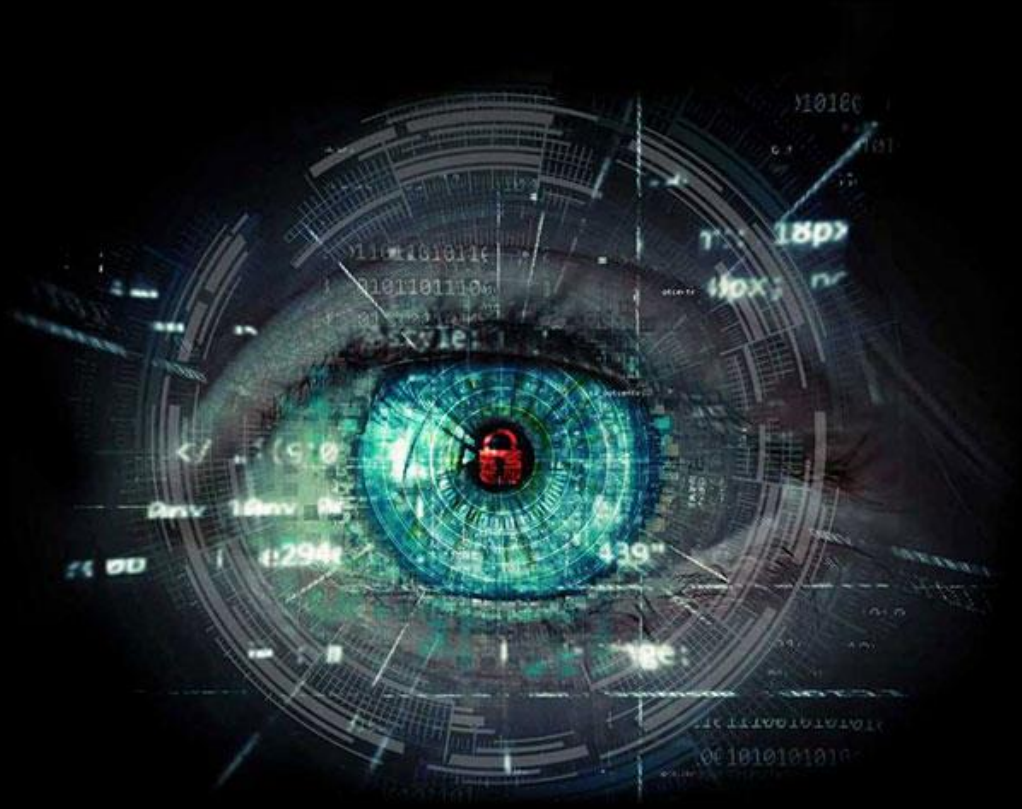
Κυβερνοασφάλεια στην Υγεία της Κρήτης

μια νέα εποχή ανατέλλει

Μοσχοβάκης Γιώργος
Δ/ντής Πληροφορικής
7ης Υγειονομικής Περιφέρειας
[Κρήτης]

Κυβερνοασφάλεια



01 Τι είναι

Η κυβερνοασφάλεια είναι η συλλογή λογισμικού, ανθρώπων, διαδικασιών και συστημάτων που προστατεύουν έναν οργανισμό από μη εξουσιοδοτημένη πρόσβαση και κακόβουλες επιθέσεις διασφαλίζοντας τη διαθεσιμότητα των πόρων

02 Γιατί Είναι Σημαντική

- Προστασία από κακόβουλες επιθέσεις
- Προστασία Ευαίσθητων Πληροφοριών
- Διαθεσιμότητα συστημάτων
- Διατήρηση Επιχειρησιακής Εμπιστοσύνης
- Συμμόρφωση με Κανονισμούς

03 Ποιους αφορά

- Στελέχη πληροφορικής
- Χρήστες
- Διοικήσεις
- ΟΛΟΥΣ!

2022 CRIME TYPES

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

Πηγή: https://www.techopedia.com/

2022 τύποι επιθέσεων

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

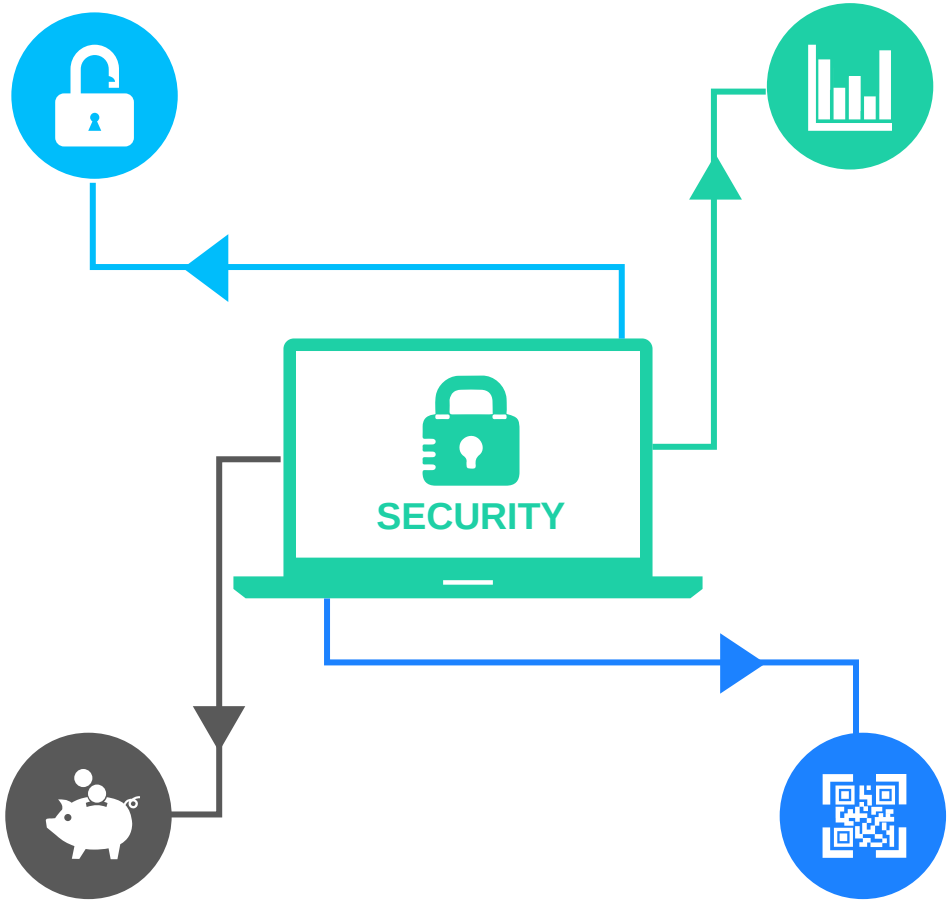
Πόσο ασφαλείς είναι οι κωδικοί πρόσβασης

Υπάρχουσα κατάσταση

στις ΜΥ της Κρήτης

Firewalls σε κάθε μονάδα υγείας

Κάθε μονάδα υγείας έχει κεντρικό firewall (με συγκεκριμένους κανόνες ACL) και δεν επαφίεται μόνο στο κεντρικό firewall του SYZEFXIS



Blacklists

Ορισμένα νοσοκομεία έχουν ιδιαίτερα ανεπτυγμένα προγράμματα ανίχνευσης κακόβουλων emails, άλλες μονάδες έχουν blacklists μη επιτρεπόμενων sites που ανανεώνονται αυτόματα κα

Antivirus σε κάθε μονάδα υγείας

Όλες οι μονάδες υγείας μας έχουν στους υπολογιστές antivirus που ενημερώνεται κεντρικά και σε τακτική βάση

Κανονισμός λειτουργίας

Κάθε χρήστης πληροφοριακών συστημάτων υπογράφει τον **κανονισμό λειτουργίας** πληροφοριακών συστημάτων της μονάδας υγείας που ανήκει, ενώ μέσω αντίστοιχης **αίτησης** του, παίρνει τα διαπιστευτήρια που απαιτούνται για την εργασία του.

Αρκούν τα μέτρα αυτά;

Η απάντηση δυστυχώς είναι ΟΧΙ

CYBERHIMPREX
Cybersecurity of Healthcare
Improved in a X-border perspective

CYBERHIMPREX

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Cybersecurity of Healthcare Improved in a X-border perspective

Αποτελείται από τρεις Οργανισμούς που ασχολούνται με την υγεία (HCOs) που βρίσκονται στην Ελλάδα, την Ιταλία και την Ισπανία, και από το Università Cattolica del Sacro Cuore (Ιταλία) σε ρόλο συντονιστή.

Έχει στόχο τη βελτίωση των δυνατοτήτων κυβερνοασφάλειας των τριών HCOs, αξιοποιώντας επίσης διασυνοριακές λύσεις. Η κυβερνοασφάλεια αποκτάται ενεργώντας, σύμφωνα με ανθρωπο-τεχνικές προσεγγίσεις

- Στην ενημέρωση / εκπαίδευση
- Στην οργάνωση/διαδικασίες
- Στην επένδυση αγοράς συστημάτων ασφαλείας
- Στη προαγωγή της ανταλλαγής δεδομένων και γνώσεων μεταξύ οργανισμών.

11 Δράσεις θα υλοποιηθούν από κοινού από τους HCOs:

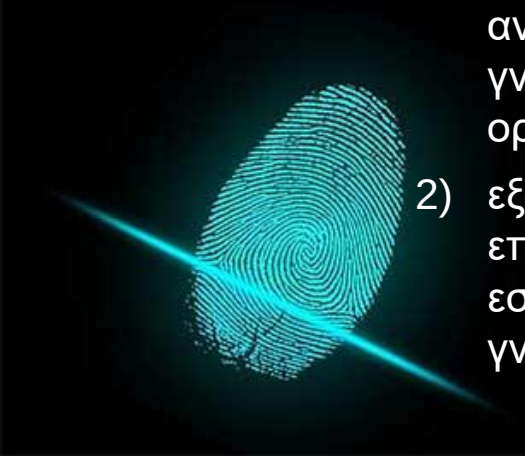
1) Δημιουργία μιας διασυνοριακής εφαρμογής ασφαλούς κοινής χρήσης δεδομένων
2) Βελτίωση της διαδικασίας προμηθειών στον κυβερνοχώρο μέσω της ευθυγράμμισης με τις Οδηγίες ENISA.
3) 7 από τις 11 δράσεις υιοθετούν λύσεις που έχουν αναπτυχθεί από δύο έργα για το H2020: CUREX και PANACEA. Ο Συντονιστής και οι τρεις HCOs υπήρξαν εταίροι σε αυτά τα έργα.
4) περιλαμβάνουν δράσεις προαγωγής ασφάλειας στον κυβερνοχώρο, εκπαίδευση και ευαισθητοποίηση/ανάπτυξη δεξιοτήτων του υγειονομικού προσωπικού.
5) Το έργο θα παραδώσει επίσης μια μελέτη περίπτωσης για να παρέχει στους υπεύθυνους χάραξης πολιτικής με συστάσεις προώθησης, υποστήριξης και διευκόλυνσης
    - της ολιστικής προσέγγισης για την ασφάλεια στον κυβερνοχώρο
    - επενδύσεων για συμμόρφωση με τους κανονισμούς
    - διασυνοριακών πρακτικών

CYBERHIMPREX

CYBERHIMPREX
Cybersecurity of Healthcare
Improved in a X-border perspective

Βασικοί στόχοι

1) Υλοποίηση ενός συνόλου πρωτοβουλιών εμπνευσμένων από την πεποίθηση ότι η κυβερνοασφάλεια επιτυγχάνεται ενεργώντας, σύμφωνα με μια κοινωνικο-τεχνική προσέγγιση, **και στα τρία στοιχεία ενός Οργανισμού Υγείας** (Άνθρωποι, Οργανισμός/Διαδικασίες, Τεχνολογία) και αξιοποιώντας την ανταλλαγή δεδομένων και γνώσεων μεταξύ των οργανισμών
2) εξασφάλιση κατάλληλης επικοινωνίας, διάδοσης και εσωτερικής ανταλλαγής γνώσεων.



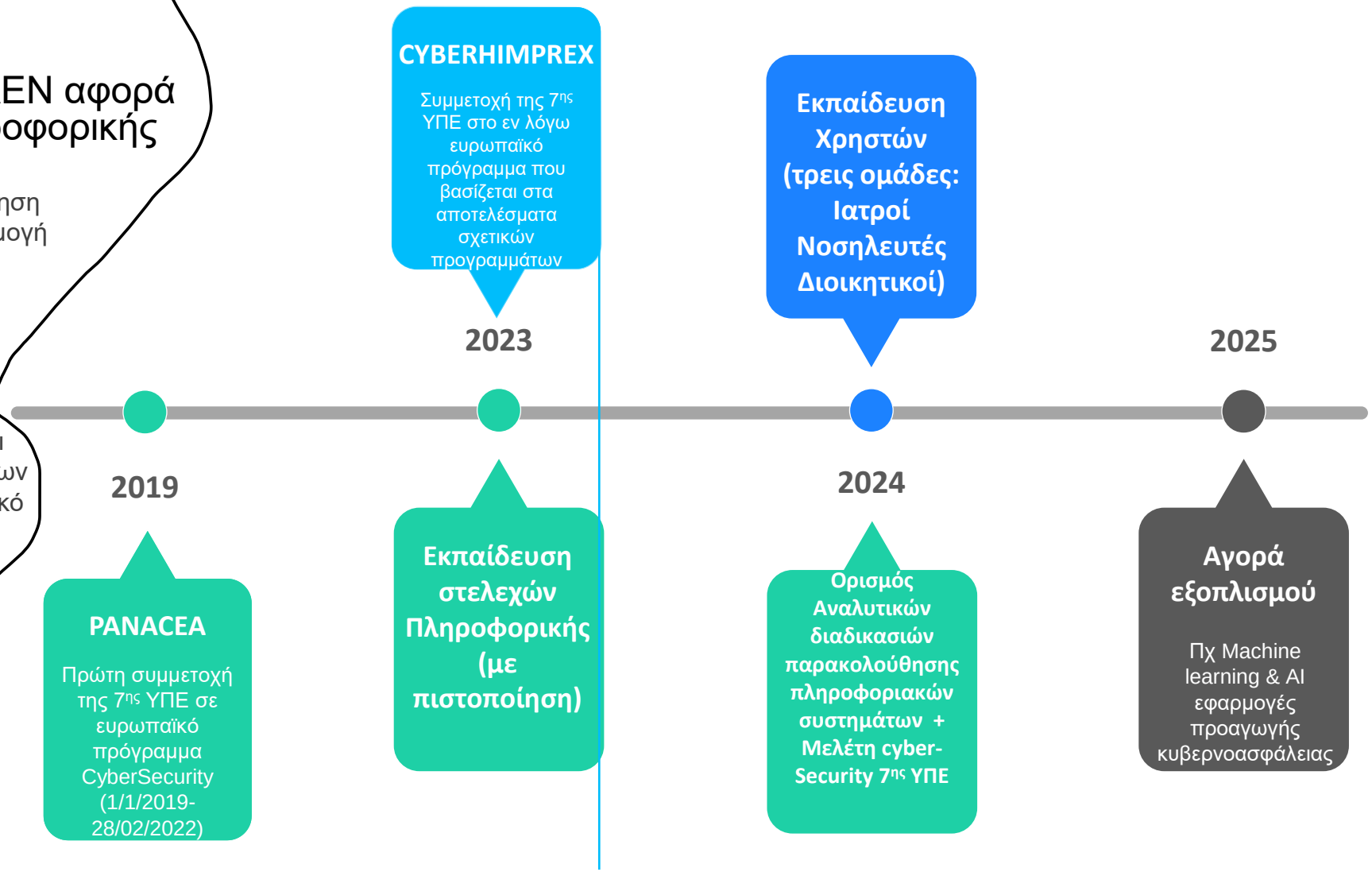
	Investment areas and Lines of intervention		Solution (EU Project)
Cross border Data/Knowledge sharing			
1	Set-up a cross-border inter-organizational secure data sharing capability via a new tool.		SISP (PANACEA)
People			
2	Improve cybersecurity skills of technical staff, via multi-method training		NCSF (CUREX), AWA (ECHO)
3	Raise cybersecurity staff awareness via customized nudging and education pills		SBNT, TECT (PANACEA), CH (CUREX)
4	Set-up the new cybersecurity "angel" role via dedicated training		RGT (PANACEA)
Organization/Processes			
5	Improve cybersecurity orientation of the procurement process via alignment with ENISA guidelines		
6	Improve the cybersecurity governance organization and system via a stakeholder involvement approach and new tools		RGT (PANACEA)
Technology			
7	Improve web navigation system security via *web proxy*.		
8	Improve business continuity via an immutable backup system.		
9	Reduce the Attack Surface via Operating Systems (OS) update		
10	Improve Security by Design capability via new supporting tools		SDSP, CST (PANACEA)

7η ΥΠΕ Κρήτης: Ανατέλλει μια νέα εποχή

Γιατί:

Η κυβερνοασφάλεια ΔΕΝ αφορά μόνο τα στελέχη πληροφορικής

- Αφορά κυρίως την ευαισθητοποίηση **όλων** των χρηστών και προσαρμογή στις διαδικασίες
- Απαιτούνται επενδύσεις τόσο σε software όσο και σε hardware
- Η συνεχής παρακολούθηση είναι επιτακτική, που σημαίνει εκτός των άλλων προσλήψεις σε προσωπικό πληροφορικής



Συμπέρασμα

Απαιτούνται:

- Μελέτη κυβερνοασφάλειας/ευπάθειας. Σημαντική επένδυση στην εκπαίδευση / ενημέρωση των χρηστών. Πιστοποίηση στελεχών πληροφορικής στην ασφάλεια πληροφοριακών συστημάτων.
- Ορισμός πλήρων καταγεγραμμένων διαδικασιών ασφαλείας (πχ σε κάθε είσοδο/μετακίνηση/έξοδο χρήστη) **ΚΑΙ** συμμόρφωση σε αυτές. Συνεχής επικαιροποίηση διαδικασιών ασφαλείας.
- Συστήματα παρακολούθησης της δικτυακής κίνησης ή/και των χρηστών της μονάδας και ενημέρωσης του υπευθύνου ασφαλείας σε πιθανό εντοπισμό απειλής
- Συνεργασία με Εθνικούς οργανισμούς (πχ Εθνικό Φορέα Κυβερνοασφάλειας), ENISA και άλλες μονάδες υγείας, ώστε να καταστεί δυνατή η γρήγορη ενημέρωση/προσαρμογή σε πιθανές επιθέσεις, βέλτιστες πρακτικές κα.

Σας ευχαριστώ

Μοσχοβάκης Γιώργος
Ηλεκτρολόγος Μηχανικός & Μηχανικός Η/Υ ΕΜΠ, Msc
Δ/ντής Πληροφορικής 7ης ΥΠΕ