DIGITAL SECURITY AUTHORITY

CYPRUS CHAMBER OF COMMERCE AND INDUSTRY

CYCSO CYPRUS CYBERSECURITY ORGANIZATION

Προς: Όλα τα Μέλη του ΚΕΒΕ 08/11/18

Από: Αρχή Ψηφιακής Ασφάλειας, ΚΕΒΕ, Κυπριακός Οργανισμός Κυβερνοασφάλειας

Θέμα: 8 Κρίσιμα Μέτρα Κυβερνοασφάλειας (8 Cybersecurity Critical Controls)

Αγαπητά Μέλη,

Στα πλαίσια της υλοποίησης ενός λεπτομερούς και πολύπλευρου προγράμματος κυβερνοασφάλειας, υπάρχουν εκατοντάδες μέτρα ασφάλειας τα οποία ένας οργανισμός μπορεί να πάρει για προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών του κατά τη μεταφορά, επεξεργασία και αποθήκευση τους. Τα τελευταία χρόνια, έχουν αναπτυχθεί πολλά πρότυπα ασφάλειας και πλαίσια απαιτήσεων στην προσπάθεια να αντιμετωπιστούν οι πολύπλευρες απειλές και κίνδυνοι για τις σημαντικές πληροφορίες των οργανισμών, καθώς και των πληροφοριακών υποδομών τους. Όμως, πολλά από αυτά τα πρότυπα και πλαίσια απαιτούν την αιτιολογημένη χρήση μεγάλου αριθμού μέτρων και είναι αρκετά πολύπλοκα στην εφαρμογή τους (με τη συνεπακόλουθη αύξηση βεβαίως στα επίπεδα κυβερνοασφάλειας).

Παράλληλα, αναγνωρίζεται ότι κάποια από τα μέτρα αυτά θεωρούνται σημαντικότερα άλλων (έχουν τον μεγαλύτερο θετικό αντίκτυπο στα επίπεδα ασφάλειας ενός οργανισμού). Βάσει των αποτελεσμάτων πολλών ερευνών και των συσσωρευμένων εμπειριών της κοινότητας ασφάλειας (security community) τα τελευταία χρόνια, διάφοροι οργανισμοί (εθνικοί και διεθνείς) έχουν καταρτίσει καταλόγους με τα πιο σημαντικά μέτρα ασφάλειας που επιφέρουν τη μέγιστη θωράκιση έναντι του φάσματος απειλών σε πληροφοριακά συστήματα – τα μέτρα αυτά ονομάζονται κρίσιμα μέτρα ασφάλειας (critical security controls).

Πέρα από τα μέτρα που θεωρούνται τα πιο κρίσιμα, και τα οποία είναι σχεδιασμένα για άμεση εφαρμογή, μια ολοκληρωμένη προσέγγιση για θέματα ασφάλειας είναι αρκετά πιο πολύπλευρη και περιέχει μεγάλο αριθμό τεχνολογικών, διαδικαστικών και διοικητικών μέτρων για τη μέγιστη προστασία. Για παράδειγμα, **η επιμόρφωση / εκπαίδευση των χρηστών κάθε επιχείρησης / οργανισμού** που έχουν πρόσβαση σε συστήματα πληροφοριών σε βασικές αρχές κυβερνοασφάλειας / ασφάλειας υπολογιστών, με ανάλογη έμφαση και στην φυσική ασφάλεια. Σύμφωνα με μελέτες τόσο της Ευρωπαϊκής Επιτροπής, όσο και ιδιωτικών οργανισμών κυβερνοασφάλειας, η συντριπτική πλειονότητα των περιστατικών έκθεσης της ασφάλειας ενός οργανισμού /

E: secretariat@cycso.org
Twitter: @Cycsocyber
T: 22889744
PO BOX 21455

επιχείρησης σε κινδύνους και κακόβουλες επιθέσεις, οφείλεται στην έλλειψη επαρκών γνώσεων εκ μέρους του ανθρώπινου παράγοντα.

Για σχετική καθοδήγηση και βέλτιστες πρακτικές, αλλά και για γενική επιμόρφωση του ανθρώπινου δυναμικού σας σε βασικές αρχές κυβερνοασφάλειας, μπορείτε να απευθύνεστε στον Κυπριακό Οργανισμό Κυβερνοασφάλειας, μέσω ηλεκτρονικού ταχυδρομείου, στο secretariat@cycso.org ή στο τηλ 22889744.

Είναι καλό επίσης να αναγνωρίζεται ότι τα θέματα ασφάλειας αφορούν ολόκληρο τον οργανισμό, και όχι μόνο το τεχνικό / IT τμήμα, και ως τέτοια αφορούν όλα τα κλιμάκια και τμήματα του. Μόλις ένα συμβούλιο/ηγεσία έχει καθορίσει τους εταιρικούς κινδύνους και έχει καθορίσει τις προσδοκίες του για την ασφάλεια, η συμμόρφωση με αυτές τις προσδοκίες πρέπει να εφαρμοστεί σε όλα τα επίπεδα της επιχείρησης. Θα πρέπει επίσης να καθορίζονται κυρώσεις για τη μη συμμόρφωση, να κοινοποιούνται και να επιβάλλονται από το διοικητικό συμβούλιο ή την ηγεσίας της επιχείρησης. Επιπλέον, το διοικητικό συμβούλιο/ηγεσία, σε συντονισμό με τα ανώτερα διοικητικά στελέχη, είναι υπεύθυνοι για τη διασφάλιση των κατάλληλων οργανωτικών λειτουργιών, των πόρων και της υποστηρικτικής υποδομής, που πρέπει να διατίθενται και να χρησιμοποιούνται σωστά για την εκπλήρωση μιας καλά διαρθρωμένης στρατηγικής ασφάλειας για την επιχείρηση.

Η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ), έχοντας αναπτύξει και εφαρμόζοντας τα πιο κάτω κρίσιμα μέτρα ασφάλειας στον Δημόσιο Τομέα (ως μέρος της υλοποίησης της Στρατηγικής Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας, με τη συμβολή και άλλων αρμοδίων αρχών), το ΚΕΒΕ και ο Κυπριακός Οργανισμός Κυβερνοασφάλειας (CYCSO), συνεργάζονται για την προώθηση της εφαρμογής αυτών των κρίσιμων μέτρων και από τις επιχειρήσεις.

Η ΑΨΑ, το ΚΕΒΕ και ο CYCSO σας προτείνουν τα παρακάτω 8 κρίσιμα μέτρα ασφαλείας, με στόχο να υιοθετηθούν από όλες τις επιχειρήσεις και οργανισμούς στο δημόσιο ή/και ιδιωτικό τομέα, συμβάλλοντας έτσι στην ενδυνάμωση της κυβερνο-ανθεκτικότητας της Κυπριακής Οικονομίας και Κοινωνίας.

Κρίσιμο Μέτρο 1 – Εισαγωγή ενημερώσεων (επικαιροποίηση) ασφαλείας λειτουργικού συστήματος (Updates – Operating System Security Patches)

Τα λειτουργικά συστήματα που βρίσκονται σε χρήση παρουσιάζουν ευπάθειες (vulnerabilities) οι οποίες επιτρέπουν σε κακόβουλους εισβολείς να παρακάμπτουν

δικλίδες ασφαλείας, με δυσάρεστες συνέπειες στην ασφάλεια ενός υπολογιστή και στις πληροφορίες που διακινεί, επεξεργάζεται ή/και αποθηκεύει. Οι εταιρείες ανάπτυξης λειτουργικών συστημάτων εκδίδουν ενημερώσεις ασφάλειας (security updates) σε τακτά χρονικά διαστήματα, ως αποτέλεσμα νέων ευπαθειών και κινδύνων που αναγνωρίζονται. Το παρόν κρίσιμο μέτρο ασφάλειας αφορά την έγκαιρη εισαγωγή αυτών των ενημερώσεων στα διάφορα συστήματα (υπολογιστές, εξυπηρετητές, εξοπλισμό δικτύου, κλπ.). Στις πλείστες περιπτώσεις, η εισαγωγή αυτή μπορεί να γίνει με αυτοματοποιημένο τρόπο, ωστόσο θα πρέπει ο χρήστης να εισαγάγει αυτή την ρύθμιση.

Κρίσιμο Μέτρο 2 – Εισαγωγή ενημερώσεων ασφαλείας εφαρμογών (Updates – Application Security Patches)

Τα λογισμικά προγράμματα / εφαρμογές που βρίσκονται εγκατεστημένα σε κεντρικούς εξυπηρετητές και υπολογιστές χρηστών παρουσιάζουν ευπάθειες (vulnerabilities) οι οποίες επιτρέπουν σε κακόβουλους εισβολείς να παρακάμπτουν τις δικλίδες ασφαλείας και να αποκτούν πρόσβαση στις πληροφορίες που είναι αποθηκευμένες εκεί. Οι εταιρείες ανάπτυξης λογισμικών εφαρμογών εκδίδουν ενημερώσεις ασφάλειας (security updates) σε τακτά χρονικά διαστήματα, ως αποτέλεσμα νέων ευπαθειών που αναγνωρίζονται. Το παρόν κρίσιμο μέτρο ασφάλειας αφορά την εισαγωγή αυτών των ενημερώσεων σε λογισμικές εφαρμογές τύπου εξυπηρετητή (server applications) όπως είναι οι εξυπηρετητές ιστοσελίδων (web servers), οι βάσεις δεδομένων (database servers), καθώς επίσης και σε πελατειακές εφαρμογές (client applications) όπως είναι τα προγράμματα περιήγησης/φυλλομετρητές ιστοσελίδων (web browsers) και οι πρόσθετες λογισμικές εφαρμογές που ενσωματώνονται στους φυλλομετρητές (web browser addons/plugins/toolbars – Java RE, Adobe Reader, Adobe Flash, κλπ.). Στις πλείστες περιπτώσεις, η εισαγωγή αυτή μπορεί να γίνει με αυτοματοποιημένο τρόπο, ωστόσο θα πρέπει ο χρήστης να εισαγάγει αυτή την ρύθμιση.

Κρίσιμο Μέτρο 3 – Περιορισμός Προνομιών Χρηστών (User Privilege Restriction)

Οι χρήστες με διαχειριστικά προνόμια (administrative privileges) σε λειτουργικά συστήματα και εφαρμογές είναι σε θέση να προβούν σε σημαντικές αλλαγές στη διαμόρφωση και τη λειτουργία τους, να τροποποιήσουν κρίσιμες ρυθμίσεις ασφαλείας και να έχουν πρόσβαση σε ευαίσθητες πληροφορίες. Οι διαχειριστές τομέα (domain administrators) έχουν παρόμοιες δυνατότητες σε έναν ολόκληρο τομέα δικτύου, ο οποίος συνήθως περιλαμβάνει όλους τους σταθμούς εργασίας (workstations) και διακομιστές (servers) του δικτύου, καθώς και σε όλα τα στοιχεία τοπικού δικτύου. Οι εισβολείς χρησιμοποιούν συχνά κακόβουλο κώδικα στην προσπάθεια τους να εκμεταλλευτούν

τρωτά σημεία σε σταθμούς εργασίας και διακομιστές. Ο περιορισμός των διαχειριστικών προνομίων του χρήστη περιορίζει τις δυνατότητες του κακόβουλου λογισμικού του εισβολέα να αποκτήσει περαιτέρω πρόσβαση, όπως για παράδειγμα να εξαπλωθεί σε άλλους υπολογιστές, να αποκρύψει την ύπαρξή του ώστε να εξακολουθήσει να υπάρχει και να λειτουργεί ακόμα και μετά την επανεκκίνηση του υπολογιστή, να αποκτήσει εμπιστευτικές πληροφορίες ή να αντισταθεί στις προσπάθειες απομάκρυνσης / διαγραφής. Οι διαχειριστές τομέα πρέπει να φροντίσουν για τον περιορισμό των προνομίων αυτών. Αν δεν υφίσταται, θα πρέπει να οριστεί διαχειριστής τομέα άτομο με επαρκείς γνώσεις ασφάλειας πληροφοριακών συστημάτων.

Κρίσιμο Μέτρο 4 – Πολιτική για Κωδικούς Ασφάλειας (Password Policy)

Στις πλείστες περιπτώσεις, η πρόσβαση των χρηστών στα συστήματα πληροφορικής σε οργανισμούς και επιχειρήσεις ελέγχεται μέσω ενός συνδυασμού ονόματος χρήστη και κωδικού ασφάλειας (username and password), μέσω των οποίων ο χρήστης ουσιαστικά 'αποδεικνύει' την ταυτότητα του και έτσι το σύστημα επιτρέπει την πρόσβαση. Αφού ισχύει αυτό, και αφού το username συνήθως είναι εύκολο να προσδιοριστεί από κάποιον τρίτο (π.χ. ενιαίο username convention, κλπ.), καθίσταται ύψιστης σημασίας ο κωδικός ασφάλειας. Αποτελεί (στις πλείστες περιπτώσεις) τη μόνη ασπίδα ασφάλειας όσο αφορά την πρόσβαση μη-εξουσιοδοτημένων ατόμων σε συστήματα πληροφορικές (και σε ατομικούς ηλεκτρονικούς υπολογιστές). Ως εκ τούτου, πρέπει ο κωδικός ασφάλειας του κάθε χρήστη να χαρακτηρίζεται από ένα επαρκές επίπεδο δυσκολίας σε ότι αφορά τη δυνατότητα αποκάλυψης του (strong password), για να μην αποτελέσει τον αδύναμο κρίκο σε περίπτωση επίθεσης. Το παρόν κρίσιμο μέτρο ασφάλειας αφορά τη σύνταξη του κωδικού ασφάλειας, καθώς και τον τρόπο με τον οποίο χρησιμοποιείται από τον κάθε χρήστη. Προτείνεται όπως ο κάθε οργανισμός διαμορφώσει πολιτική για κωδικούς υπολογιστών, καθιστώντας το υποχρεωτικό όπως ο κάθε υπάλληλος συμμορφωθεί και βελτιώσει την ανθεκτικότητα/πολυπλοκότητα του κωδικού του.

Κρίσιμο Μέτρο 5 – Ασφάλεια Τερματικών Υπολογιστών (Endpoint Security)

Η 'ασφάλεια τερματικών' αναφέρεται σε μέτρα φυσικής και ηλεκτρονικής ασφάλειας σε τερματικό εξοπλισμό χρηστών (σταθμούς εργασίας, φορητούς υπολογιστές, κλπ.), για αποφυγή πρόσβασης από μη εξουσιοδοτημένους χρήστες. Αν και αποτελεί κρίσιμο στοιχείο της αμυντικής γραμμής των πληροφοριακών συστημάτων, συχνά παραβλέπεται, με αποτέλεσμα την έκθεση των οργανισμών σε κινδύνους όπως μόλυνση από κακόβουλο λογισμικό, παράνομη πρόσβαση σε κρίσιμες πληροφορίες, απώλεια συσκευών, κ.ά. Ο σκοπός του μέτρου αυτού είναι να μην επηρεαστεί η εύρυθμη λειτουργία συστημάτων,

αλλά να ενισχυθούν τα επίπεδα ασφάλειας στα τερματικά σημεία των δικτύων, είτε με νέα συστήματα είτε με βελτιώσεις στα υφιστάμενα. Ένα καλό σύστημα προστασίας από ιούς (antivirus) και antispyware (και γενικά για όλων των ειδών κακόβουλων λογισμικών) σε συνεργασία με τον τοίχο προστασίας (firewall) σε επίπεδο τερματικού, είναι αναγκαία ώστε να μπορεί να υπάρχει αποτελεσματική προστασία, εξασφαλίζοντας πως όλοι οι υπολογιστές θα παραμείνουν χωρίς κακόβουλο λογισμικό (malware), ακόμα και αν βρεθούν εκτός των περιμετρικών συστημάτων ασφαλείας. Το τείχος προστασίας σε επίπεδο τερματικού μπορεί να εμποδίσει κακόβουλους χρήστες (hackers) και να αποτρέψει κάποια εισβολή που μπορεί να αποβεί μοιραία για τα ευαίσθητα δεδομένα που υπάρχουν αποθηκευμένα.

Κρίσιμο Μέτρο 6 – Ασφαλισμένη Παραμετροποίηση (Secure Configuration - Hardening)

Τα λειτουργικά συστήματα δεν είναι εξ' ορισμού ασφαλισμένα και ως εκ τούτου είναι ευάλωτα σε κακόβουλες επιθέσεις. Συνεπώς, με βάση τις βέλτιστες πρακτικές ασφάλειας (security best practices), είναι φρόνιμο αυτά να θωρακίζονται κατά την αρχική τους εγκατάσταση ούτως ώστε να μειωθεί ο αριθμός των αδυναμιών / τρωτών σημείων που μπορεί να εκμεταλλευτούν πιθανοί εισβολείς. Η διαδικασία θωράκισης (system hardening procedure) είναι καλό να εφαρμόζεται σε όλα τα λειτουργικά συστήματα ενός οργανισμού είτε αυτά είναι εγκατεστημένα σε κεντρικούς εξυπηρετητές (servers), ηλεκτρονικούς υπολογιστές χρηστών (workstations) ή εξοπλισμό δικτύου (network equipment). Η διαδικασία θωράκισης των λειτουργικών συστημάτων έχει ως στόχο τη μείωση των πιθανών σημείων παράνομης εισόδου (unauthorised entry points) σ' αυτά, μέσω της απενεργοποίησης των αχρείαστων και τη θωράκιση των αναγκαίων υπηρεσιών τους, ούτως ώστε να μην είναι εύκολο να τύχουν εκμετάλλευσης από κακόβουλους εισβολείς. Πέραν τούτου η ανεξέλεγκτη χρήση φορητών συσκευών αποθήκευσης τύπου USB σε τερματικά μπορεί να οδηγήσει σε καταστροφικές συνέπειες για την ασφάλεια του τερματικού ή/και του συστήματος.

Κρίσιμο Μέτρο 7 – Εφεδρικά Αντίγραφα (Backups)

Η τήρηση εφεδρικών αντιγράφων (Backups) βοηθά στη προστασία και επαναφορά όλων των δεδομένων που υπάρχουν σε Συστήματα Πληροφοριών και Εφαρμογών, Λειτουργικών Συστημάτων, Βάσεις Δεδομένων και Σύστημα Δικτύωσης. Τα δεδομένα αυτά διατρέχουν άμεσο κίνδυνο να καταστραφούν (μερικώς ή ολικώς) από ανθρώπινο λάθος, καταστροφή ή δυσλειτουργία του λογισμικού, καταστροφή ή δυσλειτουργία του υλισμικού, κακόβουλες ζημίες, κλοπή και φυσικές καταστροφές, κλπ. Η παρουσία σχεδίου ανάκτησης δεδομένων και η τήρηση επαρκών εφεδρικών αντιγράφων (Backups)

σε τακτά χρονικά διαστήματα είναι επιβεβλημένη για όλα τα πληροφοριακά συστήματα που διατηρούνται σε έναν οργανισμό, ούτως ώστε σε περίπτωση καταστροφής δεδομένων οι δραστηριότητες του οργανισμού να μπορούν να συνεχιστούν απρόσκοπτα.

Κρίσιμο Μέτρο 8 – Επιτρεπόμενες Εφαρμογές (Application Whitelisting)

Κάθε οργανισμός δύναται να λειτουργεί διάφορες εφαρμογές / λογισμικά στα συστήματα πληροφορικής για επιχειρησιακούς σκοπούς. Η επιβολή τεχνικού περιορισμού ώστε να περιορίζονται οι εφαρμογές που δύναται να λειτουργούν / τρέχουν στον εξοπλισμό πληροφορικής ενός οργανισμού είναι μια από τις πιο σημαντικές δικλίδες ασφάλειας που αποσκοπεί στο να περιορίσει την δυνατότητα κακόβουλων λογισμικών να εισβάλουν επιτυχώς και επιπλέον να διασφαλίσει ότι μόνο εφαρμογές / λογισμικά που είναι εγκεκριμένα (και ενδεχομένως είναι ασφαλή) μπορούν να «τρέξουν». Ο περιορισμός αυτός επιτυγχάνεται με την κατάρτιση καταλόγου επιτρεπόμενων εφαρμογών (whitelisting) και την υλοποίηση του περιορισμού λειτουργίας μη εγκεκριμένων εφαρμογών / λογισμικών σε τεχνικό επίπεδο.

Με εκτίμηση,

Γιώργος Μιχαηλίδης
Επίτροπος Ρυθμίσεως
Ηλεκτρονικών Επικοινωνιών
Και Ταχυδρομείων

Μάριος Τσιακκής
Γενικός Γραμματέας ΚΕΒΕ

Κωνσταντίνος Τσιούρτος
Εκ. Διευθυντής CyCSO