Business IT
solutions & services
Powered by PROFESSIONAL IT security

Cromar Innovation Lab for Digital Risks

CROMAR
INNOVATION LAB

Interview

Cromar Innovation Lab for Digital Risks

Συναντήσαμε τον John Croker, CEO και τον Νίκο Γεωργόπουλο Cyber, Tech, Information & Privacy Risks Advisor του Cromar Insurance Group και είχαμε την ευκαιρία να συνομιλήσουμε μαζί τους στα πλαίσια μια συνέντευξης, για μια σειρά σημαντικών θεμάτων, όπως οι αναδυόμενες απειλές σχετικά με το κυβερνοέγκλημα, η βέλτιστη διαχείριση των κυβερνοκινδύνων η αναγκαιότητα και τα οφέλη από την ασφάλισης Cyber Insurance καθώς επίσης και το νέο Κέντρο Καινοτομίας, Cromar Innovation Lab for Digital Risks, που δημιούργησε η εταιρία για να ενισχύσει ολιστικά την καινοτομία και την ανάπτυξη του τεχνολογικού Οικοσυστήματος στην Ελλάδα.

Ο Νίκος Γεωργόπουλος (αριστερά) και ο John Croker (δεξία)

Όλες οι τάσεις στο τομέα του κυβερνοεγκλήματος δείχνουν να είναι αυξητικές ποσοτικά και εξελισσόμενες ποιοτικά. Ποιες είναι κατά τη γνώμη σας, οι βασικές παράμετροι που καθορίζουν το σημερινό τοπίο των απειλών στον ψηφιακό κόσμο και τις οποίες θα πρέπει άμεσα να αντιμετωπίσουν οι επιχειρήσεις και οργανισμοί;

J.C. Η οικονομική ύφεση λόγω του πολέμου στην Ουκρανία, θα ενισχύσει το κυβερνοέγκλημα το οποίο αυξάνεται σημαντικά σε περιόδους ύφεσης. Οι κυβερνοεπιθέσεις πολλαπλασιάζονται διαρκώς και οι συνέπειες τους μπορούν να πλήξουν οικονομικά τις επιχειρήσεις. Η συγκράτηση ή μείωση των επενδύσεων στην κυβερνοασφάλεια και κυβερνοασφάλιση αυξάνει την πιθανότητα μη επιτυχούς αντιμετώπισής των κυβερνοεπιθέσεων από τις επιχειρήσεις.

Το 2023 αναμένεται να αυξηθούν τα μηνύματα ηλεκτρονικού ψαρέματος τόσο σε όγκο όσο και σε ποιότητα. Το **ransomware**, λογισμικό που κλειδώνει τα συστήματα και απαιτείται καταβολή λύτρων, θα εξακολουθήσει να αποτελεί μια συνεχή απειλή για τα εταιρικά συστήματα όσο και τα **περιστατικά παραβίασης εταιρικών email** (BEC) με σκοπό την απόκτηση του ελέγχου των εταιρικών συστημάτων και την απόσπαση εταιρικών χρημάτων μέσω αλλοίωσης εταιρικών τιμολογίων.

Η αύξηση της χρήσης **MFA** σαν εργαλείο προστασίας της πρόσβασης στα εταιρικά συστήματα έχει γίνει πλέον στόχος των κυβερνοεγκληματιών, οι οποίοι κάνουν καμπάνιες με στόχο την απόσπαση πρόσβασης στους κωδικούς που παράγονται με την διαδικασία αυτή.

Η **κατανόηση του κινδύνου**, η **συνεχής εκπαίδευση του ανθρώπινου δυναμικού**, η **επένδυση στην κυβερνοασφάλεια και την κυβερνοασφάλιση**, είναι τα όπλα που έχουν στην διάθεσή τους οι επιχειρήσεις για την αντιμετώπιση του κυβερνοεγκλήματος.

Με βάση λοιπόν αυτές τις απειλές, ποια πρέπει να είναι η στρατηγική και εκείνα τα μέτρα που πρέπει άμεσα να λάβουν οι επιχειρήσεις και οι οργανισμοί προκειμένου να διαχειριστούν με το βέλτιστο δυνατό τρόπο τους κινδύνους, με επίκεντρο την επένδυση στην κυβερνοασφάλεια και στην κυβερνοασφάλιση;

Ν.Γ. Κάθε επιχείρηση με τη βοήθεια ειδικών κυβερνοασφάλειας πρέπει να φτιάξει το **κατάλληλο πλάνο για την διαχείριση των κυβερνοκινδύνων** και να δώσει έμφαση στην εκπαίδευση του ανθρώπινου δυναμικού της.

Οι **ασφαλιστικές εταιρίες** ζητούν από τις μικρομεσαίες επιχειρήσεις και πιθανούς πελάτες να υιοθετήσουν **τεχνικά μέτρα ασφαλείας** για την πρόληψη, τον εντοπισμό και την ανταπόκριση στα σημερινά εξελιγμένα περιστατικά παραβίασης ασφάλειας τα ακόλουθα:

- Έλεγχος πρόσβασης του χρήστη μέσω ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) και η χρήση Εικονικού Ιδιωτικού Δικτύου (VPN) για απομακρυσμένη πρόσβαση. **Μη ύπαρξη MFA σημαίνει μη ασφαλίσιμη εταιρία.**
- **Εκπαίδευση ευαισθητοποίησης του Ανθρώπινου Δυναμικού στον κυβερνοχώρο.** Η έλλειψη εκπαίδευσης ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας για την προστασία του οργανισμού από το ransomware. **Το μεγαλύτερο ποσοστό περιστατικών παραβίασης ασφάλειας οφείλεται σε ανθρώπινο λάθος** και τουλάχιστον ένας στους τρείς ανεκπαίδευτους χρήστες πέφτουν θύματα περιστατικών ransomware.
- **Ύπαρξη αντίγραφου ασφαλείας δεδομένων και ελεγμένες διαδικασίες ανάκτησής τους.** Μια σωστή διαδικασία δημιουργίας αντιγράφων ασφαλείας δεδομένων με ελεγμένη διαδικασία ανάκτησής της είναι ένας αποτελεσματικός τρόπος για να μετριαστεί ο κίνδυνος μιας επίθεσης ransomware.
- **Εγκατάσταση ενημερώσεων διορθώσεων προγραμμάτων.** Η εγκατάσταση ενημερώσεων διορθώσεων προγραμμάτων ειδικά εκείνων που χαρακτηρίζονται ως κρίσιμες μπορεί να συμβάλει στον περιορισμό των ευπαθειών ενός οργανισμού σε επιθέσεις ransomware.
- **Ύπαρξη Πλάνου Αντιμετώπισης Περιστατικών Παραβίασης Ασφάλειας**

Interview

Για τις μεγαλύτερες επιχειρήσεις ζητούνται περισσότερα μέτρα ασφαλείας τα οποία εξαρτώνται και από την δραστηριότητά τους..

Τι ανταγωνιστικά πλεονεκτήματα μπορεί να προσφέρει η ασφάλιση cyber insurance στο νέο περιβάλλον όπως αυτό διαμορφώνεται σήμερα; Σε τι είδους επιχειρήσεις απευθύνεται;

J.C. Η ασφάλιση cyber insurance βοηθά τις εταιρίες θύματα περιστατικών παραβίασης ασφάλειας, να αντιμετωπίσουν τις οικονομικές συνέπειες και να συνεχίσουν τη λειτουργία τους. **Η ασφάλιση Cyber Insurance κάνει πιο αποτελεσματικό το Πλάνο Αντιμετώπισης Περιστατικών μιας εταιρίας**, γιατί μέσω της ασφάλισης η εταιρία αποκτά πρόσβαση σε εξειδικευμένους παρόχους με εμπειρία στη διαχείριση περιστατικών παραβίασης ασφάλειας.

Η ασφάλιση cyber insurance **απευθύνεται σε όλες τις εταιρίες** ανεξαρτήτως μεγέθους, οι οποίες έχουν όμως υλοποιήσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διαχείριση του κυβερνοκινδύνου. Ας μην ξεχνάμε ότι οι κίνδυνοι ransomware και BEC δεν εξαρτώνται από το μέγεθος της εταιρίας που ασφαλίζεται. Στην πράξη όμως, τα ποσοστά ασφάλισης των μικρομεσαίων επιχειρήσεων είναι πολύ μικρά. Το πρόβλημα οφείλεται κυρίως στη μη κατανόηση του κινδύνου, στην έλλειψη μέτρων ασφαλείας και στην έλλειψη επενδύσεων στον τομέα της κυβερνοασφάλειας.

Ποια είναι τα βασικά χαρακτηριστικά στην παγκόσμια και στην Ελληνική αγορά σε σχέση με το Cyber Insurance; Οι ασφαλιστικές εταιρίες έχουν επανεκτιμήσει τις διαδικασίες ανάληψης κινδύνου; Πόσο οι Ελληνικές εταιρίες είναι έτοιμες να κατανοήσουν και να επενδύσουν σε αυτή την ανάγκη;

Ν.Γ. Η παγκόσμια αγορά της ασφάλισης cyber insurance εκτιμάται ότι το **2040** θα φτάσει τα **$4.7τρις δολάρια**. Σήμερα η παγκόσμια αγορά εκτιμάται ότι είναι €12.8δις δολάρια με το μεγαλύτερο μέρος της να είναι στην Αμερική. Ο αναμενόμενος ετήσιος ρυθμός ανάπτυξης της αγοράς είναι διψήφιος και είναι της τάξεως του **25%.**

Μετά από 24 μήνες συνεχούς αύξησης των ασφαλίστρων παρατηρείται διεθνώς μια σταθεροποίηση του κόστους ασφάλισης μετά τη μείωση των ζημιών από περιστατικά ransomware που παρατηρήθηκε το τελευταίο τρίμηνο του 2022.
Η μείωση αυτή οφείλεται στην επιλεκτική ανάληψη κινδύνων από τους ασφαλιστές, τα αυξημένα μέτρα ασφαλείας που ζητούνται από τις προς ασφάλιση εταιρίες τη μείωση των κεφαλαίων κάλυψης που προσφέρουν, την αύξηση των απαλλαγών, την εισαγωγή συνασφάλισης και την αλλαγή της νομοθεσίας για την αντιμετώπιση των περιστατικών ransomware από την Αμερικανική Αρχή Ξεπλύματος μαύρου Χρήματος.
Η νέα πολιτική ανάληψης κινδύνου ζητά από τον ασφαλισμένο ή την υπό ασφάλιση εταιρία να αποδείξει ότι έχει εφαρμόσει ενισχυμένα επίπεδα ελέγχου ασφάλειας για την πρόληψη, τον εντοπισμό και την ανταπόκριση στα σημερινά εξελιγμένα περιστατικά παραβίασης ασφάλειας.
Η μη επένδυση στην κυβερνοασφάλεια και στην κυβερνοασφάλιση οφείλεται κυρίως στη μη κατανόηση του κινδύνου. Για την κατανόηση του κινδύνου απαιτείται συνεχής εκπαίδευση των εταιριών. Σε αυτό τον τομέα **η συνεργασία εταιριών παρόχων λύσεων ασφάλειας πληροφοριών και ασφαλιστικών εταιριών είναι απαραίτητη.**
Η μη επένδυση στην κυβερνοασφάλεια και στην κυβερνοασφάλιση λόγω μη κατανόησης του κινδύνου δεν αφορά μόνο την Ελλάδα είναι παγκόσμιο φαινόμενο.

Όλοι σήμερα μιλούν για την Τεχνητή Νοημοσύνη, τη μηχανική εκμάθηση και προσφάτως βρίσκεται στην κορυφή της ατζέντας το ChatGPT. Πόσο επηρεάζουν την ασφάλιση Cyber Insurance όλα αυτά;

J.C. Το ChatGPT αποτελεί ένα, κατά βάση, γλωσσικό μοντέλο τεχνητής νοημοσύνης με την βοήθεια του οποίου οι κυβερνοεγκληματίες μπορούν να δημιουργήσουν πειστικά και εξατομικευμένα μηνύματα phishing σε μεγάλη κλίμακα τα οποία θα είναι πολύ πιο δύσκολο να διακριθούν από τους χρήστες. Η χρήση αυτών των τεχνολογιών θα αυξήσει τον αριθμό των επιτυχημένων επιθέσεων phishing.
Το Phishing αποτελεί ένα σημαντικό παράγοντα που επιτρέπει στους επιτιθέμενους να αποκτήσουν πρόσβαση σε εταιρικά συστήματα. Η μεταβολή του κινδύνου που επιφέρει η χρήση των παραπάνω τεχνολογιών επηρεάζει σημαντικά την κυβερνοασφάλιση.

Τι έχει κάνει ο δικός σας οργανισμός προκειμένου να βοηθήσει τις επιχειρήσεις να διαχειριστούν αποτελεσματικά τους κινδύνους του κυβερνοχώρου και γενικότερα των κινδύνων που προκύπτουν από τον ψηφιακό μετασχηματισμό τους;

Ν.Γ. Στόχος μας ήταν και είναι να γίνουμε το **σημείο αναφοράς, για ασφαλιστικά προϊόντα Digital Risks** (Cyber Insurance, ασφαλίσεις εταιριών τεχνολογίας και ασφαλιστικά προϊόντα που καλύπτουν Intellectual Property, NFTs, Crypto Wallets, Blockchain Technology, Smart Contracts).
Για αυτό δημιουργήσαμε το Κέντρο Καινοτομίας, **Cromar Innovation Lab for Digital Risks**, για να ενισχύουμε την καινοτομία εντός και εκτός της εταιρίας.
Παρακολουθούμε τις διεθνείς εξελίξεις στον τεχνολογικό τομέα, και πως αυτές επηρεάζουν τα επιχειρηματικά μοντέλα δημιουργώντας ασφαλιστικές λύσεις **Digital Risks** και υπηρεσίες που υποστηρίζονται από εξειδικευμένες ασφαλιστικές αγορές.
Οι ασφαλιστικές λύσεις που προσφέρουμε εξυπηρετούν την ανάπτυξη του Τεχνολογικού Οικοσυστήματος στην Ελλάδα. Η ασφάλιση των εταιριών αυτών είναι αναγκαία για τη συμμετοχή τους σε έργα και την ανάπτυξή τους εντός & εκτός Ελλάδος.
Συμμετέχουμε επίσης σε **Ευρωπαϊκά Προγράμματα** (SECONDO) με θέματα που σχετίζονται με την κυβερνοασφάλεια και την κυβερνοασφάλιση σε συνεργασία με διεθνή Πανεπιστήμια και εξειδικευμένες εταιρίες με σκοπό την δημιουργία γνώσης εσωτερικά και μεταφορά γνώσης σε συνεργάτες, ασφαλισμένους και εταιρίες.
Η Cromar έχει βραβευθεί από τους **Lloyds** με βραβείο Καινοτομίας για την εκπαιδευτική μηχανή **www.cyberinsurancequote.gr** και το **Cromar Innovation Lab for Digital Risks** έχει βραβευθεί **στο διαγωνισμό Digital Finance Awards 2023.**
Επίσης έχει βραβευθεί με το βραβείο Φίλιππος Μωράκης Disruptive Innovation 2022.

CROMAR
INNOVATION LAB