Κυβερνο-ασφάλεια για μικρές και μεσαίες επιχειρήσεις

www.inter-datasecurity.com
sales@inter-datasecurity.com
tel +30 2410 670030

Εισαγωγή

Γεγονός είναι ότι μεγάλο ποσοστό των μικρομεσαίων επιχειρήσεων είναι ευάλωτο σε κυβερνο-επιθέσεις και άλλα είδη ψηφιακών απειλών. Αναμφισβήτητα αυτό οφείλεται εν μέρη σε ελλιπή επίγνωση. Σε κάποιες υπάρχει η αντίληψη ότι το θέμα αφορά μόνο τις μεγάλες επιχειρήσεις. Σε άλλες υπάρχει ναι μεν η ανησυχία αλλά επίσης η αμφιβολία για τα μέτρα που μπορούν να εφαρμοστούν και αν η επιχείρηση διαθέτει την οικονομική δυνατότητα να τα στηρίζει.

Το παρόν έγγραφο στοχεύει στην ενημέρωση, σε επίπεδο διοίκησης, περί των απειλών και των μέτρων προστασίας που πιστεύουμε ότι μπορεί να πάρει η πλειοψηφία των μικρομεσαίων επιχειρήσεων.

Δεν μπαίνει σε τεχνικές λεπτομέρειες και δεν ισχυριζόμαστε ότι καλύπτει όλες τις περιπτώσεις εξαντλητικά. Επίσης, οι εξελίξεις στο αντικείμενο είναι τόσο ραγδαίες που μετά από κάποιο διάστημα το περιεχόμενο ενδέχεται να μην είναι πια εξ' ολοκλήρου επίκαιρο.

Αποποίηση Ευθυνών

Περιεχόμενα

Ο καθένας μας μπορεί πλέον να έχει ένα σύστημα πληροφορικής στη διάθεσή του, καθώς επίσης πρόσβαση στο Internet. Και αυτά δουλεύουν εύχρηστα, αξιόπιστα, γρήγορα και με περιορισμένο κόστος.

Συνεπώς επίσης οι επιχειρήσεις εκτελούν τις εργασίες τις ψηφιακά όσο αυτό είναι δυνατόν και εκμεταλλεύονται το Internet με τις ατελείωτες δυνατότητές του.

Η πληροφορία είναι πλέον το πολυτιμότερο αγαθό.

Αυτό το γνωρίζουν επίσης οι εγκληματίες οι οποίοι εκμεταλλεύονται το Internet για να πράττουν με πολύ μικρό ρίσκο εντοπισμού, σχετικά ξεκούραστα, σε μεγάλη κλίμακα και με πάρα πολλούς τρόπους. Είναι λογικό ότι ένα μέρος της εγκληματικότητας έχει στραφεί στο Internet.

Στα "δημοφιλέστερα" είδη απειλών ανήκουν:

Ransomware. Ο επιτήδειος με κακόβουλο λογισμικό κρυπτογραφεί τα δεδομένα του θύματος και ζητά λύτρα για να τα δώσει πίσω. Χάρη του ψηφιακού νομίσματος οι επιτήδειοι μπορούν να πληρωθούν μέσω Internet ενώ μένουν σε πλήρη ανωνυμότητα.

Άλλο κακόβουλο λογισμικό. Πέρα από το Ransomware υπάρχει μεγάλη ποικιλία κακόβουλου λογισμικού το οποίο στοχεύει άμεσα ή έμμεσα στο απόσπασμα χρημάτων ή την δημιουργία ζημίας.

Επιθέσεις σε υποδομή εξ' αποστάσεως πρόσβασης. Οι περισσότεροι οργανισμοί διαθέτουν πλέον την υποδομή που παρέχει σε κάποιον εξ 'αποστάσεως πρόσβαση στο σύστημα πληροφορικής, όπως για εργασία από το σπίτι ή για παροχή τεχνικής υποστήριξης. Είναι αυτονόητο ότι οι επιτήδειοι προσπαθούν να παραβιάζουν αυτές τις υποδομές για να αποκτήσουν πρόσβαση στο εσωτερικό δίκτυο του οργανισμού-θύματος.

Phishing, SMShing. Μηνύματα email ή SMS, συνήθως με κάποιο link στο περιεχόμενο και με παραπλανητικό κείμενο που προκαλεί τον παραλήπτη να πατήσει το link αυτό. Η συνέχεια εξαρτάται από την φαντασία του επιτήδειου. Για παράδειγμα ένα website που μοιάζει με αυτό της τράπεζάς σας και σας ζητά τους κωδικούς πρόσβασης.

Account Takeover. Στην περίπτωση αυτή κάποιος καταφέρνει να παίρνει τον έλεγχο ενός λογαριασμού του θύματος, συνήθως σε κάποια cloud υπηρεσία ή εφαρμογή. Όπως το Gmail ή το Office365. Αυτό επιτρέπει στον επιτήδειο να υποκρίνεται τον πραγματικό ιδιοκτήτη του λογαριασμού προς όφελος δικό του, ζημιά άλλων ή συνδυασμό αυτών.

Ανερχόμενα είδη απειλών:

Πέρα από τα προαναφερόμενα υφιστάμενα είδη απειλών, υπάρχουν φυσικά και νέα ανερχόμενα.

Επιθέσεις σε κινητά τηλέφωνα. Συνήθως με κακόβουλο λογισμικό και για την απόκτηση πληροφοριών ή τον έλεγχο των εφαρμογών στην κινητή συσκευή. Άλλο σενάριο είναι η παρακολούθηση του ιδιοκτήτη του κινητού (που βρίσκεται, με ποιον μιλάει και τι λέει).

Επιθέσεις προς iOT – Internet of things συσκευές. Αφορά έξυπνες συσκευές οι οποίες εμπεριέχουν έναν υπολογιστή και έχουν αλληλεπίδραση με το Internet, για την διαχείρισή τους ή/και την συλλογή και επεξεργασία των πληροφοριών που παράγονται από την συσκευή. Παραδείγματα: έξυπνες κάμερες, VoIP τηλέφωνα, οικιακές συσκευές με Wifi και πολλά άλλα. Οι συσκευές αυτές αποτελούν ουσιαστικά υπολογιστές και χρειάζονται επομένως τακτικά αναβαθμίσεις του λογισμικού τους. Αυτό αμελείται συνήθως με αποτέλεσμα οι συσκευές να είναι ευάλωτες σε επιθέσεις. Επιθέσεις που συνήθως έχουν ως σκοπό να εκμεταλλευτούν μία συσκευή iOT για την απόκτηση πρόσβασης σε ένα δίκτυο – οικιακό ή επιχειρησιακό.

AI – τεχνητή νοημοσύνη. Η τεχνητή νοημοσύνη χρησιμοποιείται πλέον όπου αυτό είναι δυνατόν και ανοίγει νέες δυνατότητες για γρηγορότερα και ευκολότερα αποτελέσματα. Η AI χρησιμοποιείται επομένως επίσης από επιτήδειους για την ανάπτυξη και εκτέλεση νέων ειδών επιθέσεων. Πιο γρήγορα και πιο αποτελεσματικά.

Supply chain attacks. Για τον υπόκοσμο οι πιο ενδιαφέρον στόχοι αποτελούν οι πλούσιοι οργανισμοί και οι οργανισμοί σημαντικοί για την κοινωνία. Αυτοί όμως είναι και πολύ καλά προστατευμένοι. Μία τακτική είναι η επίθεση σε κάποια λιγότερα καλά προστατευμένη οντότητα, η οποία συνεργάζεται με τον οργανισμό-στόχο. Ο σκοπός εδώ είναι η διείσδυση στον μεγάλο οργανισμό διαμέσου του μικρού.

Επιθέσεις σε μεγάλους cloud παρόχους. Οι οποίοι είναι πάρα πολύ καλά προστατευμένοι, αλλά λόγω μεγέθους και σημασίας αποτελούν επίσης μόνιμο στόχο. Περιστατικά είναι επομένως αναμενόμενα και αυτά θα έχουν τότε μεγάλο αντίκτυπο.

ΠΟΙΟ ΕΙΝΑΙ ΤΟ ΡΙΣΚΟ ΣΑΣ

Οι συνέπειες μίας κυβερνο-επίθεσης μπορούν να είναι πολύ σοβαρές. Άμεσα ή έμμεσα. Μερικές από αυτές είναι:

Απώλεια χρημάτων. Για παράδειγμα στην περίπτωση του Ransomware ή άλλος εκβιασμός. Αρκετά θύματα αποφασίζουν να πληρώσουν μην έχοντας άλλη εναλλακτική.

Απώλεια ή αλλοίωση δεδομένων. Σε περίπτωση που δεν υπάρχει backup ή το backup δεν είναι αρκετά πρόσφατο ή έχει αλλοιωθεί και αυτό, μια επιχείρηση μπορεί να βρεθεί χωρίς τα δεδομένα για να λειτουργεί. Πράγμα που μπορεί να είναι καταστροφικό. Σε περίπτωση που η αλλοίωση δεν γίνεται αντιληπτή η επιχείρηση μπορεί να παράγει λανθασμένα αποτελέσματα ή προϊόντα με όλες τις συνέπειες αυτών.

Διακοπή λειτουργίας / παραγωγής. Μία επίθεση μπορεί να έχει ως συνέπεια μία επιχείρηση να μην μπορεί να λειτουργεί η να υπολειτουργεί για ένα διάστημα.

Νομικές ευθύνες / προστίμα. Το θύμα μίας επίθεσης μπορεί να βρεθεί εκτεθειμένο σε νομικές ευθύνες. Για παράδειγμα στην περίπτωση διαρροής προσωπικών δεδομένων.

Ευθύνη προς τρίτους. Το ενδεχόμενο ευθύνης προς τρίτους φαίνεται ήδη από τα προαναφερθέντα. Αλλά επίσης ένας οργανισμός που έχει πέσει θύμα μπορεί άθελά του να προκαλεί ζημία σε τρίτους.

Βλάβη στην φήμη. Γίνεται κατανοητό από τα προαναφερόμενα και μπορεί να είναι ανεπανόρθωτη.

Απώλεια πελατών. Ως συνέπεια των προαναφερθέντων.

Βλάβη σε εξοπλισμό. Είναι θεωρητικά δυνατόν οι αλλαγές σε παραμέτρους λειτουργίας ενός μηχανήματος να προκαλέσουν βλάβη σε αυτό.

Προσωπικός κίνδυνος. Πρόκειται για μία ακραία περίπτωση αλλά πέφτοντας θύμα μίας κυβερνο-επίθεσης μπορεί να εμπλακείτε με τον υπόκοσμο θέτοντας σε κίνδυνο εσάς και τους δικούς σας.

ΟΙ ΕΠΙΔΙΩΞΕΙΣ ΤΩΝ ΕΠΙΤΗΔΕΙΩΝ

Δεν είναι όλοι οι επιτήδειοι ίδιοι. Υπάρχουν διάφορες κατηγορίες, η κάθε μία με τα κίνητρά της.

Κατηγορίες επιτήδειων:

Επιτήδειοι με την στήριξη κρατών

Πρόκειται για εξαιρετικά καλά στελεχωμένους και εξοπλισμένους οργανισμούς που ανήκουν σε κάποιο κράτος ή πληρώνονται από αυτό. Οι αποστολές τους είναι κατασκοπεία, ηλεκτρονικός πόλεμος μεταξύ χωρών, τρομοκρατία κλπ. Μία 'απλή' επιχείρηση μπορεί να πέσει (μόνο) κατά λάθος θύμα από αυτών.

Χακτιβιστές

Είναι ομάδες με έντονη ιδεολογία που νιώθουν την ανάγκη να ακουστούν και είναι πρόθυμοι να φτάσουν στα άκρη για να το πετύχουν. Θα κάνουν κυβερνο-επιθέσεις για να προκαλέσουν επανάσταση, αναστάτωση, αποδιοργάνωση, βλάβη σε φήμη κλπ.

Εγκληματίες / κλέφτες

Είναι αυτοί που επιδιώκουν άμεσα ή έμμεσα το χρήμα. Για παράδειγμα μέσω ransomware ή κλοπή ιδιότητας.

Εκ των έσω επιτήδειοι

Ένας οργανισμός μπορεί να έχει εσωτερικούς εχθρούς οι οποίοι στοχεύουν σε κλοπή χρημάτων ή εκδίκηση.

ΣΕ ΠΟΙΟΥΣ ΕΠΙΤΙΘΕΝΤΑΙ

Και εδώ υπάρχουν κατηγορίες, όπως:

Σε όλο τον κόσμο

'Η σε όποιον μπορούμε να πιάσουμε'. Ο επιτήδειος δεν έχει επιλέξει συγκεκριμένο θύμα. Χρησιμοποιεί έναν μαζικό τρόπο επίθεσης με πάρα πολλά υποψήφια θύματα οπότε είναι στατιστικά σχετικά βέβαιος ότι 'κάτι θα πιάσει'. Είναι προφανώς η μέθοδος που απαιτεί την ελάχιστη επένδυση από τον επιτήδειο. Όλοι μας πρέπει να περιμένουμε τα σχετικά είδη επίθεσης, όπως:

Phishing

Emails με κακόβουλα επισυναπτόμενα

Επίθεση σε υποδομή εξ αποστάσεως πρόσβασης

Τηλεφωνήματα από άτομα τα οποία προσπαθούν να μας πείσουν ότι καλούν για να μας παρέχουν τεχνική υποστήριξη

Κακόβουλα websites

Σε επιλεγμένους στόχους επιχειρήσεις

Εδώ ο επιτήδειος έχει κάνει προεργασία. Έχει μάθει μερικά πράγματα για το υποψήφιο θύμα του. Όπως για παράδειγμα όταν πρόκειται για μία επιχείρηση: ποια είναι η επιχείρηση, ποιο είναι το αντικείμενο, που βρίσκεται, πόσα είναι τα κέρδη, ποιος ηγείται. Στη συνέχεια μπορεί να εκτελέσει επιθέσεις που έχουν μεγαλύτερη πιθανότητα επιτυχίας, όπως:

CEO fraud – παράδειγμα: ο επιτήδειος γνωρίζει το όνομα του CEO της επιχείρησης και έχει δει στα social media ή από email autoresponder ότι εκείνος/η βρίσκεται σε ταξίδι. Δημιουργεί ένα Gmail account το οποίο μοιάζει με το όνομα του CEO και στέλνει από εκεί ένα email προς το λογιστήριο της επιχείρησης αναφέροντας ότι πρέπει να γίνει επειγόντως μεταφορά συγκριμένου ποσού χρημάτων σε συγκεκριμένο λογαριασμό.

Ψεύτικα τιμολόγια – ο επιτήδειος έχει βρει τα στοιχεία τιμολόγησης και το αντικείμενο εργασίας της επιχείρησης και στέλνει πολύ απλά ένα ψεύτικο τιμολόγιο στο λογιστήριο προς πληρωμή. Το πιστεύετε ή όχι υπάρχουν λογιστήρια τα οποία απλά πληρώνουν όποιο τιμολόγιο έρχεται.

Δελεαστικές προτάσεις (πώληση πληροφοριών, προτάσεις συνέντευξης κλπ.) – Παράδειγμα: Ο επιτήδειος έχει μάθει το αντικείμενο της επιχείρησης και το email του υπευθύνου. Στέλνει ένα email στο οποίο προσφέρει με ένα σχετικά χαμηλό κόστος έναν μεγάλο κατάλογο με στοιχεία επικοινωνίας υποψήφιων πελατών. Εφόσον πληρωθεί το τίμημα ο κατάλογος δεν έρχεται ποτέ.

Στην εφοδιαστική αλυσίδα

Επίθεση στον μικρό με στόχο τον μεγάλο. Εδώ ο επιτήδειος είναι το πιθανότερο το οργανωμένο έγκλημα. Έχει κάνει πολλή προεργασία επιλέγοντας τον στόχο (μεγάλος ή σημαντικός οργανισμός). Έχει βρει με ποιους μικρότερους και τυχόν ευάλωτους συνεργάζεται. Στη συνέχεια έχει μελετήσει τους

μικρότερους αυτούς και στοχεύει σ 'έναν ή περισσότερους από αυτούς με σκοπό να χρησιμοποιήσει τον μικρό ως σκαλοπάτι για να διεισδύσει στον μεγάλο.

Οι μέθοδοι είναι ατελείωτες και εξελίσσονται συνεχώς. Αναφέρονται μερικά σημαντικά παραδείγματα.

Password attacks – ο επιτήδειος αποκτά πρόσβαση γνωρίζοντας ή μαντεύοντας username και password. Αυτό έχει μεγάλο ποσοστό επιτυχίας γιατί:

- Σε πολλές συσκευές ασφάλειας ο κόσμος διατηρεί το εργοστασιακό username και password, το οποίο είναι γνωστό. Το βρίσκεις απλά στο Internet
- Πολλής κόσμος χρησιμοποιεί passwords τα οποία μαντεύονται εύκολα
- Πολλής κόσμος χρησιμοποιεί το ίδιο password για πάρα πολύ καιρό
- Πολλής κόσμος χρησιμοποιεί το ίδιο password για πολλές διαφορετικές προσβάσεις
- Σε πολλά περιβάλλονται εργασίας οι εργαζόμενοι χρησιμοποιούν τα ίδια passwords ή τουλάχιστον γνωρίζουν τα passwords των συναδέλφων τους
- Χρήστες που χρησιμοποιούν ένα δύσκολο (δηλαδή καλό) password, συχνά το σημειώνουν αλλιώς δεν μπορούν να το θυμηθούν, αλλά δεν προσέχουν που τοποθετούν το σημείωμα

Μολυσμένα USB sticks – το USB stick είναι από τα πιο πρακτικά μέσα για την μεταφορά αρχείων και έτσι πολλά από αυτά πηγαίνουν από υπολογιστή σε υπολογιστή. Το πιθανότερο είναι ότι κάποια στιγμή θα καταλήξει ένα κακόβουλο αρχείο στο USB stick το οποίο μετά μεταδίδεται σε όποιον επόμενο υπολογιστή συνδέεται. Στα είδη USB sticks συμπεριλαμβάνονται επίσης smartphones, εξωτερικοί δίσκοι USB και ό,τι άλλο συνδέεται με USB και έχει αποθηκευτικό χώρο.

Εκμετάλλευση ευπαθειών σε λογισμικό ή συσκευές – Εννοούνται ευάλωτα σημεία από λάθη ή ανικανότητα πρόβλεψης των κατασκευαστών. Τα ευάλωτα σημεία αυτά μπορούν να εκμεταλλευτούν για την κατάχρηση του εν λόγω προϊόντος για κυβερνο-επιθέσεις. Η εκμετάλλευση αυτή είναι από τους δημοφιλέστερους μεθόδους των επιτήδειων γιατί:

- Ανακαλύπτονται, διερευνόνται και δημοσιεύονται από τρίτους. Δηλαδή τα βρίσκει έτοιμα ο επιτήδειος, συνήθως μαζί με περιγραφή του τρόπου εκμετάλλευσης
- Οι κατασκευαστές σπεύδουν να εξαλείψουν τις ευπάθειες με νέες εκδόσεις του λογισμικού τους. Όμως σε πάρα πολλά περιβάλλοντα η εγκατάσταση των νέων εκδόσεων αυτών αργεί μήνες. Αυτό δίνει στους επιτήδειους ένα μεγάλο παράθυρο χρόνου για σχετικά εύκολες επιθέσεις.

Phishing emails – δείτε περιγραφή στην ενότητα "Κατάσταση και εξέλιξη Κυβερνο-επιθέσεων", σελ.4

Επίθεση σε Υποδομές εξ αποστάσεως πρόσβασης. – δείτε περιγραφή στην ενότητα "Κατάσταση και εξέλιξη Κυβερνο-επιθέσεων" σελ. 4

Account takeover – δείτε περιγραφή στην ενότητα "Κατάσταση και εξέλιξη Κυβερνο-επιθέσεων" σελ. 4

Wifi & iOT attacks – δείτε περιγραφή στην ενότητα "Κατάσταση και εξέλιξη Κυβερνο-επιθέσεων" σελ.4

Drive by downloads – Σε περίπτωση χρήσης ενός ευάλωτου browser (φυλλομετρητής), κακόβουλα websites μπορούν να "φυτέψουν" κακόβουλο περιεχόμενο στον υπολογιστή χωρίς απαραίτητα ο χρήστης να κάνει 'κλικ' σε κάτι.

Τηλεφωνήματα για δήθεν υποστήριξη – Επιτήδειοι τηλεφωνούν υποδυόμενοι την τεχνική υποστήριξη μίας γνωστής εταιρείας (πχ τη Microsoft). Προσπαθούν να καθοδηγήσουν τον χρήστη να κατεβάσει και να εγκαταστήσει κάποιο πρόγραμμα για να μπορούν ύστερα να βοηθήσουν. Στην πραγματικότητα ο επιτήδειος θα χρησιμοποιήσει το πρόγραμμα αυτό για να πάρει τον έλεγχο του υπολογιστή με όλες τις συνέπειες αυτού

ΜΕΤΡΑ ΠΡΟΛΥΨΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ

Στη συνέχεια θα αναφερθούν μέτρα τα οποία μπορεί να λάβει μία μικρομεσαία επιχείρηση. Ξεκινώντας από τα απολύτως ελάχιστα (πολλά από τα οποία δεν έχουν άμεσο κόστος). Πρέπει να τονιστεί ότι οι κίνδυνοι εξελίσσονται συνεχώς και επομένως το ίδιο πρέπει να ισχύει για τα μέτρα προστασίας σε μία επιχείρηση.

Outsourcing

Από τα προαναφερθέντα πρέπει να έχει γίνει κατανοητό ότι η κυβερνο-ασφάλεια είναι μία πολύ σοβαρή υπόθεση για κάθε οργανισμό. Ταυτόχρονα οι εξελίξεις τόσο στις απειλές όσο στα μέτρα αντιμετώπισης είναι ραγδαίες. Πιστεύουμε ότι για την πλειοψηφία των (μικρομεσαίων) επιχειρήσεων δεν είναι δυνατόν να χειρίζεται το θέμα από την ίδια την επιχείρηση. Το αποτέλεσμα θα είναι ανεπαρκές και επομένως η όποια επένδυση αναποτελεσματική.

Μία σοφή αντιμετώπιση είναι η συνεργασία της επιχείρησης με μία εταιρεία με τις κατάλληλες γνώσεις κυβερνο-ασφάλειας και την κατάλληλη υποδομή για να αναλάβει αποτελεσματικά την προστασία της επιχείρησης.

Απόλυτα ελάχιστα μέτρα χωρις αμεσο κοστος
Σε αυτά υπάρχουν αρκετά τα οποία δεν κοστίζουν άμεσα χρήματα.

Πρέπει να υπάρχει κάποιος υπεύθυνος

Αν δεν υπάρχει κάποιος υπεύθυνος και υπόλογος τότε η αποτελεσματικότητα ή μάλιστα η ύπαρξη μέτρων κυβερνο-ασφάλειας είναι εντελώς αβέβαια. Ο υπεύθυνος μπορεί να είναι ο εξωτερικός συνεργάτης στην περίπτωση που η επιχείρηση έχει αναθέσει τα θέματα κυβερνο-ασφάλειας. Αν όχι τότε θα είναι κάποιος της ίδιας της επιχείρησης, πιθανόν χωρίς ειδικές γνώσεις αλλά κάποιος πρέπει να είναι.

Γραπτή πολιτική ασφάλειας

Για τον περιορισμό των κινδύνων πρέπει να τηρούνται κανόνες και να εφαρμόζονται συγκεκριμένοι τρόποι εργασίας. Προφορικά αυτό δεν γίνεται. Σε περίπτωση που η επιχείρηση έχει αναθέσει την κυβερνο-ασφάλεια σε τρίτο τότε εκείνος θα βοηθήσει με την πολιτική. Αλλιώς θα χρειαστεί να το κάνει η ίδια η επιχείρηση όσο μπορεί καλύτερα. Εννοείται ότι η πολιτική αυτή δεν είναι στατική. Εξελίσσεται συνεχώς γιατί αλλάζουν οι ανάγκες της επιχείρησης και αλλάζουν οι απειλές.

Ολοι να προσέχουμε

Όλοι οι εργαζόμενοι πρέπει να ακολουθούν την πολιτική ασφάλειας και επίσης να λειτουργούν συνειδητά και με μία πολύ καλή δόση σκεπτικισμού ώστε να είναι όσο το δυνατόν πιο έτοιμοι να αντιληφθούν κάτι ύποπτο.

Αυτό αφορά όλους τους τρόπους επικοινωνίας (email, fax, τηλέφωνο, social media, websites, επισκέπτες) και γενικότερα την συμπεριφορά στην εργασία.

Φυσική Ασφάλεια

Φυσική πρόσβαση στο πληροφοριακό σύστημα θα πρέπει να υπάρχει μόνο στον βαθμό που αυτό είναι απαραίτητο. Δεν χρειάζονται όλοι πρόσβαση στον server για παράδειγμα και σε πάρα πολλές επιχειρήσεις είναι συγκεκριμένοι εκείνοι που χρειάζονται πρόσβαση σε έναν υπολογιστή. Ζημία από αναρμόδια άτομα μπορεί να προκληθεί από απροσεξία ή επίτηδες και σε περίπτωση που δεν ελέγχεται η φυσική πρόσβαση δεν μπορεί να βρεθεί ο υπαίτιος σε περίπτωση ενός περιστατικού.

Αναβαθμίσεις σε προγράμματα , λειτουργικά συστήματα, iOT συσκευών

Έχει ήδη αναφερθεί ότι πολλές επιθέσεις στοχεύουν σε ευπάθειες σε λογισμικό και συστήματα. Είναι επομένως μείζονος σημασίας να εξαλείφονται οι ευπάθειες αυτές με την έγκαιρη εγκατάσταση αναβαθμίσεων και επιδιορθώσεων λογισμικού. Παρατηρείται πάρα πολύ μεγάλη αμέλεια σε αυτό στην αγορά.

Μην κρατάτε δεδομένα που δεν χρειάζεστε

Αυτό που δεν έχετε δεν μπορούν να σας το πάρουν. Αν τηρείτε αρχείο με πληροφορίες τότε είστε επίσης υπεύθυνος για τις πληροφορίες αυτές. Όπως για παράδειγμα προσωπικά δεδομένα αλλά όχι μόνο αυτά. Η διαρροή αυτών των δεδομένων από οποιαδήποτε αίτια εκθέτει την επιχείρηση σε πολλαπλές προκλήσεις συμπεριλαμβανόμενα προστίμα, βλάβη στη φήμη, απώλεια ανταγωνιστικού πλεονεκτήματος κ.α. Επομένως καταστρέψτε όλα τα δεδομένα που δεν χρειάζεστε. Σε περίπτωση που πρόκειται για χαρτί οπωσδήποτε περάστε το από έναν καταστροφέα ώστε να μην μπορεί κανείς να "ψαρέψει" τα δεδομένα σας από τα σκουπίδια.

Δεν υπάρχουν δωρεάν προγράμματα ή υπηρεσίες

Στο πλαίσιο της μείωσης κόστους πολλοί από μας χρησιμοποιούν προγράμματα και ψηφιακές υπηρεσίες που δεν χρειάζονται αγορά. Εκ πρώτης όψεως αυτή φαίνεται μία αυτονόητη και έξυπνη επιλογή αλλά υπάρχει και η άλλη πλευρά του νομίσματος. Η πραγματικότητα είναι ότι δεν υπάρχουν δωρεάν προγράμματα ή υπηρεσίες. Με κάποιο τρόπο πληρώνονται. Αν δεν έχετε αγοράσει τότε προφανώς δεν είστε εσείς ο πελάτης αλλά το πιθανότερο είστε το εμπόρευμα.

Τα 'δωρεάν' προγράμματα

Η πια αθώα και ακίνδυνη περίπτωση είναι αυτή ενός προγράμματος το οποίο προσφέρεται δωρεάν σε κάποια έκδοση από την οποία λείπουν λειτουργίες. Ο δημιουργός με τον τρόπο αυτό ελπίζει να γίνει γνωστή η εφαρμογή του και αρκετοί να την αγοράζουν ώστε να μπορεί να ζει από αυτό.

Άλλη περίπτωση είναι αυτή του 'open source' λογισμικού. Πρόκειται για νόμιμες και δωρεάν εφαρμογές δημιουργημένες από εθελοντές, συνήθως από την επιστημονική κοινότητα. Παρόλο που υπάρχουν πάρα πολύ καλές και γνωστές εφαρμογές, δεν εγγυάται η ποιότητα, η εξέλιξη και η ασφάλεια τους. Επίσης σημαντικό είναι ότι φυσικά δεν μπορεί κανείς να απαιτεί την ύπαρξη οργανωμένης τεχνικής υποστήριξης.

Και φυσικά αν χρησιμοποιείτε 'σπασμένα' προγράμματα τότε αφενός είστε παράνομοι και ρισκάρετε τις επιπτώσεις, αφετέρου δεν γνωρίζετε πως έχει αλλοιωθεί η εφαρμογή και ποιες ενδεχόμενες παρενέργειες κρύβει.

Οι 'δωρεάν' υπηρεσίες

Πάρα πολλές μικρομεσαίες επιχειρήσεις έχουν αποφασίσει να εξαρτώνται από 'δωρεάν' υπηρεσίες για πολύ σημαντικές και λιγότερα σημαντικές καθημερινές εργασίες.

Το email

Αποκορύφωμα είναι το email, ένα εργαλείο ζωτικής σημασίας για κάθε επιχείρηση. Η χρήση ενός δωρεάν email παρόχου όπως gmail, yahoo, hotmail διευκολύνει γιατί είναι 'δωρεάν' και η υποδομή είναι πάντοτε και παντού προσβάσιμη. Το μόνο που χρειάζεται είναι πρόσβαση στο Internet. Όμως κάτι κρύβεται πίσω από αυτό. Ο πάροχος πουλάει διαφημίσεις σε τρίτους και τις βλέπετε εσείς. Και για να μπορεί να πουλάει τις διαφημίσεις καλύτερα αναλύει ό,τι μπορεί από τα emails σας για να δημιουργεί ένα όσο το δυνατόν λεπτομερέστερο προφίλ. Μάλιστα ανταλλάσονται και πληροφορίες με τρίτους για την βελτιστοποίηση του προφίλ αυτού. Έτσι μετά από ένα διάστημα γνωρίζει ποιος είστε, που μένετε, την ηλικία σας, την οικογενειακή σας κατάσταση, την οικονομική σας κατάσταση, ποιο φαγητό σας αρέσει, ποια είναι τα χόμπι σας, ποιοι είναι οι φίλοι σας, που ψωνίζετε, τι ψωνίζετε και πόσο συχνά κλπ. Εννοείται ότι πλέον χρησιμοποιείται και τεχνητή νοημοσύνη για τις αναλύσεις αυτές. Έχοντας το λεπτομερές προφίλ αυτό ο πάροχος μπορεί να χρεώνει τους διαφημιζόμενους πολύ περισσότερα γιατί η διαφήμιση θα γίνει σε επιλεγμένους στόχους. Πέρα από την διαφήμιση όμως δεν γνωρίζουμε για ποιον άλλο σκοπό χρησιμοποιούνται τα προφίλ τώρα ή στο μέλλον και πόσο καλά προστατεύονται. Η Yahoo στο παρελθόν έχει ήδη πέσει θύμα διαρροής προσωπικών δεδομένων σε μεγάλη κλίμακα.

Έχοντας υπόψη όλα αυτά η χρήση του 'δωρεάν' email δεν είναι πια μία τόσο σοφή επιλογή. Πληρώνοντας για το email της (και δεν είναι και τόσο μεγάλο το κόστος) μία επιχείρηση θα αποφεύγει το profiling. Θα έχει το δικό της domain (δηλαδή το email θα είναι στο στυλ info@mycompany.com) το οποίο είναι πολύ καλύτερο για την ταυτότητα της επιχείρησης. Μία

μικρομεσαία επιχείρηση το πιθανότερο δεν θα θέλει να φιλοξενεί τον δικό της email server οπότε θα επιλέξει έναν πάροχο με τα μέτρα ασφάλειας που τις ταιριάζουν και θα μπορεί μάλιστα να συνεργαστεί και με τρίτους οι οποίοι παρέχουν επί πλέον επίπεδα ασφάλειας.

Social Media

Τα social media θεωρούνται σχεδόν "must" ως πολύ δυνατό εργαλείο για την δωρεάν προβολή των επιχειρήσεων. Εδώ όμως τα πράγματα είναι ακόμα πολύ χειρότερα. Οι εταιρείες πίσω από τα social media δεν έχουν απολύτως κανένα άλλο κίνητρο από το Profiling και το κέρδος από τις πωλήσεις (προσωπικών) δεδομένων. Όποιος (ιδιώτης ή επιχείρηση) χρησιμοποιεί τα social media πρέπει να γνωρίζει ότι είναι εκτεθειμένος στο έμμεσο ρίσκο που προέρχεται από την γνωστοποίηση του προφίλ του, των εκφράσεων και των πράξεων του. Ένα πολύ απλό παράδειγμα: Αν 'ποστάρετε' σε κάποιο social media ότι βρίσκεστε σε διακοπές τότε κάποιος κακόβουλος μπορεί να εκμεταλλευτεί το στοιχείο αυτό.

Για πολλούς δεν αποφεύγεται η χρήση των social media αλλά από άποψη κυβερνο-ασφάλειας αποτελούν ρίσκο. Όσο λιγότερα αποκαλύπτουμε, τόσο το καλύτερο.

Περιορισμός στο αντικείμενο εργασίας

Η ενασχόληση με προσωπικά ενδιαφέροντα στην ώρα εργασίας και η χρήση της υποδομής της επιχείρησης για αυτά, μπορεί να θέτει την επιχείρηση σε περισσότερο ρίσκο από όσο χρειάζεται. Για τον απλό λόγο αυτό συνιστάται να αποφεύγεται. Για παράδειγμα η χρήση του εταιρικού laptop για online παιχνίδια είναι κακή ιδέα. Όπως και η πλοήγηση σε websites που δεν χρειάζονται για την εργασία.

Δημιουργήστε και τηρήστε ένα σχέδιο για επανόρθωση από καταστροφή

Το να είστε προετοιμασμένος για το χειρότερο είναι πάρα πολύ καλό. Στο βαθμό που αυτό είναι δυνατόν σκεφτείτε τι είναι όλα αυτά που θα μπορούσατε να πάθετε και τι θα μπορείτε τότε να κάνετε για να επανέρχεστε από την κατάσταση κρίσης.

Παραδείγματα:

Χάνετε το ηλεκτρικό ρεύμα. Μπορείτε να έχετε μία γεννήτρια ή ίσως δεν σας πειράζει να είστε χωρίς ρεύμα για κάποιες ώρες/μέρες.

Χάνετε το τηλέφωνο ή/και το Internet. Ίσως να μπορείτε προσωρινά να κάνετε κάτι με τον πάροχο κινητής τηλεφωνίας σας. Αν η επιχείρηση είναι εξαρτώμενη από cloud υπηρεσίες τότε αυτό πιθανόν να είναι ένα πολύ σοβαρό θέμα που θέλει καλή σκέψη.

Χάνετε κάποια σημαντικά δεδομένα, για παράδειγμα από ransomware. Πιθανόν με μία καλή τακτική backup δεν θα επηρεάζεστε δραματικά από ένα τέτοιο περιστατικό.

Χάνετε το κτίριο ή την πρόσβαση στο κτίριο…

Τα μέτρα που αναφέρθηκαν ως τώρα δεν έχουν άμεσο κόστος. Ακολουθούν ελάχιστα μέτρα τα οποία έχουν κόστος. Στην αξιολόγησή σας συνιστάται τα σημαντικότερα κριτήρια να είναι η ποιότητα του προϊόντος και της τεχνικής υποστήριξης που το συνοδεύει και όχι η τιμή αγοράς. Το κόστος σας δεν είναι η τιμή αγοράς κάποιων προϊόντων αλλά το κόστος της μακροχρόνιας αποτελεσματικής προστασίας της επιχείρησής σας.

Backup – αντίγραφα ασφάλειας

Το backup είναι το Α και το Ω για την περίπτωση που χάνετε τα δεδομένα σας από οποιαδήποτε αίτια. Αλλά θα πρέπει να γίνει σωστά.

Ανάλογα με τις ανάγκες της επιχείρησης μπορεί να είναι αρκετό να αντιγράφονται απλά τα σημαντικά δεδομένα, ή να είναι προτιμότερο να χρησιμοποιείται μία ειδική εφαρμογή για backup.

Σε κάθε περίπτωση υπάρχουν κάποιες ορθές πρακτικές:

Versioning

> Αν γίνεται το backup συνεχώς στο ίδιο μέσον τότε κινδυνεύετε να μην έχετε backup σε περίπτωση που χαλάσει το αποθηκευτικό μέσον του backup ή σε περίπτωση που έχουν αλλοιωθεί τα δεδομένα και όταν γίνει αυτό αντιληπτό έχουν περάσει ήδη στο backup. Καλή πρακτική είναι να υπάρχουν πολλαπλά μέσα για backup και να τηρούνται διάφορες εκδόσεις. Για παράδειγμα ένα backup για κάθε μέρα της εβδομάδας συν ένα ξεχωριστό εβδομαδιαίο.

Δοκιμές restore

> Το backup είναι σημαντικό αλλά το restore (η επαναφορά του) είναι εξίσου σημαντικό. Άρα πρέπει ανά διαστήματα να γίνεται ένα δοκιμαστικό restore για να βεβαιωθεί ότι όλα λειτουργούν καλά.

Αποθήκευση εκτός δικτύου/κτιρίου

> Σε περίπτωση που το backup αποθηκεύεται στον ίδιο χώρο με τα πρωτότυπα δεδομένα, τότε σε ένα περιστατικό κλοπής ή φυσικής καταστροφής του χώρου, μπορεί μετά να μην υπάρχει backup. Καλό είναι να διατηρείτε το backup ή ένα περιοδικό backup σε άλλο χώρο.

Anti Malware (endpoint protection) σε όλα τα μηχανήματα

Χωρίς την προστασία μίας ποιοτικής εφαρμογής Anti Malware είναι πλέον θέμα ελάχιστου χρόνου μέχρι να προσβληθεί ένας υπολογιστής από κάποια επίθεση. Όλα τα μηχανήματα πρέπει να είναι προστατευμένα. Παλαιά μιλούσαμε για Anti-Virus αλλά μία εφαρμογή endpoint protection κάνει πλέον πολύ περισσότερο από αυτό. Προστατεύει από κακόβουλο λογισμικό, περιέχει τοπικό Firewall, προστατεύει κατά την περιήγηση στο Internet και, αναλόγως του κατασκευαστή μπορεί να έχει και άλλες λειτουργίες όπως αυτόματη εγκατάσταση αναβαθμίσεων και επιδιορθώσεων προγραμμάτων, ειδική προστασία κατά του ransomware κ.α.

Είναι σημαντικό να υπάρχει κεντρική διαχείριση ώστε να μπορεί να εφαρμοστεί μία εταιρική πολιτική ασφάλειας και να μπορεί να υπάρχει παρακολούθηση. Το endpoint protection αποτελεί αντικείμενο

όπου η ανάθεση της παρακολούθησης και διαχείρισης σε εξωτερικό συνεργάτη μπορεί να είναι η καλύτερη επιλογή.

Περιμετρικό Firewall / UTM

Ένα περιμετρικό Firewall (τοίχος προστασίας) αποτελεί πύλη προστασίας μεταξύ του Internet και του δικό σας τοπικού δικτύου και είναι επομένως ζωτικής σημασίας.
Για την σύνδεσή σας στο Internet ο πάροχος σας έχει εγκαταστήσει ένα router στην επιχείρησή σας. Το router αυτό είναι υπεύθυνο για την δρομολόγηση της επικοινωνίας μεταξύ την επιχείρησή σας και το υπόλοιπο Internet.

Τα περισσότερα από αυτά τα routers εμπεριέχουν μερικές πολύ βασικές λειτουργίες ενός firewall. Δεν παρέχουν όμως αρκετή ασφάλεια για να προστατεύουν μία επιχείρηση από μοντέρνες απειλές.

Για τον λόγο αυτό συνιστάται έντονα η τοποθέτηση ενός πραγματικού Firewall, και φυσικά η ρύθμισή του με τους απαραίτητους κανόνες για την κάλυψη των αναγκών της δικής σας επιχείρησης. Η ρύθμιση του Firewall απαιτεί εξειδικευμένες γνώσεις.

Ακολουθούν οι σημαντικότερες διαφορές μεταξύ router και Firewall:

Ενσωματώνοντας ένα τείχος προστασίας, η επιχείρηση μπορεί να ενισχύσει την ασφάλειά της μέσα από τις παρακάτω δυνατότητες που αυτό προσφέρει:

Προηγμένες Λειτουργίες Φιλτραρίσματος: Φιλτράρισμα των πακέτων του δικτύου και του περιεχομένου τους σε βάθος. Παρακολούθηση των ενεργών συνδέσεων και ευφυή λήψη αποφάσεων με βάση το περιεχόμενο της κίνησης. Αποκλεισμός κακόβουλου περιεχόμενου που ενδέχεται να παρακάμψει το απλό φιλτράρισμα των δρομολογητών οι οποίοι δεν εξετάζουν το πραγματικό περιεχόμενο των πακέτων.

Ενισχυμένη Προστασία από Επιθέσεις: Προηγμένα συστήματα ανίχνευσης (IDS) και πρόληψης εισβολής (IPS) που αναγνωρίζουν κακόβουλη δραστηριότητα, εξελιγμένες επιθέσεις και ανώμαλη συμπεριφορά, σε πραγματικό χρόνο. Αντίθετα, δρομολογητές δεν έχουν σχεδιαστεί για να εντοπίζουν τέτοιες επιθέσεις και δεν μπορούν να διακρίνουν μεταξύ νόμιμης και κακόβουλης εσωτερικής κίνησης.

Έλεγχος σε επίπεδο εφαρμογής: Αποκλεισμός συγκεκριμένων τύπων κίνησης με βάση τις εφαρμογές ή τα πρωτόκολλα που χρησιμοποιούνται, όπως συγκεκριμένων ιστοσελίδων ή υπηρεσιών, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση. Ο δρομολογητής δεν κάνει καθόλου έλεγχο σε επίπεδο εφαρμογής.

Λεπτομερής Έλεγχος πρόσβασης: Λεπτομερής έλεγχος της κίνησης δημιουργώντας κανόνες με βάση τους τύπους κίνησης, τους ρόλους και τα δικαιώματα των χρηστών, περιορίζοντας την πρόσβαση μόνο σε πόρους και υπηρεσίες που αυτοί χρειάζονται, σε αντίθεση με τις περιορισμένες δυνατότητες των δρομολογητών.

Υποστήριξη Εικονικών Ιδιωτικών Δικτύων (VPN): Πιο αξιόπιστες δυνατότητες VPN σε σχέση με τους δρομολογητές, υποστηρίζοντας πιο πολλά πρωτόκολλα VPN, ισχυρότερους αλγόριθμους κρυπτογράφησης και χαρακτηριστικά όπως η πολύ-παραγοντική πιστοποίηση (multi-factor authentication) για ενισχυμένη ασφάλεια.

Καταγραφή και Δημιουργία Αναφορών: Πιο εκτεταμένες δυνατότητες καταγραφής και δημιουργίας αναφορών σε σύγκριση με τους δρομολογητές, επιτρέποντας την παρακολούθηση της δραστηριότητας του δικτύου, την ανάλυση των συμβάντων ασφαλείας διατηρώντας έτσι πλήρη ορατότητα του δικτύου.

Ασφάλεια Περιεχομένου στην email κίνηση

Το email είναι ένα από τα σημαντικότερα εργαλεία σε σχεδόν όλες τις επιχειρήσεις και χρησιμοποιείται έντονα. Ακριβώς για αυτόν τον λόγο υπάρχει μεγάλη ποσότητα και μεγάλη ποικιλία επιθέσεων μέσω email.

Μία επιχείρηση η οποία χρησιμοποιεί μία πληρωμένη υποδομή email, έχει την δυνατότητα να εφαρμόζει επί πλέον λειτουργίες ασφάλειας. Τόσο για το φιλτράρισμα ανεπιθύμητου εισερχόμενο περιεχόμενο, τόσο επίσης για την αποφυγή ανεπιθύμητης διαρροής περιεχομένου προς τα έξω.

Έτσι αυξάνεται σημαντικά το επίπεδο προστασίας της επιχείρησης καθώς επίσης η παραγωγικότητά της.

Προστασία στο browsing

Όταν ανοίγουμε άγνωστες ιστοσελίδες με τον φυλλομετρητή (browser) τότε δεν μπορούμε να γνωρίζουμε αν είναι κακόβουλες ή όχι. Είναι επομένως σημαντικό να υπάρχει μηχανισμός προστασίας την ώρα εκείνη. Ο μηχανισμός αυτός μπορεί για παράδειγμα να βρίσκεται ενσωματωμένος στο Endpoint Protection. Επίσης ένα περιμετρικό UTM Firewall συνήθως ενσωματώνει web proxy για τον σκοπό αυτό.

Εξ αποστάσεως πρόσβαση με προστασία VPN & MFA

Σχεδόν όλες οι επιχειρήσεις εκμεταλλεύονται πλέον την δυνατότητα για εξ αποστάσεως πρόσβαση στο πληροφοριακό τους σύστημα. Για την συντήρηση και διαχείριση των συστημάτων και, στην μετά Covid εποχή, για εργασία από το σπίτι.

Εξ αποστάσεως πρόσβαση επιδιώκουν όμως επίσης οι επιτήδειοι οι οποίοι γνωρίζουν ότι υπάρχει η υποδομή. Είναι εύκολα κατανοητό ότι, σε περίπτωση που η υποδομή για εξ αποστάσεως πρόσβαση δεν προστατεύεται επαρκώς, σύντομα η επιχείρηση θα πέσει θύμα μίας επίθεσης. Το λιγότερο που πρέπει να κάνει η επιχείρηση είναι η σύνδεση θα αποτελείται από VPN. Δηλαδή ένα κρυπτογραφημένο κανάλι επικοινωνίας, το οποίο υλοποιείται με το περιμετρικό Firewall της επιχείρησης. Η πρόσβαση στο VPN επιτυγχάνεται με username και password. Σε περίπτωση που ένας επιτήδειος καταφέρει και αποκτήσει το password, τότε το VPN χάνει την αξία προστασίας του. Για τον λόγο αυτό συνιστάται ο εμπλουτισμός του VPN με Multiple Factor Authentication (MFA). Στην περίπτωση αυτή ο χρήστης χρειάζεται ένα στοιχείο ακόμα για την πρόσβαση. Όπως ένα password μίας χρήσης ή το δακτυλικό του αποτύπωμα.

Πέρα από τα απόλυτα βασικά μέτρα είναι αυτονόητο ότι υπάρχουν ακόμα πολλά πιο προχωρημένα μέτρα. Αναφέρονται εδώ μερικά τα οποία σίγουρα είναι πολύ χρήσιμα και για την μικρομεσαία επιχείρηση και σε ορισμένες απαραίτητα.

Outsourcing

Για την αποτελεσματική χρήση των τεχνολογιών που ακολουθούν χρειάζονται εξειδικευμένες γνώσεις. Γι' αυτό συνιστάται η ανάθεση σε εξωτερικό συνεργάτη με τις γνώσεις αυτές.

Endpoint Detection & Response (EDR)

Η αλήθεια είναι ότι, όποια και να είναι τα μέτρα προστασίας που εφαρμόζουμε, υπάρχει η πιθανότητα πάλι κάτι να περάσει και η επιχείρηση να πέσει θύμα μίας επίθεσης. Όταν συμβεί αυτό, τότε είναι ζωτικής σημασίας αυτό να γίνει αντιληπτό άμεσα ώστε να περιορίζεται η ζημία. Αυτό επιτυγχάνεται με την τεχνολογία Endpoint Detection & Response.

Στην πράξη υπάρχει ένας agent (μικρό πρόγραμμα) εγκατεστημένος στα μηχανήματα, ο οποίος παρακολουθεί την δραστηριότητα του μηχανήματος και στέλνει επιλεκτικές πληροφορίες σε μία cloud υποδομή φιλοξενούμενη στον κατασκευαστή του EDR. Εκεί οι πληροφορίες αυτές αναλύονται σε συνδυασμό με παρόμοιες πληροφορίες από συστήματα αλλού ανά τον κόσμο. Στόχος είναι έτσι να μπορεί να αντιληφθεί μία διείσδυση με αρκετά μεγάλο ποσοστό σιγουριάς. Στην περίπτωση αυτή ειδοποιείται το κατάλληλο άτομο για επέμβαση. Σε πολλές λύσεις EDR υπάρχουν επίσης κάποιες δράσεις που μπορούν να γίνουν αυτόματα όπως η απομόνωση ενός μηχανήματος από το δίκτυο για να μην μπορεί να κάνει περαιτέρω ζημία.

Στην περίπτωση που το EDR διαχειρίζεται από εξωτερικό συνεργάτη, ονομάζεται Managed Detection & Response (MDR).

Vulnerability Management – Διαχείριση Ευπαθειών

Όπως έχει αναφερθεί στην ενότητα "Πως επιτίθενται" (σελ. 10) ένας δημοφιλής τρόπος επίθεσης είναι εκείνος που εκμεταλλεύεται γνωστές ευπάθειες σε εφαρμογές λογισμικού ή συστήματα.

Είναι επομένως εύλογο ότι αν μία επιχείρηση γνωρίζει εγκαίρως ποιες ευπάθειες υπάρχουν στα συστήματά της και τις διορθώνει, τότε έχει πετύχει ένα πάρα πολύ σημαντικό βήμα προστασίας.

Το Vulnerability Management είναι η δραστηριότητα στην οποία εντοπίζονται οι ευπάθειες και οργανώνεται η διόρθωσή τους. Με την βοήθεια μίας υποδομής (συνήθως cloud) σαρώνονται τα συστήματα προς έλεγχο για τον εντοπισμό των ευπαθειών. Στη συνέχεια δημιουργείται γραπτή αναφορά με τα αποτελέσματα. Για την διόρθωση χρειάζεται σε λιγότερο ή μεγαλύτερο βαθμό επέμβαση από διαχειριστή. Εκείνος θα κρίνει επίσης ποια συστήματα είναι πιο κρίσιμα και χρήζουν επομένως προτεραιότητας.

Συνεχώς εμφανίζονται καινούριες ευπάθειες και έτσι το Vulnerability Management είναι μία επαναλαμβανόμενη δραστηριότητα για ανθρώπους με τις κατάλληλες γνώσεις ώστε να μπορούν να ερμηνεύσουν τα αποτελέσματα.

Endpoint DLP (Data Leakage Prevention)

Για την επιχείρηση που επιθυμεί να εφαρμόζει μέτρα προστασίας για την αποφυγή διαρροής διαβαθμισμένου περιεχομένου από τους σταθμούς εργασίας, υπάρχει το Endpoint DLP.

Πρόκειται για εφαρμογή η οποία εγκαθίσταται στον σταθμό εργασίας και παρακολουθεί/ελέγχει την επικοινωνία με κάθε δυνατή πύλη εξόδου από το μηχάνημα. Δηλαδή συσκευές που συνδέονται στην USB διεπαφή, το email, uploads σε websites, social media, το τοπικό δίκτυο κλπ.

Επιτρέπει τον ορισμό κατηγοριών περιεχομένου με διάφορους τρόπους όπως λεξικά και regular expressions (λεκτικά μοτίβα)και την δημιουργία πολιτικών που ορίζουν τον περιορισμό εξαγωγής περιεχομένου ως συνδυασμό του περιεχομένου, του χρήστη, του μηχανισμού εξαγωγής κλπ.

Privileged Access Management – PAM

Ένα σύστημα PAM ελέγχει και περιορίζει την πρόσβαση σε συστήματα της επιχείρησης. Συνήθως πρόκειται για πρόσβαση εξ αποστάσεως αλλά μπορεί να είναι και από μέσα από την επιχείρηση. Τα εν λόγο συστήματα είναι συνήθως κρίσιμα όπως servers ή, σε μία βιοτεχνία, μηχανήματα παραγωγής. Όμως και εδώ μπορούν να είναι οποιαδήποτε συστήματα. Οι εν λόγω χρήστες είναι συνήθως άτομα με προσαυξημένα δικαιώματα πάνω στα συστήματα αλλά θα μπορούσαν να είναι και απλοί χρήστες οι οποίοι για παράδειγμα εργάζονται από το σπίτι.

Το σύστημα PAM:

- Ορίζει ποιος χρήστης έχει πρόσβαση, σε ποια μηχανήματα, πότε και για ποια διάρκεια
- Περιορίζει τι μπορεί να κάνει ο χρήστης αυτός
- Καταγράφει όλες τις πράξεις του χρήστη

Το PAM αποτελεί επομένως ένα ισχυρότατο εργαλείο για την πρόληψη περιστατικών ασφάλειας και σε περίπτωση ενός περιστατικού, για την εξερεύνηση των αιτιών.

Συστηματική Πολιτική Ασφάλειας

Στην περίπτωση που υπάρχει ο εξωτερικός συνεργάτης ασφάλειας, μπορεί να γίνει μία πιο αναλυτική πολιτική ασφάλειας και μπορεί να παρακολουθείται καλύτερα αν τηρείται πραγματικά η πολιτική αυτή. Και αυτό θα είναι ένα σημαντικό εργαλείο για την αποτροπή περιστατικών.

ΑΝ ΕΧΕΤΕ ΠΕΣΕΙ ΘΥΜΑ / ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΟΥ

Η αντιμετώπιση ενός περιστατικού εξαρτάται από πολλούς παράγοντες, ανάμεσά τους και απρόβλεπτους. Επομένως δεν υπάρχει συνταγή.

Μπορούν να δοθούν μερικές συμβουλές που θα βοηθήσουν στον περιορισμό της ζημίας.

Αποσυνδεθείτε από Internet

Ώστε εξωτερικοί παράγοντες στο Internet να μην μπορούν να χειροτερέψουν την κατάσταση

Ζητήστε βοήθεια από εταιρεία πληροφορικής

Το πιθανότερο είναι να μην έχετε τις γνώσεις και την ψυχραιμία να αντιμετωπίζετε το συμβάν. Ζητήσετε βοήθεια από ειδικούς. (Η αστυνομία δεν είναι ειδική στην πληροφορική)

Μην πειραματίζεστε

Το πιθανότερο είναι ότι θα κάνετε τα πράγματα χειρότερα

Αν κινδυνεύουν τρίτοι εξ αιτίας σας …

Τότε έχετε πιθανόν (ηθική) υποχρέωση να τους ενημερώσετε

Αν έχετε υποχρέωση αναφοράς (GDPR, NIS2)

Μπορεί να έχετε νομική υποχρέωση να ενημερώσετε τις αρχές για το περιστατικό. Αν δεν το κάνετε τότε ρισκάρετε πρόστιμο

Μένετε ψύχραιμοι – όσο γίνεται

Αξιολογήστε τις δυνατότητές σας, φτιάξτε πλάνο και εκτελέστε

Αυτό σε συνεργασία με τον εξειδικευμένο συνεργάτη σας

ΥΠΟΧΡΕΩΤΙΚΗ ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑ

Το Internet έχει ενσωματωθεί στην σύγχρονη κοινωνία. Έτσι είναι εύλογο να επιβάλλεται νομοθεσία για την χρήση του και την ασφάλεια.

Κανονισμοί συμμόρφωσης υπάρχουν εδώ και χρόνια στην Αμερική. Στην Ευρώπη ξεκίνησαν πριν από λίγα χρόνια και φυσικά αναμένεται περαιτέρω εξέλιξη.

Μερικοί Κανονισμοί συμμόρφωσης στην Ευρώπη είναι:

GDPR

Πλέον πολύ γνωστό. Υπάρχει από το 2018 και αφορά την προστασία προσωπικών δεδομένων. Προδιαγράφει υποχρεωτικά μέτρα προστασίας που πρέπει να εφαρμόζουν οργανισμοί και επιχειρήσεις. Υπάρχει νομοθεσία και κυρώσεις για την μη-συμμόρφωση.

NIS2

Είναι σχετικά καινούριο. Αφορά μέτρα κυβερνο-ασφάλειας που πρέπει να εφαρμόζουν οργανισμοί κρίσιμοι για την κοινωνία, καθώς επίσης οργανισμοί και επιχειρήσεις που συνεργάζονται μαζί τους. Επηρεάζει επομένως ένα πάρα πολύ μεγάλο εύρος επιχειρήσεων. Μεγάλες και μικρές.

Τον Οκτώβριο του 2024 προβλέπεται η εφαρμογή σχετικής νομοθεσίας και από τον Απρίλιο του 2025 θα είναι δημοσίως γνωστοί οι οργανισμοί που πρέπει να συμμορφώνονται με το NIS2.

Η Inter Engineering είναι διανομέας προστιθέμενης αξίας αφοσιωμένος σε λύσεις και υπηρεσίες Κυβερνοασφάλειας διεθνώς.

Με προϋπηρεσία άπό το 1991 και επικέντρωση σε τεχνική εξειδίκευση η εταιρεία ανήκει στους ικανότερους παίκτες της αγοράς. Στενή συνεργασία με το κανάλι άρτια εκπαιδευμένων συνεργατών/μεταπωλητών εγγυάται τοπική διαθεσιμότητα εξειδικευμένων ικανοτήτων σε όλη τη περιοχή ενώ η συνεργασία με κορυφαίες εταιρίες και οργανισμούς εγγυάται τις πιο σύγχρονες και αποτελεσματικές λύσεις. Ο οργανισμός συμβάλλει ενεργά στην συνειδητοποίηση του κοινού και την καταπολέμηση σύγχρονων απειλών.

Για επικοινωνία:

sales@inter-datasecurity.com

Τηλ. +30.2410.670030

Inter Engineering®
World of Cyber Security!