמת קוראי התגים לטכנולוגיה
- הטמעת כלי ייעודי להגנת סייבר ← כדוגמת Vanguard

November

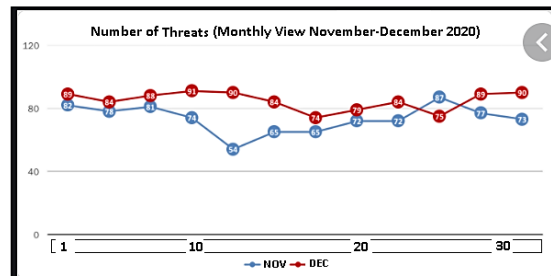
2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

December

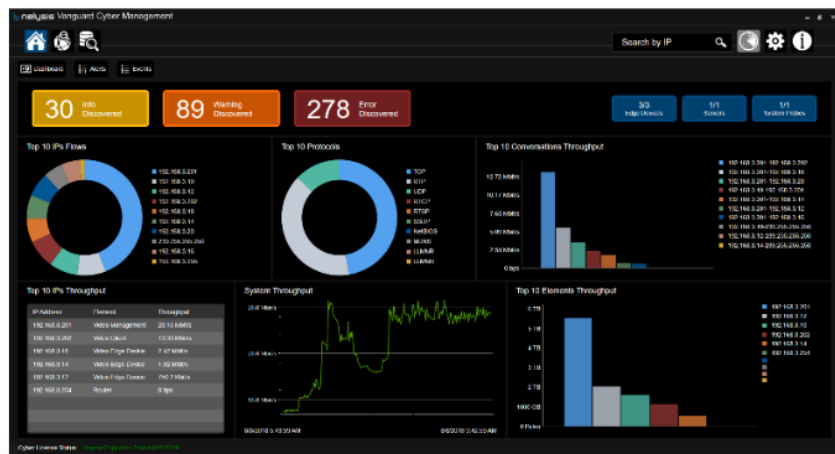
2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			



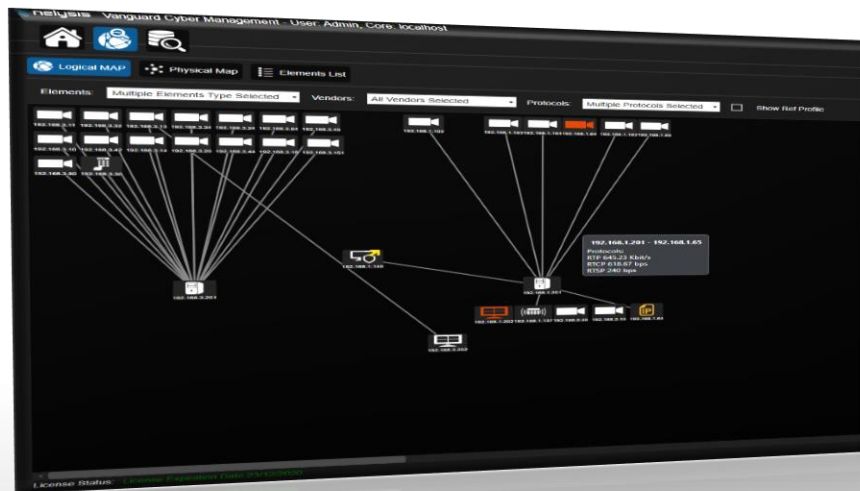
- בינה מלאכותית (AI) - בהגנת סייבר יש להטמיע תוכנה עם יכולות AI במטרה "ללמוד" תהליכים בארגון.
- זיהוי סממני תקיפה או חשיפת פרצות מתבסס על השוואה וזיהוי חריגות אנומליה בין "שגרה" שנלמדה ע"י AI לבין מדדי הנתונים שנאספים בזמן אמת ברמת הרכיב הפיזי הבודד.

בהגנת סייבר יש להטמיע תוכנת AI במטרה "ללמוד" תהליכים. המערכת לומדת אוטומטית את כל הרכיבים ברשת ומגבשת פרופיל פעילות "בשגרה". כל חריגה מהשגרה תציג בדשבורד התראה עם:



- שם יצרן
- מערכת הפעלה
- גרסת קושחה (Firmware)
- פרוטוקולים בשימוש
- רוחב פס
- מספרי תהליכים (Process #)
- כתובות IP כולל MAC Address
- מספר Port
- זיהוי מתג תקשורת מקושר

למערכת יכולת מיפוי וסיווג של כל נכסי הרשת, עם מחולל מפות טופולוגיה לוגיות ופיזיות להצלבת מדדים ואימות סיכונים, זיהוי חדירה פיזית, Man In The Middle, שינויים ברשת, פרוטוקולים לא מורשים, התקפת סיסמאות, Brute Force, גלישה אסורה באינטרנט ואיומים נוספים.





- נועל ערוצי USB בשרתים ותחנות
- מאפשר קישור של התקני USB מוכרים בלבד
- מתריע על הכנסת USB שאינו מוכר/מאושר
- נתמך על ידי מערכת הניהול
- מאפשר הפצת מידע מוצפן להתקן ה-USB



- המערכת מופרדת מהרשת כך שאינה משפיעה ואינה מושפעת מהאירועים.
- מיקוד הגנה על מערכות הביטחון והבקרה ושמירה על פעילות תקינה ורצופה.
- ניתוח שוטף של התעבורה והקשרים בין הרכיבים השונים, כך שההגנה היא על כל מרכיבי מערכת הבטחון והבקרה.
- התראה ויזואלית בכל מקרה של חריגה מהתנהגות תקינה.
- מערכת ניהול גרפית וידידותית למשתמש.

לפרטים נוספים על המערכת ממומחי הבטחון של בינת יישום מערכות
לחצו כאן והשאירו פרטים <<





בינת יישום מערכות

תודה!