www.plant-management.gr

PLANT management

ΤΕΥΧΟΣ 206 - ΑΠΡΙΛΙΟΣ-ΙΟΥΝΙΟΣ 2009

Λύσεις Track and Trace

Φωτοβολταϊκά και περιβάλλον

Παρουσίαση της ΒΙΠΕ Ηπείρου

Αφιέρωμα Συσκευασία


Γ. Αναστασόπουλος


Ε. Δεσπότου


Χ. Πρωτογερόπουλος


Ο. Γαβρανίδης

ΚΩΔΙΚΟΣ 1561

Οι Ρόλοι ως Μέσο Οργάνωσης της Πρόσβασης στα Πληροφοριακά Συστήματα

του Σωτήρη Γκαγιαλή, Ερευνητή ΕΜΠ, Σχολή Μηχανολόγων Μηχανικών, Τομέας Βιομηχανικής Διοίκησης & Επιχειρησιακής Έρευνας

Η ασφάλεια της πληροφορίας στο σύγχρονο επιχειρησιακό περιβάλλον μπορεί να επιτευχθεί μέσω του τρίπτυχου διοίκησης της ασφάλειας, διαχείρισης των κινδύνων και συμμόρφωσης με κατάλληλα πρότυπα. Το ιδανικό μοντέλο ελέγχου και η ασφάλεια της πληροφορίας περιλαμβάνει συστατικά όπως τα δικαιώματα πρόσβασης (authorizations), το διαχωρισμό των καθηκόντων (segregation of duties), τη δυνατότητα ελέγχου και απολογισμού (auditability), καθώς και το δομημένο έλεγχο της πρόσβασης. Ο πιο αποτελεσματικός τρόπος συνδυασμού και υλοποίησης αυτών είναι μέσω της προσέγγισης ελέγχου της πρόσβασης των χρηστών βάσει ρόλου (Role Based Access Control ή RBAC). Η προσέγγιση αυτή περιλαμβάνει τη δημιουργία οργανωτικών ρόλων για συγκεκριμένες εργασίες εντός του οργανισμού και στη συνέχεια τη σύνδεση του προσωπικού με συγκεκριμένους ρόλους. Οι ρόλοι αυτοί, που σχετίζονται περισσότερο με την οργάνωση παρά με τα πληροφοριακά συστήματα, στη συνέχεια υλοποιούνται τεχνικά μέσω ενός συστήματος ελέγχου της πρόσβασης και τα σχετικά δικαιώματα αντιστοιχίζονται στους συστημικούς ρόλους. Με τον τρόπο αυτό, σε κάθε μέλος του οργανισμού ανατίθενται συγκεκριμένα δικαιώματα πρόσβασης σύμφωνα με τους ρόλους τους οποίους λαμβάνει. Η χρήση των ρόλων διευκολύνει τον έλεγχο της πρόσβασης στα πληροφοριακά συστήματα, που αντικατοπτρίζουν τις πραγματικές απαιτήσεις των θέσεων εργασίας του προσωπικού του οργανισμού. Ο έλεγχος της πρόσβασης βάσει ρόλων επιτρέπει την αποφυγή απομονωμένων και μονοδιάστατων λύσεων που γενικά περιορίζουν την αποτελεσματική λειτουργία ενός

οργανισμού, αντιμετωπίζοντας τον έλεγχο και τη διαχείριση των δικαιωμάτων πρόσβασης με ολοκληρωμένο τρόπο για το σύνολο των πληροφοριακών συστημάτων.

Χαρακτηριστικά ενός Εργου Ελέγχου της Πρόσβασης Βάσει Ρόλων

Τα έργα ελέγχου της πρόσβασης των χρηστών βάσει ρόλων χαρακτηρίζονται σε αρκετές περιπτώσεις ως δαπανηρές ή χωρίς τέλος προσπάθειες, δημιουργώντας το εύλογο ερώτημα αν αξίζει τον κόπο και το κόστος ο σχεδιασμός και η υλοποίηση μίας τέτοιας λύσης. Κατά συνέπεια, είναι πολύ σημαντικό να κατανοηθούν και να καταγραφούν οι πιθανοί επιχειρησιακοί στόχοι και τα οφέλη που θα μπορούσαν να οδηγήσουν σε επιτυχημένες υλοποιήσεις.

Ανάλογα με το είδος ή το μέγεθος του οργανισμού, οι κύριοι στόχοι που θα πρέπει να ληφθούν υπόψη, αποτελώντας τους παράγοντες που καθορίζουν ένα έργο εισαγωγής του ελέγχου της πρόσβασης των χρηστών βάσει ρόλων περιλαμβάνουν:

- Την επιβολή πολιτικών ασφάλειας στα πληροφοριακά συστήματα
- Τη διαχείριση του κύκλου ζωής των χρηστών
- Την απαίτηση συμμόρφωσης με πρότυπα και κανονισμούς
- Την επίτευξη ανταγωνιστικού πλεονεκτήματος
- Τη μείωση του κόστους διαχείρισης

Κάθε προσπάθεια υλοποίησης ενός έργου ελέγχου της πρόσβασης των χρηστών βάσει ρόλων θα πρέπει επίσης να προσδιορίζει το αναμενόμενο αποτέλεσμα σύμφωνα με τον αρχικό προσδιορισμό των απαιτήσεων, προκειμένου να ικανοποιήσει:

- Την αποδοτική λειτουργία του οργανισμού και τη βελτίωση των επιχειρησιακών διαδικασιών
- Τον προσδιορισμό του διαχωρισμού των καθηκόντων και την επιβολή του
- Τη βελτιωμένη διαχείριση των εξουσιοδοτήσεων και τον έλεγχο της πρόσβασης των χρηστών στα πληροφοριακά συστήματα
- Το βελτιωμένο έλεγχο και απολογισμό
- Τη δυνατότητα να αντιμετωπιστούν οι διαπιστώσεις του ελέγχου (audit)
- Τη μείωση του ρίσκου
- Τη συνέπεια στον προσδιορισμό ρόλων που ανατίθενται στους χρήστες
- Την ευκολία διαχείρισης
- Τη βελτίωση της ικανοποίησης των χρηστών

Μοντέλα Ελέγχου της Πρόσβασης Βάσει Ρόλων

Τα μοντέλα ελέγχου της πρόσβασης των χρηστών βάσει ρόλων χρησιμοποιούν ιεραρχίες ρόλων και πλήθος περιορισμών της πρόσβασης και επομένως είναι δυνατόν μέσω των ρόλων να αποτυπωθεί μία πληθώρα πολιτικών ασφαλείας των πληροφοριακών συστημάτων. Επιπλέον, η χρήση ρόλων για την οργάνωση των δικαιωμάτων πρόσβασης απλοποιεί τον τρόπο διαχείρισης της ασφάλειας στην πρόσβαση σε λειτουργίες και δεδομένα. Για παράδειγμα, εάν ένας χρήστης μετακινηθεί από ένα Τμήμα του οργανισμού σε ένα άλλο, τότε απλά μπορούν να του ανατεθούν οι ρόλοι του νέου Τμήματος και της νέας θέσης εργασίας και να του αφαιρεθούν οι παλαιοί ρόλοι. Χωρίς τη χρήση ενός μοντέλου ρόλων θα έπρεπε να ανακληθούν ξεχωριστά οι παλαιές άδειες πρόσβασης του χρήστη και να του παρασχεθούν νέες ειδικές άδειες πρόσβασης. Επιπλέον, ενδεχομένως να έπρεπε να επιβληθούν περιορισμοί διαχείρισης προκειμένου να αποφευχθούν κρούσματα χρήσης της πληροφορίας με αδόκιμο ή δόλιο τρόπο.

Ο διαχωρισμός των καθηκόντων (separation of duties) αποτελεί ένα σημαντικό ζήτημα το οποίο είναι απολύτως σχετικό με τη υιοθέτηση των ρόλων για τον έλεγχο της πρόσβασης των χρηστών. Η σημασία του διαχωρισμού των καθηκόντων έγκειται στη μείωση του κινδύνου απάτης, μη επιτρέποντας στον οποιονδήποτε να έχει επαρκή πρόσβαση μέσα στο σύστημα για να διαπράξει την απάτη. Τέτοιοι περιορισμοί πρόσβασης μπορούν εύκολα να εκφραστούν χρησιμοποιώντας τη λογική του διαχωρισμού των καθηκόντων στο μοντέλο των ρόλων, στις αναθέσεις ρόλων σε χρήστες και στις αναθέσεις των δικαιωμάτων πρόσβασης στους ρόλους.

Ο έλεγχος της πρόσβασης βάσει ρόλων προσφέρει αρκετά πλεονεκτήματα σε σχέση με τις κλασσικές μεθόδους απόδοσης πρόσβασης στα πληροφοριακά συστήματα απευθείας στους χρήστες. Στα πλεονεκτήματα αυτά περιλαμβάνεται η απλοποίηση της διαχείρισης χρηστών και δικαιωμάτων πρόσβασης καθώς και η δυνατότητα αποτελεσματικού ελέγχου και απολογισμού των εξουσιοδοτήσεων των χρηστών. Εφαρμόζοντας ένα μοντέλο ελέγχου της πρόσβασης βάσει ρόλων, τα δικαιώματα πρόσβασης ανατίθενται στους ρόλους και όχι στους χρήστες. Επομένως οποιαδήποτε τροποποίηση στα δικαιώματα πρόσβασης γίνεται στους ρόλους και αυτομάτως τροποποιούνται τα δικαιώματα των χρηστών που τους έχουν λάβει, μειώνοντας το διαχειριστικό φόρτο. Επιπλέον, η ανάθεση ρόλων στους χρήστες και η αφαίρεση ρόλων από αυτούς μπορεί να γίνεται αυτόματα χρησιμοποιώντας ειδικά συστήματα ροής εργασίας, τα οποία διευκολύνουν αρκετά τη σχετική διαδικασία. Η παροχή πληροφορίας στους χρήστες περιορίζεται σε αυτήν που προβλέπουν οι ρόλοι που ανατίθενται σε αυτούς, ενώ είναι ευκολότερη η επιβολή της όποιας πολιτικής ασφάλειας των πληροφοριών.

Οφέλη από τη χρήση των ρόλων υφίστανται και στο διαχειριστικό κόστος, καθώς οι διαχειριστές των

συστημάτων εφαρμόζουν τους ρόλους για το σύνολο των πληροφοριακών συστημάτων. Τέλος, ο έλεγχος της πρόσβασης βάσει ρόλων παρέχει την απαιτούμενη συμμόρφωση με κανονισμούς και πρότυπα, τα οποία είναι υποχρεωμένος να εφαρμόζει ο οργανισμός.

Εφαρμογή Μοντέλων Διαχείρισης των Ρόλων

Σήμερα υπάρχουν αρκετές δημοσιεύσεις σε θεωρητικό επίπεδο αλλά και πρότυπα που στοχεύουν στον προσδιορισμό των ρόλων, τη δημιουργία τους και τη συστημική υλοποίησή τους. Η πιο ευρέως γνωστή προσέγγιση είναι η «NIST RBAC» η οποία καθιερώθηκε ως πρότυπο το 2004 (ANSI INCITS 359), προσδιορίζοντας τις αρχές και τους κανόνες για την υιοθέτηση ενός μοντέλου Ελέγχου της Πρόσβασης Βάσει Ρόλων (RBAC).

Η διαχείριση των ρόλων αποτελεί επιχειρησιακό πρόβλημα που έχει επίδραση στα πληροφοριακά συστήματα και για το λόγο αυτό απαιτεί συγκεκριμένους χειρισμούς. Πριν την υλοποίηση οποιουδήποτε μοντέλου ελέγχου της πρόσβασης των χρηστών με τη χρήση ρόλων, θα πρέπει να έχουν προηγηθεί ορισμένα απαραίτητα βήματα, συμπεριλαμβανομένων της δημιουργίας μίας ομάδας διαχείρισης των ρόλων, της καθιέρωσης μίας διαδικασίας σχετικής με τον κύκλο ζωής των ρόλων στο πλαίσιο μίας συνολικής προσέγγισης για τη διαχείριση των δικαιωμάτων πρόσβασης και των χρηστών του οργανισμού.

Ο κύκλος ζωής των ρόλων, γενικά περιλαμβάνει τις φάσεις του προσδιορισμού των ρόλων, της απόδοσής τους στους χρήστες, της ανασκόπησης και ελέγχου των δικαιωμάτων πρόσβασης, της συντήρησης των ρόλων και της αναθεώρησης αυτών όποτε κριθεί απαραίτητο. Στην αγορά υπάρχουν αρκετά εργαλεία διαχείρισης του κύκλου ζωής των ρόλων, τα οποία μπορούν να βοηθήσουν στην υιοθέτηση των βέλτιστων πρακτικών, αλλά σε καμία περίπτωση δεν θα πρέπει να υιοθετηθούν άκριτα για την επίτευξη άμεσων αποτελεσμάτων, καθώς κάθε οργανισμός έχει αρκετές ιδιαιτερότητες οι οποίες θα πρέπει να ληφθούν προσεκτικά υπόψη.

Από τη μία, η δημιουργία και υλοποίηση των ρόλων μπορεί να αντιμετωπιστεί ως έργο πληροφορικής, όπου στην περίπτωση αυτή αναζητείται η λύση με μία προσέγγιση bottom-up, σύμφωνα με την οποία οι ρόλοι διαμορφώνονται για ένα σύνολο δικαιωμάτων πρόσβασης στα πληροφοριακά συστήματα.

Από την άλλη, η αντιμετώπιση των ρόλων από την επιχειρησιακή οπτική οδηγεί σε προσεγγίσεις top-down, όπου χρησιμοποιούνται τα οργανογράμματα ως βασικά συστατικά στη διαμόρφωση των ρόλων. Η καταλληλότερη προσέγγιση βρίσκεται κάπου στη μέση και θα πρέπει να είναι υβριδική, ανάλογα με την κάθε εξεταζόμενη περίπτωση. Η διαμόρφωση των ρόλων θα πρέπει σίγουρα να ξεκινάει από την καταγραφή των θέσεων εργασίας των υπαλλήλων και των περιγραφών των δραστηριοτήτων που πραγματοποιούν μέσα από τα πληροφοριακά συστήματα, αλλά θα πρέπει παράλληλα να λαμβάνεται υπόψη ο τρόπος λειτουργίας και παραμετροποίησης του κάθε πληροφοριακού συστήματος.

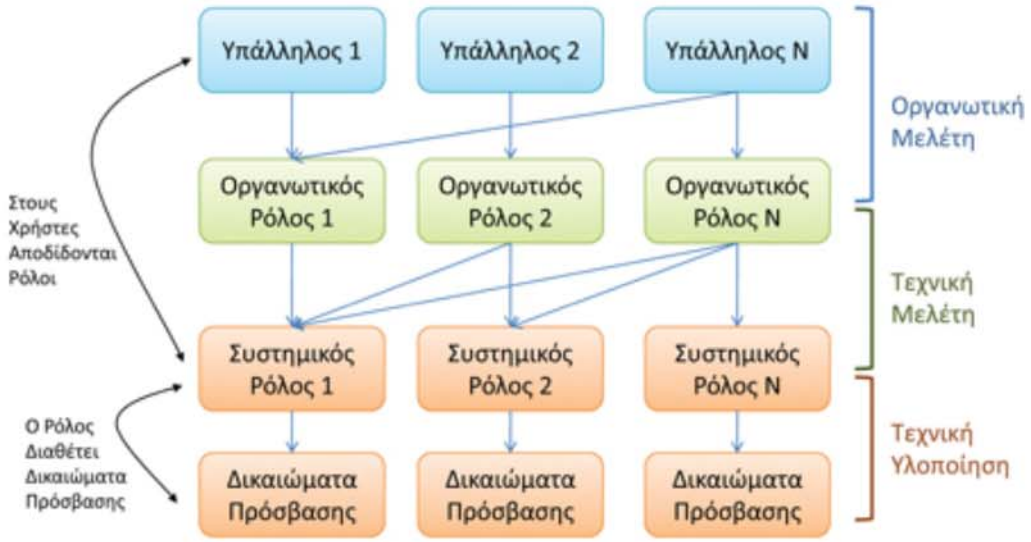
Χαρακτηριστικό είναι το παράδειγμα των ERP συστημάτων που καλύπτουν το σύνολο των επιχειρησιακών διαδικασιών με τη χρήση συγκεκριμένων κινήσεων (transactions), χωρισμένων σε υποσυστήματα (modules). Η διαμόρφωση των ρόλων για τέτοια συστήματα θα πρέπει να περιλαμβάνει οπωσδήποτε μία ανάλυση του τρόπου χρήσης του συστήματος από κάθε χρήστη σε αντιπαραβολή με το job description της θέσης εργασίας του. Απαιτείται η αναλυτική καταγραφή των κινήσεων που θα χρησιμοποιεί ο κάθε χρήστης ανά υποσύστημα του ERP σε σχέση με τις εργασίες που του έχουν ανατεθεί και στη συνέχεια θα πρέπει να εξετάζονται προσεκτικά τα δικαιώματα πρόσβασης που θα αποδοθούν στον υπό διαμόρφωση ρόλο για την εκτέλεση των κινήσεων αυτών χωρίς να παραβιάζονται οι περιορισμοί πρόσβασης στην πληροφορία από μη σχετικές θέσεις εργασίας και χρήστες.

Ο καθορισμός πολύ λεπτομερώς ορισμένων ρόλων μπορεί να οδηγήσει σε επίπονες προσπάθειες που διαρκούν πολύ καιρό ή που τελικά τα μοντέλα των ρόλων δεν είναι εφικτά να υλοποιηθούν.

Στην αντίθετη περίπτωση, οι πολύ γενικοί ρόλοι μπορεί να μην παρέχουν τα επιθυμητά αποτελέσματα ελέγχου και περιορισμού των δικαιωμάτων πρόσβασης. Μία καλή τακτική θα ήταν να εντοπιστούν αρχικά τα κρίσιμα σημεία στα οποία θα πρέπει να δοθεί έμφαση και τα οποία μπορούν (και πρέπει) να δώσουν άμεσα αποτελέσματα ελέγχου της πρόσβασης. Ειδικά για την περίπτωση ενός νέου πληροφοριακού συστήματος μεγάλου εύρους, όπως είναι τα συστήματα ERP, θα πρέπει να ισχύει ο κανόνας: εκκίνηση με κάτι μικρό (βασικοί κρίσιμοι ρόλοι), το οποίο στη συνέχεια βελτιώνεται και επεκτείνεται μέσω μίας επαναληπτικής διαδικασίας αναθεωρήσεων.

Η λογική των ρόλων που δημιουργούνται ενισχύει την αλλαγή της κουλτούρας του οργανισμού αλλά και του τρόπου που σκέφτονται και ενεργούν οι άνθρωποι. Δεν θα πρέπει να υποτιμάται η διάσταση της επίδρασης των ρόλων στην επιχειρησιακή κουλτούρα και για το λόγο αυτό είναι αναγκαίο να υπάρχει σχέδιο διαχείρισης των αλλαγών και επικοινωνίας του έργου, έτσι ώστε όλοι οι εμπλεκόμενοι να συμμετέχουν ενεργά εξαρχής.

Για την τεχνική διαχείριση των ρόλων στο σύνολο των επιχειρησιακών πληροφοριακών συστημάτων υπάρχουν αρκετές τεχνολογικές λύσεις και μηχανισμοί πιστοποίησης χρηστών και εξουσιοδοτήσεων. Η υλοποίηση τέτοιων λύσεων θα πρέπει να είναι το επόμενο βήμα μετά την



Σχήμα: Η Λογική του Ελέγχου Πρόσβασης με Βάση τους Ρόλους

υλοποίηση των ρόλων προκειμένου να ενοποιηθούν οι έλεγχοι πρόσβασης, να διαχειριστούν οι κίνδυνοι και να εξασφαλιστεί η συμμόρφωση με τους κανονισμούς.

Συμπεράσματα

Μια από τις προκλήσεις που πρέπει να αντιμετωπιστούν κατά την υλοποίηση πληροφοριακών συστημάτων είναι η διαχείριση της πρόσβασης των χρηστών. Οι ρόλοι αποτελούν το μέσο αποτελεσματικής διαχείρισης και ελέγχου της πρόσβασης στα επιχειρησιακά συστήματα. Οι ρόλοι αντιμετωπίζονται συχνά ως ένα σύνθετο και απαιτητικό έργο για τον οργανισμό.

Η εμπειρία από παρόμοια έργα καταδεικνύει ότι η πολυπλοκότητα των μοντέλων ρόλων είναι περιορισμένη και διαχειρίσιμη για τα περισσότερα πληροφοριακά συστήματα, ακόμα και για τα ERP συστήματα όπως το SAP. Σημεία κλειδιά για τον προσδιορισμό και την υλοποίηση ρόλων χαρακτηρίζονται η χρήση ξεκάθαρα ορισμένων επιπέδων ρόλων που συνθέτουν το σύνολο των ρόλων για τον οργανισμό, η ύπαρξη συστηρά καθορισμένων εξουσιοδοτήσεων για τους ρόλους στο πλαίσιο της διαχείρισης του κύκλου ζωής τους, καθώς και η διάκριση του συνολικού έργου σε επιμέρους έργα για τους οργανωτικούς ρόλους εντός της επιχείρησης και τους συστημικούς ρόλους ανά πληροφοριακό σύστημα. Είναι πιο εύκολο να διαχειριστούν οι ρόλοι σε οργανωτικό επίπεδο και στη συνέχεια να συνδεθούν με άλλους συστημικούς ρόλους, παρά να διαχειρίζονται τα δικαιώματα πρόσβασης ανεξάρτητα για κάθε ένα πληροφοριακό σύστημα.

Σε κάθε περίπτωση, οι προσπάθειες σχεδιασμού και υλοποίησης ρόλων θα πρέπει να βασίζονται στις ανάγκες της επιχείρησης και επομένως, είναι κρίσιμο να εξασφαλίζεται η συμμετοχή όλων των εμπλεκομένων. Η προσέγγιση που θα ακολουθεί θα πρέπει να είναι ολιστική, ενσωματώνοντας τις οπτικές της επιχειρησιακής οργάνωσης και των διαδικασιών, της πληροφορικής, καθώς και της διαχείρισης της πρόσβασης και του ελέγχου, όλα με έμφαση στην ίδια την επιχείρηση και τις ιδιαιτερότητές της. Προκειμένου να είναι επιτυχημένη η υλοποίηση των ρόλων, είναι απαραίτητο η διαμόρφωσή τους πρώτα από όλα να προσαρμόζεται στην επιχείρηση και στις λειτουργίες της, παρά στα πληροφοριακά συστήματα. Οι ρόλοι δεν αφορούν μόνο τις εφαρμογές της πληροφορικής και τον έλεγχο της πρόσβασης των χρηστών σε αυτές, αλλά απεικονίζουν τη σχέση των ανθρώπων με τον οργανισμό. Για το λόγο αυτό, ένα έργο ανάπτυξης ενός μοντέλου ρόλων για τον έλεγχο της πρόσβασης των χρηστών στα συστήματα της επιχείρησης, θα πρέπει να αντιμετωπίζεται τόσο ως έργο πληροφορικής όσο και ως έργο οργάνωσης.

Ο κ. Γκαγκαλής είναι Μηχανολόγος Μηχανικός, στέλεχος του Τομέα Βιομηχανικής Διοίκησης & Επιχειρησιακής Έρευνας του ΕΜΠ. Ειδικεύεται σε θέματα ανασχεδιασμού των επιχειρησιακών διαδικασιών, εφοδιαστικής αλυσίδας και πληροφορικών συστημάτων. Διαθέτει εμπειρία σε πλήθος εφαρμοσμένων μελετών σε ιδιωτικές επιχειρήσεις και δημόσιους οργανισμούς, καθώς επίσης διδακτικό και ερευνητικό έργο στο ΕΜΠ.