ΠΛΗΡΩΜΕΝΟ ΤΕΛΟΣ
Τ.Υ.Π.Α. Γραφείο Κ.Κ. ΠΑΤΡΑΣ
Αριθμός Αδείας 34
Κωδικός 2581
ΕΚΔΟΤΗΣ
ΕΛΤΑ Hellenic Post

Αφιέρωμα
& Ημερίδα για την Κυβερνοασφάλεια

Σελ. 2, 7-18

ΟΜΙΛΗΤΕΣ ΗΜΕΡΙΔΑΣ

Η Εβδομαδιαία
Οικονομική Εφημερίδα της Αχαΐας

Μαιζώνος 94 | 262 21 Πάτρα
Τηλ: 2610 620 574

www.symboulos.gr
e-mail: symboulo@otenet.gr
Τιμή Φύλλου: 1,00 €

Περίοδος Γ' | **Αρ. Φύλλου 1370**
Παρασκευή 20 Σεπτεμβρίου 2024

Σύμβουλος επιχειρήσεων

27ο Forum Ανάπτυξης 2024 Υβρίδιο 23-24 Νοεμβρίου
Σελ. 18

ΡΟΜΑΝΤΖΑ
Αντιπαράθεση για αντλιοστάσιο

Αντίθετο στην ανέγερση του αντλιοστασίου στην περιοχή της Ρομάντζας είναι το ΤΕΕ Δυτικής Ελλάδος, προτείνοντας την λύση της υπογειοποίησης. Ο Δήμος από την πλευρά του υποστηρίζει ότι δεν θα προκύψει όχληση καθώς «θα κατασκευαστεί ένας οικίσκος, ύψους 3 μέτρων, σε έναν χώρο 2,2 στρεμμάτων».

Σελ. 19

Ρήξη στον ΕΕΣΠ

Και επισήμως αποχώρησε η πρόεδρος του ΕΕΣΠ Ερμιόνη Διονυσάτου από την παράταξη του Γιώργου Βαγενά, ζητώντας συστράτευση για τα προβλήματα.

Σελ. 3

> Ανάπλαση παραλιακού Μετώπου Πάτρας με προϋπολογισμό 12 εκ. ευρώ

Νέο Όραμα

και ζητήματα χρηματοδότησης για τις παρεμβάσεις

Μεγάλο ζητούμενο είναι ο χρόνος ολοκλήρωσης, καθώς είναι πιθανό το επόμενο διάστημα να υποβληθούν ενστάσεις. Θα αλλάξει όψη η παραλιακή ζώνη της Πάτρας που ορίζεται μεταξύ των οδών Ηρώων Πολυτεχνείου – Όθωνος Αμαλίας – Ακτή Δυμαίων έως τις προβολές των οδών Π. Κανελλοπούλου και Ε. Βενιζέλου και επί πλέον στο τμήμα που ορίζεται δυτικά της οδού Αώου.

Με το ποσό των 12 εκατομμυρίων ευρώ θα χρηματοδοτηθεί το έργο της ανάπλασης του παραλιακού μετώπου της Πάτρας. Στόχος η ανάδειξη του μόλου της Αγίου Νικολάου αλλά και η σύνδεση της περιοχής με τις αναπλάσεις που είναι σε εξέλιξη.

Ο Περιφερειάρχης Νεκτάριος Φαρμάκης εκφράζει την ικανοποίησή του για την ένταξη. Ο Αντιδήμαρχος Πολεοδομικού Σχεδιασμού του Δήμου Πατρέων Παναγιώτης Μελάς θεωρεί ωστόσο ότι τα 12 εκατομμύρια ευρώ είναι λίγα για το εύρος των παρεμβάσεων που έχουν αποφασιστεί και θεωρεί επιβεβλημένη την εξεύρεση και άλλων πόρων για να ολοκληρωθεί το έργο.

Σελ. 4

ολοΓραφία

Του **Παναγιώτη Γιαλένιου**

Καθημερινότητα και Κυβερνοασφάλεια

Τα ζητήματα της Κυβερνοασφάλειας έχουν γίνει πλέον αναπόσπαστο κομμάτι της καθημερινότητάς μας, καθώς όλο και περισσότερα περιστατικά επιθέσεων έρχονται στο φως. Ένα χαρακτηριστικό παράδειγμα συνέβη πριν λίγες μέρες σε μια έμπορο της περιοχής μας, η οποία ξαφνικά είδε έναν σεβαστό ποσό να εξαφανίζεται από τον τραπεζικό της λογαριασμό. Όπως η ίδια εξομολογήθηκε, «Σάστισα και έδωσα στοιχεία». Οι δράστες ήταν επιτήδειοι κυβερνοαπατεώνες, που την παγίδευσαν με πειστικές ψεύτικες πληροφορίες.

Τα περιστατικά αυτά δεν περιορίζονται μόνο σε μεμονωμένους πολίτες, αλλά αφορούν επίσης δημόσιους φορείς και μεγάλους οργανισμούς. Πρόσφατα, το Πυροσβεστικό Σώμα υπήρξε θύμα μιας κυβερνοεπίθεσης, όταν στον λογαριασμό του σε γνωστό μέσο κοινωνικής δικτύωσης δημοσιεύτηκε ανάρτηση που ανέφερε ότι ο λογαριασμός είχε χακαριστεί.

Οι επιθέσεις αυτού του είδους δεν είναι σπάνιες, ούτε περιορισμένες. Τις τελευταίες μόνο ημέρες, ο κυβερνοχώρος έχει βιώσει εκατοντάδες περιστατικά μικρής ή μεγάλης κλίμακας, υπογραμμίζοντας την επιτακτική ανάγκη για αποτελεσματική κυβερνοασφάλεια.

Ξεχωριστό γεγονός που απασχολεί τις τελευταίες ημέρες την παγκόσμια επικαιρότητα είναι η διήμερη επίθεση του Ισραήλ στα συστήματα επικοινωνίας τη Χεσμπολάχ στο Λίβανο , που άφησε πίσω της 26 νεκρούς και πάνω από 3.200 τραυματίες. Αυτά τα περιστατικά τονίζουν την παγκόσμια διάσταση του προβλήματος, καθώς κυβερνοεπιθέσεις δεν γνωρίζουν σύνορα. Να σημειωθεί ότι χώρες όπως το Ισραήλ ηγούνται της παγκόσμιας προσπάθειας για την αντιμετώπιση κυβερνοεπιθέσεων. Το Ισραήλ κατέχει το 40% των παγκόσμιων επενδύσεων στον τομέα, ενώ η κυβερνοασφάλεια έχει ενσωματωθεί στην εκπαίδευση, από τα σχολεία μέχρι τα πανεπιστήμια.

Μπροστά σε αυτή την αυξανόμενη απειλή, η ευαισθητοποίηση και η ενημέρωση είναι καθοριστικές. Με αυτό το στόχο, ο «Σ.Ε.» διοργανώνει την Δευτέρα 23 Σεπεμβρίου, στην Πάτρα ημερίδα με τίτλο «Ψηφιακός μετασχηματισμός και Κυβερνοασφάλεια: κίνδυνοι, υποχρεώσεις και ευκαιρίες». (Σχετικό αφιέρωμα έχουμε σήμερα στις σελ 7-18).

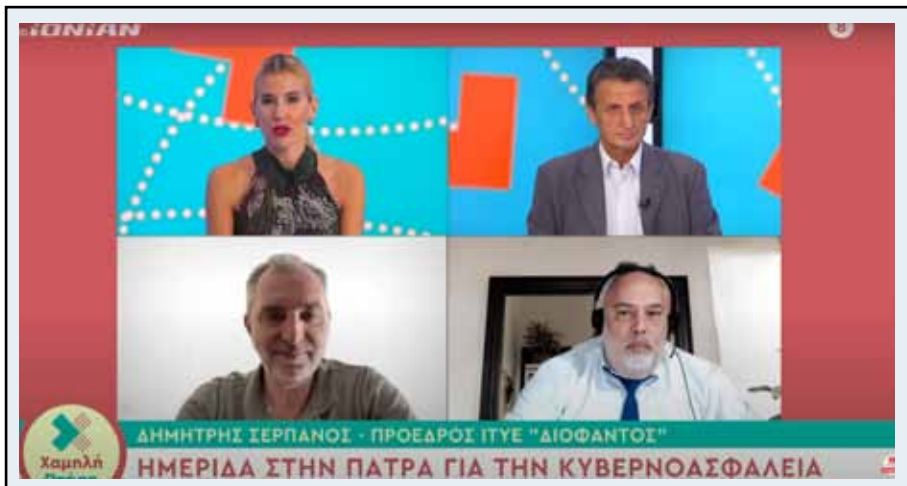
Η Ημερίδα θα επικεντρωθεί στις προκλήσεις της κυβερνοασφάλειας, ειδικά ενόψει της εφαρμογής του ευρωπαϊκού κανονιστικού πλαισίου NIS 2 τον Οκτώβριο, το οποίο θέτει νέες αυστηρότερες υποχρεώσεις για τις επιχειρήσεις. Ο κανονισμός NIS 2 αποτελεί ενίσχυση του αρχικού κανονισμού, με στόχο την καλύτερη προστασία των κρίσιμων τομέων της οικονομίας, όπως η υγεία, η ενέργεια και οι ψηφιακές υποδομές.

Οι συμμετέχοντες στην ημερίδα θα έχουν την ευκαιρία να ενημερωθούν για τις εξελίξεις σε καινοτόμα εργαλεία κυβερνοασφάλειας, όπως η χρήση τεχνητής νοημοσύνης, κρυπτογραφικών τεχνικών και συστημάτων ανίχνευσης απειλών. Επιπλέον, θα συζητηθούν οι ευκαιρίες που προκύπτουν από την υιοθέτηση αυτών των τεχνολογιών, όπως η μείωση του κόστους από πιθανές απώλειες δεδομένων ή η ενίσχυση της εμπιστοσύνης με τους πελάτες.

Οι ομιλίες και οι παρουσιάσεις θα δώσουν στους συμμετέχοντες μια σφαιρική εικόνα των νέων τάσεων στην κυβερνοασφάλεια και θα προσφέρουν πρακτικές συμβουλές για τη θωράκιση των επιχειρήσεων από τις κυβερνοαπειλές. Σημαντικές εταιρείες όπως η Space Hellas και η Dell Technologies θα παρουσιάσουν ολοκληρωμένες λύσεις, ενώ εκπρόσωποι φορέων θα μιλήσουν για τις δράσεις που έχουν αναλάβει έως τώρα.

Η διοργάνωση της ημερίδας δεν είναι τυχαία, καθώς η κυβερνοασφάλεια αποτελεί θεμελιώδη παράγοντα για την επιβίωση και ανάπτυξη των επιχειρήσεων στη σημερινή ψηφιακή εποχή.

Στους συμμετέχοντες θα χορηγηθούν πιστοποιητικά παρακολούθησης, προσθέτοντας επιπλέον κίνητρο για την ενεργή συμμετοχή.



> *Ενόψει της πολύ ενδιαφέρουσας Ημερίδας για την Κυβερνοασφάλεια, που διοργανώνει ο «Σύμβουλος Επιχειρήσεων», ο κορυφαίος περιφερειακός τηλεοπτικός σταθμός Ionian TV μας φιλοξένησε στην εκπομπή του «ΧΑΜΗΛΗ ΠΤΗΣΗ», που παρουσιάζει η εκλεκτή δημοσιογράφος Αγγελική Σπυροπούλου. Μαζί με τον Πρόεδρο του ΙΤΥΕ «Διόφαντος» καθ. Δημήτριο Σερπάνο και τον κ. Γιάννη Αναστασάκο, Γενικό Διευθυντή Sales & System Integration της Space Hellas αναφερθήκαμε στην επικαιρότητα το θέματος της Κυβερνοασφάλειας και στους λόγους που αξίζει, ιδιοκτήτες και Διευθυντές επιχειρήσεων (CEOs, COOs, Γενικοί Διευθυντές, Οικονομικοί Διευθυντές), Διευθυντικά στελέχη πληροφορικής (CIOs, IT Directors, IT Managers), εκπρόσωποι της Τοπικής Αυτοδιοίκησης και οργανισμών, της Πανεπιστημιακής και ερευνητικής κοινότητας και εκπρόσωποι επιχειρήσεων και φορέων τεχνολογίας να είναι παρόντες στην Ημερίδα της Δευτέρας. Δείτε το επεισόδιο της εκπομπής «ΧΑΜΗΛΗ ΠΤΗΣΗ» στο κανάλι του IONIAN TV.*

Ένα εικονικό Φαρμακείο στη Θεσσαλονίκη και το μήνυμά του

Ο Φαρμακευτικός Σύλλογος Θεσσαλονίκης (ΦΣΘ) με το βλέμμα στραμμένο στο μέλλον, πρωτοπορεί και αναδεικνύει τον σημαντικό ρόλο του φαρμακοποιού στη σύγχρονη κοινωνία.

Με αφορμή τον εορτασμό της Παγκόσμιας Ημέρας Φαρμακοποιού, που έχει οριστεί στις 25 Σεπτεμβρίου, ο ΦΣΘ διοργανώνει ένα συμβολικό αλλά και ενημερωτικό γεγονός την Κυριακή 22 Σεπτεμβρίου.

Συγκεκριμένα, ένα εικονικό φαρμακείο θα στηθεί στο χώρο μπροστά από το Βασιλικό Θέατρο, στην παραλία της Θεσσαλονίκης, από τις 10 το πρωί έως τις 7 το βράδυ. Στόχος της εκδήλωσης αυτής είναι η ενημέρωση του κοινού για τις πολλαπλές υπηρεσίες που παρέχουν τα φαρμακεία και η ευαισθητοποίηση σε θέματα υγείας. Οι πολίτες θα έχουν την ευκαιρία να συζητήσουν με εθελοντές φαρμακοποιούς-μέλη του ΦΣΘ και να ενημερωθούν για σημαντικά ζητήματα, όπως η δωρεάν διάθεση self tests για τον καρκίνο του παχέος εντέρου, οι εμβολιασμοί ενηλίκων, η σωστή χρήση των αντιβιοτικών και ο ρόλος της άσκησης και της διατροφής στην πρόληψη και αντιμετώπιση του διαβήτη.

Παράλληλα, θα υπάρχουν ενημερωτικά περίπτερα από φαρμακευτικές εταιρείες με πληροφορίες για προϊόντα που διατίθενται στα φαρμακεία, προσφέροντας χρήσιμα έντυπα για θέματα υγείας. Το βράδυ της ίδιας ημέρας, ο Λευκός Πύργος θα φωταγωγηθεί με πράσινο χρώμα, στέλνοντας ένα ισχυρό μήνυμα υπέρ της δημόσιας υγείας και του ρόλου του φαρμακοποιού.

Το φετινό μήνυμα της Παγκόσμιας Ημέρας Φαρμακοποιού είναι «Φαρμακοποιοί: ικανοποιώντας τις ανάγκες υγείας παγκοσμίως». Οι φαρμακοποιοί, ως αναπόσπαστο κομμάτι της Πρωτοβάθμιας Φροντίδας Υγείας, συμβάλλουν ενεργά με την επιστημονική τους κατάρτιση και τις δεξιότητές τους στην ενίσχυση των εθνικών συστημάτων υγείας. Με τη συνεχή εκπαίδευση και την ενημέρωση, εξασφαλίζουν ότι οι ασθενείς έχουν πρόσβαση σε ασφαλή και αποτελεσματική φαρμακευτική αγωγή. Έτσι, ο ρόλος τους αναδεικνύεται κρίσιμος, τόσο σε τοπικό όσο και σε παγκόσμιο επίπεδο, για την προαγωγή της υγείας και την αντιμετώπιση των σύγχρονων προκλήσεων στο χώρο της υγειονομικής περίθαλψης.

Ένα ερώτημα από την πλευρά μας: Έχει προγραμματίσει ο τοπικός Φαρμακευτικός Σύλλογος κάποιες δράσεις ή εκδηλώσεις για την Παγκόσμια Ημέρα Φαρμακοποιού; Παράλληλα, με δεδομένες τις ραγδαίες εξελίξεις στον τομέα της φαρμακευτικής, διοργανώνονται συζητήσεις, συναντήσεις ή άλλες πρωτοβουλίες με τη συμμετοχή της τοπικής κοινωνίας και υπό την αιγίδα του Συλλόγου; Ειδικότερα, με την παρουσία ενός ισχυρού πανεπιστημιακού Φαρμακευτικού Τμήματος στην περιοχή, υπάρχει κάποια συνεργασία με στόχο την ανάδειξη καινοτόμων προσεγγίσεων και την ενίσχυση του διαλόγου γύρω από τα φαρμακευτικά θέματα;

Κυβερνοασφάλεια

Γράφουν στον «Σ.Ε.»

Χρήστος Μπούρας
Πρύτανης Πανεπιστημίου Πατρών

Δημήτρης Σερπάνος
Πρόεδρος ΙΤΥΕ «Διόφαντος»

Αθανάσιος Ζούπας
Πρόεδρος Δικηγορικού Συλλόγου Πατρών

Στέφανος Μίχος
Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών, Αποκεντρωμένη Διοίκηση Πελ/σου, Δυτ. Ελλάδας & Ιονίου

Νικόλαος Γ. Σκλάβος
Καθηγητής, Τμήμα Μηχανικών Η/Υ και Πληροφορικής, Πανεπιστήμιο Πατρών

Πέτρος Γανός
Προϊστάμενος Τμήματος Σχεδιασμού και Μελετών Ψηφιακών Συστημάτων Δήμου Πατρέων

Οι Νέες Προκλήσεις και οι Απαιτήσεις για την Κυβερνοασφάλεια

Η πρόσφατη παγκόσμια διακοπή λειτουργίας συστημάτων που επηρέασε αεροδρόμια, μέσα μαζικής μεταφοράς, τράπεζες και μέσα ενημέρωσης ανέδειξε την ευαλωτότητα των τεχνολογικών υποδομών. Το περιστατικό, που προκλήθηκε από προβληματική ενημέρωση λογισμικού και όχι από κυβερνοεπίθεση, υπογραμμίζει την ανάγκη για ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και της ανθεκτικότητας των δικτύων. Σε έναν ολοένα και πιο διασυνδεδεμένο κόσμο, όπου οι επιπτώσεις από τέτοια συμβάντα μπορούν να είναι εκτεταμένες, η προστασία των κρίσιμων υποδομών γίνεται υψίστης σημασίας.

Η κυβερνοασφάλεια αποτελεί ένα από τα πιο κρίσιμα ζητήματα της ψηφιακής εποχής, με τις απειλές στο κυβερνοχώρο να αυξάνονται και να εξελίσσονται ραγδαία. Από την προστασία προσωπικών δεδομένων μέχρι την ασφάλεια των δικτύων κρίσιμων υποδομών, οι επιχειρήσεις και οι οργανισμοί καλούνται να ενισχύσουν τις άμυνές τους για να προστατεύσουν τόσο την ίδια την ύπαρξή τους όσο και την εμπιστοσύνη των πελατών και των συνεργατών τους.

Σε αυτό το πλαίσιο, η νέα οδηγία της Ευρωπαϊκής Ένωσης, NIS II, έρχεται να οριοθετήσει ένα σύγχρονο και απαιτητικό πλαίσιο για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων, επιβάλλοντας αυστηρότερες υποχρεώσεις στις επιχειρήσεις και τους οργανισμούς. Οι αλλαγές που επιφέρει η οδηγία αυτή δεν είναι απλά θέμα συμμόρφωσης με τους κανονισμούς, αλλά αντανακλούν την ανάγκη για την ενίσχυση της κυβερνοασφάλειας σε μια εποχή όπου οι επιθέσεις γίνονται όλο και πιο σύνθετες και απειλητικές.

Η τεχνολογία είναι αναπόσπαστο κομμάτι της καθημερινότητας, με τις περισσότερες επιχειρήσεις να εξαρτώνται άμεσα από τα ψηφιακά τους δίκτυα για να λειτουργήσουν. Από τραπεζικές συναλλαγές και αγορές μέσω διαδικτύου μέχρι υπηρεσίες υγείας και διακυβέρνησης, η εξάρτηση από τον κυβερνοχώρο είναι πλέον καθολική. Η ανάγκη για προστασία αυτών των συστημάτων από κακόβουλες επιθέσεις είναι, επομένως, επιτακτική.

Η κυβερνοασφάλεια δεν περιορίζεται μόνο στην προστασία από ιούς και ηλεκτρονικές παραβιάσεις. Περιλαμβάνει ένα ευρύ φάσμα μέτρων και τεχνολογιών, που διασφαλίζουν την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριών.

Η αυξημένη εξάρτηση από το διαδίκτυο, σε συνδυασμό με τη ραγδαία ανάπτυξη του Internet of Things (IoT) και της τεχνητής νοημοσύνης, δημιουργούν ένα περιβάλλον όπου οι κίνδυνοι είναι πιο διαδεδομένοι από ποτέ. Οι συνέπειες μιας κυβερνοεπίθεσης μπορεί να είναι καταστροφικές, περιλαμβάνοντας απώλεια δεδομένων, οικονομικές ζημίες, νομικές ευθύνες και, σε κάποιες περιπτώσεις, απώλεια ζωής. Έτσι, η επένδυση στην κυβερνοασφάλεια δεν είναι απλά μια επιλογή, αλλά αναγκαιότητα για κάθε οργανισμό που θέλει να επιβιώσει και να αναπτυχθεί στο σημερινό ψηφιακό τοπίο.

Η Οδηγία NIS II: Υποχρεώσεις και Ευθύνες

Η οδηγία NIS II, που εκδόθηκε από την Ευρωπαϊκή Ένωση, αντικαθιστά την πρώτη οδηγία NIS (Network and Information Systems Directive), θέτοντας πιο αυστηρούς κανόνες για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων. Στόχος της είναι να αντιμετωπίσει τις νέες προκλήσεις της ψηφιακής εποχής και να ενισχύσει την ανθεκτικότητα των κρίσιμων υποδομών απέναντι στις κυβερνοαπειλές.

Η οδηγία επεκτείνει τις υποχρεώσεις συμμόρφωσης σε περισσότερους τομείς, όπως η υγεία, η ενέργεια, οι τράπεζες, οι χρηματοπιστωτικές αγορές και οι ψηφιακές υπηρεσίες. Οι οργανισμοί αυτοί καλούνται να εφαρμόσουν μέτρα που διασφαλίζουν την ανθεκτικότητα των πληροφοριακών συστημάτων τους και να αναπτύξουν πολιτικές διαχείρισης κινδύνου. Επιπλέον, η NIS II εισάγει πιο αυστηρές κυρώσεις για τη μη συμμόρφωση, συμπεριλαμβανομένων σημαντικών οικονομικών προστίμων.

Μια από τις κύριες αλλαγές της NIS II είναι η διεύρυνση του φάσματος των επιχειρήσεων που υπόκεινται σε αυτήν. Ενώ η αρχική οδηγία NIS επικεντρώθηκε σε ορισμένους κρίσιμους τομείς, η νέα οδηγία καλύπτει περισσότερους οργανισμούς και επιχειρήσεις, συμπεριλαμβανομένων των παρόχων ψηφιακών υπηρεσιών και των εταιρειών που δραστηριοποιούνται στον τομέα της πληροφορικής. Αυτή η διεύρυνση αποσκοπεί στην αποτελεσματικότερη προστασία του ψηφιακού οικοσυστήματος της Ευρώπης.

Επιπλέον, η NIS II ενισχύει τη συνεργασία μεταξύ των κρατών μελών της Ε.Ε. μέσω της ανταλλαγής πληροφοριών και της ανάπτυξης κοινών μεθοδολογιών για την αντιμετώπιση των κυβερνοαπειλών. Η έμφαση στην έγκαιρη ανίχνευση και ανταπόκριση στις απειλές είναι βασικό στοιχείο της οδηγίας, καθώς η πρόληψη και η ταχεία αντίδραση αποτελούν κλειδιά για την επιτυχή αντιμετώπιση των κινδύνων.

Η ανάγκη για ισχυρή κυβερνοασφάλεια δεν είναι πλέον ζήτημα επιλογής, αλλά μια αδήριτη αναγκαιότητα για όλους τους οργανισμούς, ανεξαρτήτως μεγέθους ή τομέα δραστηριότητας. Η οδηγία NIS II δεν έρχεται απλά για να επιβάλλει κανόνες, αλλά για να θέσει τις βάσεις για έναν πιο ασφαλή και ανθεκτικό ψηφιακό κόσμο.

Σε αυτή την κατεύθυνση, οι επιχειρήσεις καλούνται να επενδύσουν σε τεχνολογίες και ανθρώπινο δυναμικό, να αναπτύξουν κουλτούρα ασφάλειας και να υιοθετήσουν στρατηγικές διαχείρισης κινδύνου που θα τις θωρακίσουν απέναντι στις διαρκώς αυξανόμενες απειλές. Η συμμόρφωση με τις απαιτήσεις της NIS II δεν θα πρέπει να θεωρείται απλώς ως μια νομική υποχρέωση, αλλά ως μια ευκαιρία για ενίσχυση της αξιοπιστίας και της ανταγωνιστικότητας σε μια παγκοσμιοποιημένη αγορά.

Η εποχή απαιτεί εγρήγορση και προσαρμοστικότητα. Σε έναν κόσμο όπου οι επιθέσεις στον κυβερνοχώρο μπορούν να πλήξουν την κοινωνική σταθερότητα και την οικονομική ανάπτυξη, η κυβερνοασφάλεια δεν αφορά μόνο τους ειδικούς. Είναι ευθύνη όλων, από τους οργανισμούς και τις επιχειρήσεις μέχρι τα ίδια τα κράτη, να λάβουν τα κατάλληλα μέτρα για την προστασία του ψηφιακού μέλλοντος.

Στην επικαιρότητα των ζητημάτων που αφορούν την Κυβερνοασφάλεια αναφέρεται το σημερινό αφιέρωμα του «Σ.Ε» με εξαιρετικά άρθρα ειδικών από πολλούς χώρους. Τα κείμενά τους θα αξιοποιηθούν και στην σημαντική εκδήλωση που διοργανώνει η εφημερίδα την Δευτέρα 23 Σεπτεμβρίου από 10:00 -14:00 στο ξενοδοχείο My Way στην Πάτρα (Όθωνος Αμαλίας 16).

Η Ημερίδα είναι ενταγμένη στο πλαίσιο των δράσεων του «Δικτύου Forum Ανάπτυξης» και θα είναι υβριδική (με φυσική παρουσία ομιλητών και συνέδρων στο ξενοδοχείο My Way στην Πάτρα, ενώ θα μεταδίδεται ζωντανά από το επίσημο site της διοργάνωσης www.forumanaptixis.gr και πολλά συνεργαζόμενα social media).

Αναλυτικά για το πρόγραμμα της Ημερίδας στη γειτονική σελίδα. Όλα όσα διαμειφθούν σε αυτή θα παρουσιάσουμε στο επόμενο φύλλο μας. Τα video της εκδήλωσης που θα μεταδοθεί live μέσω της πλατφόρμας www.forumanaptixis.gr θα είναι αναρτημένα στη συνέχεια στη σχετική ενότητα για on demand θέαση ανα πάσα στιγμή από κάθε ενδιαφερόμενο.

Ημερίδα Κυβερνοασφάλειας

«Ψηφιακός μετασχηματισμός και κυβερνοασφάλεια: Κίνδυνοι, υποχρεώσεις και ευκαιρίες»

23 Σεπτεμβρίου 2024, Ξεν. «My Way» Πάτρα - Live: www.forumanaptixis.gr

Αναλυτικό Πρόγραμμα

9:30-10:00 Προσέλευση-Εγγραφές – Καφές

Α΄ ΕΝΟΤΗΤΑ 10:00-12:00

«Νέες οδηγίες και κανονισμοί για την Κυβερνοασφάλεια – Κίνδυνοι και υποχρεώσεις»

Προεδρείο: **Δημήτρης Σερπάνος**, Πρόεδρος ΙΤΥΕ «Διόφαντος», **Παναγιώτης Γιαλένιος**, εκδότης εφ. «Σύμβουλος Επιχειρήσεων»

ΧΑΙΡΕΤΙΣΜΟΙ

Χρήστος Μπούρας, Πρύτανης Πανεπιστημίου Πατρών

Πλάτων Μαρλαφέκας, Πρόεδρος Επιμελητηρίου Αχαΐας

Κλεομένης Μπάρλος, Πρόεδρος Συνδέσμου Επιχειρήσεων και Βιομηχανιών Πελοποννήσου και Δυτικής Ελλάδος

Νάντια Λιάπη, Group CIO, Group Director GRC Services, Space Hellas

ΟΜΙΛΗΤΕΣ

Δημήτρης Σερπάνος, Πρόεδρος ΙΤΥΕ «Διόφαντος», Καθηγητής Πανεπιστημίου Πατρών

Θέμα: Κυβερνοασφάλεια: Κίνδυνοι, Απειλές και Άμυνες

Ιωάννης Αλεξάκης, Γεν. Διευθυντής Επιτελικού Σχεδιασμού, Εθνική Αρχή Κυβερνοασφάλειας

Θέμα: Εθνική Αρχή Κυβερνοασφάλειας: Στρατηγική και Στόχοι

Γεώργιος Στεργιόπουλος, Επίκουρος Καθηγητής, Πανεπιστήμιο Αιγαίου

Θέμα: Κατακτώντας το NIS2: Οδηγός για την Πλοήγηση στην Οδηγία ΕΕ 2022/2555

Β΄ ΕΝΟΤΗΤΑ 12:00-14:00

«Ανάπτυξη τεχνολογικών εφαρμογών Κυβερνοασφάλειας - Λύσεις και ευκαιρίες»

Προεδρείο: **Αθανάσιος Ζούπας** πρόεδρος Δικηγορικού Συλλόγου Πατρών, **Παναγιώτης Γιαλένιος**, εκδότης εφ. «Σύμβουλος Επιχειρήσεων»

ΠΑΡΟΥΣΙΑΣΕΙΣ

Νάντια Λιάπη, Group CIO, Group Director GRC Services, Space Hellas

Θέμα: «Thank God for NIS II»

Σταμάτης Τσολακίδης, Data Center Sales Executive, Greece, Cyprus & Malta, Dell Technologies

Θέμα: «Recovering Your Business from a Sophisticated Ransomware or Cyberattack»

Σωκράτης Κελέσογλου, Senior Cybersecurity Presales Consultant, Space Hellas

Θέμα: «NIS 2 in Practice»

Αντιγόνη Δόβα, Field Product Manager, Dell Client solutions

Θέμα: «Security on End User devices»

Δρ. Θεόδωρος Κομνηνός, Διευθυντής Πληροφοριακών Συστημάτων, Εφαρμογών και Κυβερνοασφάλειας, ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ

Θέμα: «Κυβερνοασφάλεια σε δημόσια πληροφοριακά συστήματα και εφαρμογές»

Δημήτρης Ανεστόπουλος, Προϊστάμενος Διεύθυνσης Ψηφιακής Διακυβέρνησης ΠΔΕ

Θέμα: «Ζητήματα Κυβερνοασφάλειας στην Περιφέρεια Δυτ. Ελλάδας»

Δρ. Στέφανος Μίχος, Υπ. Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών, Αποκεντρωμένη Διοίκηση Πελ/σου, Δυτ. Ελλάδας & Ιονίου

Θέμα: «Θωράκιση κρίσιμων υποδομών, ασφάλεια και νέες τεχνολογίες»

Δρ. Πέτρος Γανός, Προϊστάμενος Τμήματος Σχεδιασμού και Μελετών Ψηφιακών Συστημάτων Δήμος Πατρέων

Θέμα: «Κυβερνοασφάλεια στην Τοπική Αυτοδιοίκηση»

Πολιτικές του Πανεπιστημίου Πατρών για την κυβερνοασφάλεια

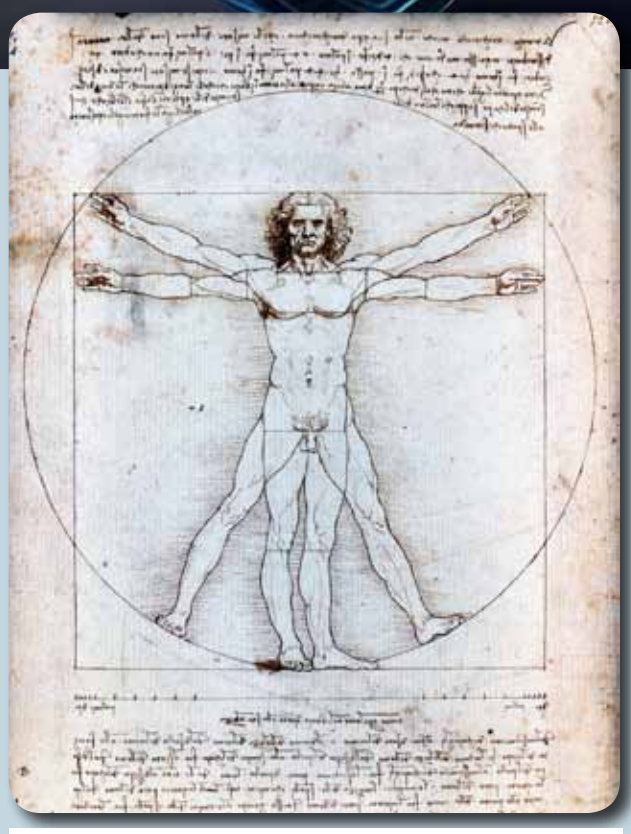
Γράφει ο ***Χρήστος Μπούρας***

Η πολιτική του Πανεπιστημίου Πατρών για την κυβερνοασφάλεια βασίζεται σε μια διαστρωματωμένη προσέγγιση που ξεκινά από την ασφάλεια άυλων πόρων όπως το λογισμικό και τα δεδομένα, συνεχίζει στην ασφάλεια των servers και του δικτύου και καταλήγει στη φυσική ασφάλεια των κρίσιμων υποδομών ενώ ο έλεγχος και η καταγραφή πρόσβασης διατρέχει τα στρώματα που συνιστούν την κυβερνοασφάλεια κάθετα.

Η ασφάλεια λογισμικού και δεδομένων σκοπεύει να εγγυηθεί την ορθή και αποδοτική λειτουργία του λογισμικού, την ακεραιότητα και ασφάλεια των σημαντικών δεδομένων και να προστατεύσει χρήστες και υποδομές από κακόβουλο λογισμικό. Η προστασία από κακόβουλο λογισμικό γίνεται με χρήση μηχανισμών ασφαλείας content filtering με έμφαση στην κύρια πηγή εισόδου κακόβουλου λογισμικού που είναι τα εισερχόμενα e-mails. Για την ασφαλή λειτουργία των λογισμικών χρησιμοποιούνται αξιόπιστες και ενημερωμένες πλατφόρμες ανάπτυξης εφαρμογών καθώς και βιβλιοθήκες λογισμικού που προέρχονται από έμπιστες πηγές και συντηρούνται ενεργά. Επιπλέον, τα λειτουργικά συστήματα είναι ενημερωμένα και ρυθμισμένα με ασφαλή τρόπο. Για την ασφάλεια των δεδομένων, λαμβάνονται αντίγραφα ασφαλείας από όλα τα σημαντικά συστήματα πληροφορικής σε ημερήσια βάση, συνδυάζοντας με τον κατάλληλο τρόπο τις διαθέσιμες τεχνολογίες (full, incremental, differential). Υποδομές εικονικών μηχανών (virtual machines) γίνονται backup τόσο σε επίπεδο πλήρους VM όσο και σε επίπεδο των περιεχόμενων δεδομένων. Ο έλεγχος ακεραιότητας των αντιγράφων ασφαλείας γίνεται σε περιοδική βάση. Τηρείται κατάλογος με όλα τα χρησιμοποιούμενα λογισμικά ώστε ανά πάσα στιγμή να είναι δυνατός ο έλεγχος της κατάστασης ενημέρωσής τους.

Τέλος, ο χειρισμός και η προστασία των δεδομένων γίνεται με τέτοιο τρόπο, ώστε να διευκολύνεται η εφαρμογή του Γενικού Κανονισμού Προστασίας δεδομένων (GDPR).

Οι servers και οι σταθμοί εργασίας του ιδρύματος είναι διαμορφωμένοι με όλες τις βασικές ρυθμίσεις ασφάλειας με βάση διεθνώς αποδεκτά πρότυπα και οδηγίες για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών. Χρησιμοποιούνται μόνο υποστηριζόμενες εκδόσεις των λειτουργικών συστημάτων ενώ βρίσκονται προστατευμένοι πίσω από firewall ρυθμισμένο με την αρχή των λιγότερων δυνατών προσβάσεων. Γίνεται απενεργοποίηση λογαριασμών που δεν σχετίζονται πλέον με κάποιον χρήστη ενώ γίνεται εκχώρηση ελάχιστων απαιτούμενων δικαιωμάτων πρόσβασης σε λογαριασμούς υπηρεσιών. Λειτουργούν μόνο οι θύρες (ports), τα πρωτόκολλα και οι δικτυακές υπηρεσίες που είναι απαραίτητες για τη διεκπεραίωση των επιχειρησιακών λειτουργιών. Οι χρήστες με standard δικαιώματα (non-privileged) δεν μπορούν να απενεργοποιήσουν ή να τροποποιήσουν τις ρυθμίσεις ασφάλειας στο λειτουργικό τους σύστημα. Οι σταθμοί εργασίας στα κτήρια των διοικητικών υπηρεσιών έχουν υποχρεωτικά εγκατεστημένο antivirus λογισμικό. Τηρείται κατάλογος με όλους τους servers, ώστε ανά πάσα στιγμή να είναι δυνατός ο έλεγχος της αξιολόγησης και βέλτιστης χρήσης των υποδομών.



Vitruvian Man Leonardo Da Vinci

Η ασφάλεια του πανεπιστημιακού δικτύου βασίζεται στη σωστή οργάνωση και καταγραφή του. Λεπτομερή δικτυακά διαγράμματα απεικονίζουν όλες τις δικτυακές συνδέσεις και τη θέση των δικτυακών συσκευών στο δίκτυο. Το εσωτερικό δίκτυο είναι οργανωμένο σε διακριτά υποδίκτυα με βάση λογική οργάνωση αλλά και το επίπεδο κρισιμότητας και ευαισθησίας των διάφορων τομέων. Η απομακρυσμένη πρόσβαση χρηστών στο εσωτερικό δίκτυο του Οργανισμού γίνεται μέσω VPN (Virtual Private Network). Το δίκτυο προστατεύεται από δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών για την ανίχνευση και πρόληψη επιθέσεων ενώ συστήματα παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών σας είναι σε συνεχή λειτουργία. Γίνεται χρήση πρωτοκόλλου SSL για ασφαλή σύνδεση μεταξύ συστημάτων. Τηρείται αναλυτικός κατάλογος με την κατάσταση όλων των δικτυακών συσκευών για τον έλεγχο και την οργάνωσή τους.

Οι κτηριακές εγκαταστάσεις που φιλοξενούν τους servers του Πανεπιστημίου Πατρών (computer room) διαθέτουν σύστημα συναγερμού, πλεονασμό (redundancy) σε συστήματα και κυκλώματα δικτύωσης, UPS και ηλεκτρογεννήτρια για την αδιάλειπτη παροχή ρεύματος και τη δυνατότητα ελεγχόμενου κλεισίματος μηχανημάτων και συσκευών, συστήματα πυρανίχνευσης και πυρόσβεσης καθώς και σύστημα ψύξης με αυτοματοποιημένους ελεγκτές θερμοκρασίας. Επιπλέον της βασικής υποδομής που βρίσκεται στο κτήριο της κεντρικής βιβλιοθήκης, λειτουργεί και εφεδρική υποδομή στο κτήριο διοίκησης συνδεδεμένη με την κεντρική μέσω αρχιτεκτονικής «Disaster control» επιτρέποντας στους servers που έχουν ενταχθεί στην υποδομή να εκκινήσουν άμεσα από την εφεδρική σε περίπτωση καταστροφικού συμβάντος στην κύρια.

Οι μηχανισμοί ελέγχου και καταγραφής πρόσβασης είναι κρίσιμης σημασίας για την κυβερνοασφάλεια καθώς εξασφαλίζουν λογοδοσία και δυνατότητα ανίχνευσης συμβάντων και διατρέχουν κάθετα τους άλλους τομείς της πολιτικής ασφάλειας. Ο έλεγχος πρόσβασης στα συστήματα και τους σταθμούς επιβάλλει πως το προσωπικό του οργανισμού και οι εξωτερικοί συνεργάτες που αποκτούν λογαριασμό αναγνωρίζονται με μοναδικό τρόπο που είναι το UPnet ID. Η πρόσβαση στα πληροφοριακά συστήματα σε εξουσιοδοτημένους χρήστες γίνεται με βάση τις αρχές των ελάχιστων προνομίων (least privilege). Χρησιμοποιείται Single sign On πιστοποίηση χρηστών με βάση το Shibboleth όπου ο χρήστης μπαίνει σε όλες τις υπηρεσίες με έναν μοναδικό κωδικό. Διατηρείται LDAP κατάλογος με όλους τους λογαριασμούς χρηστών, ο οποίος περιέχει τα απαραίτητα στοιχεία κάθε προσώπου, τα προνόμια πρόσβασης σε υπηρεσίας και τον χρόνου λήξης αυτών. Η εκχώρηση δικαιωμάτων πρόσβασης γίνεται με βάση διακριτούς ρόλους, έτσι ώστε οι χρήστες να έχουν πρόσβαση αποκλειστικά και μόνο στο είδος της πληροφορίας που είναι απαραίτητη για την εκτέλεση των εργασιακών καθηκόντων τους.

Σε κάθε server ή δικτυακό σύστημα τηρούνται αρχεία καταγραφής συμβάντων (event logs). Τα αρχεία καταγραφής συμβάντων περιλαμβάνουν λεπτομερή metadata όπως πηγή γεγονότος, ημερομηνία, χρήστης, χρονοσήμανση, IP διεύθυνση πηγής, IP διεύθυνση προορισμού. Τα αρχεία καταγραφής συμβάντων είναι προσβάσιμα μόνο από λογαριασμούς με αυξημένα δικαιώματα.

Ο Χ. Ι. Μπούρας είναι Πρύτανης του Πανεπιστημίου Πατρών και Καθηγητής στο Τμήμα μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής

Κυβερνοασφάλεια: Αναγκαιότητα και διαδικασίες

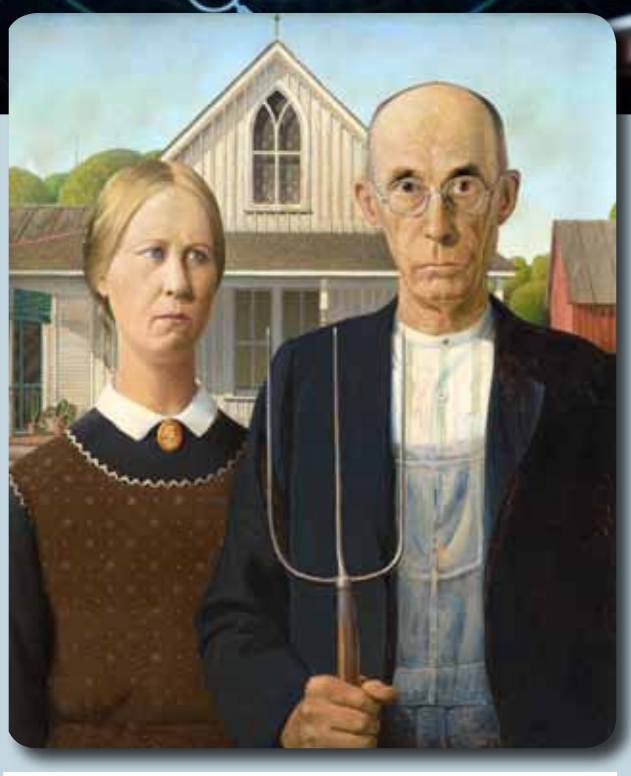
Γράφει ο ***Δημήτρης Σερπάνος***

Η ανάπτυξη του δημόσιου Διαδικτύου τη δεκαετία του 1990 ξεκίνησε μια επανάσταση που εξελίσσεται και θα συνεχίσει για μεγάλο χρονικό διάστημα, επηρεάζοντας σχεδόν όλες τις πλευρές της ζωής.

Η εύκολη και φθηνή πρόσβαση σε ψηφιακά συστήματα και υπηρεσίες, σε συνδυασμό με την πρόοδο της τεχνολογίας υπολογιστικών συστημάτων έχει οδηγήσει στη σημερινή πραγματικότητα της εύκολης πρόσβασης από κινητές συσκευές σε σύνθετες υπηρεσίες, όπως τραπεζικές, εκπαιδευτικές, υγείας και άλλες, στην αυτοματοποίηση σύνθετων διαδικασιών στη βιομηχανία, στη λειτουργία και διαχείριση των κρίσιμων υποδομών όπως τα ηλεκτρικά δίκτυα, τα υδρευτικά δίκτυα και τα δίκτυα μεταφορών, στην ανάπτυξη αποτελεσματικών αυτόνομων οχημάτων, στα κρυπτονομίσματα, στα κοινωνικά δίκτυα, κοκ. Το Διαδίκτυο έχει επηρεάσει σχεδόν όλες τις δραστηριότητες μας ατομικά και κοινωνικά.

Η επιταχυνόμενη ψηφιοποίηση διαδικασιών, η οποία γίνεται παγκοσμίως, προσφέρει σημαντικά πλεονεκτήματα στην καθημερινότητά μας και σημαντικές βελτιώσεις στις ατομικές και κοινωνικές δραστηριότητες. Όμως, τα πλεονεκτήματα της συνοδεύονται από φαινόμενα κακής χρήσης από κακόβουλους χρήστες που δημιουργούν κινδύνους για την ορθή, αποτελεσματική και ασφαλή χρήση ψηφιακών εφαρμογών και υπηρεσιών. Η κακόβουλη χρήση υπολογιστικών συστημάτων και δικτύων είναι ένα φαινόμενο δεκαετιών, το οποίο αυξάνεται ως συνάρτηση της αυξανόμενης ψηφιοποίησης και της ευρύτερης χρήσης ψηφιακών εφαρμογών και υπηρεσιών. Τα παραδείγματα είναι πολλά και καλύπτουν όλο το φάσμα ψηφιακών υπηρεσιών. Είναι γνωστή η περίπτωση απολυμένου υπαλλήλου δήμου που έκανε παρέμβαση στα αυτοματοποιημένα συστήματα του δήμου και γέμισε με λύματα λίμνη πάρκου ως εκδίκηση. Πριν λίγα χρόνια μεγάλη εταιρεία διαχείρισης αγωγών πετρελαίου έγινε όμηρος επιτιθέμενων προγραμματιστών που έθεσαν συστήματα της εκτός λειτουργίας ζητώντας λύτρα και δημιουργώντας μεγάλο πρόβλημα παροχής καυσίμων και ακολούθως στις μεταφορές στις ΗΠΑ για πολλές ώρες. Τον Δεκέμβριο του 2015, μέρη της Ουκρανίας έμειναν χωρίς ηλεκτρική ενέργεια για ώρες μετά από κυβερνοεπίθεση στα συστήματα διαχείρισης ηλεκτρικής ενέργειας παρόχων. Οι τράπεζες και οι οικονομικοί οργανισμοί, όπως τα χρηματιστήρια, είναι επίσης δημοφιλείς στόχοι αντίστοιχων κυβερνοεπιθέσεων. Περιπτώσεις οικονομικής απάτης με χρήση ψηφιακών συστημάτων και εφαρμογών παρουσιάζονται συχνά σε δημοσιεύματα.

Είναι σαφές ότι η κυβερνοασφάλεια είναι βασική απαίτηση στον αυξανόμενο ψηφιακό κόσμο. Το πρόβλημα της κυβερνοασφάλειας είναι ιδιαίτερα οξύ στις κρίσιμες υποδομές που είναι απαραίτητες για τη λειτουργία και την ευζωία των πολιτών. Δυσλειτουργίες στην οικονομική ζωή, στην παροχή και διαχείριση ενέργειας, υδάτων, μεταφορών, υπηρεσιών υγείας μπορούν να οδηγήσουν σε σημαντικές οικονομικές απώλειες πολιτών, οργανισμών και κρατών καθώς και σε σημαντικές ζημιές συμπεριλαμβανόμενης και της απώλειας ανθρώπινης ζωής. Παρά το γεγονός ότι επικρατεί η άποψη ότι η κυβερνοασφάλεια είναι θέμα τεχνολογίας, η κυβερνοασφάλεια είναι μια διαδικασία η οποία περιλαμβάνει, τουλάχιστον, πολιτικές, διαχείριση, τεχνολογία, εκπαίδευση και ενημέρωση. Βασικό στοιχείο αποτελεί η ανάλυση κινδύνων για τα συστήματα και τις εφαρμογές που πρέπει να προστατευθούν. Τα προηγούμενα παραδείγματα κυβερνοεπιθέσεων υποδεικνύουν ότι οι επιτιθέμενοι διαφοροποιούνται ανάλογα με τις ικανότητες και τα μέσα που διαθέτουν, καλύπτοντας μεγάλο φάσμα. Επιθέσεις γίνονται σε ορισμένες περιπτώσεις από άτομα που έχουν βασικές γνώσεις τεχνολογίας και πρόσβαση στα συστήματα και τις εφαρμογές. Σε άλλες περιπτώσεις, εγκληματικές ομάδες με καλά εκπαιδευμένα στελέχη και σημαντικούς οικονομικούς και τεχνολογικούς πόρους επιτυγχάνουν παραβίαση συστημάτων με εξωτερικές επιθέσεις. Σε περιπτώσεις όπως αυτές των προβλημάτων του ηλεκτρικού δικτύου της Ουκρανίας, υπάρχουν βάσιμες υποψίες ότι ο επιτιθέμενος ήταν άλλο κράτος. Είναι ευνόητο ότι η σχεδίαση οποιασδήποτε κυβερνοάμυνας πρέπει να βασίζεται σε ανάλυση κινδύνου λαμβάνοντας υπόψη τα χαρακτηριστικά του δυνητικού επιτιθέμενου, συμπεριλαμβανομένων των πόρων που μπορεί να διαθέτει.



American Gothic Grant Wood

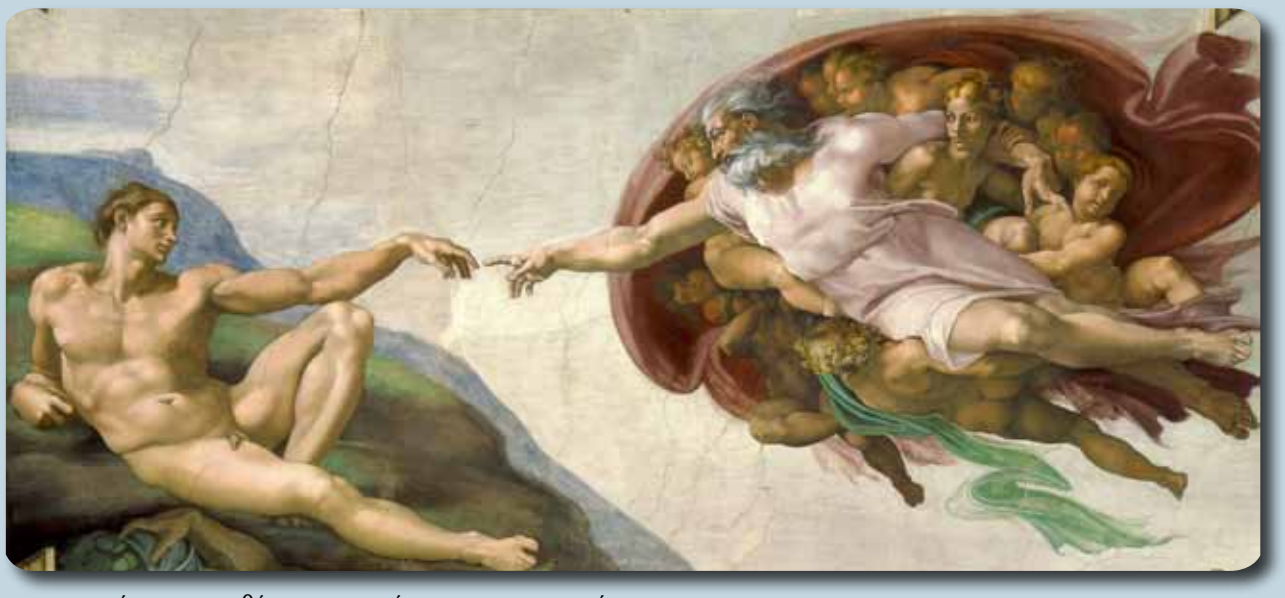
Η ανάλυση κινδύνων οδηγεί σε καταγραφή των κινδύνων, και οδηγεί στην απαρίθμηση δυνητικών απειλών και επιθέσεων από τις οποίες πρέπει να προστατεύεται το σχετικό σύστημα ή υπηρεσία. Η τεχνολογία παρέχει ισχυρούς μηχανισμούς για άμυνα και προστασία, όπως μηχανισμούς για αναγνώριση ατόμων και συστημάτων, για προστασία από διαρροή στην επικοινωνία, για έλεγχο δικαιωμάτων πρόσβασης κοκ. Όμως, ο συνδυασμός μηχανισμών για την επίτευξη του επιθυμητού αποτελέσματος δεν προστατεύεται πάντα από τεχνολογικές λύσεις καθώς πολλές αποφάσεις σε μια συνολική λύση περιλαμβάνουν αποφάσεις ατόμων και χειρισμό μηχανισμών και δεδομένων από άτομα. Η εμπειρία έχει δείξει ότι ο ανθρώπινος παράγοντας είναι το πιο ευάλωτο στοιχείο μιας λύσης κυβερνοασφάλειας. Πως μπορεί να προστατευθεί ένας υπολογιστής, για παράδειγμα, αν ο διαχειριστής του δεν προστατεύσει τους κωδικούς του και διαρρεύσουν σε κακόβουλους χρήστες; Είναι απαραίτητη, προφανώς, η δημιουργία πολιτικής και μηχανισμών διαχείρισης των κωδικών υπολογιστικών συστημάτων σε έναν οργανισμό. Επιπλέον, για την ορθή εφαρμογή των πολιτικών, την κατανόηση των κινδύνων, των απειλών και δυνητικών επιθέσεων χρειάζεται εκπαίδευση του προσωπικού και των χρηστών των συστημάτων και των εφαρμογών.

Η συνεχής πρόοδος και εξέλιξη υπολογιστικών συστημάτων και ψηφιακών υπηρεσιών σε συνδυασμό με την αυξανόμενη ψηφιοποίηση απαιτούν τη συνεχή αναμόρφωση αναλύσεων κινδύνων, απειλών και επιθέσεων καθώς και τη συνεχή προσαρμογή μηχανισμών, διαχείρισης και πολιτικών. Το εξελισσόμενο ψηφιακό περιβάλλον απαιτεί συνεχή προσαρμογή σε όλα τα επίπεδα της διαδικασίας της κυβερνοασφάλειας. Όπως αναδεικνύουν το τελευταίο διάστημα και παγκόσμιοι πηγέτες, η κυβερνοασφάλεια αποτελεί βασικό στοιχείο της εθνικής ασφάλειας πλέον.

Ο κ. Δημήτρης Σερπάνος είναι Πρόεδρος στο ΙΤΥΕ «ΔΙΟΦΑΝΤΟΣ», καθηγητής στο Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, της Πολυτεχνικής Σχολής του Πανεπιστημίου Πατρών στο Τομέα Ηλεκτρονικής και Υπολογιστών (Dipl.-El.-Eng. (Comp. Eng.) M.Sc. Ph.D. (Univ. Princeton)

Η νομική αντιμετώπιση των προκλήσεων της Κυβερνοασφάλειας

Γράφει ο ***Αθανάσιος Ζούπας***



Creation of Adam Michelangelo

Η ευρύτατη χρήση του διαδικτύου και η καθημερινή χρήση του για την επικοινωνία, τις οικονομικές συναλλαγές, την αποθήκευση δεδομένων, την ανάπτυξη επιχειρήσεων, την εκτέλεση συναλλαγών, την διαφήμιση και σε τόσες άλλες κρίσιμες λειτουργίες, καθιστά επιτακτική και αναγκαία την προστασία όλων των χρηστών προκειμένου να μην πέσουν θύματα ηλεκτρονικών εγκλημάτων.

Η ασφάλεια στον κυβερνοχώρο αποβλέπει στην προστασία των συστημάτων, των δικτύων, των εφαρμογών, των υπολογιστών και γενικά των συσκευών από ψηφιακές απειλές και κατ΄επέκταση και στην ασφάλεια του χρήστη.

Όλοι όσοι χρησιμοποιούμε κάποια συσκευή και συνδεόμαστε με το διαδίκτυο είναι σίγουρο ότι έχουμε δεχθεί, δεχόμαστε και θα δεχόμαστε ψηφιακές απειλές.

Οι δράστες από τον υπολογιστή τους και μέσω του διαδικτύου επιτίθενται σε ένα άλλο υπολογιστή, ο οποίος είτε αποτελεί το στόχο τους είτε αποτελεί το μέσο για φτάσουν στο στόχο τους. Ο λόγος είναι απλός με την διασύνδεση των διάφορων ψηφιακών συστημάτων, «χακάροντας» το ένα σύστημα, μπορεί να βρεθείς και στα υπόλοιπα διασυνδεδεμένα ψηφιακά συστήματα. ΄Αρα πρέπει να ασφαλιστούν όλες τις πιθανές είσοδοι κάθε εγκληματία. Κατά την περίοδο της πανδημίας καθιερώθηκε η τηλεργασία και αυξήθηκε ο αριθμός των χρηστών και κατ΄ επέκταση ο αριθμός των δυνητικών σημείων πρόσβασης για τους επιτιθέμενους, αφού η χρήση του διαδικτύου επεκτάθηκε σε νοικοκυριά και κινητές συσκευές που συνδέονται με το διαδίκτυο, με αποτέλεσμα να υπάρχουν νέα και πολλά τρωτά σημεία προς εκμετάλλευση.

Η Κυβερνοασφάλεια περιλαμβάνει την πρόληψη και την ανίχνευση επιθέσεων, την προστασία από την απώλεια δεδομένων και την αποκατάσταση από επιθέσεις. Οι επιθέσεις μπορεί να περιλαμβάνουν κακόβουλο λογισμικό (malware), επιθέσεις τύπου phishing, επιθέσεις άρνησης υπηρεσίας (DDoS), και πολλές άλλες μορφές απειλών που αποσκοπούν στην απόκτηση μη εξουσιοδοτημένης πρόσβασης ή στην καταστροφή κρίσιμων πληροφοριών.

Οι πιο γνωστοί τρόποι επίθεσης είναι οι ιοί (viruses) ένα κακόβουλο λογισμικό που συνήθως προσκολλάται σε άλλο λογισμικό και μπορεί να του προκαλέσει βλάβη, οι Σκώληκες (worms) που είναι αυτοαναπαραγόμενα κακόβουλα προγράμματα που εξαπλώνονται μέσω των δικτύων με σκοπό να δημιουργήσουν κενά ασφαλείας οι Δούρειοι Ίπποι (Trojans) που είναι κακόβουλα προγράμματα που εμφανίζονται ως χρήσιμα και όταν εγκατασταθούν αποκτούν πρόσβαση στα δεδομένα του χρήστη. Άλλοι τρόποι είναι το Email Phishing οι επιτιθέμενοι δηλαδή στέλνουν email που φαίνονται νόμιμα για να πείσουν τους χρήστες να αποκαλύψουν προσωπικά δεδομένα ή να κατεβάσουν κακόβουλο λογισμικό, το Voice Phishing Οι επιτιθέμενοι χρησιμοποιούν τηλέφωνα για να προσποιηθούν ότι είναι νόμιμοι οργανισμοί και να πείσουν τα θύματα να αποκαλύψουν ευαίσθητες πληροφορίες, το SMS Phishing οι επιτιθέμενοι στέλνουν SMS με κακόβουλους συνδέσμους ή ζητούν πληροφορίες από τα θύματα κλπ.

Το έγκλημα στον κυβερνοχώρο είναι μια εξελισσόμενη μορφή εγκλήματος, πέρα από κράτη και σύνορα. Οι δράστες του εγκλήματος στον κυβερνοχώρο (κυβερνοεγκληματίες) και τα θύματά τους μπορεί να βρίσκονται σε διαφορετικές περιοχές του πλανήτη γεγονός που καταδεικνύει την ανάγκη για μια διεθνή αντίδραση.

Η νομική αντιμετώπιση της κυβερνοασφάλειας βρίσκει πολλές προκλήσεις, οι οποίες σχετίζονται με την ταχύτητα των τεχνολογικών εξελίξεων, την παγκόσμια φύση των κυβερνοεπιθέσεων και την ανάγκη για διεθνή συνεργασία.

Το πρώτο νομικό κείμενο σε διεθνές επίπεδο που ρυθμίζει τα θέματα αντιμετώπισης του κυβερνοεγκλήματος είναι η Σύμβαση της Βουδαπέστης (Cybercrime Convention) του Συμβουλίου της Ευρώπης, η οποία υπογράφηκε το 2001. Η Σύμβαση της Βουδαπέστης κυρώθηκε με το Νόμο 4411/2016 ο οποίος αποτελεί τον πρώτο Νόμο για την αντιμετώπιση του Κυβερνοεγκλήματος στην Ελλάδα.

Αποτελεί την πρώτη διεθνή συνθήκη για τα εγκλήματα που διαπράττονται μέσω του Διαδικτύου και άλλων δικτύων υπολογιστών και αφορά ιδίως, τις παραβιάσεις των δικαιωμάτων πνευματικής ιδιοκτησίας, την απάτη που σχετίζεται με τους υπολογιστές, την σεξουαλική εκμετάλλευση ανηλίκων και τις παραβιάσεις της ασφάλειας των δικτύων.

Στην Ευρωπαική Ένωση η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών 2016 καθώς και η Οδηγία (ΕΕ) 2016/1148 Network Infrastructure Security για την ασφάλεια των συστημάτων δικτύων και πληροφοριών (γνωστή και ως οδηγία NIS), έθεσαν, σε επίπεδο ΕΕ, τις αρχές για την διασφάλιση ενός κοινού επιπέδου ασφάλειας στον κυβερνοχώρο σε όλους τους κρίσιμους τομείς, όπως η ενέργεια, οι μεταφορές, η χρηματοδότηση και η υγειονομική περίθαλψη. Στην Ελλάδα η Οδηγία NIS ενσωματώθηκε με το Νόμο 4577/2018. Ήδη έχει εκδοθεί μία βελτιωμένη οδηγία η ΝΙΣ 2, η οποία βασίζεται στην οδηγία NIS 1 αλλά επεκτείνει το πεδίο εφαρμογής της.

Όπως είναι λογικό με την εξάπλωση της ψηφιοποίησης στην καθημερινή ζωή των πολιτών και των επιχειρήσεων η σημασία της κυβερνοασφάλειας αποτελεί άμεση προτεραιότητα και είναι αναγκαία για την ασφάλεια και την ευημερία της κοινωνίας. Ακόμα περισσότερο όταν ο πολίτης - χρήστης υποχρεώνεται από την πολιτεία να εκτελεί ηλεκτρονικά όλο και περισσότερες συναλλαγές του.

Ο Αθανάσιος Ζούπας είναι Πρόεδρος του Δικηγορικού Συλλόγου Πατρών

Κυβερνοασφάλεια: Η Σημασία και οι Προκλήσεις της Ψηφιακής Εποχής

Γράφει ο ***Στέφανος Μίχος***

Στην εποχή της ψηφιακής επανάστασης, η κυβερνοασφάλεια έχει αναδειχθεί σε έναν από τους πιο κρίσιμους τομείς για την προστασία των πληροφοριών και των υποδομών μας.
Καθώς οι τεχνολογίες εξελίσσονται και οι διαδικτυακές απειλές γίνονται ολοένα και πιο περίπλοκες, η ανάγκη για αποτελεσματικά μέτρα κυβερνοασφάλειας είναι πιο επιτακτική από ποτέ.

Τι είναι η Κυβερνοασφάλεια;

Η κυβερνοασφάλεια αφορά στις πρακτικές και τις τεχνολογίες που αναφέρονται για την προστασία συστημάτων υπολογιστών, δικτύων και δεδομένων από κακόβουλες επιθέσεις, ζημιές ή μη εξουσιοδοτημένη πρόσβαση. Περιλαμβάνει μια σειρά από στρατηγικές, όπως η κρυπτογράφηση, η ανίχνευση εισβολών, η εκπαίδευση χρηστών και η ανάπτυξη πολιτικών ασφαλείας.

Οι Κύριες Απειλές

Οι απειλές στον τομέα της κυβερνοασφάλειας είναι ποικίλες και συνεχώς εξελισσόμενες. Ορισμένες από τις πιο συχνές περιλαμβάνουν:

1. Malware: Κακόβουλο λογισμικό που μπορεί να μολύνει υπολογιστές και δίκτυα, προκαλώντας ζημιές ή κλοπή δεδομένων.

2. Phishing: Τεχνικές εξαπάτησης που δηλώνουν για να αποκτήσουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.

3. Ransomware: Ένα είδος κακόβουλου λογισμικού που κλειδώνει τα δεδομένα του χρήστη και χρειάζεται λύτρα για την αποκατάστασή τους.

4. Επιθέσεις DDoS: Επιθέσεις που στοχεύουν στην υπερφόρτωση ενός δικτύου ή μιας υπηρεσίας, καθιστώντας τη μη διαθέσιμη στους χρήστες.

5. Παραβιάσεις προσωπικών δεδομένων: Επιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων.

Παράγοντες Απειλών

(α) Κυβερνοεγκληματίες

Οι κυβερνοεγκληματίες είναι ομάδες ή φυσικά πρόσωπα που

χρησιμοποιούν τις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) για την τέλεση κακόβουλων ενεργειών. Συχνά εμπλέκονται σε παράνομες δοσοληψίες στο επονομαζόμενο Dark Web, όπου προβαίνουν σε αγοροπωλησία κακόβουλων εφαρμογών ή πληροφοριών για πιθανούς στόχους.

(β) Τρίτα κράτη

Περιλαμβάνει ομάδες οι οποίες είτε ανήκουν είτε χρηματοδοτούνται από κράτη και αποσκοπούν, κατά βάση, στο να εξαπολύσουν επιθέσεις που θα επιφέρουν μεγάλο αντίκτυπο στην παροχή βασικών / ουσιωδών υπηρεσιών από Φορείς.

(γ) Ακτιβιστές

Στόχος των ακτιβιστών είναι η προώθηση κάποιας κοινωνικής αλλαγής ή πολιτικής ατζέντας ή αντεπίθεσης για την τόνωση του εθνικού φρονήματος, η οποία συχνά συνοδεύεται από προειδοποίηση για παύση της «γενεσιουργού αιτίας» υπό την απειλή της παράτασης ή/και επανάληψης ή/και κλιμάκωσης της επίθεσης.

(δ) Εσωτερικές απειλές

Αφορά σε υπαλλήλους οργανισμών που προβαίνουν, είτε εκούσια είτε ακούσια, σε κακόβουλες ενέργειες. Λόγω της φύσης και του επιπέδου πρόσβασης σε συστήματα και πληροφορίες ενός Φορέα, καθώς και της προσέγγισης περιμετρικής ασφάλειας που υιοθετούν αρκετοί Φορείς, οι εσωτερικές απειλές αποτελούν τον μεγαλύτερο παράγοντα απειλών και έναν από τους πιο δύσκολους στην αναγνώριση και αντιμετώπισή τους.

The School of Athens Raphael

Η Σημασία της Κυβερνοασφάλειας

Η κυβερνοασφάλεια είναι ζωτικής σημασίας για πολλές πτυχές της σύγχρονης ζωής. Από τις Επιχειρήσεις μέχρι τις Κυβερνητικές Υπηρεσίες και τους απλούς Πολίτες, η προστασία των δεδομένων και των υποδομών είναι κρίσιμη για την ασφάλεια και την εμπιστοσύνη. Ορισμένοι από τους λόγους που καθιστούν την κυβερνοασφάλεια τόσο σημαντική περιλαμβάνουν:

- **Προστασία Δεδομένων**: Η διαρροή προσωπικών ή ευαίσθητων πληροφοριών μπορεί να έχει σοβαρές συνέπειες, όπως οικονομικές αποδόσεις και ζημιά στη φήμη.
- **Διασφάλιση Επιχειρηματικής Συνεχούς Λειτουργίας**: Οι επιθέσεις μπορούν να διακόψουν τη λειτουργία μιας επιχείρησης, προκαλώντας σημαντικά οικονομικά πλήγματα.
- **Εμπιστοσύνη Πελατών**: Οι πελάτες είναι πιο πιθανό να συνεργαστούν με επιχειρήσεις που αποδεικνύουν ότι λαμβάνουν σοβαρά υπόψη την ασφάλεια των δεδομένων τους.

Προκλήσεις στην Κυβερνοασφάλεια

Παρά την αυξανόμενη συνειδητοποίηση της σημασίας της κυβερνοασφάλειας, υπάρχουν πολλές προκλήσεις που πρέπει να αντιμετωπιστούν:

1. Εξέλιξη των Απειλών: Οι κυβερνοεγκληματίες γίνονται ολοένα και πιο ευφυείς, χρησιμοποιώντας προηγμένες τεχνικές για να παρακάμψουν τα μέτρα ασφαλείας.

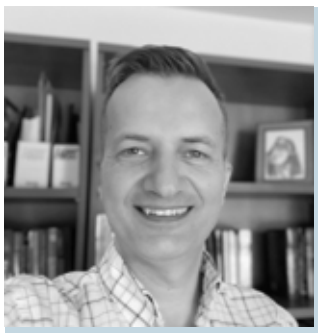
2. Έλλειψη Εξειδικευμένου Προσωπικού: Υπάρχει έλλειψη επαγρύπνησης στον τομέα της κυβερνοασφάλειας, γεγονός που καθιστά δύσκολη την αποτελεσματική προστασία των συστημάτων.

3. Ασφάλεια στο Cloud: Καθώς περισσότερες επιχειρήσεις μεταφέρουν τα δεδομένα τους στο cloud, η ασφάλεια αυτών των υπηρεσιών γίνεται ολοένα και πιο κρίσιμη.

Συμπεράσματα

Καθώς οι ΤΠΕ δημιουργούν έναν κόσμο διαρκώς αυξανόμενης πολυπλοκότητας σε διασυνδεδεμένα συστήματα και συσκευές, η δημόσια συζήτηση για τα θέματα κυβερνοασφάλειας και ιδιωτικότητας βρίσκεται συνεχώς στο προσκήνιο, αναδεικνύοντας την ανάγκη για ενίσχυση της προστασίας και ανθεκτικότητας των εν λόγω συστημάτων από τις συνεχώς εξελισσόμενες απειλές του σύγχρονου κυβερνοχώρου. Η κυβερνοασφάλεια είναι ένα αναπόσπαστο κομμάτι της ψηφιακής εποχής. Η προστασία των πληροφοριών και των υποδομών μας απαιτεί συνεχή προσπάθεια και προσαρμογή στις νέες απειλές. Είναι σημαντικό για τις επιχειρήσεις και τους χρήστες να επενδύσουν σε μέτρα ασφαλείας και να παραμείνουν ενημερωμένοι σχετικά με τις εκδόσεις στον τομέα της κυβερνοασφάλειας. Μόνο έτσι μπορούμε να διασφαλίσουμε ένα ασφαλές ψηφιακό μέλλον.

Ο Δρ. Στέφανος Μίχος είναι Ηλεκτρολόγος Μηχανικός & Μηχανικός Πληροφορικής, Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών (Υ.Α.Σ.Π.Ε.) ΑΠΟΚΕΝΤΡΩΜΕΝΗ ΔΙΟΙΚΗΣΗ ΠΕΛΟΠΟΝΝΗΣΟΥ, ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ & ΙΟΝΙΟΥ



Κυβερνοασφάλεια: Μια εποχή κρίσιμων ζητημάτων, ανάπτυξης και προκλήσεων

Γράφει ο ***Νικόλαος Σκλάβος***

Κυβερνοασφάλεια: στη σημερινή εποχή, αναμφισβήτητα αποτελεί περισσότερο από μια ραγδαία αναπτυσσόμενη επιστήμη και τεχνολογία αιχμής. Έχει προσελκύσει το ιδιαίτερο ενδιαφέρον, τόσο της ερευνητικής και ακαδημαϊκής κοινότητας, όσο και των αντίστοιχων τομέων της βιομηχανίας, σε πλήθος εκφάνσεων της καθημερινής ζωής.

Ιδιαίτερα, τα τελευταία χρόνια συνετέλεσαν σε έναν ταχύτατο ρυθμό ανάπτυξης και εξέλιξης της, κυρίως λόγω των ηλεκτρονικών υπηρεσιών, των τραπεζικών συναλλαγών, των διαδικτυακών αγορών, του ηλεκτρονικού πολέμου, αλλά και άλλων μορφών ανταλλαγής πληροφορίας και επικοινωνίας.

Παράλληλα βέβαια, καθημερινά καταγράφεται επίσημα (και σε πολλές περιπτώσεις «ανεπίσημα»), ένας ιδιαίτερα μεγάλος αριθμός, ευπαθειών, απειλών και επιθέσεων, από κυβερνοεγκληματίες και κάθε μορφής επιτιθέμενους.

Ωστόσο, αυτές οι μορφές επιθέσεων και κυβερνοαπειλών, δεν αποτελούν το μοναδικό κρίσιμο ζήτημα, που έχουν να αντιμετωπίσουν οι οργανισμοί και οι ομάδες που υποστηρίζουν την κυβερνοασφάλεια, στο άμεσο μέλλον. Οι νέες εξελισσόμενες τεχνολογίες, που υιοθετούνται στην επιστήμη των υπολογιστών και των τηλεπικοινωνιών, φέρνουν μαζί τους νέα κρίσιμα τρωτά σημεία και της δική τους «αχίλλειο πτέρνα», κάθε φορά.

Τεχνητή νοημοσύνη (AI): ακόμα και στο ψάρεμα (phishing).

Η εξαιρετικά μεγάλη ανάπτυξη της τεχνητής νοημοσύνης (AI) και η ευρεία υποστήριξη και χρήση αντίστοιχων εργαλείων και πλατφορμών, όπως το πολύ γνωστό σε όλους ChatGPT, έχουν ως επακόλουθο μια ιδιαίτερα αξιοσημείωτη νέα προσέγγιση από απειλές και επιθέσεις, ειδικότερα στις κατευθύνσεις του ηλεκτρονικού ψαρέματος (phishing).

Αυτού του τύπου πλατφόρμες (GenAI), αποτελούν ένα πολύ χρήσιμο και εύχρηστο εργαλείο, στα χέρια των επιτιθέμενων, για να δημιουργήσουν πιο πειστικές απάτες κοινωνικής μηχανικής και ψαρέματος, με ηλεκτρονικά μέσα. Ταυτόχρονα, οι εισβολείς έχουν τη δυνατότητα να συλλέξουν ευαίσθητες πληροφορίες και κρίσιμα δεδομένα, από φορείς, εταιρίες, οργανισμούς και άτομα, μέσα από ιστοτόπους, μέσα κοινωνικής δικτύωσης, εφαρμογές, κτλπ.

Επίσης, το τελευταίο διάστημα, εμφανίζεται πολύ συχνά και η προσέγγιση των deepfake επιθέσεων. Πρόκειται για τη δημιουργία ψεύτικου, αλλά πολύ πειστικού, περιεχομένου με ήχο, εικόνα και βίντεο, βασισμένο σε τεχνικές AI. Τέτοιας μορφής υλικό, μπορεί εύκολα να ξεγελάσει και να οδηγήσει σε παραπληροφόρηση, εκβιασμό, παρέμβαση σε ηλεκτρονικές υπηρεσίες και πολλά περισσότερα.

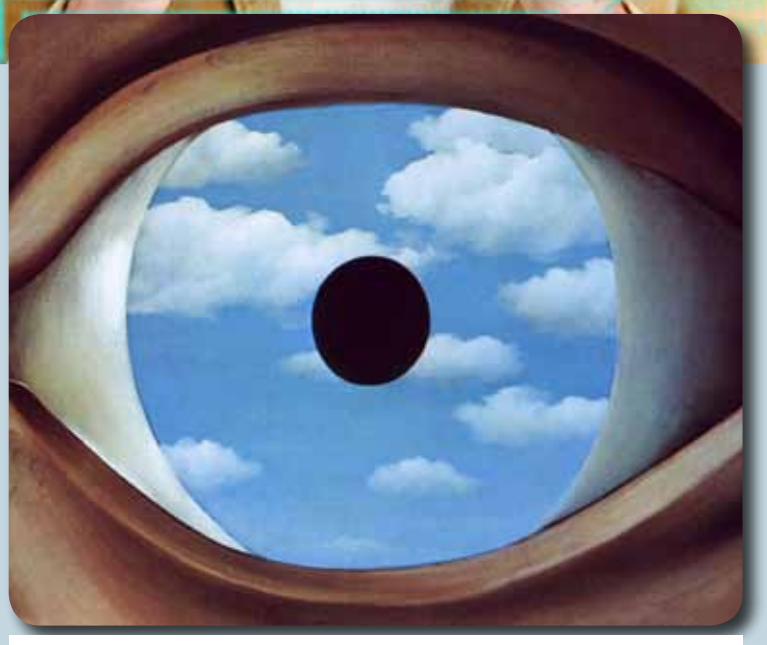
Μολυσματικό λογισμικό: το Ransomware ήρθε για να μείνει

Οι επίσημες καταγραφές σε παγκόσμιο επίπεδο έχουν αναδείξει ότι από το 2020, χρονιά ορόσημο για την εμφάνιση επιθέσεων, μολυσματικού λογισμού τύπου Ransomware, οι παραβιάσεις έχουν βασιστεί σε ποσοστό μεγαλύτερο του 25%, σε τέτοιας μορφής λογισμικό. Ιδιαίτερα κατά το προηγούμενο έτος, επισήμως έχουν καταγραφεί επιθέσεις, σε ποσοστό μεγαλύτερο του 65% στους φορείς και στους οργανισμούς, με τη χρήση αντίστοιχης μορφής λογισμικού.

Κόστος: οικονομικός προϋπολογισμός.

Σε μια δύσκολη οικονομική συγκυρία για όλο τον πλανήτη, οι εκτιμήσεις της οικονομικής ύφεσης, των επιτοκίων, των ακαθάριστων εγχώριων προϊόντων, αλλά και της γεωπολιτικής αβεβαιότητας, οδηγούν τους οργανισμούς και τους φορείς να προσανατολίζονται σε προσεκτικούς προϋπολογισμούς, με περαιτέρω μειώσεις σε κόστη κάθε μορφής.

Αν και θα περίμενε κανείς ότι οι υπηρεσίες και οι μηχανισμοί κυβερνοασφάλειας, δεν θα έπρεπε να συμπεριλαμβάνονται στις μειώσεις προϋπολογισμού, αλλά αντίθετα να ενισχύονται οικονομικά, πολλές φορές επηρεάζονται αισθητά, από τις μειώσεις προϋπολογισμού και τις περικοπές δαπανών.



The False Mirror Rene Magritte

Αγορά εργασίας: στελέχωση και δεξιότητες.

Ο συγκεκριμένος χώρος παρουσιάζει αυξανόμενες απαιτήσεις για περισσότερους μηχανικούς και γενικότερα απασχολούμενους, με ειδίκευση στον τομέα της κυβερνοασφάλειας, ενώ η εν λόγω αγορά εργασίας καταγράφει ολοένα και μεγαλύτερες ανάγκες σε ανθρώπινο δυναμικό. Σε πολλές περιπτώσεις, αναδεικνύονται λιγότερα ή οριακά επαρκή μέλη στις αντίστοιχες ομάδες, που πρέπει να επωμιστούν ολοένα και μεγαλύτερο φόρτο εργασίας.

Σημαντική αναφορά, θα πρέπει να γίνει και για τις συνεχόμενα εξελισσόμενες δεξιότητες του προσωπικού, που αναζητά η αγορά εργασίας, αλλά και του ήδη υπάρχοντος. Αρκετές είναι οι φορές που η τεχνολογική εξέλιξη της κυβερνοασφάλειας προηγείται με ταχύτερο ρυθμό, της κατάρτισης και των αντίστοιχων δεξιοτήτων του προσωπικού, που συνήθως ακολουθεί τις εξελίξεις.

Προσωπικές ελευθερίες – ιδιωτικότητα

Πολλές φορές οι έννοιες της προστασίας και της ασφάλειας, τείνουν να αποτελέσουν σημείο μη ισορροπημένης προσέγγισης των προσωπικών ελευθεριών και της ιδιωτικότητας του ανθρώπου. Πολλές υπηρεσίες και προϊόντα κυβερνοασφάλειας «θυσιάζουν» την ελευθερία του ατόμου, αλλά και κρίσιμα χαρακτηριστικά της προσωπικής του ζωής, σε μια προσπάθεια αντιμετώπισης των ανοικτών ζητημάτων του χώρου.

Ωστόσο, ο βαθμός ελευθερίας κάθε φορά, αποτιμάται αποκλειστικά και μόνο, μέσα από το σεβασμό που επιδεικνύεται προς τα δικαιώματα των πολιτών [Πηγή: Edward Snowden, «Το Μεγάλο Φακέλωμα», Εκδόσεις Ψυχογιός, 2019].

Ο Νικόλαος Γ. Σκλάβος είναι Καθηγητής στο Τμήμα Μηχανικών Η/Υ και Πληροφορικής της Πολυτεχνικής Σχολής του Πανεπιστημίου Πατρών

Κυβερνοασφάλεια στην Τοπική Αυτοδιοίκηση

Γράφει ο ***Πέτρος Γανός***

Η κυβερνοασφάλεια είναι η πρακτική και τα μέσα που χρησιμοποιούνται από τους φορείς για την προστασία συστημάτων πληροφοριών (υπολογιστών, δικτύων, δεδομένων) και χρηστών από μη εξουσιοδοτημένη πρόσβαση, που έχει σκοπό τις κακόβουλες επιθέσεις και την πρόκληση ζημιών.

Το θέμα της κυβερνοασφάλειας βρίσκεται στην πρώτη γραμμή ενδιαφέροντος τα τελευταία χρόνια, τόσο σε ευρωπαϊκό και εθνικό επίπεδο όσο και σε επίπεδο οργανισμών και φορέων. Το NIS 2 (Network and Information Security Directive 2) είναι η δεύτερη έκδοση της οδηγίας για την Ασφάλεια Δικτύων και Πληροφοριών της Ευρωπαϊκής Ένωσης, ισχύει από 16 Ιανουαρίου 2023 και τα κράτη μέλη πρέπει να την εφαρμόσουν έως την 17 Οκτωβρίου 2024. Στην Ελλάδα, η Γενική Διεύθυνση Κυβερνοασφάλειας που υπάγεται στη Γενική Γραμματεία Τηλεπικοινωνιών & Ταχυδρομείων του Υπουργείου Ψηφιακής Διακυβέρνησης έχει καταρτίσει την Εθνική Στρατηγική Κυβερνοασφάλειας (https://mindigital.gr/dioikisi/kyvernoasfaleia), στην οποία καθορίζονται οι στρατηγικοί στόχοι, οι προτεραιότητες και τα μέτρα πολιτικής και κανονιστικής ρύθμισης, με σκοπό την εξασφάλιση υψηλού επιπέδου ασφάλειας για τα συστήματα τηλεπικοινωνιών και πληροφορικής σε εθνικό επίπεδο.

Στην φετινή ΔΕΘ 2024, ιδιαίτερη αναφορά έκαναν οι υπουργοί Εσωτερικών και Ψηφιακής Διακυβέρνησης στο έργο για την προμήθεια εξοπλισμού και υπηρεσιών κυβερνοασφάλειας καθώς και στην υποστήριξη των ΟΤΑ από την Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΠ). Επίσης, η προστασία από κυβερνο-επιθέσεις και η διασφάλιση της επιχειρησιακής συνέχειας των ΟΤΑ αποτελεί ένα από τους επτά (7) βασικούς άξονες της Πρόσκλησης «Ψηφιακός Μετασχηματισμός των ΟΤΑ» που εκδόθηκε το 2023 από το Υπουργείο Ψηφιακής Διακυβέρνησης. Σύμφωνα με το Κοινό Δελτίο Τύπου των Υπουργείων Εσωτερικών και Ψηφιακής Διακυβέρνησης της 25/7/2024, από το σύνολο των προτάσεων που υπέβαλαν οι 312 Δήμοι, η πιο δημοφιλέστερη είναι η Δράση 34 «Ολοκληρωμένη υποδομή προστασίας από κυβερνοεπιθέσεις (Network Firewall, Endpoint security κλπ.) και η παροχή συστήματος τηλε-εργασίας» που επιλέχθηκε από 165 Δήμους. Καθίσταται πλέον σαφές ότι η προστασία των πληροφοριακών συστημάτων και των χρηστών των ΟΤΑ από κυβερνοεπιθέσεις θεωρείται επιτακτική ανάγκη και πρέπει να έχει μέγιστη προτεραιότητα στον στρατηγικό σχεδιασμό των ΟΤΑ.

Σκοπός της υποδομής προστασίας είναι η έγκυρη και έγκαιρη διάγνωση ανωμαλιών, η ανίχνευση κυβερνοαπειλών και επιθέσεων και η προστασία των συστημάτων του Δήμου από αυτές. Η προστασία θα πρέπει να αφορά το σύνολο ψηφιακής δραστηριότητας ήτοι: (α) το δίκτυο του φορέα (β) τους διακομιστές του φορέα (γ) τις εφαρμογές του φορέα και ιδιαίτερα τις διαδικτυακές εφαρμογές αυτού με δημόσια πρόσβαση και (δ) τις τελικές συσκευές (endpoints) των χρηστών. Η υποδομή προστασίας μπορεί να υλοποιηθεί με την ανάπτυξη ενός Πληροφοριακού Συστήματος Εντοπισμού και Διαχείρισης Συμβάντων Ασφάλειας, το οποίο εμπεριέχει τη διάθεση υλικοτεχνικής υποδομής, την ανάπτυξη εργαλείων και τεχνολογιών πληροφορικής και λογισμικού και την αξιοποίηση τηλεπικοινωνιακών συστημάτων για την ασφαλή επικοινωνία και μετάδοση δεδομένων και την προστασία από κυβερνοεπιθέσεις.

Der Schrei der Natur (Η κραυγή) Edvard Munch

Οι βασικές λειτουργίες του Συστήματος αφορούν στην παρακολούθηση και συλλογή δεδομένων και στη διαχείριση συμβάντων σχετικών με την κυβερνοασφάλεια. Πιο συγκεκριμένα, το Σύστημα θα πρέπει να είναι υπεύθυνο για την παρακολούθηση των κατάλληλων ψηφιακών στοιχείων (digital assets) που παράγουν τα αρχεία καταγραφής της τρέχουσας κατάστασης της υποδομής πληροφορικής του Δήμου, σχετικά με πιθανά συμβάντα ασφάλειας. Το Σύστημα θα πρέπει να υποστηρίζει πολλαπλές πηγές δεδομένων μεγάλου όγκου και να παρέχει τη δυνατότητα επεξεργασίας και ομογενοποίησης των δεδομένων για την ασφαλή αποθήκευση της πληροφορίας. Τα δεδομένα που θα συλλέγονται περιλαμβάνουν πλήθος πληροφοριών, όπως αρχεία καταγραφής του συνόλου των Υποσυστημάτων και Εφαρμογών του Δήμου (log files) και συσχετιζόμενων πληροφοριακών συστημάτων, τα γεγονότα που αντιμετώπισε ο χρήστης, τις κινήσεις που έκανε, την "ψηφιακή" κατάσταση της υποδομής κατά τη στιγμή μίας επίθεσης, κ.α. Το Σύστημα θα πρέπει να παρέχει τη δυνατότητα αποθήκευσης της συλλεγόμενης πληροφορίας σε βάση δεδομένων, ακολουθώντας μια προσέγγιση που θα εγγυάται την ασφάλεια, ακεραιότητα, αποδοτική ανάκτηση και γρήγορη αναζήτησή τους ανά πάσα στιγμή. Επίσης, η ανάκτηση των δεδομένων θα πρέπει εύκολα και με κατανοητό τρόπο να οδηγεί στην πλήρη καταγραφή και έλεγχο των ενεργειών ως προς την αντιμετώπιση των συμβάντων ασφάλειας. Επίσης θα πρέπει να υποστηρίζεται η δυνατότητα παραγωγής αναφορών με αυτόματο τρόπο καθώς και η ικνηλάτηση των αιτιών ενός συμβάντος ασφάλειας και ο προσδιορισμός των ενεργειών που σχετίζονται με αυτό. Τέλος, το λογισμικό προστασίας από κυβερνοαπειλές θα πρέπει να δίνει τη δυνατότητα στους χρήστες να αξιολογούν τις εντοπισμένες απειλές και επιθέσεις σε διάφορα επίπεδα επικινδυνότητας και να ενημερώνονται για βέλτιστες πρακτικές για την προστασία από κυβερνοαπειλές.

Η υλοποίηση ενός Συστήματος με τα ανωτέρω χαρακτηριστικά αποτελεί ένα σημαντικό βήμα για την ευθυγράμμιση του Δήμου με την Εθνική Στρατηγική Κυβερνοασφάλειας και την ετοιμότητα του να ανταποκριθεί σε ένα σύγχρονο περιβάλλον στον Κυβερνοχώρο για την αντιμετώπιση συμβάντων ασφάλειας και την προστασία και ανθεκτικότητα των υποδομών του.

Ο Δρ. Πέτρος Γανός είναι Προϊστάμενος Τμήματος Σχεδιασμού και Μελετών Ψηφιακών Συστημάτων Δήμου Πατρέων

Η Ευαλωτότητα των Ψηφιακών Συστημάτων: Μαθήματα από την Πρόσφατη Κρίση Κυβερνοασφάλειας

Η πρόσφατη μαζική διακοπή των συστημάτων πληροφορικής που προκλήθηκε από προβλήματα της Microsoft και της CrowdStrike φέρνει στο προσκήνιο τη βαθιά ευαλωτότητα των σύγχρονων ψηφιακών συστημάτων και αναδεικνύει τα παγκόσμια προβλήματα κυβερνοασφάλειας που αντιμετωπίζουν οργανισμοί και επιχειρήσεις. Τα τεχνολογικά μπλακ άουτ που προκύπτουν από τέτοιες καταστάσεις δεν αποτελούν απλά τεχνικές ανωμαλίες, αλλά αποκαλύπτουν την εξάρτηση της παγκόσμιας οικονομίας από τα ψηφιακά συστήματα και την έλλειψη ανθεκτικότητας σε κρίσιμα συστήματα ασφαλείας. Η έκταση και η κλίμακα των επιπτώσεων είναι ανησυχητικές, επισημαίνοντας τη δυσκολία αντιμετώπισης απρόβλεπτων τεχνολογικών ατυχημάτων και απειλών στον κυβερνοχώρο.

Το πρώτο και ίσως πιο σημαντικό συμπέρασμα από το συγκεκριμένο περιστατικό είναι η αυξημένη εξάρτηση της παγκόσμιας οικονομίας και των υποδομών από ψηφιακά συστήματα. Ο ψηφιακός μετασχηματισμός των επιχειρήσεων έχει δημιουργήσει έναν κόσμο όπου οι τεχνολογικές λύσεις δεν είναι απλά συμπληρωματικές αλλά θεμελιώδεις για την ομαλή λειτουργία των επιχειρήσεων και των κρατικών οργανισμών. Από αεροπορικές εταιρείες μέχρι τράπεζες και συστήματα υγείας, η διακοπή της λειτουργίας των υπολογιστών και των δικτύων μπορεί να προκαλέσει σημαντική δυσλειτουργία, ακόμη και παράλυση των βασικών δραστηριοτήτων.

Η συγκεκριμένη κρίση επιβεβαίωσε ότι τα συστήματα πληροφορικής είναι ιδιαίτερα ευάλωτα ακόμη και σε φαινομενικά μικρά λάθη ή ελαττώματα λογισμικού. Η CrowdStrike, ένας από τους μεγαλύτερους παρόχους τεχνολογίας ασφαλείας, προκάλεσε το πρόβλημα μέσω μιας ενημέρωσης λογισμικού που επηρέασε τα Windows. Το γεγονός ότι ένα ελάττωμα σε ένα κομμάτι λογισμικού μπορεί να προκαλέσει παγκόσμια αναταραχή δείχνει πόσο εύθραυστο είναι το σύστημα στο σύνολό του. Τα συστήματα ασφαλείας που προορίζονται για την προστασία των δεδομένων και των υποδομών μπορεί να γίνουν, λόγω εσωτερικών σφαλμάτων, η αιτία εκτεταμένων διακοπών. Αυτό το φαινόμενο αναδεικνύει τον κίνδυνο που συνεπάγεται η ολοένα και αυξανόμενη πολυπλοκότητα των ψηφιακών συστημάτων.

Επιπλέον, η κρίση αυτή δείχνει πώς η ψηφιακή ασφάλεια δεν είναι απλώς θέμα προστασίας από εξωτερικές επιθέσεις, όπως κυβερνοεπιθέσεις, αλλά εξίσου και θέμα ανθεκτικότητας έναντι εσωτερικών σφαλμάτων και ατυχημάτων. Οι αναφορές ότι ορισμένα συστήματα χρειάζονται μέχρι και 15 επανεκκινήσεις για να επανέλθουν πλήρως, και η ανάγκη για χειροκίνητες διαδικασίες αποκατάστασης από τους τεχνικούς της CrowdStrike, υπογραμμίζουν τη δυσκολία της αποκατάστασης σε περιπτώσεις κρίσεων πληροφορικής. Οι διακοπές αυτές δεν επιλύονται με απλές διαδικασίες, αλλά απαιτούν συστηματική παρέμβαση, γεγονός που καθιστά τα συστήματα εξαιρετικά ευάλωτα σε προβλήματα μεγάλης κλίμακας.

Ένα άλλο σημαντικό συμπέρασμα είναι η πολυπλοκότητα των σχέσεων μεταξύ των διαφορετικών προμηθευτών και τεχνολογικών λύσεων. Στη συγκεκριμένη περίπτωση, το λογισμικό ασφαλείας της CrowdStrike, που διαδραματίζει κρίσιμο ρόλο στην προστασία συσκευών και δεδομένων, προκάλεσε πρόβλημα στα λειτουργικά συστήματα της Microsoft, επηρεάζοντας τους πελάτες της πλατφόρμας Azure. Το ζήτημα αυτό τονίζει τη σημασία των συνεργασιών και της αλληλεξάρτησης στον κυβερνοχώρο, ενώ παράλληλα υπογραμμίζει την ανάγκη για πιο ολοκληρωμένες και συντονισμένες διαδικασίες ασφάλειας.

Οι επιπτώσεις αυτού του συμβάντος φέρνουν επίσης στο προσκήνιο τη σημασία της ταχείας απόκρισης και αποκατάστασης σε περίπτωση ψηφιακής κρίσης. Παρόλο που η CrowdStrike και η Microsoft ανέπτυξαν γρήγορα διορθώσεις για το πρόβλημα, οι δηλώσεις των ειδικών ότι η πλήρης αποκατάσταση μπορεί να διαρκέσει ημέρες ή και εβδομάδες αναδεικνύουν την αδυναμία των συστημάτων να ανακάμψουν άμεσα. Αυτή η καθυστέρηση μπορεί να προκαλέσει τεράστια οικονομική ζημία στις επιχειρήσεις, ενώ ταυτόχρονα διακυβεύεται η εμπιστοσύνη των πελατών στις τεχνολογικές λύσεις.

> *Η ανάγκη για αναθεώρηση των στρατηγικών κυβερνοασφάλειας είναι επιτακτική. Οι επιχειρήσεις και οι οργανισμοί πρέπει να υιοθετήσουν πιο προηγμένα συστήματα ασφαλείας που δεν θα επικεντρώνονται μόνο στην προστασία από εξωτερικούς κινδύνους, αλλά και στην ανθεκτικότητα σε εσωτερικά σφάλματα.*

Παράλληλα, η ευρύτερη εικόνα των κυβερνοαπειλών που αντιμετωπίζει ο κόσμος σήμερα γίνεται πιο ξεκάθαρη. Ενώ σε αυτή την περίπτωση δεν υπήρχε κυβερνοεπίθεση, οι συνέπειες δείχνουν πώς τα ελαττώματα και τα σφάλματα στο λογισμικό μπορούν να είναι εξίσου καταστροφικά με μια επίθεση από χάκερ. Η ολοένα και αυξανόμενη πολυπλοκότητα των συστημάτων και η συνεχή ενσωμάτωση νέων τεχνολογιών αυξάνουν τον κίνδυνο σφαλμάτων, ενώ παράλληλα οι κυβερνοαπειλές γίνονται όλο και πιο εξελιγμένες.

Η ανάγκη για αναθεώρηση των στρατηγικών κυβερνοασφάλειας είναι επιτακτική. Οι επιχειρήσεις και οι οργανισμοί πρέπει να υιοθετήσουν πιο προηγμένα συστήματα ασφαλείας που δεν θα επικεντρώνονται μόνο στην προστασία από εξωτερικούς κινδύνους, αλλά και στην ανθεκτικότητα σε εσωτερικά σφάλματα. Οι τεχνικές αυτές θα πρέπει να περιλαμβάνουν την εφαρμογή διαδικασιών αποκατάστασης που θα επιτρέπουν την ταχύτερη και πιο αποτελεσματική ανάκαμψη σε περίπτωση κρίσης.

Επιπλέον, οι παγκόσμιοι οργανισμοί και οι κυβερνήσεις πρέπει να αναπτύξουν πιο σφιχτά πρότυπα ασφαλείας για τους προμηθευτές τεχνολογίας και να προωθήσουν τη συνεργασία μεταξύ των εταιρειών. Η διασφάλιση ότι κάθε προμηθευτής θα ακολουθεί τα υψηλότερα πρότυπα ασφαλείας και ότι θα υπάρχει επαρκής εποπτεία στις διαδικασίες ανάπτυξης λογισμικού, είναι ζωτικής σημασίας για την αποφυγή μελλοντικών καταστροφών.

Συνοψίζοντας, η κρίση της CrowdStrike και της Microsoft φανερώνει τις βαθιές αδυναμίες των σύγχρονων ψηφιακών συστημάτων και τη σημασία της κυβερνοασφάλειας σε έναν παγκοσμιοποιημένο και πλήρως ψηφιακό κόσμο. Είναι σαφές ότι η κυβερνοασφάλεια δεν αφορά πλέον μόνο την προστασία από κακόβουλες επιθέσεις, αλλά και την ανθεκτικότητα των συστημάτων έναντι των εσωτερικών τεχνολογικών αποτυχιών.

Forum ΑΝΑΠΤΥΞΗΣ 2024
ΗΜΕΡΙΔΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

- ΔΕΥΤΕΡΑ 23 / 9 / 2024 10:00-14:00
- ΥΒΡΙΔΙΚΗ ΕΚΔΗΛΩΣΗ
- Με φυσική παρουσία: Ξενοδοχείο MY WAY (Όθωνος Αμαλίας 16 Πάτρα)

LIVE στο www.forumanaptixis.gr

ΠΡΟΓΡΑΜΜΑ / ΠΡΟΣΚΛΗΣΗ

9:30-10:00 Προσέλευση-Εγγραφές -Καφές

10:00-12:00 "Νέες οδηγίες και κανονισμοί για την Κυβερνοασφάλεια – Κίνδυνοι και υποχρεώσεις"

Προεδρείο:
Δημήτρης Σερπάνος, *Πρόεδρος ΙΤΥΕ «Διόφαντος»*
Παναγιώτης Γιαλένιος, *εκδότης εφ. «Σύμβουλος Επιχειρήσεων»*

Χαιρετισμοί
- Χρήστος Μπούρας, *Πρύτανης Πανεπιστημίου Πατρών*
- Πλάτων Μαρλαφέκας, *Πρόεδρος Επιμελητηρίου Αχαΐας*
- Κλεομένης Μπάρλος, *Πρόεδρος Συνδέσμου Επιχειρήσεων και Βιομηχανιών Πελοποννήσου και Δυτικής Ελλάδος*
- Νάντια Λιάπη, *Group CIO, Group Director GRC Services, Space Hellas*

Ομιλητές
Δημήτριος Σερπάνος, *Πρόεδρος ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ και Καθηγητής Πανεπιστημίου Πατρών*
Θέμα: Κυβερνοασφάλεια: Κίνδυνοι, Απειλές και Άμυνες
Ιωάννης Αλεξάκης, *Γενικός Διευθυντής Επιτελικού Σχεδιασμού, Εθνική Αρχή Κυβερνοασφάλειας*
Θέμα: Εθνική Αρχή Κυβερνοασφάλειας: Στρατηγική και Στόχοι
Γεώργιος Στεργιόπουλος, *Επίκουρος Καθηγητής, Πανεπιστήμιο Αιγαίου*
Θέμα: Κατακτώντας το NIS2: Οδηγός για την Πλοήγηση στην Οδηγία ΕΕ 2022/2555

Θα ακολουθήσουν ερωτήσεις σε ομιλητές

12:00-14:00 "Ανάπτυξη τεχνολογικών εφαρμογών Κυβερνοασφάλειας - Λύσεις και ευκαιρίες"

Προεδρείο
Αθανάσιος Ζούπας, *Πρόεδρος Δικηγορικού Συλλόγου Πατρών*
Παναγιώτης Γιαλένιος, *εκδότης εφ. «Σύμβουλος Επιχειρήσεων»*

Παρουσιάσεις
- Νάντια Λιάπη, *Group CIO, Group Director GRC Services, Space Hellas*
  Θέμα: «Thank God for NIS II»
- Σταμάτης Τσολακίδης, *Data Center Sales Executive , Greece, Cyprus & Malta, Dell Technologies*
  Θέμα: «Recovering Your Business from a Sophisticated Ransomware or Cyberattack»
- Σωκράτης Κελέσογλου, *Senior Cybersecurity Presales Consultant, Space Hellas*
  Θέμα: «NIS 2 in Practice»
- Αντιγόνη Δόβα, *Field Product Manager, Dell Client solutions*
  Θέμα: «Security on End User devices»
- Δρ. Θεόδωρος Κομνηνός, *Διευθυντής Πληροφοριακών Συστημάτων, Εφαρμογών και Κυβερνοασφάλειας ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ*
  Θέμα: "Κυβερνοασφάλεια σε δημόσια πληροφοριακά συστήματα και εφαρμογές"
- Δημήτρης Ανεστόπουλος, *Προϊστάμενος Διεύθυνσης Ψηφιακής Διακυβέρνησης ΠΔΕ*
  Θέμα: Ζητήματα Κυβερνοασφάλειας στην Περιφέρεια Δυτ.Ελλάδας
- Στέφανος Μίχος, *Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών (Υ.Α.Σ.Π.Ε.), Αποκεντρωμένη Διοίκηση Πελ/σου, Δυτ. Ελλάδας & Ιονίου*
  Θέμα: «Θωράκιση κρισιμων υποδομών, ασφάλεια και νεες τεχνολογίες»
- Δρ. Πέτρος Γανός, *Προϊσταμένος Τμήματος Σχεδιασμού και Μελετών Ψηφιακών Συστημάτων Δήμος Πατρέων*
  Θέμα: "Κυβερνοασφάλεια στην Τοπική Αυτοδιοίκηση"

ΚΕΝΤΡΙΚΟΙ ΧΟΡΗΓΟΙ

SPACE
DELL Technologies
TITANIUM PARTNER

ΣΥΝΔΙΟΡΓΑΝΩΣΗ

UNIVERSITY OF PATRAS ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ
ΣΥΝΔΕΣΜΟΣ ΕΠΙΧΕΙΡΗΣΕΩΝ και ΒΙΟΜΗΧΑΝΙΩΝ Πελοποννήσου & Δυτικής Ελλάδος
ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΧΑΪΑΣ Από το 1836

ΜΕ ΤΗΝ ΥΠΟΣΤΗΡΙΞΗ

enterprise europe network
EDIH HEALTH
IRI BEYOND

ΧΟΡΗΓΟΙ ΕΠΙΚΟΙΝΩΝΙΑΣ

IONIAN REGIONAL TV
Σύμβουλος Online www.symboulos.gr

ΟΡΓΑΝΩΣΗ

Σύμβουλος επιχειρήσεων

ΠΛΗΡΟΦΟΡΙΕΣ: Μαιζώνος 94 Πάτρα | Τηλ: 2610-620.574 | e-mail:symboulo@otenet.gr | www.forumanaptixis.gr | @diktyoforumanaptixis.gr | κ. Π. Γιαλένιος

ΠΛΗΡΩΜΕΝΟ ΤΕΛΟΣ Τ.Κ.Κ. ΠΑΤΡΑΣ Αριθμός Αδείας 34 Κωδικός 2581
ΕΚΔΟΤΗ ΕΛΤΑ Hellenic Post

Ερύμανθος: Οι πυρόπληκτοι αγωνιούν

Αγωνία για τους πυρόπληκτους του Ερυμάνθου, οι οποίοι εξακολουθούν να ζουν σε κοντεϊνερ. Ερώτηση στο Περιφερειακό από την παράταξη Καρπέτα.

Σελ. 10

Τα οικονομικά του Δήμου Πατρέων

Καμία παρατήρηση στον Δήμο Πατρέων από τους Ορκωτούς Λογιστές, όπως ανακοινώθηκε στο Δημ. Συμβούλιο. Μεγάλο ζητούμενο η υποχρηματοδότηση.

Σελ. 3

Σελ. 19

Σήμερα η Βραδιά Ερευνητή στο νέο Δημαρχείο

Η Εβδομαδιαία
Οικονομική Εφημερίδα της Αχαΐας

Μαιζώνος 94 | 262 21 Πάτρα
Τηλ: 2610 620 574

www.symboulos.gr
e-mail: symboulo@otenet.gr
Τιμή Φύλλου: 1,00 €

Περίοδος Γ' | **Αρ. Φύλλου 1371**
Παρασκευή 27 Σεπτεμβρίου 2024

Σύμβουλος επιχειρήσεων

27ο Forum Ανάπτυξης 2024 Υβρίδιο 23-24 Νοεμβρίου
Σελ. 21

Υπογειοποίηση
Παρέμβαση του ΤΕΕ/ΤΔΕ

Επιστολή στον Πρωθυπουργό για το ζήτημα της υπογειοποίησης του τρένου απέστειλε ο Πρόεδρος του ΤΕΕ/ΤΔΕ Βαγγέλης Καραχάλιος, ζητώντας την παρέμβασή του για το ζήτημα. Και αυτό για να μην κινδυνεύσει να μείνει μετέωρος ο στόχος, που δεν είναι άλλος από την σιδηροδρομική διασύνδεση της Πάτρας με την Αθήνα.

Σελ. 5

Ημέρες Κληρονομιάς

Δράσεις που στόχο έχουν να αναδείξουν τον πολιτιστικό πλούτο της Ευρώπης πραγματοποιούνται το Σαββατοκύριακο στο Αρχαιολογικό Μουσείο Πατρών.

Σελ. 22

> Κυβερνοασφάλεια: Κίνδυνοι, λύσεις, και μια νέα ακαδημαϊκή πρωτοβουλία

Οι προκλήσεις
για δημόσιους φορείς και επιχειρήσεις

Κατά την διάρκεια της ημερίδας επίσης ανακοινώθηκε και μια σημαντική εξέλιξη καθώς το Πανεπιστήμιο Πατρών σε συνεργασία με το Πανεπιστήμιο Κύπρου και το ΙΤΥΕ «Διόφαντος» προχωρούν στην ίδρυση μεταπτυχιακού με αντικείμενο την κυβερνοασφάλεια, διότι στον συγκεκριμένο κλάδο παρουσίαζεται μεγάλη έλλειψη στελεχών.

Η μεγάλη ένταση των κυβερνοεπιθέσεων παγκοσμίως, με τζίρους που υπερβαίνουν τα 15 τρισ. ευρώ ετησίως, αλλά και η καταληκτική ημερομηνία της 18ης Οκτωβρίου, καθώς τότε θα πρέπει να εφαρμοστούν ορισμένες από τις δεσμεύσεις της κοινοτικής οδηγίας NIS2 για την κυβερνοασφάλεια σε δημόσιους φορείς και επιχειρήσεις, αναδείχτηκαν στην σχετική ημερίδα που πραγματοποιήθηκε από τον «Σ.Ε.».

Η ημερίδα έγινε σε μια άκρως επίκαιρη χρονική στιγμή, καθώς προτάθηκαν συγκεκριμένες λύσεις για την αποτροπή των κινδύνων, ενώ αναδείχτηκε και ο προβληματισμός του επιχειρηματικού κόσμου, αφού στόχο μπορεί να αποτελέσουν τόσο μικρομεσαίες επιχειρήσεις όσο και μεγάλοι φορείς και οργανισμοί.

Σελ. 9, 12-17

Σε κίνδυνο το χιονοδρομικό Καλαβρύτων;

Η βουλευτής Αχαΐας Σία Αναγνωστοπούλου και η Έφη Αχτσιόγλου κατέθεσαν κοινοβουλευτική ερώτηση προς τον υπουργό Εθνικής Οικονομίας και Οικονομικών με θέμα: «Σε κίνδυνο το μέλλον του Χιονοδρομικού Κέντρου Καλαβρύτων». Όπως αναφέρει στην ερώτηση η κ. Αναγνωστοπούλου, το κύριο πρόβλημα εντοπίζεται στην καθυστέρηση εκταμίευσης των κονδυλίων από το ΕΣΠΑ. Αυτή η κατάσταση δημιουργεί σημαντικά προβλήματα στην υλοποίηση του συνολικού έργου αναβάθμισης και στην εύρυθμη λειτουργία του χιονοδρομικού κέντρου. Αξίζει να σημειωθεί ότι υπάρχει ο κίνδυνος της μη λειτουργίας του αναβατήρα «Στύγα» καθώς η ιταλική εταιρεία που προμηθεύει τον εξοπλισμό δεν θα προχωρήσει στην πιστοποίηση του αναβατήρα χωρίς την καταβολή των οφειλομένων ποσών».

Μεταπτυχιακά στην Κυβερνοασφάλεια

Μια σημαντική είδηση από τον Πρύτανη του Πανεπιστημίου Πατρών καθώς το Ίδρυμα σε συνεργασία με το ΙΤΥΕ Διόφαντος και το Πανεπιστήμιο Κύπρου θα προχωρήσει στην υλοποίηση Μεταπτυχιακού για την κυβερνοασφάλεια.

Ειδικότερα, οι τρεις φορείς βρίσκονται στο τελικό στάδιο συζητήσεων για την ίδρυση ενός πτυχιακού με αντικείμενο την cyber security και το συγκεκριμένο πρόγραμμα θα γίνεται στα αγγλικά, δίνοντας την δυνατότητα σε χιλιάδες επιστήμονες να ασχοληθούν με ένα αντικείμενο που έχει τεράστιο ενδιαφέρον.

Η αναφορά έγινε δημόσια για πρώτη φορά στην ημερίδα για την Κυβερνοασφάλεια που διοργάνωσε ο «Σ.Ε.» και το ενδιαφέρον στην αίθουσα ήταν μεγάλο, καθώς στο διάλειμμα πολλοί από τους παριστάμενους επεδίωκαν να αντλήσουν περαιτέρω πληροφορίες. Και αυτό γιατί, όπως διαφάνηκε και στην ημερίδα, το πεδίο του τομέα της κυβερνοασφάλειας είναι ανεξάντλητο και κρίσιμο, αφού στο έλεος επιθέσεων κινδυνεύουν να βρεθούν χιλιάδες επιχειρήσεις και οργανισμοί. Οι αναλυτές και οι παριστάμενοι στην ενδιαφέρουσα ημερίδα προσδιορίζουν ότι το έγκλημα στον κυβερνοχώρο θα φθάσει τα 10,5 τρισ. δολάρια παγκοσμίως το 2025.

Γ.Η.

Ο κ. Χρήστος Μπούρας

Κρίσιμο στοιχείο η εκπαίδευση

Την απόκτηση του μεταπτυχιακού του από το Πανεπιστήμιο Πατρών στον τομέα της Ψηφιακής Οικονομίας και Διοίκησης υπενθύμισε στους παρισταμένου στην ημερίδα για την Κυβερνοασφάλεια του «Σ.Ε.», ο Πρόεδρος του Επιμελητηρίου Αχαΐας Πλάτωνας Μαρλαφέκας. Και αναγνώρισε ότι το μεταπτυχιακό για την Κυβερνοασφάλεια που προανήγγειλε ο κ. Μπούρας θα συμβάλλει σημαντικά και στην ασφάλεια των επιχειρήσεων, αφού σήμερα δεν υπάρχουν στελέχη που να επιφορτιστούν με το συγκεκριμένο αντικείμενο. Μάλιστα οι ευάλωτες στις κυβερνοεπιθέσεις είναι οι μικρομεσαίες επιχειρήσεις.

Όπως είπε ο κ. Μαρλαφέκας, στον ανανεωμένο χώρο του Επιμελητηρίου στην οδό Ρήγα Φεραίου, που αυτή την περίοδο εκτελούνται εργασίες αναβάθμισης, θα δημιουργηθεί υβριδική αίθουσα για εκπαίδευση και ενημέρωση και σε αυτή θα γίνουν προγράμματα εκπαίδευσης των εργαζομένων για να αντιμετωπίσουν περιστατικά κυβερνοεπιθέσεων. Και αυτό γιατί το 65% των εργαζομένων δεν γνωρίζει να αντιμετωπίζει τέτοιου είδους περιστατικά και η εκπαίδευσή του είναι κρίσιμος παράγοντας για την διάσωση της επιχείρησης.

Γ.Η.

Ο κ. Πλάτωνας Μαρλαφέκας

Θετική στο ρόλο των Περιφερειών η Ούρσουλα φον ντερ Λάιεν

Απαντητική επιστολή έστειλε η Πρόεδρος της Ευρωπαϊκής Επιτροπής Ursula Von Der Leyen στις 19 Σεπτεμβρίου στην κοινή επιστολή που της είχαν στείλει οι Περιφέρειες της CPMR, συμπεριλαμβανομένης και της Περιφέρειας Δυτικής Ελλάδας, σχετικά με το μέλλον της πολιτικής συνοχής. Η Πρόεδρος επισημαίνει πως ο ρόλος των περιφερειών και της τοπικής αυτοδιοίκησης είναι καθοριστικός στην πολιτική συνοχής και στα σχετικά ταμεία και παρέπεμψε για το θέμα αυτό επικοινωνία και συνεργασία με τον νέο αρμόδιο Επίτροπο, τον Εκτελεστικό Αντιπρόεδρο για τη Συνοχή και τις Μεταρρυθμίσεις, Raffaele Fitto. Όπως επισήμανε ο Αντιπεριφερειάρχης Π.Ε. Αχαΐας Φωκίων Ζαΐμης: «Η πολιτική συνοχής και τα αντίστοιχα χρηματοδοτικά εργαλεία της είναι βασικά εργαλεία ανάπτυξης για τις Περιφέρειες και αναπόσπαστο μέρος της περιφερειακής πολιτικής. Γι' αυτό τον λόγο πρέπει όλοι οι εμπλεκόμενοι φορείς να στηρίζουν την πολιτική συνοχής ανεξαρτήτου ιδεολογίας». .

Και οι αγρότες στο Αλλάζω Συσκευή για Επιχειρήσεις

Απλοποίηση των διαδικασιών, επιπλέον ενίσχυση στις επιλέξιμες δαπάνες και την ένταξη των αγροτών στους δυνητικούς δικαιούχους φέρνει η τροποποιητική Απόφαση του Υπουργού Περιβάλλοντος και Ενέργειας, κ. Θόδωρου Σκυλακάκη και του Αναπληρωτή Υπουργού Εθνικής Οικονομίας και Οικονομικών, κ. Νίκου Παπαθανάση στο πρόγραμμα «Αλλάζω Συσκευή για τις Επιχειρήσεις». Συγκεκριμένα, οι αγρότες βρίσκονται πλέον ανάμεσα στους δυνητικούς δικαιούχους του προγράμματος, με δυνατότητα υποβολής αιτήσεων από χθες, Πέμπτη 26 Σεπτεμβρίου 2024.

Ακόμα απλοποιούνται οι δυνατότητες επίτευξης του ενεργειακού στόχου που θέτει το πρόγραμμα. Συγκεκριμένα, για τις αντικαταστάσεις συσκευών (π.χ. κλιματιστικό, ψυγείο, φούρνος, αντλία θερμότητας κ.α.) θα αρκεί μία νέα βεβαίωση εκπομπών για κάθε συσκευή. Οι ενεργειακοί επιθεωρητές ή ελεγκτές θα μπορούν να την εκδίδουν (πριν και μετά την εγκατάστασή της), αντί για τη χρήση Πιστοποιητικού Ενεργειακής Απόδοσης (ΠΕΑ) ή ενεργειακού ελέγχου.

> *Από τον Οκτώβριο θα έρχεται στο κινητό ένα ηλεκτρονικό ειδοποιητήριο για πρόστιμο το οποίο θα έχει επιβληθεί για εκπρόθεσμη υποβολή δήλωσης είτε για ΦΠΑ, είτε φορολογική, είτε για τον φόρο παρακράτησης. Το πρόστιμο για ένα φυσικό πρόσωπο που δεν υποβάλλει εμπρόθεσμα τη δήλωσή του είναι 100 ευρώ. Για μια επιχείρηση με απλογραφικά στοιχεία είναι βιβλία είναι 250 ευρώ και με διπλογραφικά 500 ευρώ. Με το νέο σύστημα έγκαιρης ειδοποίησης ο φορολογούμενος μπορεί να γλυτώνει τις προσαυξήσεις.*

Επωνύμως

Είναι πολλά τα λεφτά κύριε Ντράγκι

του **Γιώργου Μαρκατάτου**

> *Η έκθεση Ντράγκι δεν αρνείται να κατονομάσει τους λόγους που έχουν οδηγήσει στη διαπίστωση ότι η παραγωγικότητα φθίνει ολοένα στην Ευρώπη σε σχέση με άλλες γεωπολιτικές ενότητες και αυτό έχει άμεσο αντίκτυπο ακόμη και κυρίως, στη δημοκρατία.*

Με αναλήθειες μας σερβίρει συχνά – πυκνά η γραφειοκρατική ελίτ των Βρυξελλών, και αυτή τη φορά διαπιστώνουμε ότι στο τελευταίο εισαγωγικό σημείωμα στην ιστοσελίδα της ανταγωνιστικότητας της εκτελεστικής εξουσίας τονίζει ότι: «Η Ευρώπη σήμερα είναι μία από τις πιο ανταγωνιστικές, δυναμικές και καινοτόμες περιοχές στον κόσμο. Ωστόσο, τα τελευταία χρόνια έφεραν ορισμένες ιστορικές προκλήσεις, συμπεριλαμβανομένης της πανδημίας COVID-19 και του επιθετικού πολέμου της Ρωσίας κατά της Ουκρανίας. Αν και η Ευρωπαϊκή Ένωση κατάφερε να αντιμετωπίσει επιτυχώς αυτές τις κρίσεις, αυτές επηρέασαν αρνητικά τη συνολική ανταγωνιστικότητά μας». Ας δούμε την αλήθεια!

Ρίγη τρόμου διαπέρασαν τους εγκεφάλους που απομένουν στους ταγούς της Ευρώπης ακούγοντας ότι απαιτούνται μαζικές κυβερνητικές και ιδιωτικές επενδύσεις, αξίας τουλάχιστον 800 δισ. ευρώ ετησίως, μεχρι τουλάχιστον το 2030!. Και μάλιστα δίπλα στον ετήσιο προϋπολογισμό της ΕΕ που αγγίζει πλέον τα 200 δις € το χρόνο! Άρα μας λέγει ο συμπαθέστατος κ. Ντράγκι ότι οι Ευρωπαίοι θα δουν να μειώνεται και μάλιστα σημαντικά το επίπεδο διαβίωσής τους. Πράγμα που εμείς οι Έλληνες γνωρίζουμε πολύ καλά τι γίνεται τόσο από την πανδημία, όσο και από τη ρωσο-ουκρανική σύρραξη.

Η έκθεση Ντράγκι δεν αρνείται να κατονομάσει τους λόγους που έχουν οδηγήσει στη διαπίστωση ότι η παραγωγικότητα φθίνει ολοένα στην Ευρώπη σε σχέση με άλλες γεωπολιτικές ενότητες και αυτό έχει άμεσο αντίκτυπο ακόμη και κυρίως, στη δημοκρατία. Και αυτό έχει γίνει πλέον κοινός τόπος να διαπιστώνουμε ότι με έναν παράγοντα την πανδημία (που έπληξε όλα τα πλάτη και τα μήκη του πλανήτη), συνακολουθούμενο από τη ρωσική εισβολή στην Ουκρανία, και μια ακατάσχετη λαθρομετανάστευση κυρίως τις παραθαλάσσιες νότιες περιοχές της ΕΕ, ολοένα και δυσχεραίνεται η ζωή των Ευρωπαίων πολιτών. Ακριβές συνεπακόλουθο είναι η παρατηρούμενη στροφή προς την άκρα δεξιά, που έχει επικυριαρχήσει σε όλο το πολιτικό σκηνικό της ΕΕ. Αλλά το βασικό σκηνικό είναι η διολίσθηση του άξονα Παρίσι – Βερολίνο, που μόλις και μετά βίας κατάφεραν οι Μακρόν και Σότζς να επιβιώσουν (τουλάχιστον για μικρό διάστημα ακόμη!)

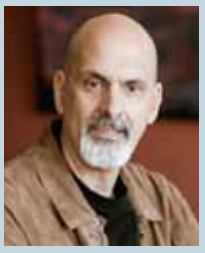
Σημασία έχει να τονιστεί ότι ο Ντράγκι δε μάσησε τα λόγια του στους ευρωβουλευτές στις 17/9/24, λέγοντας «Η Ευρώπη βρίσκεται αντιμέτωπη με μια επιλογή μεταξύ εξόδου, παράλυσης ή ολοκλήρωσης»[1]

Ένα από τα κορυφαία παραδείγματα του πρώην κεντρικού τραπεζίτη και πρώην Ιταλού πρωθυπουργού αφορά τις εταιρείες της ΕΕ δαπάνησαν περίπου 270 δισεκατομ-

Συνέχεια στη σελ. 20

Κυβερνοασφάλεια: Οι κίνδυνοι

Μια σειρά από κρίσιμες απαντήσεις στον τομέα της κυβερνοασφάλειας, σε μια ιδιαίτερα καίρια στιγμή, δεδομένου ότι το ζήτημα των επιθέσεων είναι καθημερινό, δόθηκε κατά την διάρκεια της ημερίδας με θέμα «Ψηφιακός μετασχηματισμός και Κυβερνοασφάλεια: κίνδυνοι, υποχρεώσεις και ευκαιρίες» που διοργανώθηκε την περασμένη Δευτέρα στο ξενοδοχείο My Way από τον «Σύμβουλο Επιχειρήσεων» σε συνεργασία με το Πανεπιστήμιο Πατρών, τον Σύνδεσμο Βιομηχανιών Πελοποννήσου και Δυτικής Ελλάδας, το Επιμελητήριο Αχαΐας, το ΙΤΥΕ «Διόφαντος» και με την Κεντρική Χορηγία των εταιρειών Space Hellas και Dell Technologies. Στο προεδρείο της πρώτης συνεδρίας ήταν ο εκδότης του «Σ.Ε.» Παναγιώτης Γιαλένιος και ο Πρόεδρος του ΙΤΥΕ «Διόφαντος» Δημήτρης Σερπάνος. Στον χαιρετισμό του ο κ. Γιαλένιος τόνισε μεταξύ άλλων ότι το συγκεκριμένο ζήτημα απασχολεί έντονα τις επιχειρήσεις και τον επιχειρηματικό κόσμο γενικότερα και δημιουργούνται νέες υποχρεώσεις σε φορείς και επιχειρήσεις.



Στην ημερίδα παρέστη ο Αναπληρωτής Περιφερειάρχης **Χαράλαμπος Μπονάνος** που απηύθυνε χαιρετισμό λέγοντας ότι το νέο νομοθετικό πλαίσιο αλλάζει για την κυβερνοασφάλεια και γίνεται πιο αυστηρό και η προσαρμογή στα νέα δεδομένα είναι απαραίτητη όχι μόνο για τη συμμόρφωσή μας με τις νομικές απαιτήσεις αλλά και για την ουσιαστική θωράκιση των υποδομών. «Σήμερα που έχουμε να κάνουμε με ένα νέο κόσμο, η κυβερνοασφάλεια δεν είναι τεχνικό ζήτημα αλλά πρέπει να αντιμετωπίζεται ως βασική προτεραιότητα» τόνισε χαρακτηριστικά.

> Δημήτρης Σερπάνος, Πρόεδρος ΙΤΥΕ «Διόφαντος»

«Η πρώτη επίθεση στην εφοδιαστική αλυσίδα συστημάτων»

Ο Δημήτρης Σερπάνος, Πρόεδρος του ΙΤΥΕ «Διόφαντος» στην παρουσίασή του μεταξύ άλλων τόνισε ποιες είναι οι εκφάνσεις των ψηφιακών κινδύνων για μια επιχείρηση.

Από την απάτη με πλαστά μηνύματα τραπεζών ή διωκτικών αρχών αλλά και μηνύματα που γίνονται με την χρήση του gov.gr με στόχο την υποκλοπή ευαίσθητων δεδομένων. Αναφέρθηκε επίσης εκτενώς στην πρόσφατη επίθεση που αποδίδεται στη Μοσάντ στο Λίβανο σε βάρος της Χεσμπολά, όπου προκλήθηκαν πολλαπλές εκρήξεις με την χρήση ασυρμάτων.

«Η Χεσμπολά έκανε μια έρευνα αγοράς και προμηθεύτηκε συστήματα τηλεπικοινωνιών και επέλεξαν συγκεκριμένο προμηθευτή. Μετά αγόρασαν τον εξοπλισμό τον οποίο και έλεγξαν για την ποιότητά του. Αυτός ο εξοπλισμός αποδείχτηκε ότι ήταν προβληματικός και το ενδιαφέρον της υπόθεσης είναι ότι έχουμε ένα σενάριο που πρέπει να το θυμόμαστε. Κάποιος παρήγγειλε ένα προϊόν και ο αντίπαλός του παραβίασε αυτό το προϊόν, αφού αγοράστηκε από συγκεκριμένο προμηθευτή και ο αντίπαλος υλοποίησε μια επίθεση. Αυτό είναι εξαιρετικά σημαντικό γιατί είναι μια επίθεση στην ακεραιότητα της εφοδιαστικής αλυσίδας. Η εφοδιαστική αλυσίδα σήμερα αποτελεί μια από τις κυριότερες παραμέτρους στην ανάπτυξη οποιουδήποτε συστήματος» περιέγραψε ο κ. Σερπάνος. Στη συνέχεια τόνισε με ποιο τρόπο μπορεί κάποιος να αντιμετωπίσει τις επιθέσεις που αναμένει για να οδηγηθεί σε λύση. Βασικό στάδιο είναι η αναγνώριση κινδύνων και απειλών, ακολούθως ο καθορισμός πολιτικών και η διαχείριση τους (management). Τέλος η επιλογή τεχνολογίας, η υλοποίησή, ο έλεγχος και η εκπαίδευση σε αυτές για την αντιμετώπιση της κυβερνοασφάλειας. Ως προς το προφίλ των επιτιθέμενων αυτοί είναι μοναχικοί hackers, ομάδες με κοινούς στόχους (πολιτικούς και οικονομικούς), εγκληματίες αλλά ακόμη και ολόκληρες χώρες, ωστόσο σε κάθε περίπτωση διαφέρουν τα μέσα και τα εργαλεία που χρησιμοποιούνται.

> Χρήστος Μπούρας, Πρύτανης Πανεπιστημίου Πατρών

«Αυτό είναι το τείχος προστασίας του Πανεπιστημίου»

Ο Πρύτανης του Πανεπιστημίου Πατρών Χρήστος Μπούρας παρουσίασε τις πολιτικές που ακολουθεί το ίδρυμα στον τομέα της κυβερνοασφάλειας για να αποφύγει τις επιθέσεις. Το Πανεπιστήμιο ακολουθεί την πολιτική της λεγόμενης «Διαστρωματωμένης Προσέγγισης», δηλαδή αντιμετωπίζοντας το ζήτημα της κυβερνοασφάλειας σε πολλά επίπεδα.Το email αναγνωρίζεται ως ιδιαίτερα κρίσιμη υπηρεσία για τη λειτουργία του ιδρύματος. Ένα ακόμη μέτρο που λαμβάνει το Πανεπιστήμιο είναι να διαθέτει αντίγραφα ασφαλείας. Τα δεδομένα είναι εξαιρετικής σημασίας πόρος για το ίδρυμα και η προστασία τους αποτελεί προτεραιότητα. Επίσης κρίσιμο κομμάτι αποτελούν οι servers και οι σταθμοί εργασίας που είναι διαμορφωμένοι με όλες τις βασικές ρυθμίσεις ασφάλειας με βάση διεθνώς αποδεκτά πρότυπα και οδηγίες για τα λειτουργικά συστήματα. Γίνεται απενεργοποίηση λογαριασμών που δεν σχετίζονται πλέον με κάποιον χρήστη ενώ γίνεται εκχώρηση ελάχιστων απαιτούμενων δικαιωμάτων πρόσβασης σε λογαριασμούς υπηρεσιών. Λειτουργούν μόνο οι θύρες (ports), τα πρωτόκολλα και οι δικτυακές υπηρεσίες που είναι απαραίτητες για τη διεκπεραίωση των επιχειρησιακών λειτουργιών. Οι χρήστες με standard δικαιώματα (non-privileged) δεν μπορούν να απενεργοποιήσουν ή να τροποποιήσουν τις ρυθμίσεις ασφάλειας στο λειτουργικό τους σύστημα.

> Πλάτων Μαρλαφέκας, Πρόεδρος Επιμελητηρίου Αχαΐας

«Μια νέα κυβερνοεπίθεση, κάθε 39 δευτερόλεπτα»

«Ο νέος ψηφιακός κόσμος προσφέρει απεριόριστες ευκαιρίες, αλλά φέρνει και νέες προκλήσεις», τόνισε ο Πρόεδρος του Επιμελητηρίου Αχαϊας κ. Πλάτωνας Μαρλαφέκας κατά την παρέμβασή του και αναφέρθηκε στα ανησυχητικά στατιστικά στοιχεία για τις «κυβερνοεπιθέσεις» που αυξάνονται ραγδαία σε παγκόσμιο επίπεδο, αλλά και στην χώρα μας. Επεσήμανε επίσης την ανάγκη οι επιχειρήσεις και το προσωπικό τους να προσαρμοστούν ώστε να μπορούν να αντιμετωπίσουν αυτή την σύγχρονη, επικίνδυνη πραγματικότητα.

«Τα στοιχεία δείχνουν ότι κανείς δεν είναι ασφαλής» σημείωσε ο κ. Μαρλαφέκας εξηγώντας: «Το 2023 καταγράφηκαν περισσότερες από 2.365 κυβερνοεπιθέσεις σε παγκόσμιο επίπεδο επηρεάζοντας περίπου 350 εκατομμύρια άτομα. Το κόστος των παραβιάσεων δεδομένων έχει φτάσει τα 4,88 εκατομμύρια δολάρια ανά περιστατικό κατά μέσο όρο. Κάθε 39 δευτερόλεπτα, σημειώνεται μια νέα κυβερνοεπίθεση, και το συνολικό κόστος των ζημιών από το κυβερνοέγκλημα αναμένεται να ανέλθει σε 10,5 τρισεκατομμύρια δολάρια ετησίως έως το 2025».

Αναφερόμενος στην άμυνα των επιχειρήσεων απέναντι στο κυβερνοέγκλημα, ο Πρόεδρος του Επιμελητηρίου αναφέρθηκε στην ανάγκη να στηριχθούν οι επιχειρήσεις, κυρίως οι μικρότερες, ώστε να αντιμετωπίσουν τις νέες προκλήσεις.

και οι νέες υποχρεώσεις

> Κλεομένης Μπάρλος, Πρόεδρος Συνδέσμου Επιχειρήσεων και Βιομηχανιών Πελοποννήσου & Δυτικής Ελλάδος

«Απομόνωση συστημάτων από τον έξω κόσμο»

Ο Πρόεδρος του Συνδέσμου Επιχειρήσεων και Βιομηχανιών Πελοποννήσου & Δυτικής Ελλάδος Κλεομένης Μπάρλος στην τοποθέτησή του που έγινε διαδικτυακά τόνισε μεταξύ άλλων: «Η κυβερνοασφάλεια δεν περιορίζεται στο διαδίκτυο και μόνο. Εκτός από την αντιμετώπιση μιας κυβερνοεπίθεσης, που συνήθως όλοι την έχουν αναθέσει σε κάποιον, επεκτείνεται πλέον και στον έλεγχο των συσκευών που παίρνουν μέρος στο διαδίκτυο και αυτό είναι και το κινητό, οι υπολογιστές κ.α. Θα πρέπει συνεπώς να ελέγχονται όλα όσα συμμετέχουν σε αυτή την επικοινωνία όλων με όλους, δηλαδή και τα κινητά και οι υπολογιστές και όλα τα ψηφιακά διαχειριζόμενα συστήματα. Ο έλεγχος θα πρέπει να γίνεται για την αποφυγή τηλεπαρακολούθησης αλλά και τηλεκαταστροφής που είδαμε πρόσφατα με τα γεγονότα της Μέσης Ανατολής πόσο σημαντική ενδεχομένως να είνα».

Ο κ. Μπάρλος συνέστησε επίσης την πλήρη απομόνωση των ψηφιακών συστημάτων από το διαδίκτυο ώστε να μην είναι ορατά. Ακολούθως πρότεινε την δημιουργία ενός εσωτερικού συστήματος μεταφοράς δεδομένων ώστε αυτά να μην είναι ορατά σε εξωτερικούς παράγοντες. Ήδη, όπως σημείωσε ο κ. Μπάρλος, οι φαρμακευτικοί οργανισμοί εδώ και χρόνια έχουν απαγορεύσει βασικά δεδομένα, συνδεδεμένα σε σύστημα που έχει επαφή με τον έξω κόσμο.

> Νάντια Λιάπη, Group CIO, Group Director GRC Servises, της Space Hellas

«Στόχος μας να ενισχύσουμε την τοπική οικονομία»

Η Νάντια Λιάπη, Group CIO, Group Director GRC Servises, της Space Hellas στον χαιρετισμό της, παρουσίασε το προφίλ της εταιρείας που διαθέτει και υποκατάστημα στην Πάτρα από το 1994. Η εταιρεία ιδρύθηκε το 1985 και διαθέτει ένα σημαντικό δίκτυο πελατών στη Δυτική Ελλάδα, ενώ στο πελατολόγιο συγκαταλέγονται ιδιωτικές εταιρίες, βιομηχανίες και αλυσίδες καταστημάτων.

Η εταιρεία έχει προχωρήσει σε σημαντικές εξαγορές και μια από αυτές είναι η εταιρεία Singular Logic, εταιρεία που συλλέγει τα εκλογικά αποτελέσματα, οπότε το επίπεδο κυβερνοασφάλειας είναι κάτι παραπάνω από υψηλό. «Οταν έγινε η εξαγορά έκανα να κοιμηθώ ένα εξάμηνο, είτε γιατί σχεδίαζα είτε γιατί υλοποιούσα είτε γιατί αμυνόμουν στις πάρα πολλές επιθέσεις που τότε είχαμε δεχτεί» σημείωσε η κ. Λιάπη.

Το κατάστημα της Πάτρα απαρτίζεται από 17 μηχανικούς - στελέχη της εταιρείας που εξυπηρετούν σε 24ωρη βάση τους πελάτες της εταιρείας. Επίσης η εταιρεία βασίζεται στην συνεχή εκπαίδευση των μηχανικών της με στόχο τις πιστοποιήσεις για την ποιότητα και την ασφάλεια των πληροφοριών. Η εταιρεία κάνει ετήσιο τζίρο 150 εκ. ευρώ και είναι από το 2000 στο χρηματιστήριο. Και όλα αυτά τα χρόνια εκτός από την αύξηση των κερδών κατάφερε να προχωρήσει και σε αύξηση του αριθμού των εργαζομένων που απασχολεί. Το Υποκατάστημα της SPACE HELLAS στην Πάτρα είναι κυρίαρχο στον τομέα της πληροφορικής και της ασφάλειας στην Δυτική Ελλάδα.

«Η Πάτρα έχει και πάντα είχε και ελπίζω να συνεχίσει να έχει παραγωγικές μονάδες και αυτό είναι σημαντικό γιατί είναι και πολυεθνικές, οπότε εξάγουμε και σε άλλες χώρες. Προσπαθούμε και εμείς από την πλευρά μας να ενισχύσουμε την τοπική οικονομία», κατέληξε η κ. Λιάπη.

> Ιωάννης Αλεξάκης, Γενικός Διευθυντής Επιτελικού Σχεδιασμού, Εθνική Αρχή Κυβερνοασφάλειας

«Έτσι θωρακίζουμε την ασφάλεια της χώρας»

Ο Ιωάννης Αλεξάκης, Γενικός Διευθυντής Επιτελικού Σχεδιασμού, Εθνική Αρχή Κυβερνοασφάλειας, τόνισε στην ομιλία του ότι είναι άλλο η κυβερνοασφάλεια σε επίπεδο ενός οργανισμού και άλλο σε επίπεδο χώρας. «Οσο αυξάνεται η χρήση του ίντερνετ άλλο τόσο αυξάνεται και το κυβερνοέγκλημα.

Πλέον σύμφωνα με μετρήσεις μπορούμε να πούμε ότι 9 στους 10 είμαστε έξι ώρες στο διαδίκτυο και κάνοντας χρήση προσωπικών υπολογιστών ή τηλεφώνων. Γι αυτό το κυβερνοέγκλημα αυξάνεται θεαματικά. Για το 2024 το κυβερνοέγκλημα θα φθάσει τα 10 τρις εκατομμύρια δολάρια και αναμένουμε μεταξύ 2025 και 2027 να φθάσει τα 20 τρις εκατομμύρια δολλάρια. Καταλαβαίνουμε ότι το μέγεθος είναι τεράστιο και πιο επικερδές από το εμπόριο ναρκωτικών. Εάν μιλούσαμε για την οικονομία μας χώρας από τους τζίρους του κυβερνοεγκλήματος, η χώρα αυτή θα ήταν η τρίτη παγκοσμίως. Και όλο αυτό το επιχειρηματικό μοντέλο δεν είναι τυχαίο. Είναι κανονικές ομάδες εγκληματιών που παρέχουν τις υπηρεσίες τους έναντι αμοιβής», τόνισε ο κ. Αλεξάκης.

Σε ελληνικό επίπεδο η Εθνική Αρχή Κυβερνοασφάλειας αναβαθμίστηκε με το νόμο 5086/2024 (Α' 23, 14.02.2024) και στόχος ήταν η ενίσχυση δυνατοτήτων της Αρχής σύμφωνα με τις διεθνείς και ευρωπαϊκές καλές πρακτικές.

Είναι αυτοτελές Νομικό Πρόσωπο Δημοσίου Δικαίου και όχι ανεξάρτητη αρχή και είναι υπό την ευθύνη του Υπουργείου Ψηφιακής Διακυβέρνησης. Έχουν επίσης αναβαθμιστεί οι λειτουργίες και οι δυνατότητες της Αρχής καθώς έχει τριπλασιαστεί ο αριθμός του προσωπικού με βάση τις νέες ανάγκες που έχουν προκύψει. Οι αρμοδιότητες της Αρχής είναι Ρυθμιστικές και σε αυτές περιλαμβάνονται η νομοθεσία, οι κανονισμοί καθώς επίσης μέτρα και συστάσεις. Επίσης έχει και εποπτικές αρμοδιότητες καθώς προχωράει σε ελέγχους και επιθεωρήσεις.

Διαθέτει ακόμη και κυρωτικές, με δεδομένο ότι μπορεί να επιβάλλει διοικητικές κυρώσεις αλλά και πρόστιμα.

> Γεώργιος Στεργιόπουλος, Επίκουρος Καθηγητής, Πανεπιστήμιο Αιγαίου

«Τα νέα δεδομένα της οδηγίας NIS2»

Ο Γεώργιος Στεργιόπουλος, Επίκουρος Καθηγητής, Πανεπιστήμιο Αιγαίου αναφέρθηκε στην οδηγία NIS2. Η οδηγία αυτή έρχεται να αυξήσει τον όγκο και το εύρος των οργανισμών που υπόκεινται σε κανονισμούς κυβερνοασφάλειας. Τέτοιοι οργανισμοί είναι πάρα πολλοί και το εύρος της κάλυψης από εδώ και στο εξής θα είναι μεγάλο σε σχέση με το προηγούμενο διάστημα. Με τα νέα δεδομένα και οι ίδιες οι εταιρείες θα ζητούν βοήθεια και κάλυψη από τους ίδιους τους κρατικούς οργανισμούς. «Είναι πλέον ζήτημα διακυβέρνησης και επικοινωνίας η λήψη των μέτρων» σημείωσε ο κ. Στεργιόπουλος.

Η NIS2 καλύπτει περισσότερους τομείς, συμπεριλαμβανομένης της υγείας, της διαχείρισης αποβλήτων, της δημόσιας διοίκησης και περισσότερων παρόχων ψηφιακών υποδομών.

Η NIS2 χωρίζει τους οργανισμούς σε δύο κατηγορίες στις κρίσιμες και σημαντικές οντότητες αντίστοιχα: Οι κρίσιμες οντότητες είναι εκείνες που παρέχουν υπηρεσίες που σχετίζονται με την διαβίωση του κοινωνικού ιστού (νερό, τηλέφωνο, ενέργεια). Οι βασικές ή σημαντικές οντότητες είναι περιπτώσεις οργανισμών που παρέχουν άλλες υπηρεσίες με λιγότερο κρίσιμο χαρακτήρα που παραμένει όμως σημαντικός. Ανάλογα με την κατάταξή τους οι οργανισμοί καλούνται να λάβουν συγκεκριμένα μέτρα προστασίας. Η συγκεκριμένη κατάταξη θα προχωρήσει σύντομα σε επίπεδο Ε.Ε., μιας και κάθε κράτος θα προσεγγίσει το συγκεκριμένο ζήτημα το επόμενο διάστημα και θα δώσει την σχετική λίστα.

«Η λίστα είναι πολύ μεγάλη και εάν παρέχεται μια υπηρεσία σε αρκετούς πολίτες είναι βέβαιο ότι θα είστε μέσα» επεσήμανε ο κ. Στεργιόπουλος.

NIS2: Η οδηγία που αλλάζει τα

Στο δεύτερο μέρος της ημερίδας έγινε παρουσίαση των τεχνολογικών εφαρμογών της κυβερνοασφάλειας και ποιες λύσεις και ευκαιρίες δίδονται σε αυτόν τον τομέα. Το προεδρείο της ημερίδας αποτελούσαν ο Πρόεδρος του Δικηγορικού Συλλόγου Πατρών **Αθανάσιος Ζούπας**, καθώς η κυβερνοασφάλεια έχει και νομικές επεκτάσεις καθώς επίσης και ο εκδότης του «Σ.Ε.» Παναγιώτης Γιαλένιος.

Όπως τόνισε ο κ. Ζούπας στον χαιρετισμό του «Η τεχνολογία και τα νομοθετικά πλαίσια έπονται στον τομέα αυτό, μετά την εμφάνιση του διαδικτύου. Μόλις το 2018 άρχισαν τα πρώτα νομοθετικά πλαίσια να εμφανίζονται και αντιλαμβάνεστε ότι πλέον είναι μεγάλο πρόβλημα το να νομοθετείς νωρίς, διότι δεν καλύπτεις όλες τις περιπτώσεις και δεν ξέρεις και τις περιπτώσεις που πρέπει να καλύψεις. Από την άλλη όταν νομοθετείς αργά ήδη κάποια πράγματα έχουν συμβεί και δεν μπορείς να τα καλύψεις. Έτσι νομοθετείς με γνώμονα κυρίως το μέλλον». Αναφερόμενος στην Εθνική Αρχή Ασφάλειας ο κ. Ζούπας τόνισε ότι πλέον στην χώρα μας έχει δημιουργηθεί ένα ασφαλές πλαίσιο στον τομέα της κυβερνοασφάλειας. Έθεσε όμως το ζήτημα με ποιο τρόπο οι επιχειρήσεις μπορούν πλέον να προστατευθούν. Και αυτό γιατί σήμερα ορισμένες μόνο επιχειρήσεις έχουν τα κατάλληλα στελέχη τα οποία είναι ψηφιακά ενημερωμένα για τον τομέα της κυβερνοασφάλειας. Ωστόσο σημείωσε ότι «τι γίνεται άραγε με τον απλό πολίτη ο οποίος μετά την πανδημία υποχρεώθηκε να κάνει όλες τις συναλλαγές του ηλεκτρονικά, υποχρεώνεται να

πληρώσει ηλεκτρονικά τον ΕΦΚΑ και να κάνει επίσης ηλεκτρονικά την τραπεζική του συναλλαγή; Αυτό που είναι ψηφιακά αναλφάβητος και αδαής και πέφτει εύκολα θύμα απάτης, πώς άραγε μπορεί να προστατευτεί στον τομέα της κυβερνοασφάλειας;». Και κατέληξε σημειώνοντας ότι πλέον είναι πολύ δύσκολο να ληφθούν ουσιαστικά μέτρα για τον απλό πολίτη αφού είνα χιλιάδες οι χρήστες του διαδικτύου.

> Νάντια Λιάπη, Group CIO, Group Director GRC Services, της εταιρείας Space Hellas

«Θα λογοδοτούν οι διοικήσεις στις κυβερνοεπιθέσεις!»

Η Νάντια Λιάπη, Group CIO, Group Director GRC Services, της εταιρείας Space Hellas αναφέρθηκε στην οδηγία NIS2, φέρνοντας αρχικά ένα παράδειγμα από την ίδια της την κόρη που όταν ήταν τριών χρονών είχε πάει σε ένα παιδικό πάρτι: « Η κόρη μου ήταν τριών χρονών και έχουμε πάει μαζί σε ένα παιδικό πάρτι. Ξαφνικά τη βλέπω ανάστατη να τρέχει προς τα εμένα και αρχίζει να μου τραβάει την μπλούζα και να μου λέει «μαμά, μαμά, μαμά» και της απαντάω «τι έγινε;». Μου λέει «η μαμά της Μαρίας δεν έχει κωδικό στο κινητό της!»». Και συμπλήρωσε ότι η κόρη της έμεινε άφωνη που κάποιος δεν διέθετε κωδικό κλειδώματος για το κινητό του. Κατά την κ. Λιάπη «αυτό είναι κουλτούρα και αυτό σημαίνει εγρήγορση».

Εξηγώντας ακολούθως για το τι σημαίνει η οδηγία NIS2 τόνισε ότι η οδηγία Network and Information Systems Directive 2 της Ευρωπαϊκής Ένωσης στοχεύει στη βελτίωση της ασφάλειας των δικτύων και των πληροφοριακών συστημάτων εντός της ΕΕ.

Στόχοι είναι η ενίσχυση της κυβερνοασφάλειας, δηλαδή η βελτίωση της προστασίας από ψηφιακές απειλές. Επίσης η ανθεκτικότητα και συγκεκριμένα η διασφάλιση της συνεχούς λειτουργίας των κρίσιμων υποδομών και η συνεργασία, δηλαδή η προώθηση της διεθνούς συνεργασίας και του συντονισμού μεταξύ των κρατών-μελών.

Η ημερομηνία συμμόρφωσης παραμένει η 18η Οκτωβρίου 2024, ημέρα που οι επιχειρήσεις θα πρέπει να λάβουν τα απαραίτητα μέτρα για την κυβερνοασφάλεια. Και όσοι αντιπροσωπεύουν οργανισμούς και επιχειρήσεις πρέπει να δείξουν ότι λαμβάνουν μέριμνα.

«Θα πρέπει να αναγνωρίσουμε που βρισκόμαστε σε σχέση με τις απαιτήσεις και να δούμε που βρίσκονται επίσης τα βήματά μας» τόνισε η κ. Λιάπη.

Και σημείωσε ότι οι ευθύνες θα είναι πλέον και ποινικές και δεν θα περιορίζονται στην επιβολή προστίμου.

«Είναι ευθύνες στους νόμιμους εκπροσώπους και μπορεί να φθάσουν μέχρι και αναστολή στην εκτέλεση των καθηκόντων τους για ένα μεγάλο χρονικό διάστημα» εξήγησε η κ. Λιάπη. Και έφερε το παράδειγμα ενός διοικητή νοσοκομείου που κινδυνεύει με παύση, εφόσον το ίδρυμα προσβληθεί από κακόβουλο λογισμικό ή δεχτεί κυβερνοεπίθεση και αποδειχτεί ότι δεν ελήφθησαν τα κατάλληλα μέτρα. Μάλιστα η ίδια επεσήμανε ότι στην Θεσσαλονίκη είχε μεταβεί ένα γνωστό δημόσιο πρόσωπο για να εγχειριστεί για καρκίνο με σκοπό να μην την αναγνωρίσουν. Ωστόσο οι ιατρικές της εξετάσεις, συμπεριλαμβανομένης και της μαστογραφίας της, ήταν στοιβαγμένες στο προαύλιο του νοσοκομείου. Και το όνομα της συγκεκριμένης ασθενή ήταν πολύ εύκολο να εντοπιστεί.

Η κ. Λιάπη ξεκαθάρισε ότι η εφαρμογή της οδηγίας είναι αναγκαία διότι η αξιοπιστία και η ασφάλεια των συστημάτων είναι καθοριστικές για τις οικονομικές και κοινωνικές δραστηριότητες, καθώς και για τη λειτουργία της εσωτερικής αγοράς.

Επίσης η συχνότητα, η έκταση και οι επιπτώσεις των περιστατικών ασφάλειας έχουν αυξηθεί κατακόρυφα και αποτελούν σοβαρό κίνδυνο για την εμπιστοσύνη των πολιτών και την οικονομία της Ε.Ε.

Πάντως οι διαφορές στα κράτη μέλη ως προς το επίπεδο ετοιμότητας οδηγούν σε άνιση προστασία των καταναλωτών και των επιχειρήσεων.

Με τη νέα οδηγία επιτυγχάνεται κάλυψη μεγαλύτερου ποσοστού τομέων της κοινωνίας και της οικονομίας μέσω αναθεώρησης της κρισιμότητας υποδομών και προσθήκης νέων στις ήδη υπάρχουσες.

Υπάρχει αποτελεσματικότερη ευθυγράμμιση των απαιτήσεων ασφάλειας και ενίσχυση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού για βασικές τεχνολογίες πληροφοριών και επικοινωνιών.

Δίνεται η δυνατότητα για συνεργασία και ανταλλαγή πληροφοριών μεταξύ κρατών μελών αλλά και για περαιτέρω λειτουργική συνεργασία σε βασικά ζητήματα όπως το crisis management. Σημαντικός παράγοντας επίσης με τη νέα οδηγία είναι η εναρμόνιση του καθεστώτος κυρώσεων σε όλα τα κράτη μέλη.

«Ο Δήμος Αντλάντας στις ΗΠΑ αρνήθηκε να δώσει ένα σημαντικό ποσό για την κυβερνοασφάλειά του. Τελικά για να ανακάμψει χρειάστηκε να δώσει 15 εκατομμύρια ευρώ, πολύ περισσότερα από όσα θα δαπανούσε αρχικά και ήταν λιγότερα του εκατομμυρίου» επεσήμανε η κ. Λιάπη. Η ίδια εντοπίζει τον μεγαλύτερο κίνδυνο στη Δημόσια Διοίκηση καθώς θα πρέπει να γίνει ένας έλεγχος των κινδύνων. Εξήγησε ακόμη ότι κάποτε η κουλτούρα των επιχειρήσεων ήταν να μην δεχτούνε ποτέ εισβολή στο εσωτερικό του, τώρα αυτό μοιάζει με άπιαστο όνειρο και πλέον προετοιμάζονται για το ενδεχόμενο εισβολής.

«Αυτό τεχνικά σημαίνει ότι διαχωρίζω ώστε να δεχτώ μια επίθεση σε ένα μικρότερο μέρος και να μην απλωθεί παντού και να έχω συνεργασίες που θα κάνουν λειτουργικό το σύστημα. Τότε κάνεις πραγματική άμυνα», ανέφερε η κ. Λιάπη. Ζητούμενο σε αυτές τις περιπτώσεις είναι ποιος θα λάβει τις αποφάσεις που απαιτούνται και ποιος θα μιλήσει στους εργαζόμενους για όσα συνέβησαν. Το πιο σημαντικό είναι το crisis management που θα καθορίσει και στην πορεία την αντιμετώπιση του κινδύνου.

Κυρώσεις μη συμμόρφωσης

Ανάλογα με τον διαχωρισμό των επιχειρήσεων και των οργανισμών σε βασικές οντότητες και σημαντικές οντότητες τα πρόστιμα πλέον θα είναι ιδιαίτερα υψηλά. Όσοι κατατάσσονται στις βασικές οντότητες κινδυνεύουν σε περίπτωση μη συμμόρφωσης με διοικητικά πρόστιμα ύψους κατ' ανώτατο όριο 10.000.000 ευρώ ή 2 % του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών. Όποιο από τα δύο είναι μεγαλύτερο, αυτό τελικά θα επιβληθεί. Στις σημαντικές οντότητες τα διοικητικά πρόστιμα είναι ύψους μέχρι 7.000.000 ευρώ ή 1,4 % του κατά το προηγούμενο οικονομικό έτος συνολικού παγκόσμιου ετήσιου κύκλου εργασιών. Όποιο από τα δύο είναι μεγαλύτερο, αυτό τελικά θα επιβληθεί.

Προσωρινή απαγόρευση της άσκησης διευθυντικών καθηκόντων από οποιοδήποτε φυσικό πρόσωπο ασκεί διευθυντικά καθήκοντα σε επίπεδο διευθύνοντος συμβούλου ή νόμιμου εκπροσώπου είναι κάτι υπό διαμόρφωση στον νέο νόμο.

δεδομένα στις 18 Οκτωβρίου

> Σταμάτης Τσολακίδης, Υπεύθυνος Πωλήσεων και Υποδομών για Ελλάδα, Κύπρο και Μάλτα της Dell Technologies

«Η τεχνολογία που σώζει αρχεία χιλιάδων επιχειρήσεων»

Ο Σταμάτης Τσολακίδης, Υπεύθυνος Πωλήσεων και Υποδομών για Ελλάδα, Κύπρο και Μάλτα της Dell Technologies αναφέρθηκε σε μια νέα τεχνολογία που μπορεί να προστατεύσει οργανισμούς και επιχειρήσεις και Δημόσιο Τομέα και να τους βοηθήσει να επιστρέψουν σε ομαλή λειτουργία μετά από κυβερνοεπίθεση.

Σημαντικό για μια επιχείρηση είναι να διαθέτει κρυφά αρχεία που να μην είναι φανερά στους επιτιθέμενους εισβολείς. Το 85% των εταιρειών θα πρέπει να πληρώσουν χρήματα για να προστατευθούν από μια κυβερνοεπίθεση.

«Ακούμε συνέχεια την ρήση να μην εμπιστευόμαστε τίποτα στην υποδομή μας πια και έτσι πρέπει να το αντιμετωπίζουμε. Δεν εμπιστευόμαστε τίποτα: από το laptop μέχρι το data center και οτιδήποτε άλλο είναι αυτή η υποδομή μας. Θέλουμε να φτιάξουμε ένα οικοσύστημα στο οποίο ακόμα και αν κάποιος μπει μέσα σε αυτό να μην έχει δυνατότητα να εισχωρήσει περαιτέρω στα δεδομένα μας».

Στόχος είναι να περισωθούν τα κρίσιμα δεδομένα, δηλαδή αυτά που είναι αναγκαία για την λειτουργία μιας εταιρείας.

«Θέλουμε λοιπόν να έχουμε ένα τρόπο να γυρίσουμε γρήγορα πίσω είτε μιλάμε για ημέρες είτε μιλάμε για μήνες. Το πόσο ώριμο είναι το σενάριο που έχουμε φτιάξει, θα μας δώσει αντίστοιχα και τον χρόνο που χρειαζόμαστε για να γυρίσουμε σε μια καλή κατάσταση, δηλαδή σε αυτήν που ήμασταν πριν. Αυτό μπορεί να γίνει σε ημέρες ή και σε ώρες και αυτό εξαρτάται από την φύση και των όγκο των δεδομένων που πρέπει να ανακτηθούν» επεσήμανε ο κ. Τσολακίδης.

Βασικός πυλώνας επιβίωσης σε περίπτωση κυβερνοεπίθεσης είναι τα δεδομένα να μην μπορούν να αλλάξουν από τον εισβολέα. Αυτό θα γίνει εφόσον τα δεδομένα είναι απομονωμένα.

Η DELL έχει μεγάλη εμπειρία καθώς προφυλάσσει 29 Εξαμπάιτ (EB) στο cloud και το νούμερο είναι ασύλληπτα μεγάλο.

Η λύση που προτείνει η DELL βασίζεται σε ένα δομικό στοιχείο καθώς πρόκειται για μια εφαρμογή η οποία έχει την δυνατότητα να κλειδώνει τα δεδομένα του χρήστη.

«Είναι τόσο ισχυρό που θα πρέπει να πάρετε τηλέφωνο τον δικηγόρο σας και να επικοινωνήσετε με την DELL για να ξεκλειδώσουν», ανέφερε ο κ. Τσολακίδης.

Πρακτικά τα δεδομένα κλειδώνουν για το διάστημα που ο χρήστης επιλέγει και είναι αδύνατον να έχει πρόσβαση σε αυτά ο οιοσδήποτε.

«Αυτό το δομικό στοιχείο ονομάζεται Data Domain και είναι ένας χώρος αποθήκευσης και έχει και ένα χαρακτηριστικό που μας προσφέρει το κλείδωμα των αρχείων» σημείωσε ο κ. Τσολακίδης.

Η DELL ακολουθεί την λογική της δημιουργίας μιας υποδομής που θα είναι ενωμένη με την πρωταρχική υποδομή με έναν τρόπο κατά τον οποίο τα νέα δεδομένα θα μεταφέρονται και θα αποθηκεύονται σε ασφαλές περιβάλλον.

Μόλις τελειώσει ο συγχρονισμός των δύο υποδομών, απομονώνονται και έτσι δεν μπορεί να υπάρχει πρόσβαση στα δεδομένα αυτά σε περίπτωση κυβερνοεισβολής. Αυτή η δυνατότητα απομόνωσης δίνει την δυνατότητα να μην υπάρχει πρόσβαση δεδομενων και δεν υπάρχει και πρόσβαση στην διαχείριση.

Έτσι δεν μπορεί να γίνει καμία αλλαγή από το παραγωγικό περιβάλλον. Ακολούθως η DELL παρέχει την δυνατότητα σύμπτυξης των δεδομένων αυτών και μάλιστα μπορεί να είναι αποθηκευμένα ακόμη και σε ένα server ώστε να μην χρειάζονται τεράστιοι χώροι αποθήκευσης.

> Σωκράτης Κελέσογλου, Senior Cybersecurity Presales Consultant, Space Hellas

«Είναι σωτήριο το μοντέλο «μηδενικής εμπιστοσύνης»»

Ο Σωκράτης Κελέσογλου, Senior Cybersecurity Presales Consultant, Space Hellas, αναφέρθηκε στην πρακτική πλευρά της οδηγίας NIS2, που χωρίζεται σε τρεις πυλώνες: ο πρώτος αφορά την υποδομή και τις εφαρμογές, ο δεύτερος στην στρατηγική της κυβερνοασφάλειας και ο τρίτος αφορά στην διαχείριση και αναφορά περιστατικών και την διαχείριση των κρίσεων.

Από τα μέτρα της νέας οδηγίας το πιο σημαντικό είναι η ανάλυση ρίσκου που θα πρέπει να κάνουν οι επιχειρήσεις, επίσης η επιχειρησιακή συνέχεια και ένα σημαντικό είναι η διαρκής εκπαίδευση του προσωπικού, καθώς είναι καθοριστικό σε περίπτωση κυβερνοεπίθεσης.

Σημαντική είναι επίσης και η στάση που τηρούν τα στελέχη μιας εταιρείας η ενός οργανισμού ακολουθώντας την πολιτική την «μηδενικής εμπιστοσύνης».

Όπως σημείωσε ο κ. Κελέσογλου «είναι ένα μοντέλο ασφάλειας σύμφωνα με το οποίο δεν εμπιστευόμαστε κανέναν, ούτε χρήστη ούτε συσκευή, ούτε εφαρμογή».

Αναλύοντας την «προσέγγιση μηδενικής εμπιστοσύνης» περαιτέρω ο κ. Κελέσογλου ανέφερε ότι το συγκεκριμένο μοντέλο περιλαμβάνει την επαλήθευση της ταυτότητας και της πρόσβασης συνεχώς και όχι μόνο μια φορά. Προϋποθέτει την ελαχιστοποίηση των δικαιωμάτων του κάθε χρήστη, δηλαδή ο κάθε χρήστης πρέπει να έχει τόσα δικαιώματα όσα χρειάζεται για να κάνει την δουλειά του και την συνεχή παρακολούθηση. Επιπρόσθετα απαιτείται η αυτοματοποίηση του δικτύου και των εφαρμογών και παραμετροποίηση αλλά και η πρόσβαση από οποιοδήποτε σημείο είτε εκτός είτε εντός εταιρείας. Βέβαια η συγκεκριμένη επιλογή έχει και κάποια μειονεκτήματα αλλά και ένα επιπλέον κόστος, αλλά και μια επιβάρυνση στις διαδικασίες. Ακολούθως έφερε παραδείγματα των περιβαλλόντων εταιρειών που έχουν υποτιμήσει τον κίνδυνο των επιθέσεων και με ποιο τρόπο καταβάλλεται προσπάθεια αντιμετώπισης μιας κυβερνοπίθεσης.

> Θεοτόκης Μιχαλάκης, Hybrid IT Solution Manager, της Space Hellas

«Είμαστε συνυφασμένοι με την υπόδειξη λύσεων »

Ο Θεοτόκης Μιχαλάκης, Hybrid IT Solution Manager, της Space Hellas, τόνισε ότι μετά από μια κυβερνοπίθεση, το σημαντικό είναι ποιος θα αναλάβει το βάρος ανάκαμψης από αυτή.

«Σημαντικό είναι να δεις πόσο γρήγορα θα σηκωθείς και ποια είναι η ανθεκτικότητα σου και πόσο γρήγορα θα επανέλθεις», σημείωσε χαρακτηριστικά.

Εξήγησε ακόμη ότι οι οργανισμοί και οι επιχειρήσεις αντιμετωπίζουν πάρα πολύ μεγάλες προκλησεις, σε επίπεδο back up αρχείων μέχρι και τα operating systems και το εύρος όλων αυτών των προκλήσεων είναι ιδιαίτερα διευρυμένο. Οι λύσεις που προτείνονται έχουν γίνει πιο σύνθετες και αυτές οι οργανισμοί και οι επιχειρήσεις δεν μπορούν πάντα να τις ακολουθήσουν λόγω ανθρώπινων πόρων. Και αυτό γιατί εκτός από το κομμάτι της παραγωγής έχουν να αντιμετωπίσουν και το κομμάτι της ασφάλειας. Υποστήριξε επίσης ότι δεν νοείται μια επιχείρηση να έχει τα αρχεία της σε ένα μόνο cloud, αλλά πρέπει να επιλέγει τις λύσεις των πολλαπλών cloud.

«Η Space Hellas επειδή ξεκινήσει να υποστηρίζει από παλιά κρίσιμα δίκτυα οργανισμών, τραπεζών κλπ είναι συνυφασμένη με το θέμα της ασφάλειας και έχει επενδύσει πάρα πολύ σε αυτό. Έχουμε ανθρώπους μηχανικούς οι οποίοι εκπαιδεύονται καθημερινά με τις τελευταίες εξελίξεις για όλα τα κρίσιμα θέματα που αντιμετωπίζει ένας οργανισμό σήμερα ταυτόχρονα φτιάχνει και υποδεικνύει λύσεις οι οποίες συνδέουν τα καλύτερα κομμάτια από τους καλύτερους» ανέφερε ο κ. Μιχαλάκης. Μίλησε επίσης για την άριστη συνεργασία με την DELL η οποία με τα συστήματα της μπορεί να βοηθήσει σημαντικά στο κομμάτι αυτό και οι λύσεις που προτείνονται καλύπτουν όλο το φάσμα του προφίλ των πελατών.

Τείχος προστασίας φορέων

> Αντιγόνη Δόβα, Field Product Manager, Dell Client Solutions

Η DELL εφαρμόζει αξιόπιστα συστήματα προστασίας

Η Αντιγόνη Δόβα, Field Product Manager, Dell Client solutions, στην τοποθέτησή της έκανε μια παρουσίαση των προϊόντων της εταιρείας αναφέροντας ότι η DELL έχει προϊόντα για όλα τα βαλάντια. Από τους κλασικούς «πύργους» μέχρι τους φορητούς ηλεκτρονικούς υπολογιστές, η εταιρεία έχει μια γκάμα προϊόντων που θα ικανοποιήσει τις ανάγκες όλων των πελατών. Η σειρά precision 9 απευθύνεται σε μηχανικούς και χρήστες που διαχειρίζονται βαρύ φόρτο και γενικότερα διαχειρίζονται πολύ βαριά apps, ενώ υπάρχουν και ειδικές σειρές για βιομηχανίες που απαιτούν πιστότητα, καθώς τα μηχανήματα εκτίθενται σε ακραίες καιρικές συνθήκες οπότε είναι δοκιμασμένη η αντοχή σε πτώση σκόνη και νερό. Όλα αυτά τα μηχανήματα διατίθενται με τα ανάλογα περιφερειακά συστήματα όπου η DELL είναι πρωτοπόρος.

Εξήγησε επίσης ότι το κόστος λοιπόν του εγκλήματος στον κυβερνοχώρο ξεπερνά τα 15 τρισεκατομμύρια δολάρια παγκοσμίως και διαφαίνεται ότι το κόστος αυτό αυξάνεται με ραγδαίο ρυθμό.

«Θα φτάσουμε κιόλας να πούμε σχεδόν ότι θα τριπλασιαστεί το 2028, οπότε για αυτό το λόγο καταλαβαίνουμε ότι οι κυβερνοεπιθέσεις πλέον είναι αναπόφευκτες για όλους μας. Τρεις τεράστιες κυβερνοεπιθέσεις καταγράφηκαν το 2023. Η κλοπή αρχείων του Υπουργείο Εξωτερικών των ΗΠΑ που έγινε με παραβίαση του Microsoft Exchange και κλοπή δεκάδων χιλιάδων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Επίσης η κλοπή της εταιρείας Dark Beam data protection lapse όπου εκλάπησαν 3,8 δισεκατομμύρια αρχεία και είναι μία από τις μεγαλύτερες παραβιάσεις δεδομένων στην ιστορία. Τα αρχεία περιελάμβαναν μηνύματα ηλεκτρονικού ταχυδρομείου και κωδικούς πρόσβασης χρηστών. Τέλος, η επίθεση ransomware της Royal Mail.

Η επίθεση επηρέασε 11.500 υποκαταστήματα ταχυδρομείων, πράγμα που σημαίνει ότι δεν ήταν σε θέση να χειριστούν διεθνή δέματα. Μάλιστα εδώ οι δράστες ζήτησαν και λύτρα 80 εκατομμυρίων ευρώ» ανέφερε η κ. Δόβα.

Ακολούθως εξήγησε ότι η εταιρεία χρησιμοποιεί τρία επίπεδα ασφαλείας για την προστασία από τέτοιου είδους επιθέσεις. Το πρώτο επίπεδο είναι ότι το hardware και το software πρέπει να λειτουργούν ενιαία και αυτός είναι και ο λόγος που η εταιρεία έχει επιλέξει κορυφαίους συνεργάτες ασφάλειας που παρέχουνε τηλεμετρία σε επίπεδο συσκευής ώστε να προβλέπονται μελλοντικές απειλές.

Η εταιρεία έχει εφαρμόσει την λειτουργία Dell SafeGuard and Response όπου με την χρήση πλατφορμών cloudpass solution προφέρουν προσφέρουν απομακρυσμένες λύσεις. Στόχος η πρόληψη, ο εντοπισμός και αντιμετώπιση απειλών οπουδήποτε και αν εμφανίζονται.

Σημαντική είναι επίσης και η χρήση του Dell Safe Bios το οποίο είναι ένα σύστημα που περιλαμβάνει επαλήθευση BIOS, καταγραφή Image όπως και συμβάντα και δείκτες επίθεσης στο BIOS.

Η επαλήθευση BIOS παρέχει στους πελάτες επιβεβαίωση ότι οι συσκευές είναι ασφαλείς κάτω από το λειτουργικό σύστημα, ένα μέρος όπου λείπει η ορατότητα του IT. Επίσης με το Dell SafeID, όλη η επεξεργασία και αποθήκευση κρίσιμων δεδομένων πραγματοποιείται στο τσιπ. Τέλος με το Dell SafeSupply Chain ο χρήστης βεβαιώνει ότι οι υπολογιστές είναι ασφαλείς από το πρώτο boot – secured component

Επιπρόσθετα η εταιρεία εφαρμόζει τις εξής καινοτομίες στους υπολογιστές. Με το Express Charge παρατείνει τη διάρκεια ζωής της μπαταρίας όταν τη χρειάζεται ο χρήστης. Με το Intelligent Privacy διατηρεί την οθόνη ασφαλή, όταν ανιχνεύεται θεατής και μειώνει τη φωτεινότητα του υπολογιστή όταν απομακρύνει ο χρήστης το βλέμμα του. Με το xpress Response εξασφαλίζει έξυπνα άψογη απόδοση εφαρμογών, όλα με βάση τη χρήση και το ιστορικό του χρήστη και με τα Analytics (Precision Only) δημιουργεί reports και αναλύει το σύστημα για εξατομικευμένες πληροφορίες.

> Δρ. Θεόδωρος Κομνηνός, Διευθυντής Πληροφοριακών Συστημάτων, Εφαρμογών & Κυβερνοασφάλειας, ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ

Το σύστημα προστασίας του ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ

Ο Δρ. Θεόδωρος Κομνηνός, Διευθυντής Πληροφοριακών Συστημάτων, Εφαρμογών και Κυβερνοασφάλειας, ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ αναφέρθηκε στην κυβερνοασφάλεια σε δημόσια πληροφοριακά συστήματα.

Εισαγωγικά επεσήμανε ότι λόγω της ταχύτατης ανάπτυξης της ψηφιακής υποδομής διευρύνονται οι επιθέσεις. Έτσι έχουμε επιθέσεις στα δεδομένα (cloud, on-premise), επιθέσεις στις υπηρεσίες που προσφέρει ένας φορέας, αλλά και στην φήμη του. Οι τύποι των απειλών ποικίλλουν: Μπορεί να είναι ένα κακόβουλο λογισμικό, να γίνεται με την μέθοδο phishing, ransomware, επιθέσεις με DDoS, εσωτερικές απειλές. Οι κλάδοι που πλήττονται περισσότερο από αυτές τις επιθέσεις είναι ο χρηματοοικονομικός τομέας, η υγειονομική περίθαλψη και οι κυβερνητικοί οργανισμοί. Τέλος έχει υπολογιστεί ότι τα παγκόσμια κόστη του κυβερνοεγκλήματος προβλέπεται να φτάσουν τα 10,5 τρισεκατομμύρια δολάρια ετησίως έως το 2025.

Μπορεί επίσης και η Τεχνητή Νοημοσύνη (ΤΝ) να συμβάλει σημαντικά στην Κυβερνοασφάλεια με τους εξής τρόπους:

- Αναλυτική πρόβλεψη και ανίχνευση απειλών σε πραγματικό χρόνο.
- Λειτουργία συστημάτων βασισμένα σε AI για αυτόνομη ανίχνευση και ανταπόκριση σε απειλές.
- Αναγνώριση επιθέσεων υποβοηθούμενα από ΤΝ.

Μπορεί να ακολουθηθεί η λογική του blockchain για να αντιμετωπιστεί μια κυβερνοεπίθεση, δηλαδή να δημιουργηθεί μια αποκεντρωμένη ασφάλεια για την ακεραιότητα και πιστοποίηση δεδομένων.

Σημαντική επίσης είναι η λογική που ακολουθείται μέσω της αρχιτεκτονικής του «Zero Trust». Αυτή η πολιτική βασίζεται στο να μην υπάρχει καμία εμπιστοσύνη στους χρήστες και να ζητείται η συνεχής επαλήθευση της ταυτότητας τους.

Η νέα κανονιστική NIS2 ζητά να υπάρχουν πολιτικές και διαδικασίες για:

- Διαχείριση κινδύνων
- Αντιμετώπιση περιστατικών κυβερνοασφάλειας
- Αναφορές περιστατικών
- Επιχειρησιακή συνέχεια
- Ασφάλεια εφοδιαστικής αλυσίδας

Ωστόσο για την Κυβερνοασφάλεια σε πληροφοριακά συστήματα και εφαρμογές του δημοσίου πρέπει να λάβουμε υπόψη μας τα εξής.

Μέχρι σήμερα η υλοποίηση των υπηρεσιών γίνεται σε ένα στενό χρονικό περιθώριο, ακολουθώντας την λογική ότι μια εφαρμογή «πρέπει να βγει η εφαρμογή στον «αέρα» αύριο». Σε περίπτωση κυβερνοεπίθεσης διαφαίνεται ότι υπάρχει εμπλοκή πολλών φορέων και στην πράξη έχει διαφανεί η μεταφορά ευθυνών. Επίσης πρέπει να λάβουμε υπόψη μας και την έλλειψη προσωπικού και κυρίως την δυσκολία κατανόησης της κατάστασης σε περίπτωση μιας επίθεσης. Μεγάλο ζητούμενο είναι η έλλειψη εκπαίδευσης, καθώς δεν υπάρχουν κονδύλια, χρόνος και διαθεσιμότητα προσωπικού για τέτοιες καταστάσεις. Τέλος μεγάλη είναι η έλλειψη και ζήτηση έμπειρων στελεχών για την κυβερνοασφάλεια αλλά και η τήρηση πολιτικών και διαδικασιών ασφάλειας, αφού όσο αυξάνει η ασφάλεια τόσο μειώνεται η ευκολία.

Θα πρέπει να λάβει κανείς υπόψη του και την έλλειψη κονδυλίων για την ασφάλεια με προαπαιτούμενο την αντικατάσταση του εξοπλισμού αλλά και τις ελλιπείς προδιαγραφές σε θέματα ασφάλειας και αδυναμία παρακολούθησης των παραδοτέων σε αυτούς τους τομείς. Τέλος δεν υπάρχει εμπειρία σε θέματα ασφάλειας σε υπηρεσίες εξυπηρετητές στο cloud.

Η Κυβερνοασφάλεια στο ΙΤΥΕ

Το ΙΤΥΕ πάντως από την πλευρά του έχει λάβει όλα τα απαραίτητα μέτρα προστασίας σε περίπτωση κυβερνοεπίθεσης. Διαθέτει εξειδικευμένο προσωπικό στην κυβερνοασφάλεια, εφαρμόζει πρακτικές αντιμετώπισης κυρίως με ορισμό κανόνων για τους χρήστες μέσω updates, backup, ασφαλή διακίνηση πληροφοριών. Βελτιώνει επίσης την ασφάλεια του χρήστη και του δικτύου αλλά και των συστημάτων πρόσβασης.

Το προσωπικό επίσης εκπαιδεύεται με εικονικές επιθέσεις και ενημερωτικά άρθρα, υπάρχει συμμετοχή σε σεμινάρια αλλά και σε ασκήσεις (Πανόπτης, Enisa).

Επίσης συμμετέχει στα εξής έργα:

- EL-SOC: Δημιουργία Ελληνικού Κεντρικού SOC στην ΕΑΚ
- AKADIMOS: Δημιουργία Ευρωπαϊκής Ακαδημίας Δεξιοτήτων Κυβερνοασφάλειας.
- CADMUS: Εκπαιδευτικά προγράμματα Κυβερνοασφάλειας, πλατφόρμες εκπαίδευσης εργαστήρια, σενάρια, ασκήσεις.

Ο κ. Κομνηνός συμπερασματικά τόνισε ότι οι τεχνολογίες κυβερνοασφάλειας εξελίσσονται ραγδαία και σημαντικός ο ρόλος της τεχνητής νοημοσύνης στις επιθέσεις και στην άμυνα.

Είναι σημαντική η εκπαίδευση του προσωπικού, αφού το σε περίπτωση επιθέσεων καθοριστικό ρόλο παίζει σε ποσοστό 82% το ανθρώπινο λάθος και σε 51% το phishing και γενικότερα η έλλειψη εξειδίκευσης. Κατά τον κ. Κομνηνό, η συνεργασία μεταξύ βιομηχανιών, κυβερνήσεων και ακαδημαϊκών ιδρυμάτων είναι απαραίτητη για την αντιμετώπιση των αυξανόμενων απειλών.

και εταιρειών για εισβολείς

> Δημήτρης Ανεστόπουλος, Διεύθυνση Ψηφιακής Διακυβέρνησης της ΠΔΕ

«Έτσι θωρακίζεται η Περιφέρεια Δυτικής Ελλάδος»

Ο Δημήτρης Ανεστόπουλος Μηχανικός Ηλεκτρονικών Υπολογιστών και Πληροφορικής (M.Eng., MBA, M.Ed.) από την Διεύθυνση Ψηφιακής Διακυβέρνησης της Περιφέρειας Δυτικής Ελλάδας τόνισε με ποιο τρόπο ο φορέας αντιμετωπίζει την πιθανότητα κυβερνοπίθεσης. Για τον συγκεκριμένο φορέα το ζήτημα είναι κρίσιμο λόγω του μεγάλου αριθμού υπηρεσιών και προσωπικού. Η ΠΔΕ λειτουργεί σε 50 κτήρια και προσφέρει 800 μόνιμες θέσεις εργασίας αλλά και 200 "περιστασιακές" θέσεις εργασίας. Οι προσωπικοί υπολογιστές των εργαζομένων φθάνουν τους 1.100. Η ΠΔΕ επίσης διαθέτει δεκάδες φυσικούς εξυπηρετητές στις εγκαταστάσεις της και πολλές δεκάδες εικονικοποιημένους εξυπηρετητές. Διαθέτει πληροφοριακά συστήματα στο Κυβερνητικό Νέφος (Azure) και έχει πρόσβαση σε δεδομένα πολλών δημόσιων Φορέων.

Ως προς τον τρόπο θωράκισης της Περιφέρειας Δυτικής Ελλάδος σε κυβερνοεπιθέσεις έχουν έχουν ακολουθηθεί τα εξής βήματα: Έχει γίνει προμήθεια και εγκατάσταση κεντρικού συστήματος EDR (προστασία των clients), προμήθεια και εγκατάσταση NGFW για interVLAN routing (έλεγχος του εσωτερικού δικτύου) καθώς επίσης και προμήθεια και εγκατάσταση ενεργού δικτυακού εξοπλισμού για την ελεγχόμενη διασύνδεση προσωπικών Η/Υ (desktops, laptops) στο ενσύρματο ενδοδίκτυο των κτηρίων της Περιφέρειας Δυτικής Ελλάδος.

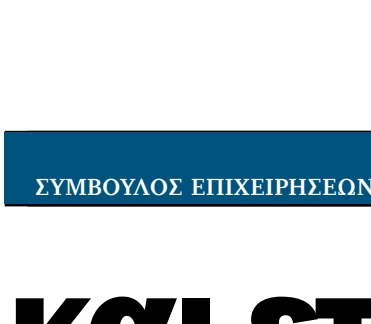
Προμήθεια και εγκατάσταση λογισμικού για την εγγυημένη ταυτοποίηση χρηστών με χρήση 2FA.

Επιπρόσθετα έχουν ληφθεί πρωτοβουλίες για την βελτίωση και παραμετροποίηση του Active Directory, Workstations και των Servers. Υπάρχει παραμετροποίηση των ασύρματων δικτύων αλλά και της υπηρεσίας file sharing με πλήρη καταγραφή των αποθετηρίων δεδομένων των Υπηρεσιών της ΠΔΕ. Επίσης γίνεται ετήσιος επανέλεγχος των επιπέδων κυβερνοσφάλειας.

Τέλος έχει δημιουργηθεί ειδική ομάδα Κυβερνοασφάλειας το προσωπικό της ΠΔΕ έχει επιμορφωθεί στο συγκεκριμένο θέμα. Την προηγούμενη χρονιά, το 2023 έγινε έγχος ασφάλειας από εξωτερικό φορέα , ενώ η ΠΔΕ ακολουθεί συνεργασίες με διάφορους δημόσιους φορείς όπως το ΥΠΕΣ, ΥΨΔ, Εθνικό CERT αλλά και την DPO και νομικούς.

> Δρ.Στέφανος Μίχος Αποκεντρωμένη Διοίκηση Πελ/σου, Δυτ. Ελλάδας & Ιονίου

Η Αποκεντρωμένη Διοίκηση και τα μέτρα αποτροπής



Αντίστοιχα ο Δρ. Στέφανος Μίχος, Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών (Υ.Α.Σ.Π.Ε.), Αποκεντρωμένη Διοίκηση Πελ/σου, Δυτ. Ελλάδας & Ιονίου μίλησε για τον τρόπο ασφάλισης της υπηρεσίας έναντι κυβερνοεπιθέσεων.

Εισαγωγικά ο κ. Μίχος ανέφερε ότι «οι νέες τεχνολογίες, όπως η τεχνητή νοημοσύνη, η δυνατότητα περαιτέρω ανάπτυξης έξυπνων μηχανών, σε συνδυασμό με τεχνολογίες νέφους και τις νέες δυνατότητες δικτύωσης των δικτύων 5ης γενιάς, έχουν τεράστιο εύρος εφαρμογών στους τομείς της υγείας, των μεταφορών, τον κατασκευαστικό τομέα, τον αγροδιατροφικό τομέα, αλλά και άλλους τομείς όπως την εθνική άμυνα. Με το δεδομένο αυτό δεν είναι τυχαίο ότι ήδη γίνεται λόγος για Internet of Everything (IoE), ή αλλιώς για την διαδικτύωση των πάντων».

Πρόσθεσε επίσης ότι όλες οι ανωτέρω ταχύτατες εξελίξεις, σε συνδυασμό με την αυξανόμενη ζήτηση για ψηφιακές εφαρμογές και υπηρεσίες, ενέχουν σημαντικές προκλήσεις. Όσο ταχύτερα εξαπλώνεται ο ψηφιακός κόσμος σε κάθε έκφανση της καθημερινής οικονομικής και κοινωνικής ζωής, τόσο εξαπλώνεται και το πεδίο για κακόβουλες και παράνομες ενέργειες. Όσο οι νέες υπηρεσίες μας επιτρέπουν μεγαλύτερη προσωποποίηση και εστίαση στις δικές μας ανάγκες, τόσο αυξάνονται οι κίνδυνοι για την εκμετάλλευση ή παραβίαση των προσωπικών μας δεδομένων.

Τα μέτρα που λαμβάνονται είναι σε επίπεδο συστήματος είναι η ανάπτυξη πολιτικής για την προστασία από κακόβουλο λογισμικό. Ακολουθείται η υλοποίηση λογισμικού προστασίας από κακόβουλα προγράμματα (anti-malware software) σε κάθε σταθμό εργασίας και server, το οποίο θα λειτουργεί με αυτοματοποιημένο τρόπο μέσω κεντρικής διαχείρισης. Αυτόματη σάρωση (anti-malware scanning) σε φορητά μέσα αποθήκευσης.

Τόνισε ακόμη ότι οι εκδόσεις των web browsers και e-mail clients που είναι εγκατεστημένοι στα συστήματα του Οργανισμού θα πρέπει να είναι οι πλέον πρόσφατες, να ενημερώνονται αυτόματα και να είναι πλήρως υποστηριζόμενες. Απαραίτητα είναι το DNS filtering για την παρεμπόδιση πρόσβασης σε γνωστά κακόβουλα domains και φιλτράρισμα του URL σε επίπεδο δικτύου. Επιβεβλημένη είναι ακόμη η εγκατάσταση συστημάτων ανίχνευσης και πρόληψης εισβολών (host-based intrusion detection / prevention systems) σε κάθε server κρίσιμης σημασίας (web, email, DNS κ.α.).

Ακόμη χρειάζεται η τήρηση και ανάλυση αρχείων καταγραφής συμβάντων. Επίσης πρέπει να γίνεται χρήση κρυπτογραφίας, λήψη αντιγράφων ασφαλείας (backup) και να ακολουθείται μια πολιτική αυθεντικοποίησης χρηστών. Απαιτούνται στην πράξη ισχυροί κωδικοί που θα αλλάζουν κάθε 6 μήνες.

> Δρ. Πέτρος Γανός, Προϊστάμενος Τμήματος Σχεδιασμού και Μελετών Ψηφιακών Συστημάτων Δήμος Πατρέων

«Οι ΟΤΑ και τα συστήματα αναχαίτισης»

Ο Δρ. Πέτρος Γανός, Προϊστάμενος Τμήματος Σχεδιασμού και Μελετών Ψηφιακών Συστημάτων Δήμου Πατρέων, αναφέρθηκε στις μεθόδους εντοπισμού και διαχείρισης των συστημάτων ασφαλείας. Τα βασικά χαρακτηριστικά είναι η αξιολόγηση της τρέχουσας κατάστασης κυβερνοασφάλειας, η διαχείριση πληροφοριών και συμβάντων ασφαλείας και η απόκριση σε συμβάντα. Καθοριστική είναι η προστασία από επιθέσεις phishing, η πληροφόρηση για απειλές και η εκπαίδευση διαχειριστών και χρηστών, όπως επίσης και η ευθυγράμμιση με την Εθνική Στρατηγική Κυβερνοασφάλειας

Υπάρχει μάλιστα ολοκληρωμένη υποδομή προστασίας από κυβερνοεπιθέσεις που εφαρμόζεται από 165 Δήμους σε όλη την χώρα. Αυτή βασίζεται στο εξής:

- Την ολιστική προστασία της υποδομής και των υπαρχόντων πληροφοριακών συστημάτων, ιστοσελίδων και διαδικτυακών εφαρμογών με δημόσια πρόσβαση
- Έγκαιρη ανίχνευση απειλών και επιθέσεων και επιτάχυνση των μηχανισμών αξιολόγησης κινδύνων και αντιμετώπισης των απειλών αυτών
- Διασφάλιση της επιχειρησιακής συνέχειας και ακεραιότητας των διαδικασιών, συστημάτων και πληροφοριών του φορέα
- Ευαισθητοποίηση στελεχών σε θέματα αντίληψης προβλημάτων κυβερνοασφάλειας και αντιμετώπισής τους.
- Καθοριστική είναι και η συμβολή των υποσυστημάτων των πληροφοριακών συστημάτων σε περίπτωση επίθεσης. Στην περίπτωση αυτή κρίνεται αναγκαία η πρακολούθηση, συλλογή και επεξεργασία δεδομένων μεγάλου όγκου, που σχετίζονται με την προστασία των ΠΣ του Δήμου από απειλές και επιθέσεις στον κυβερνοχώρο
- Πρέπει να γίνεται ανίχνευση και ανάλυση συμβάντων ασφάλειας, σχετικών με πιθανές απειλές και κυβερνοεπιθέσεις και αναγνώρισης των αιτιών αυτών
- Να υπάρχει 'εγκαιρης ενημέρωση για εξελισσόμενα σενάρια κυβερνοαπειλών και κυβερνοεπιθέσεων, αποδοτικής διαχείρισης των συμβάντων αυτών και παροχή υποστήριξης για την αντιμετώπισή τους
- Να ακολουθείται η καταγραφή βέλτιστων πρακτικών προστασίας και αποτροπής κυβερνοεπιθέσεων (υπάρχει και η ΕΣΚ)
- Διασύνδεση με το ενοποιημένο σύστημα χρηστών, καθορισμού ρόλων και δικαιωμάτων σε εσωτερικά συστήματα και εφαρμογές του Δήμου
- Υποστήριξη ασφαλούς τηλε-εργασίας (που παρέχεται μέσω VPN δικτύου) και εκπαίδευση σε θέματα κατανόησης κυβερνοαπειλών και αντιμετώπισης αντίστοιχων επιθέσεων.

Forum ΑΝΑΠΤΥΞΗΣ 2024
ΗΜΕΡΙΔΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

- ΔΕΥΤΕΡΑ 23 / 9 / 2024 10:00-14:00
- ΥΒΡΙΔΙΚΗ ΕΚΔΗΛΩΣΗ
- Με φυσική παρουσία: Ξενοδοχείο MY WAY (Όθωνος Αμαλίας 16 Πάτρα)

LIVE στο www.forumanaptixis.gr

ΠΡΟΓΡΑΜΜΑ / ΠΡΟΣΚΛΗΣΗ

9:30-10:00 Προσέλευση-Εγγραφές -Καφές

10:00-12:00 "Νέες οδηγίες και κανονισμοί για την Κυβερνοασφάλεια – Κίνδυνοι και υποχρεώσεις"

Προεδρείο:
Δημήτρης Σερπάνος, *Πρόεδρος ΙΤΥΕ «Διόφαντος»*
Παναγιώτης Γιαλένιος, *εκδότης εφ. «Σύμβουλος Επιχειρήσεων»*

Χαιρετισμοί
- Χρήστος Μπούρας, *Πρύτανης Πανεπιστημίου Πατρών*
- Πλάτων Μαρλαφέκας, *Πρόεδρος Επιμελητηρίου Αχαΐας*
- Κλεομένης Μπάρλος, *Πρόεδρος Συνδέσμου Επιχειρήσεων και Βιομηχανιών Πελοποννήσου και Δυτικής Ελλάδος*
- Νάντια Λιάπη, *Group CIO, Group Director GRC Services, Space Hellas*

Ομιλητές
Δημήτριος Σερπάνος, *Πρόεδρος ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ και Καθηγητής Πανεπιστημίου Πατρών*
Θέμα: Κυβερνοασφάλεια: Κίνδυνοι, Απειλές και Άμυνες
Ιωάννης Αλεξάκης, *Γενικός Διευθυντής Επιτελικού Σχεδιασμού, Εθνική Αρχή Κυβερνοασφάλειας*
Θέμα: Εθνική Αρχή Κυβερνοασφάλειας: Στρατηγική και Στόχοι
Γεώργιος Στεργιόπουλος, *Επίκουρος Καθηγητής, Πανεπιστήμιο Αιγαίου*
Θέμα: Κατακτώντας το NIS2: Οδηγός για την Πλοήγηση στην Οδηγία ΕΕ 2022/2555

Θα ακολουθήσουν ερωτήσεις σε ομιλητές

12:00-14:00 "Ανάπτυξη τεχνολογικών εφαρμογών Κυβερνοασφάλειας - Λύσεις και ευκαιρίες"

Προεδρείο
Αθανάσιος Ζούπας, *Πρόεδρος Δικηγορικού Συλλόγου Πατρών*
Παναγιώτης Γιαλένιος, *εκδότης εφ. «Σύμβουλος Επιχειρήσεων»*

Παρουσιάσεις
- Νάντια Λιάπη, *Group CIO, Group Director GRC Services, Space Hellas*
  Θέμα: «Thank God for NIS II»
- Σταμάτης Τσολακίδης, *Data Center Sales Executive , Greece, Cyprus & Malta, Dell Technologies*
  Θέμα: «Recovering Your Business from a Sophisticated Ransomware or Cyberattack»
- Σωκράτης Κελέσογλου, *Senior Cybersecurity Presales Consultant, Space Hellas*
  Θέμα: «NIS 2 in Practice»
- Αντιγόνη Δόβα, *Field Product Manager, Dell Client solutions*
  Θέμα: «Security on End User devices»
- Δρ. Θεόδωρος Κομνηνός, *Διευθυντής Πληροφοριακών Συστημάτων, Εφαρμογών και Κυβερνοασφάλειας ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ*
  Θέμα: "Κυβερνοασφάλεια σε δημόσια πληροφοριακά συστήματα και εφαρμογές"
- Δημήτρης Ανεστόπουλος, *Προϊστάμενος Διεύθυνσης Ψηφιακής Διακυβέρνησης ΠΔΕ*
  Θέμα: Ζητήματα Κυβερνοασφάλειας στην Περιφέρεια Δυτ.Ελλάδας
- Στέφανος Μίχος, *Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής & Επικοινωνιών (Υ.Α.Σ.Π.Ε.), Αποκεντρωμένη Διοίκηση Πελ/σου, Δυτ. Ελλάδας & Ιονίου*
  Θέμα: «Θωράκιση κρισιμων υποδομών, ασφάλεια και νεες τεχνολογίες»
- Δρ. Πέτρος Γανός, *Προϊσταμένος Τμήματος Σχεδιασμού και Μελετών Ψηφιακών Συστημάτων Δήμος Πατρέων*
  Θέμα: "Κυβερνοασφάλεια στην Τοπική Αυτοδιοίκηση"

ΚΕΝΤΡΙΚΟΙ ΧΟΡΗΓΟΙ

SPACE
DELL Technologies
TITANIUM PARTNER

ΣΥΝΔΙΟΡΓΑΝΩΣΗ

UNIVERSITY OF PATRAS ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ
ΣΥΝΔΕΣΜΟΣ ΕΠΙΧΕΙΡΗΣΕΩΝ και ΒΙΟΜΗΧΑΝΙΩΝ Πελοποννήσου & Δυτικής Ελλάδος
ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΧΑΪΑΣ Από το 1836

ΜΕ ΤΗΝ ΥΠΟΣΤΗΡΙΞΗ

enterprise europe network
EDIH HEALTH
IRI BEYOND

ΧΟΡΗΓΟΙ ΕΠΙΚΟΙΝΩΝΙΑΣ

IONIAN REGIONAL TV
Σύμβουλος Online www.symboulos.gr

ΟΡΓΑΝΩΣΗ

Σύμβουλος επιχειρήσεων

ΠΛΗΡΟΦΟΡΙΕΣ: Μαιζώνος 94 Πάτρα | Τηλ: 2610-620.574 | e-mail:symboulo@otenet.gr | www.forumanaptixis.gr | @diktyoforumanaptixis.gr | κ. Π. Γιαλένιος