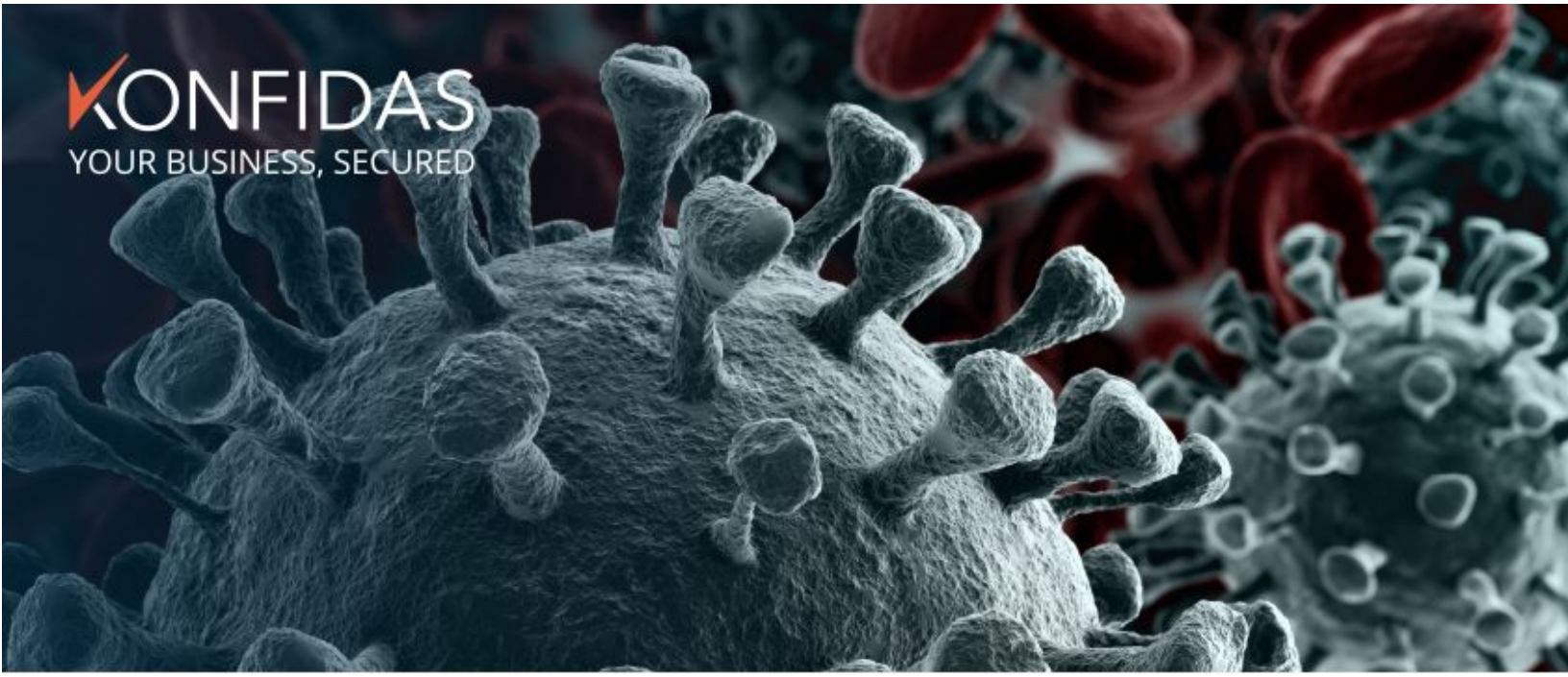


היבטי סייבר ונגיף הקורונה (COVID-19)

עדכון יומי 19.3.2020

#1

ממשלת ישראל הפיצה תקנות שעת חירום לצורך צמצום התפשטות נגיף הקורונה.

התקנות מאפשרות איסוף ועיבוד נתוני המיקום ונתיב התנועה של חולה קורונה מאומת במשך תקופה של שבועיים (14 ימים) לפני אבחונו כחולה. רשויות המדינה לא מורשות לעשות שימוש במידע זה, אלא למטרת זיהוי נתיב ההדבקה האפשרי של אותו החולה. השירות לא יעסוק, למשל, בפעילות פיקוח ואכיפה על הפרת חובת הבידוד של אותו האדם.[1]

#2

הממשל האמריקאי מוסיף מיליוני דולרים לשיפור מערכות מידע והגנת סייבר, במסגרת ההערכות לקורונה.

משרד האוצר האמריקאי מגביר את התקציב להתמודדות עם אירועי הסייבר אשר גוברים בצל התפשטות של נגיף הקורונה. כחלק מההיערכות יתוגבר תקציב משרד האנרגיה בסך 21 מיליון דולרים, תקציב משרד הפנים בסך 17 מיליון דולרים ותקציב המשרד לביטחון פנים בסך 47 מיליון דולרים. כמו כן, יתוגברו כלל התקציבים המוקדשים לצורך מימוש דרישות טכנולוגיות מידע אשר כוללות יכולות שיחות ועידה מורחבות, אמצעי אבטחת מידע ורשתות VPN, אבטחת שרתים קריטיים ופעולות נוספות להקשחת הפעילות של ארצות הברית במרחב הסייבר.[2]

[1] https://www.gov.il/he/departments/policies/dec4899_2020

[2] https://www.whitehouse.gov/wp-content/uploads/2020/03/Letter-regarding-additional-funding-to-support-the-United-States-response-to-COVID-19-3.17.2020.pdf

31 Rothschild Blvd.Tel Aviv, 6578414

Office: +972-3-6444417 | info@konfidas.com | www.konfidas.com

#3

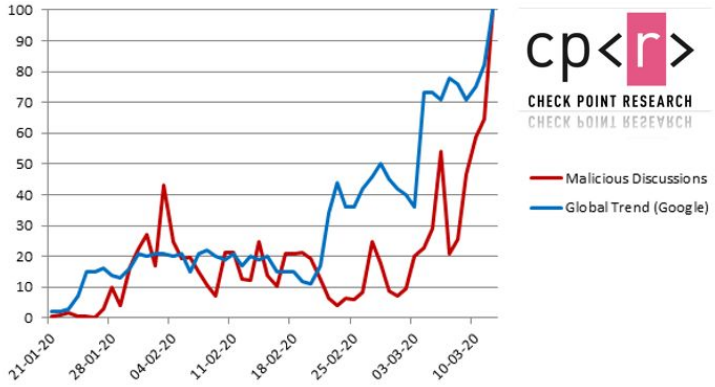
האם תקיפות סייבר כנגד בתי חולים ייפסקו בתקופת התפשטות הנגיף?

לורנס אברהמס, המייסד של Bleepingcomputer הצליח ליצור קשר עם קבוצת התוקפים שעומדת מאחורי מספר תקיפות כופרה. לורנס הפנה אליהם שאלה אחת, "האם תמשיכו לתקוף מוסדות בריאות ורפואה לאורך תקופת התפשטות נגיף הקורונה?" תגובת התוקפים הייתה שהם מנסים להימנע מפגיעה במוסדות בריאות ורפואה בזמנים אלו, אמנם לפעמים ישנן טעויות ותקלות אך הם לא שמים אותם למטרות תקיפה ייעודיות.[3]

#4

השפעת COVID-19: בשעת הסגירת של דלתות רבות במשק, האקרים נפתחים לעסקים.

סקירה של Checkpoint חושפת מעל 16,000 דומיינים חדשים הקשורים לנגיף הקורונה. מספר הדומיינים גדל פי 10 בהשוואה למצב שתועד לפני שלושה שבועות, וכ-20% מהאתרים נמצאו חשודים בקשר לפעילות של האקרים.[4]



#5

חוקרי חברת Proofpoint פרסמו דו"ח המסכם את תקיפות הסייבר בנושא הקורונה בשבועות האחרונים.

בימים האחרונים האקרים מנצלים את נגיף הקורונה לצורך ביצוע תקיפות סייבר. בין התקיפות שתועדו: זיופי מיילים עסקיים, הפצת פוגענים, קמפייני ספאם, מתקפות כופרה, וגניבת סיסמאות באמצעות phishing. המתקפות הללו הן קמפיינים רחבי היקף שכוונו כלפי משתמשים רגילים, והן קמפיינים ממוקדים, לדוגמא קמפניים שהתמקדו בבתי חולים.[5]

[3] https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/
[4] https://blog.checkpoint.com/2020/03/19/covid-19-impact-as-retailers-close-their-doors-hackers-open-for-business/
[5] https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update

#6

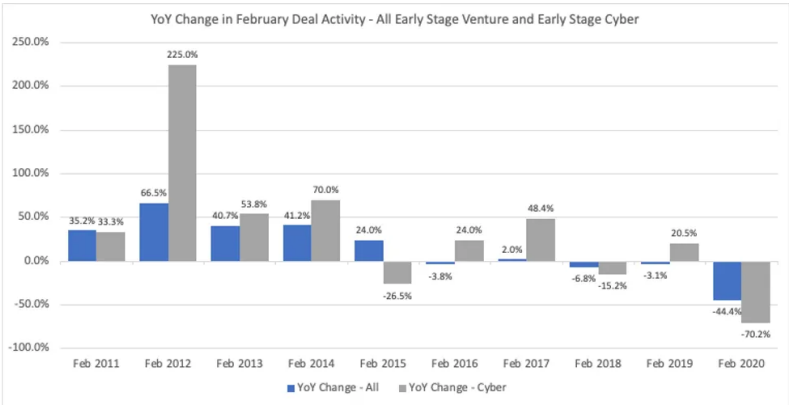
טוויטר לא יאפשרו העלאת ציוצים הקשורים למידע כוזב בנושא הקורונה.

חב' טוויטר פרסמה כי יוסרו ציוצים המכילים מניעת ייעוץ של מומחים, עידוד לשימוש בטיפולים או תרופות מזויפות וכל תוכן מטעה אשר מתחזה למומחה או לרשות הקשורה לנושא.

#7

צפי לירידה בהשקעות (Early stage) בחברות סייבר כתוצאה מנגיף הקורונה.

עוד בתחילת 2020 תמונת המצב של השקעות בתחום אבטחת המידע הייתה במגמת ירידה. על פי ניתוח של DataTribe ככל הנראה, משק אבטחת המידע יספוג ירידה נוספת עקב התפתחות בהיקף אירועי הסייבר המושפעים מנגיף הקורונה.[6]



#8

ציפייה לעלייה באירועי סייבר שתוביל לעליה בערך חברות הסייבר

Harley Lorenz Geiger מעלה סוגייה חדשה, בה הוא משווה בין עליית הצורך באמצעי ביטחון פיזי כתוצאה מהשפעת אירועי ה-9/11, לכך שיעלה הצורך באבטחת מידע כתוצאה מהתקפות הסייבר ההולכות וגוברות בצל וירוס הקורונה.[7]

[6] https://datatribe.com/dt-insight/
[7] https://twitter.com/HarleyGeiger/status/1240297394044051458

#9

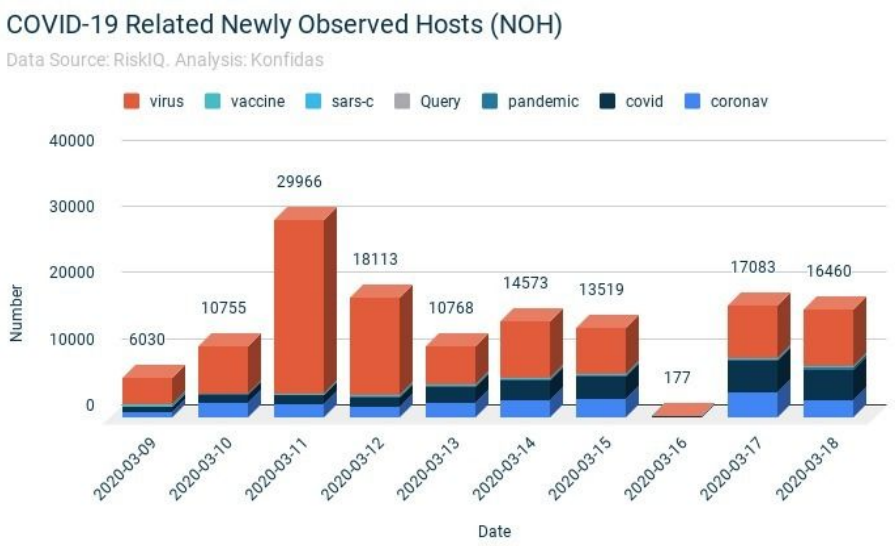
מקינזי: חלק מרכזי מההתמודדות עם הקורונה נופלת על כתפיי ה-CIO.

במהלך תקופה רגישה זו כל העיניים מושטות כלפי מנהלי מערכות המידע של החברות אשר מתמודדים עם ניהול העבודה מרחוק, המעבר החד לעבודה וירטואלית והחידושים הנוצרים כל יום שיש לעקוב אחריהם. חב' מקינזי פרסמה כתבה אשר מפרטת את הפעולות בהן מנהלי מערכות המידע צריכים להתמקד על מנת להתמודד עם המשבר העולמי.בין ההמלצות: הסתגלות מהירה לפלטפורמות עבודה חדשות, פרואקטיביות בנוגע לאבטחת מידע, דאגה יציבות תשתיות קריטיות לארגון ועוד.[8]

#10

עליה חדה בדומיינים זדוניים

על פי צ'ק פוינט, מתחילת ינואר נרשמו למעלה מ-16,000 שמות מתחם חדשים הקשורים וירוס קורונה. חברת RiskIQ יצרה מאגר Hosts a המכיל את המילים (covid, coronav, vaccine, pandemic, virus), על בסיס נתונים אלו ביצענו ניתוח של הופעת כתובות קיימות, שחלקן כנראה מיועד לצרכי תקיפה. הניתוח של קונפידס בסיס מידע על כתובות Host הקשורות ב-Covid-19 מופיע למטה. על פי צ'ק פוינט, שמות מתחם הקשורים לקורונה הם בעלי סיכוי גבוה ב-50% להיות זדוניים. בשבוע האחרון נרשמו למעלה מ- 6,000 דומיינים חדשים - עלייה של 85% בהשוואה לשבוע שעבר.[9]



[8] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-cios-moment-leadership-through-the-first-wave-of-the-coronavirus-crisis?cid=other-eml-alt-mip-mck&hlkid=146f1838179e44bb8d40368c321a03ac&hctky=9325559&hdpid=9437da35-77f1-4ce3-af64-8641c6912daa

[9] https://covid-public-domains.s3-us-west-1.amazonaws.com/index.html
https://blog.checkpoint.com/2020/03/19/covid-19-impact-as-retailers-close-their-doors-hackers-open-for-business/

#11

מומחי אבטחת מידע, ביניהם SANS ו- InfoSec, מזהירים מפני סכנות הסייבר בעבודה מרחוק.

ודאו כי תוכנת ה-VPN שלכם, שרתי החברה וכלל התוכנות לשימושכם מעודכנים. בנוסף, הקפידו להתקין עדכונים חדשים מיד עם קבלתם. כמו כן, וודאו כי הרשת הפרטית הוירטואלית שלכם מנוטרת לזיהוי פעילות חשודה וחריגה, וכי התראות אבטחה ממערכות המשרד שלכם מקבלות מענה מיידי. מומלץ גם להטמיע אימות רב-שלבי (MFA) למערכות ולחיבור ה-VPN.[10]

#12

המלצות של היורופול לעבודה בטוחה מהבית.

זמנים אלו, בהם רוב המשק עובד מהבית, חשוב להקפיד על חיבור בטוח לאינטרנט הביתי ומערכות המשרד.

גוף השיטור האירופי Europol פרסם המלצות לעבודה בטוחה מהבית אותן ניתן לממש בקלות כדי לשפר את רמת האבטחה של האינטרנט הביתי, ובכך גם את רמת האבטחה של החיבור המרוחק למערכות העבודה שלכם.[11]

#13

חברת Perception Point מציעה פתרונות סייבר מתקדמים כנגד תקיפות ה-phishing ההולכות וגוברות.

פתרונות הפלטפורמה מאפשרות התמודדות עם תקיפות דרך האימייל או באמצעות שיתוף תוכן דרך שרתי אחסון מידע ואפליקציות מסרים. זאת, בנוסף לשירותי Incident Response אוטומטיים ואנושיים. מוצרי החברה פשוטים לשימוש וניתנים להתקנה תוך 10 דקות. אין צורך במדריכי התקנה, ללא שום מאמץ מצוות ה-IT.[12]

10 https://www.zdnet.com/article/covid-19-with-everyone-working-from-home-vpn-security-has-now-become-paramount/

11 https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold

12 https://perception-point.io/

#14

סנדבוקס טכנולוגיה בע"מ מציעה מערכת חינמית אשר מיועדת לנתח קבצים חשודים ושיתוף מידע בין חוקרים.

פתרון זה שסנדבוקס מציעה מאפשר ניתוח דינמי של קבצים מבוסס למידה עמוקה וניתוח ברמת הקרנל של מערכת ההפעלה.[13]

#15

חברת Cyber Risk Aware מציעה תרגילי פישינג בחינם לחברות.

לאור עליה במתקפות הסייבר לצד התפשטות הקורונה, חברת Cyber Risk Aware מציעה לחברות לבצע תרגילי פישינג בחינם לעד כ-100 מעובדיהן. מנכ"ל החברה, סטפן בורק (Stephen Burke) סיפר בראיון ל-InfoSecurity כי הוא צופה עליה במתקפות הכופר בנוסף לעליה הניכרת בקמפני הפישינג ברחבי העולם ועל כן מנגיש פלטפורמה להתמודדות עם המצב.[14]

#16

בבלוג של קונפידס: איך לנצח את נגיף הקורונה?

אל"מ (מיל.) שי שבתאי כותב שעלינו להתחיל לחשוב על 'אסטרטגיית סיכום', כלומר כיצד עקרונות ההקלה יביאו את סיום המשבר. הוא לא משתמש במונח הידוע 'אסטרטגיית יציאה', מכיוון שהוא קשור לתוצאה לא מוצלחת, ובמשבר הזה עלינו להצליח בדרך זו או אחרת[15].

*** סוף מסמך ***

[13] https://sndbox.com/ways-to-use/
[14] https://www.infosecurity-magazine.com/news/companies-offer-free-cybersecurity/
[15] https://medium.com/konfidas/how-to-win-the-covid-19-insurgency-world-war-d5a11380ae8d

31 Rothschild Blvd.Tel Aviv, 6578414
Office: +972-3-6444417 | info@konfidas.com | www.konfidas.com