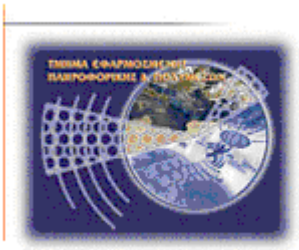
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή Εργασία

Ασφάλεια στα Microsoft Windows® μέσα στον χρόνο: Τεχνικές, Μέθοδοι και Βελτιώσεις

Μενεγάκης Ευάγγελος ΑΜ:2938

Επιβλέπων Καθηγητής: Παπαδάκης Νικόλαος

ΗΡΑΚΛΕΙΟ

2015

Abstract

This final year project is about Microsoft Windows security's methods and techniques through the recent years, starting from Windows XP and ending with Windows 10. It will examine the the improvements made through Microsoft Windows versions that were published for the achievement of a better security level.

Σύνοψη

Αυτή η πτυχιακή εργασία θέλει να δείξει τις μεθόδους και τεχνικές των Microsoft Windows κατά την διάρκεια των τελευταίων χρόνων, αρχίζοντας με τα Windows XP και καταλήγοντας με τα Windows 10. Θα μελετήσει τις βελτιώσεις που έγιναν στις διάφορες εκδόσεις των Microsoft Windows που εκδόθηκαν για να επιτευχθεί ένα καλύτερο επίπεδο προστασίας.

Table of Contents

1 Εισαγωγή

Σε αυτή την πτυχιακή εργασία θα αναφερθούν οι μέθοδοι ασφάλειας που είχαν τα Microsoft Windows από τα Windows XP μέχρι και τα τελευταία Windows 10, καθώς και βελτιώσεις που έγιναν στις πιο νέες εκδόσεις για να καλυφθούν τυχών "κενά" ασφάλειας και προγράμματα που δεν υπήρχαν σε προηγούμενες εκδόσεις με σκοπό την επίτευξη το μέγιστο δυνατό επίπεδο ασφάλειας στο λειτουργικό αυτό σύστημα.

1.1 Περίληψη

Τα Windows μέσα από τις διαφορετικές εκδόσεις τους έβαλαν νέα πρωτόκολλα και τεχνικές, όπως διαφοροποίηση του firewall και antivirus τεχνικές για την καλύτερη ασφάλεια του χρήστη του λειτουργικού συστήματος, είτε χρησιμοποιώντας προγράμματα και εφαρμογές εκτός διαδικτύου, είτε αυτά τα προγράμματα και εφαρμογές χρειάζονται σύνδεση σε κάποιο δίκτυο, είτε και στο διαδίκτυο για την λειτουργία τους.

1.2 Κίνητρο, Σκοπός και Στόχοι Εργασίας

Το σκεπτικό για την δημιουργία αυτής της εργασίας είναι για να καταλάβει κάποιος σε κάθε διαφορετική έκδοση των Windows τι τεχνικές και μέθοδοι υπήρξαν, καθώς ποιες καταργήθηκαν ή μπήκαν ως νέες ώστε έτσι να έχει μια πιο σφαιρική εικόνα και άποψη για αυτά τα λειτουργικά συστήματα σε όσο αφορά την ασφάλεια τους.

1.3 Δομή Εργασίας

Η δομή της εργασίας θα είναι σε κεφάλαια, τα οποία το καθένα θα είναι για μια ξεχωριστή έκδοση των Windows και ένα κεφάλαια για συμπεράσματα που βγήκαν μέσα από τα παρακάτω.

2 Windows XP

Ξεκινώντας με τα Windows XP που εκδόθηκαν το 2001 και βλέποντας τα στοιχεία για την ασφάλεια που διαθέτουν, παρατηρούμε ότι το πρωτόκολλο IPv6 ενσωματώνει για τα Windows το Internet Protocol security το οποίο παρέχει προστασία των IPv6 δεδομένων καθώς αυτά μεταφέρονται μέσω διαδικτύου. Το Internet Protocol security είναι δηλαδή κάποια standards που χρησιμοποιούν κρυπτογραφία κυρίως για την εξασφάλιση ασφάλειας και να παρέχει στα windows xp χαρακτηριστικά όπως αυθεντικότητα, εμπιστευτικότητα, ακεραιότητα δεδομένων.

Η μεταφορά μέσω Internet Protocol security χάρη στην κρυπτογράφηση της δεν μπορεί προφανώς να αποκρυπτογραφηθεί χωρίς το κλειδί που κρυπτογραφήθηκε. Επίσης έχει ένα checksum κρυπτογράφησης που ενσωματώνεται στο κλειδί κρυπτογράφησης, που αυτό χρησιμοποιείται για να καταλάβει ο παραλήπτης των πακέτων ότι τα πακέτα δεν παραποιήθηκαν κατά την μεταφορά. Τέλος τα πακέτα Internet Protocol security έχουν ψηφιακή υπογραφή χρησιμοποιώντας το κλειδί κρυπτογραφίας που μοιράζεται ο αποστολέας και ο παραλήπτης κατά την μεταφορά και με αυτό τον τρόπο ο παραλήπτης επιβεβαιώνει και με αυτό τον τρόπο ότι το έχει στείλει πράγματι ο σωστός αποστολέας.

Το πρωτόκολλο IPv6 παρέχει επίσης υποστήριξη για τυχών ανώνυμες διευθύνσεις, οι οποίες παρέχουν ένα επίπεδο ανωνυμίας όταν ο χρήστης μπαίνει σε διάφορους πόρους του διαδικτύου.

2.1 Windows XP Home Edition

Στην έκδοση των windows XP την Home πολύ αρχικά παρατηρούμε login βασισμένο σε διαφορετικό χρήστη κάθε φορά, γρήγορη εναλλαγή λογαριασμών των χρηστών αυτών που αυτό αξιοποιεί κατά κάποιον τρόπο την προστασία προσωπικών δεδομένων. Επίσης βλέπουμε τώρα ότι παρέχει firewall για συνδέσεις στο διαδίκτυο και έναν φάκελο όπου μπορούν οι χρήστες να διαμοιράζονται αρχεία αυτού του φακέλου που είναι στο ίδιο δίκτυο. Τα windows XP Home edition έχουν κοινά χαρακτηριστικά ασφάλειας με τα Windows NT 4.0 και τα Windows 2000 καθώς φυσικά και νέα στοιχεία και βελτιωμένα.

Ας δούμε πρώτα τα login screens όπου κάθε χρήστης έχει τον δικό του λογαριασμό για να μπει στο σύστημα με δικό του username και κωδικό πρόσβασης που αυτό εξασφαλίζει σε ένα επίπεδο ασφάλεια σε προσωπικά δεδομένα από άλλα άτομα που έχουν πρόσβαση σε αυτό τον υπολογιστή.

Η δημιουργία λογαριασμών γίνεται από έναν χρήστη που έχει δικαιώματα διαχειριστή και αυτός ορίζει το όνομα, τον κωδικό πρόσβασης και τα δικαιώματα του κάθε λογαριασμού, καθώς και τους περιορισμούς αυτού, για παράδειγμα όπως εγκατάσταση προγραμμάτων, ακόμα και φιλτράρισμα ιστοσελίδων στο διαδίκτυο.

Οι χρήστες έχουν την δυνατότητα να ανοίγουν τον λογαριασμό τους, χωρίς ο προηγούμενος λογαριασμός που ήταν ανοιχτός να τερματιστεί και να σταματήσει τυχών προγράμματα που έτρεχαν που αυτό προσφέρει ένα μεγάλο επίπεδο ευελιξίας και ασφάλειας επειδή οι “ανοιχτοί” λογαριασμοί στο σύστημα είναι εντελώς διαφορετικοί μεταξύ τους και για την επίτευξη εναλλαγής τους ζητείτε εκ νέου εισαγωγή κωδικού πρόσβασης. Αυτή η δυνατότητα εναλλαγής χρηστών δεν μπορεί να πραγματοποιηθεί σε domain που το μηχάνημα έχει windows XP. Παρακάτω βλέπουμε μια οθόνη χρηστών που μπορούν να μπουν στον λογαριασμό τους:

Εικόνα 1-Login Screen

Πηγαίνοντας τώρα να δούμε τον Internet Explorer 6 που έχουν τα windows XP, όπου ενσωματώνει το standard Platform for Privacy Preferences με το οποίο ο χρήστης μπορεί να έχει τον έλεγχο των προσωπικών του στοιχείων όταν επισκέπτεται ιστοσελίδες στο διαδίκτυο που είναι συμβατές με αυτό το standard και ζητάνε από τον χρήστη να δώσει τα προσωπικά δεδομένα που έχει επιλέξει αυτός να δίνονται. Γίνεται έλεγχος με το πρωτόκολλο http μεταξύ των ιδιωτικών προτιμήσεων που έχουν γίνει στον browser και των πολιτικών της ιστοσελίδας αυτής για να μοιραστούν αυτά τα δεδομένα.

Επίσης αυτό το standard χρησιμοποιεί cookies, τα οποία αποθηκεύονται στο σύστημα του χρήστη και απομνημονεύουν τις προσωπικές επιλογές του χρήστη για κάθε ιστοσελίδα και φυσικά ο χρήστης μπορεί να έχει επίγνωση για τις πολιτικές αυτών των cookies. Επίσης ο χρήστης έχει τον έλεγχο το αν επιτραπεί τα cookies να αποθηκευτούν στο σύστημα, να εμποδίζονται cookies που δεν ανήκουν στο domain της ιστοσελίδας που επισκέπτεται. Στην παρακάτω φωτογραφία είναι οι αυτές οι ρυθμίσεις για τα cookies που αναφέρθηκαν.

Εικόνα 2-Cookies

Μια άλλη λειτουργία του λειτουργικού συστήματος είναι το Internet Connection Sharing που έχει την δυνατότητα να συνδέονται πολλοί υπολογιστές στο διαδίκτυο χρησιμοποιώντας μια κοινή σύνδεση με ασφάλεια μεταξύ τους.

Ας δούμε όμως τον τρόπο λειτουργίας αυτής της δυνατότητας. Ένας υπολογιστής στο δίκτυο αυτό είναι ο host, ο οποίος συνδέεται απευθείας στο διαδίκτυο και μετά διαμοιράζεται αυτή την σύνδεση και με τους υπόλοιπους υπολογιστές στο δίκτυο. Αυτό γίνεται με ασφάλεια επειδή στο διαδίκτυο το μηχάνημα που φαίνεται είναι το μηχάνημα του host, επειδή όλα τα request των υπόλοιπων υπολογιστών στο δίκτυο περνάνε από τον host και έτσι κρατάνε την διεύθυνση τους κρυφή από το internet και φαίνεται μόνο στο τοπικό δίκτυο. Ο host έτσι έχει την δυνατότητα να ορίζει αυτός το addressing και ορίζει μια permanent διεύθυνση για το μηχάνημα του και παρέχει έτσι το πρωτόκολλο Dynamic Host Configuration Protocol στους υπολογιστές που είναι συνδεδεμένοι σε αυτόν, δίνοντας στον καθένα μια μοναδική διεύθυνση για να επικοινωνεί μεταξύ τους, ανάλογα με τι request και reply περιμένει ο καθένας. Η όλη αυτή δυνατότητα υπήρχε και στα windows 2000 και 98 και βελτιώθηκε με την έκδοση των XP. Επίσης το Internet Connection Sharing παρέχει Network Address Translation και Domain Name Service που χρειάζονται για το configuration των χρηστών σε αυτό το δίκτυο. Παρακάτω βλέπουμε φωτογραφία με τις επιλογές του το Internet Connection Sharing

Εικόνα 3-ICS

Επίσης, τα XP φέρνουν το Internet Connection Firewall για την προστασία από εξωτερικές επιθέσεις του συστήματος, των συσκευών και των υπολογιστών που έχουν ενεργοποιημένο αυτό το firewall είτε είναι στο τοπικό δίκτυο, είτε σε VPN, είτε με Point to point protocol over Ethernet,είτε σε συνδέσεις που έχουν γίνει με dial-up. Αυτό το firewall φιλτράρει τα πακέτα που περνάνε με το να ανοίγει δυναμικά τα ports του μόνο κατά την διάρκεια σύνδεσης σε υπηρεσίες. Αυτό παρέχει προστασία από επιθέσεις στα ports και σε παροχές όπως εκτυπωτές. Τέλος υποστηρίζεται το port mapping, το οποίο ανοίγει "τρύπες" στο firewall το οποίο θα επιτρέπει να ανοίγουν συγκεκριμένα ports για να περνάνε πακέτα που κανονικά θα μπλοκαριζόντουσαν. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο με τις ιδιότητες του firewall

Εικόνα 4-firewall

Τελειώνοντας πηγαίνουμε τώρα στους κοινόχρηστους φακέλους, όπου σε αυτούς κάθε χρήστης του συστήματος έχει πρόσβαση στα αρχεία τους, ανεξαίρετος λογαριασμού με σκοπό την εύκολη πρόσβαση σε κοινόχρηστα αρχεία που χρειάζεται να τα βλέπουν όλοι οι χρήστες του συστήματος. Είναι διαφορετική όμως η προσέγγιση στα αρχεία του φακέλου My Documents αν ο χρήστης έχει βάλει κωδικό πρόσβασης, τότε μπορεί να διαβαστεί μόνο από χρήστη με δικαιώματα διαχειριστή.

2.2 Windows XP Professional Edition

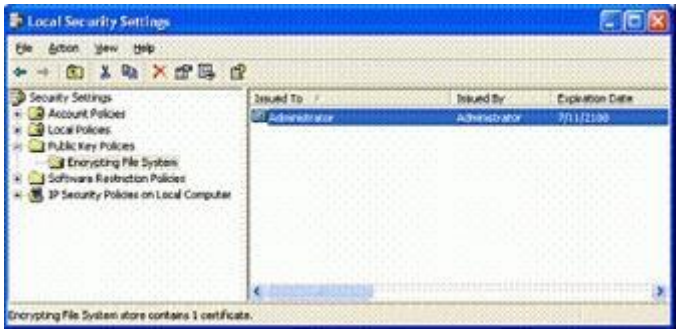
Η ασφάλεια σε αυτή την έκδοση είναι επικεντρωμένη στα αρχεία, εφαρμογές και την διαχείριση των χρηστών στο δίκτυο και η χρήση του Group Policy Objects το οποίο επιτρέπει να λειτουργεί ένα συγκεκριμένο προφίλ ασφάλειας σε πολλά συστήματα και προαιρετικά να χρησιμοποιείται η τεχνολογία του smart card η οποία εξουσιοδοτεί τους χρήστες να μπορούν να χρησιμοποιήσουν τα δεδομένα που είναι αποθηκευμένα σε αυτή την smart card.

Τα προφίλ ασφάλειας που αναφέρθηκαν τα δημιουργεί ένας χρήστης με δικαιώματα διαχειριστή και αυτά μπορούν να περιέχουν αρχεία και φακέλους με τα δικαιώματα πρόσβασης σε αυτά που ορίζει ο διαχειριστής. Επίσης μπορούν να χωριστούν οι χρήστες ανά ομάδες, η οποία κάθε ομάδα θα έχει διαφορετικά δικαιώματα όσον αφορά τους πόρους του λογισμικού.

Μια άλλη λειτουργία της έκδοσης είναι ο έλεγχος στο αν κάποιος στο σύστημα θέλει να έχει πρόσβαση με “βία”, δηλαδή να μπει με δοκιμές κωδικών για παράδειγμα, τότε έχουν πρόσβαση στο σύστημα με δικαιώματα guest χρήστη τα οποία είναι πολύ περιορισμένα ή ακόμα και να μην έχουν καθόλου πρόσβαση. Επίσης με guest δικαιώματα μπαίνουν οι χρήστες από συστήματα που δεν ανήκουν στο domain αυτού του δικτύου και προσπαθούν να αποκτήσουν πρόσβαση στο δίκτυο αυτό, αλλιώς αν ανήκουν στο domain τότε μπορούν να κάνουν πρόσβαση με τον προσωπικό τους λογαριασμό που έχει ήδη authentication.

Ένα άλλο μέτρο ασφάλειας είναι ότι λογαριασμοί που δεν έχουν ορίσει κωδικό πρόσβασης δεν μπορούν να έχουν απομακρυσμένη πρόσβαση στο δίκτυο και στους πόρους του, και στο σύστημα είναι περιορισμένοι και δεν μπορούν να τρέξουν προγράμματα χωρίς να βάλουν κάποιον κωδικό χρήστη. Βέβαια αυτός ο περιορισμός δεν έχει να κάνει με λογαριασμούς που ανήκουν ήδη στο domain και στους τοπικούς λογαριασμούς guest και για να αλλάξει αυτός ο περιορισμός γίνεται μόνο μέσω του Local Secuity Policy.

Η έκδοση των windows έχει βελτίωση επίσης στο σύστημα κρυπτογράφησης με την αρχιτεκτονική κρυπτογράφησης Encrypting File System. Η EFS έχει ως βάση την κρυπτογράφηση με δημόσιο κλειδί και οι αλγόριθμοι του είναι ο Data Encryption Standard και ο Triple DES. Έτσι αν κάποιος φάκελος κρυπτογραφηθεί που είναι σε σύστημα αρχείων NTFS, τότε αυτόματα όλοι οι υποφάκελοι και αρχεία, ακόμα και ολόκληρη βάση δεδομένων κρυπτογραφούνται και αυτά. Με αυτό τον τρόπο τα κρυπτογραφημένα αρχεία μπορεί να τα επεξεργαστεί μόνο ο χρήστης που έχει κάνει την κρυπτογράφηση, ακόμα και τα διαμοιραστεί. Η κρυπτογράφηση αυτή παραμένει ακόμα και αν μπει καινούργιο λειτουργικό στο σύστημα και έτσι διαγραφούν τα προηγούμενα μέτρα ασφαλείας. Ο EFS επίσης λειτουργεί με διαφάνεια, δηλαδή, όταν ανοίγεται ένα αρχείο, τότε αυτό αποκρυπτογραφείτε και όταν αποθηκεύεται στον δίσκο τότε κρυπτογραφείτε ξανά και αυτό γίνεται μόνο στον εξουσιοδοτημένο χρήστη που έχει τα EFS certificate και το βέβαια το ζευγάρι δημόσιων-ιδιωτικών κλειδιών κρυπτογράφησης είτε βρίσκεται στο δίκτυο, είτε δεν βρίσκεται. Αυτή η λειτουργία βέβαια του EFS μπορεί να απενεργοποιηθεί στο λειτουργικό αν δεν χρειάζεται κανείς χρήστης στο σύστημα να κρυπτογραφήσει αρχεία Στην παρακάτω φωτογραφία βλέπουμε τις επιλογές του EFS και τις επιλογές φακέλου για κρυπτογράφηση όταν είναι εκτός δικτύου



Εικόνα 5-EFS

Εικόνα 6-Encrypt Folder

Επίσης μπορούν να κρυπτογραφηθούν και αποκρυπτογραφηθούν αρχεία που είναι κοινής χρήσης στο δίκτυο και στους Web Distributed Authoring and versioning web folders στους οποίους μπορούν να αποθηκευτούν και να διαμοιραστούν με ασφάλεια κρυπτογραφημένα αρχεία στο διαδίκτυο με διαμοιρασμό αρχείων του πρωτοκόλλου http. Στην διαδικασία αποκρυπτογράφησης αρχείων σε κοινόχρηστους φακέλους είναι ότι η αποκρυπτογράφηση γίνεται στο μηχάνημα όπου είχε αποθηκευτεί το αρχείο και στέλνεται μετά σε αυτόν που το αποκρυπτογραφεί. Σε διαφορά με τα αρχεία στους Web folders όλη η διαδικασία του EFS γίνεται στον υπολογιστή και στέλνεται αρχικά κρυπτογραφημένο στον χρήστη που θέλει να κάνει την αποκρυπτογράφηση και έτσι δεν μπορούν να διαβαστούν τα αρχεία σε τυχών επίθεση κατά την μεταφορά τους.

Όσον αφορά την αποθήκευση των κλειδιών για τις κρυπτογραφήσεις, τα δημόσια κλειδιά αποθηκεύονται σε ένα χώρο προσωπικών πιστοποιητικών για κάθε λογαριασμό του λειτουργικού συστήματος ξεχωριστά με την μορφή κειμένου επειδή υπογράφονται ψηφιακά από τις αρμόδιες αρχές πιστοποίησης και γράφονται στην registry κάθε φορά που ανοίγει ο ανάλογος λογαριασμός . Αν σε περίπτωση που αυτός ο λογαριασμός μπαίνει και σε άλλα συστήματα τότε αυτά τα κλειδιά μπορούν να αποθηκευτούν οπουδήποτε και να "ακολουθούν" τον λογαριασμό στον σύστημα του domain που έκανε πρόσβαση.

Η αποθήκευση τώρα των ιδιωτικών κλειδιών κρυπτογράφησης γίνεται και αυτή ξεχωριστά για κάθε λογαριασμό σε διαφορετικό φάκελο από αυτόν για τα δημόσια κλειδιά που κρυπτογραφούνται με συμμετρική κρυπτογράφηση με το master key του χρήστη που αυτό δημιουργεί έναν μεγάλο τυχαίο αριθμό και σε περίπτωση που ο λογαριασμός μπει από διαφορετικό μηχάνημα στο domain τότε αποθηκεύεται σε συγκεκριμένο φάκελο μέχρι αυτός ο υπολογιστής να κάνει επανεκκίνηση ή αποσυνδεθεί ο λογαριασμός αυτός.

Για την διαδικασία ανανέωσης ενός πιστοποιητικού, ο χρήστης μπορεί να κάνει ένα request με την διαδικασία του autoenrollment και ολοκληρώνεται με την διαδικασία έγκρισης και

εγκαθίστανται τα νέα πιστοποιητικά αυτόματα στο σύστημα. Παρακάτω βλέπουμε φωτογραφία με το παράθυρο για την επιλογή του autoenrollment

Εικόνα 7-autoenrollment

Τα XP επίσης έφεραν την επιλογή του credentials user interface το οποίο είναι μια λύση για εξουσιοδοτημένη πρόσβαση σε συγκεκριμένους πόρους του συστήματος. Ουσιαστικά αυτό είναι ένα παράθυρο διαλόγου όπου ζητείτε όνομα λογαριασμού και κωδικός πρόσβασης για εξουσιοδότηση και η αποθήκευση αυτών των στοιχείων γίνεται με πακέτα πιστοποίησης του συστήματος και πρόσβαση σε αυτά από τα Local Security Settings που αυτά χρειάζονται για ελεγχθεί αν αυτός ο χρήστης έχει ξαναβάλει τα στοιχεία και άλλη φορά και είχε εξουσιοδοτηθεί στο παρελθόν ή ακόμα και την πρώτη φορά. Παρακάτω βλέπουμε φωτογραφία με αυτό το παράθυρο διαλόγου

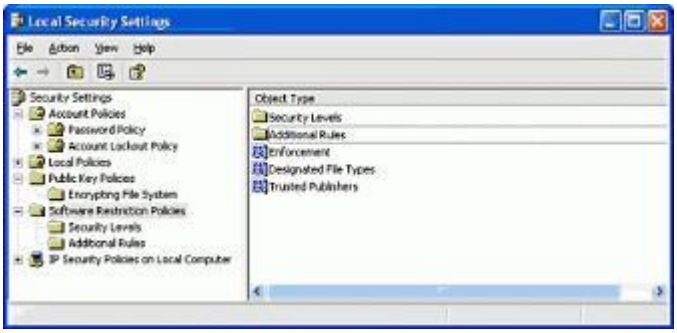
Εικόνα 8-Credential User Interface

Ένας διαχειριστής μπορεί να προσθέσει, είτε α αφαιρέσει, είτε ακόμα να επεξεργαστεί τα στοιχεία των credentials των χρηστών που θα έχουν πρόσβαση σε αυτούς τους πόρους που χρησιμοποιούν το credentials user interface.

Στα professional XP υπάρχουν διαφορές στις τεχνολογίες του διαμοιρασμού σύνδεσης στο διαδίκτυο και στο firewall. Στον διαμοιρασμό σύνδεσης ο διαχειριστής του domain μπορεί να αποτρέψει κάποιον λογαριασμό που ανήκει στην ομάδα που μπορεί να διαμοιράσει αλλά έχει συνδεθεί από μηχάνημα εξωτερικά του domain να χρησιμοποιήσει σε άλλο δίκτυο την τεχνολογία διαμοιρασμού.

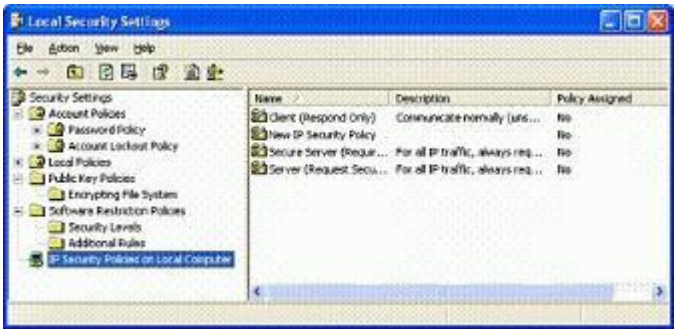
Όσον αφορά το internet connection firewall ισχύει το ίδιο με το παραπάνω και έχει προστασία η συσκευή και αν συνδεθεί σε διαφορετικό δίκτυο από αυτό του domain όπου ανήκει, είτε να μην έχει προστασία από το firewall. Η διαδικασία που ακολουθεί αυτό το firewall είναι να φιλτράρει τις συνδέσεις που προσπαθούν να γίνουν κοιτώντας έναν "πίνακα" ροής που περιέχει επιθυμητές συνδέσεις που μπορούν να γίνουν και αν δεν ανήκει σε αυτόν τον πίνακα, τότε η σύνδεση απορρίπτεται.

Κάτι πολύ αξιοσημείωτο είναι ότι ο διαχειριστής μπορεί να ελέγξει ποιες εφαρμογές θα έχουν την δυνατότητα να εκτελεστούν και από ποιόν χρήστη ή ακόμα και από ποιο μηχάνημα πάνε να εκτελεστούν και έτσι μπορούν να αποτραπούν από το να εκτελεστούν αρκετά κακόβουλα προγράμματα ακόμα και αν προσπαθούν να τα εκτελέσουν χρήστες του συστήματος με λογαριασμό, είτε ακόμα και να ορίσει κάποια προγράμματα που δεν θα μπορούν ή θα μπορούν να εκτελούνται όποτε αυτό ζητηθεί. Ο έλεγχος αυτός για να οριστεί κάποιο πρόγραμμα μπορεί να γίνει μέσω σύγκρισης των hash code των προγραμμάτων, είτε μέσω του φακέλου του προγράμματος, είτε μέσω ελέγχου αν το πρόγραμμα έχει συγκεκριμένη πιστοποίηση, είτε από ποιόν ιστότοπο πάει αυτό το πρόγραμμα να εκτελεστεί. Επίσης μπορεί να ελέγξει ο διαχειριστής ακόμα και ψηφιακά υπογεγραμμένα προγράμματα μέσω του ActiveX που ελέγχει αν το πρόγραμμα βρίσκεται σε λίστα με έμπιστους εκδότες πιστοποιητικών, είτε μπορούν να ελεγχθούν μέσω του windows installer που ελέγχει την ψηφιακή υπογραφή, είτε χρησιμοποιώντας script του visual basic που μπορούν να φέρουν ψηφιακή υπογραφή. Παρακάτω βλέπουμε φωτογραφία με ρυθμίσεις των πολιτικών ελέγχου προγραμμάτων



Εικόνα 9-policies

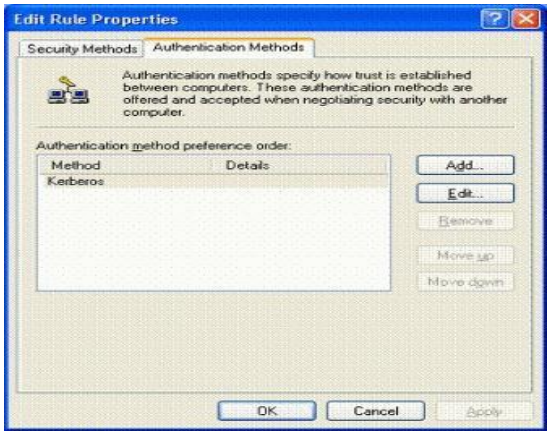
Κάτι πολύ σημαντικό που ενσωματώνουν τα Windows XP καθώς και τα Windows 2000 είναι το Internet Protocol Security το οποίο παρέχει αυθεντικότητα και ακεραιότητα, εμπιστευτικότητα των δεδομένων που μεταφέρονται κατά τις επικοινωνίες tcp/ip και την προστασία από εσωτερικές ή εξωτερικές επιθέσεις από το δίκτυο σε server και client μηχανήματα, όπως για παράδειγμα το sniffing, man in the middle attack, τροποποίηση δεδομένων, πλαστογράφηση ταυτότητας, denial of service, επίθεση στο στρώμα εφαρμογής. Αυτήν την διαδικασία την κάνει με μηχανισμούς που έχουν ως βάση την κρυπτογραφία με έναν αλγόριθμο κρυπτογραφίας και ένα κλειδί κρυπτογραφίας, δηλαδή κρυπτογραφώντας και κάνοντας hashing στα πακέτα που μεταφέρονται. Ενεργοποιείται η όλη διαδικασία μόλις πάει να ξεκινήσει μια επικοινωνία μεταξύ δύο μεριών, δηλαδή κατά την φάση του negotiation πριν ξεκινήσει η επικοινωνία οι μέθοδοι της αυθεντικότητας, κρυπτογραφίας, tunneling και hashing του Internet Protocol Security ενεργοποιούνται. Έτσι τα κλειδιά δημιουργούνται τοπικά σε κάθε μια από τις δυο μεριές για να πετύχει ο στόχος της αυθεντικότητας και μετά ξεκινάει η επικοινωνία. Σε κάθε επικοινωνία ορίζεται το επίπεδο ασφάλειας που θα υπάρχει εξαρτώμενο από το είδος της επικοινωνίας. Παρακάτω βλέπουμε φωτογραφία με τις ρυθμίσεις του Internet Protocol Security



Εικόνα 10-Internet Protocol Security

Όσον αφορά την υποστήριξη του λογισμικού σε smart cards που η δουλεία τους είναι η αποθήκευση πιστοποιητικών και ιδιωτικών κλειδιών για επίτευξη αυθεντικότητας, ανταλλαγής κλειδών και ψηφιακή υπογραφή με ευέλικτο και ασφαλή τρόπο αποθήκευσης και σε πολλά συστήματα. Για να έχει κάποιος πρόσβαση σε αυτή χρειάζεται να εισάγει έναν αριθμό PIN βάζοντας την κάρτα σε ένα smart card reader που στην διαδικασία ελέγχου του PIN ένας συνδυασμός κλειδιών ιδιωτικού-δημόσιου κρυπτογραφίας κάνουν την κρυπτογράφηση και αποκρυπτογράφηση και μεταφέρονται με τον κωδικό για να γίνει ο έλεγχος στο Kerberos Key Distribution Center . Επίσης ο κάτοχος μπορεί να ξέρει αν και κάποιος άλλος προσπαθούσε να εισάγει τον αριθμό. Επιπρόσθετα τα PIN δεν μεταφέρονται μέσα στο διαδίκτυο κατά την εισαγωγή τους που αυτό κατά κάποιον τρόπο τους κάνει πιο ασφαλές από κωδικούς πρόσβασης, καθώς και το κλείδωμα της κάρτας μετά από κάποιον αριθμό λάθους εισαγωγής PIN.

Το Kerberos v5 από το Kerberos Key Distribution Center που αναφέρθηκε είναι πρωτόκολλο προσφέρει την αυθεντικότητα σε επικοινωνίες σε διάφορα συστήματα στις επικοινωνίες μεταξύ τους με ένα μυστικό κλειδί κρυπτογραφίας και κατά την μεταφορά στοιχείων πρόσβασης στο δίκτυο. Στην διαδικασία για την επίτευξη αυθεντικότητας, που λειτουργεί με διαφάνεια, δημιουργείται ένας authenticator το οποίο ουσιαστικά είναι ένα time stamp που μαζί με την πληροφορία που έρχεται ελέγχει αν τα δεδομένα έχουν ξαναχρησιμοποιηθεί. Στην συνέχεια ένας νέος authenticator δημιουργείται και με τις κρυπτογραφημένες πληροφορίες από το Kerberos Key Distribution Center ελέγχει για την ακεραιότητα των πληροφοριών δηλαδή του PIN με τα κλειδιά και αν γίνει η πιστοποίηση αυτή δημιουργείται ένα ticket το οποίο φέρει τις πληροφορίες του χρήστη κρυπτογραφημένες και με το οποίο έτσι ο χρήστης έχει πρόσβαση χωρίς να χρειάζεται πάλι η διαδικασία πιστοποίησης για την χρονική περίοδο που το ticket είναι ενεργό. Στην παρακάτω φωτογραφία βλέπουμε τις ιδιότητες όσον αφορά τους κανονισμούς αυθεντικότητας



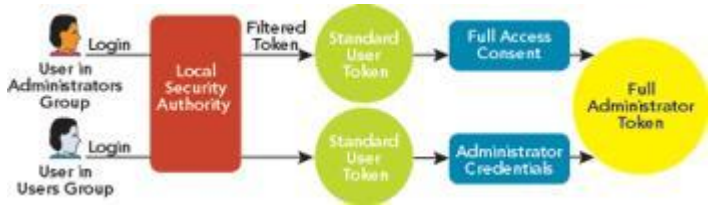
Εικόνα 11-authentication

3 Windows Vista

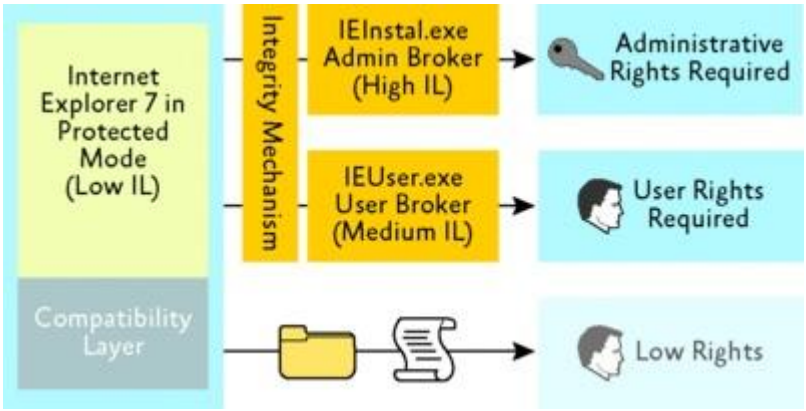
Τα Windows Vista εκδόθηκαν το 2006 και είχαν αρκετές αλλαγές στην ασφάλεια σε σχέση με τα Windows XP καθώς και βελτιώσεις σε ήδη υπάρχων τεχνολογίες, όπως την κρυπτογραφία, των έλεγχο των λογαριασμών χρηστών, windows defender, υπηρεσίες ελέγχου δικαιωμάτων χρηστών και αρχείων και αρκετά άλλα.

Αρχικά ας δούμε ότι αφορά τον έλεγχο των λογαριασμών χρηστών. Με την χρήση της τεχνολογίας code integrity εξασφαλίζει κάποιος ότι καθετί εκτελέσιμο του συστήματος του δεν έχει αλλοιωθεί από τυχών επίθεση στο σύστημα και ότι δεν τρέχουν κακόβουλα προγράμματα οδήγησης. Η τεχνολογία αυτή ενεργοποιείται με το που ξεκινήσει το λειτουργικό σύστημα και έτσι γίνεται έλεγχος για το αν έχει αλλοιωθεί κάτι στον πυρήνα του συστήματος, στο Hardware abstraction Layer και στους προγράμματα οδήγησης που τρέχουν κατά την εκκίνηση του λειτουργικού και το αν τρέχουν κακόβουλα προγράμματα οδήγησης στις μνήμες του πυρήνα και στις δυναμικές βιβλιοθήκες που είναι υπεύθυνες για την κρυπτογράφηση με το να ελεγχθεί η ψηφιακή υπογραφή τους, σε σύγκριση με την προηγούμενη φορά που ήταν ανοιχτό το λειτουργικό σύστημα.

Με την χρήση της υπηρεσίας User Account Control και όταν αυτή είναι ενεργοποιημένη από τεχνολογίες όπως την Application Information Service, installer detection και την data virtualization. Ο συνδεδεμένος χρήστης χωρίς υποχρεωτικά να είναι διαχειριστής στο internet Explorer 7 protected mode, μπορεί να τρέξει όποιες εφαρμογές επιθυμεί οι οποίες έχουν ήδη δικαιώματα διαχειριστή ή έχουν τα ανάλογα δικαιώματα χρήστη μέσω του Application Information Service. Αν ο χρήστης που είναι συνδεδεμένος είναι διαχειριστής τότε η υπηρεσία Local Security Authoring δημιουργεί ένα token πρόσβασης για τον χρήστη παρόμοιο με το token που θα φτιαχνόταν για έναν χρήστη όπου ανήκε στην ομάδα των κανονικών χρηστών που με αυτό ο χρήστης έχει την πρόσβαση στο explorer και την επιφάνεια εργασίας, αλλά χωρίς δικαιώματα στο να αλλάξει τα δικαιώματα άλλων χρηστών που χρειάζονται πάντα δικαιώματα διαχειριστή ή να κατέχει ο χρήστης token με υψηλότερο επίπεδο δικαιωμάτων που αυτό έχει να κάνει σε ποια ομάδα χρηστών βρίσκεται και τι δικαιώματα έχει αυτή η ομάδα και οι χρήστες της. Στις παρακάτω φωτογραφίες φαίνεται η διαδικασία που μπαίνουν στο λειτουργικό δυο διαφορετικοί χρήστες και τα token που λαμβάνουν με την υπηρεσία Local Security Authoring



Εικόνα 12-token



Εικόνα 13-token2

Επίσης με το User Account Control ο χρήστης ανεξαιρέτως δικαιωμάτων όταν πάει να εκτελέσει κάποια εφαρμογή ή χρειαστεί να τρέξει κάποια εφαρμογή μέσω κάποιας άλλης, τότε ο χρήστης ειδοποιείτε με ένα μήνυμα σε παράθυρο όπου ανοίγει και προειδοποιεί τον χρήστη ποια εφαρμογή πάει να εκτελεστεί και αυτός να επιλέξει ανάλογα με την χρήση του token της πλήρους πρόσβασης.

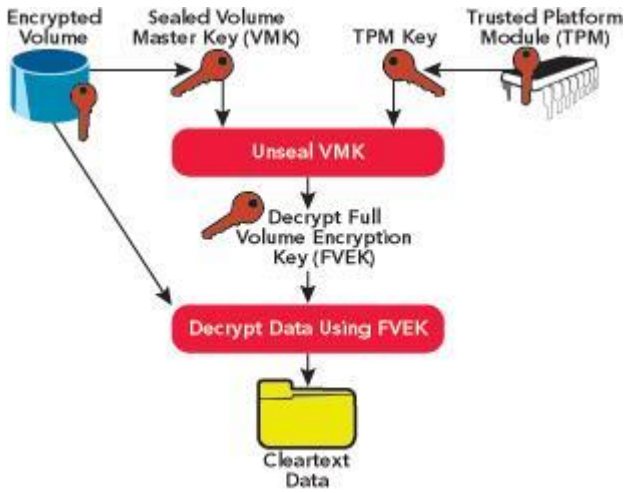
Εικόνα 14-permission window

Αν τώρα ο χρήστης που το κάνει αυτό δεν έχει δικαιώματα εκτέλεσης πάνω σε αυτό την εφαρμογή το παράθυρο που βλέπουμε παραπάνω ζητάει από τον χρήστη να εισάγει και κωδικό πρόσβασης διαχειριστή για να πάρει να δικαιώματα και να χρησιμοποιήσει το Application Information Service το token με πρόσβαση διαχειριστή, εκτός και αν αυτή η εφαρμογή που πάει να τρέξει έχει άμεση διασύνδεση με το σύστημα τότε χρειάζεται να λειτουργήσει token με πλήρη διαχειριστή. Παρακάτω στην φωτογραφία βλέπουμε το παράθυρο που ζητάει από απλό χρήστη να βάλει τον κωδικό πρόσβασης διαχειριστή για να τρέξει την εφαρμογή

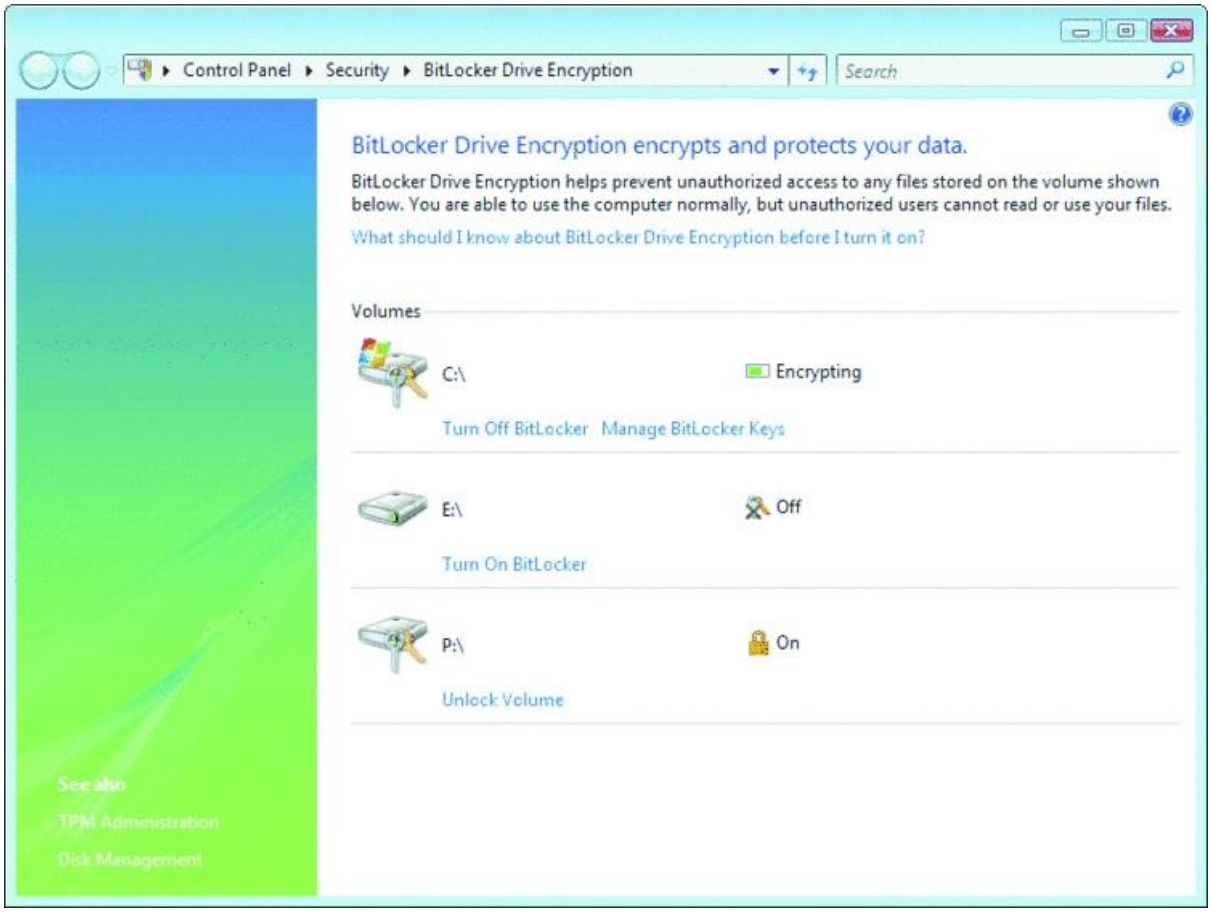
Εικόνα 15-admin password

Όσον αφορά το επίπεδο ακεραιότητας που τρέχει κάθε εφαρμογή έχει να κάνει με ποίος χρήστης τρέχει την εφαρμογή και βέβαια ένας διαχειριστής όταν τρέχει εφαρμογή τότε αυτή έχει υψηλό επίπεδο ακεραιότητας που αυτό το ορίζει ο έλεγχος Mandatory Integrity Control των Windows. Επίσης αυτό καθορίζεται και με το τι αλλαγές στο σύστημα μπορεί να κάνει η εφαρμογή, δηλαδή ο φυλλομετρητής των windows τρέχει με χαμηλό επίπεδο ακεραιότητας επειδή μπορεί να εναλλάξει στοιχεία και φακέλους που και αυτά έχουν χαμηλό επίπεδο ακεραιότητας και δεν μπορεί να πειράξει δεδομένα του χρήστη ούτε άλλα εκτελέσιμα του λειτουργικού συστήματος εκτός και αν αλλαχτούν τα Access Control Lists. Για αυτόν τον λόγο ο χρήστης που κατεβάζει αρχεία και εκτελέσιμα πρέπει να έχει επίγνωση από ποιόν φάκελο τα εκτελεί, αν έχει χαμηλό επίπεδο ακεραιότητας τότε και το εκτελέσιμο θα εκτελεστεί με χαμηλό επίπεδο και έτσι δεν θα έχει πρόσβαση στα αρχεία του χρήστη.

Ας δούμε τώρα τα μέτρα ασφάλειας όσον αφορά τα αρχεία του χρήστη είτε βρίσκονται στον σκληρό δίσκο, είναι σε σέρβερ του δικτύου, είτε μοιράζονται με άλλα άτομα. Τα windows Vista φέρνουν το BitLocker το οποίο έχει την δυνατότητα να κρυπτογραφήσει ολόκληρο σύστημα για εξασφάλιση μεγαλύτερης ασφάλειας αρχείων με την χρήση του Full Volume Encryption Key και στην συνέχεια ξανακρυπτογραφείται με την χρήση του Volume Master Key το οποίο είναι "σφραγισμένο" στο chip ασφαλείας Trusted Platform Module. Επίσης το Trusted Platform Module μπορεί από ανάλογη ρύθμιση να ζητάει PIN πριν κρυπτογραφήσει με το Volume Master Key, είτε να γίνει ρύθμιση και ένα κλειδί να αποθηκευτεί σε εξωτερικό σκληρό δίσκο/USB και να βάζει το Volume Master Key κατά την εκκίνηση του λειτουργικού συστήματος και αν δεν υπάρχει εγκατεστημένο από πριν το Trusted Platform Module, τότε το κλειδί που βρίσκεται στον εξωτερικό σκληρό αποκρυπτογραφεί στην εκκίνηση το Full Volume Encryption Key. Στην συνέχεια αν το BitLocker είναι ενεργοποιημένο τότε ξεκλειδώνεται το Volume Master Key με τις κατάλληλες πληροφορίες και αυτό με την σειρά του αποκρυπτογραφεί το Full Volume Encryption Key και μετά αυτό με την δική του σειρά αποκρυπτογραφεί την αποθηκευμένη πληροφορία. Τέλος για αυτό το θέμα υπάρχει ασφάλεια αν το κρυπτογραφημένο σύστημα πάει να ανοίξει από άλλο μηχάνημα, τότε το BitLocker πάει σε λειτουργία recovery μέχρι ότου εισαχθεί ο κωδικός recovery. Στις παρακάτω φωτογραφίες βλέπουμε την διαδικασία της αποκρυπτογράφησης του BitLocker και το παράθυρο της εφαρμογής.



Εικόνα 16-BitLocker

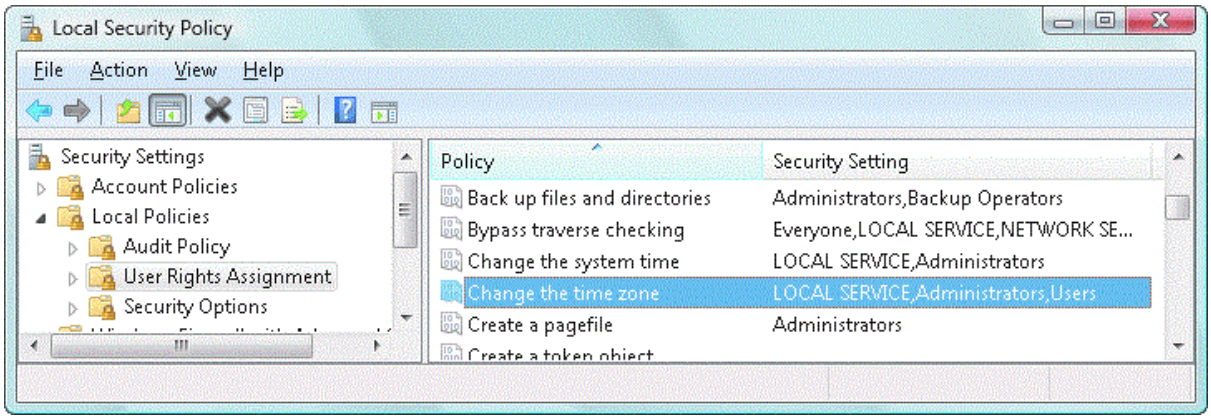


Εικόνα 17-BitLocker2

Επίσης έχει βελτιωθεί στα windows vista το σύστημα κρυπτογράφησης το οποίο υποστηρίζει πλήρως την αποθήκευση των ιδιωτικών κλειδιών του χρήστη και των κλειδιών για domain recovery καθώς και recovery πιστοποιητικών και recovery σε Public Key Infrastructure κλειδιά, σε μέσα όπως τις smart cards που κρυπτογραφούνται με το νέο Encrypting File System και σε σκληρούς δίσκους. Επίσης το λειτουργικό κατέχει tools τα οποία χρησιμοποιούνται για να γίνει back up των κλειδιών και την αποτροπή χάσιμο χρήσιμων δεδομένων. Για τους χρήστες με δικαιώματα διαχειριστή έχουν την επιλογή να ορίσουν για αυτούς την η χρήση των smart cards με ανάλογο τρόπο και τη δυνατότητα κρυπτογράφησης "χαμηλότερης δυναμικότητας". Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο του BitLocker

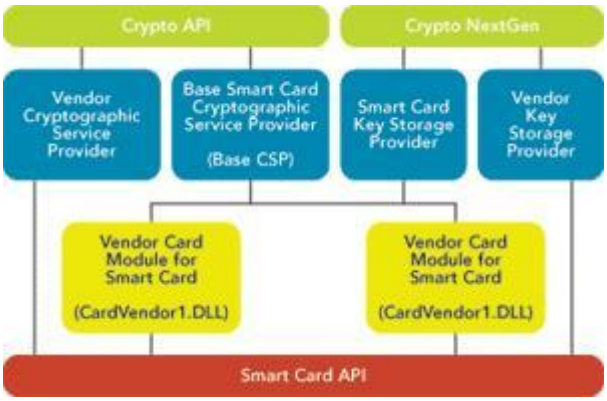
Με την έκδοση των Vista μπορούν να απαπτηχθούν πολλαπλοί μέθοδοι παρόχων για αυθεντικότητα των multifactor credentials χωρίς αυτός να διαγράφει κάποιον παροχέα single factor credentials για την διαδικασία πιστοποίησης αυθεντικότητας, βάζοντας μια εγγραφή πληροφοριών της βιβλιοθήκης στην registry και εξάγοντας έτσι το API των παρόχων αυθεντικότητας.

Επίσης μια νέα λειτουργία στο λειτουργικό είναι η προστασία εγγραφών σε συγκεκριμένες περιοχές όπως τα Program Files και την registry από το Access Control List από χρήστες που δεν έχουν τα απαραίτητα δικαιώματα και έτσι αυτή η εγγραφή δρομολογείται στον φάκελο virtual store που βρίσκεται στα αρχεία του χρήστη που προσπάθησε να κάνει την εγγραφή που απαγορεύτηκε και όλη αυτή η διαδικασία ονομάζεται data virtualization και data redirection. Αλλά όλοι οι κανονικοί χρήστες χωρίς απαραίτητα δικαιώματα διαχειριστή μπορούν να επέμβουν σε υπηρεσίες όπως την ώρα του συστήματος, τις ρυθμίσεις σύνδεσης με ασύρματο τρόπο, διαχείριση επιλογών ενέργειας όπως φωτεινότητα, εγκατάσταση κρίσιμων ενημερώσεων, ActiveX και συσκευών όπως εκτυπωτές. Στην παρακάτω φωτογραφία βλέπουμε τις πολιτικές του local security



Εικόνα 18-local security policy

Ας πάμε τώρα στο Cypto NextGen το οποίο είναι μια πλατφόρμα που επιτρέπει στους χρήστες να δημιουργήσουν δικούς τους αλγορίθμους και εφαρμογές κρυπτογράφησης με ευέλικτο τρόπο και προσφέρει επίσης τον αλγόριθμο κρυπτογράφησης Elliptic Curve Cryptography και το Base Smart Card Cryptographic Service Provider και το Key Storage Provider για τις smart cards στα Windows Vista. Στην παρακάτω φωτογραφία βλέπουμε την υποδομή λειτουργίας του Base Smart Card Cryptographic Service Provider



Εικόνα 19-BCSP

Για τα services τώρα των Vista, κάθε υπηρεσία κατέχει ένα Security Identifier το οποίο παρέχεται από το Service Hardening και έτσι η κάθε υπηρεσία επιτρέπεται σαν ασφαλές πόρος του συστήματος αν υπάρχει ανάλογη εγγραφή στα Access Control Lists βάση τον security identifier τους. Έτσι αν κάποια υπηρεσία έχει μόνο δικαιώματα write, τότε μπορεί να επέμβει σε αρχεία που αφήνουν να γίνει το write σε αυτά και έτσι προστίθεται στο λειτουργικό μια πιο αυστηρή προστασία στο τι μπορεί να επηρεάσει κάθε υπηρεσία.

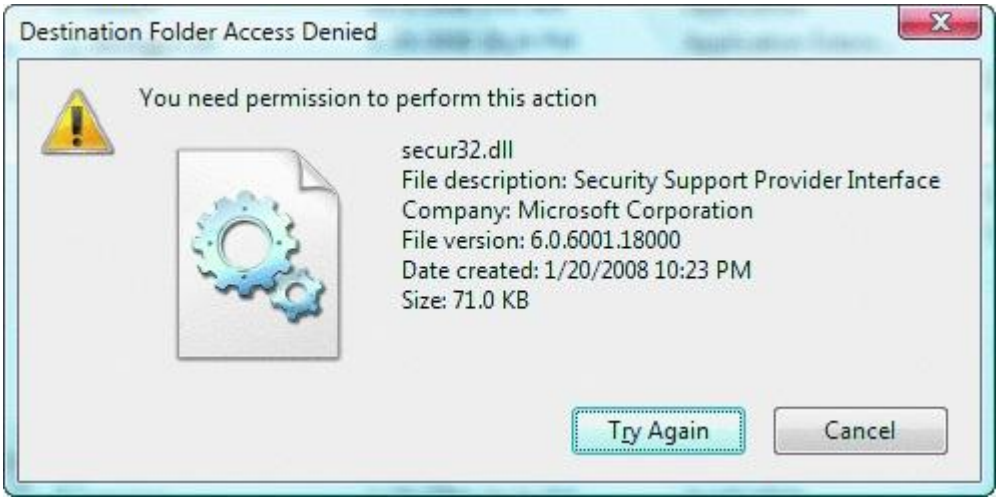
Επόμενο πολύ σημαντικό στα Vista είναι το Windows Defender το οποίο αποτρέπει το spyware, τα pop-ups σε ιστοσελίδες, επιθέσεις σε ρυθμίσεις συστήματος και επίθεση σε αρχεία του χρήστη, είτε να βρει κακόβουλα προγράμματα στο σύστημα με γρήγορο, είτε προσαρμοσμένο σκανάρισμα, καθώς και προστασία των υπάρχων αρχείων και υπηρεσιών του χρήστη και του λειτουργικού συστήματος . Επίσης αυτή η υπηρεσία παρέχει διαγραφή αρχείων δίνοντας πληροφορία για το επίπεδο επικινδυνότητας και πληροφορίες για την λειτουργικότητά τους και ενέργειες που θέλει να γίνουν σε αυτά ο χρήστης, όπως καραντίνα αυτών σε περίπτωση που είναι κακόβουλα και καχύποπτο αντίστοιχα, είτε απλά να αγνοηθούν. Η διαδικασία αυτή γίνεται όταν το interface του χρήστη στέλνει τα διαμορφωμένα δεδομένα με χρήση του Remote Procedure Call στην υπηρεσία του

Windows Defender που τρέχει στο Local Service. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο του Windows Defender

Εικόνα 20-Windows Defender

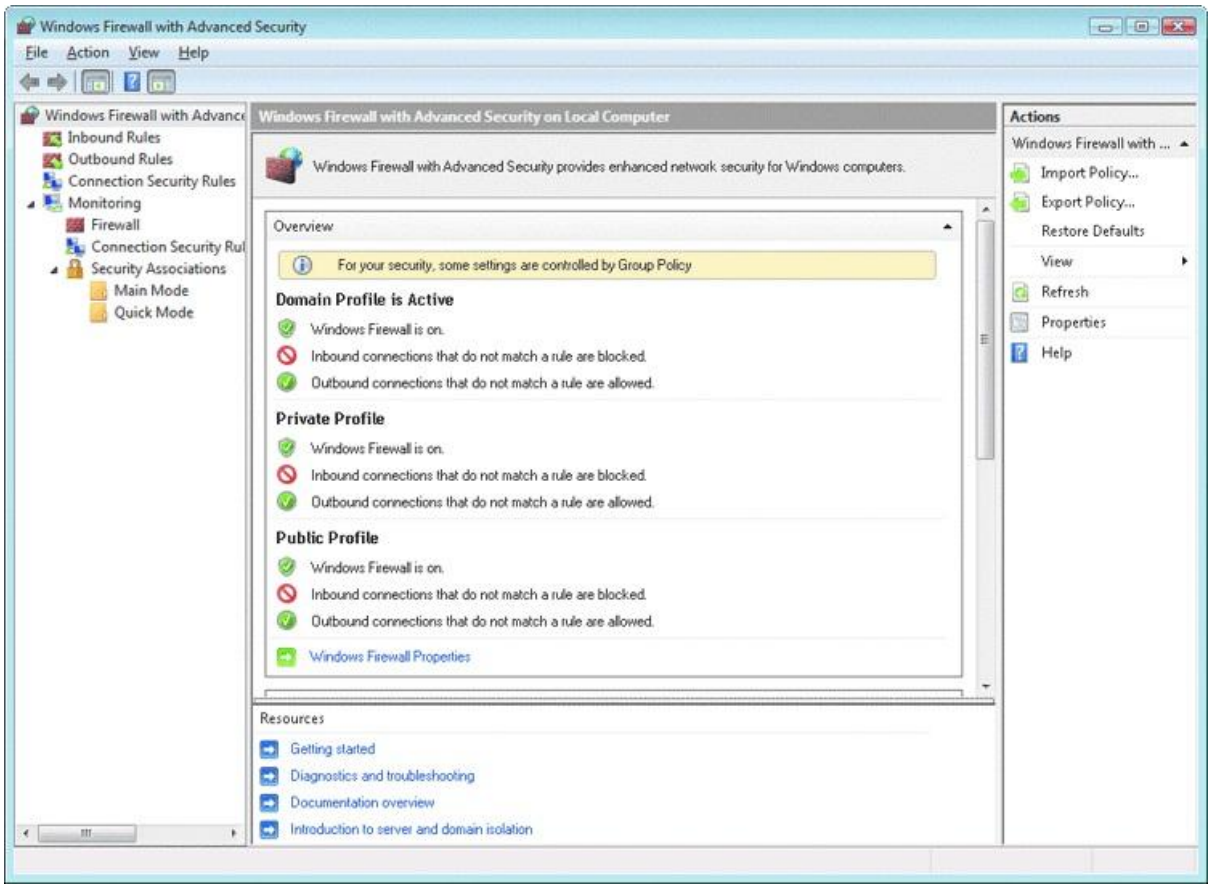
Ας δούμε τώρα τις υπηρεσίες για διαχείριση των δικαιωμάτων οι οποίες παρέχουν ασφάλεια σε αρχεία που δεν έχουν δικαίωμα να σταλούν με ηλεκτρονικό ταχυδρομείο, είτε να χρησιμοποιηθούν σε κάποιο από τα προγράμματα του Microsoft Office και σε άλλα προγράμματα με χρήση πνευματικών δικαιωμάτων παρέχοντας πιστοποιητικά χρήστη, δικαιώματα χρήσης, templates περί πολιτικής πνευματικών δικαιωμάτων και κρυπτογράφηση σε αρχεία και πληροφορίες και προστασία αυτών. Επίσης παρέχεται η προστασία δικαιωμάτων σε αρχεία με το XML Paper Specification Viewer.

Ας αναφερθούμε στην τεχνολογία τώρα του windows resource protection όπου περιορίζει την πρόσβαση σε κρίσιμα αρχεία συστήματος που αποτελούν μέρος της εγκατάστασης του λογισμικού και απαγορεύει αυτά να τροποποιηθούν ή να διαγραφούν ώστε να προσφέρεται η σταθερότητα του συστήματος ακόμα και χρήστης με δικαιώματα διαχειριστή, με μόνη εξαίρεση κάτι να παρέμβει σε αυτά είναι η υπηρεσία windows module installer. Στην παρακάτω φωτογραφία βλέπουμε περίπτωση στο να γίνει τροποποίηση σε ένα από αυτά τα αρχεία



Εικόνα 21-restriction

Κάτι τελευταίο για το λειτουργικό αυτό είναι η βελτίωση του firewall με την εισαγωγή του Windows Filtering Platform το οποίο παρέχει την λειτουργία πυρήνα του firewall και την επεκτασιμότητα υποδομής του. Αυτό σημαίνει ότι υπάρχει η δυνατότητα φιλτραρίσματος σε μέρη όπως το στρώμα εφαρμογών. Επίσης παρέχεται τώρα ο περιορισμός σε εφαρμογές, εκτελέσιμα, ομάδες χρηστών και υπηρεσιών, σε συγκεκριμένες συνδέσεις που ορίζει το Internet Protocol Security. Παρακάτω βλέπουμε το παράθυρο του ανανεωμένου firewall



Εικόνα 22-Vista Firewall

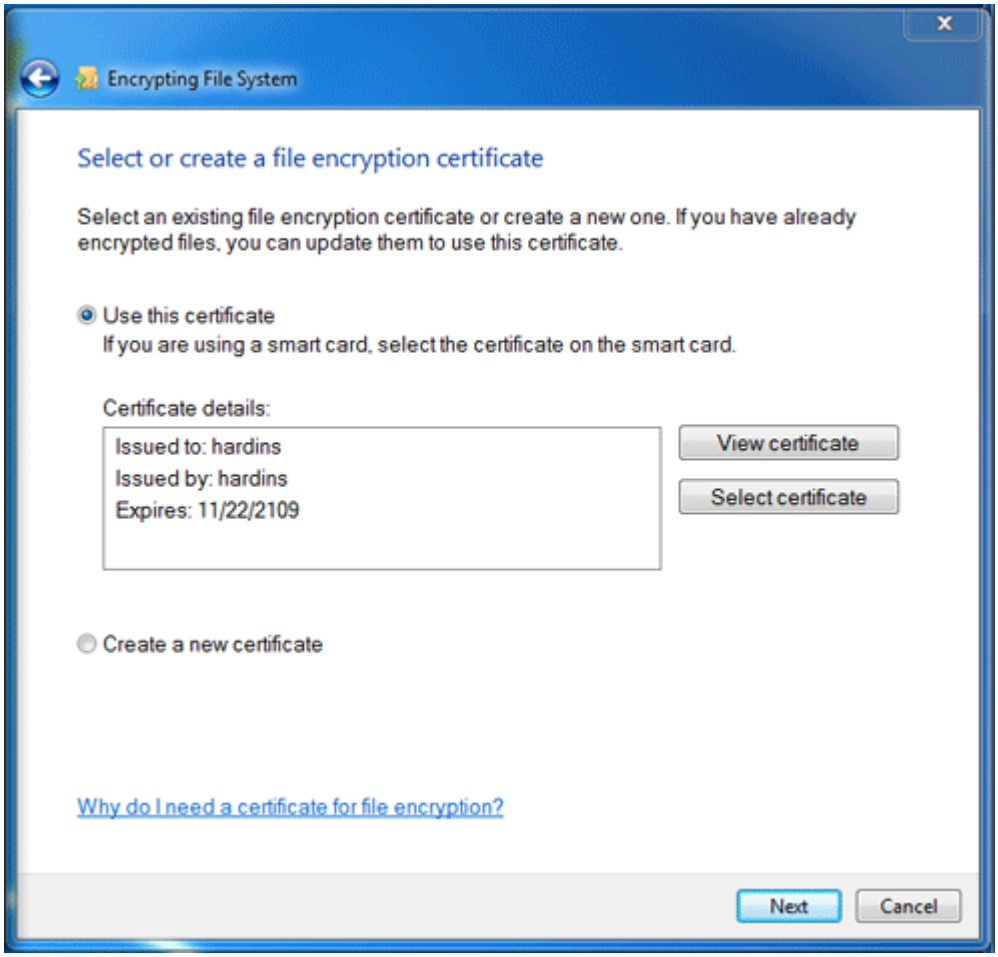
4 Windows 7

Συνεχίζουμε με την έκδοση των windows 7 που εκδόθηκαν το 2009 που εισάγουν νέα στοιχεία που αφορούν την ασφάλεια του λειτουργικού, καθώς και βελτιώσεις σε ήδη υπάρχων τεχνολογίες ασφάλειας που υπήρχαν από προηγούμενες εκδόσεις των windows.

Αρχικά, μια αλλαγή και βελτίωση που έγινε στα windows 7 σε σύγκριση με τα windows Vista είναι στο ActiveX το οποίο είναι υπεύθυνο να εγκαθιστά αντικείμενα για διευκόλυνση του χρήστη στο πρόγραμμα internet explorer με την άδεια ενός χρήστη με δικαιώματα διαχειριστή όταν ζητείτε η χρήση του από ιστοσελίδες που το υποστηρίζουν. Επίσης ένας διαχειριστής μπορεί να επιλέξει να εγκαθίστανται μόνο από ιστοσελίδες όπου ανήκουν στην λίστα του explorer την Trusted sites που έχουν τοποθετηθεί από την Group Policy και επειδή θα βρίσκονται σε αυτή την λίστα κανονικοί χρήστες domain μπορούν να εγκαθιστούν χαρακτηριστικά του ActiveX από τις συγκεκριμένες τοποθεσίες στο διαδίκτυο.

Αλλαγές έγιναν επίσης στο BitLocker που κρυπτογραφεί δεδομένα που βρίσκονται σε συσκευές όπως εξωτερικοί σκληροί δίσκοι και usb με χρήση exFAT, FAT32, FAT16 και NTFS. Οι αλλαγές είναι ότι στα windows 7 το partition που χρειάζεται δημιουργείται αυτόματα και δεν είναι ορατό στο windows explorer και έτσι δεν γράφονται σε αυτό τα δεδομένα αν δεν επιλεχθεί να γίνει κάτι τέτοιο για να λειτουργήσει το BitLocker και το μέγεθος που χρειάζεται για το system είναι 100 MB. Η διαδικασία γίνεται με χρήση κωδικού ή smart card και ενός κωδικού για recovery με 48 ψηφία που έχει την δυνατότητα να αποθηκευτεί στα Active Directory Domain Services για να χρησιμοποιηθεί αν αποτύχουν οι μέθοδοι ανάκτησης όπως η απώλεια κωδικού. Επιπλέον δυνατότητες στα windows 7 είναι ότι ο διαχειριστής μπορεί να επιλέξει ότι όλες οι αφαιρούμενες συσκευές αποθήκευσης να είναι προστατευμένες με το BitLocker, καθώς και την δυνατότητα να επιλέξει τις μεθόδους για ξεκλείδωμα του BitLocker από τις συσκευές αυτές και μεθόδους ανάκτησης των δεδομένων. Επίσης θα έχει την δυνατότητα από το Group Policy με τις απαραίτητες ρυθμίσεις και ενέργειες να έχει ένα δημόσιο κλειδί που ονομάζεται data recovery agent που είναι για όλο το domain και έτσι θα έχει δικαίωμα να ξεκλειδώσει οποιοδήποτε BitLocker στο domain το οποίο κλειδί θα πρέπει να έχει δηλωθεί στο Public Key Policies. Οι ρυθμίσεις που πρέπει να γίνουν το Group Policy για να γίνει το παραπάνω είναι να οριστούν μέθοδοι για να γίνει η ανάκτηση σε οποιοδήποτε σύστημα. Μπορεί να προστατευθεί τώρα ακόμα και σύστημα με λειτουργικό σύστημα το οποίο δεν υποστηρίζει το Trusted Platform Module.

Ας πάμε στο Encrypting File System όπου έγιναν βελτιώσεις και στην κρυπτογράφηση και ενσωματώνει το Advanced Encryption Standard, τον Secure Hash Algorithm, την Elliptic Curve Cryptography και την κρυπτογραφία για smart cards. Έτσι με το Elliptic Curve Cryptography το Encrypting File System έχει συμβατότητα με την κρυπτογράφηση Suite B και την υποστήριξη κρυπτογραφημένων αρχείων που δημιουργήθηκαν σε προηγούμενες εκδόσεις των windows. Επίσης βοηθάει στο να φτιάχνονται αυτό-υπογεγραμμένα πιστοποιητικά όπου ορίζεται από τον χρήστη το μέγεθος του κλειδιού για την κρυπτογράφηση, όταν δεν είναι διαθέσιμο κάποιο Certification Authority τα οποία όμως δεν υποστηρίζονται από όλους τους οργανισμούς για λόγους ασφαλείας. Επίσης ένας διαχειριστής έχει την δυνατότητα να αρνείται το σύστημα να δημιουργούνται αρχεία με το Encrypting File System που δεν υποστηρίζουν το Suite B. Αυτά που εμπεριέχονται στο Suite B είναι ο Advanced Encryption Standard128, Elliptic Curve Digital Signature Algorithm, Elliptic Curve Diffie Hellman, Secure Hash Algorithm, πρωτόκολλο αυθεντικότητας Transport Security Layer καθώς και το Encrypting File System. Παρακάτω βλέπουμε φωτογραφία με ένα παράθυρο του Encrypting File System



Εικόνα 23-Encrypting File System

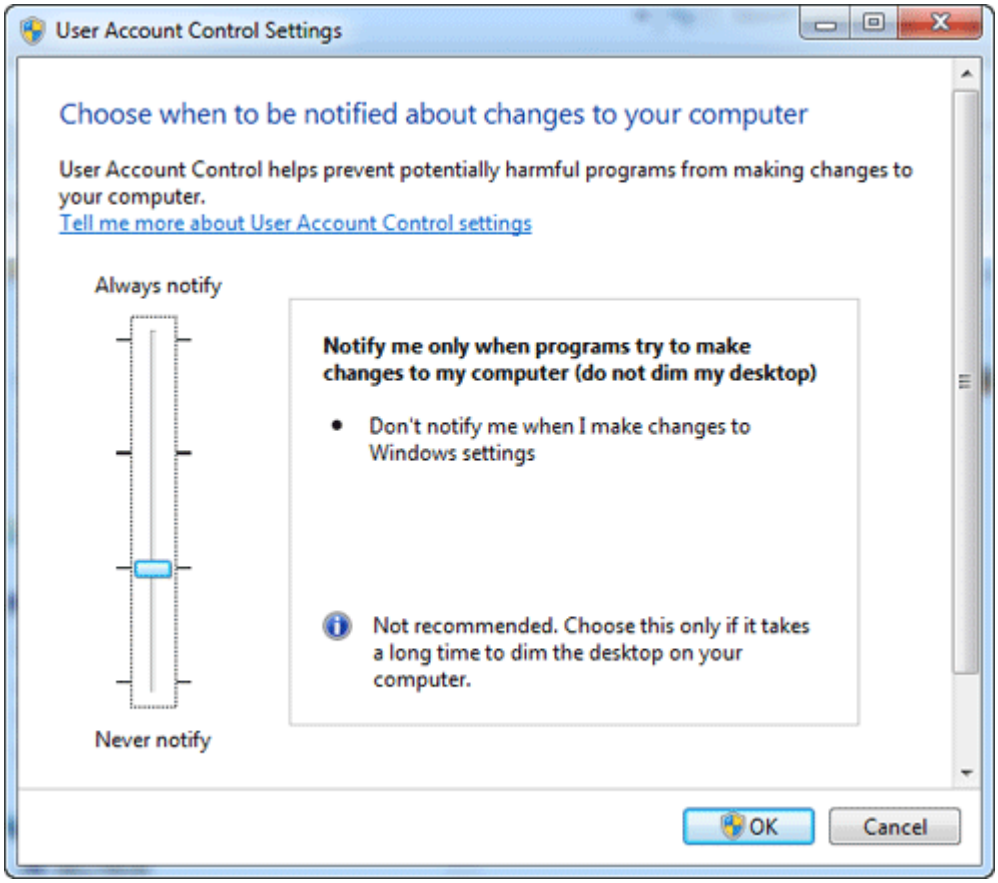
Κάποιες αλλαγές υπάρχουν επίσης και στην υπηρεσία Kerberos V5 όπου οι σουίτες DES cipher είναι απενεργοποιημένες, αλλά μπορούν να ενεργοποιηθούν αν αυτές χρειαστούν και αντίστοιχα έχουν ενεργοποιηθεί οι σουίτες AES256 και AES128 και RC4. Επίσης υποστηρίζεται τώρα η Elliptic Curve Cryptography για smart cards που χρησιμοποιούν το πιστοποιητικό X.509.

Στο πρωτόκολλο αυθεντικότητας NTML έχουμε αλλαγές επίσης. Αυτές είναι ότι χρειάζεται ένα ελάχιστο όριο κρυπτογράφησης των 128 bit είτε για υπολογιστές server και client για την εγκατάσταση του λογισμικού, όπου και οι συσκευές δικτύου και τα λειτουργικά συστήματα πρέπει να το υποστηρίζουν αυτό. Ακόμα και όταν γίνεται επικοινωνία με συστήματα όπου έχουν προηγούμενες εκδόσεις τότε λειτουργεί η τεχνολογία του NTML με σχετική ρύθμιση.

Επιπρόσθετα, αλλαγές υπάρχουν και στις πολιτικές ελέγχου ασφάλειας χρησιμοποιώντας την Local Computer Policy όπου μπορούν να γίνουν τώρα πιο λεπτομερείς αλλαγές μέσω της επιλογής Advanced Audit Policy Configuration που επιτυγχάνεται μέσω των Group Policy. Έτσι υπάρχει βελτίωση στα προειδοποιητικά μηνύματα εφαρμογών που παρουσιάζουν την αιτία που βλέπει ο χρήστης αυτό το μήνυμα και ακόμα την δυνατότητα παρακολούθησης επιλεγμένων αντικειμένων με την χρήση του Group Policy Object με σκοπό την καλύτερη κατανόηση των εφαρμογών που πάνε να εκτελεστούν είτε με επιτυχία, είτε με αποτυχία.

Αλλαγή έχουμε και στην αλληλεπίδραση του χρήστη με το Trusted Platform Module μέσω του Microsoft Management Console που αυτό είναι γνωστό ως Trusted Platform Module services που χρησιμοποιείται για την διαχείριση του Trusted Platform Module hardware στο κάθε μηχάνημα και την επίτευξη του reset στο Trusted Platform Module lockout value mode η οποία βοηθάει σε αποτροπή αλλοιώσεων και επιθέσεων στο σύστημα στέλνοντας ανάλογα μηνύματα για ένα συγκεκριμένο χρονικό διάστημα ή μέχρι να τερματιστεί ο υπολογιστής.

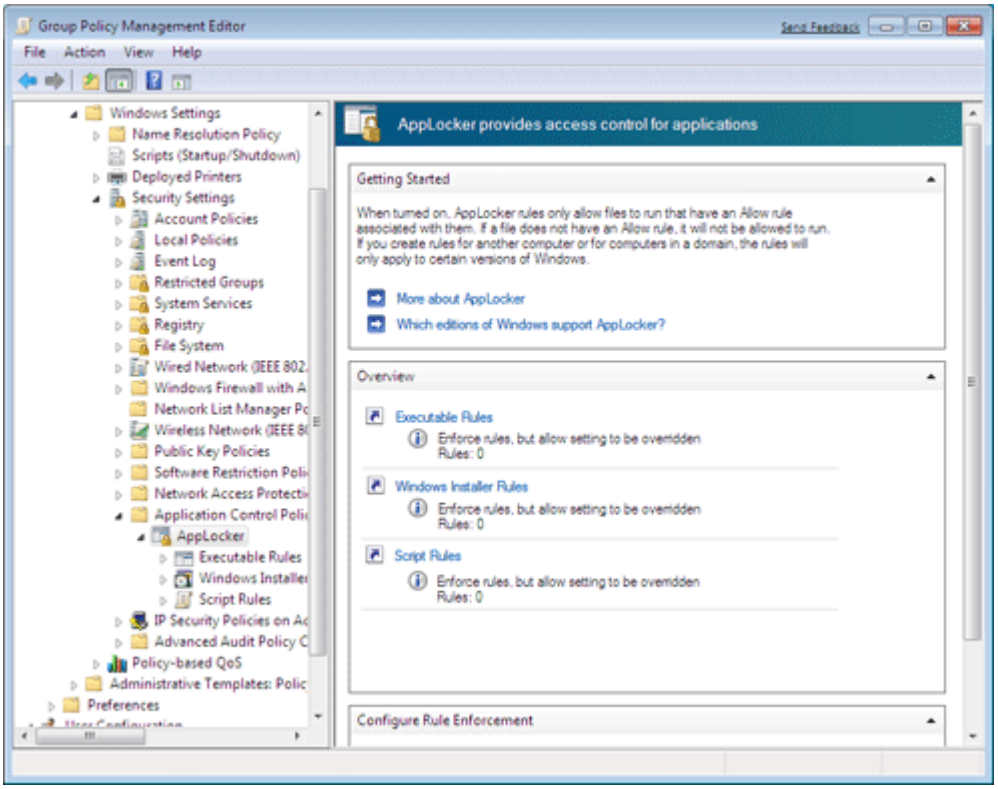
Ας πάμε τώρα σε σημαντικές αλλαγές που αφορούν την διαχείριση χρηστών όσον αφορά την λειτουργικότητα. Αυτές είναι ότι ένας κανονικός χρήστης μπορεί να κάνει παραπάνω πράγματα χωρίς την άδεια διαχειριστή, επίσης ένας διαχειριστής αλλάζει τα δικαιώματα των υπόλοιπων χρηστών στο υπολογιστή από τον πίνακα ελέγχου, τώρα παρέχονται επιπλέον πολιτικές τοπικής ασφάλειας που επιτρέπουν σε τοπικούς διαχειριστές να αλλάζουν τα μηνύματα που αφορούν τον έλεγχο διαχείρισης χρηστών για τους κανονικούς χρήστες μέσω των Local Security Policies και σε Admin Approval Mode. Αυτά που μπορεί να κάνει ένας κανονικός χρήστης χωρίς άδεια διαχειριστή είναι να μπορεί να εγκαθιστά ενημερώσεις των windows και προγράμματα οδήγησης αυτών, να έχει την δυνατότητα να μπορεί να δει τις ρυθμίσεις των windows, να μπορεί να χρησιμοποιεί και να επικοινωνεί με συσκευές Bluetooth, καθώς να μπορεί να κάνει reset σε αντάπτορα δικτύου, διάγνωση αυτού και repair, εγκατάσταση και αφαίρεση προγραμμάτων που δεν κάνουν αλλαγές στον υπολογιστή, σύνδεση συσκευών, back-up, αλλαγές στην επιφάνεια εργασίας και αλλαγές στις ρυθμίσεις εξατομίκευσης. Όσον αφορά τις αλλαγές ενός χρήστη διαχειριστή, αυτός μπορεί να ρυθμίσει τις ειδοποιήσεις του συστήματος σε τέσσερις κατηγορίες και στην υπηρεσία εγκατάστασης ActiveX να επιτρέπει την αλλαγή των ρυθμίσεων του ActiveX μέσων του Group Policy. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο του user account control με τα τέσσερα επίπεδα ειδοποιήσεων



Εικόνα 24-notification's level

Ας πάμε τώρα σε κάτι καινούργιο του λειτουργικού, που ονομάζεται AppLocker το οποίο είναι η νέα έκδοση του Software Restriction Policies το οποίο έλεγχε ποίες εφαρμογές μπορούν να εκτελεστούν. Στο AppLocker ο χρήστης μπορεί να γράψει κανόνες για το ποία προγράμματα θα εκτελούνται ή δεν θα εκτελούνται ανάλογα με το όνομα του προγράμματος ή προϊόντος, τον εκδότη, τον αριθμό έκδοσης, την ψηφιακή υπογραφή και έτσι δεν χρειάζεται να γίνει αλλαγή στον προηγούμενο κανόνα με την χρήση hash ή τοποθεσίας της εφαρμογής. Επίσης από ένα διαχειριστή μπορεί να αποφασιστούν οι κανόνες για εφαρμογές σε χρήστες σε ένα συγκεκριμένο σύστημα. Αν οι

κανόνες ισχύουν για ένα συγκεκριμένο πρόγραμμα, αυτό δεν σημαίνει ότι ισχύουν οι κανόνες και για τις βιβλιοθήκες ή άλλα αρχεία όπως msi που βρίσκονται μαζί τους στον φάκελο και πρέπει να δημιουργηθεί ξεχωριστός κανόνας για αυτά τα αρχεία. Επίσης στο AppLocker υπάρχει η επιλογή του να τεσταριστεί του πως θα επιδρούσε ο κάθε κανόνας, χωρίς αυτό να γίνει αναγκαστικά πράξη και τέλος μπορεί να δημιουργηθούν rules creation wizards οι οποίοι θα φτιάχνουν αυτόματα κανόνες προγεγραμμένους. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο του AppLocker



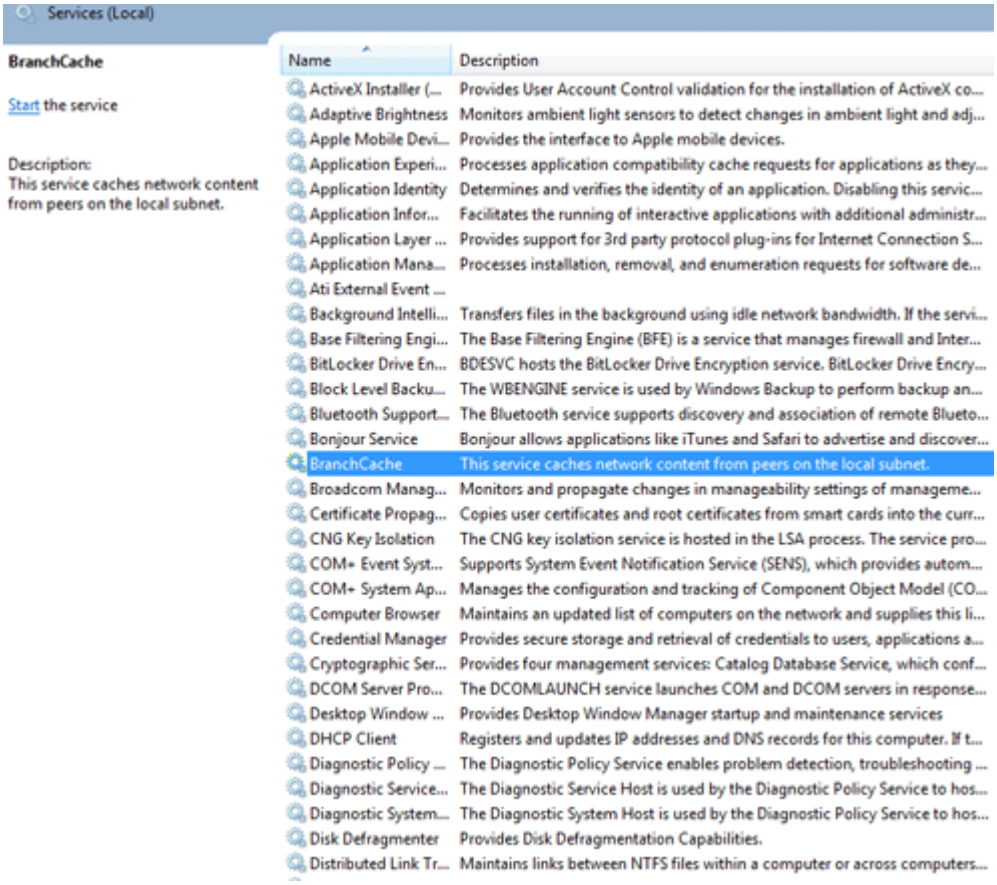
Εικόνα 25-AppLocker

Συνεχίζοντας με κάτι άλλο καινούργιο το οποίο είναι οι ρυθμίσεις για Enhanced Storage Access. Οι συσκευές του Enhanced Storage είναι αυτές που υποστηρίζουν το πρωτόκολλο IEEE 1667 που προσφέρουν αυθεντικότητα σε επίπεδο υλικού των συσκευών αυτών και με το Enhanced Storage Access μπορεί κάποιος χρήστης να διαχειριστεί τις πολιτικές των συσκευών μέσω του Group Policy που υποστηρίζουν αυθεντικότητα κωδικού πρόσβασης και πιστοποιητικού. Αυτές οι ρυθμίσεις είναι το να μπορούν οι χρήστες να βάζουν πιστοποιητικά στις συσκευές που υποστηρίζουν το Certificate Authentication Silo, επίσης να μπορούν οι συσκευές αυτές να συνδέονται σε usb root hubs, να επιτρέπονται μόνο επιλεγμένες συσκευές ανάλογα με κατασκευαστή ή ID να συνδεθούν στον υπολογιστή, είτε να απαγορευτεί η επιλογή του να εισάγεται κωδικός πρόσβασης για ξεκλείδωμα αυτών των συσκευών, περιορισμός χρήσης αυτών και κλείδωμα τους όταν κλειδώνεται και ο υπολογιστής. Αυτές οι πολιτικές πάνε σε όλους τους υπολογιστές που τυχών βρίσκονται στο domain και κάθε πολιτική έχει το δικό της registry key.

Επόμενη προσθήκη είναι και το Negotiate Authentication Protocol package που είναι ένα security support provider που παρέχει αυθεντικότητα και ασφάλεια και υποστηρίζει επίσης τα NTLM και Kerberos. Αυτό γίνεται με το να γίνεται επικοινωνία με το πρωτόκολλο αυθεντικότητας όταν γίνονται αιτήσεις για αυθεντικοποίηση από υπολογιστές του domain. Το NTLM που αναφέρθηκε είναι ένα πρωτόκολλο αυθεντικότητας το οποίο πιστοποιεί τα μηχανήματα που κάνουν αίτηση χωρίς αυτά να στέλνουν κάποιον κωδικό πρόσβασης στον εξυπηρετητή, με μηνύματα για διαπραγμάτευση της αίτησης, έλεγχος για την αυθεντικότητα του αιτών υπολογιστή και πραγματοποίηση της αυθεντικοποίησης. Για το Kerberos που είναι ένας μηχανισμό αυθεντικοποίησης βασισμένο σε ένα

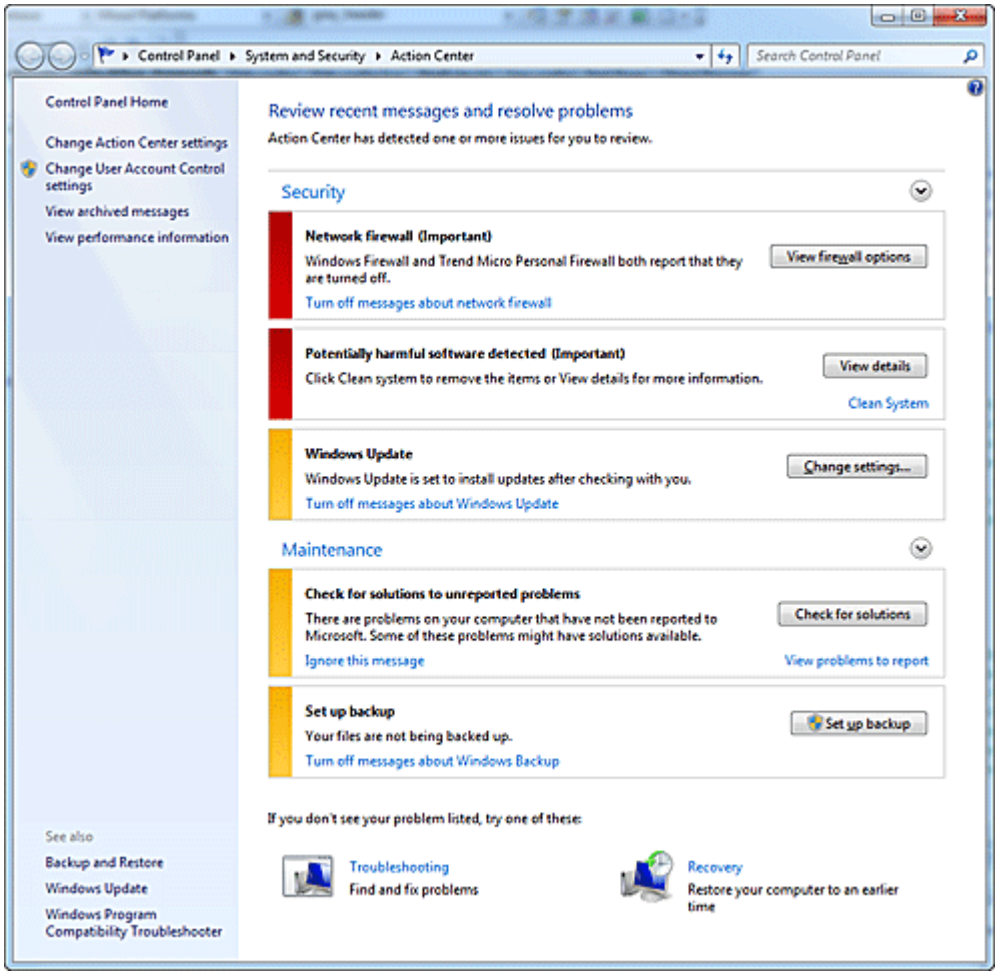
πρωτόκολλο αυθεντικότητας έχει αναφερθεί παραπάνω. Ένα extension του Negotiate Authentication Protocol package είναι το NegoExts που είναι και αυτό πακέτο αυθεντικότητας που δρα για εφαρμογές της Microsoft και άλλων εταιριών λογισμικού. Αυτές οι δράσεις είναι ότι μπορεί να κάνει τα αρχεία να μπορούν να είναι προσβάσιμα σε σελίδες SharePoint και να μπορούν να τροποποιηθούν με εφαρμογές του Microsoft office καθώς και του του Microsoft office live, υθεντικοποίηση χρηστών μέσω του windows live και CardSpace. Οι όλες αυτές διαδικασίες επιτυγχάνονται με το να φορτώνεται το extension στο Local System Authority κατά την εκκίνηση και αν γίνει αίτηση, ανάλογα πάντα των αιτών, το extension επικοινωνεί με το SSP και με τα στοιχεία και πολιτικές που του δίνονται τα κρυπτογραφεί και τα στέλνει στο SSP και αυτό δημιουργεί ένα token ασφαλείας και αν αυτή η διαδικασία αποτύχει τότε θα εμφανιστεί μήνυμα αποτυχίας χωρίς να υπάρξουν άλλοι μέθοδοι αυθεντικότητας μέσω αυτού.

Μια άλλη τεχνολογία που ήρθε είναι το BranchCache το οποίο δημιουργεί μια cache μνήμη ενός αρχείου ή μιας εφαρμογής τοπικά και αν κάποιος χρήστης του τοπικού υποδικτύου με τα ανάλογα δικαιώματα χρειάζεται αυτό το αρχείο, μπορεί να το κατεβάζει από αυτή την cache μνήμη και όχι από το δίκτυο. Παρακάτω βλέπουμε φωτογραφία με αυτή την επιλογή



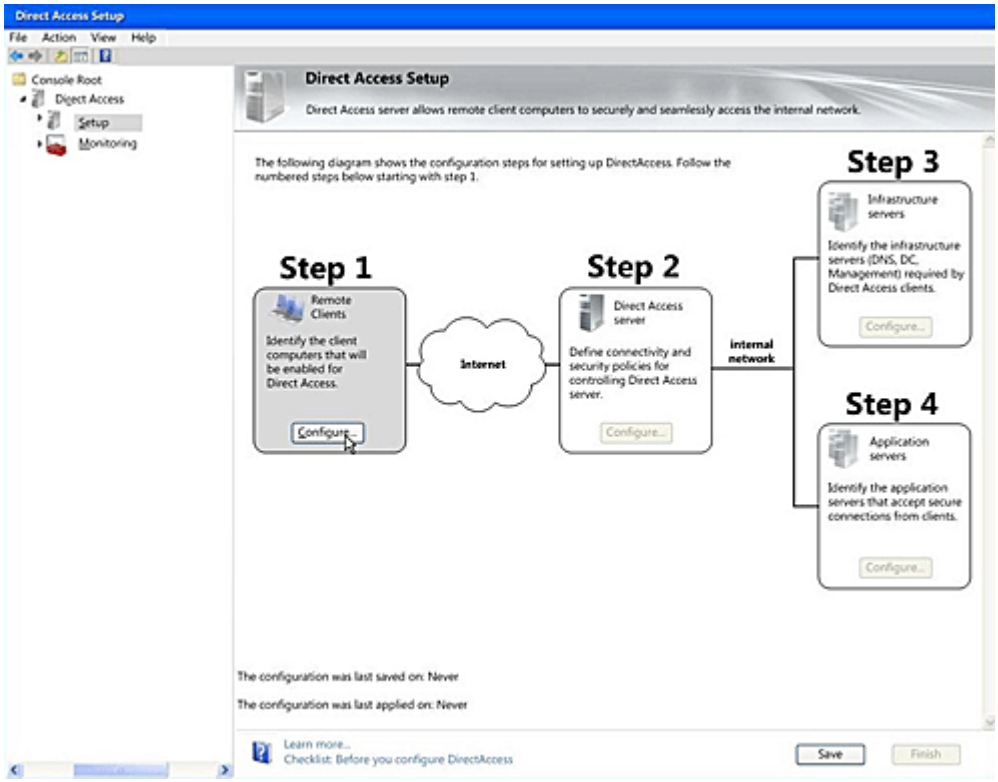
Εικόνα 26-branch cache

Μια άλλη μικρή αλλαγή είναι ότι το security center έχει μεταφερθεί στο action center όπως φαίνεται στην παρακάτω φωτογραφία και ο χρήστης ενημερώνεται για τυχών αλλαγές του συστήματος



Εικόνα 27-action center

Κάτι βέβαια πιο σημαντικό που προστέθηκε είναι το Direct Access στο οποίο απομακρυσμένοι χρήστες χωρίς την χρήση VPN να συνδέονται στο δίκτυο τους, όπως φαίνεται η διαδικασία αυτή στην παρακάτω φωτογραφία



Εικόνα 28-Direct Access

Ο φυλλομετρητής που εισήχθη ασφάλεια σε αυτόν στα windows 7 είναι ο internet explorer 8 όπου υπερτερεί σε θέματα που έχουν να κάνουν με exploits σε browser, τρωτά σημεία στους web servers και σε επιθέσεις social engineering. Αρχικά ένα μέτρο ασφαλείας ενάντια σε επιθέσεις που τρέχει κώδικας στην μνήμη, όμως να φαίνεται σαν μη-εκτελέσιμο είναι το Data Execution Prevention και το No Execute. Συνδυασμένα αυτά τα δυο με το Address Space Layout Randomization κάνει πιο δύσκολο τέτοιου είδους επιθέσεις να περάσουν στον browser και τα add-on του. Αλλαγές βλέπουμε επίσης και όσον αφορά το πώς διαχειρίζεται ο internet explorer το ActiveX στις οποίες κατατάσσετε ο έλεγχος σε ποίες ρυθμίσεις επιδέχεται ενέργεια στο ActiveX από κάποια ιστοσελίδα που το χρειάζεται. Έτσι ο χρήστης λαμβάνει μήνυμα να ενημερωθεί ποια ενέργεια χρειάζεται να γίνει στο ActiveX και να επιλέξει αν επιτρέπεται στη συγκεκριμένη ιστοσελίδα. Αυτό μπορεί να λειτουργήσει ακόμα και σε κανονικούς χρήστες, χωρίς δικαιώματα διαχειριστή. Αν έτσι ένας χρήστης εγκαταστήσει κακόβουλη ρύθμιση του ActiveX, τότε ισχύει αυτή μόνο για το δικό του λογαριασμό και όχι για όλους που βρίσκονται στο σύστημα, αν και ένας διαχειριστής domain μπορεί να απενεργοποιήσει αυτή την λειτουργία.

Στον internet explorer 8 υπάρχει και η επιλογή του protected mode όπως ήταν και στον internet explorer 7, όπου αυτή η επιλογή βοηθούσε στο να αποτρέπεται να εισέλθει κακόβουλος κώδικας. Η διαφορά είναι ότι μέσα στον ίδιο ανοιχτό browser ο internet explorer 8 μπορεί να ανοίξει tabs που είναι protected και "μη" protected, αλλά απενεργοποιείται το protected όταν ανοίγει ο browser σε ζώνη local intranet εκτός και αν το αλλάξει αυτό κάποιος διαχειριστής. Για εφαρμογές που δεν ανήκουν στα windows και χρειάζεται να τρέξουν στον browser αναλαμβάνεται από το application protocol prompt, αλλά έτσι μεγαλώνει ο κίνδυνος σε επιθέσεις και έτσι το prompting γίνεται πριν τρέξει κάποια εφαρμογή. Για αποφυγή επιθέσεων όπως το keystroking έχει γίνει το path όπου γράφει κάποιος στον browser, read-only, και επιλέγοντας μέσω παραθύρου ο χρήστης κάποιο αρχείο που θέλει να επιλέξει και δεν εμφανίζεται στο διαδίκτυο το path αυτού του αρχείου.

Επίσης ένα φίλτρο λειτουργεί σε κάθε σελίδα στο διαδίκτυο όπου ελέγχει αν τρέχει κάποιο κακόβουλου script και αποτρέποντας το να τρέξει και ενημερώνοντας με ανάλογα μήνυμα. Όσον

αφορά τις αιτήσεις από το domain μέσω του browser με την βοήθεια του XDomain Request το οποίο επικοινωνεί με την σειρά του με το World Wide Web Consortium αν η ιστοσελίδα υποστηρίζει αυτό το αντικείμενο, καθώς επίσης υποστηρίζεται το postMessage το οποίο επιτρέπει την επικοινωνία των στοιχείων IFRAME.

Αλλαγές υπάρχουν και στους αλγορίθμους για τον έλεγχο των Multipurpose Internet Mail Extensions όπου απαγορεύει ο browser το sniffing, τις φωτογραφίες, κώδικα να εκτελεστεί σε email. Επίσης αποτρέπεται το detect σε MIME και την αποθήκευση μη έμπιστων αρχείων HTML ώστε πρώτα να αποθηκεύονται τοπικά πριν ανοιχτούν. Επίσης μια άλλη πολύ χρήσιμη ενέργεια ασφάλειας είναι όταν αν ένας χρήστης χρειαστεί να κλικάρει ένα αντικείμενο σε σελίδα που έτσι θα τρέξει κάποιος κώδικας ίσος κακόβουλος, όπως στέλνοντας στοιχεία σε κάποιο άλλο email.

Μια διευκόλυνση και τρόπος ασφάλειας είναι να γίνεται highlight το όνομα του domain στο URL για επίγνωση του χρήστη την ταυτότητα της ιστοσελίδας που έχει επισκεφτεί. Επίσης ενάντια των κακόβουλων προγραμμάτων και ολόκληρων ύποπτων ιστοσελίδων είναι και η προσθήκη του φίλτρου smartscreen η οποία τα μπλοκάρει ακόμα και αν δεν έχουν μπλοκαριστεί από κάποιο anti-virus δείχνοντας ανάλογο μήνυμα στον χρήστη .

Συνεχίζουμε με νέα στοιχεία που έχουν να κάνουν με τα προσωπικά στοιχεία του χρήστη στον browser, βάζοντας την επιλογή Αγαπημένα και την διαγραφή του ιστορικού που αυτό δίνει περισσότερο έλεγχο σε cookies, αποθηκευμένους κωδικούς και προσωρινά αρχεία του διαδικτύου. Για να μην αποθηκευτούν όλα αυτά ο χρήστης μπορεί να ανοίγει τον browser σε InPrivate παράθυρο. Επίσης υπάρχει και το InPrivate φιλτράρισμα το οποίο ανιχνεύει και μπλοκάρει cookies ανίχνευσης και κακόβουλα scripts. Τέλος για τις περιοχές του δικτύου που αναφέρθηκαν πριν κατατάσσονται σε κατηγορίες ασφάλειας, δηλαδή για ζώνη του διαδικτύου και περιορισμένες σελίδες η ασφάλεια είναι υψηλή, για έμπιστες ιστοσελίδες η ασφάλεια είναι μεσαίου επιπέδου και για local intranet ζώνες είναι μεσαίου-χαμηλού επιπέδου.

Ας πάμε τώρα σε κάτι διαφορετικό όπου είναι η διαχείριση λογαριασμών για τις υπηρεσίες. Έτσι ένας διαχειριστής επιλέγει μια εφαρμογή να τρέχει σαν local service, network service ή local system είτε να περιορίσει τα δικαιώματα για κάθε εφαρμογή. Για να γίνει αυτή η διαχείριση λογαριασμών χρησιμοποιείται το windows power shell.

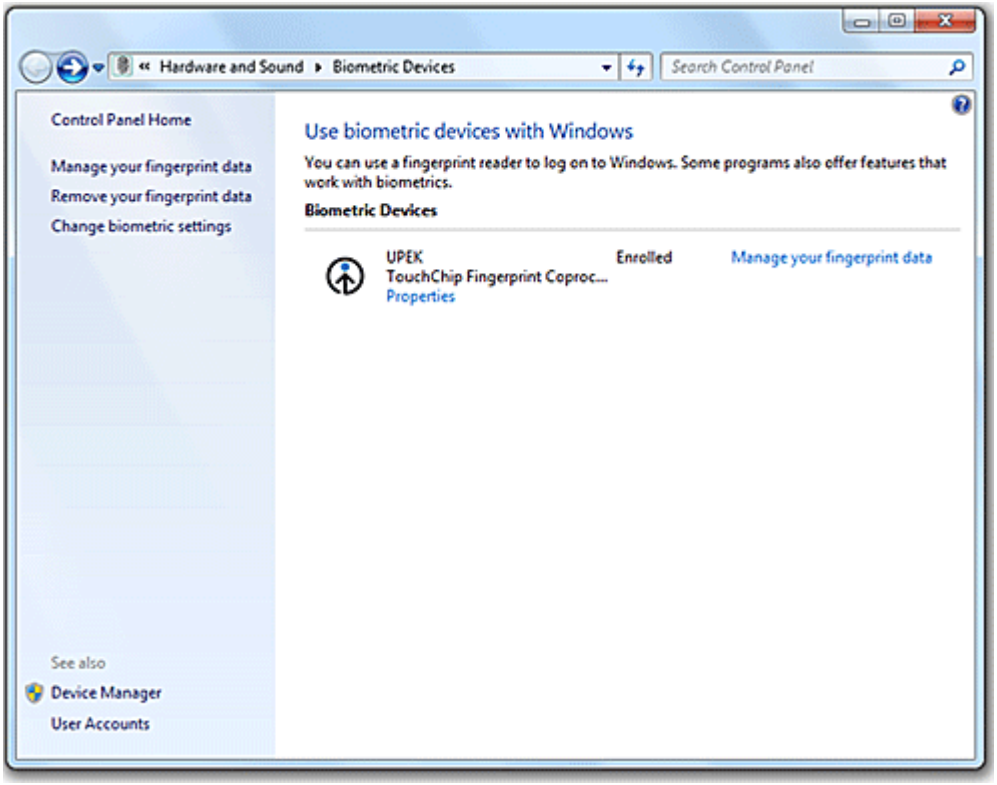
Για διευκόλυνση σε διαμοιρασμό αρχείων μεταξύ υπολογιστών σε μικρά δίκτυα ήρθε η επιλογή της σύνδεσης των online IDs με τους λογαριασμούς που έχει ο χρήστης στα windows με εξακρίβωση αυθεντικότητας με την χρήση πιστοποιητικών με το πρωτόκολλο public key cryptography based user to user το οποίο θα ισχύει σε επιλεγμένους υπολογιστές να λειτουργεί και δεν εμποδίζει άλλους τοπικούς ή domain λογαριασμούς να συνδέονται σε αυτό το μηχάνημα. Η λειτουργία αυτού του πρωτοκόλλου ενεργοποιείται όταν υπολογιστές κάνουν αιτήσεις αυθεντικότητας χρησιμοποιώντας τα online ID και αυτό με την σειρά του χρησιμοποιεί ένα τοπικό πιστοποιητικό και ανταλλάσει την πολιτική με τον αιτών υπολογιστή. Όταν ο αιτών υπολογιστής εξακριβώσει την ταυτότητα το πιστοποιητικό στέλνεται στον άλλο υπολογιστή δημιουργώντας ένα token ασφαλείας και έτσι τελειώνει η διαδικασία για επίτευξη αυθεντικότητας.

Με τα windows 7 έρχεται και το plug and play των smart cards. Δηλαδή μπορούν να χρησιμοποιηθούν smart cards από προμηθευτές που έχουν εκδώσει τους drivers τους μέσω των windows update, για οποιαδήποτε λειτουργικότητα της smart card, χωρίς την βοήθεια κάποιου άλλου λογισμικού κατεβάζοντας τους με τον ίδιο τρόπο που κατεβαίνουν και άλλοι drivers συσκευών.

Κάτι καινούργιο επίσης είναι ο περιορισμός και ανάλυση σε αυθεντικότητα με NTLM, συλλέγοντας πληροφορία, ανάλυση των πακέτων NTLM και περιορισμός αυτών των πακέτων ώστε να γίνει έλεγχος σε αυτά με καλύτερο πρωτόκολλο αυθεντικότητας όπως το Kerberos.

Κάτι άλλο καινούργιο που προστέθηκε στο λειτουργικό είναι biometric service, που χρησιμοποιούνται από συσκευές ελέγχου δαχτυλικού αποτυπώματος για είσοδο στον λογαριασμό είτε να μην έχουν πρόσβαση σε αυτόν, ανάλογα με τι έχει οριστεί από τον διαχειριστή. Όλο αυτό γίνεται

με το windows biometric framework το οποίο φέρνει σε λειτουργία του biometric readers για να κάνουν την ανάγνωση δαχτυλικού αποτυπώματος είτε χρειάζεται αυτό για είσοδο στο λειτουργικό ή σε κάποια εφαρμογή. Στην παρακάτω φωτογραφία βλέπουμε την επιλογή αυτή



Εικόνα 29-biometric

Έρχεται επίσης η έκδοση 1.2 του πρωτόκολλου transport layer security καθώς και το πρωτόκολλο secure socket layer που χρησιμοποιούν το πακέτο αυθεντικότητας schannel και έτσι υποστηρίζεται η επικοινωνία server και client με αλγόριθμο hash και να γίνονται δεκτά μόνο συγκεκριμένα hash και αλγόριθμοι αυθεντικότητας καθώς και τέλος υποστηρίζεται το Suite B cipher.

Κάτι πολύ σημαντικό που προστέθηκε επίσης είναι η απαγόρευση από το τερματίζονται συγκεκριμένα data pages με το να οριστούν σαν μη-εκτελέσιμες. Αυτό γίνεται με το Data Execution Prevention που είναι σε δυο μορφές: hardware enforced και software enforced, ενάντια σε επιθέσεις στη μνήμη και ενεργοποιείται από τον διαχειριστή. Η hardware enforced μορφή κάνει όλες τις περιοχές της μνήμης μη-εκτελέσιμες με επεξεργαστή ποτ υποστηρίζει το Data Execution Prevention. Από την άλλη η μορφή software enforced τρέχει σε όλους τους επεξεργαστές και μπορεί να προστατέψει πεπερασμένο αριθμό εκτελέσιμων του συστήματος. Άλλη μια τεχνική για προστασία από επιθέσεις μνήμης είναι το address space layout randomization, όπου κάνει randomize τις περιοχές των προγραμμάτων και έτσι είναι δύσκολο να προβλεφθούν όλες οι θέσεις μνήμης που χρησιμοποιούνται από ένα πρόγραμμα.

Προστασία στα Structured Exception Handler φέρνει το Structured Exception Handler Overwrite Protection με το να γίνεται compile η εφαρμογή που χρειάζεται με το SAFESEH κατά την φάση σύνδεσης και ένας άλλος τρόπος είναι ο δυναμικός έλεγχος στα exception του thread ότι δεν έχουν διαστρεβλωθεί πριν την διαδικασία του exception handler. Το exception handler είναι record μαζί με το next pointer του exception registration record που βρίσκεται στο thread’s stack.

Τέλος υπάρχουν βελτιώσεις και στην ασφάλεια συστημάτων DNS με το DNS System Security Enhancements για προστασία της αυθεντικότητας, ακεραιότητας δεδομένων και αυθεντικότητα της πηγής των δεδομένων με την χρήση δημόσιων κλειδιών κρυπτογραφίας από το DNS root zone για ψηφιακή υπογραφή.

5 Windows 8 & 8.1

Προχωρώντας στα Windows 8 που εκδόθηκαν το 2012 όπου έχουν γίνει σημαντικές βελτιώσεις σε θέματα προστασίας ενάντια σε ιούς και κακόβουλο λογισμικό από το διαδίκτυο, καθώς και βελτιώσεις κατά την εκκίνηση του λειτουργικού, την πρόσθεση των virtual smart cards, βελτιώσεις στα windows explorer, BitLocker, κρυπτογράφηση και τρόπος εισόδου στο λειτουργικό σύστημα καθώς και πολλά άλλα που θα τα δούμε παρακάτω.

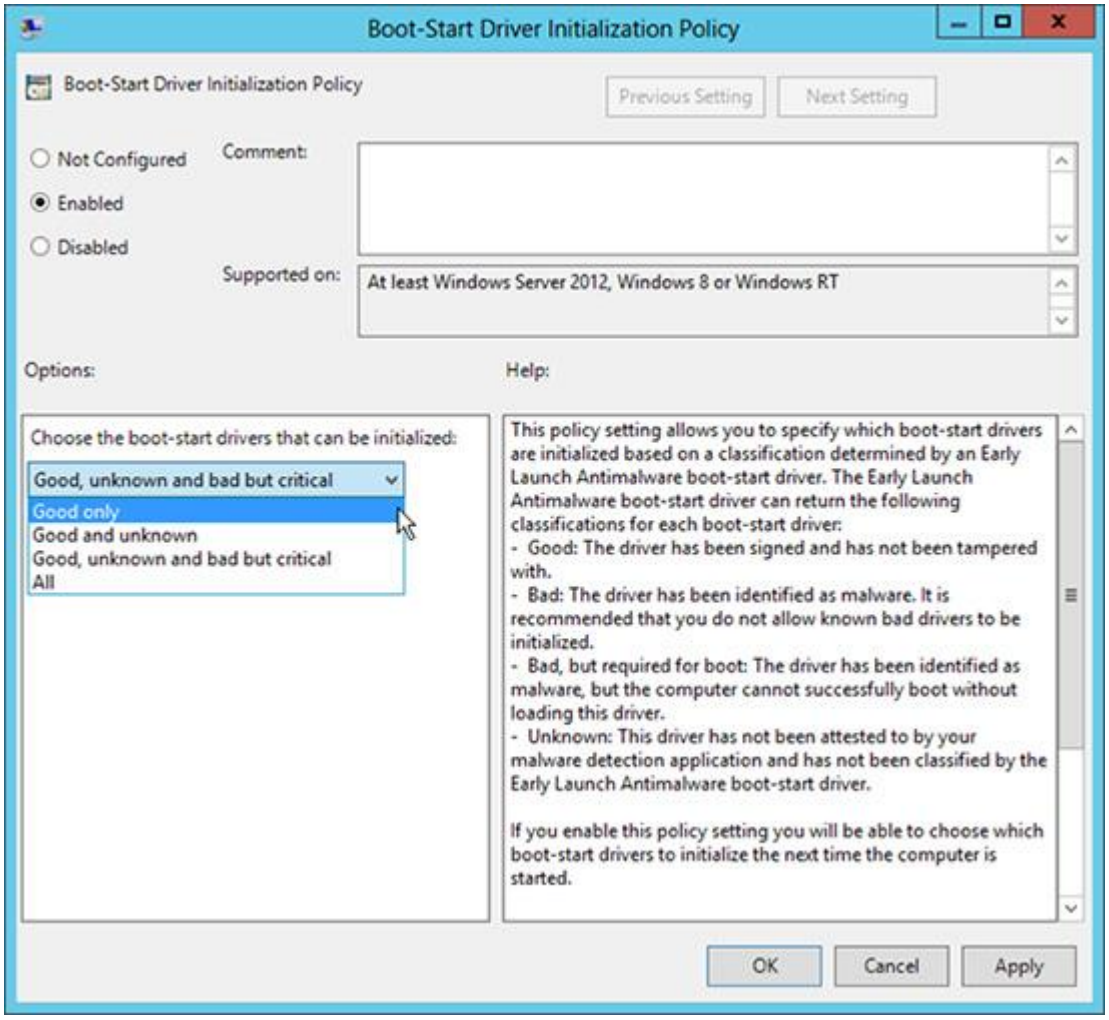
Ας πάμε πρώτα στα μέτρα που έχουν παρθεί για να αποτρέπουν το κακόβουλο λογισμικό όσο αφορά την προστασία του υλικού του μηχανήματος, στην εκκίνηση του λειτουργικού, στον λογαριασμό του χρήστη και στα αρχεία συστήματος. Έτσι η νέα έκδοση windows ενσωματώνει το λογισμικό UEFI, TPM chips και την τεχνολογία ασφαλούς εκκίνησης που βοηθάνε στις μεθόδους ασφαλείας και διατήρηση της ακεραιότητας των στοιχείων του λειτουργικού. Το UEFI που προαναφέρθηκε έρχεται για να αντικαταστήσει το BIOS το οποίο προσφέρει την ίδια λειτουργικότητα με το BIOS με επιπλέον στοιχεία ασφάλειας και όχι μόνο, καθώς τρέχει στην εκκίνηση του μηχανήματος πριν από κάθε άλλο πρόγραμμα, όπως γινόταν και στο BIOS. Έχει την δυνατότητα να κάνει ελέγχους ακεραιότητας στην ψηφιακή υπογραφή αυτού του λογισμικού μέσω των firmware rootkits. Επίσης χρειάζεται η λειτουργία του για το Secure και Measured Boot.

Το TPM που αναφέρθηκε επίσης είναι υπεύθυνο για την αποθήκευση κλειδιών κρυπτογράφησης και hashes και κλειδιών για το BitLocker, virtual smart cards και άλλα πιστοποιητικά, επίσης για ψηφιακές υπογραφές με ιδιωτικά κλειδιά που δεν μπορεί το λειτουργικό να χρησιμοποιήσει, καθώς και υπολογισμούς κρυπτογραφίας.

Αναφέρθηκε επίσης και το Secure Boot το οποίο όταν τρέχει στην εκκίνηση, γίνεται έλεγχος αν υπάρχει ακεραιότητα στην ψηφιακή υπογραφή του bootloader και είναι υπογεγραμμένη από ένα έμπιστο Certificate Authority που βρίσκεται καταχωρημένο στην βάση δεδομένων του UEFI. Τρέχοντας το Secure Boot δεν δίνει περιορισμό το λειτουργικό που θα τρέξει μετά να είναι μόνο Windows, αν αυτό το λειτουργικό που θα τρέξει έχει bootloader υπογεγραμμένο από το Ceritficate Authority της Microsoft, είτε να ρυθμιστεί το UEFI να εμπιστεύεται bootloader και hashes που δεν είναι υπογραμμένα από το Ceritficate Authority της Microsoft, είτε να απενεργοποιηθεί φυσικά το Secure Boot τα οποία μπορούν να γίνουν μόνο από τον χρήστη και όχι από κάποιο κακόβουλο λογισμικό.

Ας δούμε τώρα τι γίνεται αφού ολοκληρώσει την δουλειά του το Secure Boot και συνεχίζεται η φάση για την εκκίνηση του λειτουργικού. Εκεί αναλαμβάνει το Trusted Boot όπου ελέγχει αν όλα τα στοιχεία των windows έχουν ακεραιότητα και είναι έμπιστα ελέγχοντας την ψηφιακή υπογραφή του πυρήνα του λειτουργικού πριν φορτωθούν και ο πυρήνας με την σειρά του ελέγχει όλα τα άλλα στοιχεία που χρειάζονται για την εκκίνηση όπως τους drivers εκκίνησης, τα αρχεία εκκίνησης και τα Early Launch Antimalware και αν ανιχνευθεί ότι κάτι από αυτά έχει πειραχτεί το Trusted Boot θα το επιδιορθώσει.

Αναφέρθηκε το Early Launch Antimalware το οποίο ελέγχει τους boot drivers που χρειάζονται πριν ξεκινήσει το λειτουργικό για τυχόν επιθέσεις που έχουν γίνει με υπογραφές malware και να τα μπλοκάρει, τα οποία malware ελέγχονται και στην συνέχεια από το windows defender αν υπάρχουν. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο ρυθμίσεων του Boot Start

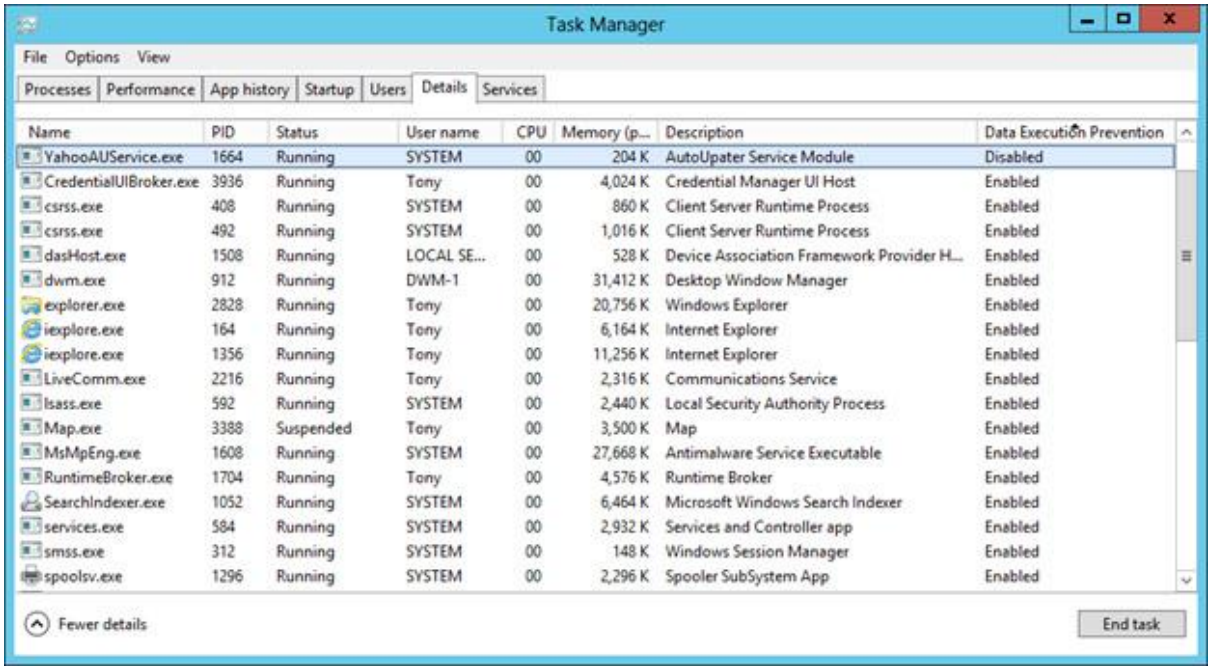


Εικόνα 30-Boot Start

Τώρα για την αντιμετώπιση των rootkits και bootkits που εγκαθίστανται πριν τα malware και δεν μπορούν να ανιχνευτούν από τα antimalware έρχεται να δράσει το measured boot που αναφέρθηκε το οποίο ελέγχει οποιοδήποτε στοιχείο έχει να κάνει με την εκκίνηση και αν βρει κάτι κακόβουλο δημιουργείται ένα log με αυτά με το οποίο ο remote attestation server ελέγχει και αυτός τα στοιχεία εκκίνησης και αν βρει κάτι τότε μπλοκάρει την σύνδεση με πόρους του δικτύου και σύνδεση με το δίκτυο. Η όλη αυτή διαδικασία γίνεται με το να αποτρέπει το TPM να παραποιηθεί αυτό το log και ξεκινάει ο remote attestation client και επικοινωνεί με το τον remote attestation server που ο server παρέχει ένα μοναδικό κλειδί κάθε φορά για να μην στέλνεται κάθε φορά η ίδια αναφορά. Μετά ο client δίνει το κλειδί στο TPM, με αυτό να υπογράψει ψηφιακά το log και έτσι κάποιο malware δεν μπορεί να παραποιήσει το log χωρίς να ανιχνευτεί αυτή η κίνηση. Τέλος ο client στέλνει το log στον server για να γίνει επιβεβαίωση και να αποφασίσει αν γίνει κατάσταση καραντίνας δικτύου ή να μπορεί να γίνει κανονική σύνδεση στο δίκτυο και σε πόρους αυτού.

Ας πάμε τώρα στην διασφάλιση προστασίας του πυρήνα του λειτουργικού συστήματος. Αυτό γίνεται με το να ελέγχονται σημεία στην μνήμη όπου έχει αποθηκευτεί σημαντικός κώδικας και δεδομένα και αν έχουν πειραχτεί από κακόβουλο κώδικα, αυτός να διαγράφεται. Επίσης μέσω του Address Space layout Randomization που είχε αναφερθεί και σε προηγούμενη έκδοση των windows οι κρίσιμες εφαρμογές γίνονται randomize σε ποιες θέσεις μνήμης θα αποθηκευτούν για να είναι έτσι πιο δύσκολη η επίθεση σε αυτές.

Στα windows 8 βελτιώθηκε επίσης η τεχνολογία data execution prevention που υπήρχε και στα windows 7. Αυτή η τεχνολογία χρησιμοποιεί το No Execute και έτσι απαγορεύει την ακύρωση εκτέλεσης σε συγκεκριμένες θέσεις μνήμης που τρέχουν κρίσιμο κώδικα, αυτή η τεχνολογία χρειάζεται επεξεργαστές που υποστηρίζουν την τεχνολογία του data execution prevention. Στην παρακάτω φωτογραφία βλέπουμε ότι όλες οι εφαρμογές έχουν ενεργοποιημένο το data execution prevention και μόνο στην πρώτη δεν είναι



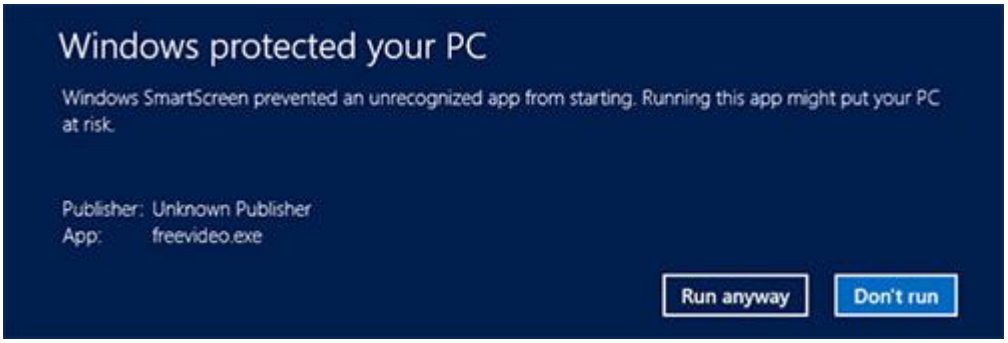
Εικόνα 31-data execution prevention

Ας πάμε τώρα στις θέσεις μνήμης που τρέχουν δεδομένα δυναμικών εφαρμογών, οι οποίες ονομάζονται heaps οι οποίες προστατεύονται από το να αλλοιωθούν με το να είναι randomized η θέση στην οποία τρέχουν και ανάλογα σε ποια θέση μνήμης βρίσκονται, πριν και μετά από αυτήν θα έχουν προστεθεί οι λεγόμενες guard pages οι οποίες πρέπει να δεχτούν αυτές πρώτα κάποια επίθεση και μετά η συγκεκριμένη θέση μνήμης , το οποίο σημαίνει σήμα για αλλοίωση μνήμης και έτσι τερματίζεται η εφαρμογή αυτή. Επίσης καμία εφαρμογή δεν μπορεί να επέμβει στην θέση μνήμης που καταλαμβάνεται από το σύστημα και έχει ως μίνιμουμ 64 KB σε συγκεκριμένη θέση της μνήμης.

Ας πάμε τώρα στην προστασία όσον αφορά το προφίλ του χρήστη όπως με το windows defender, smartScreen, internet explorer, windows store και AppLocker.

Ας αρχίσουμε με το ανανεωμένο windows defender που είναι τώρα anti-spyware, anti-malware και anti-virus. Υποστηρίζει το Early Launch Antimalware που προαναφέρθηκε και έτι μπορεί να ανιχνεύσει και rootkits και αποτρέπει από το να εκτελεστεί κάποιος driver αν έχει επηρεαστεί από rootkit.

Συνεχίζουμε με το smartScreen στο internet explorer και σε άλλους φυλλομετρητές που χρησιμοποιούνται και ελέγχει όλα τα URL και τις λήψεις του χρήστη και αν χαρακτηριστεί ως ύποπτη χρησιμοποιώντας έλεγχο με ψηφιακή υπογραφή θα ενημερωθεί ο χρήστης ή ακόμα και να το μπλοκάρει ανάλογα τι έχει ορίσει ο διαχειριστής στο Group Policy όπως φαίνεται σχετικό μήνυμα στην παρακάτω φωτογραφία. Το smartScreen μπορεί επίσης να απενεργοποιηθεί με ανάλογη ενέργεια στα Group Policy.



Εικόνα 32-Application

Προχωράμε στον νέο browser των windows 8, τον internet explorer 10 για να δούμε τις βελτιώσεις που έχουν να κάνουν με την παροχή ασφάλειας. Βελτίωση έχει γίνει στο protected mode όπου κατανέμεται η εφαρμογή τυχαία σε ένα ευρύ φάσμα μνήμης για να είναι πιο δύσκολο στις επιθέσεις στη μνήμη να το πειράξουν. Επίσης στο protected mode όταν ο χρήστης πάει να ανοίξει ένα αρχείο για τυχόν ανέβασμά του, τρέχει μια ειδική διεργασία για παροχή ασφάλειας κατά το ανέβασμα. Επίσης αυτό το mode απαγορεύει στα tab του να μπαίνουν στο διαδίκτυο χρησιμοποιώντας στοιχεία του χρήστη στο domain. Το protected mode λειτουργεί πάντα όταν ο χρήστης βρίσκεται στο windows store και δεν τρέχει add-ons και η εκτέλεση του adobe flash επιτρέπεται μόνο σε έμπιστους ιστότοπους. Όσον αφορά γενικά την προστασία στον internet explorer 10 έχει εισαχθεί το φίλτρο Improved cross site scripting που αποτρέπει τις cross site scripting επιθέσεις.

Ας πάμε τώρα στο windows store αφού προαναφέρθηκε. Οι εφαρμογές που κατεβαίνουν από αυτό έχουν μικρό δείκτη να είναι κακόβουλες αφού περνάνε έλεγχο πριν ανέβουν στο store και έχουν μικρή γκάμα δυνατοτήτων και δικαιωμάτων για να τρέχουν μόνο τις νόμιμες διεργασίες τους επειδή τρέχουν στον AppContainer. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο που λέει σε ποία στοιχεία θα επιδρά μια εφαρμογή

Εικόνα 33-App

Συνεχίζουμε με το AppBlocker που έχει και αυτό αναβαθμιστεί σε σύγκριση με την έκδοση του στα windows όπου είναι υπεύθυνο για ποιες εφαρμογές μπορούν να εκτελεστούν και από ποιόν. Σε αυτή την νέα έκδοση, οι κανόνες είναι πιο απλοί και όταν επιλεχτεί ένας installer να επιτρέπεται ή να μην επιτρέπεται, τότε αφορά και όλα τα άλλα αρχεία που έχουν να κάνουν με αυτόν. Καθώς πιο απλούς κανόνες με κριτήριο τον εκδότη εφαρμογών και κανόνες που ισχύουν για εφαρμογές που ανήκουν στο store είτε δεν ανήκουν σε αυτό, καθώς και ρύθμιση δικαιοδοσίας για εκτέλεση ή μη εκτέλεση ολόκληρου σετ εφαρμογών με κριτήριο το όνομα προγράμματος ή του εκδότη προγραμμάτων. Στην παρακάτω φωτογραφία βλέπουμε παράθυρο με κανόνα όσον αφορά τον εκδότη εφαρμογών

Εικόνα 34-Publisher rule

Προχωρώντας στο BitLocker όπου είναι υπεύθυνο για κρυπτογράφηση και διασφάλιση της ακεραιότητας των δεδομένων σε οποιοδήποτε μέσο αποθήκευσης έχουν γίνει αλλαγές από τις προηγούμενες εκδόσεις του. Αλλαγή είναι ότι και οι κανονικοί χρήστες μπορούν να αλλάζουν το PIN και τον κωδικό πρόσβασης, είναι γρηγορότερο στην κρυπτογράφηση σε ολόκληρη την συσκευή αποθήκευσης ή και μόνο των δεδομένων της, το κλειδί για ανάκτηση χρησιμοποιείται μόνο σε περίπτωση καταστροφής του δίσκου ή απώλειας κωδικού ασφαλείας ή PIN, χρήση του σε self encryption drives και δυνατότητα από διαχειριστές να χρησιμοποιούν tools του BitLocker για ήδη κρυπτογραφημένα μέσα αποθήκευσης. Επίσης προστέθηκε το Network Unlock το οποίο παρέχει την δυνατότητα σε υπολογιστές που είναι προστατευμένου από το BitLocker και υποστηρίζει UEFI και το dynamic host configuration protocol, όταν συνδέονται σ δίκτυο που έχει windows deployment server να ανοίγουν αυτόματα, αλλιώς να χρειάζεται η εισαγωγή PIN υποχρεωτικά.

Πάμε τώρα στους τρόπους πρόσβασης που έχουμε νέους στα windows 8 αλλά και ήδη υπάρχων ανανεωμένους. Μια από τις νέες προσθήκες είναι το ξεκλείδωμα του υπολογιστή μέσω κλικ σε συγκεκριμένα σημεία σε φωτογραφίες, που έτσι είναι αρκετά δύσκολο να μαντέψει κάποιος ποια σημεία της φωτογραφίας είναι τα ορίσματα για ξεκλείδωμα, αφού κάθε φωτογραφία αποτελείται από πάρα πολλά pixels. Αν ο χρήστης ξεχάσει ποια σημεία έχει επιλέξει, τότε μπορεί να μπει στο σύστημα και με την κλασική εισαγωγή κωδικού πρόσβασης. Στην παρακάτω φωτογραφία βλέπουμε παράδειγμα με τρία σημεία στην εικόνα για ξεκλείδωμα

Εικόνα 35-Picture Password

Όσον αφορά τους κωδικούς πρόσβασης και την αποτροπή των επιθέσεων brute force, μετά από συγκεκριμένο αριθμό λάθος προσπαθειών, ανάλογα με την ρύθμιση του διαχειριστή, ο λογαριασμός χρήστη μπορεί να αποσυνδέεται, είτε να υπάρχει χρονικό όριο μέχρι την επόμενη επαναπροσπάθεια εισαγωγής κωδικού πρόσβασης. Αν υπάρχει η επιλογή του BitLocker και ανιχνευθεί επίθεση brute force, τότε μπαίνει το σύστημα σε recovery mode μέχρι ότου δοθεί κωδικός ανάκτησης.

Μια επόμενη προσθήκη είναι τα virtual smart cards οι οποίες προσφέρουν πολύ μεγαλύτερη ευκολία σε σύγκριση με τις smart cards που χρειαζόντουσαν τον smart card reader. Έτσι ο χρήστης εισάγει στον υπολογιστή το πιστοποιητικό της κάρτας και αυτό προστατεύεται από το TPM και ουσιαστικά αυτός ο υπολογιστής γίνεται η smart card που σε κάθε ενέργεια βέβαια που χρειάζεται η χρήση της smart card, εισάγεται το PIN, χωρίς την φυσική σύνδεση της smart card ή του reader.

Επίσης υποστηρίζεται και το Direct Access που είχε αναφερθεί και στο κεφάλαιο των windows 7 όπου οι χρήστες χωρίς την χρήση VPN, μπορούν να συνδεθούν στο δίκτυό τους από όποια περιοχή και να βρίσκονται, έχοντας πρόσβαση στο διαδίκτυο σαν να βρισκόντουσαν μέσα στο domain τους με διασφαλισμένη διαφάνεια, κρυπτογραφία και αυθεντικότητα της σύνδεσης, ακόμα και αν το δίκτυο αυτό χρησιμοποιεί IPv4.

Ας δούμε κάτι άλλο που ονομάζεται dynamic access control το οποίο προστατεύει αρχεία και φακέλους με συγκεκριμένους κανόνες με κριτήρια την ομάδα χρηστών και τις συσκευές που θα έχουν δικαιώματα σε αυτά ακόμα και αν αυτά μεταφερθούν σε άλλα συστήματα. Σε συνδυασμό με το dynamic access control οι διαχειριστές μπορούν να έχουν και την επίγνωση για το ποιοι χρήστες κάνουν ενέργειες σε αρχεία και πληροφορίες αυτών.

Μια άλλη νέα υπηρεσία είναι η provable pc health, η οποία παρέχει απομακρυσμένη ανάλυση του υπολογιστή μέσω του secure data client σε μια υπηρεσία cloud η οποία αν βρει κάποιο σφάλμα στο σύστημα, τότε στέλνει μήνυμα στο secure data client με πιθανές λύσεις για την επίλυση του προβλήματος και αυτό πίσω στον χρήστη.

Υπάρχει τώρα επίσης η δυνατότητα να ελεγχθεί η ακεραιότητα και αυθεντικότητα των δημόσιων και τοπικών κλειδιών και των πιστοποιητικών. Μέσω του TPM based key storage provider δημιουργείται διασύνδεση του ιδιωτικού κλειδιού και του υπολογιστή και αποτρέπει στο ιδιωτικό κλειδί να βγει από αυτό το σύστημα από μεριάς client, ελέγχοντας επίσης την ακεραιότητα των κλειδιών.

Επίσης όπως και στα windows 7, έτσι και στα windows 8 έχουμε το πρωτόκολλο transport player security το οποίο χρησιμοποιείται για την διασφάλιση των δεδομένων που αποστέλλονται

μεταξύ εφαρμογών σε ένα μη έμπιστο δίκτυο. Επίσης έχει την ιδιότητα για αυθεντικοποίηση server και client μηχανημάτων και να κρυπτογραφεί μηνύματα που στέλνονται.

Επίσης σε ότι αφορά την απομακρυσμένη πρόσβαση, ήρθε το restricted admin mode όπου έτσι ένας χρήστης με στοιχεία διαχειριστή επικοινωνεί με ένα μηχάνημα host μέσω των remote desktop services. Όταν γίνεται ο έλεγχος ότι ο χρήστης που συνδέεται έχει δικαιώματα διαχειριστή τότε επιτυγχάνεται σύνδεση.

Η αποτροπή σε επιθέσεις code injection από διάφορες κακόβουλες εφαρμογές εμποδίζεται από το local security authority service, καθώς επίσης πιστοποιεί τους χρήστες που προσπαθούν να μπουν σε λογαριασμό του λογισμικού είτε τοπικά, είτε απομακρυσμένα.

Επόμενη προσθήκη είναι το protected users group στο οποίο οι χρήστες που ανήκουν σε αυτό μπορούν να μπουν σε λογαριασμό χρησιμοποιώντας το πρωτόκολλο Kerberos με την χρήση AES cipher suite και ο ίδιος λογαριασμός δεν μπορεί να συνδεθεί από άλλο σύστημα και καθώς είναι συνδεδεμένος πρέπει να κάνει έλεγχο πιστοποίησης κάθε τέσσερις ώρες.

Επίσης μπορεί να ελεγχθεί ποιος χρήστης θα συνδέεται μέσω της πολιτικής forest based active directory από έναν διαχειριστή που θα έχει επίγνωση των υπόλοιπων λογαριασμών του συστήματος, είτε domain και θα μπορεί να κάνει έλεγχο αυθεντικότητας σε αυτούς.

Ασφάλεια προστίθεται επίσης και στην αποθήκευση και απομνημόνευση ονομάτων των λογαριασμών και των κωδικών τους πρόσβασης στις εφαρμογές του windows store και ιστοσελίδων μέσω του credential locker.

Το fingerprint biometric υπάρχει επίσης και στα windows 8, όπου συμβάλει ώστε να γίνεται η είσοδος των χρηστών μέσω του δαχτυλικού αποτυπώματος σε συσκευή της υπηρεσίας για επίτευξη αυθεντικότητας του χρήστη.

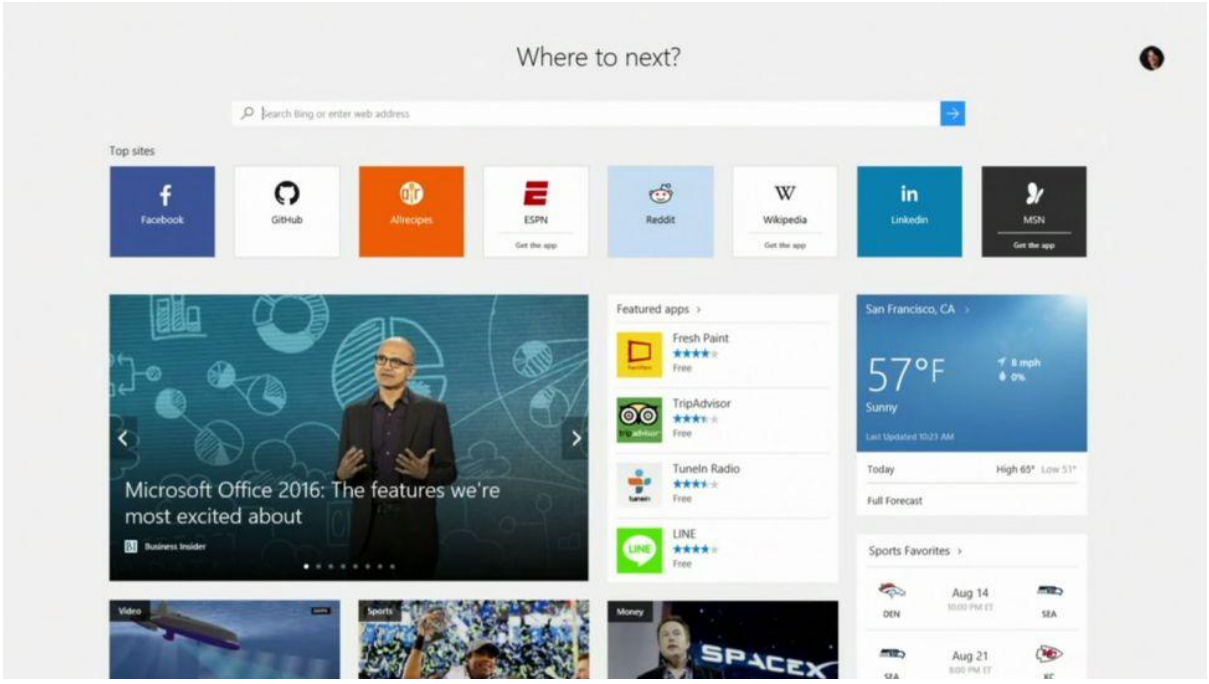
Τέλος, μια άλλη προσθήκη είναι το selective wipe για διασφάλιση ασφάλειας σε δεδομένα που βρίσκονται σε domain που ανήκουν σε κάποια εταιρία με το να κρυπτογραφεί ένα κλειδί για αυτά με το encrypting file system που τοποθετείται στο credential locker και να είναι προσβάσιμα μόνο από τον χρήστη που χρησιμοποίηση την εφαρμογή αυτή. Επίσης διασφαλίζει τα συνημμένα στην εφαρμογή ηλεκτρονικού ταχυδρομείου που έχει την πολιτική exchange activeSync και επίσης τους φακέλους σε domain, τους Work Folders.

6 Windows 10

Για τα windows 10 πού είναι η νεότερη έκδοση των windows το 2015 έχουν γίνει κάποιες βασικές αλλαγές όσον αφορά την ασφάλεια, αλλά βέβαια με νεότερες αναβαθμίσεις περιμένουμε ακόμα περισσότερα. Μέχρι τώρα μπορούμε να δούμε αναβαθμίσεις όπως τα νέα browser internet explorer 11 και windows edge, αναβαθμίσεις στο BitLocker, στις ρυθμίσεις ασφαλείας όσον αφορά το λειτουργικό και τις συσκευές, στο VPN, στο user account control και τις προσθέσεις των device guard, credential guard και το Microsoft passport.

Όσον αφορά το BitLocker τώρα μπορεί να κρυπτογραφήσει συσκευές που ανήκουν σε domain Azure Active Directory και αποθηκεύει το κλειδί ανάκτησης εκεί με σκοπό την ευκολότερη πρόσβαση σε αυτό το κλειδί. Επίσης υπάρχει η δυνατότητα χρήσης της πολιτικής data protection-allow direct memory access για το μπλοκάρισμα των DMA ports των συσκευών κατά την εκκίνηση. Καθώς μια συσκευή είναι κλειδωμένη, όλα τα DMA port που δεν έχουν χρησιμοποιηθεί, απενεργοποιούνται και τα υπόλοιπα συνεχίζουν να λειτουργούν και ξαναενεργοποιούνται όταν η συσκευή ξεκλειδώσει. Μια νέα επίσης πολιτική εισήχθη στο Group Policy που ρυθμίζει το μήνυμα στο pre-boot recovery και ανακτά το URL που φαίνεται στην οθόνη του pre-boot recovery. Όσο αφορά το BitLocker σε αρχεία έχουν εισαχθεί περιορισμοί οι οποίο θα αφορούν άτομα και εφαρμογές τα οποία δεν θα έχουν δικαιώματα επεξεργασίας, αποθήκευσης και διαμοιρασμού στα αρχεία που φυλάσσονται παρέχοντας τέσσερα επίπεδα ασφαλείας. Το πρώτο ονομάζεται block το οποίο εμποδίζει τα άτομα που δεν έχουν δικαιώματα από το να έχουν πρόσβαση σε αρχεία, το επόμενο επίπεδο ονομάζεται override που αν κάποιος δεν έχει δικαιώματα πάνω σε ένα αρχείο ειδοποιείται από το σύστημα. Επόμενο επίπεδο είναι το audit στο οποίο δεν μπλοκάρεται καμία κίνηση και το τελευταίο επίπεδο το off στο οποίο δεν ελέγχεται κανένα αρχείο. Αν κάποιο αρχείο που προστατεύεται, εισαχθεί σε κάποια άλλη συσκευή χωρίς δικαιοδοσία, τότε διαγράφεται από αυτή την συσκευή με ανάλογη εντολή για την συγκεκριμένη συσκευή. Αν βρίσκεται σε επίπεδο block τότε οι προστατευμένες εφαρμογές μπορούν να επικοινωνήσουν μόνο με άλλες προστατευμένες εφαρμογές και όχι άλλες που τρέχουν στο σύστημα. Επίσης οι χρήστες που δεν έχουν δικαιώματα σε συγκεκριμένα αρχεία δεν μπορούν να τα διαμοιράσουν με οποιονδήποτε τρόπο, όπως το cloud, ούτε να τα χρησιμοποιήσουν με πονηρό όπως να τα μετονομάσουν πρώτα.

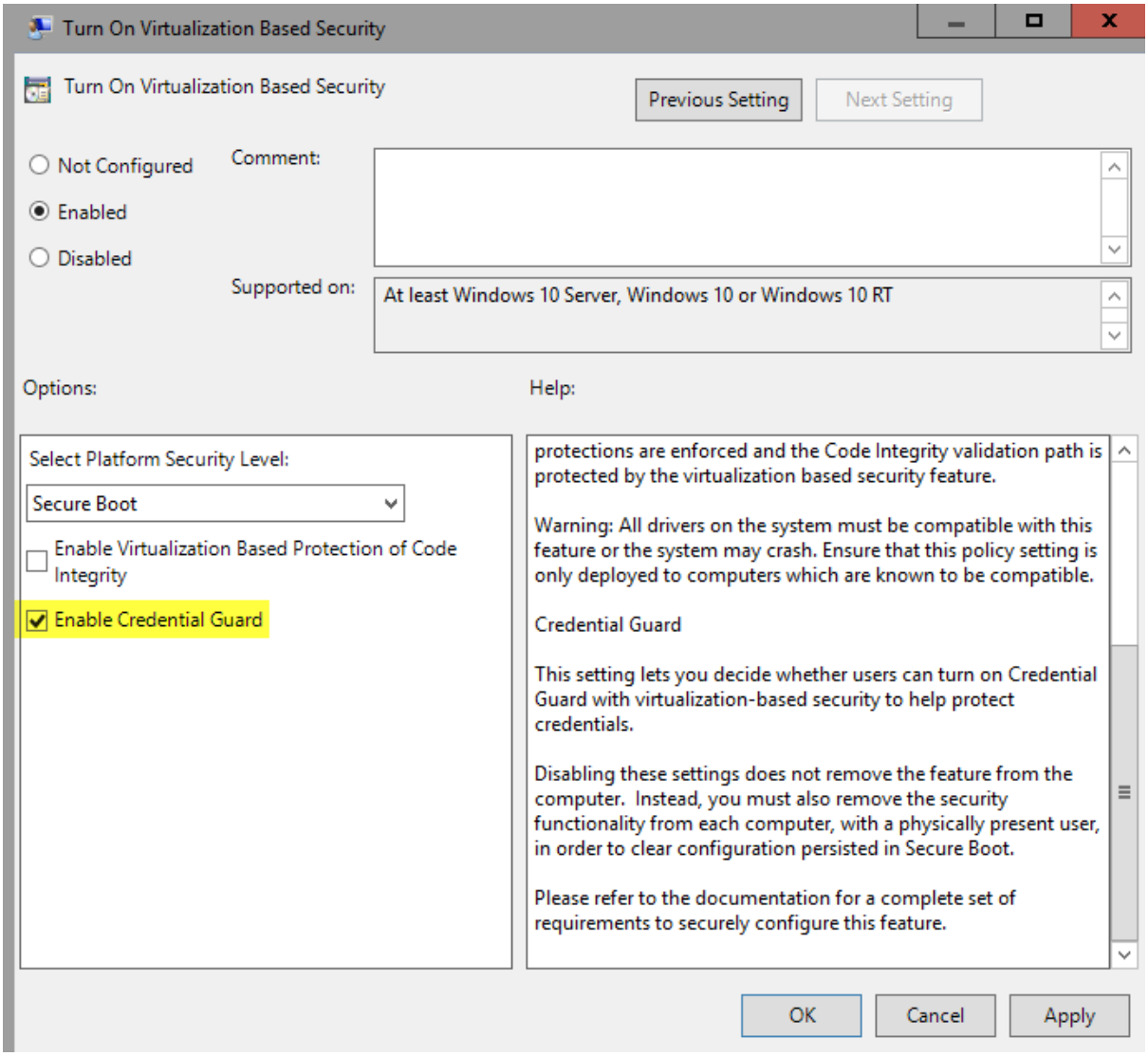
Προχωράμε στα νέα browser. Ας πάρουμε πρώτα το windows edge όπου αυτός ο browser έχει την προσθήκη του web note όπου σε αυτό ο χρήστης μπορεί να βάλει σχολιασμούς, επισημάνσεις και URLs. Διαθέτει επίσης το reading view όπου δίνει την δυνατότητα εκτύπωσης διαδικτυακών εγγράφων ανάλογα με το μέγεθος της οθόνης και την αποθήκευση των ιστοσελίδων και pdf στο reading list. Μια άλλη προσθήκη είναι το cortana όπου η δυνατότητα του είναι η επισήμανση λέξεων σε κείμενα που με ένα κλικ σε αυτές ο χρήστης λαμβάνει πληροφορίες για αυτές από το διαδίκτυο χωρίς να κλείνει η τρέχων σελίδα. Κάτι τελευταίο είναι ότι έχει την συμβατότητα με τον internet explorer 11 με σελίδες του ανήκουν στο enterprise mode site list και στο corporate intranet. Στην παρακάτω φωτογραφία βλέπουμε ένα tab του windows edge



Εικόνα 36-windows edge

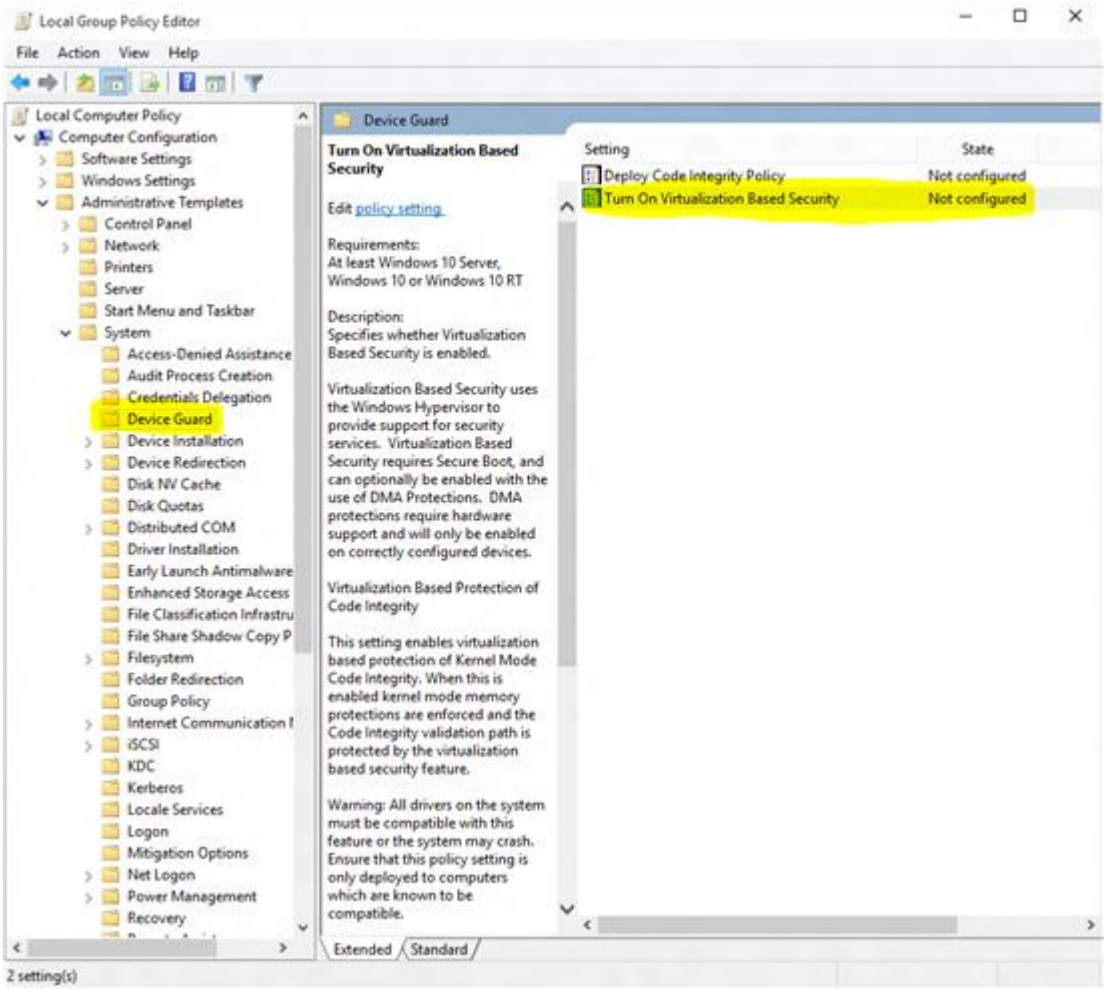
Συνεχίζουμε με τον internet explorer 11 όπου υποστηρίζει εννέα modes εγγράφων στα οποία περιλαμβάνονται modes παρόμοια με προηγούμενες εκδόσεις του browser. Είναι γρηγορότερος με την βοήθεια του javascript rendering, το δίκτυο και τα γραφικά και μπορεί να τρέχει σε windows 7 και 8.1. Υποστηρίζει τα HTML5, webGL και css3 που χρειάζονται σε νέες ιστοσελίδες, καθώς και τα smartScreen και protected mode για μεγαλύτερη ασφάλεια όπως υπήρχαν και σε προηγούμενες εκδόσεις. Επίσης μπορεί να χρησιμοποιηθεί το internet explorer administration kit και τα MSI για πρόσβαση σε περισσότερες πολιτικές.

Συνεχίζουμε με μια άλλη νέα προσθήκη, το credential guard σε windows 10 enterprise που υποστηρίζουν UEFI, secure boot, 64 bit αρχιτεκτονική, second level address translation και να μην είναι το μηχάνημα virtual. Το credential guard απομονώνει "μυστικά" τα οποία προηγούμενες εκδόσεις αποθήκευαν στο local security authority, που έχουν πρόσβαση σε αυτά μόνο εφαρμογές που έχουν το δικαίωμα αυτό. Προσφέρει ασφάλεια στο hardware του μηχανήματος με το να χρησιμοποιεί τεχνικές όπως το secure boot. Επίσης εφαρμογές μπορούν να εκτελούνται σε ένα προστατευμένο περιβάλλον που είναι απομονωμένο από το υπόλοιπο λειτουργικό σύστημα προστατεύοντας τα στοιχεία του χρήστη ακόμα και αν ένα κακόβουλο λογισμικό τρέχει στο υπόλοιπο λειτουργικό, αυτή η δυνατότητα ονομάζεται virtualization based security. Οι ρυθμίσεις του credential guard μπορούν να γίνουν από το Group policy, το WMI, το windows power shell και την γραμμή εντολών. Η διαδικασία αυτή επιτυγχάνεται με το να επικοινωνεί η υπηρεσία local security authority του λειτουργικού με την αντίστοιχη στο απομονωμένο περιβάλλον. Με το credential guard δεν επιτρέπονται οι drivers συσκευών, ούτε πρωτόκολλα αυθεντικότητας όπως τα Kerberos και NTLM, παρά μόνο εκτελέσιμα του συστήματος που έχουν να κάνουν με ασφάλεια και είναι ψηφιακά υπογεγραμμένα. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο ενεργοποίησης του credential guard



Εικόνα 37-credential guard

Ας πάμε στην επόμενη νέα προσθήκη που είναι το device guard σε windows 10 enterprise που υποστηρίζουν UEFI, trusted boot καιvirtualization based security που κλειδώνει τις συσκευές για να μπορούν να τα εκτελούνται σε αυτές μόνο έμπιστες εφαρμογές που είναι υπογεγραμμένες μόνο από έμπιστους πάροχους αυθεντικότητας, όπως το windows store, την ψηφιακή υπογραφή του ίδιου του χρήστη μέσω του public key infrastructure είτε κάποια υπηρεσία web είτε ανήκει στην Microsoft, είτε όχι, που είναι έμπιστη και έτσι αποτρέπονται και πολλές επιθέσεις σε αυτές και τα malware. Χρησιμοποιεί το virtualization based security για την απομόνωση της υπηρεσίας code integrity μόνο στον kernel, ώστε να επιτρέπεται η χρήση των ψηφιακών υπογραφών της υπηρεσίας και σε άλλες εφαρμογές. Έτσι προστασία παρέχεται σε συσκευές που στην εκκίνηση υποστηρίζουν UEFI secure boot που αποτρέπει τα rootkits. Στην συνέχεια μετά την εκκίνηση ξεκινάνε οι υπηρεσίες hyper-v virtualization based security και το kernel mode code integrity για προστασία του kernel, των drivers, το σύστημα από τα malware και το trusted platform module για προστασία δεδομένων στου χρήστη. Επίσης ελέγχονται τα εκτελέσιμα σε μεριά του χρήστη με την χρήση του UMCI. Πριν χρησιμοποιηθεί το device guard πρέπει να δημιουργηθεί μια πολιτική για Code Integrity που παρέχεται από την Microsoft, το οποίο είναι ουσιαστικά ένα έγγραφο XML που έχει επιλογές των ρυθμίσεων για τον kernel και την μεριά του χρήστη και τους περιορισμούς που θα υπάρχουν. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο του device guard

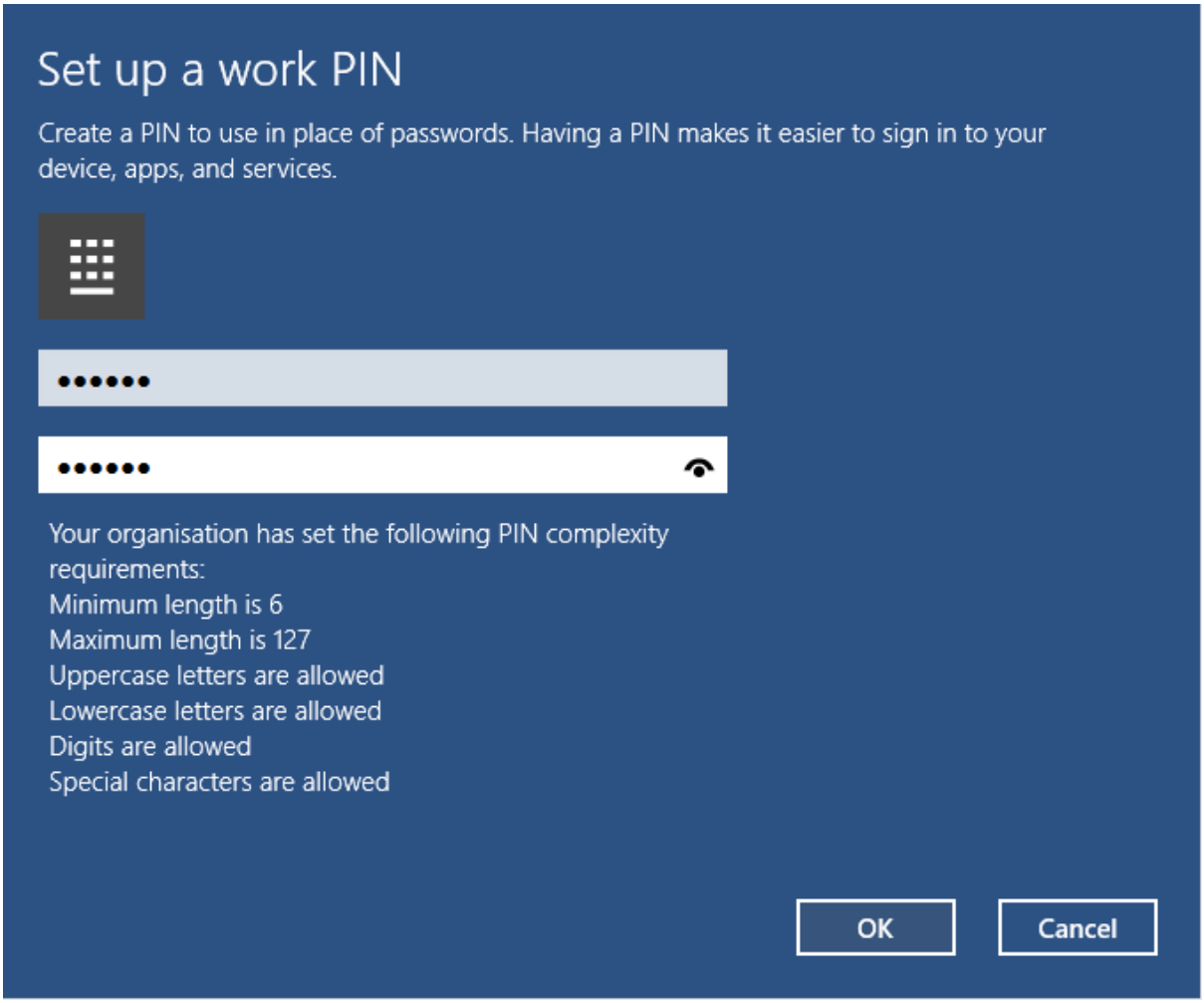


Εικόνα 38-device guard

Μια άλλη προσθήκη σε enterprise και στην έκδοση για κινητές συσκευές, είναι το unenrollment στο οποίο αν χρήστες εναλλάσσονται στις συσκευές, τότε αφαιρούνται τα πιστοποιητικά, οι enterprise εφαρμογές και τα VPN προφίλ, αλλά μένουν τα δεδομένα και εφαρμογές του χρήστη.

Το lockdown συσκευών είναι επίσης σημαντικό όπου μια δυνατότητα είναι ότι όταν μπαίνει στην συσκευή ένας lockdown χρήστης τότε εμφανίζονται οι εφαρμογές που έχουν επιλεγχθεί.

Προχωράμε στο Microsoft passport το οποίο μπορεί να αντικαταστήσει τους κωδικούς για τον λογαριασμό των windows, του active directory, του Microsoft azure active directory ή ακόμα και υπηρεσιών που δεν ανήκουν στην Microsoft και υποστηρίζουν fast ID online, με την χρήση του Microsoft hallo ή ενός PIN για την απόκτηση του passport και ταυτόχρονα την αποτροπή επιθέσεων replay και brute force προς τους κωδικούς. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο δημιουργίας PIN



Εικόνα 39-PIN

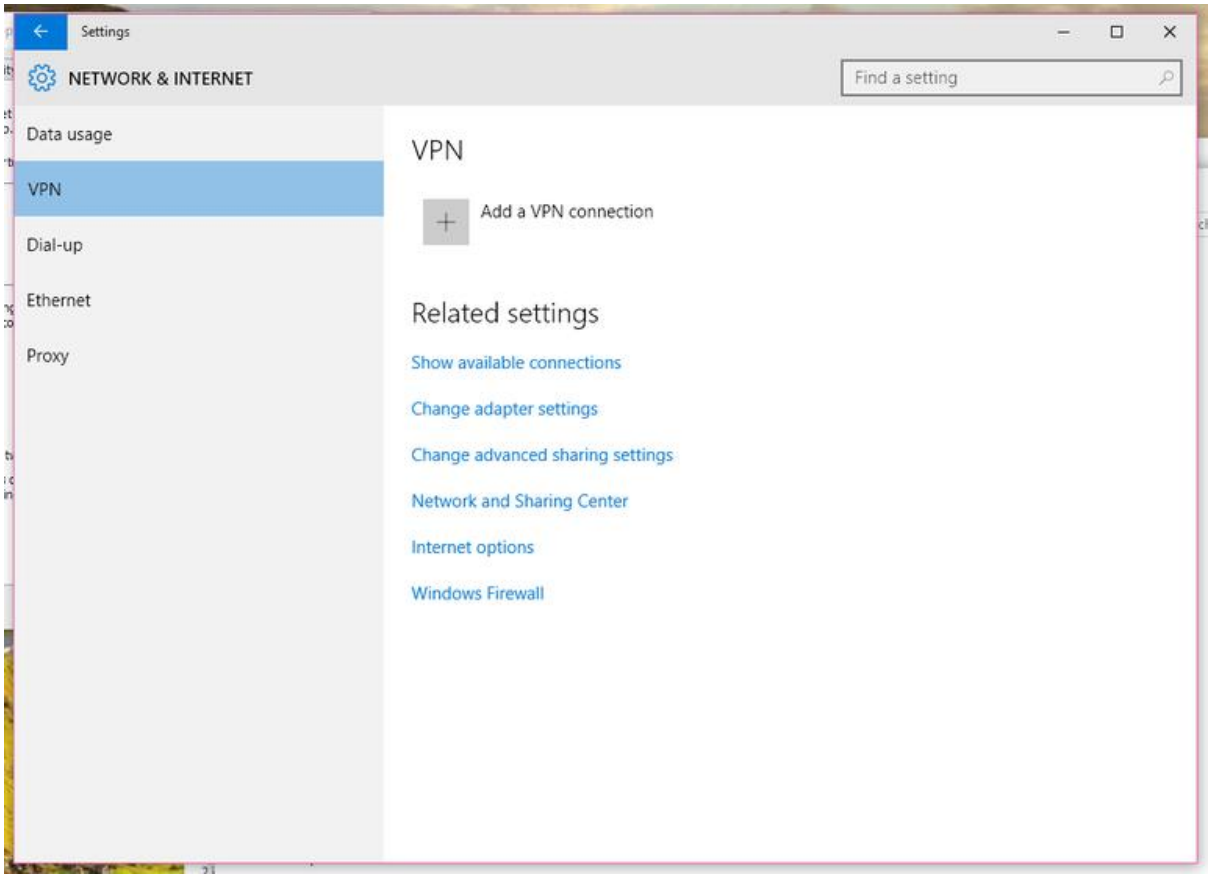
Πάμε τώρα στα provisioning packages τα οποία βοηθούν στην διαμόρφωση των συσκευών χωρίς να φτιάχνονται συνέχεια images, παρά μόνο ένα provision package το οποίο μπορεί να μπει σαν attachement σε email, είτε να κατέβει από το διαδίκτυο, είτε να βρίσκεται σε κάποια εξωτερική συσκευή αποθήκευσης. Αυτά τα packages που αποτελούνται από sets γραμμένων εντολών στα windows image και Configuration Designer, έχουν την δυνατότητα να διαμορφώσουν πιστοποιητικά, πολιτικές, προφίλ συνδεσιμότητας όπως ρυθμίσεις wifi, ρυθμίσεις των μενού εκκίνησης, εφαρμογές, αρχεία και πολλά άλλα.

Έχουμε δύο νέες προσθήκες και στο security auditing τις audit group membership και audit PNP activity. Με την audit group membership μπορεί κανείς να διαμορφώσει τις πληροφορίες για το group membership που έχουν να κάνουν με την διαδικασία εισόδου στο λειτουργικό ή την χρησιμοποίηση κάποιου πόρου του δικτύου, όπως ένας κοινόχρηστος φάκελος. Με την audit PNP activity όπου λειτουργεί όταν συνδέεται κάποια εξωτερική συσκευή και ελέγχονται τυχών αλλαγές στο hardware του συστήματος.

Όσον αφορά το user account control έχει εισαχθεί η δυνατότητα του integration with the antimalware scan interface το οποίο ελέγχει για τυχόν malware στο σύστημα και αν βρεθεί κάτι, τότε τα δικαιώματα διαχειριστή μπλοκάρονται.

Τέλος για ότι αφορά το virtual private network όπου σε αυτό μπορεί να επιλεχτεί το always on στο οποίο ένα προφίλ εισάγεται αυτόματα σε περίπτωση user sign on ή αλλαγής δικτύου, είτε

με την εκκίνηση των εφαρμογών package family name for universal windows platform και των file path for classic windows. Εισήχθησαν επίσης φίλτρα με τις κατηγορίες κανόνων app based και traffic based. Στην μια μόνο επιλεγμένες εφαρμογές μπορούν να λειτουργήσουν στο VPN interface και στην άλλη μόνο traffic που έχει τα επιλεγμένα ports, διευθύνσεις και πρωτόκολλα μπορούν να περάσουν. Επίσης η επιλογή lockdown που αναφέρθηκε προηγουμένως μπορεί να οριστεί και στο VPN όπου σε αυτό ο χρήστης δεν μπορεί να διακόψει την σύνδεση, να διαγράψει κάποιο προφίλ. Επίσης σε κάθε συσκευή επιτρέπεται μόνο ένα lockdown VPN που θα χρησιμοποιεί σύνδεση force tunnel που θα έχει συνεχή σύνδεση, και αν δεν έχει καθόλου σύνδεση τότε οπουδήποτε traffic έρχεται απέξω μπλοκάρεται. Στην παρακάτω φωτογραφία βλέπουμε το παράθυρο ρυθμίσεων ενός VPN



Εικόνα 40-VPN

7 Συμπεράσματα

Όσο προχωρεί ο καιρός τόσο ποιο πολύ κίνδυνοι υπάρχουν στο διαδίκτυο και έτσι συνεχώς κάθε εταιρία λογισμικού προσπαθεί να φτιάξει τεχνολογίες για την αποτροπή αυτών των κινδύνων στις εκδόσεις νέων λειτουργικών, εφαρμογών, υπηρεσιών και συσκευών, χωρίς να αποτελεί εξαίρεση η Microsoft. Γενικά, για όσο διάστημα ο άνθρωπος γράφει κώδικα, θα βλέπουμε κενά ασφαλείας που θα ανακαλύπτονται μελλοντικά.

Βιβλιογραφία

[1] Logal Kugler, Windows 7 security features
http://www.computerworld.com/article/2519599/microsoft-windows/five-windows-7-security-features-that-businesses-need-to-know-about.html

[2] Shane O'Neill, the best security features in windows 7 http://www.techworld.com/operating-systems/the-best-security-features-in-windows-7-3211725/

[3] Eric Geier, windows 8 put its hidden security features to work
http://www.pcworld.com/article/2027593/windows-8-put-its-hidden-security-features-to-work-.html

[4] Eric Geier, windows 8 seurity what's new
http://www.pcworld.com/article/255776/windows_8_security_whats_new.html

[5] Alfonso Barreiro, what you should know about windows 8 security features
http://www.techrepublic.com/blog/it-security/what-you-should-know-about-windows-8-security-features/

[6] Peter Bruzzese, windows 8.1 the key security impovements
http://www.infoworld.com/article/2612834/microsoft-windows/windows-8-1--the-key-security-improvements.html

[7] Paul Thurrott, what's new in windows 8.1 security http://windowsitpro.com/windows-8/whats-new-windows-8-1-security

[8] Mary Branscombe, windows 8.1 security what's been improved
http://www.techradar.com/news/software/operating-systems/windows-8-1-security-what-s-been-improved-1156705

[9] Kelly Jackson Higgins, Microsoft windows 10 three security features to know about
http://www.darkreading.com/cloud/microsoft-windows-10-three-security-features-to-know-about/d/d-id/1320650

[10] Jim Alkove, windows 10 security and intentity protection for the modern world
http://blogs.windows.com/business/2014/10/22/windows-10-security-and-identity-protection-for-the-modern-world/

[11] John Brandon, three important security features arriving with windows 10
http://www.techradar.com/news/software/operating-systems/three-important-security-features-arriving-with-windows-10-1272224

[12] Tom Spring, top windows 10 security features explained http://www.crn.com/slide-shows/security/300077470/top-windows-10-security-features-explained.htm

[13] Ricky & Monique Magalhaes, windows 10 privacy and security features at a glance
http://www.windowsecurity.com/articles-tutorials/windows_10_security/windows-10-privacy-and-security-features-glance-part1.html

[14] Gordon Gottsegen, the windows 10 security settings you need to know
http://www.wired.com/2015/08/windows-10-security-settings-need-know/