InfoSec 2014 in Cyberspace:

"התמודדות בנק ישראל עם זירת הסייבר"

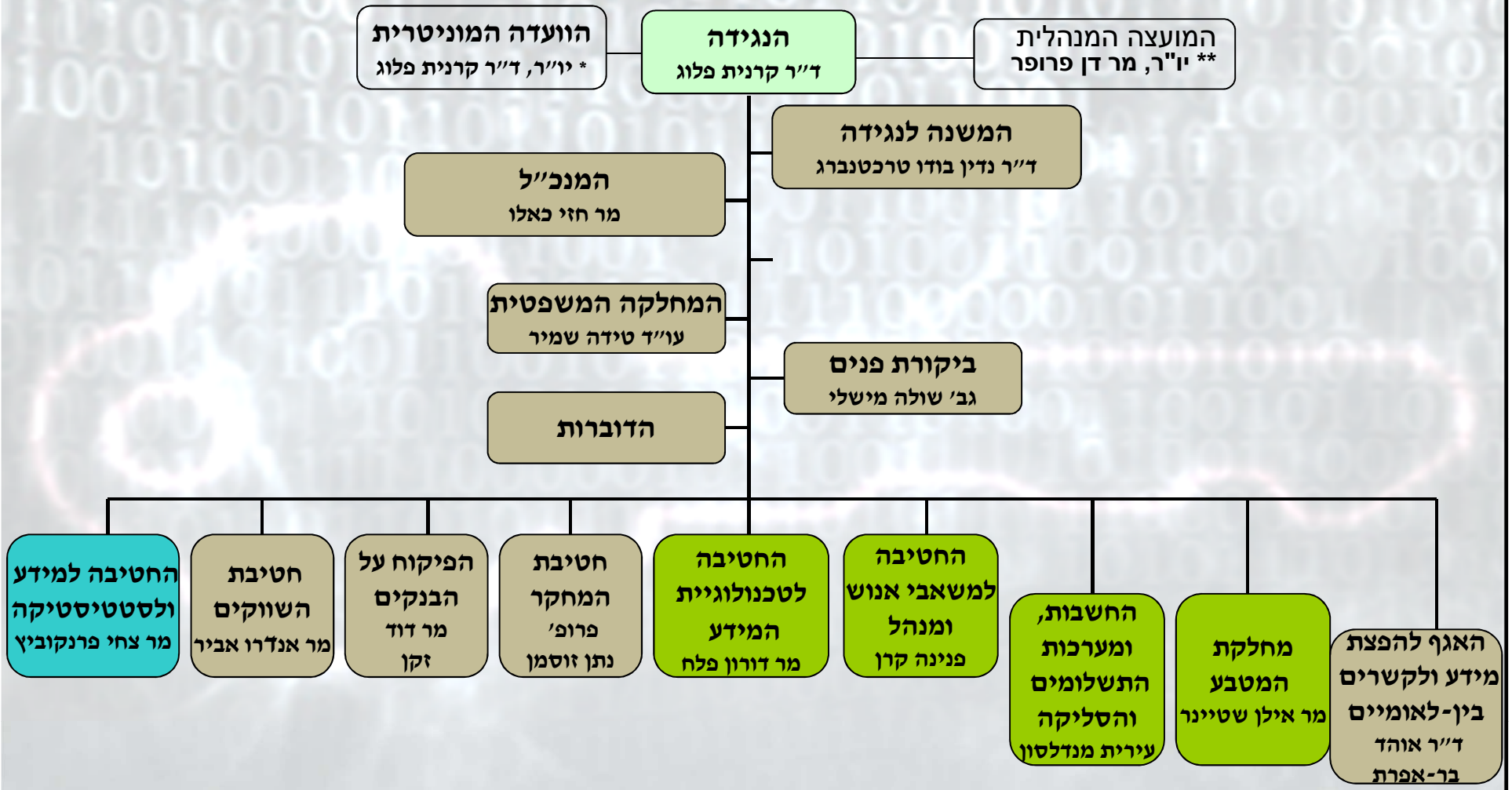
חזי כאלו

מנכ"ל בנק ישראל

תוכן עניינים

- בנק ישראל – כללי
- היקפי ומגמות תקיפות סייבר בארץ ובעולם
- שחקנים בזירת הסייבר ויעדי התקיפה
- עקרונות יסוד
- אסטרטגיית אבטחת המידע
- תחומי האבטחה מפני פעילות הסייבר
- יעדים
- התמודדות

בנק ישראל - המבנה הארגוני



* יו"ר הוועדה המוניטארית היא הנגידה. בוועדה חברים המשנה לנגידה, ר' חט' המחקר ועוד שלושה חברים שאינם עובדי הבנק.

** יו"ר המועצה המנהלית הוא חיצוני לבנק. במועצה עוד ארבעה חברים חיצוניים, הנגידה והמשנה לנגידה.

תפקידי ליבה של הבנק המרכזי

- ניהול מדיניות מוניטארית
- פיקוח והסדרה של מערכת הבנקאות
- ניהול יתרות מטבע החוץ של המדינה
- תמיכה בפעילות סדירה של שוק מטבע החוץ
- ייעוץ כלכלי לממשלה
- הסדרת מערכות תשלומים וסליקה
- הנפקת מטבע והסדרת מערכת המזומנים
- בנקאי של הממשלה

היקפי ומגמות תקיפות סייבר בארץ ובעולם

- עלייה של 350% במספר המדינות בהן נרשמו אירועי סייבר מאושרים (על פי דו"ח verizon).
- **1/3 מהתקריות כוון לבנקים ולמגזר הפיננסי.**
- **מספר הטרויאנים ליישומי מובייל של בנקים הוכפל רק ברבעון הראשון של שנת 2014!**
- **כל מספר חודשים (שבועות) מתגלה עוד מופע של וירוס שאחראי לגניבה של עשרות מיליוני יורו/דולר.** ב- 7.5 דווח על פריצה שהתבצעה למערכות המידע של חברת אורנג בצרפת לגניבת מידע על 1.3 מיליון מלקוחות החברה. ב- 6.5 נפרצו ארבעה חשבונות "טוויטר" של Wall Street Journal ע"י "הצבא הסורי האלקטרוני".
- עפ"י דו"ח של חברת מקינזי בשיתוף עם World Economic Forum, אומדן הפוטנציאל לנזק כספי עולמי של פערים באבטחת מידע, הוא 21 טריליון דולר.

שחקנים בזירת הסייבר ויעדי התקיפה

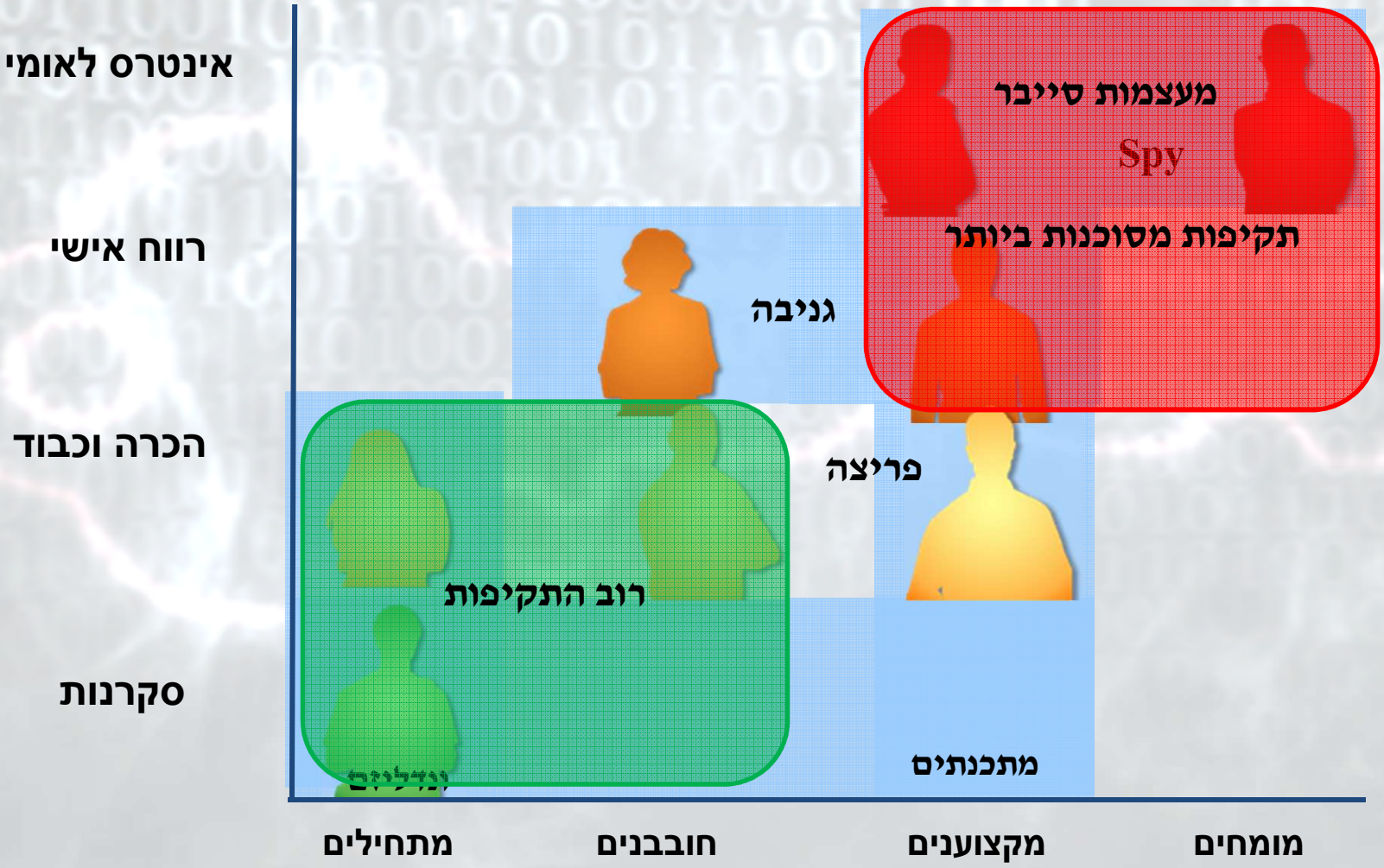
שחקנים

- מעצמות
- מדינות
- תאגידים וארגונים גדולים
- ארגוני טרור
- האקטיביסטים
- האקרים
- גורמים פליליים

יעדי התקיפה

- ריגול
- שיבוש מערכות
- גניבת כסף
- מחאה
- טרור קיברנטי

שחקנים בזירת הסייבר



עקרונות יסוד

- **<u>עצמאות ואחריות: בנק ישראל אחראי לקבלת החלטות ולהשלכותיהן וזאת מעבר לרגולציה והנחיות שונות.</u>**
- **<u>עבודה עצמית והיעזרות בבכירי היועצים החיצוניים.</u>**
- מודל האבטחה חייב להתחשב בקשרים ובתלויות העסקיות הפנימיות והחיצוניות המתורגמות לקשרים אפליקטיביים.
- תעדוף הגנת המשאב הקריטי אשר לכאורה אינו נמצא בארגון. זאת מעבר לשיבוש מערכות ומידע ולפגיעה במוניטין.
- **<u>הגנת שכבות תוך שימוש בטכנולוגיות חדשות, על פי best of bread.</u>**
- **<u>שיתופי פעולה תוך-ארגוניים, בין ארגוניים, בין מגזריים, לבד לא ניתן להגן.</u>**

אסטרטגיית אבטחת המידע

- מערכות המידע של בנק ישראל והשירותים שהוא מספק פנימית ולמשק מוגדרים כתשתית ממוחשבת קריטית ברמה הלאומית.
- פגיעה בבנק המרכזי מהווה פגיעה בסמל שלטון ופגיעה במערכת הבנקאית כולה.
- רגולטור וסמל למערכת הבנקאית והפיננסית.
- בנק ישראל כפוף לרגולציה מחמירה והדוקה של ראמ.

תחומי אבטחה והתגוננת מפני פעילות הסייבר

מנהל וארגון

- ניהול אבטחת מידע
- אסטרטגיה, מדיניות ונהלים
- **ניהול סיכונים / סקרים**
- הגורם האנושי
- **מודעות אבטחת מידע**
- מניעת זליגת מידע

המגזר הפיננסי

- הפיקוח על הבנקים
- ראמ
- מטה סייבר
- **מודיעין סייבר מגזרי**
- חדר מצב מגזרי

אבטחת מערכות

- פיתוח מאובטח, רכש ותחזוקת מערכות
- **אבטחת שרשרת אספקה**
- **אבטחת יישומים**
- **ניהול זהויות והרשאות**
- אבטחת מערכות תפעול ייצור ובקרה

אבטחת תשתיות

- **אבטחת הרשת**
- **אבטחת שרתים**
- **אבטחת תחנות עבודה**
- **אבטחת גישה מרחוק והתקנים ניידים**
- ניטור ובקרה
- **טיפול באירועים**
- **התגוננות מתקיפות ממוקדות "מתחת לרדאר"**

יעדים

- מניעת תקיפה משמעותית על פי רמות הפגיעה:
  1. מימוש איום הייחוס – גניבת נכסים.
  2. שיבוש תפקוד מערכות מידע.
  3. **<u>פגיעה במוניטין.</u>**
- הובלת המערכת הפיננסית בתחום.
- **<u>שיתופי פעולה עם כל המגזרים.</u>**

התמודדות

- ✓ סיום הקמת מערכת SIEM
- ✓ התנעת פעולות מרכז SOC
- ✓ רכישת כלים ומיומנות לחקר אירועי אבטחה + תרגיל

תודה על ההקשבה!