Interconnect
Cloud Services

מבוא לאיומי הסייבר המודרניים לעסקים

מוגש על ידי אינטרקונקט שירותי ענן

https://interconnect.co.il

ספטמבר 2021

אבי בלושטיין, CTO

כל הזכויות שמורות לאינטרקונקט. אין להעתיק או לעשות שימוש בתכני מצגת זו ואין להכניס בה כל שינוי.

Interconnect
Cloud Services

נעים להכיר !

אינטרקונקט היא ספק ענן פרמיום בישראל

מערכות החברה מספקות תשתית מהירה, שרידה, יציבה ומאובטחת לארגונים רבים בישראל – מקטנים ועד ענקיים ברמת בנקים וחברות אשראי.

אבי בלושטיין, CTO

בעל ותק של עשרות שנים בתחום הנדסת תוכנה ומערכת, ניהול מוצר וניהול פיתוח בהיי-טק, תשתיות תקשורת, עולם ה-Telecom וה-IT, עולם ה-FinTech וה-Big Data, עולם היישומים המוניציפליים, תחום ה-Data Centers, מערכי שרתים HPC ועיבוד נתונים מהיר, אבטחת מידע ועוד...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

נתחיל ב-"למה" ?

- **כל אחד מכם יודע לשמור על הבית והמשרד שלו**
  מגדרים את הבית. נועלים דלתות. מתקינים סורגים. מתקינים אזעקה. מתקינים מצלמות. מפעילים מוקד. עורכים ביטוח תכולה...

- **כל אחד מכם יודע לשמור על הרכב שלו**
  נועלים דלתות. מתקינים אזעקה. מתקינים משבת. מתקינים מערכת איתור. עורכים ביטוח בפני גניבה...

- **מיעוטכם יודע לשמור על הטלפון או המחשב שלכם**
  ולמה? כי את היתר חינכו ולימדו אתכם מגיל צעיר והאיומים מוחשיים יותר...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

נמשיך ב-"בפני מי" ?

- **בבית אתם מתגוננים בפני גנבי רכוש**
  מטרתם לפרוץ לכם הביתה ולגנוב כסף מזומן וחפצים יקרי ערך...

- **ברכב אתם מתגוננים בפני גנבי רכוש**
  מטרתם לפרוץ לכם לרכב ולגנוב תיקים, חלקים מהרכב או הרכב כולו...

- **בעולם הדיגיטלי אתם מתגוננים בפני גנבי מידע**
  מטרתם לגנוב מידע יקר ערך או לגנוב כספים באופן ישיר או במרמה...

כאן האיום אינו גלוי לעין, הדרכים לפגוע בכם מגוונות יותר וגרוע מכך – ברוב המקרים לא תדעו שהפורץ שם עד אשר סיים מלאכתו בניחותא.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect Cloud Services

כדי להבין את ההווה צריך להבין את העבר

עולם הסייבר עובר התפתחות הדרגתית

הפריצות הלכו והשתכללו מגרימת נזק וקונדס למעשי שוד וגניבה.
אופן הפריצה הלך והשתכלל מקוד טיפש למערכת AI לומדת.
ההגנות בפני פריצה הלכו והשתכללו בהתאמה.
הפורצים הלכו ושכללו את השיטות עוד יותר...

בכדי שתוכלו להבין כיצד הסיכונים הלכו וגדלו נסקור את התפתחות עולם הסייבר והנוזקות מקדמת דנן.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

הבה נחזור מעט בזמן...

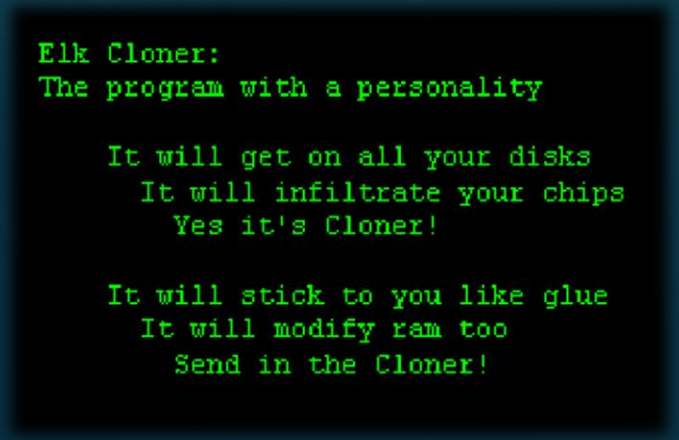
בתחילת דרכו של עולם המחשוב הפורצים היו מדינתיים

עיקר המאמץ והמשאבים שעמדו לרשות גורמים היו ברמה הממשלתית

ה-'האקרים' הראשונים התמקדו בפיראטיות ובבדיחות

הפריצות הראשונות בין שנות ה-70 לשנות ה-90 התמקדו בעיקר ברישוי תוכנה אם למטרה כלכלית ואם כמשחקי כבוד בין קבוצות צעירים מתחרות.

הוירוסים והנוזקות הראשונות היו בדיחות לא מזיקות שהוצמדו למשחקים.
הוירוסים הבאים שהחלו לצוץ כבר מחקו דיסקים קשיחים במטרה לגרום נזק נבזי ללא כל תמורה.



זהו השלב שבו זה כבר חדל להיות בדיחה.

כאן העולם החל לחוש ולהיחשף לחומרת הנזק.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

מה עוד היה קורה אז...

מערכות מידע היו חשופות לחלוטין לאינטרנט

נאיביות של גופים הביאה לחשיפת רשתות תקשורת באופן ישיר, למטרה טובה או מתוך חוסר מודעות, בפני תוקפים שיכלו לתקוף אותן כל אימת שחפצו.

שיטת התקיפה הנפוצה ביותר היתה Brute Force

כשמה כן היא – התפרצות 'ברוטלית' ונטולת עידון למערכת **דרך ניסוי כמות גדולה של צירופים שונים של סיסמאות עד הצלחה**. שיטה זו עובדת לא רע אפילו כיום !

שיטה נוספת היתה ניצול הצפנות חלשות ופרצות

שכן באופן טבעי הטכנולוגיות היו בוסר והמודעות היתה מוגבלת...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

מהי נוזקה ?

- **תוכנה לא רצויה** (Unwanted Application)

זוהי תוכנה המותקנת במכשיר שלכם באופן גלוי או סמוי **ומטרתה שונה ממה שאתם מצפים שתעשה**. הנזק מתוכנה כזו הוא חדירה לפרטיות, הטרדת פרסומות והשפעה על אופן השימוש שלכם במחשב או בטלפון ללא נזק מהותי.

- **נוזקה** (Malware)

זוהי תוכנה שמטרתה באופן מוחלט להסב לכם ולסביבתכם נזק של ממש – אם דרך פגיעה במידע או בציוד (למשל באיראן) ואם דרך גניבת מידע וגרימת נזק ממוני בדרך של חשיפת מידע או גניבת כספים בדרך של תחבולה.

תוכנה לא רצויה מעיקה.
נוזקה פוגעת באופן ממשי.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

ביצד פועלת נוזקה ?

נוזקה פועלת בסתר

העקרון הבסיסי של כל גנב הוא פעולה בחשאי. זהו גם העקרון שבו פועלת הנוזקה ומטרתה לא להתגלות – בוודאי טרם כניסתה לפעולה.

נוזקה תופסת טרמפ על נשא

הנוזקה לרוב אינה תוכנה עצמאית אלא חבילת קוד זדוני המולבשת על נשא – שיכול להיות קובץ תוכנה אך גם קבצים מסוגים אחרים כמו קבצי Word תמימים למראה. זה כמובן מקשה על גילויה.

הנוזקה פועלת להפיץ עצמה

מרגע פעולתה היא לרוב פועלת להדבקת עוד קורבנות בדרכים מגוונות.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

הבה נחזור שוב בזמן...

ההתקפות בשנות ה-90 ותחילת שנות ה-2000

התבססו בעיקר על הפצת וירוסים ותולעים שרובם הגיעו מתוכנות נגועות וכן התקפות על ממשקים הפתוחים לרשת האינטרנט, שהלכה והפכה פופולארית.

הוירוס או התולעת היו תוכנות המשכפלות עצמן במהירות

הוירוסים הופצו במטרה להזיק ממחשב למחשב דרך דיסקטים נגועים, קבצים נגועים הנשלחים בדואר אלקטרוני ודרך רשת התקשורת המקומית.

התולעים דילגו עצמאית דרך פרצות שונות ברשת ומשם הדביקו עוד ועוד מחשבים ועוד ועוד רשתות אחרות.

בשני המקרים מדובר בתוכנה זדונית הפועלת בשקט מבלי שתחושו בה.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

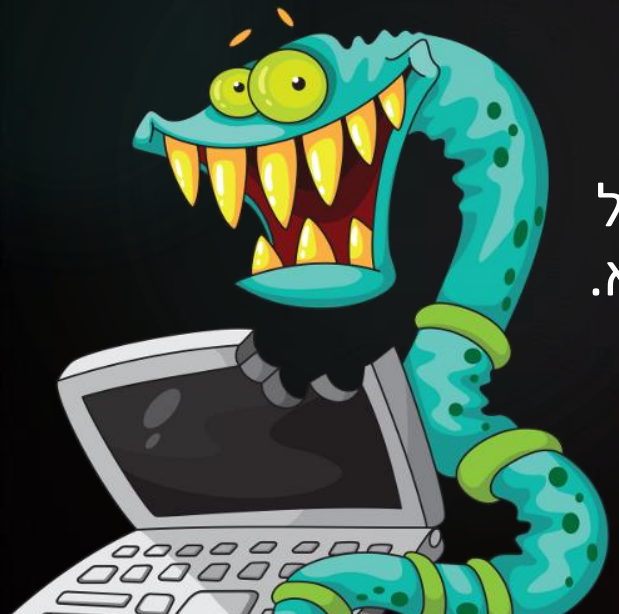
מהו עקרון פעולתם ?

הוירוסים הועברו מקורבן לקורבן בתום לב

קוד המקור של הוירוס היה לרוב מולבש על קבצי EXE או DLL והיה מופעל **על ידי המשתמש** עם הפעלת הקובץ או התוכנה, רץ ברקע ומבצע את זממו תוך הדבקת עוד קבצים במחשב, בכוננים חיצוניים וברשת ככל שניתן. הדורות המשוכללים אף היו שולחים דואר אלקטרוני נגוע מתוך תוכנות הדוא"ל בשמכם.

התולעים נעו עצמאית ברשת

בניגוד לוירוסים, התולעים היו קוד שהופעל **על ידי תוקף** לשם ניצול פרצות בשרתים ברשת ומרגע חדירתן היו ממשיכות לפעול עצמאית לביצוע הנזק ולהדבקת שרתים נוספים ללא צורך בנשא.



ההבדל העיקרי בין השניים היה נעוץ באופן העברת הנוזקה.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

מה היו ההגנות שעמדו לרשותנו אז ?

מי לא מכיר את האנטי-וירוס ?

ששמו מתאר את תפקידו בכל שהאיומים שהתמודדו עמם דאז היו וירוסים בלבד. תוכנות אלו סרקו את הקבצים וחיפשו **וירוסים מוכרים בלבד לפי קוד המקור שלהם שהוטבע בקובץ והיה יחסית קל לזיהוי (זיהוי 'חתימה').**

מי לא שמע על צ'ק-פוינט ?

חומות האש – ששמה של החברה נקשר בהן דאז – היו אמצעי הגנה חדש שעקרון פעולתו היה בראש ובראשונה **שליטה על התקשורת הנכנסת והיוצאת והגבלת הגישה לרשת מבחוץ.**

נשמע טריוויאלי? לקח לעולם זמן להבין זאת...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

מתחילים להתקרב לימינו...

הפורצים החלו להשתכלל...

ככל שהאנטי-וירוסים השתכללו – הפורצים הבינו שצריך להשקיע יותר.

מטרות הפריצה החלו להשתנות...

הפריצות הראשונות עסקו בגרימת נזק והפחדה.
הפריצות החדשות החלו כבר לשמש לגניבת מידע משרתים ולגניבת סיסמאות או פריצה לחשבונות בנק.

זהו השלב שבו התקנאו הפורצים בחברות האנטי-וירוס המרוויחות הון על גבם וגם להם הרי מגיע נתח מהעוגה...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

הבירו את הסוס הטרויאני

החל את דרכו במיתולוגיה היוונית

עקרון פעולתו מאוד פשוט – קיבלתם מתנה בלשהי הכוללת מרכיב שלא כל כך ציפיתם או רציתם לקבל (נוזקה).

העקרון היה דומה לוירוס אך אופן ההדבקה היה שונה

בניגוד לוירוסים שהדביקו קבצי EXE של תוכנות – סוסים טרויאנים היו מסתתרים בתוכנות חינמיות, בקבצי פריצה של Office או Windows וגרוע מכל – במסמכי Word או מסמכי Excel שהכילו קוד VB זדוני.

להבדיל מוירוס הסוס הטרויאני היה מופעל באופן יזום על ידכם, בתום לב, מבלי שידעתם שברקע הוא הכיל נוזקה מוסתרת וסמויה נוסף על הערך הגלוי שלו שאליו אתם כן מודעים והתפתיתם לקבל.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

אילו נוזקות הכילו הטרויאנים ?

הדרג הקל : מזריקי פרסומות

מונטיזציה דרך החדרת פרסומות קופצות לדפדפנים ו-'חטיפת תוצאות חיפוש' (Search Hijacking) למטרת רווח מקליקים. **מעצבן אבל סביל.**

בדרג הבינוני : גניבת מסמכים

העלאת התוכן של המחשבים שלכם או הטלפונים אל שרתי התוקף במטרה לגנוב מידע מסחרי או סתם בריית מידע למטרות פרסום. **מזיק אבל ברמה מוגבלת (למעט מידע סודי שנגנב כמובן).**

ברובד החמור : שליטה מרחוק וגישה למערכות

שליטה מלאה במחשבים ושרתים מרחוק ללא ידיעתכם ו/או הקלטת ההקלדות שלכם במקלדת **לשם גניבת סיסמאות ופרטי גישה למערכות רגישות !**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

ביצד השתכללו ההגנות ?

האנטי-וירוס כעת הפך גם לאנטי טרויאני

המערכות השתכללו מזיהוי של 'חתימות' ידועות לבחינה – אמנם עודנה שטחית – של התנהגות קבצים ויישומים **בניסיון להבין האם הם מתנהגים באופן חשוד או ניגשים למקומות רגישים.**

חומות האש החלו להשתכלל מעבר לחסימות בלבד

מושגים דוגמת **Data Leak Prevention** או **Intrusion Detection** החלו להפוך סטנדרטיים, אנטי-וירוסים החלו להיות מיושמים כבר בחומת האש והמושג "חומת אש" הלך והתעצב לקראת קונספטים חדשים של הגנה משולבת.... **Next Generation**.

המהפך הגדול בתעשיה היה תחילת ההבנה כי כנראה שהתוקף כבר חדר ומעבר ממניעה לזיהוי.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

ואז הגיע הסמארטפון...

ועמו הרשתות החברתיות ומגוון השירותים המקוונים

מה שהיווה כר פורה ומופלא להפצת נוזקות במגוון פורמטים, מגוון אמצעי הפצה, מגוון שיטות וגרוע מכל – מגוון מכשירים...

האיום הופך רב-ממדי

העקרון הבסיסי בהגנה בכל תחום הוא תחימת האזור המוגן והגדרת גבולותיו.

עם הגעת הסמארטפונים והתפתחות המחשבים הניידים והטאבלטים – נפרצו גבולות הגזרה וכעת ההתקפה יכולה להיות בכל מקום, באמצעים שונים, איננה צריכה להיות ממוקדת רק במשרד ויכולה להתרחש בכל שעה – גם בבית.

זהו השלב שבו ההתקפה עברה להיות על כל מהלך חייכם.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

ברוכים הבאים אל העתיד

כל מכשיר המצוי בשימושכם כיום נתון להתקפה

כל המכשירים כיום מבוססים מערכות הפעלה פגיעות **והמצב רק מחמיר עם כניסת תחום ה-**IoT. משעון יד חכם דרך רכב אוטונומי, מכונת הכביסה וכלה ברמקול BT.

כל תמונה וכל קישור שאתם מקבלים מסוכנים להחריד

רמת ההתקפות כיום כה משוכללת שמספיק שתפתחו תמונה לכאורה או אפילו תענו לשיחת וידאו ב-WhatsApp בכדי להדביק לכם את המכשיר בנוזקה ומשם את המחשב שלכם בבית ומשם את המחשב במשרד.

הלחץ הגובר לחדשנות מביא לפגמים רבים במוצרים

כמות הפיצ'רים גדלה בעוד שכמות הבדיקות מצטמצמת ומוצרים רבים מוצאים דרכם לשוק 'לא מבושלים' בלשון המעטה – בעיקר בעידן הבועה.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

ברוכים הבאים אל העתיד

אופני ההתקפה השתכללו ומשלבים טכניקות תעתוע

החל מדואר אלקטרוני מתחזה דרך הודעות SMS מטעות ובלה בפרופילים מזויפים ברשתות חברתיות המתעתעים בכם לחשוב שמסמך שקיבלתם הוא הצעת עבודה. **תחום זה קרוי "הנדסה חברתית".**

ההתקפות הפכו לאמצעי כלכלי בשוק של מיליארדים

הנוזקות למטרת נזק פרחו מן העולם. **כיום מטרת ההתקפות היא כלכלית לחלוטין והן הפכו ממוסדות בידי חברות מבוססות וגופים מדיניים.**

שיטות הגילוי והמניעה הפכו קשות ביותר

עם מיסוד ההתקפות וההשקעה במו"פ על ידי התוקפים הפכה מלאכת הגילוי קשה במיוחד **ומוחות מבריקים רבים מגיעים לצד הלא נכון של המתרס.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

הידעת שאת/ה סוס טרויאני?

- **כל אחד מכם הוא כעת סוס-טרויאני מהלך פוטנציאלי**
  כל מכשיר שאתם נושאים בידיכם, בתיקכם או עונדים על ידכם הוא פצצה מתקתקת המחכה להתפוצץ מבלי שאתם מודעים לכך.
  מטען הנפץ הדיגיטלי יכול לשבת שם ולהמתין לשעת הכושר גם שנה ויותר.

- **כל אחד מכם הוא חייל בזירת קרב גדולה מכם מהותית.**
  כל אחד מכם אחראי לשמור על עצמו ועל אחרים **וכל טעות שלכם עשויה להכריע את כל המערכה.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

אם לא התייאשתם עוד...

הגענו לתכלס...

התגוננות מתחילה בהבנה והכרת האיומים

לא בכדי מצגת זו סוקרת בהדרגה את התפתחות האיומים.

התגוננות מתחילה ונגמרת בהפעלת הראש

אין ארוחות חינם, אין מתנות מהגרלה של קוקה-קולה, אין זכיה בלוטו הספרדי
ואם זה נראה כמו ברווז, נשמע כמו ברווז והולך כמו ברווז – זה סוס טרויאני !

התגוננות מתחילה בחוסר אמון מוחלט בכולם

אל תסמכו על כך שאחרים ידאגו לכם ואל תסמכו על כך שמישהו אחר בדק עבורכם או שמי ששלח לכם הרגע מסמך הוא מי שאתם חושבים שהוא.
המצב כיום מטורף וכל חבר או עמית לעבודה עשוי להיות תוקף במסווה.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

מהם רבדי ההגנה הבסיסיים

שליטה בתקשורת הנכנסת והיוצאת

באמצעות השיטה הקלאסית של חומת האש ובשילוב אמצעים מתקדמים יותר דוגמת DLP, IDP/IDS שהוזכרנו בעבר וכן אמצעים להגנה אפליקטיבית דוגמת WAF לאפליקציות מבוססות ווב.

הקשחת תחנות קצה ושרתים

צמצום החשיפה והשירותים הפועלים למינימום הנדרש יחד עם מינימום הרשאות לביצוע שינויים או הפעלת יישומים. זהו נושא פתוח לפרשנות ושנוי במחלוקת **ואנו נתקלים בארגונים המתעללים במשתמשים ללא הגיון.**

התקנת תוכנות הגנה בתחנות הקצה (Endpoints)

מאנטי-וירוסים ועד תוכנות ניטור לוגים ואירועי אבטחה בתחנות.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

מהם רבדי ההגנה הבסיסיים

סינון דואר אלקטרוני

דרך מניעת וצמצום SPAM ובעיקר זיהוי קבצים נגועים או מקורות ושולחים בלתי מהימנים וחסימת האיום בטרם הגיע לנמען.

גיבוי מקיף ושילוב או שימוש בשירותי ענן

מתוך הנחה כי אין אמצעי הגנה מושלם **ויש להיערך ליום שאחרי.**

חינוך, הסברה ותרגול

שכן בסופו של דבר מרבית החדירות שאירעו בעולם נגרמו לבסוף על ידי הגורם האנושי שנפל בפח כלשהו או פותה על ידי תוקף.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

ביצד מזהות תוכנות הגנה את הנוזקות

- **זיהוי נוזקה מבוסס חתימה** (Signature)

  השיטה **היעילה ביותר להתגוננות בפני איומים מוכרים בלבד**. מבוססת 'חתימות' של קטעי קוד נוזקות שנותחו בעבר וחיפושן בקבצים בעת גישה אליהם או הפעלתם.

- **זיהוי נוזקה מבוסס התנהגות** (Behavioral)

  זיהוי נוזקה דרך ניתוח קוד ברגע הפעלתו ומעקב אחר פעולות שנעשות במערכת תוך **בלימת ריצתו ברגע שנעשה ניסיון לפעולה המוכרת או חשודה כמזיקה.** בזירה זו מתחרות מרבית תוכנות ההגנה כיום (EDR...).

- **ניתוח ארגז-חול** (Sandboxing)

  במקרה חשד – משלוח הקובץ **לסביבה ייעודית, סגורה ומבודדת והפעלתו שם תוך מעקב אחד התנהגותו באופן מלא לשם ניתוח איומים פוטנציאליים.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

ביצד מזהות תוכנות הגנה את הנוזקות

מעקב אחר התנהגות קולקטיבית

טכניקות מודרניות המביטות לא רק בתחנת קצה אלא **במכלול כל הרשת ומחפשות דפוסים חריגים או פעילות חשודה** הנראית במזיקה (EDR...).

ניתוח תעבורה יוצאת ונכנסת בתחנות

תוך זיהוי מקורות או יעדים מוכרים כמפוקפקים, זיהוי ערוצי תקשורת המשמשים נוזקות מוברות וכן **זיהוי התנהגות חריגה של תעבורת רשת השונה מהותית מהתעבורה הרגילה**.

האתגר הקשה ביותר להתמודדות על ידי התוכנות – ושם עיקר התחרות ביניהן – הנו איומים לא מוכרים וחדשים, המוכרים כ-Zero Day Attack.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

האיום מספר 1 : כופרות

הנוזקה הנפוצה והמזיקה ביותר נכון להיום

מפותחת בידי ארגונים וקבוצות פריצה ממוסדות המגלגלים מיליארדי דולרים
'פטורים ממס' ומשקיעים סכומי עתק במו"פ ובקמפייני תקיפה.

עקרון פעולה פשוט של חטיפה למטרת כופר

בתחילת דרכן היו מצפינות את כל מערכות הלקוח ונדרש כופר לשחרורן.
כיום המידע מועבר לידי התוקף טרם הצפנתו ומשמש לסחיטת
הקורבן תוך איום לפרסם סודות עסקיים או נתונים מביכים.

הדבקה במגוון האמצעים הגדול ביותר

קבצים נגועים, פתיונות ברשתות חברתיות, טרויאנים בתוכנות
חינם, דואר אלקטרוני נגוע, גניבת סיסמאות **ואף 'אדם מבפנים'.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

האיום מספר 1 : כופרות

פעמים רבות הארגון הנפגע נמצא על כוונת התוקף

התוקפים עוקבים אחר הארגון ועובדיו, **מזהים חולשות ומזהים עובדים פעילים ברשתות חברתיות ושמים אותם על הכוונת.**

מרבית ההדבקות מגיעות מדואר אלקטרוני מהונדס

אם דרך קובץ PDF / Word / Excel או אחר נגוע ואם דרך דואר המתחזה להודעה ממחלקת המחשוב או מ-365 במטרה לגנוב סיסמא !

חלק מההדבקות מגיעות מקישור זדוני

קיבלתם קישור מוזר לסרטון מצחיק? קיבלתם קישור מוזר במייל או מייל עם תוכן שנראה קצת שונה מהרגיל ?

לחיצה רגעית רק להציץ בו עשויה להפיל את כל הארגון בפח !

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

האיום מספר 1 : כופרות

תוכנות הגנה איכותיות מזהות חלק מהכופרות

כופרות מדור 'ישן' מזוהות באמצעות 'חתימות' קוד ו-'חתימות התנהגותיות'.
נוזקות מדור חדש מזוהות חלקית על ידי ניתוח Sandbox וניתוח התנהגותי מעמיק (מונח שזכה לכינוי שווקי EDR).

ברגע שקיים חשד להדבקה יש לפעול מיידית

הפעולה הראשונה לביצוע היא 'תלישת' כבלי תקשורת וחשמל.
בכל שניה שעוברת מוצפן או נגנב עוד ועוד מידע. אין זמן לדיבורים.

גיבוי ושירותי ענן איכותיים הנם פתרון חלקי

מהווים בעיקר פתרון לבעיית אבדן הגישה למידע. **הם אינם פתרון לבעיית פרסום המידע וכופרות תוקפות גם אותם.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 2 : פישינג

- **החל בטריק הכי ותיק בספר** (העוקץ הניגרי)
  מכתבים מנסיך ניגרי, זכיה בלוטו הספרדי או מכתב מטופש בשפה עילגת המאיים כי צילם אתכם בעירום גולשים בפורנו. **עקרון הבסיס הוא תפוצה אקראית בניסיון 'לדוג' פראייר שישלם כסף.**

- **דרך התחזות לגורמים לגיטמיים** (Social Engineering)
  מכתבים מ-Paybal, מ-Bankleuumi, מ-Kvich6 או הודעה From Your IT Department בדרישה לשינוי סיסמא. **מטרתם גניבת פרטי הזדהות דרך דף דמה המדמה דף כניסה לשם קציר סיסמאות גישה.**

- **וכלה במתקפה ממוקדת ליירוט העברות כספים**
  אלו המסובנים ביותר שכן הם **מתחזים לצד הממתין לתשלום ומטעים את הצד השני להעביר כספים לידי התוקף.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

איום מספר 2 : פישינג

עיקר ההגנה במערכות סינון SPAM

אך יש לזכור שהמערכות אינן מושלמות והתוקפים משפרים את אופן הניסוח מפעם לפעם כך שהדוא"ל הזדוני יחדור את ההגנות.

הגדרות SPF / DMARC ו-Reverse Ptr מונעות זיופים

שכן הן מגדירות אילו שרתים יכולים לשלוח דוא"ל בשם הדומיין וכל מקור אחר יחשב מיידית כזיוף. **לצערנו ארגונים לא מועטים אינם מקפידים על כך בצד המקבל ובצע השולח.**

חתימות דיגיטליות מעולות לאימות זהות !

במיוחד ועם דגש על **גורמים המאשרים העברות כספים.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

איום מספר 2 : פישינג

קו ההגנה האחרון והחשוב הוא שיקול הדעת שלכם

משהו מוזר לכם בניסוח של המייל ?

האם הקישור מוביל ל-paypal.com או **ל-buymycarnow.biz ?**

האם הטקסט במייל מופיע כתמונה ? (טריק להתחמקות מסורק SPAM)

האם כתובת השולח היא קשקוש מסוג 1fdawije@sdjsadsd.com ?

האם העברית עילגת או שיש רווחים מוזרים בין אותיות במילים ?

האם מבקשים מכם בקשה מיוחדת וחריגה ?

כל סימן קטן וחשוד הוא סימן גדול ומובהק שכנראה עוקצים אתכם.

אם יש ספק – לא נכנסים לקישור או לקובץ

ואם אתם מתבקשים לשנות סיסמא, גשו לאתר שלא דרך הקישור **אלא באופן יזום בכתובתו הידועה והמוכרת.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 2.5 : קישורי פישינג

מי לא מכיר את אתר 150.co.il ?

אתרים מסוג זה מהווים סכנה קיומית לארגונים שכן זהו אתר פרטי שאיננו נתון לשום ביקורת ואיננו עומד בסטנדרטים כלשהם **ומציע כלי שליטה מרחוק שאין שום פיקוח על מהימנותם**. הפעלת כלים דוגמת Anydesk מאתר זה מאפשרת לכל תוקף להשתלט על המחשב שלכם במידה והצליח לפרוץ לאתר ולהחליף את תכניו !

נכנסים לבנק דרך אתר kafe.co.il

90% מכם בכלל לא יביטו האם הכתובת שאליה נשלחתם מאתר זה היא אכן כתובת הבנק. פריצה לאתר זה או אפילו פעולה זדונית של בעלי אתר כזה יכולה לשלוח אתכם לכל דף מהונדס אחר.

אין להשתמש באתרי אינדקס ואתרי קיצורים מכל סוג שהוא.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

איום מספר 3 : מערכות לא מעודכנות

עדכוני תוכנה מתקנים פרצות שהתגלו

אי התקנת עדכוני תוכנה שקולה לדהרה ברכב עם תקלה ידועה בבלמים.
זוהי מגיפה המכה בארגונים ונפוצה במיוחד בשרתי דואר Exchange הסובלים חדשות לבקרים מפרצות שמתגלות בהם.

עדכוני תוכנה רלוונטיים לא רק למחשבים אישיים

הם רלוונטיים לטלפונים סלולריים, לטאבלטים, לנקודות גישה אלחוטיות, לנתבי תקשורת ומתגי תקשורת, למדפסות וסורקים, לבקרי השקיה, לבקרי חשמל, למכשירי DVR/NVR, לרמקולי Bluetooth, לבקרי טמפרטורה ומיזוג אוויר, למערכות בית חכם, למערכות רכב חכם ולמערכות הצנטריפוגות באיראן....

כל מכשיר אלקטרוני כיום מכיל תוכנה בדרג כלשהו ויצרנים בעלי שם דואגים לתקן תקלות ופרצות בתוכנה דרך עדכונים באתרי היצרן.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 3 : מערכות לא מעודכנות

הפריצה למערכות אלו איננה דורשת סיסמא

אופן הפריצה מבוסס על ניצול (Exploit) של באג כלשהו או חולשה כלשהי בפרוטוקול הצפנה לשם גילוי מפתח ההצפנה, מעקף מערכת האימות כליל או התקיפה החמורה ביותר : **Remote Code Execution.**

התקפה מסוג RCE מנצלת חולשה במנגנון מרוחק להפעלת קוד בתוך המערכת המותקפת דרך ניצול החולשה להחדרת קוד ומניפולציה להפעלתו.

מנגנוני אימות מחוכמים ככל שיהיו אינם יעילים

שכן חולשות במערכת מאפשרות מעקף מנגנוני האימות מבלי שיכנסו לפעולה כלל.

מצב זה שקול לקו מאז'ינו הצרפתי שפשוט נעקף על ידי הגרמנים...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

איום מספר 3 : מערכות לא מעודכנות

האחריות לעדכוני תוכנה מוטלת עליכם

אם הנכם מנהלי מחשוב האחריות לוודא כי עדכוני תוכנה וחומרה מותקנים כראוי במערכות השונות **מוטלת עליכם**. מחובתכם להתעדכן בפרסומי היצרנים, להפעיל כלים ולוודא באופן תדיר כי כלל המערכות שבאחריותכם מעודכנות.

אם הנכם משתמשים פרטיים האחריות לעדכן את המחשבים, הטלפונים ושאר המוצרים שבבעלותכם **מוטלת על כתפיכם** באותה המידה.
לא עדכנתם? אתם מסכנים את עצמכם ומקום עבודתכם !

המכשיר ישן ולא נתמך יותר ?

יתכן והגיע המועד להחליפו בדור מתקדם יותר או לחדול שימוש בו כליל.
כמוצא אחרון – יש לבודדו ככל שניתן מממשקים חיצוניים דוגמת רשת האינטרנט ולנתקו מכל מערכת בלתי חיונית.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 4 : חומר גלוי או לא מאובטח

הרמה הבסיסית והמטופשת ביותר ?

לא פעם מעלים עובדים מסמכים וחומר רגיש – בין אם ברמה עסקית ובין אם כזה המכיל מידע רפואי או חסוי – לשירותי שיתוף קבצים ציבוריים באופן גלוי, לא מבוקר **ונגיש לעיני כל תוך רמיסת כל מערך ההגנה על המידע.**

החזקת חומר רגיש בטלפונים או במחשבים ניידים

מצב זה נפוץ במיוחד עם השימוש במערכות שיתוף קבצים דוגמת Google Drive, One Drive, Dropbox או בקרב אנשי 'שטח' המעתיקים חומר למכשירים ניידים.

ללא הצפנת החומר וללא בקרת גישה למכשירים – אבדן מכשיר או השארתו ללא השגחה, ולו לרגעים ספורים, עשויה להסב נזק מהותי.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 4 : חומר גלוי או לא מאובטח

המניעה מתחילה בחינוך ומסתיימת באכיפה

חינוך, הדרכה וחשוב מכל – **סיווג המידע כרגיש והחתמת עובדים על סודיות** – יסייעו להנחלת תהליכי ושיטות עבודה מוקפדות. הרגל מגונה שיש להפטר ממנו הוא כי "לכולם יש גישה להכל" **ואכיפה נוקשה, בלתי סלחנית ונחרצת של עבירות אבטחת מידע** תביא להרתעת יתר הארגון מזלזול בנהלים.

סיסמאות והצפנת מידע

בסביבות בהן נשמר חומר רגיש במחשבים או בטלפונים ניידים **חובה ליישם סיסמת גישה ויש לשקול יישום הצפנות מידע דוגמת BitLocker** לכל הפחות – בכדי להקנות רובד בסיסי של מניעת גישה בלתי מורשית.

זכרו: מידע שנגנב אין להשיב ואת הגלגל אין להחזיר לאחור.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 4 : חומר גלוי או לא מאובטח

- **גישה למערכות מידע יש להצפין ולאבטח ב-VPN**
  בכל שניתן להגביל גישה למערכת לממשק מוצפן וסגור – כן תקטן חשיפת המערכת בפני עיניים בלתי רצויות ותקטן חשיפתה להתקפות.

- **מומלץ לעשות שימוש באימות כפול** (MFA/2FA)
  אימות המבוסס על שני מפתחות – לדוגמה סיסמא ותעודת SSL, סיסמא וברטיס חכם או סיסמה המופקת דינמית לזמן קצר (OTP) – יבטיחו כי גם אם נגנבה סיסמא באחד מהאופנים שפורטו קודם התוקף יתקשה לעשות בה שימוש ללא יתר המפתחות.

זכרו: מידע שנגנב אין להשיב ואת הגלגל אין להחזיר לאחור.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 5 : אתרים נגועים וזדוניים

גלשתם ב-YNET אז מה כבר יכול לקרות ?

מסתבר שדי הרבה. בתקופת Adobe Flash התגלו לא מעט אתרים שהכילו פרסומות או קישורים חיצוניים שהכילו נוזקה שאפשרה חדירה למחשב.
בדפדפנים קיימות חולשות המאפשרות לתוקפים לנצלן מתוך דף אינטרנט תמים למראה.

אין דין כל דפדפן זהה

הדפדפן הפגיע ביותר כיום הוא Internet Explorer המיושן.
זה לא מונע מאתרים ממשלתיים ישראלים ומערכות מקוונות שונות לדרוש אותו דווקא בגלל טכנולוגיית ActiveX הפגיעה שלו וזה גורם למשתמשים רבים **לעבוד איתו באורח קבוע – מה שמהווה סיכון קיצוני.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 5 : אתרים נגועים וזדוניים

מהן שיטות התקיפה ?

ניצול חולשות ופגיעויות שונות במנגנונים הקיימים ומובנים בדפדפנים שמטרתם שיפור חוויית הגלישה.

ניצול חולשות במנגנוני תוספים ופיתוי גולשים להתקין תוספים זדוניים.

הטעיית גולשים ללחיצה על תיבות אישור המאפשרות התקנה או הפעלת קוד זדוני (האישור מנוסח באופן מתעתע)

מהו הנזק הנגרם ?

ברמה הפשוטה – התקנת מקפיצי פרסומות וחוטפי תוצאות חיפוש.
ברמה הבינונית – גניבת מידע אישי ומידע פרטי לטובת פרסום והטרדה.
ברמה הגבוהה – Coin Miner המשתמש במחשב שלכם לכרייה !
ברמה החמורה – השתלטות והתקנת טרויאנים וכופרות במחשב !

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 5 : אתרים נגועים וזדוניים

ממה יש להיזהר במיוחד ?

זוכרים את 150.co.il ? זוכרים את kafe.co.il ?

אתרים מקישורים שונים שקיבלתם ב-Facebook או במייל.

אתרים המציעים קבצי Torrent, סרטי חינם, פריצות לתוכנות ועוד...

אתרים המציעים לכם משחקים מקוונים או רכילות עסיסית.

אתרים בעלי כתובות אקראיות http://wqejwiwj.29220odm.biz.

אתרים המציעים לכם עדכונים ודרייברים למחשב ולהתקנים (!)

כיצד ניתן להתגונן ?

אין פתרון מלא לכלל האיומים אך הפתרון החשוב ביותר הוא עדכוני תוכנה למערכת ההפעלה ולדפדפנים.

נוסף לכך תמהיל של תוכנות הגנה טובות, סינון תכנים זדוניים וגישה אחראית, חשדנית וזהירה ימזערו **חלקית** את החשיפה לסיכונים אלו.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

איום מספר 6 : קישורים זדוניים

קיבלתם הודעה המכילה קישור ?

ברמה הבסיסית והפשוטה – ההודעה היא אודות זכיה בלוטו או הודעה אודות הלוואה בתנאים אטרקטיביים.
ברמה הקשה יותר להתמודדות – ההודעה היא מגורם לגיטימי לדוגמה מהבנק, מרשות הדואר אודות חבילה או התור שקבעתם, מחברת DHL עם בקשה לשחרור ממכס או הודעת תשלום ארנונה מהעירייה.

קיים קושי לדעת האם זו הודעה זדונית או לגיטימית

שכן פעמים רבות אתם באמת מחכים לחבילה כלשהי שרכשתם ואם לא די בכך הרי שבהודעות SMS מקובל להשתמש בכתובות מקוצרות דוגמת https://bit.ly/pay123 **וקיים קושי אמיתי לדעת האם הקישור אמין או זדוני!**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 6 : קישורים זדוניים

סרקתם QR Code של מבצע בסופר ?

יתכן והשלט של המבצע הוצב בידי גורמים זדוניים !
ברגע שסרקתם את הקוד המכשיר שלכם גלש לאתר זדוני והפעיל תוכנה שהתקינה עצמה מבלי שבכלל ידעתם (כך בין היתר פועלות חברות דוגמת NSO בחלק מהמקרים).

קפצה לכם הודעה מוזרה במחשב ?

המבילה הודעה כי האנטיוירוס שלכם **לכאורה** זיהה פריצה או ש-Windows זיהה נוזקה ומבקשת שתלחצו עליה...
הודעה מסוג זה היא בעצם חלון קטן שנפתח על ידי הדפדפן ומקורו באתר זדוני וההודעה היא בעצם **תמונה עם קישור פתיון.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 6 : קישורים זדוניים

מינימום הגנה הנו אנטיוירוס למכשיר סלולרי

אם כי רובם אינם מציעים הגנה מוחלטת בפני נוזקות מחוכמות וישנם גופים דוגמת חברת NSO המסוגלים להשתלט על מכשירים חרף כל ההגנות.

החשדנות שלכם היא ההגנה הבלעדית

חשבו שלוש פעמים לפני לחיצה על קישור ובדקו האם בכלל הזמנתם חבילה והאם מספר החבילה תואם את הרשום ?
אם קיים ספק – במקרי הודעה על חבילה **כדאי לבדוק קודם באתר רשות הדואר או חברת המשלוחים האם סטטוס החבילה תואם לרשום בהודעה.**

זכרו : מרגע שלחצתם על קישור זדוני אין דרך חזרה.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 7 : התקני USB ו-Bluetooth

התקפה חדשה-ישנה שהופכת נפוצה כיום

רכשתם עכבר אלחוטי סיני ? יתכן והעכבר מפעיל לכם דברים בזמן שהלכתם להכין קפה... הבזק קטן ורגעי של חלון פקודה שלא תשימו לב אליו.

קיבלתם במתנה Disk On Key בכנס ? ברגע שתחברו אותו למחשב – אכלתם אותה מבלי שתדעו...

הכירו את כבל הטעינה החכם (חכם עליכם)

התקפה חדשה שצצה לאחרונה. כבלי טעינה USB לטלפונים **המכילים רכיבי נוזקה** מובנים או משדר אלחוטי המאפשר לתוקף להשתלט לכם על המחשב מרחוק ולבצע את זממו.

כל הנדרש הוא שתחברו את הכבל למחשב.

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 7 : התקני USB ו-Bluetooth

הבירו את ה-Key Logger

רכשתם מקלדת מסין ? יתכן וקיבלתם במתנה התקן המקליט את הקלדות המקשים שלכם ומשדר לצופה מעבר לים את הסיסמא לבנק...

ראיתם משהו מוזר וקטן מחובר בין המחשב לכבל המקלדת ? בעבר זו היתה שיטת התקפה ידועה במחשבים ציבוריים. מחברים אליהם מתאם קטן וסמוי ותקשורת המקלדת עוברת דרכו ומוקלטת...

קשה מאוד להתגונן בפני התקפות מסוג זה

מסיבה זו ארגונים רגישים מקפידים לרכוש ציוד ממותג מיצרנים מוכרים בלבד
אך גם כאן מסתתרת הפתעה (רמז: נדון בהמשך... Supply Chain...)

זכרו: טכנולוגיית המזעור כיום הפכה כל בורג וכל כבל תמים להתקן תקיפה !

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

איום מספר 8 : מחשבים ללא השגחה

הלכתם לרגע לשירותים או להכין קפה ?

ישבתם בבית קפה וקמתם לרגע מהמחשב הנייד רק להשליך כוס לפח ?
תוקף החומק לרגע קט מאחורי גבכם עשוי לחבר התקן USB ל-2 שניות ואז להמשיך בדרכו. **זה כל מה שנדרש**.

השארתם מחשב במעבדת מחשבים ?

יתכן והבחור במעבדה הוא לא מי שחשבתם וגם אם כן – יתכן והוא עושה שימוש בכלים נגועים בתום לב וחוסר ידיעה !
המחשב שקיבלתם חזרה מתיקון עשוי להיות פצצה מתקתקת.

לא פעם נתקלנו בטכנאים העושים שימוש בכלים
מפוקפקים או מסוכנים מתוך חוסר ידיעה...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

איום מספר 8 : מחשבים ללא השגחה

נתתם לילדים לשחק Fortnite במחשב שלכם ?

כמעט בטוח שהמחשב שלכם כבר נגוע בנוזקה...

יצאתם מהמשרד לישיבת הנהלה ?

אם לא נעלתם את המחשב **אחד העובדים או עובר אורח חמקמק עשוי להתיישב ולעשות בו כראות עיניו....**

מקרה קיצוני יותר? פריצה בלילה שבמסגרתה נגנב לכם השרת...

אז מהו הפתרון ?

לא עוזבים לרגע מחשב מבלי לנעול אותו.

מבטלים אפשרות הפעלת התקני USB ללא אישור.

מגדירים נעילה אוטומטית למחשבים ותחנות.

פוקחים עיניים ונוהגים בזהירות !

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 9 : Man In The Middle

התחברתם ל-WiFi של בית הקפה או נתב"ג ?

אז זהו שלא בטוח שזה מה שעשיתם...
מאוד יתכן שהתחברתם למחשב של תוקף שיושב במרחק קצר, מתחזה לרשת האלחוטית **ומקליט את כל התעבורה שלכם** או תוקף לכם את המחשב.

ההתגוננות כאן פשוטה מאוד

לא מתחברים כלל לרשתות ציבוריות אלא לנקודה חמה בטלפון (Hotspot).

אם כבר כן התחברתם – **השתמשו בהצפנת VPN לגלישה ולעבודה** בכדי למנוע מהתוקף להקליט את התעבורה שלכם בקלות.

זכרו : מרגע שהתחברתם למספר רגעים – יתכן וכבר אכלתם אותה...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 10 : Supply Chain Attack

הפריצה מתחילה אצל הספקים שלכם !

בכדי לפרוץ לכם למערכות לאו דווקא יש צורך לפרוץ אליכם ישירות אלא די בפריצה לספקי השירות שלכם – מאנשי המחשוב החיצוניים, דרך תוכנות המכילות קוד זדוני שהותקנו על ידי ספקים מבלי שידעו ובלה בחבלה ברכיבי המחשבים שלכם עוד בשלב היצור.

המקרה המפורסם ביותר לאחרונה : SuperMicro

יצרן פופולארי המציע שרתים זולים ומהווה ספק OEM ליצרנים רבים אחרים דוגמת Nimble, Nutanix ולקוחות גדולים כמו Apple.

קבלן משנה סיני המייצר את לוחות האם הכניס, בלחץ הממשל הסיני, רכיב ריגול זעיר לכל השרתים מתוצרת החברה. הפרצה התגלתה במזל רב...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 11 : פרצות בתוכנות ובאתרים

הטרף הקל ביותר לתוקפים הוא שרתי Web

המובילים שבהם הם ה-IIS של חברת מיקרוסופט ושרתי WordPress.
התוקפים עושים שימוש בפרצות בשרתים לא מעודכנים, בתוספים לא עדכניים או לא מתוחזקים ויותר מכל – **בקוד אתר רשלני או לא מושכל** המאפשר למשל טעינת קבצים (תוקף טוען קובץ ASPX ומריץ אותו בשרת !) או הזרקת קוד למשל בשדה המשתמש או הסיסמא (SQL Injection).

ריבוי פרצות במוצרי ושירותי Microsoft השונים

שרתי דואר Exchange ו-365, שרתי Azure AD, שרתי Terminal/RDS הפתוחים לעולם, שרתי מדפסות ומערכות ההפעלה Windows בכללותן. יש שיאמרו להגנתם שזהו פועל יוצא של הפופולאריות שלהם...

זכרו: כל מה שפתוח לעבר האינטרנט מהווה כר נוח לנסיונות לפריצה...

כל הזכויות שמורות לאינטרקונקט שירותי ענן

איום מספר 12 ומעלה ...

- **ישנם אינספור איומים אחרים וקצרה היריעה מלהכיל**

מאמצעים לזיהוי הקלדות אקוסטיים ועד מצלמות תרמיות המסוגלות לקרוא את התכנים במסכים ממרחק לפי עוצמת התאורה...

מתקיפה של טלפונים ועד האזנה לשיחות שלכם בסלון דרך הרמקול החכם...

ממעקב אחר מסלול נסיעתכם ועד האזנה לשיחות שלכם – **מה שכיום נעשה באופן אקטיבי על ידי Google, Facebook ואחרים.**

כל הזכויות שמורות לאינטרקונקט שירותי ענן

Interconnect
Cloud Services

ואיפה אתם נכנסים לתמונה ?

אם אתם מנהלים בארגון

מתפקידכם לוודא כי האנשים הטכניים מצד אחד - מקפידים על עדכונים, על קבלת התרעות, על שימוש בכלים נכונים, על גיבויים ועוד...
ומצד שני – כי העובדים, המשתמשים והספקים שלכם מודעים ומבינים מהי חובת הזהירות שעליהם לנקוט ואין לסמוך רק על מחלקת המחשוב !

אם אתם אנשי מחשוב בארגון

מתפקידכם לטפל בכל האספקטים הטכניים שנדונו כאן וקצרה היריעה מלהכיל אך מתפקידכם גם **לחנך ולהנחות עובדים ומנהלים בהנחיות אלו !**

אם אתם עובדים בארגון

מתפקידכם להזהר ולהקפיד על מעשיכם בכל מהלך.
אל לכם לסמוך על אחרים או להניח כי זו הבעיה של מישהו אחר !

כל הזכויות שמורות לאינטרקונקט שירותי ענן

וזו הזדמנות גם להכיר את היתרונות בענן

◀ אינטרקונקט מציעה כיום את הסביבות הבטוחות ביותר

מתשתיות מוגנות תת-קרקעיות, שרידות שרתים ומערכות תשתית בכל הרבדים ועד מערכי הגנה, גילוי, בקרה, זיהוי איומים, תגובה והתאוששות המקיפים ביותר בארץ ואף בעולם – המלווים לקוחות מקטנים ועד גדולים.

◀ הפתרונות של אינטרקונקט הם הכלכליים ביותר

שכן כל ניסיון ליישם את רבדי ההגנה והשרידות באופן עצמאי או בשילוב ספקים שונים יהפוך נטל כלכלי מהותי על הארגון וכאן יתרונו של הפתרון המשולב, המיושם על ידנו כיום עבור בנקים, חברות אשראי, חברות סייבר, גופים ממשלתיים וגופים עסקיים מהגדולים במשק.

Interconnect
Cloud Services

רוצים לדעת עוד ?

04-8409091