

שיעור 4

תורת ההגנה בסייבר 2.0 של מערך הסייבר הישראלי.
עיונים במסגור אבטחת הסייבר של ENISA.

הכרות עם תוכניות מקבילות NIST

- להכיר את התכניות, כיצד נוצרו ולמה נועדו.
- להבין כיצד ליישם את התכנית (אחת מהן) בארגונים השונים.
- לפתח גישה ביקורתית ויישומית למדיניות סייבר בארגונים!
- להבין כיצד התכניות שונות (ודומות) לתכנית ה-NIST.

סיבות הקמה

סיבות להקמה/פרסום

- איומים גוברים: מתקפות סייבר הפכו לאיום ממשי המשפיע על תשתיות לאומיות, עסקים קטנים וגדולים, ומערכות ממשלתיות.
- חוסר אחידות בהגנה: ארגונים רבים התקשו להתמודד עם אתגרי הסייבר בצורה אחידה ויעילה, מה שדרש יצירת מסגרת אחידה.
- פגיעה אפשרית במוניטין ובכלכלה: מתקפות סייבר עלולות לגרום לנזקים כלכליים כבדים ולפגיעה באמון הציבור.

תמצית התכנית

 השפעה	 מטרות	 מוטיבציה	 שחקנים
<p>פגיעה בחיי אדם / בטיחות אובדן הכנסה / נזק כלכלי IQ גניבת פגיעה במוניטין הרס תשתית הפללה / תביעה סנקציות והגבלות אובדן אמון ציבור/משקיעים פגיעה ברציפות תפקודית איכות הסביבה תודעתית</p>	<p>פגיעה ושיבוש מידע</p> <p>קניין רוחני</p> <p>דלף מידע רגיש</p> <p>שירותים</p> <p>תדמית ומוניטין</p>	<p>ריגול צבאית מל"מ פוליטית רווח פיננסי השבתה / הפרעה / חבלה יתרון תחרותי אנרכיה / כאוס נקמה / מרמור טקטיקה / אסטרטגיה חברתית / מוראלית פרסום הצהרה</p>	<p>ממשלה / שליחים / חסות ארגוני פשע עובד בעל הרשאות גופי טרור האקטיביסטים מתחרה עסקי האקר בודד ומיומן סקריפט קידים</p>

היסטוריה: למה מערך הסייבר הוקם ולמה המסמך פורסם

צפוף מידי למצגת – אנא עיינו בעמוד 114-115 במסמך:

<https://www.idi.org.il/media/19666/what-is-cyber-security-part-two.pdf>

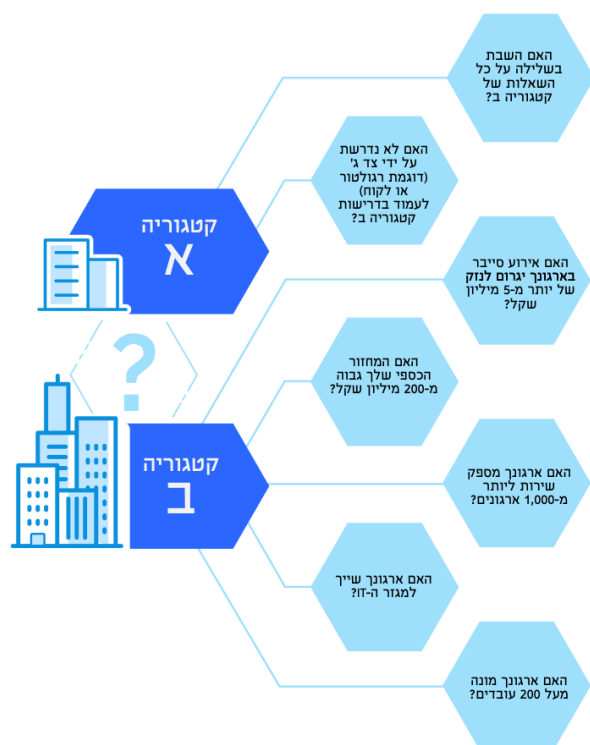


תמצית התכנית

קטגוריזציה:

- הארגונים מחולקים לשתי קטגוריות עיקריות לפי פוטנציאל הנזק מאירוע סייבר:
- קטגוריה א': ארגונים עם פוטנציאל נזק בינוני-נמוך.
 - קטגוריה ב': ארגונים עם פוטנציאל נזק גבוה, הדורשים תהליכי ניהול סיכונים מורחבים.

תמצית התכנית



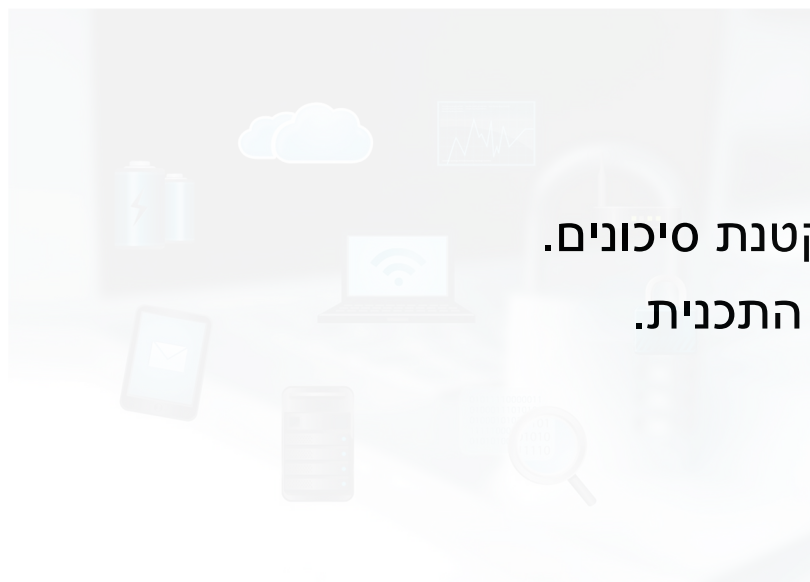
תמצית התכנית

תהליך ניהול סיכונים

- הגדרת קטגוריה: מיפוי הארגון.
- זיהוי ואפיון סיכונים: הבנת האיומים והערכותם.
- בניית תכנית פעולה: הכנת תכנית מותאמת להקטנת סיכונים.
- ביקורת ובקרה: ביצוע בדיקות שוטפות לתקפות התכנית.

עקרונות מרכזיים

- אחריות הנהלה על ניהול הסיכונים.
- שימוש במודיעין עדכני.
- התאמת רמת ההגנה לפוטנציאל הנזק.



תמצית התכנית

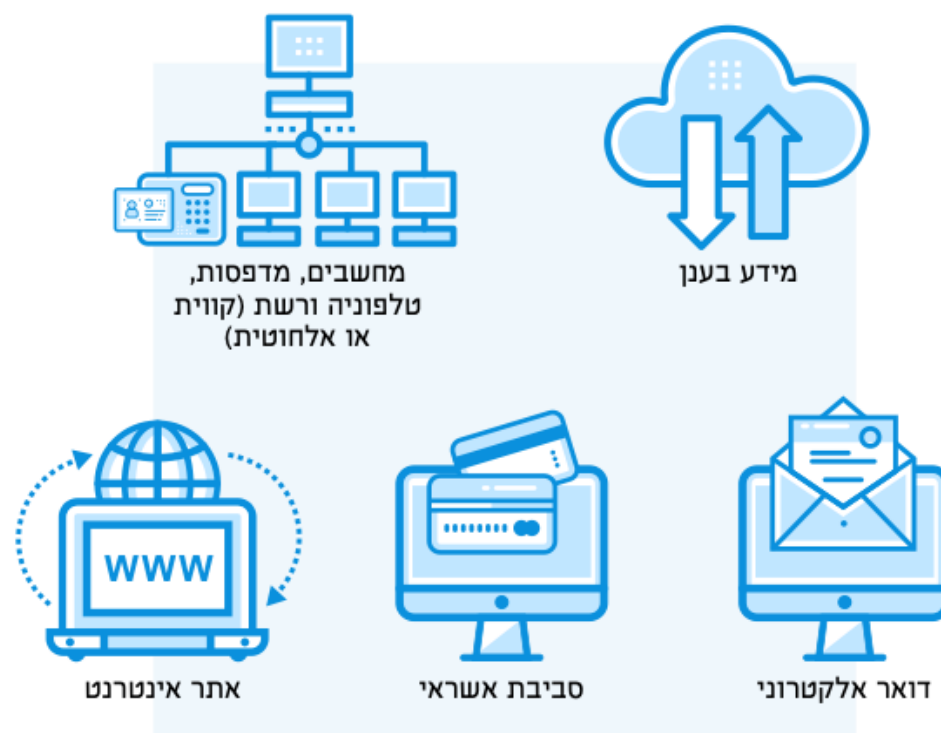
עבור ארגון מקטגוריה א:



עבור ארגון מקטגוריה ב:



תמצית התכנית



דוגמה למיפוי יעדי הגנה בארגון מקטגוריה א'

תמצית התכנית

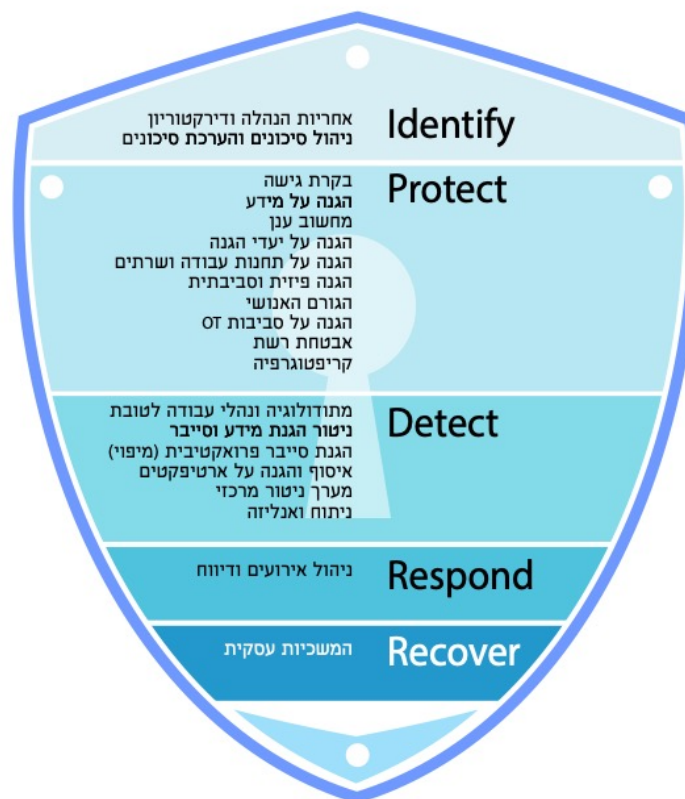
להלן טבלת עזר למילוי נתונים:

ייעדי הגנה שמופו בארגון				כגון: אתר אינטרנט, מאגר לקוחות, עמדות קצה, שרת מיילים, שרת גיבויים וכו'
משפחת הבקרה	קיים/לא קיים	אפקטיביות הבקרה	עלות מימוש	שקלול הנתונים/תעדוף
אחריות הנהלה				
מניעת קוד זדוני				
הצפנה				
מחשוב ענן ורכש תוכנות				
הגנה על המידע				
הגנה על מחשבים				
משאבי אנוש				
תיעוד וניטור				
אבטחת רשת				
המשכיות עסקית				

תוכנית העבודה המוצעת תאושר על ידי מנהל/ת הארגון.

תמצית התכנית

מסגרת בקורת תורת ההגנה



קריאה מתוך התכנית עצמה



מקור:

https://www.gov.il/he/pages/cyber_security_methodology_2

קריאה מתוך התכנית עצמה



מקור:

https://www.gov.il/he/pages/cyber_security_methodology_2

ארגון ה- The European Union Agency for Cybersecurity

שאלה: מדוע יש צורך בארגון ומסמכי מדיניות/נהלים כלל-אירופאיים?



ארגון ה- The European Union Agency for Cybersecurity

הקמה

- ENISA הוקמה ב-2004 בעקבות רגולציה (EC מס' 460/2004 של הפרלמנט האירופי והמועצה).
- הסיבות להקמה כללו את הצורך בתיאום ושיתוף פעולה בין מדינות האיחוד בתחום אבטחת הסייבר, במיוחד לאור העלייה באיומי סייבר והצורך בהגנה על תשתיות קריטיות.

מטרות ותפקידים

- ENISA שואפת להשיג רמה גבוהה ומשותפת של אבטחת סייבר ברחבי האיחוד האירופי.
- הסוכנות תורמת למדיניות הסייבר של האיחוד, מחזקת את אמון הציבור במוצרים, שירותים ותהליכים דיגיטליים באמצעות תכניות הסמכה, ומשתפת פעולה עם מדינות החברות וגורמים נוספים.

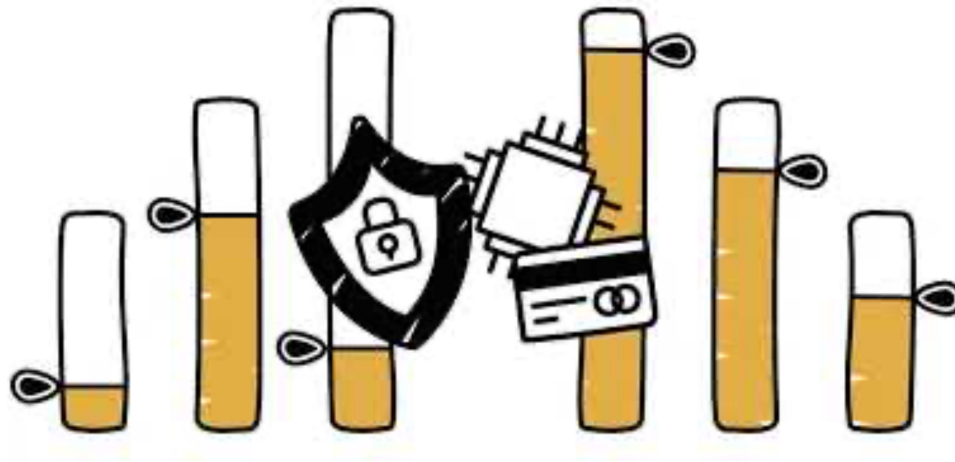


ארגון ה- The European Union Agency for Cybersecurity
























מקור: <https://www.youtube.com/watch?v=6Nq9OgZ5gsM>

ארגון ה- The European Union Agency for Cybersecurity



עיונים במסמכי ה- The European Union Agency for Cybersecurity

 Awareness Rating Awareness Campaigns, SME Cybersecurity, All-in-a-Box	 Certification Cybersecurity Certification Framework, From Candidate to Certification Scheme	 Cloud Cloud Security
 COVID-19	 Critical Infrastructure Telecom sector, Energy sector, Health sector, Finance sector, Maritime sector, Rail sector, Aviation sector, Internal Infrastructure	 Cryptography
 Cyber Crisis Management	 Cyber Threats Threat Landscape	 Cybersecurity Policy Policy Observatory, NIS Directive 2, eIDAS, European Electronic Communications Code, Data Protection
 Education European Cybersecurity Challenge (ECSC), International Cybersecurity Challenges (ICCC), European Cybersecurity Skills Framework (ECSF)	 Emerging Technologies Internet of Things (IoT), Artificial Intelligence (AI)	 Foresight
 Incident Reporting For Telecom, For Trust Providers, For Digital Service Providers (DSD Directives), Cybersecurity Incident Report and Analysis System – Visual Analysis	 Incident response EU CYCLON, CSIRTs Network, CSIRT Map, Cooperation with CSIRTs, Situational awareness, CSIRT Inventory, Glossary	 Market Annual cybersecurity market analysis, Cybersecurity Market Analysis Framework
 National Cybersecurity Strategies National Cybersecurity Strategies Guidelines & Tools, National Cybersecurity Strategies (NCSS) Map, Public-Private Partnerships (PPPs), Information Sharing and Analysis Centers (ISACs)	 Research and Innovation R&I Roadmap, R&I observatory, EU funding in cybersecurity	 Risk Management
 Standards	 Training and Exercises Cyber Exercises, Trainings for Cybersecurity Specialists	 Vulnerability Disclosure

עיונים
בנושאים
ומסמכים:
<https://www.enisa.europa.eu/topics>

מסגרים שונים ומשונים

Country	Framework	Focus	Strengths	Weaknesses	Target Audience
USA	<u>NIST Cybersecurity Framework (CSF)</u>	Risk-based, voluntary	Flexible, customizable, integrates with other frameworks	Lacks prescriptive guidance, may be complex for small organizations	Businesses of all sizes, government agencies
Independent/ Switzerland	<u>ISO 27001:2013</u> <u>ISO 27002:2022</u>	Information security management, prescriptive	Well-established, globally recognized, comprehensive	Can be rigid, bureaucratic, expensive to implement	Organizations of all sizes seeking certification
Cross-European	<u>ENISA Cybersecurity Framework</u>	Risk management, threat intelligence	EU-focused, considers emerging threats, filtered!	Less mature than other frameworks, limited adoption outside EU	EU organizations, public administrations
China	<u>TC260</u>	National security, critical infrastructure	Government-backed, compliance-driven	Lacks transparency, limited international recognition	Chinese organizations, critical infrastructure providers, personal use, by industry
UK	<u>NCSC Cyber Essentials: Small Business Guide</u>	Basic cyber hygiene, essential controls	Simple, affordable, good starting point	Not as comprehensive as other frameworks, may not be sufficient for high-risk organizations	Small and medium businesses, organizations with limited resources
Israel	<u>תכנית מוכנת</u> <u>ארגון למשבר</u> <u>סייבר</u> <u>תורת ההגנה</u>	Basic cyber hygiene, essential controls, incident response	Simple, affordable, good starting point	Not as comprehensive as other frameworks, may not be sufficient for high-risk organizations	Management level, public

סיכום ושאלות



שיעור 5

הסמכות ומסגורים בינלאומיים:
ועוד ISO2700X, SOC2, CSA, GDPR