ΝΟΕΜΒΡΙΟΣ 2025

ΕΝΗΜΕΡΩΤΙΚΟ ΔΕΛΤΙΟ Ν.2

GO CLOUD GO SECURE

🚀 Καλωσορίστε στο Go Cloud! Go Secure!

Αγαπητέ αναγνώστη,

Χαιρόμαστε πολύ που σε ξαναβλέπουμε! Διαβάζεις το 2ο Ενημερωτικό Δελτίο του έργου μας Go Cloud! Go Secure!

Πολλά έχουν συμβεί από το προηγούμενο Ενημερωτικό Δελτίο! Δοκιμάσαμε και οριστικοποιήσαμε τη CSI Matrix, συναντηθήκαμε από κοντά στη Βουλγαρία, στην υπέροχη πόλη Σόφια και βουτήξαμε βαθιά στην ανάπτυξη του εκπαιδευτικού υλικού του Go Cloud.

Το τεύχος αυτό είναι γεμάτο χρήσιμες πληροφορίες και πόρους, με τη βοήθεια των οποίων μπορείς να ενισχύσεις ακόμη περισσότερο το επίπεδο της κυβερνοασφάλειάς σου.

Σε ευχαριστούμε που είσαι μαζί μας!

Η ομάδα του Go Cloud

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Κύρια Σημεία

Εσωτερικές και εξωτερικές δοκιμές του CSI Matrix

Στο πλαίσιο του WP2–A5 «Δοκιμή, αξιολόγηση και βελτίωση του ψηφιακού CSI Matrix», οι εταίροι πραγματοποίησαν δοκιμές σε πραγματικές συνθήκες για να αξιολογήσουν πόσο χρήσιμο, κατανοητό και φιλικό προς τον χρήστη είναι το Cloud Security Implementation (CSI) Matrix.

Εσωτερική Δοκιμή

Προσωπικό που δεν είχε συμμετάσχει στην ανάπτυξη του Matrix το δοκίμασε και έδωσε αμερόληπτα σχόλια. Επτά άτομα με εμπειρία σε εργαλεία κυβερνοασφάλειας βρήκαν τις ευπάθειες και τις ενέργειες μετριασμού κατάλληλες και εκτίμησαν την πρακτική αξία του εργαλείου. Το Matrix κρίθηκε διαισθητικό, εύκολο στην πλοήγηση και με χρήσιμο χρωματικό σύστημα κινδύνου. Μικρά προβλήματα, όπως εξαγωγή σε PDF ή περιστασιακό “πάγωμα”, δεν επηρέασαν την θετική αξιολόγηση. Όλοι δήλωσαν ότι θα το χρησιμοποιούσαν και θα το σύστηναν.

Εξωτερική Δοκιμή

Κάθε εταίρος ξεπέρασε τον στόχο συμμετεχόντων, συλλέγοντας σχόλια από προσωπικό ΜΜΕ, ειδικούς IT/cloud, εκπαιδευτές VET και άλλους επαγγελματίες. Η ομάδα είχε ισορροπία μεταξύ έμπειρων και νέων χρηστών, παρέχοντας πλήρη εικόνα. Το Matrix κρίθηκε σαφές, χρήσιμο και πρακτικό για εργασία και εκπαίδευση. Το 90% δήλωσε ότι θα το χρησιμοποιούσε επαγγελματικά και όλοι ότι θα το σύστηναν. Το εργαλείο ήταν διαισθητικό, σταθερό και εύκολο στη χρήση, με λίγα μικρά τεχνικά προβλήματα.

ΤΟ MATRIX ΕΙΝΑΙ ΕΤΟΙΜΟ!

Ανακαλύψτε το CSI Matrix και προστατέψτε το cloud περιβάλλον σας!

Με χαρά ανακοινώνουμε ότι το Cloud Security Implementation (CSI) Matrix, το πρώτο αποτέλεσμα του έργου Go Cloud! Go Secure! Erasmus+, είναι πλέον διαθέσιμο στην ιστοσελίδα του έργου.

Κύριοι χρήστες του CSI Matrix είναι οι ΜΜΕ που χρησιμοποιούν ή σκέφτονται να χρησιμοποιήσουν υπηρεσίες cloud, αλλά δεν διαθέτουν δικές τους ομάδες ασφαλείας ή εμπειρογνωμοσύνη σε θέματα cloud security.

Το εργαλείο έχει σχεδιαστεί για να είναι απλό, ευέλικτο και φιλικό προς τις ΜΜΕ, χωρίς υπερβολική τεχνική ορολογία, και στηρίζει οργανισμούς που θέλουν να υιοθετήσουν υπεύθυνα λύσεις cloud διατηρώντας ταυτόχρονα την ασφάλεια.

Οι ΜΜΕ απλώς επιλέγουν το cloud μοντέλο που χρησιμοποιούν, και το Matrix αναδεικνύει, αξιολογεί και προτείνει τρόπους αντιμετώπισης των κινδύνων που σχετίζονται με το συγκεκριμένο μοντέλο.

Το CSI Matrix λειτουργεί σε τέσσερα απλά βήματα:

1. Επιλέξτε τα μοντέλα υπηρεσιών cloud: Αρχικά, ενημερώστε μας για τις υπηρεσίες cloud που χρησιμοποιείτε ήδη ή σκοπεύετε να χρησιμοποιήσετε.
2. Δείτε τους σχετικούς κινδύνους: Με βάση τις επιλογές σας, θα σας παρουσιάσουμε μια λίστα με τις απειλές ασφαλείας που είναι πιο πιθανό να επηρεάσουν την επιχείρησή σας.
3. Μπορείτε να αξιολογήσετε κάθε απειλή με βάση τον κίνδυνο που ενέχει για την εταιρεία σας. Με αυτόν τον τρόπο, μπορείτε να επικεντρωθείτε σε ό,τι έχει πραγματικά σημασία για εσάς.
4. Λάβετε σαφείς συμβουλές: Για κάθε απειλή, παρέχουμε εύκολες συμβουλές και ενέργειες με βάση το γνωστό OWASP Top 10 - έναν αξιόπιστο οδηγό που χρησιμοποιούν ειδικοί σε θέματα ασφάλειας σε όλο τον κόσμο.

Στο τέλος της διαδικασίας, μπορείτε να κατεβάσετε ένα προσωποποιημένο PDF με όλα τα αποτελέσματα και τις προτάσεις. Εκτός από τα Αγγλικά, το εργαλείο είναι διαθέσιμο και σε πέντε ακόμη ευρωπαϊκές γλώσσες.

Διακρατική Συνάντηση #2

16–17 Οκτωβρίου 2025, Σόφια

Το έργο **“Go Cloud! Go Secure!”** πραγματοποίησε πρόσφατα τη **δεύτερη διεθνή συνάντηση στη Σόφια της Βουλγαρίας**, υπό τη φιλοξενία της **Acta Consulting**. Εταίροι από Ουγγαρία, Ιταλία, Αυστρία και Κύπρο συγκεντρώθηκαν για να αξιολογήσουν την πρόοδο και να σχεδιάσουν τα επόμενα βήματα.

Ένα βασικό αποτέλεσμα του έργου, το Cloud Security Implementation (CSI) Matrix, ένα ψηφιακό εργαλείο αυτοαξιολόγησης, δοκιμάστηκε διεξοδικά. Στο πλαίσιο του εξωτερικού πιλοτικού προγράμματος, 38 επαγγελματίες από πέντε χώρες παρείχαν σχόλια, με 100% να το συστήνουν σε άλλους. Το 81,1% χαρακτήρισε τη λογική αξιολόγησης κινδύνου «πολύ χρήσιμη» και οι συμμετέχοντες επιβεβαίωσαν τη σταθερή απόδοση του εργαλείου. Η εσωτερική δοκιμή με επτά στελέχη ανέδειξε επίσης την αξία του, με μόνο μικρές προτάσεις βελτίωσης.

Στην επόμενη φάση, το Work Package 3 θα παραδώσει το μοντέλο υλοποίησης CSI σε πέντε βήματα:

1. Ανάλυση – απογραφή υπηρεσιών, χάρτης κινδύνων, συμμόρφωση
2. Ορισμός – πολιτικές, ρόλοι, στόχοι
3. Σχεδιασμός – μέτρα, εκπαίδευση
4. Υλοποίηση – τεχνικά βήματα, ενημέρωση προσωπικού
5. Επαλήθευση – δοκιμές, ανατροφοδότηση
6.

Το CSI Model βοηθά τις ΜΜΕ να υιοθετήσουν ασφαλή cloud συστήματα, καθοδηγώντας τις στη χαρτογράφηση κινδύνων, την εφαρμογή μέτρων ασφάλειας και τη συνεχή προστασία. Αυτή η προσέγγιση αυξάνει την ψηφιακή ετοιμότητα, μειώνει τους κυβερνοκινδύνους και ενισχύει την εμπιστοσύνη των πελατών.

Στο μέλλον, το Work Package 4 θα παρέχει εκπαιδευτικό υλικό, όπως προ-αξιολόγηση, πρόγραμμα σπουδών CSI και διαδικτυακή πύλη. Το πρόγραμμα σπουδών θα είναι διαθέσιμο αργότερα μέσα στο έτος, με μικρής διάρκειας εκπαιδευτικά βίντεο βασισμένα σε πραγματικά επιχειρηματικά παραδείγματα να κυκλοφορούν στις αρχές του 2026.

Συναρπαστικά έργα για την ενίσχυση της κυβερνοασφάλειάς σας

🚀 Εκπαίδευση Κυβερνοασφάλειας για Ανθεκτικότητα στην Επιχειρησιακή Τεχνολογία (OT)

https://csector.eu/

Το **CSecTOR** εξοπλίζει τις ΜΜΕ στον τομέα της μεταποίησης και άλλους κρίσιμους τομείς υποδομών με δεξιότητες κυβερνοασφάλειας για OT.

Εστιάζει στον ***εντοπισμό ευπαθειών, την εφαρμογή μέτρων προστασίας και την ανάπτυξη σχεδίων αντίδρασης σε περιστατικά*** για τα συστήματα επιχειρησιακής τεχνολογίας.

Το έργο παρέχει ***προσαρμοσμένη μεθοδολογία, εργαλείο αυτοαξιολόγησης και blended + e-learning πλατφόρμα για να ενισχύσει την ανθεκτικότητα*** σε τομείς όπως χημικά, πλαστικά, υφάσματα, υπηρεσίες κοινής ωφέλειας, πετρέλαιο & φυσικό αέριο και μεταφορές.

🚀Κοινή Πρωτοβουλία Ανάπτυξης Δεξιοτήτων στον Κυβερνοχώρο για την Ενίσχυση της Ευρωπαϊκής Βιομηχανίας

https://encrypt40.eu/

Το **Encrypt 4.0** ενισχύει την ικανότητα των ΜΜΕ στη μεταποίηση να προστατεύουν τα δεδομένα, τα συστήματα και τις λειτουργίες τους στο πλαίσιο της Industry 4.0.

Το έργο βοηθά τις εταιρείες να ***εντοπίζουν, να αναλύουν και να αντιμετωπίζουν τους κυβερνοκινδύνους***, ενώ υποστηρίζει την ανάπτυξη ενός πιο εξειδικευμένου ανθρώπινου δυναμικού στον τομέα της κυβερνοασφάλειας.

Παρέχει πρακτικά, εύχρηστα εργαλεία, όπως το ***Cyber Risk Audit Matrix, εργαστήριο εκπαίδευσης κυβερνοασφάλειας και συλλογή πραγματικών περιστατικών με στρατηγικές άμυνας.***

Το Encrypt 4.0 προωθεί ***διαδραστική, βασισμένη σε έργα μάθηση, ενδυναμώνει τους διευθυντές ΜΜΕ να υιοθετούν προληπτικές πρακτικές κυβερνοασφάλειας και ενθαρρύνει τη διάδοση γνώσης για να ενισχύσει την ανθεκτικότητα και την ψηφιακή ετοιμότητα*** στο βιομηχανικό οικοσύστημα.

Ο συναρπαστικός κόσμος της κυβερνοασφάλειας

Υπάρχουν κυβερνοπειρατές!

Ο όρος «phishing» (απατηλές προσπάθειες για απόκτηση ευαίσθητων πληροφοριών) προέρχεται από την ιδέα της χρήσης δολώματος (π.χ. email ή ιστότοπου) για να «τσιμπήσει» τα θύματα, όπως οι ψαράδες χρησιμοποιούν δόλωμα για να προσελκύσουν τα ψάρια. Στο εκπαιδευτικό μας υλικό θα μάθετε περισσότερα για το phishing.

Ο πρώτος ιός δεν ήταν απάτη

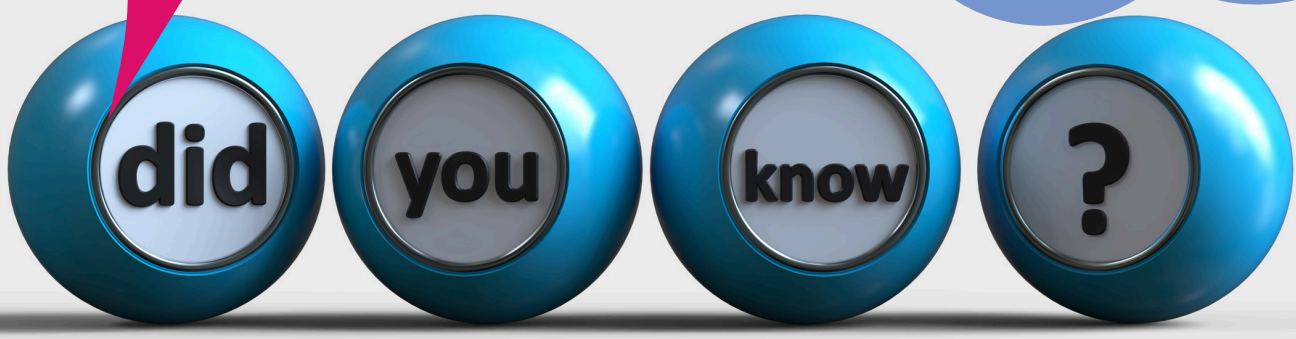
Ο πρώτος γνωστός ιός υπολογιστή ονομάστηκε Creeper και δημιουργήθηκε στις αρχές της δεκαετίας του 1970 ως πρόγραμμα που αναπαραγόταν μόνο του. Δεν προκαλούσε ζημιά – απλώς εμφάνιζε το μήνυμα: "Είμαι ο Creeper, πιάσε με αν μπορείς!" Ήταν περισσότερο απόδειξη έννοιας παρά κακόβουλη επίθεση.

Οι κωδικοί πρόσβασης παραμένουν μεγάλο αδύναμο σημείο

Ο πιο κοινός κωδικός πρόσβασης στον κόσμο εξακολουθεί να είναι «123456», παρά τις πολυετείς προειδοποιήσεις για τους αδύναμους κωδικούς. Στην πραγματικότητα, περίπου το 80% των παραβιάσεων δεδομένων οφείλονται σε αδύναμους ή κλεμμένους κωδικούς πρόσβασης.

Υπάρχουν περισσότερες κυβερνοεπιθέσεις από ό,τι φαντάζεστε

Ο μέσος όρος των καθημερινών κυβερνοεπιθέσεων είναι εντυπωσιακός: περίπου 30.000 ιστοσελίδες παραβιάζονται κάθε μέρα. Αυτό σημαίνει πάνω από 20 ιστοσελίδες το λεπτό!



GO CLOUD GO SECURE

2024-1-AT01-KA220-VET-000245093

Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.