ΕΦΑΡΜΟΓΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΣΕ MICROSOFT ΥΠΟΔΟΜΗ

Διπλωματική Εργασία

ΑΘΑΝΑΣΟΠΟΥΛΟΣ ΝΙΚΟΛΑΟΣ ΜΤΕ1703
nathanaso@ssl-unipi.gr

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Τις τελευταίες δεκαετίες η τεχνολογική εξέλιξη υπήρξε ραγδαία. Η τεχνολογία όλο και περισσότερο εισήλθε στην καθημερινότητα του σύγχρονου ανθρώπου, επηρεάζοντας τον τρόπο με τον οποίο εργάζεται, την κοινωνική του ζωή, το βιοτικό του επίπεδο. Τα προϊόντα τεχνολογίας , ως καταναλωτικά αγαθά, γίνονται όλο και πιο φθηνά με αποτέλεσμα περισσότερες κοινωνικές ομάδες να έχουν πρόσβαση σε αυτά. Κρίσιμες κοινωνικές υπηρεσίες όπως η παροχή ενέργειας και ύδρευσης, μεταφορές, υπηρεσίες υγείας αλλά και οι επιχειρήσεις, ανεξάρτητα του αντικειμένου της δραστηριότητας τους έχουν συνδεθεί άρρηκτα με πληροφοριακά συστήματα. Εύλογα τίθεται το ερώτημα, πόσο επηρεάζει μια πιθανή αποτυχία ενός πληροφοριακού συστήματος την σύγχρονη κοινωνική και οικονομική δομή; Πως μπορεί να μετρηθεί το αποτέλεσμα μιας πιθανής αποτυχίας; Τι μέτρα προστασίας απαιτούνται σε κάθε περίπτωση; Μέσω της επιστήμης της ασφάλειας πληροφοριακών συστημάτων, οι οργανισμοί και οι επιχειρήσεις καλούνται να απαντήσουν στα παραπάνω ερωτήματα.

Ο τρόπος με τον οποίο αντιμετωπίζει ο κάθε οργανισμός τον τομέα της ασφάλειας ποικίλει. Σε πολλές περιπτώσεις, η ασφάλεια νοείται ως σύνολο τεχνολογικών μέτρων για την προστασία των πληροφοριακών συστημάτων και των πληροφοριών που διαχειρίζεται ο οργανισμός. Σε άλλες, η ασφάλεια χρησιμοποιείται ως μέσο ελέγχου κόστους και αύξησης της απόδοσης του πληροφοριακού συστήματος. Ανάλογα με το βαθμό εξάρτησης ενός οργανισμού με τρίτα μέρη, η ασφάλεια χρησιμοποιείται για τη διασφάλιση των νομικών και συμβατικών υποχρεώσεων, τη διασφάλιση της επιχειρησιακής συνέχειας κ.α.

Η ασφάλεια δεν αφορά αποκλειστικά την τεχνολογία ,τους ανθρώπους ή τη νομοθεσία. Είναι ένα *οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Π.Σ., αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή*.[1] Επομένως για να εφαρμοστεί η ασφάλεια ως σύνθετη διεργασία, απαιτείται από τους οργανισμούς να εφαρμόσουν Συστήματα Διαχείρισης (ITSM). Το τμήμα του συνολικού Συστήματος Διαχείρισης του οργανισμού, που αφορά στην ασφάλεια πληροφοριών ονομάζεται Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).

Η στρατηγική του οργανισμού, ο σκοπός του, οι πολιτικές και οι διεργασίες οι οποίες τον διέπουν, η κουλτούρα των ανθρώπων, η αλληλεπίδραση με τρίτα μέρη, είναι μερικοί από τους παράγοντες οι οποίοι θα πρέπει να λαμβάνονται υπόψη όταν σχεδιάζονται τα Συστήματα Διαχείρισης. Βασικός τους στόχος είναι να προσδίδουν αξία, συνεισφέροντας στην επίτευξη των στόχων που θέτει ο εκάστοτε οργανισμός. Διεθνή πρότυπα, βέλτιστες πρακτικές και μεθοδολογίες, έχουν δημοσιευθεί ώστε να βοηθήσουν τα εμπλεκόμενα μέρη να εφαρμόσουν

[1] ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ “Εισαγωγικά θέματα”- Σωκράτης Κάτσικας

αποτελεσματικά Συστήματα Διαχείρισης. Ανάλογα το κάθε ένα, επικεντρώνεται σε συγκεκριμένους τομείς πληροφοριακής διοίκησης (COBIT, ITIL, ISO, AGILE, DEVOPS).

Ως θεωρητική βάση για την ανάπτυξη της διαδικτυακής εφαρμογής που θα παρουσιαστεί στην παρούσα εργασία, επιλέχθηκε η βιβλιοθήκη ITIL. Κύριοι πυλώνες της συγκεκριμένης μεθοδολογίας είναι η ευθυγράμμιση του πληροφοριακού συστήματος ενός οργανισμού με τον επιχειρησιακό του ρόλο και η παροχή ποιοτικής υπηρεσίας προς τον τελικό καταναλωτή. Πραγματεύεται την καλύτερη κατανόηση των αναγκών του οργανισμού ως προς της αρχές της ασφάλειας (διαθεσιμότητα, ακεραιότητα ,εμπιστευτικότητα), τη διαχείριση του κόστους και της συνολικής απαιτούμενης προσπάθειας.

ΠΕΡΙΓΡΑΦΗ ΒΑΣΙΚΩΝ ΕΝΝΟΙΩΝ

Η βιβλιοθήκη ITIL είναι ένα σύνολο βέλτιστων πρακτικών το οποίο περιλαμβάνει όλες τις πτυχές ενός Συστήματος Διαχείρισης. Ακολουθεί μια δομή πυραμίδας στην κορυφή της οποίας περιγράφονται οι βέλτιστες πρακτικές για το σχεδιασμό της στρατηγικής του πληροφοριακού συστήματος (Service[2] Strategy). Η στρατηγική περιγράφει έναν κύκλο διαχείρισης της υπηρεσίας που λαμβάνει ο τελικός καταναλωτής μέσω του σχεδιασμού, της μεταφοράς και των απαραίτητων λειτουργιών της υπηρεσίας (Service Design – Service Transition – Service Operation) .

Η διαδικτυακή εφαρμογή που θα παρουσιαστεί στην παρούσα εργασία, θα μπορεί να διαχειριστεί όλες τις διεργασίες της Διαχείρισης Περιστατικών η οποία περιλαμβάνεται στο Service Operation. Μια συνήθης ροή περιλαμβάνει τη διαδικασία εξακρίβωσης ενός περιστατικού και την καταγραφή του, την κατηγοριοποίηση και την προτεραιοποίηση ανάλογα με όρους που θέτει ο κάθε οργανισμός, την ανάθεση του καταγεγραμμένου αιτήματος σε ομάδες επίλυσης, την επίλυση και την καταγραφή της , την ενημέρωση του τελικού χρήστη για την αποκατάσταση της υπηρεσίας. Βασικός σκοπός της Διαχείρισης Περιστατικών κατά ITIL, είναι η αποκατάσταση της υπηρεσίας το συντομότερο δυνατό σε περιπτώσεις μη αναμενόμενης λειτουργίας ή μειωμένης απόδοσης.

Ως υποσύνολο της διαδικασίας Διαχείρισης Περιστατικών, η εφαρμογή θα μπορεί να διαχειριστεί και περιστατικά ασφάλειας[3]. Λόγω του ότι οι διαδικασίες Διαχείρισης Περιστατικών Ασφάλειας διαφέρουν μεταξύ των οργανισμών, η εφαρμογή θα μπορεί να εισάγει πληροφορίες

[2] “A service is a means of delivering value to customers by facilitating outcomes customers want to achieve, but without the ownership of specific costs and risks.”

[3] Περιστατικό ασφάλειας, είναι ένα μοναδικό γεγονός ή μια ακολουθία ανεπιθύμητων γεγονότων που έχουν σημαντική πιθανότητα να θέσουν σε κίνδυνο τις υπηρεσιακές λειτουργίες του οργανισμού ή να απειλήσουν την ασφάλεια πληροφοριών.

για τα βασικά βήματα διαχείρισης που θέτει ο NIST[4]. Τα κύρια βήματα αφορούν τον εντοπισμό και την ανάλυση ενός περιστατικού ασφάλειας, τον περιορισμό, την αντιμετώπιση και την ανάκαμψη της υπηρεσίας, την καταγραφή αναφορών και τις μετέπειτα ενέργειες του οργανισμού οι οποίες σχετίζονται με περιστατικά ασφάλειας.

Σε κάθε περίπτωση διαχείρισης ενός περιστατικού ή ενός περιστατικού ασφάλειας, ο οργανισμός θα πρέπει να αξιοποιεί την εμπειρία και τη γνώση ώστε να βελτιώνει συνεχώς την απόδοση του πληροφοριακού του συστήματος και να περιορίζει τα κόστη. Μέσω της συνεχόμενης καταγραφής των περιστατικών, δύναται να προκύψει μια γνωσιακή βάση δεδομένων (known error database KEDB) η οποία αποτελεί χρήσιμο εργαλείο για τις ομάδες αντιμετώπισης.

ΠΕΡΙΓΡΑΦΗ ΕΦΑΡΜΟΓΗΣ – ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

Η παρούσα εργασία αποτελεί ένα εγχειρίδιο εγκατάστασης διαδικτυακής εφαρμογής η οποία δύναται να εξυπηρετήσει ένα Σύστημα Διαχείρισης. Η εν λόγω εφαρμογή θα μπορεί να διαχειριστεί όλες τις διεργασίες της Διαχείρισης Περιστατικών και Περιστατικών Ασφάλειας και χαρακτηρίζεται από τις παρακάτω δυνατότητες:

- Εξουσιοδοτημένη πρόσβαση βασισμένη σε ρόλους (RBAC)

Οι χρήστες που μπορούν να συνδεθούν στην εφαρμογή, αυθεντικοποιούνται μέσω Directory Services (Microsoft LDAP) και στη συνέχεια λαμβάνουν το κατάλληλο ρόλο εντός της εφαρμογής.

- Προσαρμοσμένη επιφάνεια χρήστη

Η κάθε ομάδα μέσω του RBAC εξουσιοδοτείται να βλέπει τις αντίστοιχες φόρμες καταγραφής ή/και ανάθεσης συμβάντων

- Επιλογή περιστατικού από προκαθορισμένο κατάλογο υπηρεσιών (service catalog)

Για να μην καταναλώνονται άσκοπα ανθρώπινοι πόροι, οι χρήστες μπορούν να δηλώσουν συμβάντα αποκλειστικά από κατάλογο υπηρεσιών που προσφέρει ο οργανισμός.

- Αυτόματη προτεραιοποίηση συμβάντων

[4] National Institute of Standards and Technology

Η εφαρμογή προτεραιοποιεί τα συμβάντα ως αποτέλεσμα του συνδυασμού κρισιμότητας και επίπτωσης στον οργανισμό.

- Αυτόματη ανάθεση σε ομάδες

Η εφαρμογή αναθέτει αυτόματα συμβάντα ή περιστατικά ασφάλειας σε προκαθορισμένες ομάδες.

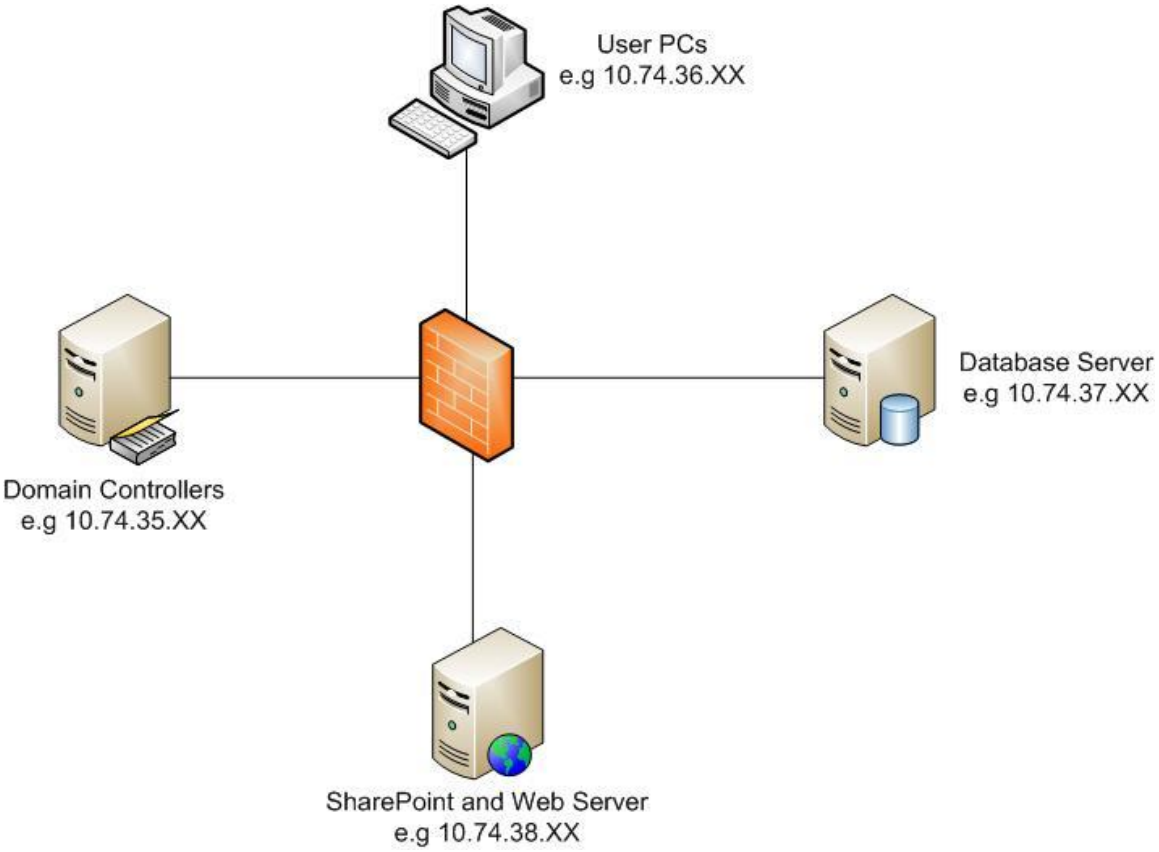
- Δημιουργία KEDB

Οι χρήστες της εφαρμογής μπορούν να αναζητούν περιστατικά χρησιμοποιώντας λέξεις κλειδιά, με σκοπό την αποκατάσταση της υπηρεσίας στο βέλτιστο δυνατό χρόνο.

Για την ορθή αντιμετώπιση ενός περιστατικού, οι χρήστες καλούνται να εκτελέσουν συγκεκριμένες ενέργειες, ανάλογα με το ρόλο που τους έχει αποδοθεί. Ένα σύνηθες διάγραμμα ροής παρουσιάζεται σε επόμενη ενότητα. Όσο αφορά τη διαδικασία αντιμετώπισης περιστατικών ασφάλειας, λόγω του ότι διαφέρει σημαντικά από οργανισμό σε οργανισμό δεν παρουσιάζεται συγκεκριμένο διάγραμμα. Αναφέρονται όμως χαρακτηριστικοί ρόλοι που περιέχονται σε διαδικασίες προτύπων και βέλτιστων πρακτικών (υπεύθυνος ασφάλειας, ομάδα διαχείρισης περιστατικών ασφάλειας κτλ).

ΔΙΚΤΥΑΚΗ ΠΡΟΕΤΟΙΜΑΣΙΑ

Στο παρακάτω διάγραμμα παραγράφεται μια παραγωγική εγκατάσταση, ενώ ο πίνακας περιγράφει τις απαραίτητες επικοινωνίες μεταξύ των συστημάτων.



Source	Destination	Ports
User PC	Domain Controllers	Microsoft-DS: port 445 TCP, UDP Kerberos: port 88 TCP, UDP LDAP: port 389 UDP DNS: port 53 TCP, UDP RPC: Dynamically-assigned ports TCP, unless restricted
User PC	SharePoint Servers	HTTP-HTTPS: 80 ,443 or custom web application configured port
SharePoint Servers	Database Servers	MS-SQL: 1433 TCP MS-SQL: 1434 UDP

SharePoint Servers	Domain Controllers	Microsoft-DS: port 445 TCP, UDP Kerberos: port 88 TCP, UDP LDAP: port 389 UDP DNS: port 53 TCP, UDP RPC: Dynamically-assigned ports TCP, unless restricted EPMAP: port 135 TCP, UDP NTP: port 123 UDP

ΠΡΟΕΤΟΙΜΑΣΙΑ ΥΠΟΔΟΜΩΝ

A.Ενεργοποίηση Directory Services

Για να μπορεί να ελεγχθεί η προσβασιμότητα στην δικτυακή εφαρμογή που θα δημιουργήσουμε αλλά και τις δυνατότητες των χρηστών εντός της εφαρμογής , θα ενεργοποιήσουμε Directory Services. Σε MS Server 2012 R2 με στατική IP διεύθυνση, υλοποιούμε τα παρακάτω:

1. Άνοιγμα Server Manager Console→Manage→Add Roles and Features
2. Στο νέο παράθυρο, στο βήμα Before You Begin →NEXT
3. Στο βήμα Installation Type→Role-based or feature based installation→Next
4. Στο βήμα Server Selection επιλέγουμε τον τρέχοντα server όπου εμφανίζεται η στατική του IP→NEXT
5. Στο βήμα Server Roles→Active Directory Domain Services. Θα εμφανιστεί νέο παράθυρο στο οποίο αναφέρει τα προ απαιτούμενα features που πρέπει να εγκατασταθούν. Επιλέγουμε Include management tools→Add features. Επιστρέφοντας στο αρχικό παράθυρο → Next
6. Στο βήμα Features επιβεβαιώνουμε ότι είναι μαρκαρισμένα τα features .Net Framework 4.5,Group Policy Management, Remote Server Administration Tools, User Interfaces and Infrastructure και Windows PowerShell → Next
7. Στο βήμα AD DS→Next
8. Στο βήμα Confirmation → Restart the destination server automatically if required→Install

Στο σημείο αυτό ο server θα ξεκινήσει να εγκαθιστά όλα τα δομικά στοιχεία του Active Directory. Μπορούμε να κλείσουμε το παράθυρο ή να παρακολουθούμε την εγκατάσταση μέχρι

το σημείο που θα αρχίσει η βασική παραμετροποίηση. Όταν ολοκληρωθεί η εγκατάσταση θα εμφανιστεί μήνυμα Configuration Required . Installation succeeded on *Server.* Στη συγκεκριμένη υλοποίηση ο server ονομάζεται ALLCOMPONENTS.

9. Στο Notifications (εικονίδιο πάνω δεξιά) θα εμφανιστεί ένα κίτρινο τρίγωνο. Πατώντας σε αυτό επιλέγουμε Promote this server to a domain controller
10. Στο βήμα Deployment configuration→Add a new forest και συμπληρώνουμε το όνομα του νέου domain. Για τους σκοπούς της άσκησης το domain θα ονομαστεί myitsm.gr→Next
11. Στο βήμα Domain Controller Options αφήνουμε τα functional levels ως έχουν. Καταχωρούμε τον κωδικό DSRM. Στη συγκεκριμένη άσκηση θα είναι "23@#wesdxc"
12. Στο βήμα DNS options→Next
13. Στο βήμα Additional options επιβεβαιώνουμε ότι αναφέρεται «MYITSM»→Next
14. Στο βήμα Paths αναφέρονται οι διαδρομές αποθήκευσης των δομικών στοιχείων του Active directory →Next
15. Στο βήμα Review Options→ Next (μπορούμε να αποθηκεύσουμε το παραγόμενο PowerShell script για μελλοντική χρήση ή παραμετροποίηση)
16. Στο βήμα Prerequisite Check γίνεται αυτόματος έλεγχος των προ απαιτούμενων. Θα εμφανιστεί μήνυμα All prerequisite checks passed successfully καθώς και μερικά warnings που αφορούν DNS λόγω σχεδίασης. Πατώντας Install θα ξεκινήσει η τελική εγκατάσταση. Ο server θα επανεκκινήσει και στην αρχική του οθόνη θα εμφανιστεί πλέον ο πρώτος χρήστης του νέου domain MYITSM\Administrator

Ο server πλέον είναι ο πρώτος domain controller του domain που δημιουργήσαμε. Πατώντας το εικονίδιο των windows (κάτω δεξιά) , θα έχουν εμφανιστεί τα Administrative tools. Επιλέγοντας από την λίστα το εργαλείο Active Directory Users and Computers, μπορούμε να φτιάξουμε τους χρήστες (users) και τους ρόλους (Security Groups) που θα χρησιμοποιήσουμε μετέπειτα στις ITSM ροές.

Β.Δημιουργία Χρηστών και Ρόλων

Για τις ITSM ροές που θα ακολουθήσουν θα χρησιμοποιήσουμε τους παρακάτω ρόλους (security groups) καθώς και τους χρήστες που θα ανήκουν σε αυτούς. Σε επόμενη ενότητα θα επεξηγήσουμε τη σημασία του κάθε ρόλου και τις ενέργειες που καλείται να κάνει εντός της εφαρμογής που θα δημιουργήσουμε. Ακολουθώντας τα παρακάτω βήματα , ο υποψήφιος υλοποιητής θα δημιουργήσει ένα νέο Organizational Unit (OU) και μέσα σε αυτό τους χρήστες και τους ρόλους.

Δεν χρησιμοποιούμε τους «φακέλους» της δομής που εμφανίζονται ήδη. Αποτελούν διαφορετικά δομικά στοιχεία του Active Directory, ονομάζονται containers και δεν επιδέχονται πολιτικές ασφάλειας από το domain.

1. Από το εικονίδιο των windows→Administrative tools→Active directory users and computers
2. Δεξί κλικ στο domain (myitsm.gr)→New→Organizational Unit→ Στο πεδίο Name: For_ITSM
3. Στο νέο OU “For_ITSM” δεξι κλικ→New→User
4. Συμπληρώνουμε υποχρεωτικά Full Name, User logon Name→Next
5. Συμπληρώνουμε password→Next→Finish
   Για τον κάθε χρήστη που θα χρησιμοποιούμε στην εφαρμογή , επαναλαμβάνουμε το βήμα 3,4,5 χρησιμοποιώντας κάθε φορά μοναδικό User Logon Name.
6. Στο νέο OU “For_ITSM” →δεξι κλικ→New→Group
7. Στο πεδίο Group name συμπληρώνουμε SimpleUsers επιβεβαιώνοντας τις επιλογές Global και Security→OK
   Για τους ρόλους HelpDeskAgents ,SecondLevelSupport, CISO, InformationSecurity, CrisisResponseTeam επαναλαμβάνουμε τα βήματα 6,7.
8. Εντάσσουμε τουλάχιστο 1 χρήστη για τους σκοπούς της άσκησης σε κάθε ένα group. Δεξί κλίκ πάνω σε κάποιο user→Add to a group→ πχ HelpDeskAgents→OK
   Θα πρέπει όλοι οι παραπάνω ρόλοι να περιέχουν έναν χρήστη.

C.Εγκατάσταση βάσεων δεδομένων (SQL Server)

Για τις ανάγκες τις εφαρμογής θα πρέπει να εγκατασταθούν οι κατάλληλες βάσεις δεδομένων. Λόγω του ότι η εφαρμογή που θα δημιουργήσουμε αργότερα θα παραχθεί σε περιβάλλον SharePoint θα εγκαταστήσουμε SQL server. Μπορείτε να βρείτε το λογισμικό από https://www.microsoft.com/en-us/sql-server/sql-server-downloads# σε δοκιμαστική έκδοση 180 ημερών. Κάνοντας mount το ISO αρχείο και δεξί κλικ στο setup application file, Run As Administrator.

1. Στο βήμα Installation→New SQL Server stand-alone installation or add features to existing installation
2. Στο βήμα Product Key→Specify a free edition→Evaluation
3. Στο βήμα License Terms→I Accept the license terms→Next
4. Στο βήμα Microsoft Update→Next
5. Στο βήμα Product Updates→Next (θα εμφανίσει error που μπορούμε να αγνοήσουμε)
6. Στο βήμα Install setup files θα εμφανίσει 2 warnings. Είπαμε και προηγούμενα ότι δεν θα πρέπει σε παραγωγικό περιβάλλον να συνυπάρχουν οι ρόλοι στον ίδιο server, ειδικά ο domain controller δεν θα πρέπει να συνυπάρχει με κανένα άλλο ρόλο.
7. Στο βήμα Feature Selection→Instance Features→Database Engine Services. Επιβεβαιώστε τη διαδρομή εγκατάστασης του SQL server→Next
8. Στο βήμα Instance Configuration→Next
9. Στο βήμα Server Configuration→ SQL Server Agent=Automatic.
10. Στο βήμα Database Engine Configuration→Specify SQL Server Administrators→Add Current User (θα εισαχθεί ως SQL admin ο χρήστης myitsm\administrator)→Next
11. Στο βήμα Ready to Install→Install
12. Ο server μετά την επιτυχή εγκατάσταση θα ζητήσει επανεκκίνηση. Επιβεβαιώστε πως όλα τα features έχουν εγκατασταθεί επιτυχώς →Close

Για να αποκτηθεί πρόσβαση στις βάσεις χρειάζεται να εγκατασταθεί ένα επιπλέον εργαλείο που ονομάζεται SQL Server Management Studio (SSMS) και μπορεί να γίνει download από τη διεύθυνση https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-2017. Στο εικονίδιο του αρχείου που θα κατεβάσετε, δεξί κλικ →Run as administrator

1. Επιλέξτε Install (θα γίνει αυτόματη εγκατάσταση βασικών πακέτων όπως Active Directory Authentication, Net Framework 4.6.1, Visual C++, Visual Studio Shell κ.α)
2. Στο μήνυμα επιτυχούς εγκατάστασης επιλέξτε Restart

3. Στο εικονίδιο των windows->Microsoft SQL Management studio→Server Name: ALLCOMPONENTS→Connect. Επιβεβαιώστε πως ο χρήστης συνδέεται επιτυχώς βλέποντας το πράσινο εικονίδιο της βάσης δίπλα στο ALLCOMPONENTS (SQL Server 14.0.10) .
4. Στο φάκελο Security→Logins→ Επιλέξτε τον χρήστη MYITSM\Administrator→ Δεξι κλικ→Properties→Server Roles
5. Ενεργοποιείστε τους ρόλους dbcreator,public,securityadmin,sysadmin

D.Εγκατάσταση SharePoint Server

Στο σημείο αυτό θα εγκατασταθεί η πλατφόρμα SharePoint 2016 , καθώς και τα επιμέρους προγράμματα τα οποία θα μας βοηθήσουν να σχεδιάσουμε την ITSM εφαρμογή μας. Στην πλατφόρμα θα δημιουργηθούν οι κατάλληλες ροές και θα σχεδιαστούν οι βασικές μετρικές που συνιστά το πρότυπο ITIL. Το λογισμικό είναι διαθέσιμο στη διεύθυνση: https://www.microsoft.com/en-us/download/details.aspx?id=51493 και θα χρειαστούν τα παρακάτω κλειδιά : Enterprise trial product key: NQGJR-63HC8-XCRQH-MYVCH-3J3QR -------- Standard trial product key: RTNGH-MQRV6-M3BWQ-DB748-VH7DM .

Για να ολοκληρωθεί η εγκατάσταση της πλατφόρμας θα πρέπει να εγκατασταθούν συγκεκριμένα προ απαιτούμενα.

- *Application Server Role, Web Server (IIS) Role*
- *Microsoft SQL Server 2012 Native Client*
- *Microsoft ODBC Driver 11 for SQL Server*
- *Microsoft Sync Framework Runtime v1.0 SP1 (x64)*
- *Windows Server AppFabric*
- *Microsoft Identity Extensions*
- *Microsoft Information Protection and Control Client 2.1*
- *Microsoft WCF Data Services 5.6*
- *Microsoft .NET Framework 4.6*
- *Cumulative Update Package 7 for Microsoft AppFabric 1.1 for Windows Server (KB3092423)*
- *Visual C++ Redistributable Package for Visual Studio 2012*
- *Visual C++ Redistributable Package for Visual Studio 2015*

Υπάρχει διαδικασία η οποία λειτουργεί αυτόματα εάν ο server έχει πρόσβαση στο internet αλλά και offline όπου ο υποψήφιος υλοποιητής θα πρέπει να κατεβάσει το κάθε ένα και να τα εγκαταστήσει ξεχωριστά. Θα περιγράψουμε την online διαδικασία. Δεξί κλικ στο ISO αρχείο και mount.

1. Στο αρχείο prerequisiteinstaller δεξι κλικ και run as administrator→Next

2. I accept the terms of the License Agreement→Next
3. Finish

Αν επιλεγεί χειροκίνητη εγκατάσταση θα πρέπει σε κάθε installation αρχείο δεξί κλικ, properties, Unblock στην καρτέλα General. Εγκαταστήστε το κάθε ένα αρχείο με την εντολή πχ D:\prequisiteinstaller.exe /wcfdataservices56:"C:\Prereq\WCFDataServices.exe"

Σε περίπτωση που το Windows Server AppFabric εμφανίζει error κατά την εγκατάσταση του από το auto setup: Στο εικονίδιο των windows δεξι κλικ→System→Advanced System Settings→Enviroment Variables→ Διαγράψτε το " από την τιμή της μεταβλητής PSModulePath. Ολοκληρώστε την εγκατάσταση με την εντολή:

.\WindowsServerAppFabricSetup_x64.exe /I CacheClient,CachingService,CachingAdmin /gac

Κάνοντας mount το ISO αρχείο του SharePoint2016 ,δεξί κλικ στο setup application file, Run As Administrator.

1. Εισάγετε το κλειδί που αναφέρθηκε νωρίτερα→Next
2. I accept the terms of this agreement→Continue
3. Επιλέξτε την διαδρομή εγκατάστασης→ Install Now
4. Run the SharePoint Configuration wizard now→Close
5. Στο νέο παράθυρο του Configuration Wizard→Next
6. Yes στο pop up παράθυρο
7. Create a new server farm→Next
8. Database server= η στατική IP του database server (10.10.10.2 η εικονική μηχανή) , Username και Password (myitsm\administrator - 23@#wesdxc) →Next
9. 23@#wesdxc ως passphrase (2 φορές καταχώρηση)→ Next
10. Επιλογή «Single Server Farm» → Next
11. Στο σημείο αυτό θα ζητηθεί η δικτυακή πόρτα που θα χρησιμοποιεί η εφαρμογή ώστε να κάνουμε Login στην σελίδα διαχείρισης. Επιλέγουμε την 4700 τυχαία (από 1-65535) και NTLM authentication→Next
12. Προκύπτει το τελικό Configuration που περιγράφεται στον τελικό πίνακα→Next
13. Στο pop up παράθυρο εισάγετε να credentials του myitsm\administrator
14. Θα ανοίξει η configuration σελίδα της sharepoint farm.

Ε. Εγκατάσταση Sharepoint designer

Για να μπορέσουμε να επεξεργαστούμε τις τιμές και τα πεδία που θα εισάγουμε στην εφαρμογή θα χρειαστούμε την εφαρμογή Sharepoint Designer που είναι διαθέσιμη στη διεύθυνση https://www.microsoft.com/en-us/download/details.aspx?id=35491 .

1. Από το sharepointdesigner_64bit→Δεξι κλικ και Run as administrator
2. Επιλογή «Accept the license agreement»→Continue
   Επιλογή «Install Now»

ΥΛΟΠΟΙΗΣΗ ΔΙΑΔΙΚΑΣΙΩΝ ΚΑΙ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ

Στο σημείο αυτό θα ξεκινήσουμε την υλοποίηση των ITIL διαδικασιών. Αρχικά θα πρέπει να δημιουργήσουμε στην πλατφόρμα μια νέα web εφαρμογή και πάνω σε αυτή θα δημιουργήσουμε τις βασικές σελίδες και θα εισάγουμε την λογική που επιθυμούμε. Ανοίγοντας την εφαρμογή SharePoint 2016 Central Administration (στη δική μας περίπτωση θα μας ανοίξει την σελίδα http://allcomponents:4700/default.aspx) εισάγουμε τα στοιχεία του myitsm\administrator.

1. Από το Central administration→Application Management→Manage web application
2. Από την καρτέλα web applications→NEW (παρατηρούμε πως υπάρχει ήδη ως εφαρμογή η σελίδα διαχείρισης της φάρμας που δημιουργήσαμε στην προηγούμενη παράγραφο)
3. Στο πεδίο Create a new IIS web site = ITSMPORTAL
4. Στο πεδίο URL = http://ITSMPORTAL:80

Αφήνουμε την default port 80 εκτός αν επιθυμούμε διαφορετικά (πχ 443 αν επιλέξουμε κάποιο certificate ή κάποιο άλλο high port) και επιβεβαιώνουμε τα πεδία DATABASE SERVER και DATABASE NAME (στη δική μας περίπτωση οι τιμές είναι 10.10.10.2 και WSS_Content αντίστοιχα). Στο τέλος του παραθύρου επιλέγουμε OK. Στη κεντρική σελίδα του central administration θα εμφανίζεται πλέον το όνομα και το url της νέας εφαρμογής.

Επόμενο βήμα είναι να δημιουργήσουμε ένα νέο site collection. Θα φιλοξενήσει τις σελίδες της εφαρμογής που μόλις δημιουργήσαμε.

1. Από το central administration→application management→Create site collection
2. Επιβεβαιώνουμε πως στο πεδίο Web Application = http://itsmportal και συμπληρώνουμε τίτλο και μια περιγραφή στα αντίστοιχα πεδία.
3. Στο πεδίο template selection → Collaboration→Team Site

4. Στο πεδίο Primary Site Collection Administrator→Browse→Active Directory και στο πεδίο search=administrator→search. Επιλέγουμε τον χρήστη myitsm\administrator →OK
5. Επιστρέφοντας στην αρχική σελίδα →OK

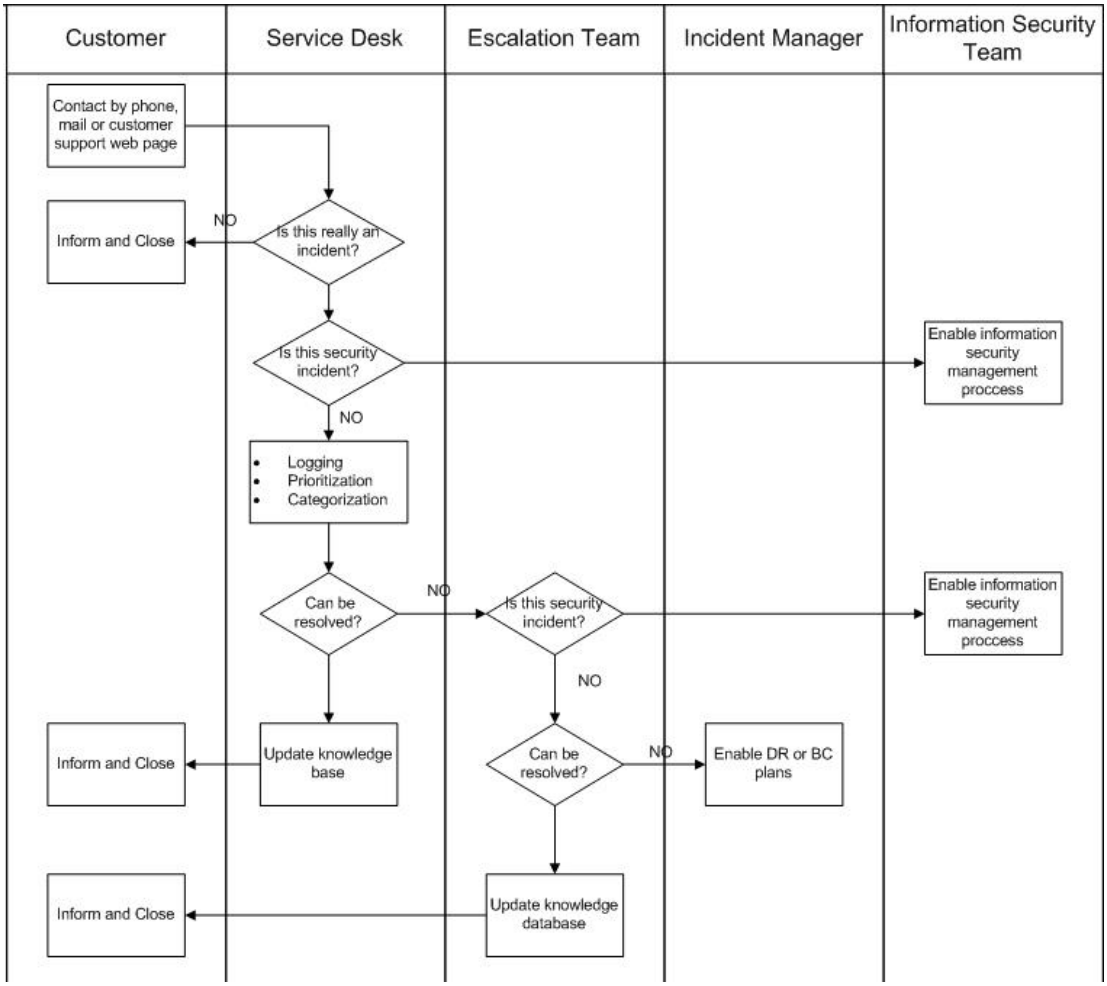
A. Διαχείριση περιστατικών και περιστατικών ασφάλειας

Όπως αναφέρθηκε και προηγούμενα, μια από τις βασικές διαδικασίες που θα υλοποιήσουμε είναι η διαδικασία διαχείρισης περιστατικών. Βασικό μέλημα της διαδικασίας κατά ITIL είναι η επαναφορά μιας υπηρεσίας , μετά από μη αναμενόμενη λειτουργία ή μειωμένη αποδοτικότητα. Δεν περιλαμβάνει βήματα εξεύρεσης της αιτίας του προβλήματος, αυτή αφορά τη διαδικασία διαχείρισης προβλημάτων (problem management). Στόχος είναι η άμεση ανταπόκριση στο αίτημα του χρήστη , ο οποίος δε μπορεί να καταναλώσει μια υπηρεσία.

Βασικό στοιχείο της incident management είναι ο ρόλος του service desk. Της ομάδας δηλαδή η οποία επιφορτίζεται με την αρχική καταγραφή, την κατηγοριοποίηση και την προτεραιοποίηση, την επίλυση ή την ανάθεση σε κατάλληλη ομάδα και την ενημέρωση του αρχικού χρήστη. Το service desk χρησιμοποιεί συνήθως μια γνωσιακή βάση δεδομένων η οποία περιέχει λύσεις για προαναφερθέντα προβλήματα. Είναι ένα πολύ χρήσιμο εργαλείο το οποίο βοηθά στο να διατηρηθούν τα επιθυμητά επίπεδα υπηρεσιών, τα γνωστά SLAs. Στη συγκεκριμένη υλοποίηση ο χρήστης θα έχει τη δυνατότητα να αναζητήσει λύσεις, δίνοντας λέξεις κλειδιά στα κατάλληλα πεδία.

Κατηγοριοποίηση ενός καταγεγραμμένου περιστατικού ,συνήθως δεν επαφίεται αποκλειστικά στην κρίση ενός service desk agent. Οι ITSM εφαρμογές χρησιμοποιούν πίνακες με τιμές που έχουν προκύψει από risk ή business impact analysis, παράδειγμα των οποίων θα παρουσιάσουμε κατά την υλοποίηση.

Η διαδικασία διαχείρισης περιστατικών μπορεί να ενεργοποιήσει και άλλες διαδικασίες, πχ διαχείριση περιστατικών ασφάλειας, διαχείριση προβλημάτων, διαχείριση αλλαγών κτλ. Λόγω του ότι ο σκοπός της εργασίας είναι η υλοποίηση μιας διαδικασίας στην πλατφόρμα Sharepoint και όχι η επεξήγηση του προτύπου ITIL, θα ορίσουμε μια βασική incident management διαδικασία με απλές ροές και εξόδους όπως περιγράφεται στο παρακάτω διάγραμμα.



Όσο αφορά τη διαχείριση περιστατικών ασφάλειας, θα δημιουργήσουμε στην εφαρμογή μας τα κατάλληλα πεδία, ώστε οι χρήστες να μπορούν να ακολουθήσουν τη μεθοδολογία του NIST που συνοψίζεται στον παρακάτω πίνακα.

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

* Recommendations of the National Institute of Standards and Technology, Publication 800-61

Γράφοντας στον iexplorer http://itsmportal , θα εμφανιστεί η αρχική σελίδα της εφαρμογής που θα αρχίσουμε να δημιουργούμε. Στο άνω δεξιά σημείο , στο εικονίδιο γρανάζι, επιλέγουμε Site settings→Site Content Types→Create. Συμπληρώνουμε τα πεδία Name=Incident, Parent content type=List Content type, Parent Content type=Item και επιλέγουμε OK. Σε αυτό το content type που θα χρησιμοποιεί πλέον η εφαρμογή μας, θα δημιουργήσουμε τα κατάλληλα πεδία που θα χρησιμοποιεί η incident management ροή μας.

1. Site settings→Site Content Types→Επιλέγουμε Incident (αυτό που μόλις φτιάξαμε)
2. Στην περιοχή columns→add from new site column
3. Συμπληρώνουμε\επιλέγουμε : Column name=Summary, The type of information in this column is=Multiple lines of text, Require that this column contains information=Yes, Number of lines for editing=10 , αφήνουμε τα υπόλοιπα πεδία ως έχουν.

Επαναλαμβάνουμε τη διαδικασία για Column name=Resolution, Column name=Containment, Column name=Recovery και Column name=Crisis Team Notes.

1. Site settings→Site Content Types→Επιλέγουμε Incident (αυτό που μόλις φτιάξαμε)
2. Στην περιοχή columns→add from new site column
3. Συμπληρώνουμε\επιλέγουμε : Column name=Product, The type of information in this column is=Choice, Type each choice on a separate line = Default, Accounting Application 1, Accounting Application 2, Hyper-V Servers, Network Devices, User Application 1, User Application 2.

Επαναλαμβάνουμε τη διαδικασία για :

Column name	Type each choice on a separate line
Service	Default Accounting Infrastructure Client Facing
Urgency	Default Low Medium High
Impact	Default Low Medium High
Priority	Default Low Medium High Critical
Assigned Group	Service Desk Escalation Team Incident Manager Information Security Team Crisis Response Team
Security Incident	YES NO
Item Status	New Assigned In Progress Resolved

	Closed

1. Site settings→Site Content Types→Επιλέγουμε Incident (αυτό που μόλις φτιάξαμε)
2. Στην περιοχή columns→add from new site column
3. Συμπληρώνουμε\επιλέγουμε : Column name=Incident Created Date, The type of information in this column is=Date and Time, Date & Time format=Date & Time, default value=Today's date.

Επαναλαμβάνουμε τη διαδικασία για :

Column name	Values
Resolution Time Target	The type of information in this column is=Date and Time, Date & Time format=Date & Time, default value=**NONE**
Actual Resolution Time	The type of information in this column is=Date and Time, Date & Time format=Date & Time, default value=**NONE**

1. Site settings→add an app→custom list→ Συμπληρώνουμε το όνομα της λίστας INCIDENTS
2. Από το δεξί μενού επιλέγουμε τη νέα λίστα IINCIDENTS →Καρτέλα LIST→List Settings
3. Επιλέγουμε Advanced Settings→Allow management of content types=YES→OK
4. Επιστρέφοντας στη σελίδα INCIDENTS:SETTINGS επιλέγουμε Add from existing site content types
5. Επιλέγουμε Custom content types και ADD το content type=Incident→OK
6. Επιστρέφοντας στη σελίδα INCIDENTS:SETTINGS επιλέγουμε Change new button order and default content type→Τσεκάρουμε το Content type=Incident→OK

B. Δημιουργία αυτοματισμών

Στο σημείο αυτό θα δημιουργήσουμε κανόνες οι οποίοι θα συμπληρώνουν αυτόματα πεδία της λίστας INCIDENTS σύμφωνα με τις τιμές που θα εισάγει ο χρήστης κατά την καταχώρηση ενός νέου περιστατικού. Ακόμα θα δημιουργήσουμε κανόνες οι οποίοι θα είναι υπεύθυνοι για τις μετρικές που θα χρησιμοποιεί η ITSM εφαρμογή μας.

Από την Home Page→Edit→Insert→Web Part. Επιλέγουμε Από τη λίστα Categories το Apps, από τη λίστα Parts την λίστα INCIDENTS και ADD.

Ανοίγουμε το SharePoint designer tool→Open Site→Επιλέγουμε το http://itsmportal →Open.

1. Από τη στήλη Site Objects επιλέγουμε workflows
2. Από το κουμπί List Workflow επιλέγουμε INCIDENTS
3. Στο παράθυρο συμπληρώνουμε αντίστοιχα το όνομα της κάθε μίας ροής . Θα ξεκινήσουμε από τους κανόνες προτεραιοποίησης σύμφωνα με τους παρακάτω πίνακες. Η προτεραιοποίηση είναι το αποτέλεσμα της τιμής του πεδίου IMPACT και της επιλογής από τον χρήστη του πεδίου URGENCY.

		URGENCY		
IMPACT		Low	Medium	High
	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

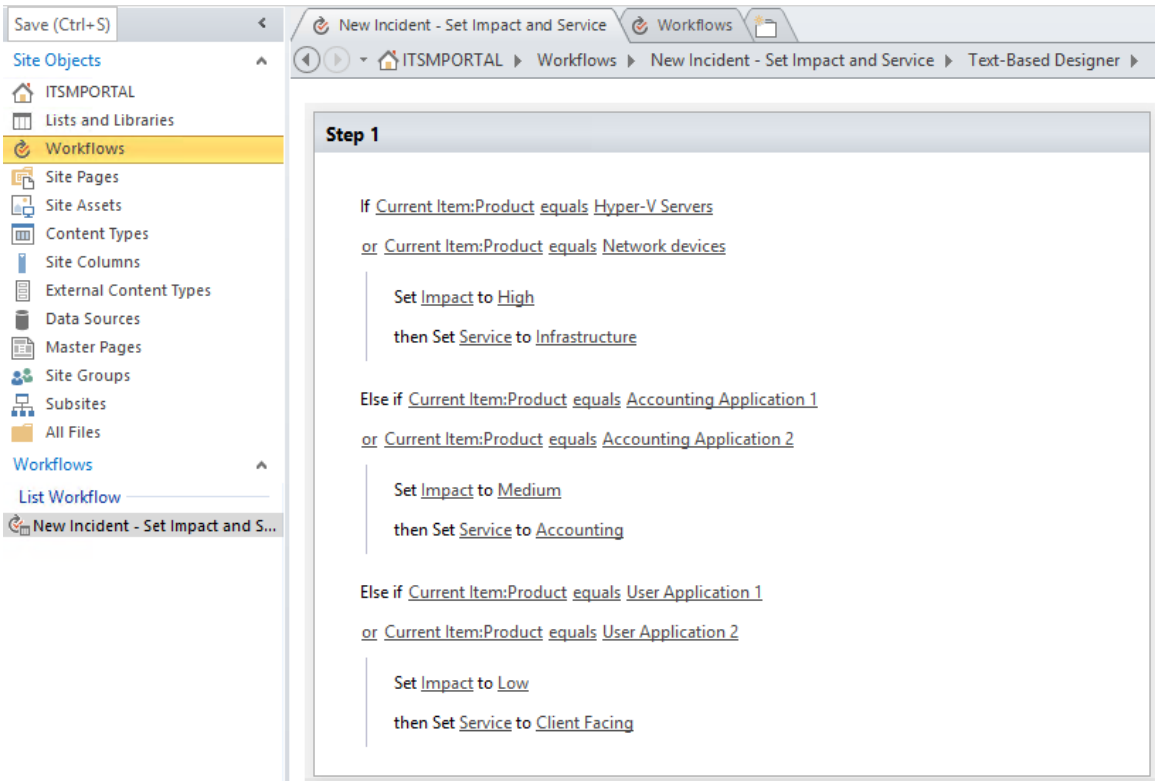
Priority Result	Resolution Target Time
Low	48 Hours
Medium	16 Hours
High	4 hours
Critical	1 hour

PRODUCT	IMPACT
Accounting Application 1	Low
Accounting Application 2	Low
User Application 1	Medium
User Application 2	Medium
Hyper-V Servers	High
Network Devices	High

4. Στο πεδίο Step 1, πατάμε στον κενό χώρο ENTER
5. Στο πεδίο γράφουμε If any και πατάμε ENTER
6. Επιλέγουμε value και Fx. Data source= current item, field from source=Product→ OK
7. Από το drop down menu του equals value επιλέγουμε Hyper-V Servers

8. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε if any και πατάμε ENTER
9. Πατώντας πάνω στο “and” , αλλάζει σε “or” . Επιλέγουμε value και Fx. Data source= current item, field from source=Product→ OK
10. Από το drop down menu του equals value επιλέγουμε Network Devices
11. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε set field και πατάμε ENTER
12. Στο field επιλέγουμε Impact, στο value επιλέγουμε High
13. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε set field και πατάμε ENTER
14. Στο field επιλέγουμε Service, στο value επιλέγουμε Infrastucture
15. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε Else και πατάμε ENTER
16. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε If any και πατάμε ENTER

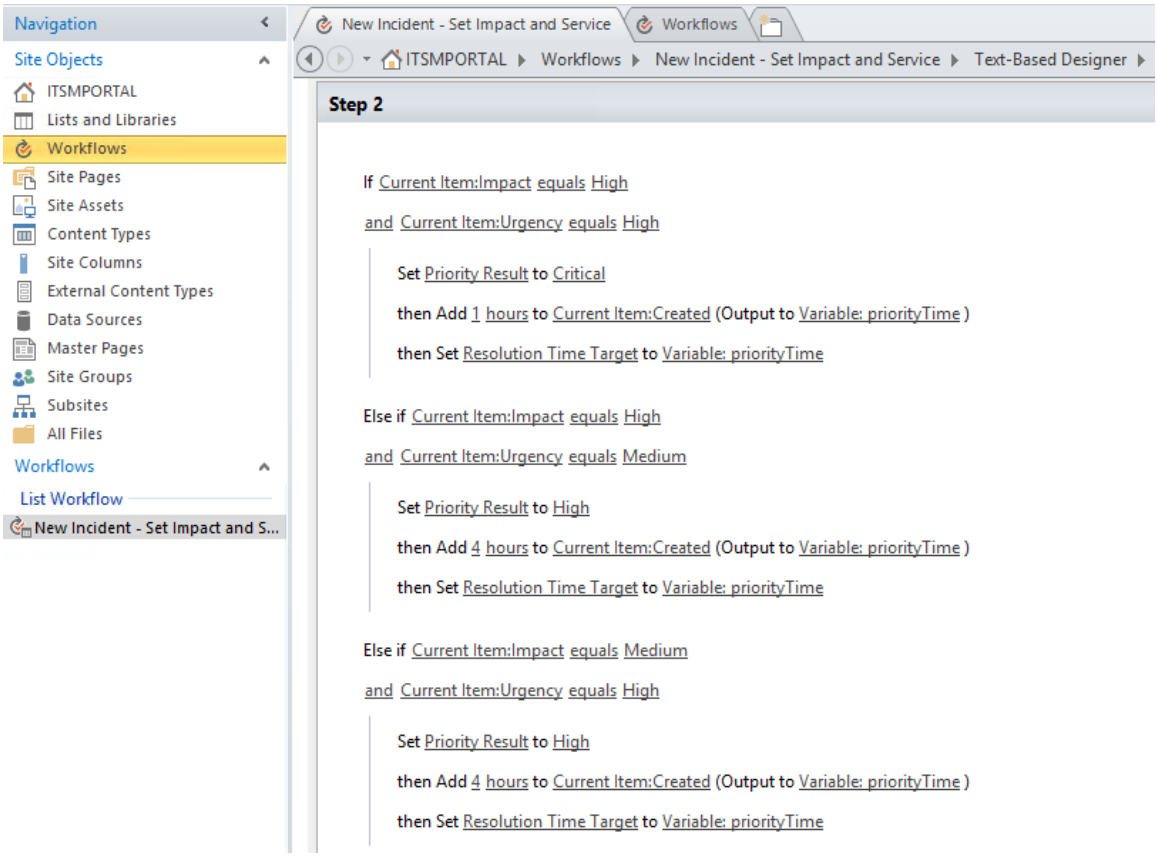
Αυτό που δημιουργείται, είναι οι κανόνες που διαβάζουν το Product που καταχωρεί ο χρήστης και θέτουν αυτόματα τις τιμές Service και Impact. Επαναλαμβάνοντας τα βήματα 4 -16 , δημιουργούμε τους κανόνες αυτόματης συμπλήρωσης για όλα τα Products. Όταν καταλήξουμε όπως στην παρακάτω εικόνα, πατάμε το κουμπί Publish.

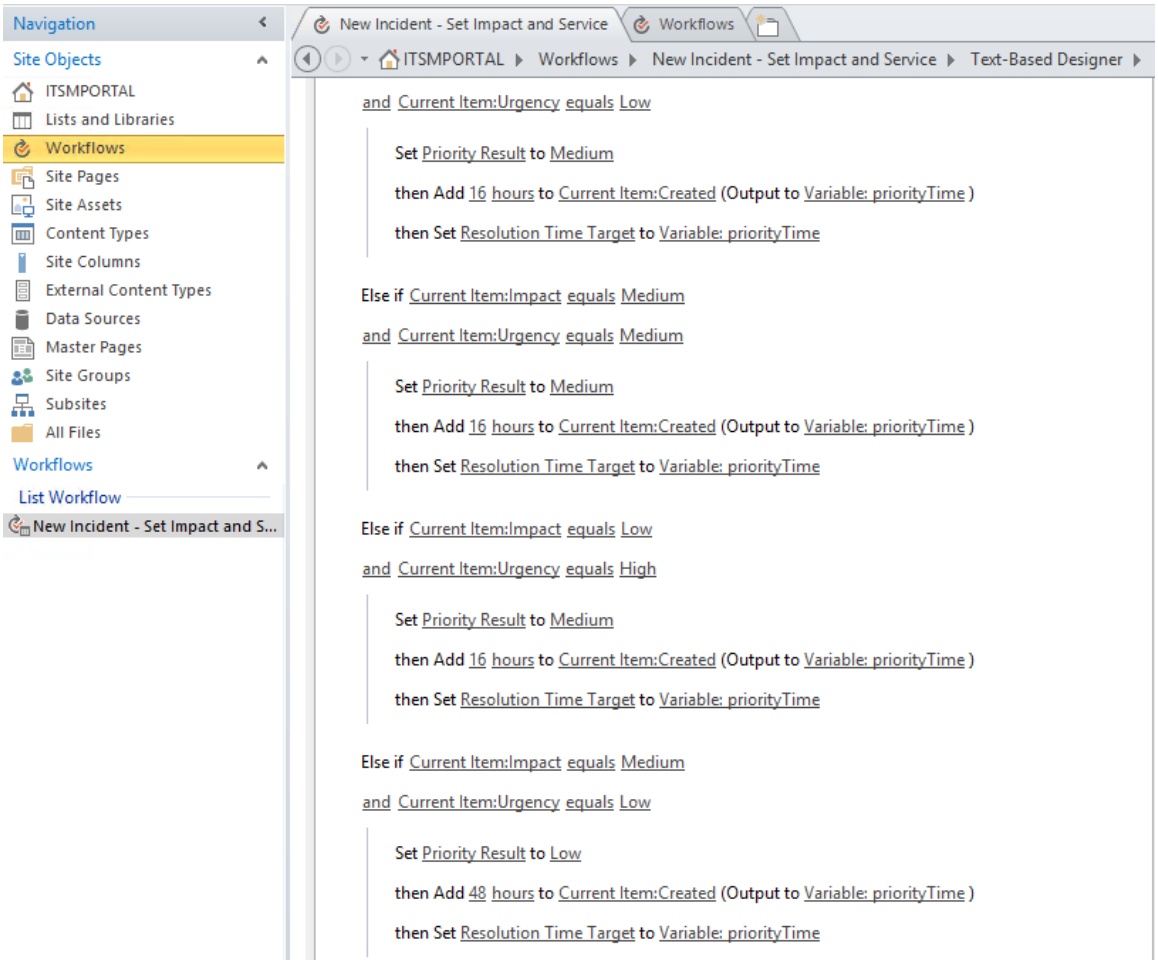


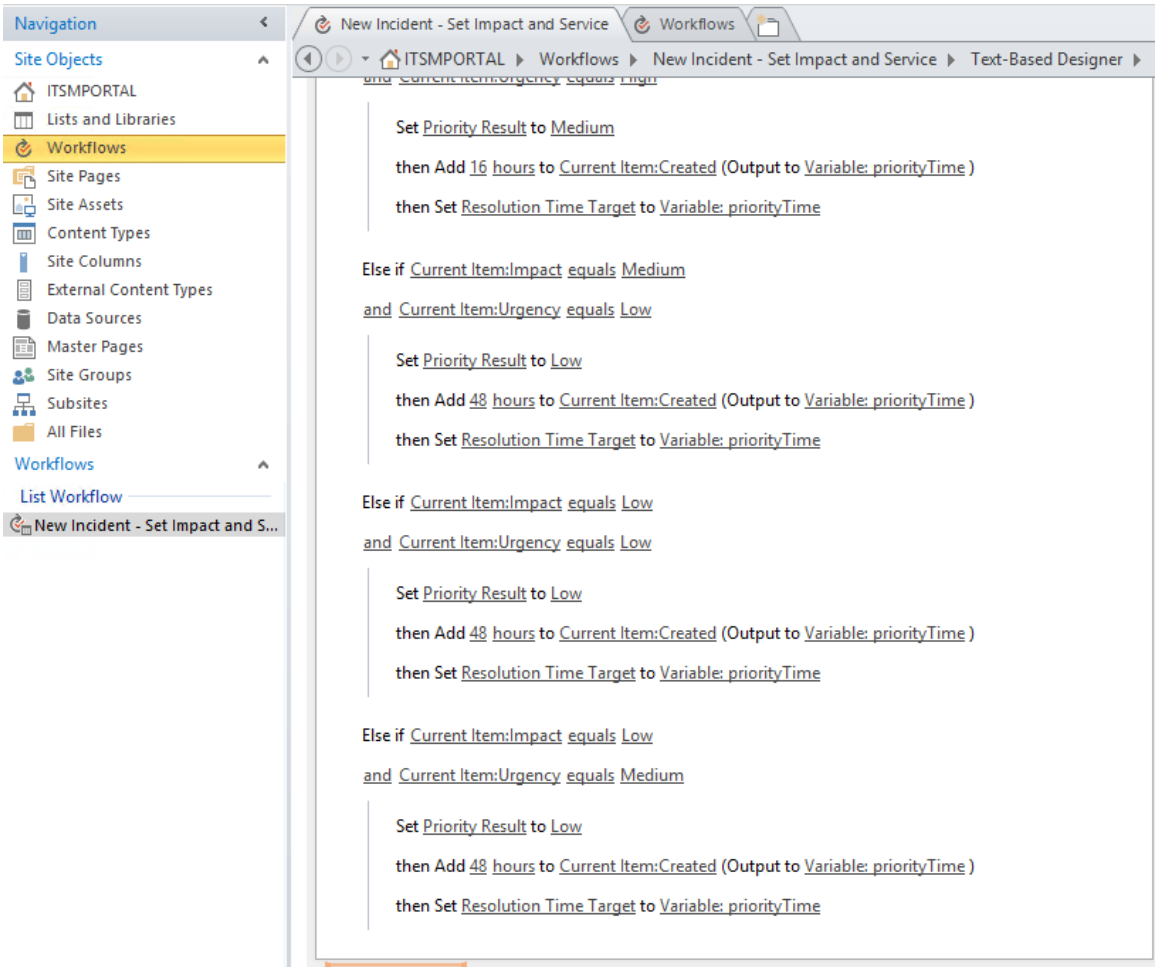
Στη συνέχεια, δημιουργούμε τους κανόνες οι οποίοι συνδυάζουν τις τιμές των πεδίων Impact και Priority, προτεραιοποιούν το αίτημα και ορίζουν το Resolution Target Time. Για να τρέξει σειριακά , αμέσως μετά το σύνολο των κανόνων που μόλις δημιουργήσαμε , πατάμε το κουμπί STEP. Έτσι δημιουργείται ένα νέο πλαίσιο με όνομα Step 2 στο οποίο θα εισάγουμε τους παρακάτω κανόνες.

1. Στο πεδίο Step 2, πατάμε στον κενό χώρο ENTER
2. Γράφουμε if any και πατάμε ENTER
3. Επιλέγουμε value και Fx. Data source= current item, field from source=Impact→ OK
4. Από το drop down menu του equals value επιλέγουμε high
5. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε if any και πατάμε ENTER
6. Επιλέγουμε value και Fx. Data source= current item, field from source=Urgencyt→ OK
7. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε set field και πατάμε ENTER
8. Επιλέγουμε από το πεδίο field την τιμή Priority Result και value=critical
9. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε add time και πατάμε ENTER
10. Αλλάζουμε το 0 σε 1, το minutes σε hours και το date →Fx→data source=workflow variables and parameters, field from source=variable:priorityTime→OK . Αλλάζουμε το output to= variable:priorityTime
11. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πληκτρολογούμε set field και πατάμε ENTER.
12. Επιλέγουμε από το πεδίο field την τιμή Resolution Time Target και value=critical και από το value →FX→ data source=workflow variables and parameters, field from source=variable:priorityTime→OK
13. Κάτω ακριβώς από τη γραμμή που δημιουργήθηκε , στο κενό χώρο, πατάμε το κουμπί Else-If Branch

Επαναλαμβάνουμε τα βήματα 2 έως 13 ώστε να καλύψουμε όλους τους πιθανούς συνδυασμούς προτεραιοποίησης. Η τελική εικόνα θα είναι όπως παρακάτω. Στο τέλος επιλέγουμε το κουμπί Publish ώστε να ενεργοποιηθούν οι κανόνες στην εφαρμογή μας.


Navigation
Site Objects
ITSMPORTAL
Lists and Libraries
Workflows
Site Pages
Site Assets
Content Types
Site Columns
External Content Types
Data Sources
Master Pages
Site Groups
Subsites
All Files
Workflows
List Workflow
New Incident - Set Impact and S...
New Incident - Set Impact and Service
Workflows
ITSMPORTAL ▸ Workflows ▸ New Incident - Set Impact and Service ▸ Text-Based Designer ▸
Step 2
If Current Item:Impact equals High
and Current Item:Urgency equals High
Set Priority Result to Critical
then Add 1 hours to Current Item:Created (Output to Variable: priorityTime)
then Set Resolution Time Target to Variable: priorityTime
Else if Current Item:Impact equals High
and Current Item:Urgency equals Medium
Set Priority Result to High
then Add 4 hours to Current Item:Created (Output to Variable: priorityTime)
then Set Resolution Time Target to Variable: priorityTime
Else if Current Item:Impact equals Medium
and Current Item:Urgency equals High
Set Priority Result to High
then Add 4 hours to Current Item:Created (Output to Variable: priorityTime)
then Set Resolution Time Target to Variable: priorityTime


Navigation
Site Objects
ITSMPORTAL
Lists and Libraries
Workflows
Site Pages
Site Assets
Content Types
Site Columns
External Content Types
Data Sources
Master Pages
Site Groups
Subsites
All Files
Workflows
List Workflow
New Incident - Set Impact and S...
New Incident - Set Impact and Service
Workflows
ITSMPORTAL ▸ Workflows ▸ New Incident - Set Impact and Service ▸ Text-Based Designer ▸
and Current Item:Urgency equals Low
Set Priority Result to Medium
then Add 16 hours to Current Item:Created (Output to Variable: priorityTime)
then Set Resolution Time Target to Variable: priorityTime
Else if Current Item:Impact equals Medium
and Current Item:Urgency equals Medium
Set Priority Result to Medium
then Add 16 hours to Current Item:Created (Output to Variable: priorityTime)
then Set Resolution Time Target to Variable: priorityTime
Else if Current Item:Impact equals Low
and Current Item:Urgency equals High
Set Priority Result to Medium
then Add 16 hours to Current Item:Created (Output to Variable: priorityTime)
then Set Resolution Time Target to Variable: priorityTime
Else if Current Item:Impact equals Medium
and Current Item:Urgency equals Low
Set Priority Result to Low
then Add 48 hours to Current Item:Created (Output to Variable: priorityTime)
then Set Resolution Time Target to Variable: priorityTime



C. Παραμετροποίηση σελίδας και δικαιωμάτων

Σε αυτό το σημείο θα δημιουργήσουμε τα κατάλληλα sharepoint groups, θα κάνουμε τη διασύνδεση τους με τα αντίστοιχα του Active Directory και θα παραμετροποιήσουμε το περιεχόμενο της κεντρικής σελίδας ανά κατηγορία χρηστών.

1. Ανοίγοντας την σελίδα http://itsmportal με τον user administrator επιλέγουμε άνω δεξιά το εικονίδιο γρανάζι και Site Settings
2. Επιλέγουμε Site Permissions και Create Group
3. Στο πεδίο name συμπληρώνουμε SimpleUsers και στο πεδίο Choose the permission level group members get on this site τσεκάρουμε τα Edit και Contribute permissions. Πατάμε το κουμπί Create.
4. Επιλέγουμε από την λίστα των group το group που μόλις δημιουργήσαμε (πχ SimpleUsers)
5. Από το κουμπί New→Add Users→γράφουμε myitsm\simpleusers →Share

Επαναλαμβάνουμε τη διαδικασία και όλα τα groups που θα χρησιμοποιηθούν στις ITSM ροες (HelpDeskAgents ,SecondLevelSupport, CISO, InformationSecurity, CrisisResponseTeam) .

Στη συνέχεια θα διαγράψουμε ότι περιεχόμενο υπάρχει στην HOME σελίδα και θα δημιουργήσουμε αντικείμενα (web parts) τα οποία θα εμφανίζουν το κατάλληλο περιεχόμενο ανά κατηγορία χρηστών. Θα δημιουργήσουμε «VIEWS» και στη συνέχεια θα τα αντιστοιχίσουμε με την κατάλληλη ομάδα χρηστών.

1. Επιλέγουμε στην αρχική σελίδα το κουμπί INCIDENTS
2. Από την καρτέλα LIST επιλέγουμε Create View
3. Από την στήλη Start from an existing view επιλέγουμε All Items
4. Στο πεδίο View Name = RESOLVED INCIDENTS, επιλέγουμε τις στήλες ID, Created,Product,Title,Resolution,Item Status
5. Στο πεδίο Show items only when the following is true: Επιλέγουμε Item Status→Is equal to→Resolved→or→ Item Status→is equal to→Closed
6. Πατάμε το κουμπί OK

Επαναλαμβάνουμε τη διαδικασία δημιουργώντας τα παρακάτω Views:

Όνομα View	Παράμετροι
CREATE NEW REQUEST	Display: ID, Created, Product, Title, Item Status, Title (linked to edit menu) Show items only when the following is true: Product is equal to #
SERVICE DESK - OPEN INCIDENTS	Display: ID, Created, Product, Title, Item Status Show items only when the following is true: Security Incident is equal to No AND Assigned Group is equal to Service Desk OR Item Status is equal to Assigned
SERVICE DESK - CLOSED INCIDENTS	Display: ID, Created, Product, Title, Item Status Show items only when the following is true: Security Incident is equal to No AND Assigned Group is equal to Service Desk AND Item Status is equal to Resolved OR Item Status is equal to Closed
ESCALATION TEAM - OPEN INCIDENTS	Display: ID, Created, Product, Title, Item Status

	Show items only when the following is true: Security Incident is equal to No AND Assigned Group is equal to Escalation Team AND Item Status is equal to Assigned OR Item Status is equal to In Progress
ESCALATION TEAM - CLOSED INCIDENTS	Display: ID, Created, Product, Title, Item Status Show items only when the following is true: Security Incident is equal to No AND Assigned Group is equal to Escalation Team AND Item Status is equal to Resolved OR Item Status is equal to Closed
INCIDENT MANAGER - OPEN INCIDENTS	Display: ID, Created, Product, Title, Item Status Show items only when the following is true: Security Incident is equal to No AND Assigned Group is equal to Incident Manager AND Item Status is equal to Assigned OR Item Status is equal to In Progress
INCIDENT MANAGER - CLOSED INCIDENTS	Display: ID, Created, Product, Title, Item Status Show items only when the following is true: Security Incident is equal to No AND Assigned Group is equal to Incident Manager AND Item Status is equal to Resolved OR Item Status is equal to Closed
INFORMATION SECURITY TEAM - OPEN INCIDENTS	Display: ID, Created, Product, Title, Item Status Show items only when the following is true: Security Incident is equal to Yes AND Assigned Group is equal to Information Security Team AND Item Status is equal to Assigned

	OR Item Status is equal to In Progress
INFORMATION SECURITY TEAM - CLOSED INCIDENTS	Display: ID, Created, Product, Title, Item Status Show items only when the following is true: Security Incident is equal to Yes AND Assigned Group is equal to Information Security Team AND Item Status is equal to Resolved OR Item Status is equal to Closed
CRISIS RESPONSE TEAM - ALL INCIDENTS	Display: ID, Created, Product, Title, Item Status Show items only when the following is true: Assigned Group is equal Crisis Response Team

Αφού δημιουργήθηκαν όλα τα VIEWS, θα συνδεθούν με τα web parts και τα κατάλληλα security groups. Στην HOME σελίδα επιλέγουμε το κουμπί Edit και την καρτέλα Format Text. Από το κουμπί Text Layout επιλέγουμε τη διαμόρφωση με όνομα Two Columns. Θα χωρίσουμε δηλαδή την επιφάνεια εργασίας των χρηστών σε δύο μέρη. Στο ένα θα εμφανίζουμε τα ανοιχτά αιτήματα και στο άλλο τα κλειστά. Στην περίπτωση των απλών χρηστών θα εμφανίσουμε τα αιτήματα που έχουν ολοκληρωθεί και τη δυνατότητα να καταχωρούν νέα. Από την καρτέλα Insert:

1. Επιλέγουμε Web Part
2. Από το Categories→Apps→Incidents→Add
3. Θα εμφανιστεί στην επιφάνεια εργασίας ένα web part, κάθε φορά με αυξανόμενο αριθμό. Επάνω δεξιά επιλέγουμε Edit Web Part
4. Ανοίγει δεξιά άνω νέο παράθυρο στο οποίο αλλάζουμε τα:
   Selected View = RESOLVED ITEMS
   Title = RESOLVED INCIDENTS
   Target Audiences = Simple Users
5. Επιλέγουμε OK

Επαναλαμβάνουμε τη διαδικασία για τα παρακάτω Web Parts:

Όνομα Web Part	Παράμετροι
CREATE NEW REQUEST	Selected View = CREATE NEW REQUEST Title = CREATE NEW REQUEST Target Audiences = Simple Users
SERVICE DESK - OPEN INCIDENTS	Selected View = SERVICE DESK - OPEN INCIDENTS Title = SERVICE DESK - OPEN INCIDENTS Target Audiences = HelpDeskAgents
SERVICE DESK - CLOSED INCIDENTS	Selected View = SERVICE DESK - CLOSED INCIDENTS Title = SERVICE DESK - CLOSED INCIDENTS Target Audiences = HelpDeskAgents
ESCALATION TEAM - OPEN INCIDENTS	Selected View = ESCALATION TEAM - OPEN INCIDENTS Title = ESCALATION TEAM - OPEN INCIDENTS Target Audiences = SecondLevelSupport
ESCALATION TEAM - CLOSED INCIDENTS	Selected View = ESCALATION TEAM - CLOSED INCIDENTS Title = ESCALATION TEAM - CLOSED INCIDENTS Target Audiences = SecondLevelSupport
INCIDENT MANAGER - OPEN INCIDENTS	Selected View = INCIDENT MANAGER - OPEN INCIDENTS Title = INCIDENT MANAGER - OPEN INCIDENTS Target Audiences = CISO
INCIDENT MANAGER - CLOSED INCIDENTS	Selected View = INCIDENT MANAGER - CLOSED INCIDENTS Title = INCIDENT MANAGER - CLOSED INCIDENTS Target Audiences = CISO
INFORMATION SECURITY TEAM - OPEN INCIDENTS	Selected View = INFORMATION SECURITY TEAM - OPEN INCIDENTS Title = INFORMATION SECURITY TEAM - OPEN INCIDENTS Target Audiences = InformationSecurityTeam
INFORMATION SECURITY TEAM - CLOSED INCIDENTS	Selected View = INFORMATION SECURITY TEAM - CLOSED INCIDENTS Title = INFORMATION SECURITY TEAM - CLOSED INCIDENTS

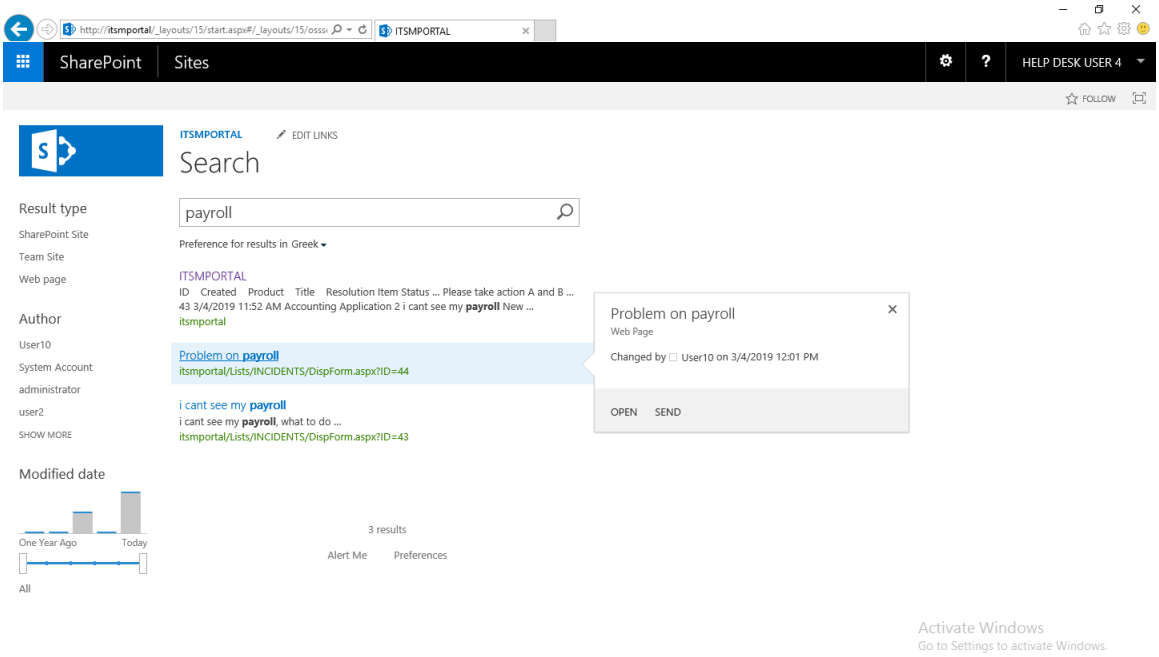
	Target Audiences = InformationSecurityTeam
CRISIS RESPONSE TEAM - ALL INCIDENTS	Selected View = CRISIS RESPONSE TEAM - ALL INCIDENTS Title = CRISIS RESPONSE TEAM - ALL INCIDENTS Target Audiences = CrysisResponseTeam

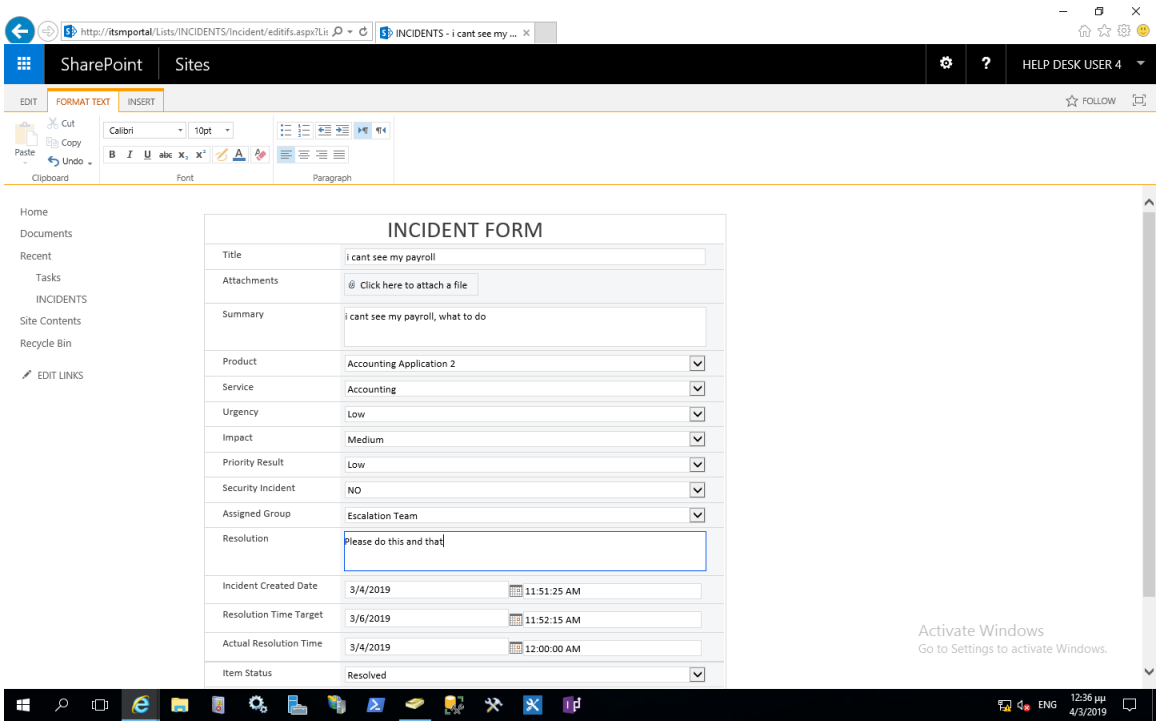
D. Ενεργοποίηση γνωσιακής βάσης δεδομένων

Αναφέραμε νωρίτερα πως στη βιβλιοθήκη ITIL θεωρείται βασικό στοιχείο η ύπαρξη γνωσιακής βάσης δεδομένων. Ένα κεντρικό σημείο δηλαδή στο οποίο καταγράφεται η εμπειρία και η γνώση των ανθρώπων που καλούνται να αντιμετωπίσουν περιστατικά, περιστατικά ασφαλείας ή απλά αιτήματα χρηστών του πληροφοριακού συστήματος. Γι αυτό το λόγο θα ενεργοποιήσουμε μια δυνατότητα του share point το search service application. Με αυτό τον τρόπο θα δώσουμε τη δυνατότητα στις ομάδες ανάθεσης να ψάχνουν χρησιμοποιώντας λέξεις-κλειδιά και να βρίσκουν άμεσα την λύση χρησιμοποιώντας καταγεγραμμένη πληροφορία από περιστατικά του παρελθόντος.

1. Με τον χρήστη administrator, ανοίγουμε το central administration.
2. Επιλέγουμε Manage service applications
3. Επιλέγουμε Search Service Application (το πρώτο από τα δύο που εμφανίζονται)
4. Από τη στήλη crawling → content sources→New content source
5. Στο πεδίο Name = ITSM web app
6. Στο πεδίο Content Source Type = Sharepoint sites
7. Στο πεδίο Start Addresses = Http://itsmportal
8. Στο πεδίο Crawl Schedules = Enable Continuous Crawls

Στο παρακάτω παράδειγμα ο help desk agent, χρησιμοποιώντας τη λέξη κλειδί payroll αναζητά προηγούμενα περιστατικά βρίσκοντας άμεσα τη λύση.


SharePoint
Sites
HELP DESK USER 4
FOLLOW
ITSMPORTAL
EDIT LINKS
Search
Result type
SharePoint Site
Team Site
Web page
Author
User10
System Account
administrator
user2
SHOW MORE
Modified date
One Year Ago
Today
All
payroll
Preference for results in Greek
ITSMPORTAL
ID Created Product Title Resolution Item Status ... Please take action A and B ...
43 3/4/2019 11:52 AM Accounting Application 2 i cant see my payroll New ...
itsmportal
Problem on payroll
itsmportal/Lists/INCIDENTS/DispForm.aspx?ID=44
i cant see my payroll
i cant see my payroll, what to do ...
itsmportal/Lists/INCIDENTS/DispForm.aspx?ID=43
3 results
Alert Me
Preferences
Problem on payroll
Web Page
Changed by User10 on 3/4/2019 12:01 PM
OPEN
SEND
Activate Windows
Go to Settings to activate Windows.
http://itsmportal/Lists/INCIDENTS/DispForm.aspx?ID=44
ENG
12:08 μμ
4/3/2019


SharePoint
Sites
HELP DESK USER 4
EDIT
FORMAT TEXT
INSERT
FOLLOW
Paste
Cut
Copy
Undo
Clipboard
Calibri
10pt
Font
Paragraph
Home
Documents
Recent
Tasks
INCIDENTS
Site Contents
Recycle Bin
EDIT LINKS
INCIDENT FORM
Title
i cant see my payroll
Attachments
Click here to attach a file
Summary
i cant see my payroll, what to do
Product
Accounting Application 2
Service
Accounting
Urgency
Low
Impact
Medium
Priority Result
Low
Security Incident
NO
Assigned Group
Escalation Team
Resolution
Please do this and that
Incident Created Date
3/4/2019
11:51:25 AM
Resolution Time Target
3/6/2019
11:52:15 AM
Actual Resolution Time
3/4/2019
12:00:00 AM
Item Status
Resolved
Activate Windows
Go to Settings to activate Windows.
ENG
12:36 μμ
4/3/2019

ΕΠΙΛΟΓΟΣ

Ολοκληρώνοντας τις παραπάνω ενέργειες προκύπτει μια δικτυακή εφαρμογή ικανή να διαχειριστεί αιτήματα χρηστών και να τα δρομολογήσει αυτόματα στις κατάλληλες ομάδες ανάθεσης. Χρησιμοποιώντας κανόνες, το αίτημα του χρήστη συνδέεται με τις προσφερόμενες υπηρεσίες του οργανισμού και χαρακτηρίζεται ως προς την κρισιμότητα και την προτεραιοποίηση του. Η εφαρμογή ελέγχει τα δικαιώματα του χρήστη χρησιμοποιώντας directory services και προσαρμόζει την επιφάνεια εργασίας ανάλογα με τους ρόλους που έχουν ορίσει οι διαχειριστές. Τέλος, υποστηρίζεται γνωσιακή βάση δεδομένων η οποία ενημερώνεται αυτόματα και με συνεχόμενο τρόπο.

Για τη δημιουργία της παραπάνω εφαρμογής χρησιμοποιήθηκαν αποκλειστικά out of the box δυνατότητες των προϊόντων που αναφέρθηκαν, εξαλείφοντας την ανάγκη για ανάπτυξη κώδικα σε οποιοδήποτε στάδιο. Η εφαρμογή θα μπορούσε να εμπλουτιστεί με περισσότερες δυνατότητες συνεργασίας πχ κοινά ημερολόγια, on line chat κτλ αλλά δεν αποτελούσε σκοπό της συγκεκριμένης εργασίας.

Ως επέκταση των δυνατοτήτων της εφαρμογής θα μπορούσε να είναι η δημιουργία αναφορών χρησιμοποιώντας sharepoint web parts. Στην παρούσα εργασία δεν κατέστη δυνατό μια τέτοια υλοποίηση γιατί στην συγκεκριμένη έκδοση της υποδομής, η δυνατότητα έχει διακοπεί από τον κατασκευαστή. Υπάρχουν όμως εναλλακτικοί τρόποι όπως η δημιουργία αναφορών απ’ ευθείας από τη βάση δεδομένων είτε χρησιμοποιώντας web parts άλλων κατασκευαστών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Σωκράτης Κάτσικας, UNIPI 2018, ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ “Εισαγωγικά θέματα”

National Institute of Standards and Technology, 2012, Computer Security - Incident Handling Guide

ISACA, 2009, An Introduction to the Business Model for Information Security

Olga M. Londer, Penelope Coventry, 2016, Microsoft SharePoint 2016 Step by Step

BMC Software Inc. , 2016, Best Practice Insights - Focus On: ITIL® Service Operation For ITIL 2011

Microsoft TechNet Library