

Η SecPoint προσφέρει τα ισχυρότερα προϊόντα Penetration Testing που χρειάζεται μία επιχείρηση

Συνέντευξη του *Victor Christiansenn*,
Διευθυντή Πωλήσεων της *Secpoint*



Η αξιολόγηση της ευπάθειας μέσω των δοκιμών διείσδυσης σε ενσύρματα και ασύρματα δίκτυα καθώς και οι προτάσεις της εταιρείας Secpoint για την επίτευξη μιας συνολικής πολιτικής ασφάλειας στις επιχειρήσεις, αποτελούν τα βασικά σημεία της συνέντευξης που μας παραχώρησε ο *Victor Christiansenn*, Διευθυντής Πωλήσεων της *Secpoint*.

Πόσο σημαντική είναι κατά την υλοποίηση μιας πολιτικής ασφάλειας σε μία επιχείρηση ή οργανισμό, η αξιολόγηση της ευπάθειας μέσω των δοκιμών διείσδυσης σε ένα δίκτυο και πώς αυτή επιτυγχάνεται;

Καταρχήν, το Penetration Testing γίνεται αναγκαίο με το πέρασμα των χρόνων, αφού πολλές νέες ευπάθειες ανα-

καλύπτονται κάθε έτος, ακόμα και στα δημοφιλή Adobe Acrobat Reader, Firefox, Internet Explorer, Chrome, Windows και πολλά ακόμα, τα οποία είναι ευρέως διαδεδομένα. Δεύτερον, εάν 5 χρόνια πριν, κάποιος μπορούσε να εισβάλει στο website της εταιρείας σας και να σας αφήσει απλά ένα δυσάρεστο μήνυμα, για παράδειγμα: **Dr d00m hacked this site**, σήμερα είναι σίγουρο πως οι συμ-

INTERVIEW

μορίες οργανωμένου εγκλήματος μπορούν να κάνουν στην εταιρεία σας ζημιά ανυπολόγιστης αξίας. Στις μέρες μας, οι hackers μπορούν να εισβάλουν στις ευαίσθητες πληροφορίες των μεγάλων οργανισμών, όπως Τράπεζες και να υποκλέψουν πολύ σημαντικές πληροφορίες, που μπορούν ακόμα και να τις πουλήσουν εκτός από το να τις εκμεταλλευτούν οι ίδιοι. Ενδεικτικά να αναφέρουμε ότι 285 εκατομμύρια εισβολές καταγράφηκαν για το 2008, σύμφωνα με την έκθεση της εταιρείας Verizon. Επίσης έχει καταγραφεί η τάση ότι το οργανωμένο έγκλημα στρέφεται πλέον στην εισβολή των δικτύων των μεγάλων επιχειρήσεων. Στις μέρες μας, είναι ευκολότερο να γίνει αυτό αφού η πολυπλοκότητα του IT εξοπλισμού αυξάνεται συνεχώς και η ασφάλεια αφήνεται συχνά εκτός προϋπολογισμού. Από τα παραπάνω καταλαβαίνουμε πως είναι εξαιρετικά σημαντικό για μία εταιρεία να υπάρχει μία υπηρεσία που θα μπορεί να την προστατεύει από τυχόν επιθέσεις, αλλά και να ανακαλύπτει τις ευπάθειες του δικτύου της, ώστε να μπορούμε να τις διορθώνουμε το συντομότερο δυνατό. Οι περισσότερες εταιρείες έχουν κάποιο firewall και νομίζουν πως μόνο με αυτό είναι ασφαλείς, οι hackers όμως ανακαλύπτουν καθημερινά νέες τεχνικές, προκειμένου να μπορούν να εισβάλουν στο δίκτυό μας. Αυτό σημαίνει πως σήμερα μπορεί να είμαστε ασφαλείς και αύριο να είμαστε εκτεθειμένοι. Η SecPoint προσφέρει τα ισχυρότερα προϊόντα Penetration Testing, τα οποία χρειάζεται μία επιχείρηση για να ελέγξει ολόκληρο τον IT εξοπλισμό της. Πλέον θα είναι απαραίτητα για τους διευθυντές IT, αφού ο νέος νόμος που θα ισχύσει σύντομα σε όλες τις χώρες της ΕΕ θέτει το διευθυντή μιας επιχείρησης προ των ευθυνών του. Χρησιμοποιώντας λοιπόν τα προϊόντα της SecPoint

μπορούμε όχι μόνο να βρούμε τις αδυναμίες του συστήματός μας, αλλά και να τις επιλύσουμε.

Ποια είναι τα πλεονεκτήματα που προσφέρουν οι λύσεις τις οποίες προτείνει η Secpoint για τις δοκιμές διείσδυσης;

Ένα από τα κύρια χαρακτηριστικά του Penetrator είναι ότι έρχεται με περισσότερους από 13.000 μοναδικούς ελέγχους ευπάθειας, που ενημερώνονται σε καθημερινή βάση. Το πολύ εύχρηστο και φιλικό προς το χρήστη Interface, επιτρέπει τον προγραμματισμένο και αυτοματοποιημένο έλεγχο, έτσι ώστε ο πελάτης να μπορεί να ελέγξει όλα τα συστήματά του ανά τακτά χρονικά διαστήματα και να λαμβάνει e-mail όταν υπάρχουν νέες ευπάθειες. Μόνο όταν γνωρίζουμε τις ευπάθειες του δικτύου μας, μπορούμε και να τις επιλύσουμε. Ο Penetrator παρέχει δηλαδή ολοκληρωμένες λύσεις για το πώς θα επιλύσουμε τα προβλήματα.

Είναι γεγονός ότι πολλές επιχειρήσεις επιλέγουν πλέον για το δίκτυό τους ασύρματη τεχνολογία WiFi. Πόσο ασφαλή όμως είναι τα πρότυπα που χρησιμοποιούνται (WEP, WPA) και ποιοι είναι οι κίνδυνοι που ελλοχεύουν στη χρήση ασύρματων δικτύων;

Το WiFi είναι όντως ένας νέος πολύ σημαντικός τρόπος δικτύωσης, που χρησιμοποιείται πλέον από τις περισσότερες επιχειρήσεις. Ελάχιστες από αυτές, όμως, φροντίζουν να είναι ασφαλές το ασύρματο δίκτυό τους. Εύκολα μπορεί κάποιος να εισβάλει μέσω του WiFi στα αρχεία της εταιρείας σας και να σας κάνει ζημιά ανυπολόγιστης αξίας.



Καταρχήν θα πρέπει να αναφέρουμε ότι πολλές επιχειρήσεις ακόμα χρησιμοποιούν την ξεπερασμένη κρυπτογράφηση WEP, που έχει σπάσει πολλά χρόνια πριν. Ο λόγος είναι απλός. Πολλές επιχειρήσεις χρησιμοποιούν παλαιούς εκτυπωτές και εξοπλισμό, που υποστηρίζονται μόνο WEP. Βλέπουμε επίσης σε πολλούς πελάτες που γνωρίζουν τη χρησιμοποίηση ισχυρότερης κρυπτογράφησης WPA και WPA2, αλλά χρησιμοποιούν έναν αδύνατο κωδικό πρόσβασης, όπως «thunderball». Χαρακτηριστικά, εάν το Access Point έχει την ονομασία του πελάτη, τότε συνήθως και το password είναι παραπλήσιο με το όνομα του πελάτη. Αυτό κάνει το δίκτυό σας προσβάσιμο σε οποιονδήποτε hacker θέλει να βλάψει την επιχείρησή σας. Επίσης βλέπουμε πλέον ένα νέο τρόπο επίθεσης σε πελάτες. Τα Windows ψάχνουν πάντα το εταιρικό σας δίκτυο που λειτουργεί καθημερινά, ακόμα και όταν δεν είστε στην επιχείρησή σας. Εάν για παράδειγμα, προσπαθήσετε σε έναν αερολιμένα με το laptop σας να χρησιμοποιήσετε το ασύρματο δίκτυό του - ενώ συνήθως μπαίνετε από το εταιρικό σας δίκτυο - το laptop θα προσπαθεί να βρει το εταιρικό σας δίκτυο. Έτσι, εάν τύχει να είναι κάποιος κακόβουλος στο αεροδρόμιο και αντιληφθεί ότι το laptop σας ψάχνει το εταιρικό σας δίκτυο, μπορεί τεχνητά να δημιουργήσει μία σύνδεση στο laptop του και έπειτα μία στα Windows του laptop σας και να σας συνδέσει αυτόματα, χωρίς να καταλάβετε τίποτα. Με αυτόν τον τρόπο μπορεί να πάρει το handshake του wpa ή wpa2 του εταιρικού σας δικτύου, καθώς επίσης και να έχει πλήρη πρόσβαση στα αρχεία του υπολογιστή σας.

Τι προτείνει λοιπόν η SecPoint για τον έλεγχο ασφάλειας των ασύρματων δικτύων ;

Η SecPoint προτείνει μια ιδιαίτερα ισχυρή λύση για τον έλεγχο της ασφάλειας των ασύρματων δικτύων, που ονομάζεται Portable Penetrator. Με το Portable Penetrator μπορούμε να ελέγξουμε τα ασύρματα δίκτυα με κωδικοποίηση WEP, WPA και WPA 2, έτσι ώστε να εξασφαλίσουμε τα ασύρματα δίκτυα της επιχείρησης. Το Portable Penetrator έρχεται με την πιο εξελιγμένη τεχνολογία για τα ασύρματα δίκτυα και παρέχει ολοκληρωμένες πληροφορίες για το πώς να κάνετε το WiFi δίκτυό σας ασφαλέστερο. Επίσης, μία ακόμα διαπίστωση είναι, ότι θα μπορούσε σε 3 μήνες από την αγορά του Portable Penetrator να βρεθεί ένας νέος τρόπος για να σπάσει το WiFi της εταιρείας. Αυτή η διαπίστωση δείχνει τη σημαντικότη-

τα του να ελέγχουμε τακτικά το δίκτυό μας, ενώ αξίζει να σημειωθεί πως το Portable Penetrator ενημερώνεται αυτόματα με τα πιο πρόσφατα updates.

Σήμερα γίνεται ολοένα και πιο ισχυρή η τάση ενοποίησης διαχείρισης των απειλών με τη χρήση των συσκευών UTM. Πώς αξιολογείτε τη συγκεκριμένη εξέλιξη και τι πρέπει να προσέχει κάποιος όταν αγοράζει μία συσκευή UTM;

Είναι αλήθεια ότι οι επιχειρηματικοί πελάτες αναγνωρίζουν πως πλέον υπάρχει δυνατότητα με την κατοχή μιας συσκευής να λυθούν πολλά από τα προβλήματα ασφάλειας, με την ελάχιστη δυνατή συντήρηση. Κατά την αγορά ενός UTM θα πρέπει κάποιος να προσέξει αν κάνει συχνά updates και αν στην τιμή του συμπεριλαμβάνονται όλα τα modules. Η SecPoint έχει εξειδικευτεί στις συσκευές UTM και έχει δημιουργήσει πλέον παράδοση, αφού βρίσκεται στο χώρο για περισσότερα από 6 χρόνια. Οι συσκευές της Secpoint προσφέρουν ενοποιημένες λύσεις Anti-Spam, Anti Virus, Web Filtering, Web Proxy, Intrusion Prevention και content filtering.

Ποια λύση προτείνει η Secpoint όσον αφορά τις συσκευές UTM και τι πλεονεκτήματα προσφέρουν;

Η Secpoint προτείνει τη βραβευμένη συσκευή με το όνομα Protector, για την οποία θα πρέπει να αναφέρουμε ότι ενημερώνεται κάθε τέταρτο με τα νέα features και 4 φορές ημερησίως με τα πιο πρόσφατα database definitions. Η εγκατάστασή του είναι πολύ εύκολη και γρήγορη προς το χρήστη, ενώ δεν είναι απαραίτητο να αλλάξετε τίποτα στο δίκτυό σας. Ο κάθε χρήστης μπορεί να ελέγχει αυτόνομα τα δικά του Spam, έτσι ώστε πολύ εύκολα να έχει τη δυνατότητα να διαχειριστεί την πολιτική του δικού του spam και να βάζει κάποια mail στη black list ή άλλα ταχυδρομεία που δεν θέλει να λαμβάνει και όλα αυτά να ισχύουν μόνο για το λογαριασμό του. Με το Antivirus υποστηρίζουμε προμηθευτές όπως Bitdefender, Kaspersky, Norman, ClamAV, ενώ με το Web Proxy μπορούμε να εξασφαλίσουμε γρηγορότερο και ασφαλέστερο internet. Επίσης με το Web Filter μπορούμε να εφαρμόζουμε διαφορετική πολιτική αναλόγως το τμήμα της εταιρείας, όπως για παράδειγμα να απαγορεύσουμε από το τμήμα πωλήσεων να μπαίνει στο Facebook. Τέλος, με τα Intrusion Preventions μπορούμε να αποτρέψουμε όλες τις επιθέσεις των hackers. **ITSecurity**