

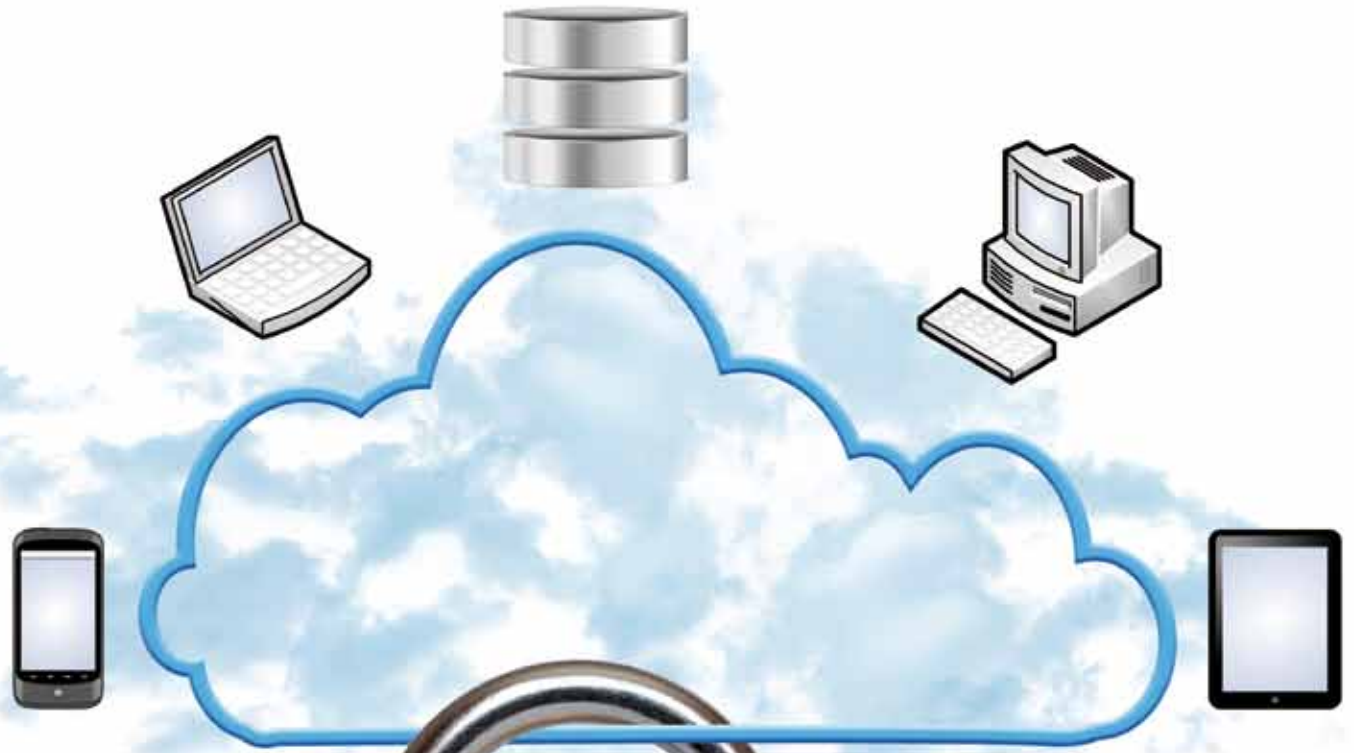
Digital Safety

מוסף טכנולוגיות סייבר לקוראי כלכליסט, מרץ 2020

איך מנקים את הקבצים שמגיעים
לארגון מווירוסים ונוזקות - מבלי
לפגוע בעבודה השוטפת?

המודל החדש של הסייבר
סקיוריטי: במקום לעצור מתקפות
- מונעים אותן מראש

כיצד מפתחים
פתרונות אבטחת מידע
עבור תעשיית הרכב?




**המעבר לעבודה בענן
חושף את הארגון שלכם לאתגרי
אבטחת מידע חדשים -
וברדור מסבירים איך להתמודד
איתם (עמ' 4)**

**תשבץ היגיון
סייבר לעובדים
מהבית!**

כלכליסט

המחלקה המסחרית
תוכן שיווקי

ניהול והפקה:
 חברת פפריקה www.paprikapro.com

 עורכת: חוה טרטנר
 עיצוב: נעה כהן
 מנהלת הפקה: ענבל פלג 052-3232130
 מכירות: טל גודלי-חתוכה 054-5853013
 זכויות היוצרים על התצלומים
 המופיעים בעיתון שייכות למפרסמים
 ולאתר depositphotos.com
 גילוי נאות:
 המוסף הינו בהפקת חברת פפריקה הפקות
 בע"מ בשיתוף עם המחלקה המסחרית
 של כלכליסט. מערכת עיתון כלכליסט ו/או
 חברת פפריקה אינן אחראיות לתוכן המודעות
 וכן מבקשות להבהיר כי המוסף הינו פרסומי
 ואין לראות במאמרים ו/או במודעות משום
 המלצה מכל סוג שהוא.

כלכליסט
 המחלקה המסחרית
 תוכן שיווקי

11 / ענן מתגלגל: ב-Cymotive מלמדים את תעשיית הרכב איך להיזהר גם בעידן הענן

12 / רגישות גבוהה: הפתרון של Ericom מאפשר גלישה נוחה באינטרנט - גם לארגונים פיננסיים וביטחוניים

13 / המפתח לפטנטים חזקים עבור חברות בכלל וחברות סייבר בפרט

14 / ישראל - הראשונה בעולם שמטילה רגולציית סייבר על מפעלי חומרים מסוכנים

14 / המדינה תקים בבאר שבע מרחב סייבר לניסויים בתחבורה חכמה

15 / תשבץ היגיון בנושא סייבר

03 / גם בימי שגרה: סקורנט מקבוצת אמן מציעה את פתרון ה-Privileged Security Access של חברת סייברארק

03 / COVID 19 מגדיר מחדש את דיני הפרטיות

04 / ברדור שומרים על המידע שלכם בסביבת הענן - בלי להאט את קצב הפיתוח

07 / עומדת בשער: Odix מנקה את הקבצים הארגוניים - ומונעת כניסה של נוזקות פנימה

08 / קרוב ל-100% הצלחה: האלגוריתם של דיפ אינסטינקט יודע לזהות גם איומים חדשים

10 / השטח האסור: מוצרי Quest מנהלים הרשאות בחוכמה - ומזהים מיד כל חריגה

ענן טריפל סי קיבל הכרה בתור VMware Cloud Verified הענן הראשון בישראל!

הענן של טריפל סי נבחר מתוך 4,000 שותפים עולמיים ביותר מ-120 מדינות, בתור ענן המציע שירותים מבוססים טכנולוגיית VMware.

ענן טריפל סי - הענן של ישראל!

vmware
 CLOUD
 VERIFIED



Triple C
 הענן של ישראל

CCC.CO.IL | *6440

מערכת ניהול סיסמאות - החיבור למערכות הליבה של הארגון מתאפשר באמצעות ניהול סיסמאות: פתרון זה מעניק למשתמש גישה למערכות הרלוונטיות, בלי שידע את שם המשתמש והסיסמא. בנוסף, הסיסמא למערכות אלו מתחלפת באופן אוטומטי בתדירות שנקבעת מראש. כך מונעים חשיפה או שימוש לרעה בהרשאות בעלות רגישות גבוהה.

הקלטת שנים - כל הסשנים מוקלטים, לצורך ביצוע בקרה, ניתוח מקרים חשודים והגעה למקור הסכנה במידת הצורך.

באופן זה, מספק פתרון ה-PAS של סייברארק מענה מלא לצרכי הארגון בעיצומו של משבר הקורונה וגם הרבה אחריו, לצורך מתן גישה מרחוק לעובדים ולספקים.

ניטור בזמן אמת - פתרון ה-PAS של סייברארק כולל מודול המנטר בזמן אמת התנהגות חשודה, באמצעות אנליזה ולמידת מכונה. אם המשתמש הריץ למשל פקודות חשודות, מנהל המערכת יקבל מיד הודעה עם פרטי המשתמש, כתובת ה-IP שלו והפקודה החשודה. בנוסף, אפשר לנהל את הסשן ואף לסגור אותו בצורה אוטומטית.

Securenet מקבוצת Aman היא אינטגרטור מוביל ובעל ניסיון רב שנים בהטמעת פתרונות סייברארק.

לפרטים נוספים:
www.aman.co.il

בצל הקורונה: הפתרון לעבודה מהבית בצורה מאובטחת

יותר ויותר ארגונים מאפשרים עבודה מהבית כדי להגן על העובדים מהידבקות בקורונה - אך מה בנוגע להדבקה ופגיעה במערכות הליבה בארגון? כך תסגרו את פרצות האבטחה הנגרמות בעקבות עבודה מהבית

מתן גישה ישירה מרחוק למערכות הליבה של הארגון חושף אותו לשתי פרצות אבטחה קריטיות: האפשרות של שימוש לרעה בפרטי התחברות למערכות הליבה, וסכנה להדבקה מערכות הליבה בווירוסים ונוזקות שאליהם חשוף המחשב האישי.

עבודה מהבית בצורה מאובטחת: איך זה מתאפשר?

סקיורנט מקבוצת אמן מציעה את פתרון ה-Privileged Access Security של חברת סייברארק, המספק מספר שכבות אבטחה:

גישה מאובטחת למשאבי הארגון - החיבור למערכות החברה מתבצע בשיטת Reserve Proxy, שרת החוצץ בין המחשב האישי של העובד מהבית לבין מערכות הארגון ומספק שכבת הגנה המונעת הדבקה של מערכות הארגון.

בימים האחרונים, יותר ויותר ארגונים עוברים לעבודה מהבית לתקופה לא ידועה - לאור העלייה התלולה במספר הישראלים הנמצאים בבידוד והרצון להימנע מהדבקות נוספות. לעבודה מהבית אמנם יש יתרונות רבים, אך בהיעדר כלים מתאימים, האמצעי שמסייע למניעת הידבקות בנגיף עלול להוביל להדבקה מערכות הליבה של הארגון בווירוסים, תוכנות זדוניות ושאר מזיקים.

גישה מרחוק לעובדים: מהן הסכנות המרכזיות?

ארגונים רבים מעניקים גישה מרחוק לעובדים באמצעות טכנולוגיית ה-VPN, שאמורה לספק חיבור מאובטח למערכות הארגון. ואולם, חיבור תחנת עבודה של עובד מהבית למערכות הארגוניות חושף אותן לאיומים מבחוץ. הבעיה רק מחריפה כשהעבודה מהבית כרוכה במתן גישה למערכות פנים-ארגוניות, כדוגמת שרתי Exchange, מערכות לניהול בסיסי נתונים, שרתי קבצים ועוד.

COVID 19 מגדיר מחדש את דיני הפרטיות / עו"ד דן חי ו-רועי סננס

גוברת. הצלחנו ללמוד את אופי הנגיף, וכשלמדנו כיצד הוא מידבק - הבנו כי אנו אלה שצריכים לשנות את התנהגותנו. במדינות בהן סטנדרט הפרטיות שונה מאשר במדינות המערב, לא בחלו באמצעים והחלו בניטור התנהגות תוך מעקב אחר תנועות במרחב - הכל כדי לעצור את התפשטות הנגיף. שימוש במידע לשם עצירת נגיף נראית כמטרה נעלה, אך במדינות בהן אין משטר דמוקרטי, החשש הוא מפני המטחח והשימושים הנעלמים מן העין. בישראל הותקנו תקנות החירום המאפשרות מעקב. התקנתן נעשתה באישון ליל ובמה שמרגיש כמחטף. התקנות רחבות ומקנות סמכויות שאינן ברוחות למשרד הבריאות - גוף שיכולתו הטכנולוגית לשמור על מידע בעל ערך כה רב, מוטלת בספק. הגוף המבצע הוא השב"כ. הרסן שוחרר. מעטה הפרטיות שהיה קיים נרמס במעטה של צו חירום, ללא כל פיקוח שמתחייב בפעילות שכזו. התחושה היא, שאם היו פועלים לחקיקה עדכנית ומותאמת בארץ, לא היה צריך את תקנות שעת החירום. חקיקה כזו הייתה נוקטת בכיוון שונה, תוך קביעת כללי התנהגות במידע בשעות חירום, כללים סדורים המאפשרים שימוש מידתי ותחת פיקוח. לא רק השב"כ היה שם, אלא גם הרשות להגנת הפרטיות. כך נוהגת דמוקרטיה.

באיכות משרד עו"ד חי ושות'



עו"ד רועי סננס



עו"ד דן חי

עליהן ולמידה של חוויות אישיות, עד לשיפור התרופה והתאמתה האישית לאדם מסוים. עם התפרצות מגפת ה-COVID-19, הקורונה, נוכחנו לדעת עד כמה אנו תלויים במידע. התלות תמיד הייתה שם אך גברה בהדרגתיות. בעזרת הכלים המתאימים והטכנולוגיה המתקדמת גם הפיריון עולה, אז התלות

הזכות לפרטיות בעלת שורשים עתיקים, אך כמו זכויות אחרות - מוגדרת מחדש עם כל אירוע משמעותי באנושות. לפני זמן לא רב, תקנות הגנת המידע האירופיות, ה-GDPR, הציבו רף חדש בכל הנוגע לזכויות במידע האישי. רוח זו נשבה מעבר לים, ותקנות דומות הותקנו גם בקליפורניה. עתה כבר הוגדר רף בינלאומי, אשר שורשיו יחדרו לכל פינה מערבית בגלובוס. התקנות השונות נושאות אופי אקס-טריטוריאלי, הן חוצות יבשות - בדיוק כפי שמידע חוצה יבשות. לכן, ברף זה גם ישראל צריכה לעמוד, שכן נמצאת בבחינה על ידי האיחוד האירופי, ואם לא תעמוד בו - תיפגע כלכלית. למרות זאת, ישראל לא עדכנה את החקיקה שלה בתחום, ונסמכת על חוק ישן משנת 1981.

את ה-GDPR עיצבו גם קולות הביקורת, שהדגישו את החשיבות שבשימוש במידע. רבות נכתב על ערך המידע בעידן מתקדם, ובעיקר - כיצד ניתן לייעל ולשפר את מערך הבריאות והתרופות, על ידי הסתכלות על קבוצות פרטניות באוכלוסייה, השפעות טיפולים ותרופות

עו"ד דן חי עומד בראש משרד דן חי ושות', המתמחה בדיני טכנולוגיה, סייבר ופרטיות ומשמש גם כיו"ר הוועדה להגנת הפרטיות בלשכת עורכי הדין • עו"ד רועי סננס עומד בראש מחלקת דיגיטל ומשפט דאטה בינלאומי במשרד דן חי ושות' ומשמש גם כיו"ר (משותף) של ועדת סייבר ורשתות חברתיות של ועד מחוז תל-אביב של לשכת עורכי-הדין.

עוברים לענן או נמצאים שם? כך תגנו על הארגון

"העולם של הענן הוא חדש ושונה"

מדוע המעבר לענן מציב אתגרים כה גדולים בפני העוסקים באבטחת מידע?

"הענן מוביל לשינוי פרדיגמה בדרך שבה ארגונים יכולים לנהל ולנטר את משאבי המחשוב שלהם. כאשר לארגון יש חוות שרתים או חדר שרתים משל עצמו, בתוך הארגון האתגרים הם יחסית ברורים - משאבי השרת, המחשבים והדאטה בייס - הכל נמצא באותה רשת ובאותו מיקום פיזי, כך שלמנהלי השרת יש שליטה מלאה על המשאבים. הם מגנים על השרתים שלהם מתקיפה פיזית, ומנגנוני ההגנה מתמקדים בהגנה היקפית נגד גישה זדונית מבחוץ, פיירוול, WAF ו-Anti DDoS.

"העולם של הענן הוא חדש ושונה. כל משאבי השרת יושבים מחוץ לארגון, בענן. משאבי השרת כבר לא נמצאים בשליטה בלעדית של הארגון, בנוסף, בעולם החדש הזה, גם גורמים עוינים, כמו האקרים, יכולים לגשת מרחוק למידע שעל השרתים - בדיוק כפי שמנהל השרת או אבטחת המידע יכול לעשות זאת. שטח התקיפה של משאבי השרת גדל פתאום, כי כולם יכולים לגשת לכל דבר, כמעט מכל מקום.

"בתחום הענן, קיים מודל האחריות המשותפת שאומר שהאחריות על אבטחת המידע באפליקציות ומשאבי המחשב משותפת לספק ולארגון עצמו, כאשר יש תחומים שעליהם אחראי הארגון וכאלה שעליהם אחראי הספק. הבעיה היא שבמקרים רבים קווי הגזרה לא ברורים. לפי מחקר של רדור, בקרב שני שלישים מהארגונים שמשתמשים בתשתיות ענן ציבוריות, לא ברור איפה עוברים גבולות האחריות. ב-50% מהארגונים הללו אירעה חשיפה של מידע כתוצאה מחוסר ההבחנה הזה. בשורה התחתונה, לארגונים בעולם הענן יש פחות שליטה ונראות על המשאבים שלהם עצמם - וכפועל יוצא מכך, החשיפה והסיכון שלהם עולים."

איך זה משפיע על ארגונים שמנסים לצלוח את האתגר הזה?

"זה אכן אתגר לא פשוט לארגונים. מצד אחד, הגמישות של הענן עולה בקנה אחד עם הרצון להאיץ תהליכי פיתוח, לענות על הדרישות של הלקוחות שצצות כל הזמן ולהגיב לתחרות, שמאלצת ארגונים להוציא גרסאות ועדכונים בקצב מהיר. מטרתם של המפתחים היא להוסיף יכולות למוצרים שהם עובדים עליהם, ולספק במהירות שירותים חדשים למשתמשים, אך המהירות הזו מייצרת אתגרי אבטחה. במקרים רבים הפיתוח רץ קדימה, בעוד שהאבטחה משתרכת מאחור. לפי מחקר נוסף של רדור, ב-70% מהארגונים משרתים גרסאות לפחות פעם בשבוע, אך למעלה מחצי מהארגונים לא מכלילים בדיקות אבטחה בתהליך שחרור הגרסה.

המעבר לענן הוא אחת ממגמות הטכנולוגיה המשמעותיות של השנים האחרונות, אשר מאפשרת לארגונים רבים גמישות גדולה יותר לצד חסכון בעלויות. אך לצד היתרונות, הוא גם מציב אתגרים משמעותיים בתחום אבטחת המידע. ברדור מסבירים מהן הסכנות העיקריות - ואיך אפשר להמנע מהן

שהיא קריטית עבור הארגון - גם למתקיף יש גישה כזו. "כאן מתחיל אובדן שליטה מסוים של הלקוח - ממצב בו הוא שולט מקצה לקצה על השרתים, החומרה, התוכנה, מערכת ההפעלה, הדאטה בייס והתקשורת כלפי חוץ - למצב שבו הוא לא יודע איפה בדיוק נמצאים כל אלה, ולאילו גורמים נוספים יש גישה לשרת. זהו שינוי פרדיגמה - משליטה מלאה, למוטת שליטה קטנה הרבה יותר, וזהו עולם חדש שצריך להתרגל אליו."

אז מדוע לעבור את ההסתגלות הזו? לדברי ויטלשטיין, "היתרון הגדול של הענן הוא הגמישות. אם אני צריך כיום לתכנן חוות שרתים, אני צריך לחשוב מה יהיו דרישות התוכנה של הארגון שלי בעוד חמש שנים, ומכאן לגזור אחורה את דרישות החומרה, לצאת לרכש ולאמן אנשים ייעודיים שינהלו את העניין. זה תהליך ארוך ויקר, וייתכן גם שבעוד שנה נבין שטעינו וקנינו מעט מדי חומרה, כך שיש לרכוש שוב, או אולי קנינו יותר מדי.

"בעבודה מול הענן, ברגע שאנחנו זקוקים לעוד שטח מחשוב - פשוט נשלם עליו ונקבל גישה מיידית. אפשר לקנות לפי הצורך. הלקוחות יכולים להרים ולהוריד שרתים כמעט בלי לתכנן מראש. אם צריכים עוד משאבים - אפשר לקבל אותם במהירות. כך ניתן לשחרר אפליקציות ושירותים במהירות גבוהה יותר, ולהגיב לשינויים בשוק הדינמי. כך שיש כאן טרייד אוף - יתרון הגמישות, מול החיסרון בשליטה ובנראות. כל זה מיתרגם גם לאבטחת המידע."

"כבר לא נכון להגיד שארגונים עוברים לענן - כי הם כבר שם", מסביר ארד ויטלשטיין, מנהל פעילות רדור ישראל ומזרח אירופה, העוסקת בהגנה על ארגונים מפני מתקפות סייבר. "באופן כללי, ניתן לראות כיום שני סוגים של ארגונים: אלה ש'נולדו' בענן (born-in-the-cloud), ופועלים שם מהיום הראשון, וכאלה שנמצאים בתהליך של מעבר לענן (cloud migration). בקרב אלה שנמצאים בתהליך של מעבר, יש כאלה שעוברים מהר או לאט יותר, אבל הכיוון הוא ברור וחד-משמעי."

כדוגמה, מביא ויטלשטיין ארגון גדול בתחום הפיננסיים בישראל, עמו נפגש לאחרונה. "תעשיית הפיננסיים נחשבת שמרנית יחסית, שכן היא מחזיקה במידע רגיש מאוד, ונתונה תחת רגולציה כבדה. ואולם, גם התעשייה הזו עוברת לענן. כאשר שוחחתי עם מנהל אבטחת המידע של הארגון, אחד המובילים בשוק, הוא אמר שהאתגר הגדול ביותר שלו כ-CISO הוא איך לאבטח את הסביבות החדשות, ובמקביל לאפשר אימוץ של סביבות פיתוח וטכנולוגיות חדשות, שיאפשרו לארגון לנצל את כל היתרונות של הענן הציבורי.



באדיבות חברת רדור

ארד ויטלשטיין, מנהל פעילות רדור ישראל ומזרח אירופה

"אם בעבר היית צריך לחדור לדטה-סנטר של הבנק כדי להיכנס לאפליקציות מסחר ועסקאות, כיום, כשהכל יושב בענן - נפתח שטח חדש עבור התוקפים", מסביר ויטלשטיין. "בעבר לא היו מאפשרים גישה מבחוץ ליישומים קריטיים, אבל כעת המצב השתנה. ברגע שאפליקציה והמידע יושבים בסביבת ענן, הגישה אליהם מתבצעת מרחוק; ואם יש גישה מרחוק לאפליקציה

הגנות חיצוניות או כנגד מתקפות שמצליחות לעבור את קו ההגנה.

"הדרישה השנייה היא הגנה אדפטיבית, שמשתנה באופן אוטומטי לפי שינויים באפליקציה או דפוסי השימוש של המשתמש. קצב השינויים של האפליקציות מהיר, והגנות חייבות להשתנות בהתאם ולהגיב לאיומים חדשים שלא נראו בעבר, כל זה מבלי להפריע להליכי הפיתוח - ומנגנונים המבוססים על למידת מכונה ובינה מלאכותית יכולים לעשות זאת באופן אוטומטי.

"אלמנט קריטי הוא מהירות הזיהוי של האיום, ומהירות הבלימה של המתקפה שמשתנה בזמן אמת. בדומה למערכת כפת ברזל, שצריכה לתת מענה מול טיל שיכול לשנות במהירות את המהירות והגובה שלו - ולשנות את התגובה שלה בהתאם, כך גם בעולם הסייבר: על המערכת לדעת לזהות שינויים או דפוסי התנהגות לא חוקיים בזמן אמת ובמהירות, וליצור מנגנוני הגנה לעצירה מהירה של אותן התקפות.

"הדרישה השלישית, קריטית לא פחות, היא היכולת לקבל תמונת מצב של ההתקפה ממקום מרכזי אחד באמצעות שילוב של ממשקי ניהול וסנכרון של המודלים השונים שלעיתים נמצאים בסביבות ענן שונות.

"התקפה יכולה להתחיל במקום מסוים ולהתפשט למקום אחר, להתחיל ברשת ולהפוך לאפליקטיבית, או לגדול ולהפוך למורכבת יותר, ולכן חשוב שמערכת הניהול, הניטור והפעלת ההגנה תהיה מרכזית גם היא. ההתקפות יכולות להיות מורכבות ומבוזרות מבחינת הטכנולוגיות השונות והטכניקות שהמתקיף משתמש בהן. גם מערכת ההגנה צריכה לדעת לזהות את אותם שינויים ולסנכרן בין מנגנוני הגנה שונים במערכת אחת, שנותנת תמונת מצב שלמה.

"חשוב לציין גם כי ככל שעובר הזמן, יותר ויותר ארגונים עובדים על כמה סביבות ענן במקביל. כך הם מגלים שיש להם סביבות שונות, כל אחת עם כלי שליטה שלה - ועליהם לאחד את כל אלה לתוך נקודת שליטה ובקרה אחת. לכן, אחת הדרישות של אבטחת מידע בענן היא ניהול מרכזי שמאפשר שליטה ובקרה על משאבים, לא משנה אם הם נמצאים בענן של אמזון, בזה של גוגל או בעולם הפיזי."

"התעבורה הזדונית נחטמת - מבלי להפריע למשתמשים לגיטימיים"

מהו הפתרון שרדור מציעה לנושא אבטחת הענן?
 "רדור פיתחה סט שלם של פתרונות ייעודיים לענן, במטרה להגן בצורה מלאה על משאבי רשת אשר רצים על גבי תשתיות ענן ציבוריות. אנחנו עוסקים בהגנה על פנים הענן, כמו טעויות קונפיגורציה והרשאות יתר של משאבים, למשל, עובד שמקבל גישה למידע שהוא לא אמור לגשת אליו. הרשאות יתר הן הסיבה ללא מעט מקרים של פריצות וגניבת מידע. משתמש מסוים קיבל הרשאות יתר, וכאשר מתקיף הצליח להתחבר <<<



מך, עולות דרישות חדשות ממוצרי אבטחת המידע. כיום, לקוחות שפועלים בסביבת ענן צריכים מנגנוני אבטחה מוכוונים או ייעודיים לענן. כלים סטנדרטיים לא יוכלו לזהות איומים אלה, ואחד הדברים החשובים בעולם אבטחת המידע הוא קודם כל לדעת לזהות את ההתקפה, ואז להשתמש בכלים חכמים מספיק כדי לעצור אותה."

אז מהן הדרישות כיום להגנות מוכוונות ענן?

"ראשית, הפתרונות צריכים לתת כיסוי של 360 מעלות בסביבת הענן. כפי שהזכרנו קודם לכן, בענן שטח החשיפה גדול הרבה יותר, ויש מספר גבוה יותר של נקודות גישה. צריך להגן על השירותים שמתארחים בענן כנגד כל כיווני התקיפה האפשריים, מבפנים ומבחוץ. הפתרון צריך להגן גם על הפנים החיצוניים של הענן, כנגד תעבורה זדונית שבאה מבחוץ, אבל גם על תוך סביבת הענן, כנגד איומים שלא ניתן להגן מהם באמצעות

"במקביל, ארגונים מחפשים כל העת טכנולוגיות חדשות שיעזרו להם לקצר את לוחות הזמנים, כגון מיקרו סרביסס (Micro-services) וטכנולוגיות Kubernetes. טכנולוגיות אלה יוצרות אתגרים אף הן, פשוט כי הן חדשות ועדיין לא מכירים אותן כל כך. היתרונות של גמישות ומהירות בענן יוצרים חשיפה גדולה יותר של הארגון ושל המידע של הלקוחות שלו."

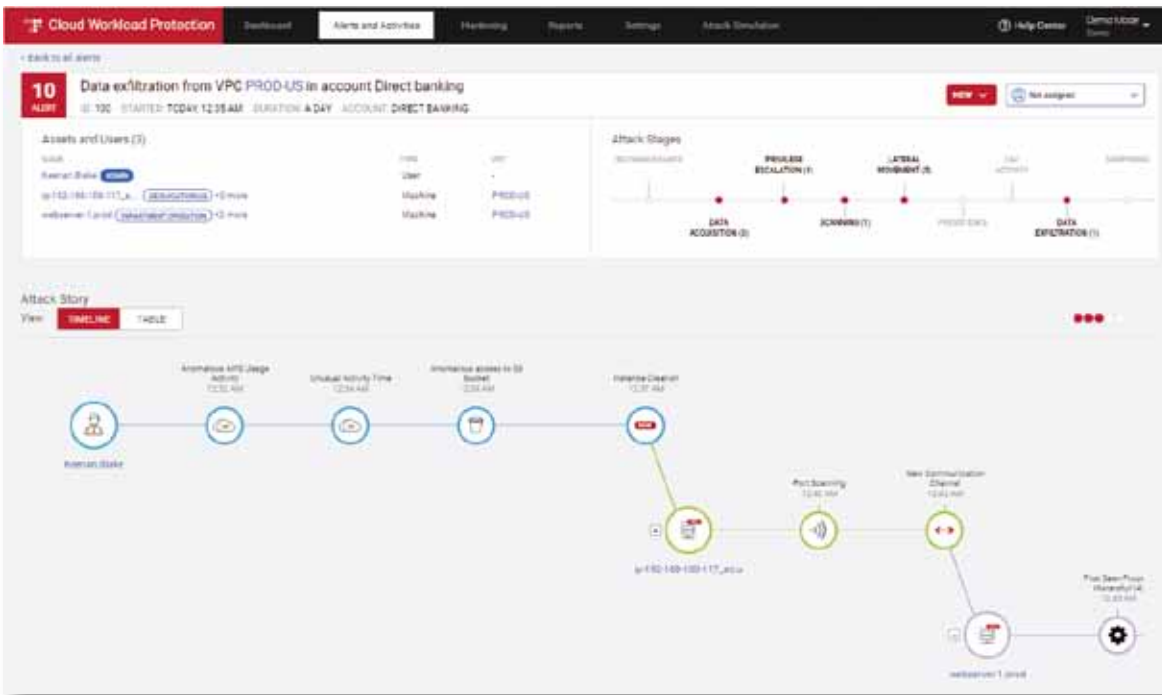
האם הכלים הקיימים היום מספקים מענה?

"אף שבשוק יש עשרות פתרונות, בפועל לרובם חסרות יכולות בתחום של אבטחת מידע - עד כמה הם מגינים על האפליקציה או המידע, או בתחום האוטומציה - עד כמה הם משתלבים עם תהליכי הפיתוח. פתרונות רבים מבוססים על הגדרות אבטחה ידניות, אבל האיומים מתפתחים בקצב מהיר, וחשוב שמערכות ההגנה יידעו להיות אדפטיביות לאותם שינויים בזמן אמת. מערך הגנה אדפטיבי הוא כזה שמבוסס על לימוד מכונה ועל כלי AI, כדי שיידע להתמודד עם השינויים בצורה מהירה ואפקטיבית.

"בכל הנוגע לאוטומציה, פתרונות רבים שקיימים כיום פותחו בגישה שמתאימה לעולם הישן, של שרתים פיזיים והגנה על דאטה סנטרים, אך הם לא התאימו את עצמם לעולם הענן ולעולמות הפיתוח מבוססי Dev Ops, אג'יל, מיקרו סרביסס (Micro-services) וכדומה. "בשורה התחתונה, שורת איומי הסייבר בענן שונה מבעבר הודות לטכנולוגיות אחרות ואתגרים שונים. כתוצאה

נא להכיר: חברת רדור

רדור היא מובילה עולמית של פתרונות ליישומים (Application delivery) ולאבטחת סייבר עבור מרכזי נתונים וירטואליים מבוססי תוכנה הנמצאים בענן. לרדור יותר מ-10,000 לקוחות ארגוניים וחברות טלקום ברחבי העולם, והיא מסייעת להם להסתגל לאתגרי השוק במהירות, לשמור על רציפות עסקית ולהשיג יעילות מקסימלית. פנו אלינו בכל שאלה: israelsales@radware.com



מוצר Cloud Workload Protection Service של רדוור מחבר אירועים נפרדים לכדי שרשרת תקיפה אחודה

איך הפתרון שלכם שונה מפתרונות אחרים שקיימים בשוק?

"הוא שונה בשני אופנים מרכזיים. ראשית, השימוש שלנו במודל אבטחה פוזיטיבי פירושו שהאבטחה מותאמת לדפוסי השימוש של המשתמשים ומתעדכנת אוטומטית, בניגוד למנגנוני אבטחה ידניים שדורשים מגע יד אדם כל הזמן. כתוצאה, אנו יודעים לתת הגנה טובה יותר מבחינת סגירת איומים, ועם אחוז טעויות נמוך יותר. האוטומציה שלנו גם מסייעת לארגונים לסגור את הפערים שבין קצב הפיתוח לקצב העדכון של האבטחה.

"שנית, המיקוד שלנו הוא בפתרונות ייעודיים לענן - סביבה שבה האיומים והאתגרים שונים מאשר בסביבת חומרה, וגם הטכנולוגיות הן שונות. לכן, רדוור משקיעה בשנים האחרונות מאמצים רבים בפיתוח פתרונות ייעודיים לענן, המותאמים לטכנולוגיות שבו. ביניהן ניתן למנות, למשל, את פתרון ה-Workload Protection להגנה על פנים סביבת הענן, ה-Kubernetes WAF להגנה על אפליקציות שרצות מעל סביבת Kubernetes, או שירותי ה-Anti-DDoS, Anti-Bot ו-WAF להגנה של הסביבה החיצונית של הענן.

זהו תחום שמשתנה מהר מאוד. מה החזון שלכם לשנים הבאות?

"ארגונים צריכים לחשוב לא רק על המצב הנוכחי שלהם, אלא היכן הם יהיו בעוד חמש שנים - ולתכנן בהתאם את ארכיטקטורת האבטחה שלהם. הבעיה היא שבעולם הטכנולוגיה מאוד קשה לחזות מה יהיה בעוד חמש שנים, ולכן חשוב לשמור על גמישות בבניית ארכיטקטורת האבטחה. החזון שלנו הוא לתת את ההגנה הטובה ביותר על בסיס הטכנולוגיות שלנו, לצד אוטומציה ואינטגרציה עם הטכנולוגיה והסביבות החדשות שארגונים מטמיעים. כך נוכל לוודא שלארגונים יש את הגמישות הדרושה להם כדי להשתנות, לצד אבטחה ששומרת על קצב אחיד עם השינויים בארגון, ולא נופלת מאחור."

עצמו, כמו Anti-DDoS, Anti-Bot ו-WAF, שתפקידים להגן על הפנים החיצוניים של הענן ולמנוע מתעבורה זדונית להגיע אל הענן מלכתחילה."

מהם יתרונות הגישה של רדוור?

"היתרון הבולט הוא הטכנולוגיה שבה אנחנו משתמשים לאיתור איומים ובלימה שלהם. אנחנו מעניקים הגנה כוללת נגד כל וקטורי התקיפה השונים, עם הגנות הן בתוך הענן והן על הפנים החיצוניים של הענן. כל המוצרים שלנו מבוססים על אלגוריתמים מתקדמים של בינה מלאכותית, שקודם כל לומדים את דפוס התעבורה והשימוש באפליקציה, ואז לומדים אוטומטית הגנות המותאמות לדפוסים האלה, ויכולים לעצור כל דפוס חריג. כתוצאה מכך, יש התאמה מירבית בין דפוסי השימוש לבין האבטחה. תעבורה זדונית תיחסם אוטומטית, בעוד שמשתמשים לגיטימיים לא יופרעו - בהתאם לגישת מודל האבטחה הפוזיטיבית.

"יתרון שני הוא ההגנה האדפטיבית. ההגנות שלנו יודעות להשתנות ולהתעדכן אוטומטית כך שאבטחת המידע לא צריכה לדרוף אחרי קצב השינויים באפליקציה, ויש תמיכה בטכנולוגיות חדשות, כמו הקוברנטיס, מולטי קלאוד וכן הלאה. היות וארגונים רבים יותר עובדים במספר עננים במקביל, התמיכה במולטי קלאוד היא יתרון חשוב - המוצרים שלנו תומכים בכל סביבות הענן המרכזיות."

"שורת איומי הסייבר בענן שונה מבעבר הודות לטכנולוגיות אחרות ואתגרים שונים. כתוצאה מכך, עולות דרישות חדשות ממוצרי אבטחת המידע. כיום, לקוחות שפועלים בסביבת ענן צריכים מנגנוני אבטחה מוכוונים או ייעודיים לענן. כלים סטנדרטיים לא יוכלו לזהות איומים אלה, ואחד הדברים החשובים בעולם אבטחת המידע הוא קודם כל לדעת לזהות את ההתקפה, ואז להשתמש בכלים חכמים מספיק כדי לעצור אותה"

לפרטים נוספים:

בקרר באתר www.radware.com

ללמוד דרך המשתמש הזה, הוא הגיע לכל מקום בלי הפרעה. "למעשה, זו דוגמה נוספת למתח שבין הרצון בגמישות ובמהירות לבין הצרכים של אבטחת המידע. כשרוצים להתקדם במהירות בעבודה, האינטרס הוא תמיד להוריד כמה שיותר מחסומים. נותנים למפתח את כל ההרשאות הקיימות, רק שרוץ קדימה - אבל זה עלול להיות פתח לצרות. פתרון ה-Workload Protection שלנו מזהה את הסיטואציה של הרשאות יתר, מסוגל לנטר תעבורת פנים ענן כנגד פעילות זדונית ויכול לאסוף אירועי אבטחה ואירועים אחרים כדי לייצר סיפור אחיד וקוהרנטי."

לדברי ויטלשטיין, "חשוב לזכור כי אחד האתגרים הגדולים בניטור מתקפה הוא שפעמים רבות, היא יכולה להימשך חודשים ארוכים. למשל, באחד האירועים המפורסמים של גניבת מידע שראינו לאחרונה, התוקף השתמש בפרצה בשרת אפליקציה כדי להכנס לרשת, מיפה את הרשת מבפנים, ואז השתמש בהרשאות יתר שהיו מוגדרות ברשת על-מנת לגשת למסד הנתונים המרכזי שלהם ולהעתיק את כל המידע שבו. זו שרשרת אירועים שלא מתרחשת בין-לילה, אלא תהליך שמתפרס על-פני מספר חודשים, ולפעמים יותר. כל הפעולות האלה מייצרות לוגים, אך אדם רגיל יתקשה לנתח אלפי שורות של לוגים כדי לחבר את האירועים השונים ולהבין שיש משתמש אחד שמנסה להגיע למקום אסור ולגנוב מידע. "מוצר ה-Workload Protection שלנו יודע להשתמש בכוח מחשוב גדול ואוטומטי, המבוסס על למידת מכונה ובינה מלאכותית, כדי לנתח מאות אלפי אירועים ולהבין אם הם קשורים זה לזה ולייצר סיפור התקפה אחוד, שמראה את שלבי ההתקדמות של התוקף צעד אחר צעד ולהתריע על כך. הוא יכול לגלות אם מדובר במתקיף שעושה את כל הפעולות הללו, ולא במשתמש לגיטימי שסתם מנסה לגשת למשהו באפליקציה. יש היום מתקיפים מתוחכמים שיוודעים לבצע התקפה בצורה מבוצרת, כדי שכלים רגילים לא יידעו לנטר אותה - וגם אם הם עולים על משהו, פעמים רבות התוצאה תהיה התרעות קטנות רבות, שלא יידעו לחבר אותן לנורת אזהרה גדולה.

"כמו כן, לאחרונה השקנו גם מוצר ייעודי להגנה על Kubernetes, הנקרא Kubernetes WAF. במקרים רבים, קוברנטיס רץ במעין ענן בתוך ענן, ולא ניתן להגן עליו רק באמצעות מוצרי ההגנה חיצוניים של הענן. המוצר החדש הוא ייעודי וייחודי להגנה על אפליקציות בסביבה זו. פרט לכך, יש לנו שורה של מוצרים המגינים על הענן

"אנחנו יודעים להתמודד גם עם איום שעדיין לא מוכר"

לשומרים בכניסה לשדה תעופה המודדים חום לכל מי שמגיע, במטרה לזהות את הסימפטום הידוע למחלה והוא "חום". אם זוהה חום - הנוסע יחסם ולא יכנס לטרמינל. הפתרון שלנו מדמה תהליך המאפשר לכל הנוסעים להיכנס לאחר שעברו חיטוי, בין אם נשאו את הנגיף ובין אם לא. אנחנו לא בודקים סימפטום אחד ידוע כי ייתכן שיש סימפטומים אחרים שמאפשרים לנוסעים לעבור בהקשר הזה ניתן לומר שלאודיקס יש את הנוסחה לניטרול ויחסים לא ידועים. ד"ר איתן מספר, כי "לאודיקס יש שתי משפחות של מוצרים הנותנים קשת פתרונות למגוון תרחישים. פתרונות המשפחה הראשונה מוטמעים ברשת הארגון על שרתי הלקוח.

"משפחת המוצרים השנייה מבוססת פתרונות ענניים במודל SaaS - תוכנה כשירות. המוצר החדש בקו זה הוא פתרון למייל של אופיס 365. אנחנו שואפים להביא לשינוי גדול בתחום ההגנה על המיילים בפלטפורמה העיקרית כיום למייל עסקי."

לאיזה שוק החברה פונה?

"אנחנו מוכרים את המוצרים שלנו בישראל ובחו"ל, בעיקר בארה"ב ואירופה. בין הלקוחות שלנו אפשר למצוא את חברות החשמל גדולות בארה"ב ומוסדות פיננסיים באירופה. בישראל, לקוחותינו כוללים את חברות הביטוח הגדולות ביותר, משרדי ממשלה ועוד. הטכנולוגיה שלנו מתאימה לכל הסגמנטים - בין אם מדובר בפיננסים, בריאות או תשתיות קריטיות. עבור כל גוף כזה, יש לנו פתרונות מותאמים כדי להגן על

הרשת שלו מפני חדירה של התקפות סייבר.

"פתרון ה-SaaS החדש שלנו פונה למאות מיליוני המשתמשים של אופיס 365, כאשר יש מעל 200 מיליון כאלה ברחבי העולם. המטרה היא להיכנס לאקו-סיסטם של מיקרוסופט, כאשר השירות שלנו יינתן בתור תוסף (פלאגין) מעל אאוטלוק."

מה התחזית שלך לשנים הקרובות בתחום הסייבר?

"אין ספק שהסייבר ימשיך להיות דומיננטי ולהתחזק, בין אם בתחום האזרחי והמסחרי ובין אם בעולם הצבאי. גם מגוון הסוגים של התקיפות מתרחב כל הזמן. כך למשל, אחת המתקפות הפופולריות כיום היא של כופרה - ברגע שאתה מפעיל את הקובץ הנגוע, הנוזקה מצפינה את כל הקבצים שלך ולא ניתן לעבוד איתם - עד שתשלם כופר. לרוב, התוקפים דורשים את התשלום בביטקוין - בגלל האנונימיות. מתקפות כופרה ניתן למצוא במנעד רחב של סכומים, החל ממתקפות קטנות המיועדות לאנשים פרטיים או עסקים קטנים ודורשות כופר באלפי דולרים בודדים ועד מתקפות במאות אלפים או מיליוני דולרים המופנות למוסדות ציבוריים וחברות."

"בסופו של דבר כשמנתחים כיצד בוצעה התקיפה מגלים כי נשלח קובץ PDF תמים הנראה כהזמנה או חשבונית וברגע שהקובץ נפתח - הנוזקה חודרת לארגון, אנחנו כאן כדי לעזור לארגונים לאבטח את עצמם ולמנוע מתקפות כאלה", מסכם ד"ר איתן.

צילום: תומר שלום



"הפתרון שלנו מדמה תהליך המאפשר לכל הנוסעים להיכנס לאחר שעברו חיטוי." ד"ר איתן מספר, מנכ"ל חברת Odix

חברת odix הישראלית החליטה לשנות גישה בהתמודדות עם איומי הסייבר - ובמקום לנסות לזהות מתקפות, היא פיתחה אלגוריתמים המנטרלים וירוסים ונוזקות אחרות מהקבצים שנמצאים בשימוש תכוף בארגון

"איומי הסייבר מתגברים ומתחזקים משנה לשנה, ופוטנציאל הנזק עצום", אומר ד"ר איתן, לשעבר מפקד מצ"ב, וכיום מנכ"ל חברת odix, שפיתחה אלגוריתמים לנטרול וירוסים ונוזקות (Malware) אחרות מקבצים ארגוניים. "טווח האיומים

רחב - מתשתיות קריטיות כמו חברות חשמל, מים וגז, שפגיעה בהן יכולה לשתק מדינה שלמה; פגיעה במוסדות פיננסיים, ששם המשמעות יותר כספית; ועוד. ככל שאנחנו מסתמכים יותר על הטכנולוגיה, אנחנו גם נחשפים יותר ויותר לאיומי סייבר, שפוטנציאל הנזק שלהם עצום."

מה הבעיה המרכזית כיום בתחום הגנת הסייבר?

"קיימות הרבה מאוד חברות בתחום, עם שפע של טכנולוגיות ורעיונות חדשים", אומר ד"ר איתן. "היינו מצפים שכל העולם יהיה מוגן ולא נראה התקפות סייבר מוצלחות - אך כל יום שומעים על האקרים שהצליחו לתקוף. אז מה קורה כאן? לפי הניתוח שלנו, הבעיה היא שנוזקות חדשות צצות כל יום, בהמוניהן. קל מאוד ליצור וירוסים חדשים כיום, יש אפילו אתרי אינטרנט שמוקדשים לכך. האנטי-וירוסים והפתרונות האחרים שקיימים לא יודעים להתמודד עם איום לא מוכר - כך שהנוזקות החדשות עוקפות אותם וחודרות לארגונים. כאן אנחנו נכנסים לתמונה.

"הטכנולוגיה שלנו בכלל לא מחפשת את הווירוס או הנוזקה - אלא פשוט מנקה את הקובץ הנגוע, וכך מונעת נזק לשאר המערכת של הארגון. אנחנו סורקים את הקבצים, ויודעים איך המבנה שלהם אמור להיות שם, וברגע שאנחנו מזהים משהו שלא אמור להיות שם, אנחנו מנטרלים אותו, ומחזירים את הקובץ למשתמש כשהוא נקי, בלי שהוא מודע בכלל לתהליך. זו טכנולוגיה אגוסטית לרשת הארגונית, המגובה בחמישה פטנטים

רשומים בארה"ב וכן במדינות באירופה, ובהן צרפת, גרמניה ואנגליה.

"אנחנו מטפלים בקבצים מסוגים מגוונים - ובהם אופיס, PDF, תמונות ו-וידאו. ממחקרים שנעשו עולה, שכ-90% מהנוזקות מועברות בקבצים מסוג אופיס, PDF וקבצי ארכיב. קבצים אלה חביבים על ההאקרים, מאחר שהם נפוצים מאוד בקרב הארגונים, ונוח להשתמש בהם כדי לתקוף את הארגון. כיום יש מעל 70 סוגי קבצים שאנחנו נותנים להם מענה, וכמובן שאנחנו ממשיכים לעבוד כל הזמן על התאמה לסוגי חדשים של קבצים, או וריאציות שלהם."

לעמוד ב"שער" של הארגון

ד"ר איתן פועל בעולם הסייבר מעל 30 שנה, זמן רב לפני שהתחום היה מוכר לציבור הרחב. הוא שירת בצה"ל 25 שנה והגיע לדרגת אל"מ, כאשר בתפקידו האחרון היה מפקד מצ"ב - שם ריכז תחת אחריותו את תחומי הסייבר בצה"ל ובמערכת הביטחון. "כבר אז נכנסנו לעולמות של הסייבר, מתוך הבנה שזה איום העתיד", הוא אומר. "בזמנו גם הובלתי את התוכנית המסודרת הראשונה להגנת המידע - ומאז אני עוסק בתחום."

לדבריו, הרעיון העומד מאחורי הטכנולוגיה של אודיקס הוא לעמוד ב"שער" של הארגון - ולנקות קבצים שעלולים לגרום נזק, לפני שהם נכנסים אליו. "ניתן להמחיש כיצד אנו פועלים עם דוגמה אקטואלית - וירוס הקורונה. הפתרונות המסורתיים לאנטי וירוסים נמשלים

לפרטים נוספים: odi-x.com

למה המודל של סייבר סקיוריטי שבור - ואיך מתקנים אותו?

מה גודל השוק של הבעיה שאתם מנסים לפתור?
 "ענק! גודל שוק האבטחה של נקודות קצה ומובייל ואבטחת מייל מוערך בידי גרטנר ב-10 מיליארד דולר בשנה, אך לדעתי זו הערכת חסר. אמנם את ההערכה מבצעים האנליסטים החשובים ביותר של תחום הסייבר, אבל הם מסתמכים אך ורק על הלקוחות שהם מכסים, ולא מתייחסים לכל העולם. לדעתי, השוק מגיע בקלות ל-20-15 מיליארד דולר בשנה. שוק הסייבר כולו מוערך ביותר מטריליון דולר בשנה".

בין המשקיעות שלנו ניתן למצוא חברות גדולות מאוד - HP, Nvidia, Bharti - Airtel, LG, סמסונג, והן איתנו בזכות הטכנולוגיה פורצת הדרך שלנו. כיום אנו מגנים על כמעט מיליון נקודות קצה, כולל הפרויקט עם HP שהוא ככל הנראה פרויקט נקודות הקצה הגדול בעולם של חברה ישראלית בתחום הסייבר שהותקן ב'מכה אחת'. למעט HP, החברה משרתת מספר לא מבוטל של חברות F500.

"יש לנו לקוחות מכל חמשת הסגמנטים העיקריים - בתחום הפיננסיים, בנקים וחברות ביטוח הגדולות בעולם; חברות תעופה גדולות; חברות טכנולוגיה מרכזיות; מוסדות אקדמיים; וארגוני בריאות. כמו כן יש לנו פתרון ייחודי לחברות שירותי אבטחה שמנהלות את האבטחה לארגונים קטנים ובינוניים".

מה הבעיה הנוכחית בשוק הסייבר, שלא מקבלת מענה?

"כדי לענות על כך, כדאי להזכיר את ההיסטוריה של חברות הסייבר. עד לאחריה, הענף כלל חברות מוכרות וגדולות, שעסקו בעיקר בטכנולוגיה שיועדות לזהות איומים קיימים. ואכן, ב-20 השנה אחרונות רוב האיומים היו 'מוכרים' - כאלה שנראו גם אתמול וגם לפני חודש. האקרים השתמשו באותן טכניקות פחות או יותר, ובהתאם, חברות אלה פיתחו פתרונות שמבוססים על הידע של אתמול. זה היה מוצלח במשך לא מעט זמן. אבל העולם הזה השתנה. האיומים השתכללו ונהיו 'לא מוכרים'. בהתאם, לפני כעשר שנים, התחלנו לראות חברות שהביאו את הבינה המלאכותית לתחום הסייבר. הן עשו את זה בעיקר עבור נקודות קצה - העולם המסובך ביותר, והיחיד שאפשר למנוע בו התקפה, וגם לעשות פעולות שלא ניתן לבצע ברשת ובפיריור. חברות הבינה המלאכותית שהתפתחו הביאו שיפורים מאוד משמעותיים, תוך יישום יכולות מעולם למידת מכונה, אך הן התמקדו, עדיין, בעיקר בעולם הווינדוס ובאיומים קיימים.

"הן אמנם שיפרו את המצב, אבל החיסרון היה ועודנו שהאיומים המתוחכמים באמת הצליחו לחמוק והיה צורך להכניס לארגון צוות גדול של מומחי אבטחה על מנת לתפעל את הפתרון שלהם.

"במקביל, נכנסו טכנולוגיות הענן לתמונה. החברות הללו שמו סנסור פשוט על נקודת הקצה - ששלח

בעוד חברות הסייבר הוותיקות יכולות לזהות רק מתקפות שכבר חדרו לארגון, המודל של דיפ אינסטינקט מזהה את האיום מראש - ומונע את הפגיעה בקרוב ל-100% מהמקרים. גיא כספי, המנכ"ל ואחד המייסדים, מסביר למה מנהלי תאגידים ברחבי העולם נמצאים בהיסטריה תמידית, מה הכיוון הבא שאליו יפנה השוק - ומה מצפה לעובדים שיצטרפו לחברה בחודשים הקרובים



צילום: יח"צ

גיא כספי, מנכ"ל חברת דיפ אינסטינקט

"העולם נתפס לא מוכן למתקפות סייבר מהסוג החדש - ובכל יום, תאגידים בכל העולם חשופים למתקפות שעולה להם מיליארדי דולרים לתקן", אומר גיא כספי, מנכ"ל חברת הסייבר הישראלית דיפ אינסטינקט. בחברה, שהודיעה לאחרונה על גיוס הון נוסף, בהיקף של 43 מיליון דולר, פיתחו מודל חדשני להתמודדות עם איומי הסייבר - באמצעות למידה עמוקה (Deep Learning). כיום, מעסיקה החברה כ-150 עובדים, מהם 100 בישראל, ויש לה יותר מ-500 לקוחות ברחבי העולם. "אנחנו שלושה אנשים, שהקימו את החברה לפני חמש שנים", מספר כספי. "אני מגיע מרקע טכנולוגי, עוסק בסייבר תקיפה והגנה, ביג דאטה ועיבוד נתונים כמעט 25 שנה כולל תפקידי ניהול בכירים בענקיות טכנולוגיה אמריקאיות; ד"ר אלי דוד, כיום מרצה מוביל לבינה מלאכותית באוניברסיטת בר אילן, מומחה בלמידה עמוקה ונחשב אחד החוקרים המובילים בעולם בתחום; וה-CTO שלנו, נדב ממון, שנמצא בניו יורק, הוא בעל ניסיון של יותר מעשור בתקיפה והגנה בסייבר במקומות שונים במערכת הביטחונית, וכן של שש שנים בצ'קפוינט בתפקידים שונים - טכנולוגיים ואופרטיביים.

"חזון החברה נולד כשהחלטנו לפתור בעיה שאין לה מענה בתחום הסייבר - מניעת איומים לפני קרות הנזק, תוך שימוש בלמידה עמוקה. גם כיום, אנחנו היחידים בעולם שמיישמים למידה עמוקה מקצה-עד-קצה (end-to-end) המבוססת על רשתות נוירוניות עמוקות בהגנת סייבר. חסמי הכניסה עדיין מאוד מאוד גבוהים ולא מאפשרים לחברות אחרות להיכנס לתחום, גם אם מדובר בחברות ענקיות, זה תחום שלא ניתן לקנות בכסף. "בכל העולם יש אולי 200 מומחים בעלי תואר PhD בלמידה עמוקה, זה ענף קטן ומצומצם. אנחנו משערים שחוף מהקבוצה שיש אצלו, כמעט 80% אחוז מכוח האדם בענף נמצאים בפייסבוק וגוגל, ועוד מעטים במיקרוסופט, יבמ, אפל ואמזון. לכן, גם חברה גדולה שרוצה להיכנס לתחום ומוכנה לשלם הרבה כסף - פשוט לא תצליח לגייס את המומחים הרלוונטיים".

סוגרים את כל החלונות

"הצלחנו לממש את החזון - למנוע איומים, ולא להסתפק בזיהוי שלהם, כמו שרוב החברות עושות. בנוסף, אנחנו החברה היחידה שיועדת להגן על מנעד רחב מאוד של מערכות הפעלה - גם בנקודות קצה, גם במובייל וגם בתווך של הרשת.

"רוב חברות הסייבר מטפלות במערכת ההפעלה וינדוס, שבה יש הכי הרבה בעיות; אבל גם במערכות אחרות, כמו אנדרואיד, chromebook, מק ועוד, בעיות האבטחה כבר נוצרות בכמויות גבוהות וברמת תחכום מתקדמת. אם נמשיל את הארגון לבית פרטי - אם אתה שומר רק על הדלת ואפשר להיכנס מהחלון, זו לא הגנה יעילה. אנחנו סוגרים את כל החלונות שמאפשרים כניסה לארגון".

מתנהלות במשטר צבאי, אבל אנחנו מאמינים שאם אנשים באים בבוקר ואין להם אתגרים ותשוקה למה שהם עושים, לא נצליח.

"סביבת העבודה שלנו היא בין המאתגרות ביותר שיש בישראל. תחום הדיפ לרנינג נמצא בליבת הפעילות שלנו ורוב האיומים שאנחנו מונעים מבוססים על האלגוריתמיקה הזו, שמשפרת ומתחדשת כל הזמן ומתממשקת לכל צוות בחברה. אנחנו היחידים שעוסקים בכך בישראל, ויש כאן אתגרים חסרי תקדים. בנוסף, מאחר שדיפ לרנינג זה אלגוריתם שאוהב לזלול דאטה, יש בחברה אתגרי ענק בנושאי ביג דאטה, תשתיות ענן, תשתיות מבוצרות ויכולות מתקדמות בעיבוד נתונים.

"העובדים שלנו משפיעים מאוד על העשייה של החברה וכיווני הפעולה שלה, והכי חשוב - משפיעים על העולם. הם חלק ממאמץ עולמי לבלימת מלחמות הסייבר ופשיעת הסייבר, ואפשר לומר שאנחנו מעין 'אינטרפול' של הסייבר עבור חברות, כי אנחנו מונעים מתקפות. זו חברה שיש בה המון פורומים ודיונים אסטרטגיים, ולא

סתם יש כאן חדר ישיבות גדול - כי לכולם יש אמירה. "העובדים שלנו נמצאים במרכז ואנחנו דואגים לפנק ולטפח אותם. בעוד שנה נעבור למשרדים חדשים שרכשנו עכשיו. יש בחברה את כל מה שעובד צריך כדי להיות מאושר. יש קשר בלתי אמצעי למנהלים, בלי דיסטנס; ואנחנו עושים הכל כדי שהעובדים יהיו מרוצים."

מה הפרופיל של העובדים בדיפ אינסטינקט?

"בישראל, יש לנו שתי קבוצות מרכזיות של עובדים. הראשונה היא של אנשים עם רקע אקדמי בכיר מאוד, מעולם הבינה המלאכותית, מדעי המחשב, מתמטיקה ומחקר סייבר. זו קבוצת הלמידה העמוקה שלנו וקבוצת המחקר. הקבוצה השנייה היא מגוונת וכוללת גם עובדים ועובדות עם רקע מחברות מובילות בשוק וגם ממערכת הביטחון, אבל מיחידות שונות לעומת אלה שבדרך כלל מגיעים לחברות סייבר. אלה אנשים עם ותק רב, של שמונה וגם עשר שנים במערכת הביטחון. אלה שהגיעו מהאזרחות עוסקים בסייבר כבר 15 שנה בערך.

"ככלל, העובדים והעובדות שלנו הם איכותיים ביותר בידע ובעובדה שהם אנשים מדהימים באישיות שלהם, אוהבי אדם, סביבה וחיים. אנחנו מחפשים עובדים עם סטייט אוף מיינד שונה, פתוחים, עצמאיים, סקרנים, עם משמעת עצמית ותשוקה לאתגרים, שלא יניחו לאתגר או לבעיה עד שיפתרו אותם. נשים וגברים שיודעים להתמודד עם שינויים ויכולים לחשוב על דרכים יצירתיות לעשות דברים, שייתנו פתרונות בעלי ערך ללקוחות שלנו.

"בחדשים הקרובים אנחנו צפויים לגדול משמעותית, בעשרות עובדים אם לא יותר, ואנחנו מחפשים את העובדים המנוסים - אלה שהם Cutting Edge בכל תחום, לא רק בסייבר. אנחנו מעניקים הזדמנות פיננסית יוצאת דופן - הנתיב שלנו הוא לא של מכירת החברה, אלא של הנפקה. מי שיצטרף אלינו יוכל להיות שותף לחזון של הגנה על העולם, לקחת חלק במלחמה הבלתי פוסקת בפשיעת הסייבר הגואה; ובנוסף, ליהנות מאירוע פיננסי מוכן. כאן לכולם יש אופציות, מהזוטר ועד הבכיר ביותר. אני כמנכ"ל רואה בזה חשיבות גדולה - ורמת הציפיות בהתאם."



מחפשים עובדים עם סטייט אוף מיינד שונה שיצטרפו לחברה. דיפ אינסטינקט

"בעוד שכל החברות האחרות עוסקות בזיהוי מתקפה אחרי שהיא כבר חדרה לארגון, אנחנו עוסקים במניעה. אחרי שיש זיהוי מתקפה קיימת, כל הארגון נכנס להיסטריה - צריך לבדוק מי נדבק באיום, לבודד את כל השאר, לנקות את כל המערכות ובתוך כך להשביט עובדים רבים. חב החברות שהן לא בסדר גודל של פורצ'ן 100 או 200 לא יודעות לעשות את זה.

"אנליסטים אומרים שיש 10 התקפות מוצלחות על תאגיד אמריקאי ביום, וזה אומר שהארגון בהיסטריה תמידית. מה שאנחנו עושים מייצר שקט ארגוני. אנחנו מונעים את האיומים, ונדוע לארגון רק אחרי שהיתה מניעה, כדי שהוא יוכל לראות כל מה שקרה ולהבין שנמנע אירוע פוטנציאלי. האם אנחנו מונעים איומים במאה אחוזים? התשובה היא לא, אבל אנחנו עושים זאת טוב יותר מכל חברה אחרת בשוק העולמי.

"ברוב המקרים אחוזי המניעה קרובים מאוד ל-100, ובמקרים הבודדים שבהם לא הצלחנו - אנחנו מטפלים בחדירה כמו כל חברות הסייבר, אבל נעשה את זה בכמות מאוד קטנה של המקרים, בלי היסטריה בכל הארגון. בארה"ב, התקיפות התכופות הן גיהנום. אפילו בדאבוס הכריזו השנה על איום הסייבר לראשונה כאיום המשמעותי ביותר על הכלכלה והשקט העולמי - פשוט כי הנזקים עצומים, ולא יודעים איך להתמודד איתם."

סביבת עבודה ליברלית

"השיטה שלנו מורידה משמעותית את שיעור ההדבקה, ושומרת על כל מערכות ההפעלה. אנחנו מגינים על כל הארגון, ולא רק על דלת הכניסה. בנוסף, המערכת שלנו יודעת לחיות ליד כל מערכת הגנה אחרת, ואין צורך להחליף את המערכת הקיימת, בניגוד לחברות אחרות. זה יתרון גדול, כי ארגונים לא כל כך אוהבים להחליף תשתיות סקיריטי קיימות. אנחנו יודעים ליצור שקט נפשי עבור חברי ההנהלה של חברות גדולות ובינוניות, כך שיוכלו לעבוד ולא לעסוק כל היום באיומי סייבר."

מה מאפיין את סביבת העבודה שלכם?

"דיפ אינסטינקט ידועה בשוק הסייבר בישראל כחיה אחרת, שונה מאוד, מכמה סיבות. הראשונה היא הדנ"א של החברה, שהוא סופר-ליברלי, רוב החברות בענף

את כל המידע לענן, המידע נותח שם, וההכרעה מה לעשות התקבלה שם. אמנם ראינו שיפור מסויים ברמת האבטחה, אבל במקביל צצה בעיה חדשה - לוקח זמן לשלוח את המידע לענן, ולא מקבלים החלטה מיידית. בזמן הזה האיומים יכולים לייצר נזק מאוד משמעותי. כמו כן, לא תמיד כל המכשירים מחוברים לרשת או לענן; ומדובר במערכות מסובכות, שדורשות המון כוח אדם. "לפני חמש שנים, כשהחברות הללו התחילו למכור, הן נחשבו לדור החדש של הסייבר סקיריטי, ואכן סיינו משמעותית לשיפור הזיהוי והטיפול באיומים קיימים וחדשים. אבל תוך ארבע או חמש שנים, ההאקרים כבר פיצחו את שיטות הפעולה שלהן. כל מי שנמצא בעמדת מפתח בעולם הסייבר יודע לומר שבין 2017 ל-2019 חלה קפיצת מדרגה מטורפת במנעד האיומים, סוג האיומים, רמת התחכום וכמות האיומים היומית החדשה שאנו חווים.

"העולם נתפס לא מוכן לדבר הזה, ואיחועי הסייבר שקרו בשלוש השנים האחרונות שיתקו מדינות שלמות. כולם זוכרים שבקיץ 2017 רכבות ובתי חולים בבריטניה לא עבדו. עברו חודשיים והגיע גל שני שתקף 70 מדינות ושיתק כולל פה בישראל משרדי ממשלה, ואחריו הגיעו עוד רבים אחרים. חברות מדווחות על נזקים מטורפים. כבר לא מדובר רק באובדן דאטה, אלא ביכולת לתפקד תחת איום.

"חברת מירסק, למשל, דיווחה של הפסדי עתק בגלל מתקפת סייבר, עקב הכאוס שנוצר כי האוניות שלה היו מושבתות. חברת הדאטה סנטרס הגדולה בעולם דיווחה בחודש שעבר על נזק של מיליארד דולר מההתקפה בשנה שעברה.

"בשלוש שנים האחרונות אין בארה"ב גוף רציני שלא חטף התקפה מוצלחת שפורסמה. יש אלפי התקפות שלא מפורסמות, כי אין רגולציה שמחייבת פרסום בארה"ב. כולם זוכרים שהיתה חדירה ל-FBI וכל הנתונים נחשפו; תקיפות אחרות היו על ארגונים כמו מורגן סטנלי, בואינג וטארגט, שהותקפה כבר פעמיים בשנה שעברה וזה עלה לה מיליארד דולר."

מדוע דיפ אינסטינקט נמצאת בעמדה שבה היא יכולה לפתור את הבעיה טוב יותר מחברות אחרות?

האויב שבפנים כבר כאן

איך לאתר, להתגונן ולהתאושש מהתקפות מתוך הארגון? / גיל באומל

Quest, המספקת פתרונות אבטחה ותאימות (Compliance) לכל סביבת מיקרוסופט - מקומית, היברידית או בענן, מציעה חבילה מלאה של פתרונות, המאפשרים לכם לאבטח את פנים החברה בצורה הדוקה לא פחות מאבטחת ההיקף, ומבטיחים עמידה מתמדת במדיניות אבטחת המידע הארגונית. הנה כמה מיתרונות הפתרונות של Quest.

● הקטנת סיכון וסגירת פערים:

ההגנה מפני האיום הפנימי מתחילה בניהול תקין. הפתרונות של Quest מוסיפים אוטומציה למשימות ניהול, כולל הקצאת הרשאות למשתמשים חדשים ושילול הרשאות למשתמשים עוזבים, במטרה לסגור פערים הנובעים מריבוי מערכות והשאררת הרשאות למשתמשים לא קיימים כדוגמה. תהליכי אישור מסודרים ומתועדים מוסיפים שכבת ניהול הרשאות ושליטה במצב הקיים.

● זיהוי פגיעויות באופן יזום

סביבת ה-IT היא דינמית, כך שיש לוודא באופן קבוע ורציף אם יש פרוצדורות או פגיעויות (vulnerabilities). פתרונות Quest מספקים אוטומציה ודיווח אחוד לתשתיות מיקרוסופט המקומיות, ההיברידיות או בענן, כך שתוכלו לקבוע בקלות למי יש גישה למה ואיך הם קיבלו גישה זו. יתר על כן, ניתן לשנות הרשאות משתמשים ישירות מממשק הדוחות. ניתן לגלות היכן נמצא המידע הארגוני הרגיש ביותר ולוודא שהוא מוגן היטב, לבדוק ולנהל את ההרשאות הקבוצתיות (GPO) בצורה קלה ואפילו לנעול אובייקטים רגישים על מנת שלא ניתן יהיה לשנות אותם.

● זיהוי והתראה של פעילות חשודה

פתרונות Quest מאפשרים לקבל התראות בזמן אמת על איומים פעילים, על ידי ביצוע אודיט מתמיד על פעילות משתמשים ומשתמשים חזקים כולל התראות על מתן הרשאות מיוחדות, שינויים לא ראויים ופעילות חשודה אחרת. ניתוח מתקדם של התנהגות משתמשים (User Behavior Analytics) המאפשר בניית מודלים ודפוסי התנהגות של משתמשים פרטניים ומגלה חריגות בפעילות. ניתן להגדיר אפילו תגובות אוטומטיות, כגון חסימת פעילות משתמשים, השבתת המשתמש או שחזור השינויים שבוצעו על ידו.

● ניתוח תקיפות בזמן אמת והתאוששות מהן

בממוצע, נדרשים לארגון 69 ימים כדי להשתלט על אירוע פריצת מידע. Quest מאפשרת לבצע תחקיר אירוע מעמיק לאירועי אבטחה במהירות ובקלות באמצעות איסוף נתונים מרכזי ומנוע חיפוש דמוי גוגל לחקירה. יתר על כן, ניתן להקים מעבדת בדיקה וירטואלית לתכנון DR של כלל ה-Active Directory Forest - ולקצר משמעותית את זמן ההתאוששות מאירוע באמצעות ממשק משתמש ידידותי.

● **עמידה ברגולציות ומדיניות אבטחת מידע ארגונית**
היכולות המוזכרות מעלה מאפשרות לארגונים לעמוד במגוון רחב של תקנות אבטחת מידע ובמדיניות האבטחה שהוגדרה בארגון. בנוסף, פתרונות Quest מציעים אפשרות לדחיסת לוגים חכמה המאפשרת לאחסן נתונים רבים יותר למשך זמן רב בצורה חסכונית במשך שנים, תוך הבטחת זמינותם לחקירות אבטחה וביקורות.

לפרטים נוספים:

www.quest.com/solutions/security-and-compliance

מתרבות והולכות. לפני זמן לא רב, רק תעשיות מסוימות היו מחויבות לרגולציה, והסמכת ISO היתה 'מספיק טובה'. אולם כעת, תקנות כמו GDPR, PCI ו-CCPA, כמו גם תקנות מקומיות, חלות על כלל הענפים. כתוצאה מכך, ארגונים נדרשים לא רק להכין את עצמם לתאימות לתקן, אלא גם לשמור עליו ללא הרף כאשר התקנות מתפתחות ומתרחבות.

כדי להשיג יעדים אלה, בראש ובראשונה עלינו לשלוט על הרשאות המשתמשים ולפקח מקרוב על מה שמתרחש בארגון. הכלים הגנריים אינם מקלים על ביצוע המשימה הזו; למעשה, 62% מהמשתמשים מודים שיש להם גישה רבה יותר ממה שהם צריכים. מערכות SIEM מספקות נראות מסוימת לפעילות המשתמשים, אך הן יקרות לרישוי, קשות לכיול ומורכבות לתפעול. יתר על כן, מערכות SIEM טובות באותה מידה כמו הנתונים המוזנים בהן - במידע המועבר על ידי כלים גנריים (native logs) יש פערים גדולים וחוסר בהירות בתחומים קריטיים. אין פלא שהתוקפים מסתובבים בממוצע 101 ימים בתוך הרשת לפני שהם מתגלים.



גיל באומל, נהל פעילות QUEST ישראל

יש גם דרך טובה יותר

כל אלה מעלים את הצורך בפתרונות המאפשרים לבצע כמה מהלכים בעת ובעונה אחת: להגביל את הנזק שמשמש (או האקר שגנב הרשאות כאלו) יכול לגרום לנכסי הארגון על ידי בקרת הרשאות חכמה, שתקפיד לוודא כי לכל עובד יש את ההרשאות והגישה המינימאלית לביצוע עבודתו; לספק התראה מיידית כאשר נעשה משהו המסכן את הארגון; לבסס קו התנהגות נורמלית עבור כל משתמש, ובכך לאתר באופן מידי התנהגות חריגה; ובעזרת כל אלה, לחקור ולהגיב במהירות לאירועי אבטחת מידע.

בימים אלה, רבים עוסקים ביצירת פתרון מהיר לעבודה מהבית, במטרה להגיש משאבים ארגוניים קריטיים שיאפשרו לעובדים להישאר פרודוקטיביים ככל האפשר. במקביל, מנמ"רים ומנהלי אבטחת מידע שוקדים על בניית הגנות היקפיות חזקות כדי לאפשר עבודה מרוחקת - אבל האם אתם מוכנים לאיומים שכבר נמצאים בתוך הרשת שלכם?

חברת QUEST (המופצת בארץ על ידי CDATA), פועלת בשוק אבטחת המידע זה יותר מ-30 שנה, במהלך פיתוח חליפת פתרונות להגנה על תשתיות מיקרוסופט הקריטיות כגון Active Directory, Exchange, File Server, TEAMS ו-Servers, SharePoint, Azure AD. בתקופה הנוכחית, יותר מתמיד, מוצרים מסוג זה הכרחיים להמשך הפעילות היומיומית של הארגון - מבלי לחשוף אותו לסיכונים אבטחה מוגברים.

בזמן שאתם נערכים לחסום את הגישה - התוקף כבר נמצא בתוך הרשת

נראה שבכל שבוע מדווחות הכותחות על דליפה של מידע, או גניבתו. כולם מודאגים מהאקרים, ולכן באופן מסורתי, ארגונים משקיעים את מירב המשאבים בהגנות היקפיות. ואולם בפועל, יותר ממחצית מהפריצות מבוצעות בידי תוקף שכבר נמצא בתוך הרשת - כמו למשל עובד שגונב מידע ארגוני במזיד כדי לעבור למשרה חדשה, או מנהל מערכת שבתום לב מבצע שגיאת תצורה קריטית. במקרים אחרים, מדובר בתוקף חיצוני שהשתלט על חשבון לגיטימי. מיקרוסופט מדווחת, כי בכל יום 95 מיליון חשבונות Active Directory נמצאים תחת ניסיון תקיפת סייבר, וכי 10 מיליון ניסיונות גישה ל-Azure AD בכל יום הם למעשה התקפות סייבר.

כתוצאה מכך, מומחי אבטחה ממליצים לארגונים להניח כי התוקף כבר נמצא בתוך הרשת שלהם. במקום זאת, במאורח, גורם לא מורשה הנמצא ברשת ינסה לגרום נזק או לגנוב את הנתונים הקריטיים בארגון. אפילו ההגנות ההיקפיות הטובות ביותר אינן יכולות לעשות דבר כדי לעצור אותו, לכן חיוני שתהיה גם מדיניות אבטחה ללב ליבו של הארגון, במטרה להגן על ה-Active Directory - היהלום שבכתר.

התוקף מסתובב בממוצע 101 ימים ברשת - לפני שהוא מתגלה

ביחוד בימים אלה, מנמ"רים ומנהלי אבטחת מידע נדרשים לתת מענה מהיר באמצעות כלים טכנולוגיים הנשענים על שירותי ענן, כדי להבטיח את ההמשכיות העסקית של הארגון. בנוסף לדרישות אלו, כמות המידע שאנו יוצרים גדלה באופן מטאורי, וחלק גדול ממנו הוא מידע בלתי מובנה במאגרי מידע בענן כגון SharePoint Online ו-OneDrive, במקום בכמה בסיסי נתונים במרכזי המחשוב המאובטחים. כתוצאה מכך, האתגר הוא לא רק בהגנה על המידע הרגיש - אלא בעצם ההבנה היכן הוא נמצא.

אם לא די בכך, תקנות העוסקות בפרטיות הנתונים

המכוניות כבר מתקשרות עם הענן - ומה עם אבטחת המידע?

כלי הרכב נהפכים לחכמים יותר, עם יכולות חיבוריות גבוהות - אך ככל שהחיבוריות לאינטרנט גוברת, גוברת גם הסכנות לתקיפה של הרכב מהרשת. אחת החלוצות בתחום הסייבר סקויריטי לרכב החכם היא CYMOTIVE הישראלית, שהוקמה בשיתוף פעולה עם קבוצת פולקסווגן העולמית

אנחנו עוסקים כל הזמן באזורים חדשים, כאלה שעוד לא נגעו בהם. אחרי הכל, תחום ה-connected vehicles הוא אזור טכנולוגי חדש יחסית, כך שאנחנו עוסקים הרבה במחקר על טכנולוגיות עתידיות, ולא פעם אנחנו הראשונים שחוקרים טכנולוגיה מסוימת בעולם האוטומוטיבי."

התמונות באדיבות חברת סיימוטיב



נדב הוס, מוביל צוות Automotive Cloud בסיימוטיב

מהו הרקע של חברי הצוות?
"הצוות מגיע מרקעים שונים ומגוונים. יש אנשים שמגיעים מחברות אנטרפרייז, מסטארטאפים, מגופי ביטחון וצבא, ואחרים שמגיעים מחברות פרטיות או אפילו מתעשיות דומות - כמו תעשיית התעופה. כמעט לכל אחד בצוות ישנה התמחות באזור אחר - למשל קריפטוגרפיה, טכנולוגיות ענן או מערכות אמבדד. אני עצמי, לפני שנכנסתי לתחום אבטחת המידע, הייתי מפתח, ומהמקום הזה חשב לי לקחת את הצוות גם לכיוונים של פיתוח מאובטח."

"אנחנו רואים את עצמנו כמעין יחידת קומנדו - לכל אחד בצוות ההתמחות שלו, ויחד אנחנו יוצרים שלם שהוא גדול מסך חלקיו. כל אחד נותן אינפוט ותובנות מהעולמות שלו, ויחד אנחנו פותרים סוגיות סייבר סקויריטי."

כיצד נראית השגרה היומיומית של עובדי סיימוטיב?
"בחברה, כחלק מההכשרה שלנו, אנחנו לומדים איך בנוי הרכב, על יחידות המחשוב שבו ואיך הן מתקשרות זו עם זו - והחוצה מהרכב אל שרתי הענן. אנחנו עובדים קרוב מאוד ללקוח, ברמה יומיומית של מיילים ושיחות, ונמצאים בקשר עם בעלי תפקידים בכירים בפולקסווגן. כאמור, בימים כתיקונם יש גם קשר פנים אל פנים - ובערך אחת לחודש-חודש וחצי אנחנו נמצאים בגרמניה, בשוודיה או איטליה, איפה שצריך."

אילו עובדים אתם מחפשים?
"אנחנו מחפשים אנשים מוכשרים מאוד בתחומם, טכניים ואיכותיים, עם תשוקה לסקויריטי. כמובן שאנחנו מחפשים אנשים מנוסים מאוד בתעשיית הסייבר-סקויריטי, אבל מוכנים לקבל גם ג'וניורים, כל עוד הם אנשים חזקים טכנית שרוצים להיכנס לתחום חדש ומתפתח, שיש הרבה מה לעשות וללמוד בו. כאמור, אנחנו נמצאים בגדילה מואצת - והפעילות שלנו מתרחבת, בדגש על הפעילות מול ארה"ב. זה פרויקט שהולך להיות מעניין מאוד, מאחר שאנחנו נכנסים לתחומים חדשים בכל הקשור לענן. לתעשיית הרכב כמו שאנחנו מכירים אותה יש קצב משלה, אבל כעת כשחברת הרכב הופכות לחברות תוכנה, ושיקולי סייבר סקויריטי מנחים את הפיתוח בכל שלב - הקצב הופך למהיר יותר, עם פיתוח באג'ייל, ואיטרציות קצרות שמאפשרות לנו להתאים את הפתרונות לדרישות במהירות."

איטלקי וגם פרויקט גדול בארה"ב שנמצא בתחילת דרכו - כך שבימים כתיקונם, הרבה מהעובדים נמצאים בנסיעות ליעדים השונים.

"בארה"ב, אנו לוקחים חלק גדול בשותפות שפולקסווגן יצרה עם מיקרוסופט, במטרה להוביל את אבטחת פלטפורמת הענן של הרכבים העתידיים של פולקסווגן. השותפות הזו הולידה ארגון תוכנה חדש תחת חברת פולקסווגן, שיקום בסמוך למשרדי מיקרוסופט שברדמונד - ואנו צפויים להשתלב בהיבטים רבים של העבודה בו ולהנחות את הצוותים כיצד לפתח תוכנה בהלימה לצרכי אבטחת המידע, משלב העלאת הדרישות, עבור בארכיטקטורה, בעיצוב ובפיתוח, ועד הטסטים והניטור."

על איזו פעילות אחראי הצוות שלך?

"אנחנו פועלים מול הדרישות של פולקסווגן לפונקציונליות שונות ברכב - ובוחנים כיצד אפשר ליישם אותן על הצד הטוב ביותר בכל הנוגע לסייבר סקויריטי. לדוגמה, אם פולקסווגן רוצה שמשתמש יוכל לפתוח את דלתות הרכב באמצעות אפליקציה בטלפון, המשמעות היא מעורבות של שירות ענן. הבקשה נשלחת לענן, עוברת עיבוד ויורדת חזרה לרכב עם הוראה לפתוח דלתות. הצוות שלי עושה הערכת סיכונים ו-Review לארכיטקטורה של הדרישה של פולקסווגן."

"בצוות יש נכון לעכשיו חמישה אנשים - אבל בשנה הקרובה הוא צפוי להכפיל ואולי אף לשלש את עצמו."



נא להכיר: סיימוטיב

סיימוטיב הוקמה לפני 3.5 שנים, על ידי שלושה יוצאי שב"כ - יובל דיסקין, שהיה ראש השב"כ, וכן תמיר בכור וצפריר כץ, ששימשו בתפקידים טכנולוגיים בכירים ואף שירתו כראשי אגפים בארגון. החברה פועלת בשותפות אסטרטגית עם קבוצת פולקסווגן, המחזיקה ב-40% מסיימוטיב, ועובדת עם כמה מהמומחים המובילים שלה - ובהם פולקסווגן, אאודי ופורשה.

מעוניינים לעבוד בסיימוטיב?

שלחו מייל ל-hr@cymotive.com

כלי הרכב של ימינו, ובוודאי אלה שיעלו על הכבישים בעתיד, מתבססים יותר ויותר על טכנולוגיה הכוללת חיבור לאינטרנט - וגם היכולות האוטונומיות שלהם הולכות ומשתפרות. למעשה, מכונת העתיד תהיה "חוות שרתים על גלגלים", כפי שמגדיר זאת נדב הוס, מוביל צוות Automotive Cloud בחברת סיימוטיב הישראלית, המספקת שירותי סייבר סקויריטי ליצרניות הרכב. לדבריו, החיבוריות הגוברת לרשת חושפת את כלי הרכב לסיכונים חדשים. "ממש כפי שמחשבים ושרתים שמחוברים לאינטרנט חשופים למתקפות מצד גורמים עוינים, כך גם הרכבים שנוסעים וייסעו בעתיד על הכביש. אבל אם בעולם המחשבים הסכנה היא גניבת מידע או השבתת פעילות הארגון - ברכב, הסכנה שונה לחלוטין. אומנם עוד לא הגענו לאוטונומיות מלאה, אבל כשהשלב הזה יגיע - לאפשרות לשלוח לרכב פקודות מרחוק יהיו השלכות על חיי אדם."

בזמן שתעשיית הרכב צועדת אל עידן התחבורה החכמה, חברות הרכב משתנות אף הן - ומיצרניות המתמקדות בברזל, פח וגלגלים, נהפכות לחברות תוכנה המספקות שיחות - אותם יצרכו המשתמשים באמצעות כלי הרכב. "החברות כבר לא מספקות רק את כלי הרכב הפיזי - אלא גם את חווית השימוש כשנמצאים בו", אומר הוס.

כיצד מתחברת סיימוטיב למהפכה הזו?

"כשותפים אסטרטגיים של קבוצת פולקסווגן, אנחנו מעורבים כמעט בכל מה שקשור לסוגיות סייבר סקויריטי הנובעות מהעולם החדש הזה, שבו מכונות מתקשרות כל הזמן עם שרתים בענן - ולכן חשופות למתקפות. אנחנו מגדירים עצמנו כחברה סגולה - יש לנו גם צד אדום, הצד התוקף, שמאתר איומים קיימים ועתידיים, וגם צד כחול - שהוא הצד המגן, שבדוק כיצד אפשר לגונן על המערכות מהאיומים הללו, כאשר מתקיים שיתוף פעולה הדוק בין הצדדים."

"סיימוטיב היא חברה גלובלית, עם כ-120 עובדים שחובם אמנם בתל אביב - אבל אנחנו נמצאים הרבה על הקו. יש לנו חברה אחת בגרמניה, פעילות בחברת תוכנה שוודית שבבעלות פולקסווגן, עבודה מול מותג יוקרה

הכירו את הפתרון החדשני והפשוט לגלישה בטוחה ברשת

בחברות וארגונים שפעילותם גישה מבחינה ביטחונית ופיננסית, חווית הגלישה ברשת היא לא פעם איטית ונחותה. חברת Ericom הישראלית מציגה פתרון מאובטח וקל לשימוש - המגן על הגולשים מכל סוגי האיומים / גלעד הבר

עם זאת, השינויים האחרונים ב-Symantec - הנובעים מרכישתה בידי Broadcom בסוף השנה שעברה - עוררו בקרב חלק מלקוחותיה הישראלים תהיות לגבי השפעתה של האסטרטגיה המוצהרת של Broadcom, התמקדות בחברות הגדולות ביותר בעולם, על המשך השימוש שלהן בפתרון ה-Fireglass ברשותן.



גלעד הבר, סמנכ"ל מכירות Ericom Software

בארגונים רבים מדי, הפתרון הוא שימוש בדפדפן וירטואלי הדורש רישיונות יקרים של מייקרוסופט, וחשוב מכך - מספק גלישה באיכות נמוכה וחויית משתמש נחותה.

חווית גלישה אחרת

חשוב לדעת כי קיימת אפשרות אחרת - Remote Browser Isolation (RBI): פתרון חדשני, מאובטח ופשוט שצובר פופולריות בקרב עוד ועוד משתמשים המגלים את קיומו. בשנים האחרונות פיתחו כמה חברות פתרונות RBI, ביניהן שתי טוענות לכתר שזכו לשבחים בינלאומיים: Fireglass, שנרכשה על ידי Symantec ב-2018, ו-Ericom Software, שפיתחה את Ericom Shield.

עבור חברות וארגונים ישראליים, בייחוד במגזרי הפיננסים, הביטחון, השירותים הציבוריים והרפואה, גלישה בטוחה היא קונספט מוכר - אבל הוא לא היה תמיד אהוב במיוחד. לצד מספר מדינות באסיה, ובראשן סינגפור ויפן, נהוגים בישראל כמה מהתקנים המחמירים ביותר בעולם לבקרת הגישה לאינטרנט בקרב משתמשים במגזרים המתאפיינים ברמת סיכון גבוהה. למרבה המזל, במרבית המקרים כבר אין צורך לעזוב את עמדת העבודה כדי לגשת למחשב מבודד עם חיבור לאינטרנט הניצב בפינת המשרד. אך לרוע המזל,

בידוד מפני כל סוגי האיומים

כתוצאה מכך פנו רבים מן הארגונים האלה ל-Ericom, כדי ללמוד כיצד Ericom Shield עשוי להוות חלופה טובה יותר, שתספק את מלאו צורכי האבטחה הנוכחיים והעדכניים שלהם בצורה של בידוד האינטרנט. Ericom Shield יכולה להגן על הלקוחות מפני כל סוגי האיומים המועברים באמצעות האינטרנט - אתרי פשינג, אתרים לגניבת אישורים, קבצים זדוניים להורדה ועוד. כמו כן, כפתרון של "גלישה עם אפס אמון" (Zero Trust Browsing), היא מבודדת את כל התוכן מנקודות קצה, הן אלה הידועות כמסוכנות והן אלה שלא. לכן היא מגינה מפני איומים בלתי ידועים ואיומי "Zero Day" בדרכים שאינן אפשריות עבור פתרונות המתבססים על גילוי ולבסוף, מאחר ש-Ericom Shield משתלבת בקלות עם כל פתרונות הפרוקסי (למעשה, מכל ספק), ניתן להוסיף אותה בקלות לרשת האבטחה הקיימת שלכם.

זרם מדיה בטוח ואינטראקטיבי

בידוד מרוחק של דפדפנים פועל באמצעות העברת כל התוכן של אתרי אינטרנט, לרבות הורדות ואתרים הנפתחים מהודעות דוא"ל, דרך דפדפנים וירטואליים מרוחקים הנמצאים בענן או ב-DMZ. רק זרם מדיה בטוח ואינטראקטיבי לחלוטין נשלח לנקודות הקצה של המשתמשים. כאשר המשתמש מפסיק לגלוש באתר, הקונטיינר בו נמצא הדפדפן מושמד, ויחד עימו הנוזקות העלולות להימצא בו.

אם אתם חושבים שגלישה בטוחה היא פתרון מגושם, איטי ויקר שאף אחד לא היה רוצה בו אלמלא היה נדרש - הגיע הזמן שתבחנו אותו מחדש. תופתעו לגלות מה אינכם רואים!

התמונות באדיבות חברת Ericom



Ericom Shield. מגינה על הלקוחות מפני כל סוגי האיומים המועברים באמצעות האינטרנט

לפרטים נוספים:

sales@ericom.com • www.ericom.com

הכותב הוא סמנכ"ל מכירות ב-Ericom Software

המפתח לפטנטים חזקים עבור חברות בכלל וחברות סייבר בפרט / גרשון פניטש



עו"ד גרשון פניטש

צילום: יח"צ
פטנט אמריקאי מספר 9,521,154 למרבה הצער, להערכת מומחים רבים, הטעות של סייבר-סוד חוזרת על עצמה בלמעלה מ-90% מהמקרים בכל החברות, תהא אשר תהא הטכנולוגיה שבשימוש. אסטרטגיה עסקית המנוהלת על ידי אנשי העסקים חותרת לכיוון מסוים; ורישום פטנט, בהובלתם של אנשים טכניים, פונה לכיוון אחר. בבוא הזמן, כשמגיעה העת להשתמש בפטנטים כדי לחסום מתחרים, הפטנטים אינם יעילים. תנאי הכרחי לפטנט מוצלח הוא אפוא אימוץ גישה עסקית על ידי החברה

לפני ובמהלך הרישום. משמע, על התאגידים לזהות מבעוד מועד, עוד בטרם הגשת הפטנט, את המטרות העסקיות האמורות להיות מושגות באמצעות הפטנט. בשלב הבא, יש לבדוק את האסטרטגיה של כל פטנט פוטנציאלי כך שיהיה ניתן להעריך עד כמה פטנט זה עשוי לחסום מתחרים. חיוני לשתף בתהליך זה אנשי עסקים ואסטרטג פטנטים. אסטרטגיה שהיא בעלת סיכויים להשיג את המטרה העסקית מהווה "אור ירוק" לרישום הפטנט. מנגד, אם לא צפוי שתושג המטרה, ראוי לזנוח את הפטנט, מחוכם ככל שיהיה. בהתחשב בעובדה שהעלויות הגלובליות של משפחת פטנטים עומדות בקירוב על 200,000 דולר לאורך קיומה, על החברות להיות זהירות יותר בגישתן לרישום הפטנט. אחרת, וכפי שאנו נתקלים בכך לא אחת, החברות תתמודדנה עם הוצאות עתק על פטנטים, ללא יכולת לקבל דבר מה בתמורה. אמר לאחרונה מנכ"ל ישראל:

"נדרש לי זמן רב כדי להגיע לתובנה זו, אולם בכל הקשור לפטנטים, או לעשות את זה כמו שצריך, או לא לעשות זאת בכלל."

פטנט טכני במקום פטנט עקרוני. על ידי התמקדות בפתרון הטכני הספציפי של אבישי, השאיר מוטי פתח לאפשרות שמתחרה יגיע לאותה תוצאה מבלי להשתמש בפתרון טכני ספציפי זה. זו בהחלט לא אשמתו של מוטי. הוא פעל על פי הנחיותיו של אבישי. שורש הבעיה הוא שאבישי, שחושב כמהנדס, הנחה את מוטי לערוך פטנט טכני המגן בסופו של דבר על פתרון טכני צר.

כיצד במקום זאת, הייתה צריכה לפעול סייבר-סוד? במקרה זה, היה עליה לפתח פטנט אסטרטגי שבבסיסו עומד רצון לחסום בפני מתחרים את האפשרות

של גניבת זרם ההכנסות, במקום למנוע מהם גניבה של פתרון טכני ספציפי. לשם כך, ראוי היה לערב שני אנשי מקצוע: גיא המנכ"ל, או איש מקצוע אחר בעל גישה

מדוע לחברות מסוימות יש מוניטין של מפתחות פטנטים חזקים, בעוד שלאחרות לא? מדוע חברות מסוימות דורשות תמלוגים בסך מיליוני דולרים בגין הפטנטים שלהן, בעוד שבקרב חברות אחרות, להבדיל, הפטנטים מהווים חלק משורת ההוצאות בדוח המאזן שלהן, ותו לא? ומדוע פטנטים של חברות מסוימות מבריחים מתחרים, כשמנגד פטנטים של חברות אחרות לא גורמים להם להניד עפעף?

התשובה היא שלא כל הפטנטים נולדו שווים. כדי להבין מדוע כך הם פני הדברים, וכיצד אתם, בתור מנהלי תאגיד, יכולים להזניק את ערכה של החברה באמצעות מערך הפטנטים שלה, הבה ניקח לדוגמה חברת הייטק היפותטית בתחום הסייבר בשם סייבר-סוד. סייבר-סוד פותרת את הבעיה של וירוסים ותולעי מחשב החודרים דרך פורטים שאינם מאושרים. אבישי, מנהל הטכנולוגיות הראשי, הוא אדם מבריק שהגה פתרון אלגנטי לבעיה

זו: לערוך רשימה של פורטים מאושרים, תוך קביעת קיומה של פעילות חשודה על ידי בדיקת זרם המידע העובר דרך פורטים שאינם מופיעים ברשימת הפורטים המאושרים. גיא המנכ"ל, המודע לכך שמשקיעים מתוחכמים תמיד שואלים על פטנטים, ביקש מאבישי להיפגש עם מוטי, עורך הפטנטים של החברה. אבישי נעתר לכך ושוחח עם מוטי, עורך פטנטים מבריק שהפגין יכולת מקצועית לחן בעניין עם

אבישי. מוטי ניסח פטנט מפורט להפליא. בדיוק כפי שאבישי תיאר זאת בפניו, מוטי הגדיר את ההמצאה כסדרות של מתגים, נתבים, רכזות וגשרים. כעבור שנתיים, הפטנט התקבל, והחברה ערכה מסיבה לכבוד הישגו של אבישי. אלא שאיש לא הבין שהפטנט הוא גרוע. מדוע? משום שישנן שלל דרכים להגיע לאותו פתרון מבלי לארגן את המתגים, הנתבים, הרכזות והגשרים באופן שנדרש במסגרת הפטנט. מתחרה שיאהב את הפתרון של סייבר-סוד יאמר לבטח: "רעיון מצוין! אני יכול להגיע לאותה תוצאה על ידי סידור אחר של המרכיבים. וכשאעשה זאת, לא אצטרך לחשוש מהפטנט של סייבר-סוד". היכן טעתה חברת סייבר-סוד? ובכן, החברה פיתחה



עסקית מובהקת, כשלצדו איש שיווק. אילו סייבר-סוד הייתה מאמצת גישה עסקית לפטנט שלה, במקום גישה טכנית גרידא, היא הייתה מבינה שבמקום למקד את הפטנט בארגון המתגים, הנתבים, הרכזות והגשרים, מוטב לרשום פטנט כללי יותר על מערכת המבוססת על רשימת פורטים מאושרים לצורך בדיקת פעילות חשודה בפורטים שאינם מאושרים. פטנט מסוג זה היה מונע מכל אחד אחר להשתמש בפתרון על בסיס אותו עקרון, ללא קשר לארגון הטכני של המרכיבים.

אם למקרא הסבר זה, תגובתכם היא: "שטויות, לא ניתן לרשום פטנט כללי כזה", חשבו שוב. זה בדיוק הפטנט שחברת Hewlett Packard רשמה. אתם מוזמנים לבדוק:

גרשון פניטש הוא שותף בפינגן, אחד המשרדים המובילים בעולם בתחום הקניין הרוחני, ומנהל את קבוצת תכנון הפטנטים האסטרטגי של המשרד ואת הפרקטיקה שלו בישראל. גרשון עבד עם למעלה מ-160 מהחברות המובילות בישראל וסייע להן להגדיל את הערכת השווי שלהן באמצעות תכנון פטנטים אסטרטגי, ולטעון טענות ולהתגונן במסגרת תביעות להפרת פטנטים בבתי משפט בארה"ב. גרשון מרצה בפקולטה לבית הספר למנהל עסקים באוניברסיטת תל אביב, שם הוא זכה בשלוש השנים האחרונות בפרס המרצה המצטיין של בית הספר, על קורס באסטרטגיית פטנטים שהוא מלמד במסגרת לימודי תואר שני במנהל עסקים (MBA).

לפרטים נוספים:

IsraellInfo@Finnegan.com
Finnegan.co.il / Finnegan.com



סרקו את הקוד כדי לצפות בסרטון על גיבוש אסטרטגיית פטנטים



סרקו את הקוד כדי לצפות בסרטון מתוך סייברטק על הגנה על פטנטים

המדינה תקים בבאר שבע מרחב סייבר לניסויים בתחבורה חכמה

ותחבורה חכמה בחברת נתיבי איילון. "מי שמצליח לחדור למרכז ניהול תנועה, יכול לשתק ערים ומטרופולינים תוך זמן קצר, ולגרום לנזקים גדולים במיוחד".

לפי התוכנית, במרחב החדש יפותחו יכולות תקיפה וניסוי של מערכות תחבורה חכמה וכלי רכב - והוא יהווה זירת ניסויים עבור חברות שירצו לבדוק את עמידות המערכות שלהן בפני תקיפות סייבר. חוקרים ואנשי הסייבר יעבירו את המערכות מסכת של ניסויים ותקיפות כדי למצוא נקודות תורפה וחולשות. לבסוף, תוענק לחברות מעין חותמת כשרות, שאמורה - כפי שמבטיחים בנתיבי איילון - לעזור לאותן חברות למכור את הטכנולוגיה שלהן ברחבי העולם.

החברות שיתפעלו וייהנו משותפי המרחב החדש ייבחרו במרכז, כאשר הבעלות תחולק חצי חצי בין המדינה לבין החברות שייבחרו. כחלק מההכנה למרכז זה חברת נתיבי איילון ונציגי משרד התחבורה ומערך הסייבר, נפגשו עם חברות מובילות בתעשיית הרכב הישראלית והעולמית וגם עם נציגים של חברות ביטחוניות.

המרחב, שאמור להתחיל לפעול בעוד כשנה, יתוקצב בסכום של עד 16 מיליון שקל - 8 מיליון שקל מצד המדינה ו-8 מיליון שקל מצד החברה שתיבחר במרכז. הכוונה היא שהמרחב, עם הקמתו בפועל והשקת היכולות שלו, יפעל כמעין מעניק תקן בפועל למערכות אשר ישולבו בהליך הקבלה של הציוד בחברות התשתית, על מנת לשמור על אבטחת מידע באותן מערכות תחבורה חכמה ציבוריות.

צילום: יח"צ



אלדי שחם, ראש אגף ניסויים ותחבורה חכמה בחברת נתיבי איילון

החידוש בהקמת המרחב הוא העובדה שלמעשה מדובר בהכרה בצורך של ממשלות (וחברות) לוודא שכולם מוגנים, לרבות התשתיות והמערכות הממוחשבות התומכות בהן. "ההגנה על מרכזי בקרה וניהול תנועה הופכת להיות משמעותית מאוד", אומר אלדי שחם, ראש אגף ניסויים

במרחב החדש יפותחו יכולות הגנה, תקיפה וניסוי של מערכות תחבורה חכמה וכלי רכב. במקביל, חברות ישראליות ובינלאומיות יוכלו לבדוק את עמידות המערכות שלהן בפני תקיפות סייבר

משרד התחבורה, חברת נתיבי איילון ומערך הסייבר הלאומי יקימו בבאר שבע מרחב סייבר לניסויים בתחבורה חכמה, שבמסגרתו תתבצע פעילות שתייצר תשתית תקינה לסייבר לתחבורה חכמה, מתוך כוונה להשפיע על התקינה הבינלאומית לכשתתפתח.

ישראל - הראשונה בעולם שמטילה רגולציית סייבר על מפעלי חומרים מסוכנים

רצפת הייצור במפעל וכיצד צדדי ג' בשרשרת האספקה 'עוזרים' להאקרים להיכנס אליו - למשל, באמצעות התחברות ישירה של ספקים מחו"ל לבקרים תעשייתיים, כי אותן חברות לא מאפשרות ללקוח לתחזק לבד את הבקרים המשתתפים בתהליך. במקרים רבים, הגישה מרוחק לא מתבצעת לפי פרקטיקות מאובטחות, בלשון

המעטה. "אנחנו הרגולטור הראשון בעולם שמנחה בנושא סייבר את תעשיית החומרים המסוכנים באופן ספציפי", סיכם. "אנחנו מנפיקים היתרי רעלים ל-4,262 עסקים ומנחים אותם בסייבר: מפעלים לייצור חומרים מסוכנים, בתי חולים, תעשיות ביטחוניות, פרמצבטיקה, דשנים ועוד. אי ציות להיתר הרעלים הוא עבירה פלילית שגוררת גם קנסות כבדים, ובמקרים קיצוניים אף מביאה לביטול ההיתר. אנחנו משתמשים בכלי חזק זה כדי להכניס דרישות סייבר למפעלי החומרים המסוכנים".



צילום: יח"צ

הן מופעלות ומבוקרות על ידי מערכות ממוחשבות כגון HMI (עמדות אדם-מכונה), בקרים, חיישנים ורכיבי שטח. לכן, אירוע סייבר במערכות אלה עלול לגרום לכשל או לשיבוש במערכות הממוחשבות שמטפלות בחומרים מסוכנים, ולהוביל לפליטת גזים מסוכנים, פיצוץ חומר מסוכן, דליקה של חומרים מסוכנים ועוד", אמר.

שביט סיפר כי "מדי יום אנשינו מסיירים בשטח, במפעלי חומרים מסוכנים, בדגש על מחשוב ברצפת הייצור. הם מסבירים לנציגי המפעלים, בליווי המחשבות, איך התוקף יכול לתקוף את רשת

יוסי שביט, ראש יחידת הסייבר בתעשייה, אגף חירום וסייבר

יחידת הסייבר לתעשייה של המשרד להגנת הסביבה פיתחה מתודולוגיה ייחודית לעריכת סקרי סיכונים במפעלים, על מנת למנוע כשלים במערכות

ישראל רושמת תקדים - והיא המדינה הראשונה בעולם שהחליטה להחיל רגולציית סייבר על מפעלים לחומרים מסוכנים. זאת, כחלק מפעילותה של יחידת הסייבר לתעשייה, שהוקמה במשרד להגנת הסביבה. תפקיד היחידה הוא להנחות גופים כגון מפעלים המחזיקים בחומרים מסוכנים, כיצד להיערך לתקיפות סייבר העוללות לגרום לדליפת חומרים מסוכנים, ועקב כך לפגוע בסביבה ובבריאות הציבור. היחידה פועלת תחת אגף חירום וסייבר במשרד להגנת הסביבה, עם הנחיה מקצועית של מערך הסייבר הלאומי ותוך שיתוף פעולה עם התאחדות התעשיינים. לדברי ראש היחידה, יוסי שביט, "פיתחנו מתודולוגיה ייחודית, ראשונה מסוגה. המתודולוגיה עוסקת בעריכת סקרי סיכונים במפעלים שמחזיקים חומרים מסוכנים ונשענת על ניהול הסיכונים מתורת ההגנה של מערך הסייבר". לדברי שביט, "כשל במערכות הייצור עקב תקיפת סייבר על המערכות הממוחשבות של המפעל עלול לגרום לאירוע חומרים מסוכנים, לפגיעה בבריאות הציבור ובסביבה. חלק ממערכות הייצור מכילות חומרים מסוכנים,

		.7	.6	.5	.4	.3		.2	.1
.10						.9			.8
		.13					.12		.11
				.15					.14
	.18	.17							.16
		.20							.19
			.25	.24	.23		.22		.21
.28				.27			.26		
					.30			.29	
	.33					.32			.31
		.35							.34

האותיות הצבועות משתלבות למושג בתחום (7.3)

אופקי

1. א' סמך בכל עת על? ע. בפשטות: שמירה על הנתונים (4,5)
8. בתוך השפה שמדברים שם, מסתתר המטבע. כשחוזר נרו יאיר (ר"ת)
9. המרחב הווירטואלי כפשוטו רומז בשמו להגנה מהתקפות על המרחב הזה.
11. אות הניצחון + שם דמות ב'חברים', מדבק בפתיחת קבצים וגם בעיטוש ולחיצת יד.
13. משני הכוונים משתמש בנשק לפגוע בחיים/רכוש.
14. תנועת רוח עם חיה שמטמינה ראשה בעת סכנה... פשפשש כדי להרוות את הצד הלא פיזי (3.5)
16. שור + סוג של חולצה + סיומת רבות = בשמירה על זה עסקינן.
17. 2 ראשונות: כלב המיילל בלילה, 2 אחרונות: עוף דורס וביחד דרגה בראשות האוכפת.
19. העניין האחר הזה הוא עבודת אלילים. חוזר כאקדמיה בעיר הקודש והכל בראשי תיבות.
20. שואל הקונה את המוכר ובעצם מתגעגע וכוסף.
21. משורר עברי בראשי תיבות חוזר כמותג ספורט עברי.
23. ניו יורק בראשי תיבות? טיול בלעז בעמודה וביחד שמירה והשגחה.
26. כלי בשח-מט אך וחוזר אויב
27. חותכת בפה + 80 בגימטריה, טעם שצבעו לבן.
29. חיה גדולה חובבת מתוק חוזרת כאריג.
30. בטעות כתוב כ: העובד אדמה, בפועל פצחן.
31. האדון האיטלקי בתוך זכרון יעקב? בעל כוונת רשע כמו התוכנות המזיקות.
33. שבטים אינדיאנים או מטבע צרפתי עתיק.
34. בלעז לא! + נשמעות נקיות, בפועל מביאות נזק גדול כשחוזרות למרחב הרשתי.
35. כשיורד מספיק כזה אפשר לחזור עליו בסקי .

אנכי

1. סכנה נוכחית שמטופלת על ידי החברות במוסף הזה. (4,4)
2. שם פרטי של שני המתמודדים שרב עם המלאך ומנצח? צאצא לעם העברי (5,2).
3. פרטי מידע נסתרים כמו אנשים שאינם כשירים וזקוקים לאפטרופוס (כתיב מלא).
4. תניעו מפה הוא בעצם חוק במשחק המלכים המחייב אתכם אם נגעתם (כתיב מלא)
5. על איזו להקה בריטית מדובר?
6. מספר השבטים חוזר בתוכי.
7. חצים דמי לא יחרץ עבור קבצים (4,5).
10. קוראת לגנב וגם להאקר.
12. דרגה שכיחה בצבא הישראלי נשמעת מרכזית במרוקו.
15. נמל תעופה בראשי תיבות שחוזר ומיילל.
18. בתוך כלי מאור נמצאת זו שמתחילה שאלות, אל תשאלי זו פשוט חיית חברבורות.
22. מתגורר עם מילת לעג, ממש יאיר: צייר, סופר וסטיריקן ותיק.
24. ירים את הכלה.
25. תחילתו נשמע כמו חית בר והוא רכב לחימה על שרשראות שחוזר מותג למעשנים.
28. קריאה לסוס + האות השלישית, התחזות להשגת פרטים אישיים.
29. רמטכ"ל ז"ל או שחקן כדורגל ז"ל? שיכול אותיות מלך תנ"כי.
30. בעברם, חוזרים דרך.
31. סוג של פילוסופיה יפנית.
32. קיצור של סימן פיסוק? נשמע חיובי כשחוזר לפחות עבור הביצים.
33. יש כזה של בריאות, ספורט או בדרך לשוק.

פתרונות

גאוגרם מום: סומטט אמזט

דמ' עע' ז'ג

זע' לנ' ג' ה' ו' ז' ח' ט' י' י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט

י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט

י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט

לואט:

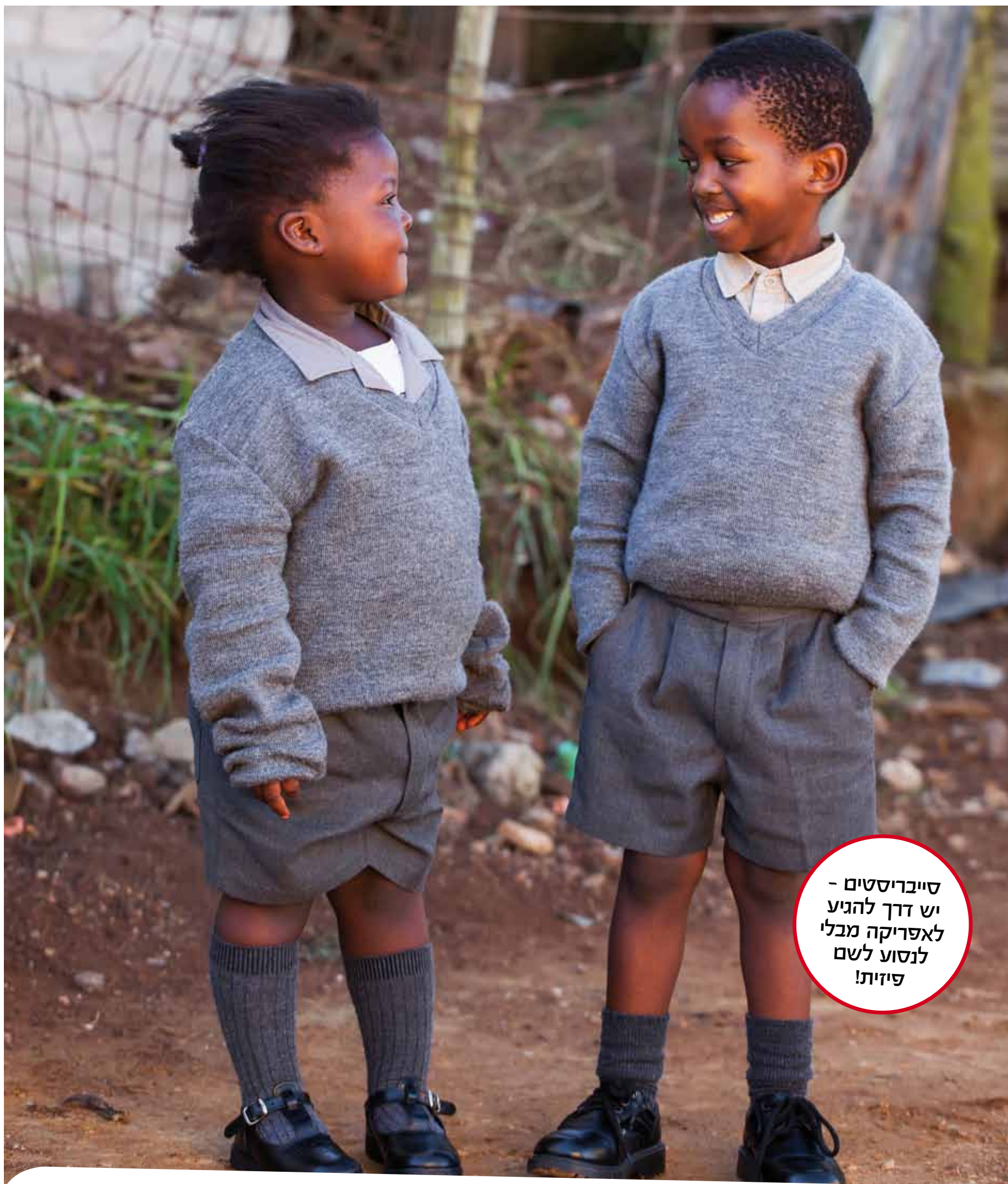
זע' ז'ג

י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט

י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט

י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט י"א י"ב י"ג י"ד י"ה י"ו י"ז י"ח י"ט

לואט:



סויבריסטים -
יש דרך להגיע
לאפריקה מבלי
לנסוע לשם
פיזית!

בואו לחשוף את פעילותכם ולאפשר שיתופי פעולה עם המגזר העסקי-תעשייתי במדינות אפריקה, וקחו חלק במדריך עסקים ישראל-אפריקה

המדריך יופץ במאי-יוני ל-11 השגרירויות הישראליות ביבשת ומהן לארגונים מקומיים ולעשרות אלפי עסקים וארגונים שזקוקים למה שיש לכם להציע.

מעניין? צרו קשר ב- lnbal@paprikap.com או ב-052-3232130

נ.ב. המדריך מחולק לסקטורים של תעשייה ומתאים גם לסוגי תעשיות אחרים. דברו איתנו