

ככל שהטכנולוגיות מתקדמות,

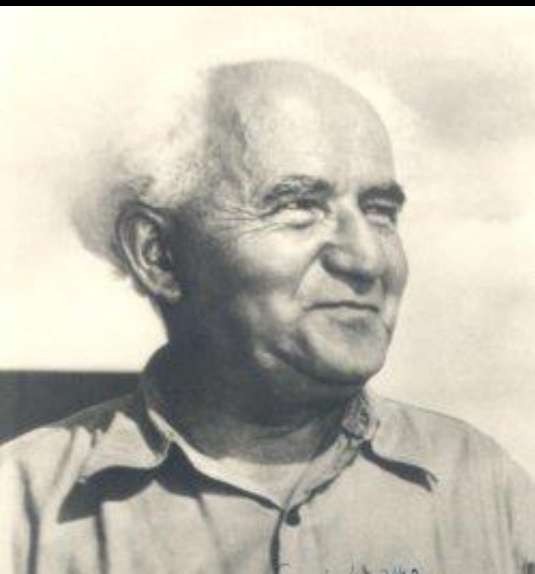
כך משתכללים גם האיומים על מערכות ERP.

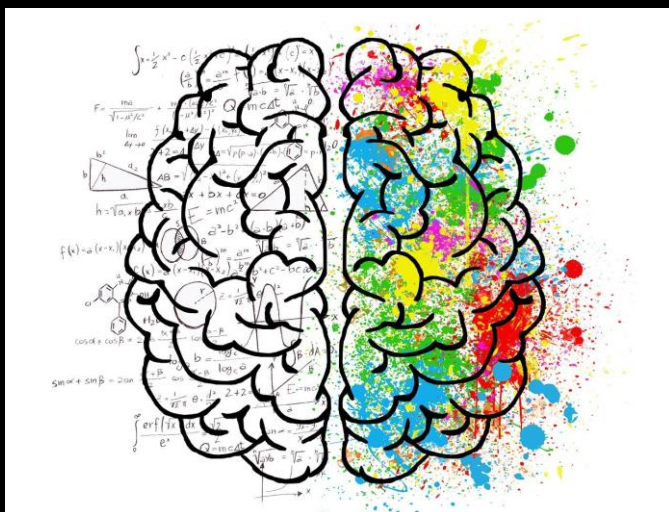
רמת ההגנה, על פי רוב, לא מותאמת

רו"ח, ms(it) בני אלון

דיטליקס טכנולוגיות תוכנה בע"מ
הגנה אקטיבית חכמה לתהליכי ה-ERP

"כך דרכן של תנועות, כמו שכך דרכם של אנשים, שמחשבתם מפגרת אחרי המאורעות. המחשבה נתלית באינרציה, בשגרה, בהרגל. המחשבה תמיד עצלה והיא מניחה שמה שהיה הוא שיהיה. מה שאין כן המאורעות. אומנם גם במאורעות יש אינרציה, אבל יש גם דינמיקה. החיים והטבע מלאים תמיד התגוששות, התאבקות של כוחות. ואין העולם קופא על שמריו, ואין ההיסטוריה קופאת על שמריה, ואין הטבע והאדם קופאים על שמריהם. אבל המחשבה על פי רוב מפגרת, וכאשר בזמן ידוע, מערכת ידועה מתחילה להתערער, עדיין המחשבה מסרבת לראות זאת, כי זה מחייב אותה למאמצים גדולים, למצוא שבילים חדשים. וזה קשה, מפני שיש כמות מוגבלת של אנרגיה לאדם והוא צריך להשקיע אותה במלחמת הקיום שלו, והוא אינו יכול להפנות את מחשבתו ולראות את השינויים .."





איך אפשר לאתר את הכשל
שהמחשבה נתלית באינרציה,
בשגרה ובהרגל?

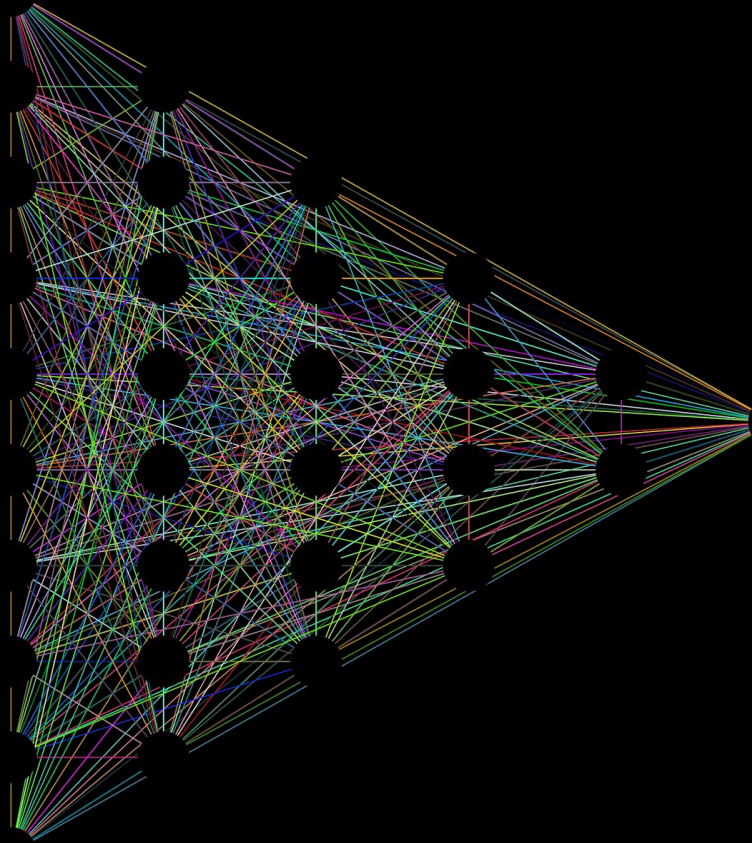
מה קורה מסביבנו ?

- הטכנולוגיות מתפתחות בקצב אקספוננציאלי.
- הגישה לטכנולוגיות זדוניות הופכת יותר ויותר נחלת הכלל.
- מגוון אמצעי התשלום בטכנולוגיות שונות גדל.

נגזרת משמעותית של מציאות זו היא,

התפשטות מרחב האיומים על המערכות הכספיות.

חשיפות



טעות בתום לב
כשל תהליכי
כשל מערכתי
רשלנות
מעילות
התקפה חיצונית

למה דווקא אצלי ?

חושבים במונחי דפוס קבוע?

מצפים שהאירועים יתנהלו על פי הציפיות שלכם ?

דרכו של המוח לחסוך אנרגיה על ידי הרגעה

איך נרגיע את עצמינו ?

נשאל, למה שיקרה לי ..

נרגע, כי השליטה חזרה אלינו, והמגננות ירדו ..

האם זאת השאלה הרלוונטית?

שילובים שנפגשים

החיבור בין המגמות – מה שמגביר הסתברות לכשל

מצד אחד, טכנולוגיות ויכולת באמצעים זמינים

מצד שני, המוטיבציות הישנות והטובות

השלכות של הונאה / מעילה / תקיפה

אירוע אירגוני מטלטל

בנוסף לפגיעה כלכלית, שיכולה להיות מהותית, יש פגיעה קשה ב:

ישרה

אמון

מוניטין של הארגון בעיני עובדיו

איך חברות וארגונים מתמודדים עם האיומים על מערכות התשלומים?

- בקרות תהליכיות ממוכנות
- בקרות ידניות בתהליך
- דוחות (כולל דוחות ביקורת , SOX)
- סקרי סיכונים תקופתיים
- חקירות ספורדיות גילויים מקריים

מה קורה בפועל?

דו"ח הפשע של Interpol לשנת 2023
עלייה משמעותית בפשעים כלכליים וטכנולוגיים

מאמרים אקדמיים בכתבי עת "Computers & Security" ו-"Journal of Financial Crime"
מחקרים רבים בתחום מדעי המחשב ואבטחת מידע שמציינים קשר ישיר בין התקדמות הטכנולוגיה וכתוצאה מכך גם הכלים הזמינים למבצעים עבירות.

דו"חות של חברות ייעוץ (Big 5)
סקרים ומחקרי שוק מספקים נתונים סטטיסטיים שמדגימים את הקשר בין התקדמות טכנולוגית לעלייה בהונאות

Today's criminals are constantly innovating to find new opportunities to infiltrate gaps in the perimeter

Fraudulent transfers to or from a platform are the most common type of platform fraud, comprising more than three-quarters of all incidents. While PwC's Global Economic Crime and Fraud Survey demonstrates C-suite concern about the rise in platform fraud, business leaders also reveal a general lack of understanding regarding their risk exposure. So, what can your organisation do to protect yourself against this new frontier for fraud and economic crime?

[PwC's Global Economic Crime and Fraud Survey 2022](#)

דו"ח של PwC משנת 2022 מדווח על כך ש-47% מהחברות
חוו סוג כלשהו של הונאה במהלך השנתיים האחרונות,
כשהטכנולוגיה משחקת תפקיד משמעותי

דו"ח אבטחת הסייבר של McAfee לשנת 2023 מדווח על עלייה בשימוש בטכנולוגיות מתקדמות לצורך מעילות והונאות.

[McAfee McAfee 2023 Threat Predictions](#)

דו"ח זה מציין כי ההתפתחות הטכנולוגית, כמו שימוש נרחב בבינה מלאכותית (AI) כלי יצירת תוכן, מקלה על פעילויות פשע מקוון. הדו"ח מדגיש כיצד כלים כמו DALL-E ו-Stable Diffusion מאפשרים לייצר תוכן מזויף ברמה גבוהה במהירות ובקלות, מה שמסייע לפושעים לייצר הונאות אמינות יותר, כולל זיופי מסמכים ונתונים.

[McAfee McAfee 2023 Consumer Mobile Threat Report](#)

הדו"ח מציין כי אפליקציות זדוניות נהיות מתוחכמות יותר ומשתמשות בכלים כמו ChatGPT כדי לשפר את הטקסטים שהן שולחות ולהימנע משגיאות דקדוק, מה שהופך את ההונאות לקשות יותר לזיהוי. אפליקציות זדוניות אלו מתמקדות בגניבת נתונים אישיים וכספים, לעיתים דרך חנויות אפליקציות לגיטימיות באמצעות עדכונים זדוניים.

הונאות פיננסיות בסייבר הם האיום הכי חם על ארגונים

Wells Fargo



היקף אי הסדרים הפיננסיים
מפעילות העובדים
בישראל מגיע
עד 9 מיליארד ש"ח בשנה

Bdicoface



גיוס הטכנולוגיה המתקדמת למלחמה בסיכונים המתפתחים

מערכות לאיתור והתרעה שוקדות כל הזמן להשתמש בטכנולוגיות מתקדמות, שיפעלו בשירות ההגנה על המערכות הכספיות, יאתרו באופן מדוייק וממוקד אירועי כשל מכל סוג, בזמן אמת, ויתריעו לגורם האחראי לטיפול בנושא. מערכת אלו הינן לומדת. הן גם מהוות תיעוד ונתיב ביקורת לאירועי כשל. המערכות נהנות מנסיון וידע קולקטיבי של החברות המשתמשות בהן.

הטכנולוגיה מאפשרת כיום מחשוב מואץ שמוביל לבינה מלאכותית אפקטיבית, ומהפכה של ממש.

מערכת דיטליקס מתלבשת על מערכות ה ERP ובסיסי הנתונים, הופכת את בסיסי הנתונים למערך טכנולוגיה של ניטור, בחינה ובקרה 24.7 של כל תנועה, בהתאם ל best practice וכלל הבדיקות הנדרשות לביצוע.

דוגמאות

הונאה באמצעות שיינוי חשבון בנק

1. האקר חודר לחשבון המייל של הספק
2. שולח מייל מתחזה לבקשה לשינוי חן בנק, עם רפרנס למיילים קודמים, מה שמייצר רמת אמינות מאוד גבוהה
3. פעולות אימות, שנעשות במייל מול הספק מגיעות את ההאקר וזכות לתשובה ממנו.
4. שיינוי חן בנק
5. ההאקר שולח מייל מתחזה לספק לגבי עיכוב צפוי בתשלום.
6. העברת הכספים לחשבון הבנק של ההאקר

Quanta Computer

ענקית ייצור אלקטרוניקה מטאיוואן שקיימת מאז שנות ה-80

בין הייתר ספקית של

Facebook

Google

NEWS

[Home](#) | [Israel-Gaza war](#) | [War in Ukraine](#) | [India Election 2024](#) | [Climate](#) | [Video](#) | [World](#) | [UK](#) | [Business](#) | [Tech](#)[Tech](#)

Google and Facebook duped in huge 'scam'

© 28 April 2017



GETTY IMAGES

The two tech giants succumbed to a well known type of scam, in which an attacker tricks the victim via innocent-looking emails

By **Chris Baraniuk**
Technology reporter

Google and Facebook have confirmed that they fell victim to an alleged \$100m (£77m) scam.

Google and Facebook have confirmed that they fell victim to an alleged \$100m (£77m) scam.

In March, it was reported that a Lithuanian man had been charged over an email **phishing attack** against "two US-based internet companies" that were not named at the time.

They had allegedly been tricked into wiring more than \$100m to the alleged scammer's bank accounts.

On 27 April, Fortune reported **that the two victims** were Facebook and Google.

The man accused of being behind the scam, Evaldas Rimasauskas, 48, allegedly posed as an Asia-based manufacturer and deceived the companies from at least 2013 until 2015.

"Fraudulent phishing emails were sent to employees and agents of the victim companies, which regularly conducted multimillion-dollar transactions with [the Asian] company," the US **Department of Justice (DOJ) said in March.**

These emails purported to be from employees of the Asia-based firm, the DOJ alleged, and were sent from email accounts designed to look like they had come from the company, but in fact had not.

The DOJ also accused Mr Rimasauskas of forging invoices, contracts and letters "that falsely appeared to have been executed and signed by executives and agents of the victim companies".

"We detected this fraud against our vendor management team and promptly alerted the authorities," a spokeswoman for Google said in a statement.

"We recouped the funds and we're pleased this matter is resolved."

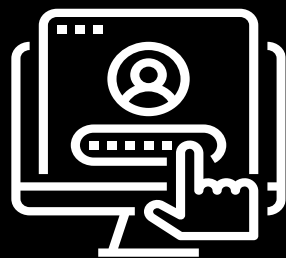
However, the firm did not reveal how much money it had transferred and recouped.

Nor did Facebook - but a spokeswoman said: "Facebook recovered the bulk of the funds shortly after the incident and has been cooperating with law enforcement in its investigation."

ניצול אפשרויות במערכות ה ERP

שכפול חשבוניות והחלפת מספר חשבון בנק

החלפת מספר
חשבון הבנק של
המועל



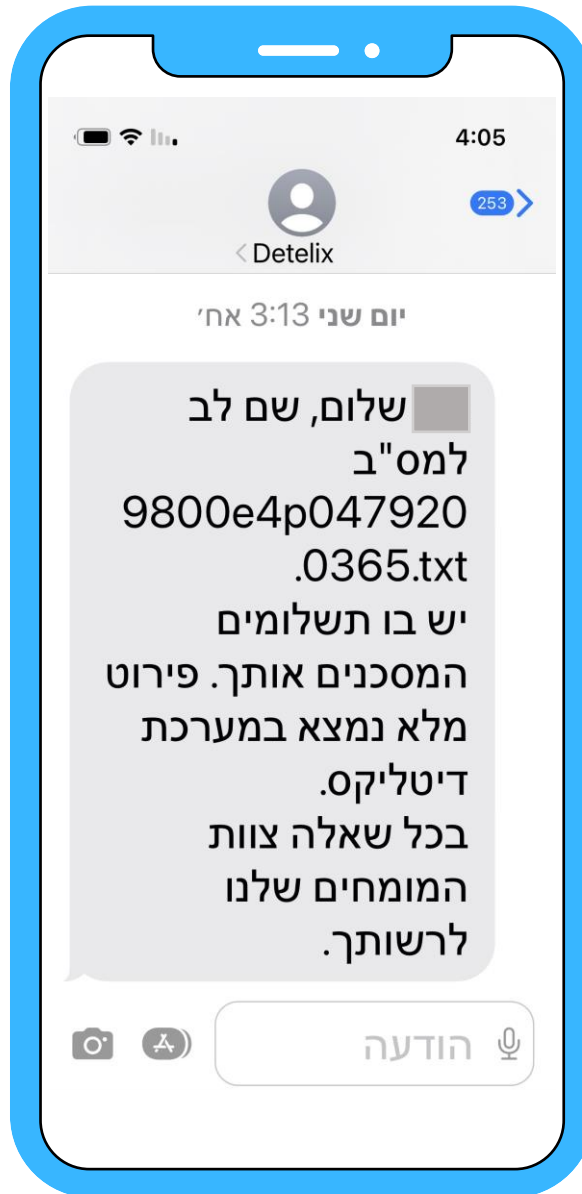
עקיפת הבקרה
המגבילה של
ERP



שכפול חשבונית



הודעת SMS





זחינו והתרענו


All Unread		By Date ▼ ↓			
From	Subject	Received ▼	Size	Categories	Mention
▼ Today					
 Information Center @ Detelix שלום רב	דיטליקס - התרעה חשובה	Mon 03/07/2023 15:14	239 KB		
▼ Yesterday					







הודעת Mail

דיטליקס - התרעה חשובה

 Information Center @ Detelix
To 

 If there are problems with how this message is displayed, click here to view it in a web browser.

 Reply  Reply All  Forward 

Mon 03/07/2023 15:14

שלום רב,

שם לב לאירועים שמערכת דיטליקס זיהה בתשלום [e4p0479200365.txt9800](#), (לפירוט האירועים אנא הקלק על שם התשלום).

מספר מקרים	אירוע
1	תשלום המבוסס על חשבונית ספק שהוזנה בעבר
1	התשלום מתבצע לחשבון בנק השונה מרשומת אב הספק

צוות המומחים שלנו עומד לרשותך בכל שאלה.

DETELIX 



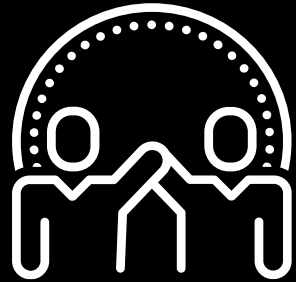
What is your Matrix?

האם יש קשרים עסקיים בין הספקים?

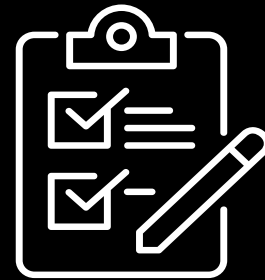


הסטת הזמנות לספק חלופי

שת"פ עם ספק
חלופי להוצאת
הכסף וחלוקתו



הודעה לספק שאין
צורך בסחורה
נוספת



התמקדות
בספק מטרה



עצירת טעות : תשלום ביתר במטבע לא נכון

כמעט תשלום ביתר
כתוצאה פער
בשערי מט"ח



קבלת חשבונית
מהספק בפאונד
והזנתה במערכת



הקמת הזמנה ביורו



ממצאים בולטים שנעצרו בשנה האחרונה

שינוי חשבון בנק ספק ע"י גורמים מורשים / איום חיצוני	הסטת תקציבים ותשלום מתקציבים לא רלוונטיים
ספקים פיקטיביים	אי עמידה בהוראות רכש תוך ניצול דרגות החופש במערכת של מדרג החתימות
יצירת בנקים לניצול (על ידי העברות בין חשבונות / התאמות ועוד)	חריגה מהסכמים, אסטרטגיות רכש, עמידה במכרזים, רכש מחוץ להסכם, פיצולים
שינוי פרטי חשבונית לאחר ביצוע התשלום לצורכי הסתרה	ניצול יתרות לקוחות / ספקים
ניפוח חשבוניות על ידי הספק בשת"פ עם מנהלת החשבונות	ניצול חשבונות מע"מ / התאמות פתוחות / יתרות ועוד
תשלומים כפולים ומיותרים (על ידי איתור בעזרת Soundex ו מודול אנליטי לאיתור חן זהה)	ניצול לרעה של שערי מטבע
תשלומים לספקים שהחברה החליטה שלא לעבוד איתם	העברות בין ספקים, העברות בין לקוחות, העברות בין לקוחות לצרכי מעילה
שימושים לרעה בספקים אלטרנטיביים	חיובי יתר ללקוחות
שינויי שם להמחאה	שינוי קובץ מס"ב לפני שידור ואף תשלום ישיר תוך עקיפת קובץ מס"ב
התאמות בנק במטרה להסתיר הוצאות	הקדמות תשלומים

AI מול בן אנוש

ה AI יחזק וישפר אותנו
אבל לעולם לא יחליף אותנו



תודה רבה בני אלון

Detelix.com

074-7022313

