ΗΛΙΑΣ ΧΑΝΤΖΟΣ

# Η Ασφάλεια είναι συνδυασμός

*Κύριε Χάντζο, είναι επαρκή τα συστήματα ασφάλειας που διατίθενται στην αγορά των νέων τεχνολογιών;*

Τα συστήματα ασφάλειας είναι σε γενικές γραμμές επαρκή. Ανάλογα με το τι τεχνολογία αγοράζεις, θα έχεις και αντίστοιχη ποιότητα. Σ' αυτό η ασφάλεια δεν είναι διαφορετική από την αγορά του αυτοκινήτου, για παράδειγμα. Το πρόβλημα δεν είναι τόσο στα συστήματα ασφάλειας, όσο το αν έχουμε επαρκή γνώση του κινδύνου που μας αφορά κι αν είμαστε σε θέση να διαχειριστούμε αυτόν τον κίνδυνο αποτελεσματικά, κάνοντας τις αναγκαίες επενδύσεις. Διαφορετικούς κινδύνους και ανάγκες ασφάλειας έχουν οι τράπεζες, διαφορετικές το δημόσιο και διαφορετικές ένα συμβολαιογραφικό γραφείο. Το πρόβλημα είναι, κατά κύριο λόγο, πρόβλημα management. Δηλαδή, αν υπάρχει γνώση του ρίσκου στο επίπεδο διοίκησης της εταιρείας / οργανισμό, προκειμένου να ληφθούν τα αναγκαία μέτρα. Στη συνέχεια βέβαια, προκύπτει το ερώτημα αν υπάρχουν οι απαραίτητες γνώσεις προκειμένου τα αναγκαία μέτρα να εφαρμοστούν σωστά, δηλαδή να γίνει σωστή υλοποίηση της τεχνολογίας και η βούληση να υπάρξουν οι αναγκαίες διαδικασίες και ο ανθρώπινος παράγοντας, προκειμένου τα μέτρα να έχουν αποτέλεσμα. Η ασφάλεια είναι συνδυασμός ανθρώπων, διαδικασιών και τεχνολογίας. Ποτέ το πρόβλημα δεν είναι μόνο τεχνολογικό.

*Ποιοι είναι οι κίνδυνοι που πρέπει να προβλεφθούν από τη βιομηχανία παραγωγής συστημάτων ασφαλείας;*

Εξαρτάται από το σύστημα ασφάλειας για το οποίο μιλάμε κάθε φορά. Σε γενικές γραμμές, οι κίνδυνοι που πρέπει να προβλεφθούν αφορούν τόσο την τεχνολογία την ίδια, όσο και τις διαφορετικές εκφάνσεις της απειλής. Δηλαδή μια

> Το πρόβλημα δεν είναι τόσο στα συστήματα ασφάλειας όσο το αν έχουμε επαρκή γνώση του κινδύνου που μας αφορά και αν είμαστε σε θέση να τον διαχειριστούμε αποτελεσματικά κάνοντας τις αναγκαίες επενδύσεις

λύση antivirus πρέπει να αντιμετωπίσει κινδύνους που σχετίζονται, καταρχήν, με τη συμβατότητα της πλατφόρμας πάνω στην οποία «τρέχει» και τις τροποποιήσεις που θα επιφέρει στην πλατφόρμα ο κατασκευαστής της. Επιπλέον, πρέπει να αντιμετωπίσει κινδύνους σε σχέση με τις αδυναμίες που ενδέχεται να έχει η ίδια η λύση, όπως δυνητικά μπορεί να έχει κάθε λύση λογισμικού. Τρίτον, θα πρέπει να είναι σε θέση να αντιμετωπίσει τις γνωστές απειλές τις οποίες θα εξαπολύσουν κακόβουλοι τρίτοι, καθώς και ένα μηχανισμό ανανέωσης που θα της επιτρέπει να παρακολουθήσει σε ένα βάθος χρόνου την εξέλιξη των κινδύνων που προέρχονται από τρίτους.

*Ο κυβερνοπόλεμος μαίνεται ή τα προβλήματα περιορίζονται σε σποραδικές συγκρούσεις;*

Πρέπει να ορίσουμε, αρχικά, τι θεωρού-

# Ανθρώπων, Διαδικασιών και Τεχνολογίας

με ως κυβερνοπόλεμο...Εγώ θα έλεγα το εξής, αν ο κυβερνοπόλεμος είναι η επιθετική δράση κατά πληροφοριακών συστημάτων χωρών σε περιόδους διεθνούς εντάσεως μεταξύ κρατών, τότε ο κυβερνοπόλεμος ακολουθεί τη ροή και την πορεία των εντάσεων αυτών. Αν κυβερνοπόλεμος είναι η παραπάνω δράση, αλλά επιπλέον κάθε άλλη δραστηριότητα κατασκοπευτικής φύσεως που σκοπεύει στη συλλογή πληροφοριών μεταξύ κρατών και όχι μόνο, προκειμένου οι πληροφορίες που συλλέχθησαν να χρησιμοποιηθούν για την απόκτηση κάποιου πλεονεκτήματος (οικονομικού, πολιτικού, στρατιωτικού), τότε θα σας απαντούσα ότι ο κυβερνοπόλεμος μαίνεται ακατάπαυστα σε παγκόσμιο επίπεδο και θα συνεχίσει να μαίνεται...Η Ελλάδα δεν αποτελεί εξαίρεση σε αυτό το περιβάλλον. Η Symantec εκδίδει ετησίως μια Έκθεση για την κατάσταση της ασφάλειας στο διαδίκτυο, όπου γίνεται εκτενής αναφορά στις δραστηριότητες που βλέπουμε να αναπτύσει το ηλεκτρονικό έγκλημα. Η Έκθεση βρίσκεται στην ιστοσελίδα www.symantec.com.

*Αναγνωρίζουν οι χρήστες πληροφοριακών συστημάτων των μεγάλων επιχειρηματικών και κρατικών οργανισμών την ανάγκη προστασίας;*

Νομίζω ότι στην Ελλάδα, σε γενικές γραμμές, υπάρχουν επιχειρήσεις οι οποίες κατανοούν τον κίνδυνο σε ό,τι αφορά την ασφάλεια των πληροφοριακών συστημάτων. Ειδικότερα στο χρηματοπιστωτικό τομέα, νομίζω πως το επίπεδο ασφάλειας είναι ήδη αρκετά καλό. Με ανησυχεί περισσότερο το επίπεδο ασφάλειας που υπάρχει στο δημόσιο τομέα και σε φορείς, οι οποίοι εποπτεύονται από το δημόσιο τομέα. Με εξαίρεση κάποιες υπηρεσίες, οι οποίες από τη φύση τους είναι ευαίσθητες και κατανοούν τη σημασία της ασφάλειας και διαθεσιμότητας των πληροφοριών, για παράδειγμα η Γενική Γραμματεία Πληροφοριακών Συστημάτων, το Υπουργείο Εθνικής Άμυνας, σε μεγάλο βαθμό υπάρχει άγνοια στο δημόσιο γύρω από τα θέματα αυτά.

*Ποιες λύσεις ενδείκνυνται για αυτές τις κατηγορίες χρηστών;*

Οι λύσεις για αυτές τις κατηγορίες χρηστών είναι περίπλοκες και συνήθως είναι ένα αποτέλεσμα των υπάρχοντων επενδύσεων που έχουν γίνει στην τρέχουσα υποδομή τους, σε συνδυασμό με τους κινδύνους που εκτιμάται ότι αντιμετωπίζουν καθώς και τις λειτουργικές τους ανάγκες. Μην ξεχνάτε ότι η ασφάλεια είναι μια λεπτή ισορροπία μεταξύ απειλών, μέσων και χρηστικότητας των μέσων αυτών. Διαφορετικές ανάγκες ασφάλειας έχει το Κ.Ε.Π. και διαφορετικούς περιορισμούς θα θέταμε στην πρόσβαση δεδομένων σε σχέση με τις βάσεις δεδομένων της Ελληνικής Αστυνομίας. Σε γενικές γραμμές, οι λύσεις γι' αυτή την κατηγορία χρηστών περιλαμβάνουν τεχνολογίες ασφάλειας τερματικών σημείων (end point protection), τεχνολογίες προστασίας από διαρροές πληροφοριών (data leakage prevention), ασφάλεια επικοινωνιών ηλεκτρονικού ταχυδρομείου (messaging security), διαχείριση εφαρμογής πολιτικής τερματικών συσκευών (end point management & compliance), έγκαιρη προειδοποίηση και διαχείριση απειλών (early warning and threat management) και διαχείριση περιστατικών ασφάλειας (security incident management). Όταν συζητάμε για ασφάλεια, είναι εξίσου σημαντικό να προστατευτεί η υποδομή όσο και οι πληροφορίες, οι οποίες βρίσκονται αποθηκευμένες και «ζουν» εντός της υποδομής. Συγχρόνως όμως, οι πληροφορίες πρέπει να είναι διαθέσιμες για να μπορεί να λειτουργήσει μια επιχείρηση/οργανισμός. Γι' αυτόν το λόγο πρέπει να προστατευτούν και οι βάσεις δεδομένων από τυχόν διαρροές και επιθέσεις, παράλληλα πρέπει να υπάρχουν εφεδρικά αρχεία αποθήκευσης (backup), αρχειοθέτηση αλλά και υπολογιστικές δομές υψηλής διαθεσιμότητας, ειδικά σε μια χώρα, όπως η Ελλάδα, με πολλούς φυσικούς κινδύνους (φωτιές, σεισμούς). Για όλα αυτά τα τεχνολογικά προβλήματα, η Symantec έχει λύσεις οι οποίες χρησιμοποιούνται ευρέως στην Ελλάδα.

> Το ηλεκτρονικό κράτος έχει πολύ δουλειά ακόμη στην Ελλάδα. Το δημόσιο πρέπει να αποκτήσει έναν ελάχιστο κοινό παρανομαστή προκειμένου να επιτύχει το όραμα της ηλεκτρονικής διακυβέρνησης

*Υπό ποιες συνθήκες ασφάλειας και οργάνωσης μπορεί να λειτουργήσει αποτελεσματικά το ηλεκτρονικό κράτος;*

Το ηλεκτρονικό κράτος έχει πολύ δουλειά ακόμη στην Ελλάδα. Το δημόσιο πρέπει να αποκτήσει έναν ελάχιστο κοινό παρανομαστή, προκειμένου να επιτύχει το όραμα της ηλεκτρονικής διακυβέρνησης και τα όσα επαγγέλεται η νέα κυβέρνηση, δηλαδή τη μετεξέλιξη του δημοσίου τομέα με τη χρήση της πληρο-

ΗΛΙΑΣ ΧΑΝΤΖΟΣ

# Η Ασφάλεια είναι συνδυασμός Ανθρώπων, Διαδικασιών και Τεχνολογίας

φορικής. Ο στόχος είναι απόλυτα εφικτός και είναι θετικό το ότι υπάρχει κάποιος με αυτό το όραμα. Αυτός ο ελάχιστος κοινός παρανομαστής πρέπει να περιλαμβάνει κοινούς κανόνες ασφάλειας, στο βαθμό του δυνατού / εφικτού, για όλες τις δημόσιες υπηρεσίες που δεν διαχειρίζονται διαβαθμισμένες πληροφορίες. Κοινές πολιτικές προτύπων, διαλειτουργικότητας και προδιαγραφών ασφάλειας στον ευρύτερο δημόσιο τομέα. Έλεγχο και εφαρμογή των κανόνων αυτών, τόσο σε τεχνικό επίπεδο (με την αγορά και χρήση της τεχνολογίας) όσο και σε ανθρώπινο επίπεδο με την εκπαίδευση των χρηστών και την εφαρμογή των κανόνων ασφάλειας από τους χρήστες.

> Δεν είναι δυνατόν να φιλοξενούμε στην Ελλάδα την Ευρωπαϊκή Υπηρεσία Πληροφοριακής Ασφάλειας (ENISA) αλλά να μην διαθέτουμε Εθνικό Κέντρο Αντιμετώπισης Ψηφιακών Απειλών (CERT) όπως όλες οι άλλες Ευρωπαϊκές χώρες

Προϋπόθεση της ηλεκτρονικής διακυβέρνησης είναι και η ευρυζωνικότητα. Τα πρόσφατα στοιχεία είναι ελπιδοφόρα για τη χώρα μας. Όμως, η ευρυζωνικότητα θα καταστήσει οξύτατο το έλλειμα ασφάλειας που ήδη έχουμε. Η νέα κυβέρνηση μιλάει για κεντρικές υπολογιστικές δομές, κέντρα αποθήκευσης και διαχείρισης δεδομένων (data centers) και για τεχνολογίες «νέφους» (cloud computing). Όλα αυτά είναι θεμιτά και η τεχνολογία υπάρχει ήδη, προκειμένου να μειωθεί στο ελάχιστο δυνατό η κατανάλωση ενέργειας από τα συστήματα αυτά, βοηθώντας την πράσινη και οικολογική ανάπτυξη. Όμως, στην καρδιά της επιτυχίας αυτών των στόχων βρίσκεται η επιτυχής αντιμετώπιση του προβλήματος της ασφάλειας. Χωρίς ασφάλεια και διαθεσιμότητα, οι κεντρικές υποδομές γίνονται το ευάλωτο σημείο του όλου συστήματος. Χωρίς ασφάλεια δεδομένων κανείς δεν πρόκειται να χρησιμοποιήσει τεχνολογίες «νέφους» και ούτω καθ'εξής. Μας λείπει η πολιτική πληροφοριακής ασφάλειας και κρισίμων υποδομών. Η πολιτική ασφάλειας πρέπει να είναι συνολική και να μην περιορίζεται μόνο στη δίωξη του ηλεκτρονικού εγκλήματος και στην κρυπτογραφία. Δεν είναι δυνατό να φιλοξενούμε στην Ελλάδα την Ευρωπαϊκή Υπηρεσία Πληροφοριακής Ασφάλειας (ENISA), αλλά να μη διαθέτουμε Εθνικό Κέντρο Αντιμετώπισης Ψηφιακών Απειλών (CERT), όπως όλες οι άλλες ευρωπαϊκές χώρες.

*Ποιο είναι το επίπεδο γνώσης και αντιμετώπισης των προβλημάτων ασφάλειας πληροφοριακών συστημάτων στην Ελλάδα;*

Το επίπεδο είναι μικτό...Σε γενικές γραμμές, υπάρχει κόσμος που κατανοεί την ασφάλεια σε συγκεκριμένους τομείς. Γίνεται, επίσης, αξιόλογη ερευνητική δουλειά στην Ελλάδα και η Symantec συνεργάζεται με ελληνικά πανεπιστήμια στον τομέα της έρευνας και ανάπτυξης τεχνολογιών στο πλαίσιο των ευρωπαϊκών ερευνητικών προγραμμάτων. Παράλληλα, όμως, υπάρχει και σε άλλους τομείς εντυπωσιακή άγνοια ή περιορισμένη αντίληψη, του τι συνιστά πολιτική ασφάλειας και αυτό είναι ιδιαίτερα ανησυχητικό.

*Ποιες είναι οι τάσεις στα συστήματα ασφάλειας;*

Σε αντίθεση με το παρελθόν, όπου οι επιθέσεις γίνονταν με σκοπό την απόκτηση φήμης / δόξας από τον επιτιθέμενο και γίνονταν εύκολα αντιληπτές, οι επιθέσεις σήμερα είναι πιο στοχευμένες και αποσκοπούν στην κλοπή εμπιστευτικών πληροφοριών. Οι επιθέσεις γίνονται εξαιτίας της αξίας που έχουν οι πληροφορίες. Για το λόγο αυτό, οι επιθέσεις

είναι πολύ πιο στοχευμένες χρησιμοποιώντας μοναδικό κακόβουλο λογισμικό. Ουσιαστικά, πρόκειται για ιούς μίας χρήσης. Τα νούμερα μιλάνε από μόνα τους. Το 2002 είχαμε περίπου 20.000 νέους ιούς. Το 2008 είχαμε περίπου 1,6 εκατομμύρια νέους ιούς. Η τάση συνεχίζεται αυξητική. Ουσιαστικά, οι ιοί

ΗΛΙΑΣ ΧΑΝΤΖΟΣ

# Η Ασφάλεια είναι συνδυασμός Ανθρώπων, Διαδικασιών και Τεχνολογίας

περνούν από την ίδια τεχνολογία ελέγχου ποιότητας που χρησιμοποιείται για τα νόμιμα προγράμματα. Η παραγωγή ιών έχει ξεπεράσει σε αριθμό την παραγωγή νομίμων προγραμμάτων. Επομένως, η τάση στις τεχνολογίες ασφάλειας είναι να πάψει ο εντοπισμός μόνο με τη χρήση «υπογραφών» (signature based detection), αλλά να χρησιμοποιείται ένας συνδυασμός υπογραφών λευκής λίστας (whitelisting), φήμης (reputation based detection) και τεχνητής νοημοσύνης (heuristic, behavioral blocking). Ήδη, η Symantec χρησιμοποιεί τις τεχνολογίες αυτές σε διάφορα προϊόντα της. Σε μεταγενέστερη φάση, πιστεύω, ότι η ασφάλεια θα οδηγηθεί στο «νέφος». Η εξαγορά της MessageLabs από τη Symantec αποσκοπεί στο να είμαστε σε θέση να παρέχουμε ακόμη πιο αποτελεσματική προστασία χρησιμοποιώντας τεχνολογίες «νέφους».

*Πώς μπορούν να προστατευθούν οι μεμονωμένοι χρήστες;*

Οι κανόνες ασφάλειας που αφορούν τους μεμονωμένους χρήστες δεν είναι πολύ διαφορετικοί από τους κανόνες ασφάλειας που εφαρμόζονται σε μια τερματική συσκευή στο περιβάλλον μιας επιχείρησης. Καταρχήν, απαιτείται η ύπαρξη κατάλληλου λογισμικού ασφάλειας. Οι λύσεις της Symantec με τα προϊόντα Norton είναι, νομίζω, πολύ δημοφιλείς στην ελληνική αγορά. Ύστερα, απαιτείται η απολύτως στοιχειώδης συντήρηση και ανανέωση του λογισμικού, η οποία είναι λίγο-πολύ αυτοματοποιημένη στις καινούργιες εκδόσεις των προϊόντων. Από εκεί και πέρα, είναι οι γενικοί κανόνες ασφάλειας...π.χ. αποφεύγετε να ανοίγετε μηνύματα από αποστολείς που δεν γνωρίζετε, μην απαντάτε σε μηνύματα που ισχυρίζονται ότι έχουν σταλεί από την τράπεζα σας, κ.τ.λ. Η ελληνική Ομάδα Δράσης για την Ψηφιακή Ασφάλεια (DART) έχει κάνει πολύ καλή δουλειά στην Ελλάδα, ενημερώνοντας το κοινό για την ασφαλή χρήση του Internet και χαίρομαι ιδιαίτερα που η Symantec έχει στηρίξει τις προσπάθειες της. Σε γενικές γραμμές, τα προϊόντα ασφάλειας για καταναλωτές παρέχουν ένα πολύ υψηλό επίπεδο ασφάλειας για το μέσο χρήστη. Από εκεί και πέρα, ακόμη κι αν ο καταναλωτής ενδιαφέρεται για κάτι πιο εξειδικευμένο, όπως τα εφεδρικά αντίγραφα ή την προστασία ανηλίκων και για αυτά υπάρχουν λύσεις από τη Symantec και άλλες εταιρείες στην αγορά. Σε πολλές περιπτώσεις, οι επιτυχημένες επιθέσεις εναντίων μεμονωμένων χρηστών οφείλονται στην εξαπάτηση τους από τους επιτιθέμενους και όχι στην παραβίαση του συστήματος ασφάλειας, εφ' όσον αυτό υπάρχει και λειτουργεί κανονικά.

> Η παραγωγή ιών έχει ξεπεράσει σε αριθμό την παραγωγή νομίμων προγραμμάτων. Επομένως η τάση στις τεχνολογίες ασφάλειας είναι να πάψει ο εντοπισμός μόνο με την χρήση «υπογραφών» αλλά να χρησιμοποιείται ένας συνδυασμός υπογραφών, λευκής λίστας, φήμης και τεχνητής νοημοσύνης

*Ποιες αναμένονται να είναι οι εξελίξεις στη διαδικτυακή οικονομία και επικοινωνία και ποιοι κίνδυνοι ελλοχεύουν;*

Κάθε χρόνο, τα δεδομένα που παράγουμε διπλασιάζονται. Επίσης, η αξία των πληροφοριών αυξάνεται. Αυτό και μόνο σημαίνει ότι τα δεδομένα θα συνεχίσουν να είναι στόχος επιθέσεων. Ακόμη σημαίνει ότι θα καταστεί ακόμη πιο δύσκολο να εμποδίσουμε τη διαρροή τους, αλλά και να μπορέσουμε να τα αρχειοθετήσουμε και διαβαθμίσουμε αποτελεσματικά, χωρίς τη βοήθεια της τεχνολογίας. Πιστεύω ότι θα δούμε πολύ περισσότερες επιθέσεις στο μέλλον και απειλές όχι μόνο σε οικονομικό, αλλά και σε πολιτικό-στρατιωτικό επίπεδο. Ήδη το ΝΑΤΟ έχει δημιουργήσει υπηρεσίες ψηφιακής ασφάλειας, ενώ οι Η.Π.Α. και άλλες χώρες αντιμετωπίζουν το διαδίκτυο ως χώρο διεξαγωγής πολεμικών επιχειρήσεων. Η προστασία της κρίσιμης πληροφοριακής υποδομής, δηλαδή της πληροφοριακής υποδομής που χρησιμοποιείται για να λειτουργήσουν οι βασικές υπηρεσίες μια χώρας (χρηματοπιστωτικές, τηλεπικοινωνίες, διανομή ενέργειας και νερού, μεταφορές) θα καταστεί στρατηγική προτεραιότητα για όλες τις αναπτυγμένες χώρες. Η Ευρωπαϊκή Ένωση, ήδη, αναπτύσσει τις σχετικές πολιτικές. Η Ελλάδα θα πρέπει να παρακολουθήσει τα ζητήματα αυτά από κοντά, αν θέλει να εκπληρώσει τις ηλεκτρονικές της φιλοδοξίες.

Ο κύριος Ηλίας Χάντζος είναι Διευθυντής Κυβερνητικών Σχέσεων Ευρώπης, Αφρικής, Ασίας, Ειρνικού της Symantec Corporation.