Διπλωματική εργασία

Ανάλυση Κυβερνοασφάλειας της Πλατφόρμας Ψηφιακού Διδύμου iNicosia

Ευγένιος Πέτρου

Πανεπιστήμιο Κύπρου

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

Μάιος 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

Κυβερνοασφάλειας της Πλατφόρμας Ψηφιακού Διδύμου iNicosia

Ευγένιος Πέτρου

Επιβλέποντας

Βάσος Βασιλείου

Η Διπλωματική Εργασία υποβλήθηκε σε μερική εκπλήρωση των προϋποθέσεων για απόκτηση πτυχίου του Τμήματος Επιστήμης Υπολογιστών του Πανεπιστημίου Κύπρου

Μάιος 2024

Ευχαριστίες

Πρώτα από όλα, ευχαριστώ από καρδιάς τον επιβλέποντα μου, Δρ. Βάσο Βασιλείου, του οποίου η εμπειρογνωμοσύνη και η διορατική καθοδήγηση υπήρξαν ανεκτίμητες καθ' όλη τη διάρκεια αυτής της διαδικασίας. Η υπομονή σας και η ακαδημαϊκή αυστηρότητά σας έχουν διαμορφώσει βαθιά την προσέγγισή μου στην έρευνα.

Είμαι επίσης εξαιρετικά ευγνώμων στα μέλη διδασκαλίας του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου, των οποίων οι διδασκαλίες μου έδωσαν τις θεμελιώδεις γνώσεις και δεξιότητες που απαιτούνται για να ξεκινήσω αυτή την έρευνα. Τα μαθήματα που παρείχαν με εξόπλισαν με τις απαραίτητες δεξιότητες και γνώσεις για να ολοκληρώσω με επιτυχία τις σπουδές μου στην Πληροφορική. Είμαι βέβαιος ότι οι πόροι και οι εμπειρίες που απέκτησα κατά τη διάρκεια των σπουδών μου στο Πανεπιστήμιο θα μου δώσουν τη δυνατότητα να ξεπεράσω τις όποιες προκλήσεις αντιμετωπίζω, ενώ ταυτόχρονα θα θέσουν τις βάσεις για μια ανταποδοτική καριέρα στον τομέα αυτό.

Οι συμφοιτητές μου, και φίλοι μου, αξίζουν ιδιαίτερη μνεία για τις αμέτρητες συνεδρίες καταιγισμού ιδεών και για την παροχή ενός κλίματος συμπαράστασης για τις ιδέες μου. Η συντροφικότητά σας υπήρξε πηγή δύναμης και κινήτρων.

Αυτή η διατριβή αποτελεί απόδειξη της συλλογικής προσπάθειας και καλής θέλησης όλων των προαναφερθέντων και γι 'αυτό, είμαι πραγματικά ευγνώμων.

Περίληψη

Η παρούσα διπλωματική εργασία εμβαθύνει στην ολοκληρωμένη μελέτη και εφαρμογή της τεχνολογίας Digital Twin, εστιάζοντας συγκεκριμένα στο έργο iNicosia, το οποίο στοχεύει στη μοντελοποίηση του αστικού τοπίου της Λευκωσίας χρησιμοποιώντας προηγμένη 3D ψηφιακή αναπαράσταση. Η εισαγωγή θέτει το σκηνικό καθορίζοντας τον σκοπό, το πεδίο εφαρμογής και την ακαδημαϊκή σημασία της μελέτης, τονίζοντας την ανάγκη αντιμετώπισης τόσο των αρχιτεκτονικών προκλήσεων όσο και των προκλήσεων στον κυβερνοχώρο που είναι εγγενείς στην εφαρμογή και διατήρηση ενός Digital Twin μιας αστικής περιοχής.

Η διπλωματική εργασία ξεκινά με μια γενική επισκόπηση της τεχνολογίας Digital Twin, παρακολουθώντας την εξέλιξή της από τις πρώτες διαστημικές αποστολές της NASA στις τρέχουσες εφαρμογές της σε διάφορους τομείς, συμπεριλαμβανομένου του πολεοδομικού σχεδιασμού. Αυτή η ενότητα εισάγει επίσης το iNicosia Digital Twin ως case study, καταδεικνύοντας το ρόλο του στην ενίσχυση της αστικής διαχείρισης. Ακολουθεί μια λεπτομερής ανάλυση ασφάλειας, όπου συζητούνται μέθοδοι όπως ζητήματα ελέγχου ταυτότητας χρήστη (user authentication), δοκιμές διείσδυσης (penetration testing) και αξιολογήσεις ευπάθειας χρησιμοποιώντας καθιερωμένα πλαίσια ασφάλειας στον κυβερνοχώρο όπως αυτά του PortSwigger. Αυτή η ενότητα στοχεύει στον εντοπισμό και την πρόταση λύσεων για την ενίσχυση της ασφάλειας της πλατφόρμας έναντι κοινών απειλών στον κυβερνοχώρο.

Επιπλέον, η διατριβή διερευνά την αρχιτεκτονική των Digital Twins συγκρίνοντας υπάρχοντα μοντέλα και ενσωματώνοντας στοιχεία από αναγνωρισμένες πλατφόρμες όπως το TM Forum και το FIWARE. Προτείνονται συστάσεις για αρχιτεκτονικές βελτιώσεις, υποστηριζόμενες από πρακτικές στρατηγικές εφαρμογής που ευθυγραμμίζονται με τα ευρήματα από συγκριτικές και λειτουργικές αναλύσεις. Οι τελευταίες ενότητες της διατριβής αφορούν την τεχνική διαμόρφωση τόσο του υλικού όσο και του λογισμικού, συμπεριλαμβανομένης της επισκόπησης της υποδομής και των στρατηγικών διαχείρισης δεδομένων που είναι κρίσιμες για τις δυνατότητες αλληλεπίδρασης και δυναμικής μοντελοποίησης σε πραγματικό χρόνο του iNicosia Digital Twin. Η διατριβή ολοκληρώνεται με μια σειρά περιπτωσιολογικών μελετών και συγκριτικών αναλύσεων που όχι μόνο υπογραμμίζουν τις επιτυχημένες εφαρμογές των ψηφιακών διδύμων, αλλά και αντλούν διδάγματα από προηγούμενες παραβιάσεις, προσφέροντας έναν οδικό χάρτη για μελλοντικές ερευνητικές κατευθύνσεις και υλοποιήσεις.

Περιεχόμενα

Κεφάλαιο 1

1. Εισαγωγή

1.1. Σκοπός

Η διατριβή μου επικεντρώνεται στην ανάλυση ασφαλείας του iNicosia Digital Twin, μιας εκτεταμένης ψηφιακής αναπαράστασης της πόλης της Λευκωσίας, γεμάτη με λεπτομερή 3D μοντέλα, δεδομένα πραγματικού κόσμου από διάφορους αισθητήρες και δυναμικές αλληλεπιδράσεις που αντικατοπτρίζουν τον παλμό της πόλης. Καθώς το digital twin ενσωματώνει πολύπλευρα δεδομένα - από υποδομές έως περιβαλλοντικές συνθήκες σε πραγματικό χρόνο - η σημασία της οχύρωσής του δεν μπορεί να υποτιμηθεί. Μια παραβίαση ή χειραγώγηση αυτών των δεδομένων θα μπορούσε να παραποιήσει την ίδια την ουσία της Λευκωσίας, ενδεχομένως στρεβλώνοντας τον πολεοδομικό σχεδιασμό, τις αποφάσεις υποδομής και πολλά άλλα. Μέσα από την έρευνά μου, στοχεύω να εμβαθύνω σε πιθανές ευπάθειες εντός της πλατφόρμας iNicosia, εισάγοντας αυστηρά μέτρα ασφαλείας και πρωτόκολλα. Ο στόχος είναι να διασφαλιστεί ότι αυτός ο ψηφιακός πυρήνας παραμένει ακριβής, αξιόπιστος και αδιαπέραστος από απειλές στον κυβερνοχώρο, διατηρώντας έτσι τη σημασία του ως ανεκτίμητο εργαλείο για τη συνεχή ανάπτυξη και ανάπτυξη της πόλης.

1.2. Πεδίο εφαρμογής της λύσης

Η διατριβή μου εμβαθύνει σε μια ολοκληρωμένη ανάλυση των μέτρων κυβερνοασφάλειας που εφαρμόζονται στην ιστοσελίδα iNicosia Digital Twin. Αυτή η ανάλυση περιλαμβάνει δύο κύριες διαστάσεις: i) την αρχιτεκτονική υλικού που υποστηρίζει τη λειτουργικότητα του ιστότοπου, συμπεριλαμβανομένων των δικτύων αισθητήρων, των μονάδων επεξεργασίας δεδομένων και των διεπαφών χρήστη, και ii) τις εξελιγμένες στρατηγικές λογισμικού που αναπτύσσονται για την ενίσχυση του ιστότοπου από απειλές στον κυβερνοχώρο. Αυτά τα μέτρα λογισμικού είναι σχολαστικά σχεδιασμένα, λαμβάνοντας υπόψη διάφορους περιορισμούς, όπως περιορισμούς τύπου δεδομένων, γεωγραφική εστίαση και λειτουργικές δυνατότητες, όλα με στόχο την ενίσχυση του πλαισίου ασφαλείας του ιστότοπου.

Σε μια εις βάθος εξερεύνηση της τεχνολογικής αρχιτεκτονικής του iNicosia Digital Twin, δίνεται ιδιαίτερη προσοχή στις πτυχές ασφάλειας του υλικού που χρησιμοποιείται. Στη συνέχεια, η συζήτηση μετατοπίζεται στο περιβάλλον λογισμικού της ιστοσελίδας, αναλύοντας λεπτομερώς τους προϋπάρχοντες μηχανισμούς ασφαλείας και αξιολογώντας την αποτελεσματικότητά τους στη διασφάλιση της ψηφιακής υποδομής. Επιπλέον, η διατριβή επισημαίνει γνωστές περιπτώσεις παραβιάσεων της ασφάλειας στον κυβερνοχώρο που έχουν

στοχεύσει παρόμοιες πλατφόρμες και αναλύει πιθανές ευπάθειες εντός της εγκατάστασης του iNicosia. Προτείνει στρατηγικές εφαρμογές πρόσθετων μέτρων ασφαλείας που θα μπορούσαν ενδεχομένως να προλάβουν και να μετριάσουν τέτοιους κινδύνους.

Επιπλέον, η διατριβή παρέχει μια λεπτομερή παρουσίαση διαφόρων σεναρίων κυβερνοεπίθεσης ειδικά προσαρμοσμένων στην ιστοσελίδα iNicosia Digital Twin. Συζητά λεπτομερώς πώς αυτές οι επιθέσεις μπορούν να προσομοιωθούν σε ένα ελεγχόμενο περιβάλλον για να κατανοήσουν καλύτερα τους μηχανισμούς και τις επιπτώσεις τους. Αυτή η μελέτη προσομοίωσης βοηθά στην ανάπτυξη ισχυρών αντιμέτρων που μπορούν να ενσωματωθούν στα πρωτόκολλα ασφαλείας του ιστότοπου. Η μελέτη ενσωματώνει επίσης μια ανασκόπηση της τρέχουσας βιβλιογραφίας για την ασφάλεια στον κυβερνοχώρο για να αντιπαραβάλει την υπάρχουσα γνώση με τα νέα ευρήματα από τις περιπτωσιολογικές μελέτες και τις προσομοιώσεις, εμπλουτίζοντας έτσι την ακαδημαϊκή και πρακτική κατανόηση της τεχνολογίες του Digital Twin Security στον κυβερνοχώρο.

Επιπλέον, είναι σημαντικό να διευκρινιστεί ότι αυτή η διατριβή δεν εμβαθύνει στις λεπτομέρειες των κανόνων και κανονισμών GDPR σχετικά με τη συλλογή δεδομένων. Αντ 'αυτού, δίνεται έμφαση κυρίως στους τεχνικούς και στρατηγικούς μηχανισμούς για να διασφαλιστεί ότι τα δεδομένα αποθηκεύονται με ασφάλεια και προστατεύονται από πιθανές απειλές στον κυβερνοχώρο. Η μελέτη διερευνά διάφορα μέτρα ασφαλείας, όπως τεχνικές κρυπτογράφησης, πρωτόκολλα ασφαλούς πρόσβασης και προηγμένες διαδικασίες ελέγχου ταυτότητας που είναι κρίσιμες για τη διασφάλιση των δεδομένων εντός της υποδομής του iNicosia Digital Twin. Εστιάζοντας στην εφαρμογή ισχυρών πλαισίων ασφαλείας και στην ενσωμάτωση τεχνολογιών αιχμής στον κυβερνοχώρο, η διατριβή στοχεύει στην παροχή αξιοποιήσιμων πληροφοριών σχετικά με τον τρόπο αποτελεσματικής θωράκισης των δεδομένων του ιστότοπου από μη εξουσιοδοτημένη πρόσβαση και επιθέσεις, αντί να πλοηγείται στις νομικές περιπλοκές των νόμων περί απορρήτου δεδομένων όπως το GDPR. Αυτή η προσέγγιση επιτρέπει μια συγκεντρωμένη εξέταση των φυσικών και ψηφιακών μέτρων ασφαλείας, διασφαλίζοντας ότι οι στρατηγικές προστασίας είναι πρακτικές και εφαρμόσιμες για την ενίσχυση της συνολικής στάσης ασφαλείας της ιστοσελίδας iNicosia Digital Twin. Αυτή η ολοκληρωμένη προσέγγιση διασφαλίζει ότι η διατριβή δεν εξετάζει μόνο θεωρητικές και πρακτικές πτυχές της κυβερνοασφάλειας, αλλά συμβάλλει σημαντικά στον τομέα προτείνοντας καινοτόμες λύσεις και στρατηγικές για την ενίσχυση της ανθεκτικότητας της ιστοσελίδας iNicosia Digital Twin έναντι των εξελισσόμενων απειλών στον κυβερνοχώρο. Μέσα από ένα μείγμα περιπτωσιολογικών μελετών, προσομοιώσεων και θεωρητικής ανάλυσης, η διατριβή στοχεύει να παρέχει ένα σχέδιο για αποτελεσματικές πρακτικές ασφάλειας στον κυβερνοχώρο στις τεχνολογίες ψηφιακών διδύμων.

1.3. Ερευνητική σημασία

Η σημασία αυτής της έρευνας έγκειται στη συμβολή της στον τομέα της Digital Twin Technology, ιδιαίτερα στην εφαρμογή της σε αστικά περιβάλλοντα. Η Digital Twin Technology είναι μια πρωτοποριακή καινοτομία στον τομέα της ψηφιοποίησης, αντιπροσωπεύοντας ένα σημαντικό άλμα προς τα εμπρός στον τρόπο με τον οποίο αλληλεπιδρούμε και διαχειριζόμαστε τόσο τα φυσικά περιουσιακά στοιχεία όσο και ευρύτερα συστήματα όπως πόλεις ή σύνθετα μηχανήματα. Τα Digital Twins αντιπροσωπεύουν μια προσέγγιση στον πολεοδομικό σχεδιασμό και τη διαχείριση, προσφέροντας απαράμιλλες γνώσεις σχετικά με τη δυναμική της πόλης μέσω δεδομένων σε πραγματικό χρόνο και 3D μοντελοποίησης. Το έργο iNicosia Digital Twin ενσωματώνει αυτή την καινοτομία, συμπυκνώνοντας ολόκληρο το αστικό τοπίο της Λευκωσίας σε

ψηφιακή μορφή, γεμάτη με λεπτομερή μοντέλα και δεδομένα αισθητήρων που αντικατοπτρίζουν την κατάσταση της πόλης σε πραγματικό χρόνο.

Καθώς το ψηφιακό δίδυμο ενσωματώνει ποικίλα και πολύπλευρα δεδομένα - που εκτείνονται από περίπλοκες υποδομές έως δυναμικές περιβαλλοντικές συνθήκες - η επιτακτική ανάγκη διασφάλισης αυτού του συστήματος είναι υψίστης σημασίας. Η παραβίαση ή η χειραγώγηση αυτών των δεδομένων μπορεί να οδηγήσει σε σημαντικές παραποιήσεις του αστικού τοπίου της Λευκωσίας. Αυτό θα μπορούσε να επηρεάσει αρνητικά τον πολεοδομικό σχεδιασμό, την ανάπτυξη υποδομών και την κατανομή των πόρων, οδηγώντας σε εκτεταμένες συνέπειες για τη διακυβέρνηση της πόλης και την ευημερία των κατοίκων της.

Εστιάζοντας στον εντοπισμό και τον μετριασμό των τρωτών σημείων εντός της πλατφόρμας iNicosia, η έρευνα αυτή στοχεύει στην ενίσχυση του ψηφιακού δίδυμου έναντι πιθανών απειλών στον κυβερνοχώρο. Αυτό δεν είναι απλώς μια τεχνική προσπάθεια, αλλά ένα κρίσιμο βήμα για να διασφαλιστεί ότι η ψηφιακή αναπαράσταση παραμένει ένας ακριβής, αξιόπιστος και αξιόπιστος πόρος. Με αυτόν τον τρόπο, η έρευνα υποστηρίζει τη χρησιμότητα του ψηφιακού δίδυμου ως ανεκτίμητο εργαλείο για την αστική ανάπτυξη, επιτρέποντας την ενημερωμένη λήψη αποφάσεων και την αποτελεσματική διαχείριση της πόλης.

Η έρευνα αυτή έχει σημασία πέρα από τα όρια της Λευκωσίας. Θέτει ένα προηγούμενο για παρόμοιες πρωτοβουλίες έξυπνων πόλεων παγκοσμίως, παρέχοντας ένα πρότυπο για την εξασφάλιση ψηφιακών διδύμων. Καθώς οι πόλεις σε όλο τον κόσμο στρέφονται όλο και περισσότερο στην ψηφιοποίηση για τη διαχείριση των πολύπλοκων οικοσυστημάτων τους, οι γνώσεις από αυτή τη μελέτη προσφέρουν πολύτιμα μαθήματα στην ασφάλεια στον κυβερνοχώρο και τη διαχείριση δεδομένων.

Αυτή η μελέτη συμβάλλει τόσο στην ακαδημαϊκή γνώση όσο και στις πρακτικές εφαρμογές στην ασφάλεια στον κυβερνοχώρο, τις αστικές μελέτες και τις ψηφιακές τεχνολογίες. Αντιμετωπίζει ένα κενό στην τρέχουσα έρευνα σχετικά με την ασφάλεια των ψηφιακών διδύμων, ειδικά στο πλαίσιο μιας ολόκληρης πόλης. Αυτό προσφέρει μια μοναδική προοπτική, συνδυάζοντας θεωρητικές αρχές ασφάλειας στον κυβερνοχώρο με πρακτικές, πραγματικές εφαρμογές σε αστικό περιβάλλον.

Τέλος, οι μακροπρόθεσμες επιπτώσεις αυτής της έρευνας είναι σημαντικές. Διασφαλίζοντας την ακεραιότητα και την ασφάλεια του iNicosia Digital Twin, η μελέτη αυτή συμβάλλει στη βιώσιμη ανάπτυξη και την ανθεκτική ανάπτυξη της Λευκωσίας. Βοηθά στην προστασία της ψηφιακής υποδομής της πόλης από απειλές στον κυβερνοχώρο, διασφαλίζοντας έτσι ότι η Λευκωσία συνεχίζει να ευδοκιμεί ως ένας δυναμικός, καλά διαχειριζόμενος αστικός χώρος.

Κεφάλαιο 2

2. Γενική Ανασκόπηση Digital Twins

2.1. Digital Twins: Θεμελιώδεις αρχές και εξέλιξη

Τεχνολογία Digital Twin

Η τεχνολογία Digital Twin αντιπροσωπεύει μια καινοτόμο ιδέα στον τομέα της τεχνολογίας των πληροφοριών και της μηχανικής, δημιουργώντας ένα εικονικό αντίστοιχο φυσικών οντοτήτων, συστημάτων ή διαδικασιών. Αυτή η τεχνολογία γεφυρώνει αποτελεσματικά το χάσμα μεταξύ του φυσικού και του ψηφιακού κόσμου. Περιλαμβάνει τα πάντα, από μικρά εξαρτήματα όπως μια βαλβίδα σε μια μηχανή έως συστήματα μεγάλης κλίμακας, όπως ολόκληρες πόλεις ή εργοστάσια παραγωγής.

Αρχικά αναπτύχθηκε κατά τη διάρκεια των προγραμμάτων εξερεύνησης του διαστήματος της NASA, ιδιαίτερα κατά τη διάρκεια των αποστολών Apollo. Η έννοια του «Digital Twin» έχει εξελιχθεί σημαντικά με την πάροδο των ετών, βρίσκοντας τις ρίζες της σε διάφορους τομείς και εφαρμογές. Ο όρος επινοήθηκε για πρώτη φορά το 2002 από τον Michael Grieves στο Πανεπιστήμιο του Michigan, ενώ συζητούσε ένα εννοιολογικό μοντέλο για το Product Life Cycle Management (PLM). Ωστόσο, η θεμελιώδης ιδέα προηγείται του όρου, με στοιχεία ανιχνεύσιμα στις πρώτες ημέρες του διαστημικού προγράμματος της NASA. Κατά τη διάρκεια των αποστολών του Apollo, η NASA χρησιμοποίησε ζεύγη συστημάτων - ένα επί του διαστημικού σκάφους και το είδωλό του πίσω στη Γη. Αυτή η ρύθμιση επέτρεψε στους μηχανικούς να προσομοιώσουν τις συνθήκες στο διαστημικό σκάφος χρησιμοποιώντας το γήινο αντίγραφο για να προβλέψουν πιθανά προβλήματα και να διαγνώσουν προβλήματα σε πραγματικό χρόνο στο διάστημα.

Καθώς η τεχνολογία προχώρησε, η φήμη των digital twins άκμασε πέρα από την αεροδιαστημική, ιδιαίτερα με την άνοδο του Internet of Things (IoT), των Big Data, του Machine Learning. Στον βιομηχανικό τομέα, εταιρείες όπως η General Electric άρχισαν να πρωτοπορούν στη χρήση digital twins γύρω στο 2010, εφαρμόζοντάς τα σε μηχανήματα και συστήματα μεγάλης κλίμακας. Αυτά τα digital twins χρησίμευσαν ως πλήρως λειτουργικά αντίγραφα φυσικών περιουσιακών στοιχείων, παρέχοντας μια ματιά σε πραγματικό χρόνο στη λειτουργία, τη συντήρηση και την υγεία τους. Αξιοποιώντας τεράστιες ποσότητες δεδομένων από αισθητήρες και λειτουργίες ρουτίνας, οι επιχειρήσεις θα μπορούσαν να προβλέψουν τις βλάβες πριν συμβούν, να

βελτιστοποιήσουν τα χρονοδιαγράμματα συντήρησης και να βελτιώσουν τη λειτουργική αποτελεσματικότητα.

Σήμερα, τα ψηφιακά δίδυμα έχουν βρει εφαρμογές σε ένα ευρύ φάσμα βιομηχανιών, από τη μεταποίηση έως τον πολεοδομικό σχεδιασμό και την υγειονομική περίθαλψη. Στην αστική ανάπτυξη, τα digital twins προσομοιώνουν τα συστήματα και τις διαδικασίες της πόλης για να βελτιστοποιήσουν τα πάντα, από τα μοτίβα κυκλοφορίας έως τις αντιδράσεις σε καταστροφές και τη χρήση ενέργειας. Στην υγειονομική περίθαλψη, χρησιμοποιούνται για τη δημιουργία λεπτομερών προσομοιώσεων ανθρώπινων οργάνων ή συστημάτων για την πρόβλεψη των απαντήσεων σε θεραπείες ή χειρουργικές επεμβάσεις πριν εφαρμοστούν στον πραγματικό ασθενή. Καθώς η τεχνολογία ψηφιακών διδύμων συνεχίζει να εξελίσσεται, υπόσχεται να γίνει ακόμη πιο αναπόσπαστο μέρος της διαχείρισης πολύπλοκων συστημάτων, προσφέροντας ένα μείγμα αναλυτικών στοιχείων σε πραγματικό χρόνο και δυνατοτήτων πρόβλεψης που οδηγούν την καινοτομία και την αποτελεσματικότητα σε σχεδόν οποιονδήποτε κλάδο.

2.2. iNicosia Digital Twin: Case Study στον Πολεοδομικό Σχεδιασμό

Το έργο iNicosia Digital Twin στη Λευκωσία της Κύπρου, χρησιμεύει ως υποδειγματικό case study που καταδεικνύει την εφαρμογή της τεχνολογίας ψηφιακών διδύμων στην ανάπτυξη έξυπνων πόλεων. Αυτό το φιλόδοξο έργο στοχεύει να ενσωματώσει ολόκληρο το αστικό τοπίο της Λευκωσίας σε ένα λεπτομερές και διαδραστικό 3D μοντέλο, ενσωματώνοντας ένα ευρύ φάσμα τύπων δεδομένων, συμπεριλαμβανομένων λεπτομερειών υποδομής, πληροφοριών κτιρίων, δικτύων μεταφορών και περιβαλλοντικών δεδομένων όπως η ποιότητα του αέρα και η χρήση ενέργειας. Το έργο προέκυψε από μια συνεργασία μεταξύ του δήμου, των τεχνολογικών εταίρων και των ακαδημαϊκών ιδρυμάτων, με στόχο την ενίσχυση της αστικής διαβίωσης, τη βελτιστοποίηση της διαχείρισης της πόλης και την προώθηση της συμμετοχικής διακυβέρνησης. Αυτή η συνεχής προσπάθεια εξελίσσεται συνεχώς καθώς καθίστανται διαθέσιμα νέα δεδομένα και τεχνολογίες, με το έργο να φτάνει σε προχωρημένο στάδιο ανάπτυξης, όπου αρκετές ενότητες λειτουργούν ήδη και χρησιμοποιούνται για πολεοδομικό σχεδιασμό και διαχείριση. Χρησιμεύει ως πρότυπο για άλλες πόλεις παγκοσμίως, αποδεικνύοντας τις δυνατότητες των ψηφιακών διδύμων στην αντιμετώπιση των σύνθετων προκλήσεων του σύγχρονου αστικού περιβάλλοντος.

Το iNicosia Digital Twin χρησιμοποιεί cutting edge technology για να παρέχει πληροφορίες σε πραγματικό χρόνο σχετικά με τη δυναμική της πόλης, επιτρέποντας στους πολεοδόμους και τους υπεύθυνους λήψης αποφάσεων να απεικονίσουν τον αντίκτυπο των αποφάσεών τους πριν τις εφαρμόσουν. Για παράδειγμα, προσομοιώνοντας τα πρότυπα κυκλοφορίας, το σύστημα μπορεί να προβλέψει και να μετριάσει πιθανά σημεία συμφόρησης πριν συμβούν. Αυτή η προορατική προσέγγιση στην αστική διαχείριση συμβάλλει στη σημαντική μείωση του λειτουργικού κόστους και στη βελτίωση της αποτελεσματικότητας των αστικών υπηρεσιών. Επιπλέον, οι δυνατότητες περιβαλλοντικής παρακολούθησης του digital twin, με την χρήση ποικίλων αισθητήρων επιτρέπουν την καλύτερη διαχείριση των πόρων, όπως το νερό και η ενέργεια, και βοηθούν στη χάραξη πολιτικών που στοχεύουν στη μείωση του αποτυπώματος άνθρακα της πόλης.

Επιπλέον, το έργο ενσωματώνει διάφορες συσκευές IoT και αισθητήρες διάσπαρτους σε όλη την πόλη για τη συλλογή δεδομένων σε πραγματικό χρόνο, τα οποία στη συνέχεια αναλύονται για την παρακολούθηση της υγείας της αστικής υποδομής. Τα δεδομένα αυτά είναι ζωτικής σημασίας για την πρόβλεψη των αναγκών συντήρησης και την πρόληψη

αστοχιών υποδομής, οι οποίες είναι ζωτικής σημασίας για τη βιωσιμότητα και την ασφάλεια του αστικού περιβάλλοντος. Το iNicosia Digital Twin ενισχύει επίσης τη δημόσια ασφάλεια ενσωματώνοντας σενάρια αντιμετώπισης καταστάσεων έκτακτης ανάγκης στο πλαίσιό του, επιτρέποντας ταχύτερη και αποτελεσματικότερη ανταπόκριση σε καταστάσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές ή τροχαία ατυχήματα.

2.3. Απειλές για την ασφάλεια στον κυβερνοχώρο σε Digital Twins και κύκλο ζωής δεδομένων

Η ασφάλεια στον κυβερνοχώρο αποτελεί πρωταρχικό μέλημα στον τομέα των Digital Twins, δεδομένης της ενσωμάτωσης πολύπλοκων και ευαίσθητων ροών δεδομένων. Το τοπίο της ασφάλειας στον κυβερνοχώρο για τα Digital Twins περιλαμβάνει μια σειρά απειλών και τρωτών σημείων, που συχνά ενισχύονται από την κλίμακα και την πολυπλοκότητα αυτών των συστημάτων. Οι κοινές απειλές περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις δεδομένων και επιθέσεις στον κυβερνοχώρο, όπως επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS), οι οποίες μπορούν να διαταράξουν τη λειτουργικότητα του ψηφιακού δίδυμου. Τα τρωτά σημεία επιδεινώνονται περαιτέρω από τις συσκευές IoT και τους αισθητήρες που χρησιμοποιούνται σε ψηφιακά δίδυμα, τα οποία μπορούν να χρησιμεύσουν ως σημεία εισόδου για επιθέσεις στον κυβερνοχώρο εάν δεν είναι επαρκώς ασφαλείς. Επιπλέον, ο τεράστιος όγκος και η ποικιλία των δεδομένων που επεξεργάζονται τα Digital Twins θέτουν σημαντικές προκλήσεις στη διαχείριση δεδομένων και την ασφάλεια. Αυτά τα δεδομένα, που συχνά περιλαμβάνουν ευαίσθητες προσωπικές πληροφορίες και λεπτομέρειες κρίσιμης υποδομής, καθιστούν τα Digital Twins ελκυστικούς στόχους για τους attackers του κυβερνοχώρου. Οι πιθανές συνέπειες τέτοιων παραβιάσεων είναι εκτεταμένες, οδηγώντας ενδεχομένως σε εσφαλμένη λήψη αποφάσεων, σε κίνδυνο στις αστικές υποδομές και σε απώλεια της εμπιστοσύνης του κοινού. Ως εκ τούτου, η διατήρηση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων εντός των Digital Twins είναι κρίσιμη, απαιτώντας συνεχή επαγρύπνηση και προηγμένα μέτρα ασφάλειας στον κυβερνοχώρο.

Στην περίπτωση του iNicosia Digital Twin, οι προκλήσεις ασφάλειας είναι πολύπλευρες λόγω της εκτεταμένης αστικής κλίμακας και της ενσωμάτωσης διαφορετικών τύπων δεδομένων και πηγών. Οι πιθανοί φορείς επίθεσης για το iNicosia περιλαμβάνουν την πειρατεία των μεταδόσεων δεδομένων, τη χειραγώγηση των εισροών δεδομένων ή την εκμετάλλευση των τρωτών σημείων στο λογισμικό που χρησιμοποιείται για τη λειτουργία του ψηφιακού δίδυμου. Τέτοιες επιθέσεις θα μπορούσαν να οδηγήσουν σε λανθασμένη αστική μοντελοποίηση, λανθασμένες αναλύσεις ή ακόμα και χειραγώγηση των συστημάτων αστικής υποδομής. Η ενσωμάτωση διαφόρων πηγών δεδομένων – από αισθητήρες κυκλοφορίας και περιβάλλοντος έως υπηρεσίες κοινής ωφέλειας και δεδομένα πολιτών – παρουσιάζει μοναδικές προκλήσεις για τη διασφάλιση της συνέπειας και της ασφάλειας των ροών δεδομένων. Για την αντιμετώπιση αυτών των απειλών, η iNicosia χρειάζεται μια ισχυρή, πολυεπίπεδη στρατηγική ασφάλειας. Αυτή η στρατηγική θα πρέπει να περιλαμβάνει όχι μόνο τεχνικές λύσεις όπως προηγμένη κρυπτογράφηση, τακτικούς ελέγχους ασφαλείας και συστήματα παρακολούθησης απειλών σε πραγματικό χρόνο, αλλά και οργανωτικά μέτρα, συμπεριλαμβανομένων ολοκληρωμένων πολιτικών ασφάλειας στον κυβερνοχώρο, εκπαίδευσης προσωπικού σε βέλτιστες πρακτικές ασφάλειας και συνεργασίας με εμπειρογνώμονες στον τομέα της ασφάλειας στον κυβερνοχώρο. Η εφαρμογή ενός τέτοιου ολοκληρωμένου πλαισίου ασφάλειας είναι

απαραίτητη για τη διαφύλαξη του ψηφιακού διδύμου από απειλές στον κυβερνοχώρο και τη διασφάλιση της αξιοπιστίας του ως εργαλείου αστικής διαχείρισης και σχεδιασμού.

Κύκλος ζωής δεδομένων και Ασφάλεια Δεδομένων στο iNicosia Digital Twin

Ο κύκλος ζωής των δεδομένων εντός του iNicosia Digital Twin είναι ένα κρίσιμο στοιχείο, που περιλαμβάνει τις φάσεις συλλογής, μετάδοσης, αποθήκευσης και επεξεργασίας. Τα δεδομένα συλλέγονται μέσω ενός εκτεταμένου δικτύου αισθητήρων και συσκευών IoT διάσπαρτων σε όλη τη Λευκωσία, συλλέγοντας πληροφορίες σε πραγματικό χρόνο για διάφορες πτυχές της πόλης. Αυτά τα δεδομένα στη συνέχεια μεταδίδονται με ασφάλεια σε κεντρικούς διακομιστές, συχνά χρησιμοποιώντας κρυπτογραφημένα κανάλια επικοινωνίας, και αποθηκεύονται σε ασφαλείς, κλιμακούμενες βάσεις δεδομένων. Τα προηγμένα μέτρα ασφάλειας στον κυβερνοχώρο, όπως τα firewalls και τα intrusion detection systems, είναι απαραίτητα για την προστασία από μη εξουσιοδοτημένη πρόσβαση και cyberthreats.

2.4. Σχέδιο για Ενίσχυση της Ασφάλειας της Πλατφόρμας iNicosia

Στο πλαίσιο του ρόλου μου, σκοπεύω να ενισχύσω σημαντικά την ασφάλεια της πλατφόρμας iNicosia Digital Twin εφαρμόζοντας μια ολοκληρωμένη, πολυεπίπεδη στρατηγική κυβερνοασφάλειας. Αυτό το σχέδιο περιλαμβάνει την ενσωμάτωση προηγμένων πρωτοκόλλων κρυπτογράφησης, όπως το AES και το TLS, για την προστασία των δεδομένων τόσο κατά τη μεταφορά όσο και σε κατάσταση ηρεμίας, διασφαλίζοντας ότι όλες οι επικοινωνίες και οι αποθηκευμένες πληροφορίες προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Αναγνωρίζοντας τη δυναμική φύση των απειλών στον κυβερνοχώρο, θα δώσω προτεραιότητα στους τακτικούς ελέγχους ασφαλείας και στις δοκιμές διείσδυσης (Penetration Testing) για τον προληπτικό εντοπισμό και τον μετριασμό των τρωτών σημείων του συστήματος. Η προσέγγιση αυτή επεκτείνεται σημαντικά με την εφαρμογή και τη δοκιμή διαφόρων γνωστών μεθόδων επίθεσης στον ιστότοπο iNicosia Digital Twin, ώστε να εξακριβωθεί η ανθεκτικότητα και η ασφάλεια του συστήματος. Συμπεριλαμβάνει την εκτέλεση στοχευμένων επιθέσεων, χρησιμοποιώντας τεχνικές όπως SQL injection, cross-site scripting (XSS), και cross-site request forgery (CSRF), με σκοπό να εντοπίσει τρωτά σημεία που ένας πιθανός επιτιθέμενος θα μπορούσε να εκμεταλλευτεί.

Οι δοκιμές αυτές είναι ζωτικής σημασίας, καθώς βοηθούν στην καλύτερη κατανόηση των αδυναμιών του ιστοτόπου. Μετά από κάθε δοκιμή, συλλέγονται δεδομένα και αναλύονται προσεκτικά για να καθοριστούν τα αποτελέσματα και οι επιπτώσεις της ενέργειας αυτής. Αυτό περιλαμβάνει την ανάλυση των τρόπων που οι επιθέσεις μπόρεσαν να διαπεράσουν τις υπάρχουσες ασφαλιστικές διατάξεις, αν τις έχουν διαπεράσει, καθώς και την αξιολόγηση του βαθμού της πιθανής ζημίας που θα μπορούσαν να προκαλέσουν.

Τα αποτελέσματα αυτής της διαδικασίας οδηγούν στη σχεδίαση και υλοποίηση ενισχυμένων μέτρων ασφαλείας, όπως πιο αυστηροί μηχανισμοί επαλήθευσης, ενισχυμένες πολιτικές ασφαλείας και βελτιωμένες τεχνολογίες κρυπτογράφησης. Αυτή η συνεχής αξιολόγηση και αναβάθμιση των συστημάτων ασφαλείας είναι θεμελιώδης για τη διασφάλιση της ακεραιότητας του iNicosia Digital Twin και της ασφάλειας των

χρηστών και των δεδομένων τους. Ένα από τα κύρια χαρακτηριστικά της στρατηγικής μου είναι η θέσπιση ισχυρών μέτρων ελέγχου πρόσβασης, συμπεριλαμβανομένης της επιβολής αυστηρών πολιτικών πρόσβασης και της εφαρμογής ελέγχου ταυτότητας πολλαπλών παραγόντων, για τον περιορισμό της πρόσβασης στο σύστημα μόνο σε εξουσιοδοτημένο προσωπικό. Αναγνωρίζοντας τον κρίσιμο ρόλο των συσκευών IoT στην υποδομή ψηφιακών διδύμων, σκοπεύω να επιβάλω αυστηρά πρότυπα ασφαλείας, συμπεριλαμβανομένων των τακτικών ενημερώσεων υλικολογισμικού και της τμηματοποίησης δικτύου, για να ελαχιστοποιήσω τον κίνδυνο εκμετάλλευσης συσκευών.

Επιπλέον, σε μετέπειτα στάδιο θεωρώ ότι είναι σημαντική η διασφάλιση της ανθεκτικότητας του συστήματος μέσω ενός καλά δομημένου σχεδίου αποκατάστασης καταστροφών (structured disaster recovery plan), συνοδευόμενου από τακτικά και ασφαλή αντίγραφα ασφαλείας δεδομένων, για τη διασφάλιση της ακεραιότητας και της διαθεσιμότητας των δεδομένων σε κάθε ενδεχόμενο, να εισαχθούν συνεχή προγράμματα κατάρτισης προσωπικού, δίνοντας έμφαση στην ευαισθητοποίηση και τις βέλτιστες πρακτικές για την ασφάλεια στον κυβερνοχώρο.

2.5. Βασικοί ενδιαφερόμενοι φορείς

1. **Δημοτική Αρχή Λευκωσίας:** θα είναι ο κύριος ενδιαφερόμενος, επιβλέποντας ολόκληρο το έργο, διασφαλίζοντας ότι ευθυγραμμίζεται με τους στόχους πολεοδομικού σχεδιασμού και ανάπτυξης της πόλης.

2. **Πολεοδόμοι και Αρχιτέκτονες:** Επαγγελματίες που θα χρησιμοποιούσαν το ψηφιακό δίδυμο για σκοπούς σχεδιασμού και ανάπτυξης, αξιολογώντας την τρέχουσα υποδομή της πόλης και προβλέποντας μελλοντικές ανάγκες.

3. **Πάροχοι τεχνολογίας:** Εταιρείες ή οργανισμοί που παρέχουν λύσεις υλικού και λογισμικού για 3D μοντελοποίηση, συσκευές IoT, ενσωματώσεις αισθητήρων, και τη συνολική πλατφόρμα ψηφιακών διδύμων.

4. **Αναλυτές Δεδομένων & Επιστήμονες:** Άτομα ή ομάδες που επεξεργάζονται και ερμηνεύουν τις τεράστιες ποσότητες δεδομένων σε πραγματικό χρόνο που συλλέγονται από τους αισθητήρες της πόλης, εξασφαλίζοντας ακριβή αναπαράσταση και πληροφορίες.

5. **Ειδικοί στον τομέα της ασφάλειας στον κυβερνοχώρο:** Ειδικοί επιφορτισμένοι με τη διασφάλιση της ασφάλειας της πλατφόρμας, την προστασία από πιθανές παραβιάσεις και απειλές στον κυβερνοχώρο.

6. **Επιτροπές Πολιτισμού & Πολιτιστικής Κληρονομιάς:** Ομάδες που επικεντρώθηκαν στη διατήρηση και την ακριβή αναπαράσταση των ιστορικών και πολιτιστικών ορόσημων της πόλης στο πλαίσιο του ψηφιακού μοντέλου.

7. **Περιβαλλοντικοί Φορείς:** Ενδιαφερόμενοι φορείς που ενδιαφέρονται για την περιβαλλοντική υγεία της πόλης, χρησιμοποιώντας τα δεδομένα για μελέτες σχετικά με τη ρύπανση, τη βλάστηση, τα καιρικά φαινόμενα κ.λπ.

8. **Τμήματα Μεταφορών & Υποδομών:** Φορείς που διαχειρίζονται τα οδικά δίκτυα της πόλης, τα δίκτυα ηλεκτρικής ενέργειας, τα συστήματα ύδρευσης κ.λπ., οι οποίοι θα χρησιμοποιούν το ψηφιακό δίδυμο για αποτελεσματική διαχείριση και μελλοντικό σχεδιασμό.

9. **Πολίτες Λευκωσίας:** Ως τελικοί δικαιούχοι, οι κάτοικοι μπορούν να είναι τόσο παθητικοί φορείς (ως πηγές δεδομένων μέσω συσκευών IoT) όσο και ενεργοί συμμετέχοντες, παρέχοντας ανατροφοδότηση, χρησιμοποιώντας την πλατφόρμα για διάφορους σκοπούς και ενδεχομένως συμμετέχοντας σε πρωτοβουλίες με γνώμονα την κοινότητα που συνδέονται με την πλατφόρμα.
10. **Εκπαιδευτικά Ιδρύματα:** Τα πανεπιστήμια και τα ερευνητικά ιδρύματα μπορούν να χρησιμοποιήσουν την πλατφόρμα για ακαδημαϊκή έρευνα, αστικές μελέτες, τεχνολογική ανάπτυξη και πολλά άλλα.

Κεφάλαιο 3

3. iNicosia Digital Twin: Μια Εις Βάθος Ανάλυση

3.1. Αρχιτεκτονική του iNicosia Digital Twin

3.2. Άλλες Digital Twin Αρχιτεκτονικές: TM and Fiware

3.3. Συγκριτική ανάλυση

3.1. Αρχιτεκτονική του iNicosia Digital Twin

Η αρχιτεκτονική iNicosia Digital Twin αντιπροσωπεύει μια πλατφόρμα που έχει σχεδιαστεί για να ενισχύσει την αστική διαχείριση και τον σχεδιασμό μέσω προηγμένων δυνατοτήτων προσομοίωσης και ανάλυσης. Δημιουργώντας ένα εικονικό αντίγραφο του αστικού περιβάλλοντος της Λευκωσίας, το σύστημα αυτό ενσωματώνει δεδομένα σε πραγματικό χρόνο από διάφορες πηγές, συμπεριλαμβανομένων συσκευών IoT, αισθητήρων και εισροών χρηστών. Αυτή η ενσωμάτωση επιτρέπει στους πολεοδόμους, τους διαχειριστές και τους πολίτες να οπτικοποιούν και να αλληλεπιδρούν με τα δυναμικά δεδομένα της πόλης με τρόπους που δεν ήταν προηγουμένως δυνατοί. Λειτουργικά, το iNicosia Digital Twin εξυπηρετεί πολλαπλούς σκοπούς. Υποστηρίζει τη λήψη αποφάσεων παρέχοντας λεπτομερείς πληροφορίες σχετικά με τις τρέχουσες συνθήκες και προγνωστικές αναλύσεις για μελλοντικά σενάρια. Αυτό διευκολύνει την αποτελεσματική διαχείριση των πόρων, τις βελτιωμένες στρατηγικές αντιμετώπισης καταστάσεων έκτακτης ανάγκης και τον αποτελεσματικότερο πολεοδομικό σχεδιασμό. Τα ισχυρά αναλυτικά εργαλεία της πλατφόρμας επιτρέπουν στους χρήστες να προσομοιώνουν τις επιπτώσεις πιθανών αλλαγών στην αστική πολιτική ή τις υποδομές, διασφαλίζοντας ότι οι αποφάσεις βασίζονται σε δεδομένα και βελτιστοποιούνται

τόσο για άμεσα όσο και για μακροπρόθεσμα αποτελέσματα. Μέσω του ολοκληρωμένου και διαδραστικού μοντέλου της, η αρχιτεκτονική του iNicosia Digital Twin συμβάλλει σημαντικά στη βιώσιμη ανάπτυξη και λειτουργική αποτελεσματικότητα της πόλης.

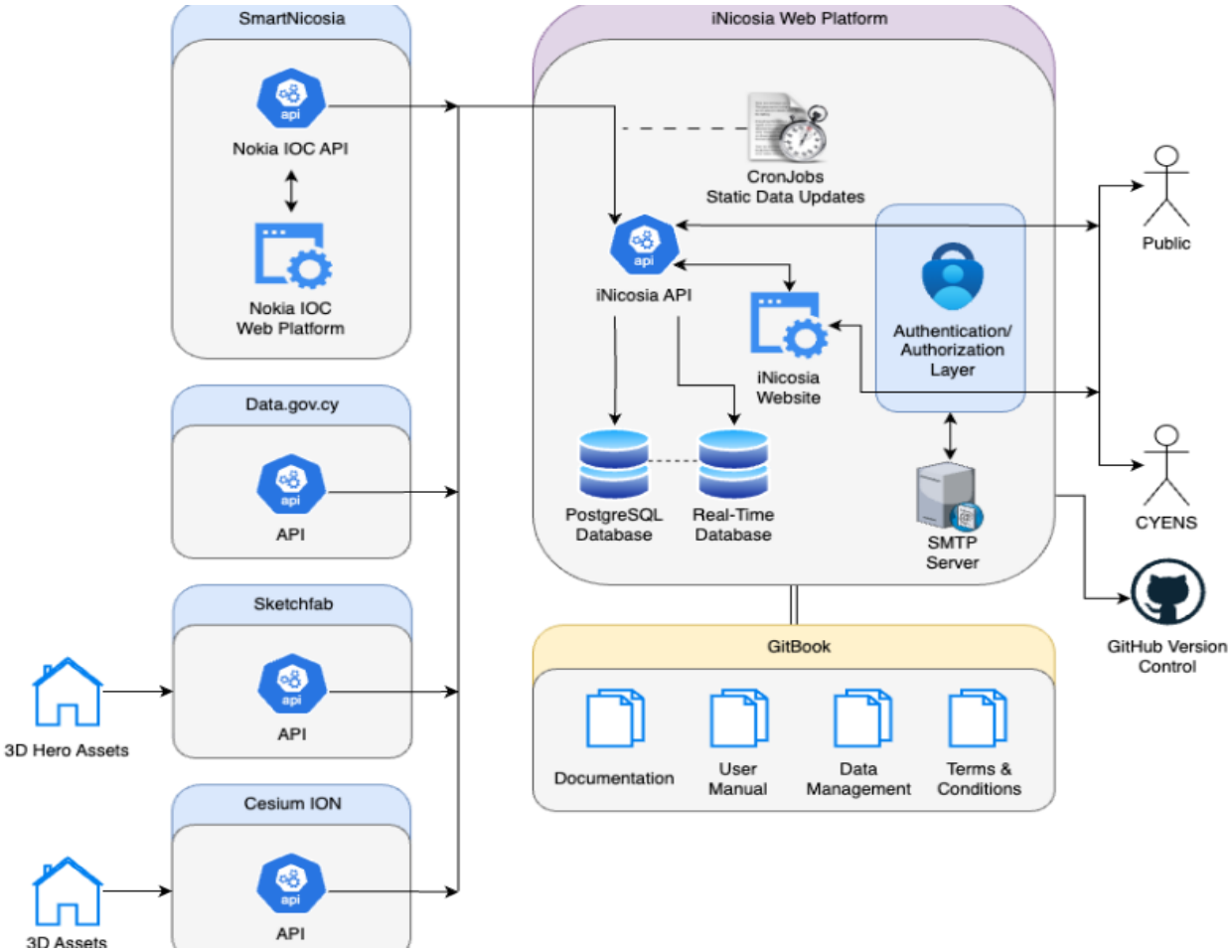

Figure 1: Diagram of the Architecture of iNicosia Digital Twin Platform

Πηγές δεδομένων και ενσωμάτωση:

1. **SmartNicosia**: Αντιπροσωπεύει ένα higher-level integration layer που συγκεντρώνει δεδομένα ή λειτουργίες ειδικά για την υποδομή της πόλης.

    - **Ρόλος και λειτουργικότητα**: Το SmartNicosia λειτουργεί ως ο κύριος κόμβος ενσωμάτωσης για την πλατφόρμα iNicosia, λειτουργώντας ως κεντρικός κόμβος που συγκεντρώνει και επεξεργάζεται ένα ευρύ φάσμα αστικών δεδομένων. Αυτό περιλαμβάνει δεδομένα διαχείρισης κυκλοφορίας, περιβαλλοντικούς αισθητήρες και μετρήσεις δημόσιας υπηρεσίας.

- **Αντίκτυπος στη διαχείριση της πόλης**: Συγκεντρώνοντας αυτές τις πληροφορίες, το SmartNicosia υποστηρίζει εξελιγμένες αναλύσεις που βοηθούν τους διαχειριστές της πόλης να λαμβάνουν αποφάσεις βάσει δεδομένων με στόχο τη βελτίωση των δημοτικών υπηρεσιών, την ενίσχυση της δημόσιας ασφάλειας και τη βελτιστοποίηση της διαχείρισης πόρων.

2. **Nokia IOC API και διαδικτυακή πλατφόρμα**: Χρησιμοποιεί την τεχνολογία Integrated Operations Center (IOC) της Nokia, παρέχοντας δεδομένα κρίσιμης υποδομής και αναλυτικά στοιχεία.

   - **Επισκόπηση τεχνολογίας**: Η ενσωμάτωση με το Integrated Operations Center (IOC) της Nokia παρέχει ένα ισχυρό πλαίσιο για παρακολούθηση και ανάλυση δεδομένων σε πραγματικό χρόνο. Η πλατφόρμα Nokia IOC αξιοποιεί τεχνολογίες IoT, μηχανικής μάθησης και μεγάλων δεδομένων για να προσφέρει διορατικές δυνατότητες ανάλυσης και πρόβλεψης.
   - **Οφέλη για το iNicosia**: Αυτή η τεχνολογία ενδυναμώνει την iNicosia με προηγμένα εργαλεία για τη διαχείριση συμβάντων, την προληπτική συντήρηση των δημόσιων υποδομών και την ενισχυμένη λειτουργική αποτελεσματικότητα σε διάφορα τμήματα της πόλης.

3. **Data.gov.cy**: Ενσωματώνεται με μια κυβερνητική πύλη δεδομένων, που χρησιμοποιείται για πρόσβαση σε δημόσια σύνολα δεδομένων σχετικά με τη Λευκωσία.

   - **Κυβερνητική συνεργασία**: Ως μέρος της ενσωμάτωσης, το iNicosia χρησιμοποιεί Data.gov.cy για πρόσβαση σε πληθώρα κυβερνητικών συνόλων δεδομένων. Αυτά τα σύνολα δεδομένων περιλαμβάνουν δημογραφικά στοιχεία, στατιστικές ακινήτων, δεδομένα δημόσιας υγείας και άλλα, τα οποία είναι ζωτικής σημασίας για τον πολεοδομικό σχεδιασμό και τη χάραξη πολιτικής.
   - **Αξιοποίηση δεδομένων**: Η πλατφόρμα χρησιμοποιεί αυτά τα κυβερνητικά δεδομένα για να εμπλουτίσει την κατανόηση της αστικής δυναμικής με βάση τα συμφραζόμενα, να υποστηρίξει την κοινωνικοοικονομική έρευνα και να διευκολύνει τη διαφάνεια και τη συμμετοχή των πολιτών, καθιστώντας τα σχετικά δεδομένα προσβάσιμα στο κοινό.

4. **Sketchfab &; Cesium ION**: Αυτές οι υπηρεσίες παρέχουν 3D μοντελοποίηση και οπτικοποίηση, με API που ενισχύουν τις χωρικές και δομικές πτυχές του ψηφιακού δίδυμου.

   - **Τεχνολογίες 3D οπτικοποίησης**: Το Sketchfab και το Cesium ION αποτελούν αναπόσπαστο μέρος του iNicosia για την παροχή λεπτομερών δυνατοτήτων 3D μοντελοποίησης και οπτικοποίησης. Αυτά τα εργαλεία επιτρέπουν στην πλατφόρμα να δημιουργεί ακριβείς και διαδραστικές αναπαραστάσεις αστικών τοπίων και έργων υποδομής.

   - **Εφαρμογή στην ψηφιακή αδελφοποίηση**: Μέσω API από αυτές τις υπηρεσίες, το iNicosia είναι σε θέση να επικαλύπτει δεδομένα σε πραγματικό χρόνο σε 3D μοντέλα πόλεων, ενισχύοντας την οπτικοποίηση της ανάλυσης δεδομένων, προσομοιώνοντας αλλαγές υποδομής και σχεδιάζοντας μελλοντικά έργα αστικής ανάπτυξης σε ένα οπτικά διαισθητικό περιβάλλον.

Figure 2: 3D Αναπαράσταση της πλατείας Ελευθερίας από το iNicosia API

Βασικά στοιχεία συστήματος:

1. **iNicosia API**: Λειτουργεί ως ενδιάμεσο λογισμικό διευκολύνοντας τη ροή δεδομένων μεταξύ της διαδικτυακής πλατφόρμας και των βάσεων δεδομένων, διασφαλίζοντας τη σωστή επεξεργασία και προώθηση των αλληλεπιδράσεων δεδομένων.

    - **Λειτουργικότητα**: Το iNicosia API λειτουργεί ως το κεντρικό ενδιάμεσο λογισμικό που ενορχηστρώνει την απρόσκοπτη ενοποίηση και αλληλεπίδραση μεταξύ της διαδικτυακής πλατφόρμας και των υποκείμενων βάσεων δεδομένων. Είναι υπεύθυνη για την αποτελεσματική δρομολόγηση, επεξεργασία και διασφάλιση των συναλλαγών δεδομένων εντός του οικοσυστήματος.

    - **Ρόλος στην αρχιτεκτονική του συστήματος:** Αυτό το API διασφαλίζει ότι όλα τα στοιχεία επικοινωνούν αποτελεσματικά, διατηρώντας τη συνέπεια και την ακεραιότητα των δεδομένων σε ολόκληρη την πλατφόρμα. Επιτρέπει modular updates και scalable integration νέων λειτουργιών ή προελεύσεων δεδομένων.

2. **Βάση δεδομένων PostgreSQL**: Χρησιμοποιείται για δομημένη αποθήκευση δεδομένων, χειρίζεται δυναμικό περιεχόμενο που τροφοδοτεί λειτουργίες της πλατφόρμας σε πραγματικό χρόνο.

    - **Διαχείριση δεδομένων**: Χρησιμοποιείται κυρίως για δομημένη αποθήκευση δεδομένων, η βάση δεδομένων PostgreSQL υποστηρίζει την πλατφόρμα iNicosia με ισχυρές δυνατότητες χειρισμού δεδομένων. Διαχειρίζεται το δυναμικό περιεχόμενο που τροφοδοτεί τις λειτουργίες της πλατφόρμας σε πραγματικό χρόνο.

    - **Επιχειρησιακή σημασία**: Αυτό το σύστημα βάσεων δεδομένων επιλέγεται για την αξιοπιστία, την ακεραιότητα των δεδομένων και τη συμβατότητά του με πολύπλοκα μοντέλα δεδομένων, τα οποία είναι σημαντικά για τις ποικίλες και εντατικές λειτουργίες δεδομένων μιας ψηφιακής δίδυμης πλατφόρμας όπως η iNicosia.

3. **Βάση δεδομένων σε πραγματικό χρόνο**: Μια εξειδικευμένη βάση δεδομένων βελτιστοποιημένη για το χειρισμό ροών δεδομένων σε πραγματικό χρόνο, απαραίτητη για δυναμικές ενημερώσεις και ανταποκρινόμενες αλληλεπιδράσεις στην πλατφόρμα.

    - **Εξειδικευμένες Δυνατότητες**: Η βάση δεδομένων σε πραγματικό χρόνο είναι προσαρμοσμένη ειδικά για τη διαχείριση ζωντανών ροών δεδομένων που απαιτούν άμεση επεξεργασία και ανταπόκριση. Αυτό το σύστημα υποστηρίζει λειτουργίες υψηλής απόδοσης και χαμηλής καθυστέρησης, οι οποίες είναι ζωτικής σημασίας για την ανάλυση δεδομένων σε πραγματικό χρόνο και τις διαδικασίες λήψης αποφάσεων.

    - **Χρησιμότητα και απόδοση**: Απαραίτητη για δυναμικές ενημερώσεις, αυτή η βάση δεδομένων διευκολύνει τις αλληλεπιδράσεις σε πραγματικό χρόνο και επιτρέπει στην πλατφόρμα να εκτελεί άμεσες αναλύσεις και ενημερώσεις δεδομένων. Η απόδοσή του επηρεάζει τη συνολική ανταπόκριση της πλατφόρμας, διασφαλίζοντας ότι οι αλληλεπιδράσεις των χρηστών και οι αυτοματοποιημένες απαντήσεις του συστήματος είναι γρήγορες και αποτελεσματικές.

    -

Figure 3: Real time Capabilities for Comparison Tools

Υπηρεσίες υποστήριξης και χρησιμότητας:

1. **Επίπεδο ελέγχου ταυτότητας/εξουσιοδότησης**: Εξασφαλίζει την πρόσβαση στην πλατφόρμα, διασφαλίζοντας ότι όλες οι αλληλεπιδράσεις πιστοποιούνται και εξουσιοδοτούνται.

    - **Ρόλος στην ακεραιότητα του συστήματος**: Το επίπεδο ελέγχου ταυτότητας χρησιμοποιεί σύγχρονα πρότυπα ασφαλείας, όπως το OAuth2 ή το JWT (JSON Web Tokens), για την αποτελεσματική διαχείριση και επικύρωση των περιόδων λειτουργίας των χρηστών. Αυτό το επίπεδο είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας και του απορρήτου των δεδομένων της πλατφόρμας και των αλληλεπιδράσεων των χρηστών.

2. **SMTP Server**: Διαχειρίζεται την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που χρησιμοποιούνται για ειδοποιήσεις, ειδοποιήσεις ή επικοινωνίες συστήματος.

    - **Χειρισμός επικοινωνίας**: Ο server SMTP (Simple Mail Transfer Protocol) είναι υπευθηνος για τη διαχείριση των επικοινωνιών ηλεκτρονικού ταχυδρομείου εντός της πλατφόρμας iNicosia. Αυτό περιλαμβάνει την αποστολή ειδοποιήσεων, ειδοποιήσεων ή οποιωνδήποτε επικοινωνιών που σχετίζονται με το σύστημα και διευκολύνουν την αλληλεπίδραση του χρήστη και τις λειτουργικές ενημερώσεις.

    - **Λειτουργική αποδοτικότητα**: Εξασφαλίζει αξιόπιστη παράδοση επικοινωνιών ηλεκτρονικού ταχυδρομείου, οι οποίες είναι ζωτικής σημασίας για την εγγραφή χρηστών, την επαναφορά κωδικού πρόσβασης, τις επιχειρησιακές ειδοποιήσεις και άλλες διοικητικές επικοινωνίες. Η αποτελεσματικότητα του διακομιστή SMTP επηρεάζει άμεσα την ικανότητα της πλατφόρμας να αλληλεπιδρά με τους χρήστες και να παρέχει έγκαιρες ενημερώσεις

.

3. **CronJobs για ενημερώσεις στατικών δεδομένων**: Προγραμματισμένες εργασίες που ενημερώνουν τακτικά το σύστημα με νέα δεδομένα, διασφαλίζοντας ότι η πλατφόρμα παραμένει ενημερωμένη.

    - **Διαχείριση δεδομένων**: Τα CronJobs είναι προγραμματισμένες εργασίες που έχουν ρυθμιστεί ώστε να εκτελούνται σε συγκεκριμένα χρονικά διαστήματα για την ενημέρωση της πλατφόρμας με τα πιο πρόσφατα δεδομένα. Αυτές οι εργασίες είναι απαραίτητες για τη διατήρηση της ακρίβειας των πληροφοριών που εμφανίζονται στην πλατφόρμα.

    - **Αξιοπιστία συστήματος**: Οι τακτικές ενημερώσεις μέσω του CronJobs διασφαλίζουν ότι η πλατφόρμα παραμένει σχετική και αποτελεσματική, παρέχοντας στους χρήστες τις πιο πρόσφατες πληροφορίες και βελτιώνοντας τη διαδικασία λήψης αποφάσεων. Αυτοματοποιούν τη διαδικασία ενημέρωσης ρουτίνας, μειώνοντας την ανάγκη για χειροκίνητες παρεμβάσεις και ενισχύοντας τη συνολική αξιοπιστία της πλατφόρμας.

Τεκμηρίωση και έλεγχος έκδοσης:

1. **GitBook**: Διαχειρίζεται την τεκμηρίωση, βοηθώντας τους χρήστες και τους προγραμματιστές να κατανοήσουν και να αλληλεπιδράσουν αποτελεσματικά με την πλατφόρμα.
    - **Διαχείριση τεκμηρίωσης**: Το GitBook χρησιμεύει ως κεντρική πλατφόρμα για τη διαχείριση ολοκληρωμένης τεκμηρίωσης για την πλατφόρμα iNicosia. Επιτρέπει στους προγραμματιστές και τους χρήστες να έχουν πρόσβαση σε ενημερωμένη τεκμηρίωση, η οποία είναι χρήσιμη για την κατανόηση των λειτουργιών της πλατφόρμας, της χρήσης API και των λειτουργικών οδηγιών.
    - **Υποστήριξη χρηστών και προγραμματιστών**: Παρέχοντας ένα σαφές και δομημένο documentation repository, το GitBook βελτιώνει την εμπειρία χρήστη και την αποτελεσματικότητα των προγραμματιστών. Βοηθά στην ενσωμάτωση νέων χρηστών και προγραμματιστών προσφέροντας οδηγούς βήμα προς βήμα, σενάρια χρήσης και τεχνικές

προδιαγραφές που διευκολύνουν την αποτελεσματική αλληλεπίδραση με την πλατφόρμα.

2. **Έλεγχος έκδοσης GitHub**: Διαχειρίζεται την ανάπτυξη της πλατφόρμας μέσω του GitHub, διευκολύνοντας τον έλεγχο εκδόσεων και τη συνεργατική ανάπτυξη.

    - **Διαχείριση Ανάπτυξης**: Το GitHub χρησιμοποιείται ως το κύριο εργαλείο για τον έλεγχο εκδόσεων και τη διαχείριση ανάπτυξης της πλατφόρμας iNicosia. Ενορχηστρώνει τις συνεργατικές προσπάθειες των προγραμματιστών παρέχοντας εργαλεία για έλεγχο κώδικα, παρακολούθηση ζητημάτων και διαχείριση εκδόσεων, διασφαλίζοντας ότι όλες οι αλλαγές τεκμηριώνονται και ενσωματώνονται συστηματικά.

    - **Συνεργατική Ανάπτυξη**: Η χρήση του GitHub διευκολύνει ένα συνεργατικό περιβάλλον όπου οι προγραμματιστές μπορούν να συνεισφέρουν στο έργο από διάφορες τοποθεσίες. Υποστηρίζει διακλάδωση και συγχώνευση, επιτρέποντας σε πολλούς προγραμματιστές να εργάζονται σε διαφορετικές λειτουργίες ταυτόχρονα χωρίς να διαταράσσουν την κύρια ροή εργασίας ανάπτυξης. Αυτή η ρύθμιση βελτιώνει την επεκτασιμότητα και την ταχύτητα ανάπτυξης, διατηρώντας παράλληλα υψηλά πρότυπα ποιότητας κώδικα.

3.2. Άλλες Digital Twin Αρχιτεκτονικές: TM και Fiware

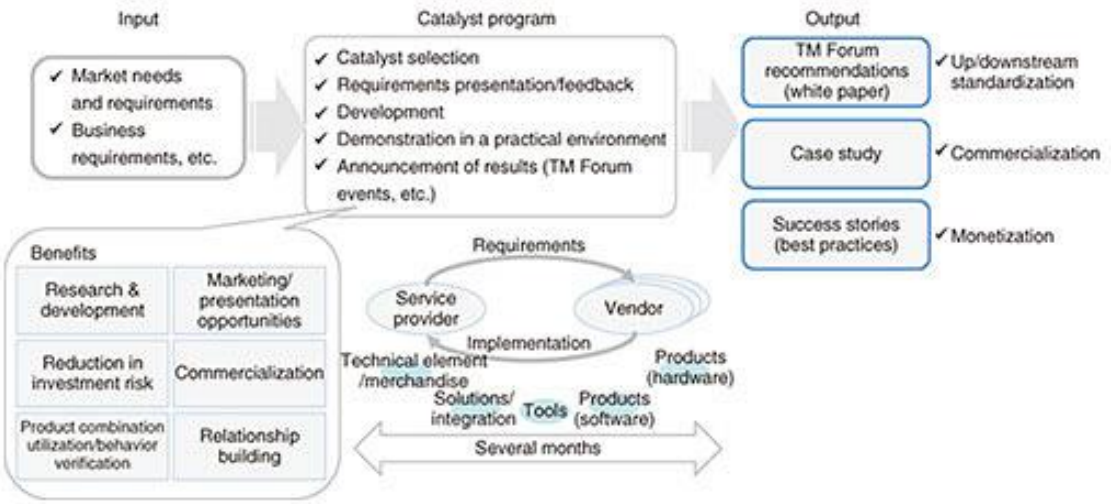

Figure 4: PoC (Catalyst) positioning at TM Forum image taken from NTT Technical Review Archives

Το TM Forum [1] ξεκίνησε ως Open Source Initiative/Network Management Forum το 1988 και είναι ο μεγαλύτερος διεθνής οργανισμός τυποποίησης στον τομέα της διαχείρισης τηλεπικοινωνιών με περισσότερους από 850 συνδεδεμένους μεγάλους παρόχους και προμηθευτές παγκοσμίως που μελετούν βιομηχανικά πρότυπα στον τομέα των επιχειρήσεων για την προώθηση της διαλειτουργικότητας. Η Open Digital Architecture (ODA) προτάθηκε ως αρχιτεκτονική του συστήματος υποστήριξης επιχειρήσεων και του συστήματος υποστήριξης λειτουργιών (BSS/OSS) και το πλαίσιο για την υλοποίηση αυτής της αρχιτεκτονικής ορίζεται ως το Open Digital Framework (ODF). Το φόρουμ συζητά επίσης κατηγορίες που καθορίζονται με βάση τις επιχειρηματικές τάσεις (projectivization), την αρχιτεκτονική, τις διεπαφές προγραμματισμού εφαρμογών (API), τα μοντέλα πληροφοριών και ούτω καθεξής που βασίζονται σε συγκεκριμένες περιπτώσεις χρήσης και σενάρια. Έχουν γίνει συζητήσεις για έργα όπως το Autonomous Network Project, το οποίο στοχεύει σε αυτόνομες λειτουργίες δικτύου, το Customer Experience Management Project, το οποίο στοχεύει στη βελτίωση της ικανοποίησης των πελατών και το Digital Ecosystem Management Project, το οποίο στοχεύει σε εφαρμογές για έξυπνες πόλεις (συμπεριλαμβανομένου του Internet of Things) κ.λπ. Διεξάγονται προγράμματα απόδειξης της ιδέας (PoC) (Catalyst) για να αποδειχθεί η σκοπιμότητα αυτών των τυποποιημένων εγγράφων όσον αφορά: υλοποίηση και εφαρμογή σε νέους επιχειρηματικούς τομείς και περίπου 40 ομάδες (μία ομάδα αποτελείται από πέντε έως δέκα μεταφορείς/προμηθευτές) συμμετέχουν ετησίως. Αυτά τα PoCs εκτίθενται αρκετές φορές το χρόνο σε εκδηλώσεις TM Forum (Digital Transformation World κ.λπ.), όπου ένας αριθμός προμηθευτών μεταφορέων επιδεικνύουν τα νέα επιχειρηματικά μοντέλα και τις τεχνικές τους δυνατότητες που συμβάλλουν στις δραστηριότητες τυποποίησης του φόρουμ.

TM Digital Twin Architecture

1. CFN Service Twin

- **Επισκόπηση χωρητικότητας δικτύου**: Ενσωματώνει Γεωγραφικά Συστήματα Πληροφοριών (GIS) για να παρέχει μια χωρική άποψη της χωρητικότητας και των λειτουργιών του δικτύου, ενισχύοντας τη λήψη αποφάσεων με γεωχωρικά δεδομένα.

- **Κύκλος χωρητικότητας**: Υλοποιεί αμφίδρομη αξιολόγηση, για δυναμικό σχεδιασμό χωρητικότητας και βελτιστοποίηση απόδοσης.

- **Παρακολούθηση ιδιωτικού δικτύου**: Ενσωματώνει Key Performance Indicators (KPIs) προσαρμοσμένα στις συγκεκριμένες ανάγκες των χρηστών, επιτρέποντας την εξατομικευμένη παρακολούθηση και διαχείριση υπηρεσιών.

2. Network Status Twin

- **Παρακολούθηση σε πραγματικό χρόνο**: Χρησιμοποιεί τεχνικές ανίχνευσης ανωμαλιών για να παρέχει άμεσες πληροφορίες σχετικά με την εύρυθμη λειτουργία του δικτύου και την κατάσταση λειτουργίας.

- **Ανάλυση βλαβών**: Χρησιμοποιεί προηγμένα διαγνωστικά για τον προσδιορισμό της βασικής αιτίας των προβλημάτων δικτύου, βοηθώντας στην ταχύτερη επίλυση και ελαχιστοποιώντας το χρόνο διακοπής λειτουργίας.

- **Εντοπισμός κινδύνου**: Χρησιμοποιεί Artificial Intelligence/Machine Learning (AI/ML) για την εκτίμηση πιθανών κινδύνων εντός της υποδομής δικτύου, επιτρέποντας προληπτικές ενέργειες έναντι προβλέψιμων ζητημάτων.

3. Physical Resource Twin

- **Χωρικοί Πόροι**: Συνδυάζει δεδομένα GIS και Computer-Aided Design (CAD) για να προσφέρει λεπτομερείς απεικονίσεις φυσικών περιουσιακών στοιχείων, όπως κτίρια και διατάξεις υποδομής.

- **Πόροι δικτύου**: Ενισχύει τη συλλογή δεδομένων και τη διαχείριση περιουσιακών στοιχείων μέσω τεχνολογιών όπως η μηχανική όραση (machine vision), η RFID και το σόναρ, οι οποίες διευκολύνουν την αυτόματη αναγνώριση πόρων και τη χαρτογράφηση τοπολογίας.

4. Υποδομή δικτύων

- **Αίθουσα εξοπλισμού**: Περιγράφει λεπτομερώς τα συγκεκριμένα στοιχεία υποδομής που στεγάζονται εντός της εγκατάστασης, διασφαλίζοντας βέλτιστες στρατηγικές τοποθέτησης και συντήρησης.

- **Σύστημα ισχύος και RAN:** Επικεντρώνεται στις λειτουργικές πτυχές των Radio Access Networks και των συστημάτων ηλεκτρικής ενέργειας εντός του δικτύου, ζωτικής σημασίας για την αδιάλειπτη παροχή υπηρεσιών.

- **Δίκτυο πυρήνα, μετάδοσης, CMNET και περιεχομένου**: Οριοθετεί τα βασικά στοιχεία του δικτύου, συμπεριλαμβανομένων των δικτύων παράδοσης περιεχομένου και των συστημάτων μετάδοσης, τα οποία αποτελούν αναπόσπαστο μέρος της απόδοσης και της επεκτασιμότητας του δικτύου.

5. Οπτικοποίηση υπηρεσίας 2B

- **Μηχανή ανάλυσης συμπεριφοράς**: Χρησιμοποιεί πορτρέτα χρήστη vehicle-to-everything (V2X) για την ανάλυση μοτίβων συμπεριφοράς, βελτιώνοντας την εμπειρία χρήστη και την ασφάλεια.

- **Μοντέλο αναγνώρισης δράσης**: Προσδιορίζει κρίσιμες ενέργειες στο πλαίσιο του Core Service Twin του V2X, βελτιστοποιώντας τις στρατηγικές απόδοσης και απόκρισης.

- **Μοντέλο προσομοίωσης ποιότητας υπηρεσιών**: Αναπτύσσει εικονικά μοντέλα σταθμών παραγωγής ενέργειας για την προσομοίωση των συνθηκών και της απόδοσης του δικτύου, βοηθώντας στην προληπτική συντήρηση και τον σχεδιασμό ανθεκτικότητας του συστήματος.

6. Αντίληψη υποβάθμισης ποιότητας

- **Ανάπτυξη Γεω-Μοντέλων**: Περιλαμβάνει τη δημιουργία γεωγραφικών μοντέλων που βοηθούν στην κατανόηση και την πρόβλεψη της υποβάθμισης της ποιότητας σε διαφορετικές περιοχές

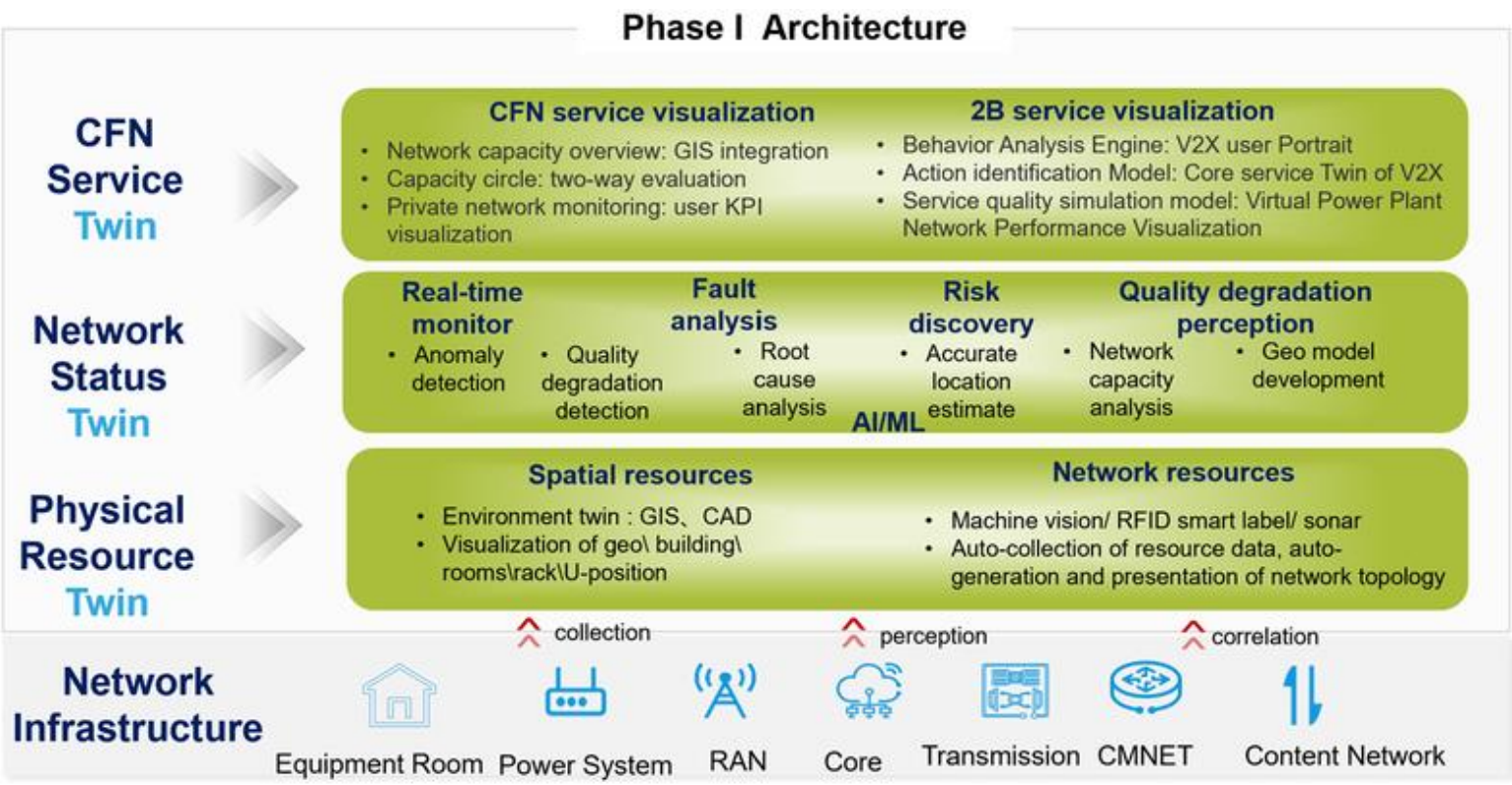

Figure 5: Digital Twin Architecture of TM Forum Platform

FIWARE for Digital Twins

Fiware Overview

Το FIWARE είναι μια δυναμική και επεκτάσιμη πλατφόρμα που έχει σχεδιαστεί για να προωθεί την ανάπτυξη έξυπνων εφαρμογών σε διάφορους τομείς όπως οι έξυπνες πόλεις, η γεωργία, η ενέργεια και άλλα. Ο πυρήνας της λειτουργικότητας του FIWARE έγκειται στο FIWARE Context Broker, ένα βασικό στοιχείο που επιτρέπει αλληλεπιδράσεις μεταξύ των φυσικών και εικονικών οντοτήτων ενός συστήματος. Αυτός ο broker αξιοποιεί μια ποικιλία Generic Enablers (GEs), οι οποίοι παρέχουν εργαλεία για το χειρισμό αλληλεπιδράσεων, τη διαχείριση δεδομένων περιβάλλοντος και την υποστήριξη διεξοδικής επεξεργασίας και ανάλυσης δεδομένων. Αυτή η αρχιτεκτονική όχι μόνο προωθεί την απρόσκοπτη

αλληλεπίδραση με συσκευές Internet of Things (IoT), αλλά διευκολύνει επίσης την ενσωμάτωση εξωτερικών συστημάτων, η οποία είναι ζωτικής σημασίας για τη διατήρηση συγχρονισμού δεδομένων σε πραγματικό χρόνο και ενημερώσεων σε ψηφιακά δίδυμα μοντέλα.

Η ισχυρή δυνατότητα της πλατφόρμας περιλαμβάνει IoT Agents που υποστηρίζουν πολλαπλά πρωτόκολλα επικοινωνίας για τον εξορθολογισμό των ροών δεδομένων από ένα ευρύ φάσμα συσκευών IoT, διασφαλίζοντας την αποδοτική και αποτελεσματική ενσωμάτωση στο περιβάλλον Digital Twins. Ένα άλλο βασικό στοιχείο, το Draco, το οποίο βασίζεται στο Apache NiFi, ενισχύει τη διαχείριση των ροών δεδομένων επιτρέποντας εξελιγμένους μετασχηματισμούς και δρομολόγηση ροών δεδομένων εντός της υποδομής ψηφιακών διδύμων. Η ασφάλεια και η διακυβέρνηση δεδομένων είναι επίσης υψίστης σημασίας στο οικοσύστημα FIWARE, με συγκεκριμένες GE που επικεντρώνονται σε ασφαλείς διαδικασίες ελέγχου ταυτότητας και εξουσιοδότησης για τον έλεγχο της πρόσβασης στις λειτουργίες της πλατφόρμας.
Η προσαρμοστικότητα του FIWARE αναδεικνύεται σε πρακτικές εφαρμογές όπως τα έξυπνα συστήματα στάθμευσης, όπου τα Digital Twins χρησιμοποιούν δεδομένα σε πραγματικό χρόνο για τη διαχείριση και την πρόβλεψη της διαθεσιμότητας στάθμευσης και της ροής της κυκλοφορίας, ενισχύοντας τη διαχείριση της αστικής κινητικότητας. Μέσω της αρθρωτής και ολοκληρωμένης εργαλειοθήκης του, το FIWARE δίνει τη δυνατότητα στους προγραμματιστές να δημιουργούν λεπτομερείς, ανταποκρινόμενες εικονικές αναπαραστάσεις φυσικών συστημάτων, ενισχύοντας έτσι τη λειτουργική αποτελεσματικότητα και τη λήψη αποφάσεων. Αυτό καθιστά το FIWARE έναν ανεκτίμητο πόρο για κάθε οργανισμό που στοχεύει να αξιοποιήσει την τεχνολογία ψηφιακών διδύμων για τη βελτιστοποίηση της απόδοσης και των αποτελεσμάτων σε διάφορους κλάδους.

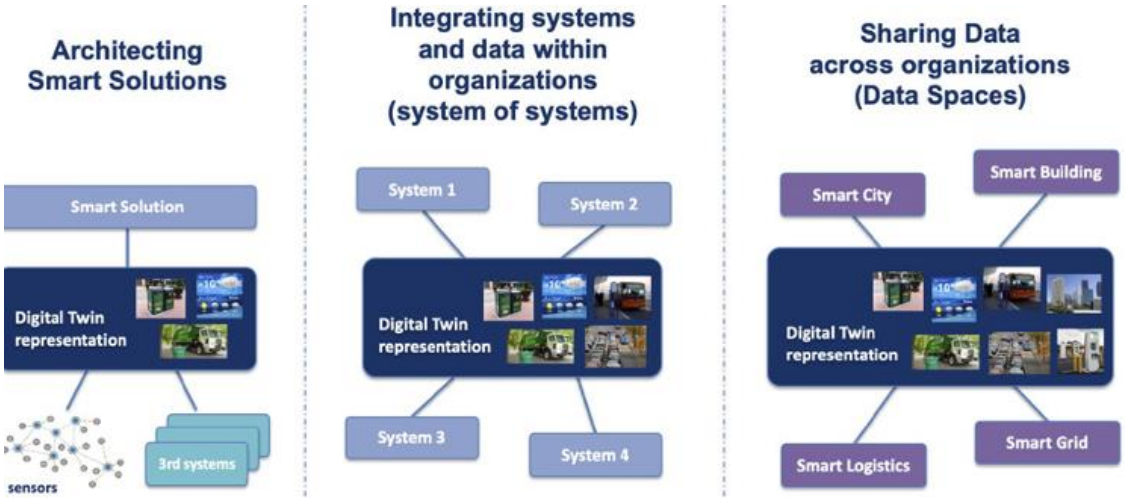

Figure 6: Levels of Integration supported by Digital Twin approach image from Position Paper of Fiware

Smart City powered by FIWARE

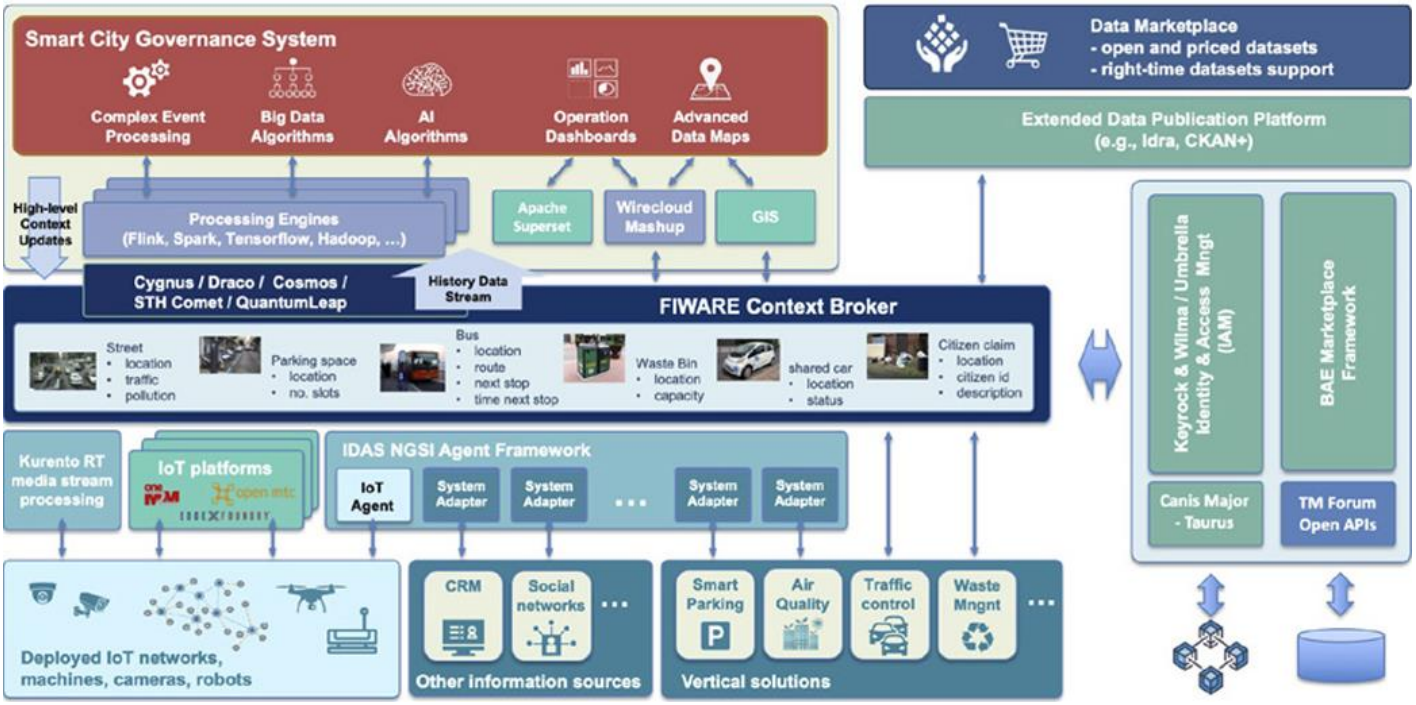

Figure 7: Example of Digital Twin Architecture from FIWARE Position Paper

Το στοιχείο Context Broker βρίσκεται στον πυρήνα της αρχιτεκτονικής, κρατώντας μια Digital Twin αναπαράσταση των πραγματικών αντικειμένων και εννοιών και περιγράφοντας τι συμβαίνει στην πόλη: δρόμους, κάδους απορριμμάτων και δοχεία, απορριμματοφόρα, λεωφορεία, φορτιστές ηλεκτρικών οχημάτων, κτίρια, εκδηλώσεις, αξιώσεις πολιτών κ.λπ. Οι διάφορες έξυπνες λύσεις που αναπτύσσονται στην πόλη (π.χ. παρακολούθηση της ποιότητας του αέρα, έξυπνη διαχείριση της κυκλοφορίας, έξυπνη στάθμευση, έξυπνη διαχείριση αποβλήτων) συνδέονται με τον environmental broker συνεισφέροντας τις πληροφορίες που διαχειρίζονται, οι οποίες είναι σχετικές με τη δημιουργία μιας ολιστικής αναπαράστασης πλαισίου / Digital Twin ολόκληρης της πόλης. Ορισμένες από αυτές τις έξυπνες λύσεις μπορεί να τροφοδοτούνται από το FIWARE (π.χ. συστήματα ελέγχου κυκλοφορίας και διαχείρισης αποβλήτων στο σχήμα), οπότε η διεπαφή τους με τον παγκόσμιο environmental broker σε επίπεδο πόλης δεν απαιτεί καμία προσαρμογή. Άλλοι μπορεί να μην τροφοδοτούνται από το FIWARE, αλλά αυτό δεν αποτελεί σημαντικό πρόβλημα, επειδή η δημιουργία προσαρμογέων συστήματος NGSI που μεταφράζονται από οποιοδήποτε API εξάγουν αυτά τα συστήματα σε NGSI-LD έχει αποδειχθεί ότι δεν είναι δύσκολη. Τελευταίος αλλά εξίσου σημαντικός, η πόλη μπορεί να αναπτύξει υποδομές αισθητήρων / καμερών μέσω των οποίων εξάγονται πολύτιμα δεδομένα. Αξιοποιώντας την πλήρη αναπαράσταση Πλαισίου / Digital Twin της πόλης, μπορεί να αναπτυχθεί το Σύστημα Διακυβέρνησης Έξυπνης Πόλης (ή Κέντρο Λειτουργίας Πόλης).

Τα εργαλεία επεξεργασίας BigData σε πραγματικό χρόνο μπορούν να χρησιμοποιηθούν βασιζόμενα σε δεδομένα που προέρχονται από πολλαπλές πηγές, εξάγοντας πιο πολύτιμες πληροφορίες για την υποστήριξη αποφάσεων. Ομοίως, τα εργαλεία παρακολούθησης μπορούν να αξιοποιήσουν αυτό το ολιστικό πλαίσιο Digital Twins αναπαράσταση της πόλης. Συμπληρώνοντας την εικόνα, η FIWARE φέρνει στοιχεία που παρέχουν τα μέσα για τον εντοπισμό συναλλαγών ψηφιακών δίδυμων δεδομένων. Αυτό παρέχει τη βάση για μια σειρά σημαντικών λειτουργιών, από τον προσδιορισμό της προέλευσης των δεδομένων έως την ελεγκτική καταγραφή ορισμένων συναλλαγών. Για εκείνους τους οργανισμούς με ισχυρές απαιτήσεις διαφάνειας και πιστοποίησης, το FIWARE φέρνει στοιχεία (π.χ. Canis Major) που διευκολύνουν την καταγραφή των αρχείων καταγραφής συναλλαγών σε διαφορετικά κατανεμημένα καθολικά / blockchains.

Η ψηφιακή δίδυμη αρχιτεκτονική της FIWARE

Η αρχιτεκτονική FIWARE Digital Twin είναι ειδικά σχεδιασμένη για να παρέχει ένα ισχυρό πλαίσιο για έξυπνη διακυβέρνηση και ολοκλήρωση της πόλης, διασφαλίζοντας την αποτελεσματική διαχείριση των αστικών περιβαλλόντων μέσω ψηφιακού μετασχηματισμού υψηλού επιπέδου. Ακολουθεί μια λεπτομερής ανάλυση κάθε στοιχείου της αρχιτεκτονικής:

1. **Σύστημα Διακυβέρνησης Έξυπνης Πόλης**
    - **Σύνθετη επεξεργασία συμβάντων**: Χρησιμοποιεί προηγμένους αλγόριθμους για την επεξεργασία και ανάλυση ροών γεγονότων από διάφορους αισθητήρες της πόλης και πηγές δεδομένων σε πραγματικό χρόνο, επιτρέποντας την άμεση ανταπόκριση σε αστικά γεγονότα και ανωμαλίες.

    - **Αλγόριθμοι Big Data**: Εφαρμόζει ισχυρές πλατφόρμες μεγάλων δεδομένων για τη διαχείριση τεράστιων ποσοτήτων δεδομένων που παράγονται από αστικές υποδομές, βελτιστοποιώντας την επεξεργασία και αποθήκευση δεδομένων.

    - **Αλγόριθμος AIs**: Ενσωματώνει τεχνητή νοημοσύνη για να ενισχύσει τις διαδικασίες λήψης αποφάσεων, να προβλέψει την αστική δυναμική και να διευκολύνει τις αυτοματοποιημένες απαντήσεις στις προκλήσεις διαχείρισης της πόλης.

- **Πίνακες εργαλείων λειτουργίας και προηγμένοι χάρτες δεδομένων**: Παρέχει ολοκληρωμένα εργαλεία οπτικοποίησης που εμφανίζουν δεδομένα και αναλύσεις σε πραγματικό χρόνο σε φιλικές προς το χρήστη διεπαφές, βοηθώντας τους διαχειριστές πόλεων να παρακολουθούν και να ελέγχουν αποτελεσματικά τις αστικές λειτουργίες.
-

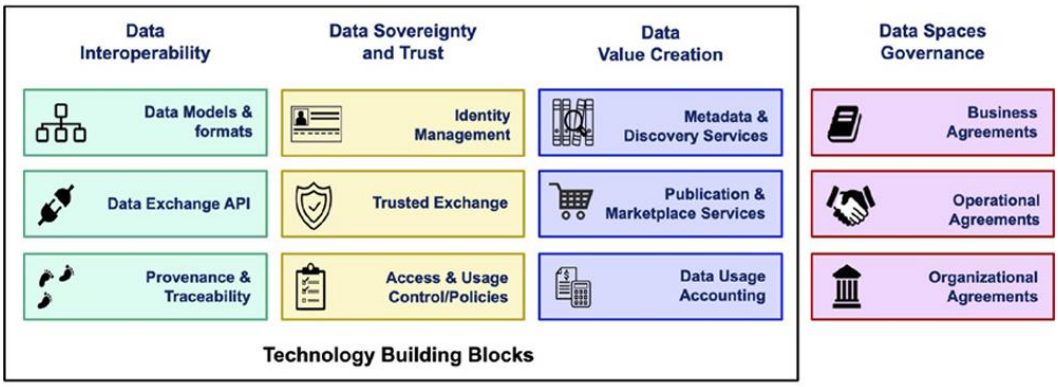

Figure 8: Data Block in Data Space from FIWARE Position Paper

2. **Μηχανές επεξεργασίας**:

- **Χρησιμοποιούμενες τεχνολογίες**: Περιλαμβάνει υπερσύγχρονες μηχανές επεξεργασίας όπως το Apache Flink για επεξεργασία ροής, το Apache Spark για επεξεργασία δεδομένων μεγάλης κλίμακας, το TensorFlow για εφαρμογές μηχανικής μάθησης και το Hadoop για χειρισμό κατανεμημένων δεδομένων.

- **Ροές δεδομένων σε πραγματικό χρόνο και ιστορικά**: Υποστηρίζει τόσο την παρακολούθηση και ανάλυση των ροών δεδομένων σε πραγματικό χρόνο, όσο και την ανασκόπηση ιστορικών δεδομένων, επιτρέποντας διαχρονικές μελέτες και άμεση δράση με βάση τις εισόδους δεδομένων σε πραγματικό χρόνο.

3. **Ενοποίηση και διαχείριση δεδομένων**:
   - **Cygnus/Draco / Κόσμος / Κομήτης STH / QuantumLeap**: Αυτά τα στοιχεία είναι αναπόσπαστα για τη διαχείριση ροών δεδομένων, όπου ο Cygnus και ο Draco λειτουργούν ως προσαρμογείς δεδομένων για ιστορικά δεδομένα, η Cosmos αποθηκεύει μεγάλα δεδομένα και η QuantumLeap χειρίζεται δεδομένα χρονοσειρών για αναλύσεις σε πραγματικό χρόνο.

- **Ενσωμάτωση IoT**: Ενσωματώνεται με πλατφόρμες IoT μέσω του IDAS NGSI Agent Framework, επιτρέποντας σε διάφορες συσκευές και αισθητήρες IoT να συνδέονται και να μεταδίδουν δεδομένα απευθείας στο κεντρικό σύστημα της πόλης.

4. **FIWARE Context Broker**:

   - **Κεντρική διαχείριση**: Λειτουργεί ως το κεντρικό νευρικό σύστημα της αρχιτεκτονικής, διαχειριζόμενο και ενορχηστρώνοντας τις αλληλεπιδράσεις μεταξύ όλων των συνδεδεμένων υπηρεσιών και του ψηφιακού δίδυμου της πόλης.

   - **Ψηφιακή δίδυμη αναπαράσταση**: Διατηρεί μια δυναμική και συνεχώς ενημερωμένη ψηφιακή αναπαράσταση της πόλης, αντανακλώντας την τρέχουσα κατάσταση και τις αλληλεπιδράσεις των φυσικών αντικειμένων και υποδομών.

5. **Κάθετες λύσεις**:
   - **Εξειδικευμένες Υπηρεσίες Πόλης**: Υλοποιεί προσαρμοσμένες εφαρμογές για διαφορετικές πτυχές της διαχείρισης της πόλης, όπως η κυκλοφορία, τα απόβλητα και η στάθμευση, οι οποίες αλληλεπιδρούν άμεσα με το Context Broker για την ενημέρωση και ανάκτηση των απαραίτητων δεδομένων.

   - **Ενσωμάτωση και επεκτασιμότητα**: Κάθε λύση έχει σχεδιαστεί για να είναι επεκτάσιμη και ολοκληρωμένη, επιτρέποντας την εύκολη προσθήκη νέων υπηρεσιών ή την επέκταση των υπαρχουσών χωρίς να διαταράσσεται το συνολικό σύστημα.

6. **Πλατφόρμα εκτεταμένης δημοσίευσης δεδομένων**:
   - **Αγορά δεδομένων**: Διαθέτει μια αγορά για την ανταλλαγή δεδομένων, διευκολύνοντας την πώληση ή την ελεύθερη ανταλλαγή συνόλων δεδομένων, ενισχύοντας τη διαθεσιμότητα και την εμπορευματοποίηση των δεδομένων.
   - **Υποστήριξη για διαφορετικές μορφές δεδομένων**: Υποστηρίζει διάφορους τύπους και πρότυπα δεδομένων, διασφαλίζοντας ευελιξία και προσβασιμότητα για τους χρήστες και τους παρόχους δεδομένων.

3.3. Συγκριτική ανάλυση

iNicosia Ψηφιακή Δίδυμη Αρχιτεκτονική

Η αρχιτεκτονική του iNicosia επικεντρώνεται κυρίως σε εφαρμογές συγκεκριμένων πόλεων, αξιοποιώντας την ενσωμάτωση δεδομένων από διάφορες τοπικές πηγές για τη διαχείριση αστικών υποδομών. Το σύστημα ενσωματώνει γεωγραφικά συστήματα πληροφοριών (GIS), διεπαφές δημόσιων δεδομένων, και τοπικές αναπτύξεις IoT. Ωστόσο, μπορεί να μην διαθέτει τις ολοκληρωμένες στρατηγικές διαχείρισης δεδομένων και την ευρύτερη επεκτασιμότητα που παρατηρείται στο FIWARE και στο TM Forum.

Ψηφιακή αρχιτεκτονική FIWARE Twin

Το FIWARE προσφέρει μια πιο γενικευμένη και κλιμακούμενη Digital Twin αρχιτεκτονική κατάλληλη για μια σειρά έξυπνων εφαρμογών, από πόλεις έως βιομηχανίες. Δίνει έμφαση στη εναλλαξιμότητα και τα open API, διασφαλίζοντας ότι διάφορα εξωτερικά συστήματα μπορούν εύκολα να ενσωματωθούν. Η δύναμη της FIWARE έγκειται στην εκτεταμένη υποστήριξή της για επεξεργασία δεδομένων σε πραγματικό χρόνο και ισχυρή διαχείριση περιβάλλοντος μέσω του Context Broker, ενισχύοντας τη λήψη αποφάσεων σε πραγματικό χρόνο σε διάφορους κλάδους.

TM Forum Ψηφιακή Δίδυμη Αρχιτεκτονική

Το TM Forum εισάγει μια εξαιρετικά εξειδικευμένη προσέγγιση προσαρμοσμένη στις τηλεπικοινωνίες, αλλά εφαρμόσιμη σε άλλους τομείς λόγω της εστίασής του στην ενσωμάτωση Digital Twin με τη Decision Intelligence (DI). Αυτή η αρχιτεκτονική υπερέχει στη λειτουργική βελτιστοποίηση και την προγνωστική ανάλυση, αξιοποιώντας εκτενώς την τεχνητή νοημοσύνη για την ενημέρωση και την αυτοματοποίηση των διαδικασιών λήψης αποφάσεων. Παρέχει ένα ισχυρό πλαίσιο για πολύπλοκα περιβάλλοντα όπου πολλές μεταβλητές επηρεάζουν τη λειτουργική δυναμική.

Κύριες Διαφορές

1. Επεκτασιμότητα και ευελιξία

Οι αρχιτεκτονικές FIWARE και TM Forum ξεχωρίζουν για την επεκτασιμότητα και την ευελιξία τους. Το μοντέλο της FIWARE είναι δομημένο γύρω από έναν ισχυρό environmental broker που διαχειρίζεται ένα ευρύ φάσμα ροών δεδομένων και

αλληλεπιδράσεων σε περιβάλλοντα έξυπνων πόλεων ή άλλα οικοσυστήματα IoT. Αυτό το πλαίσιο του επιτρέπει να ενσωματώνεται και να κλιμακώνεται απρόσκοπτα παράλληλα με μια ποικιλία έξυπνων εφαρμογών και συσκευών, προσαρμοζόμενο στα μεταβαλλόμενα φορτία δεδομένων και τις απαιτήσεις των χρηστών χωρίς σημαντική αναδιαμόρφωση.

Το TM Forum, από την άλλη πλευρά, αξιοποιεί την Open Digital Architecture (ODA) που περιλαμβάνει ένα ολοκληρωμένο σύνολο κατευθυντήριων γραμμών και προτύπων για την υποστήριξη των παρόχων ψηφιακών υπηρεσιών στη διαχείριση υπηρεσιών σε διαφορετικές πλατφόρμες. Αυτό το πλαίσιο υποστηρίζει την κλιμάκωση σε διάφορους κλάδους, επιτρέποντας την προσαρμογή και την ευελιξία στη διαχείριση υπηρεσιών, διευκολύνοντας την ευκολότερη προσαρμογή σε νέες αγορές ή μεταβαλλόμενα τεχνολογικά τοπία.

2. Προηγμένη ενσωμάτωση αναλυτικών στοιχείων και AI

Η αρχιτεκτονική του TM Forum ενσωματώνει τεχνητή νοημοσύνη για να ενισχύσει τις δυνατότητες πρόβλεψης ανάλυσης. Αυτή η ενσωμάτωση παρέχει επιχειρησιακές πληροφορίες που δεν είναι μόνο ταχύτερες αλλά και πιο ακριβείς, ενισχύοντας τις διαδικασίες λήψης αποφάσεων και τη λειτουργική αποτελεσματικότητα. Τέτοιες δυνατότητες είναι κρίσιμες σε περιβάλλοντα που απαιτούν γρήγορες απαντήσεις σε μεταβαλλόμενες συνθήκες, όπως η διαχείριση δικτύου ή οι παροχές εξυπηρέτησης πελατών.

Το FIWARE παρέχει επίσης εργαλεία για προηγμένη επεξεργασία δεδομένων σε πραγματικό χρόνο, η οποία, όταν συνδυάζεται με την ισχυρή ενσωμάτωση IoT, επιτρέπει στις πόλεις και τους οργανισμούς να αντλούν σημαντικές πληροφορίες από σύνθετα σύνολα δεδομένων. Χρησιμοποιώντας πλαίσια επεξεργασίας δεδομένων ροής όπως το Apache Flink ή το Spark, το FIWARE επιτρέπει στους χρήστες του να εκτελούν εξελιγμένες εργασίες ανάλυσης και μηχανικής μάθησης, προσφέροντας βαθιά γνώση που μπορεί να οδηγήσει σε προληπτικές αποφάσεις διαχείρισης.

3. Διαλειτουργικότητα

Η διαλειτουργικότητα αποτελεί ακρογωνιαίο λίθο τόσο των πλαισίων FIWARE όσο και TM Forum, τα οποία επικεντρώνονται στη δημιουργία οικοσυστημάτων που ευνοούν την ευρεία τεχνολογική ολοκλήρωση. Η FIWARE το επιτυγχάνει αυτό μέσω των ανοιχτών API της που επιτρέπουν την εύκολη αλληλεπίδραση με ένα πλήθος συσκευών IoT και άλλων πηγών δεδομένων, προωθώντας μια αρθρωτή προσέγγιση όπου διαφορετικά στοιχεία μπορούν να αντικατασταθούν ή να αναβαθμιστούν χωρίς να διαταραχθεί το συνολικό σύστημα. Το TM Forum παρέχει ένα παρόμοιο πλεονέκτημα μέσω του API και της αρχιτεκτονικής που βασίζεται σε συνιστώσες, η οποία όχι μόνο υποστηρίζει ψηφιακές υπηρεσίες, αλλά

διασφαλίζει επίσης ότι αυτές οι υπηρεσίες μπορούν να επικοινωνούν σε διαφορετικές πλατφόρμες και με διάφορους παρόχους δεδομένων. Αυτό το επίπεδο διαλειτουργικότητας είναι απαραίτητο για οργανισμούς που επιθυμούν να αξιοποιήσουν ένα ποικίλο σύνολο εργαλείων και συστημάτων χωρίς να είναι κλειδωμένοι σε έναν προμηθευτή ή πλατφόρμα.

Συνοψίζοντας, οι αρχιτεκτονικές FIWARE και TM Forum διαθέτουν προηγμένες δυνατότητες που τις καθιστούν ανώτερες σε σύγκριση με την αρχιτεκτονική iNicosia, κυρίως ως προς την επεκτασιμότητα, την ευελιξία, την προηγμένη ανάλυση δεδομένων και την τεχνητή νοημοσύνη, καθώς και τη διαλειτουργικότητα. Η ενσωμάτωση αυτών των χαρακτηριστικών επιτρέπει στο FIWARE και στο TM Forum να υποστηρίξουν ευρύτερες εφαρμογές σε διάφορους κλάδους και να προσφέρουν μια πιο ολοκληρωμένη και αποτελεσματική διαχείριση των ψηφιακών υπηρεσιών. Για να ενισχύσει την αρχιτεκτονική της iNicosia, συνιστάται η ενσωμάτωση πιο προηγμένων τεχνολογιών AI, η επέκταση των δυνατοτήτων διαλειτουργικότητας μέσω ανοιχτών προτύπων, καθώς και η ανάπτυξη πιο ισχυρών πλαισίων διαχείρισης δεδομένων. Αυτές οι βελτιώσεις θα καταστήσουν την iNicosia πιο ανταγωνιστική και ικανή να ανταποκριθεί στις απαιτήσεις των σύγχρονων εφαρμογών έξυπνης πόλης και πέραν αυτών.

Aspect	*iNicosia*	*FIWARE*	*TM Forum*	*INicosia Recommendations*
Core Focus	Municipal management integrating GIS, local data, and IoT devices.	Generic enablers for scalability and interoperability emphasizing real-time context-awareness.	Comprehensive business processes, especially for telecommunications, utilities, and smart cities.	Expand focus to include predictive analytics and AI for proactive urban management.
Data Processing	Basic real-time processing suited for urban management tasks.	Real-time processing with technologies like Apache Flink and Hadoop for immediate data handling.	AI integration to simulate network conditions and pre-emptively address system failures.	Incorporate dynamic data integration platforms to synthesize data from various sources, enhancing decision-making capabilities.
API and System Integration	Limited to specific urban management applications.	Extensive API support for ease of integration with existing and new technologies.	API-led connectivity with a suite of shared data models for seamless functionality across diverse platforms.	Adopt a modular architecture with extensive API support to ensure compatibility and ease of integration with new technologies.
Community and Support	Limited to local government and specific service providers.	Strong global community with rich development tools and resources.	Industry-specific solutions and tailored strategies supported by a global framework and standards.	Leverage global standards and community support to foster innovation and continuous improvement in municipal management solutions.
Security and Data Governance	Basic security measures focused on local data handling.	Emphasizes secure real-time data exchange and interoperability across smart cities.	Robust data sharing and security protocols, adhering to global standards of data privacy and security.	Implement advanced cybersecurity measures and robust data governance frameworks to safeguard user data and maintain system integrity as iNicosia scales.
Vertical Solutions and Adaptability	Primarily urban-focused without extensive industry-specific solutions.	Supports vertical smart solutions like Air Quality Monitoring, Smart Traffic, and Smart Parking connected to the Context Broker.	Specialized industry-specific solutions like Frameworx for asset management, CRM, and service delivery, highly adaptable to specific needs.	Integrate industry-specific adapters to expand reach beyond municipal management and enhance versatility in handling complex urban environments.
Predictive and AI Capabilities	Lacks advanced predictive analytics and AI integration.	Utilizes AI and machine learning to enhance city operations through real-time data insights.	Advanced AI to predict network conditions, enabling pre-emptive maintenance and operational optimizations.	Incorporate machine learning algorithms and AI capabilities to predict urban growth and infrastructure needs effectively.

Κεφάλαιο 4

4. Στρατηγικές Βελτιώσεις της Αρχιτεκτονικής του iNicosia

4.1. Συστάσεις για τροποποιήσεις ως προς την βελτίωση της ασφάλειας στο σύνολο

4.2 Συστάσεις ως προς την εφαρμογή πρακτικών ασφαλείας

4.1. Συστάσεις για τροποποιήσεις ως προς την βελτίωση της ασφάλειας στο σύνολο

1. **Ασφαλή API και προηγμένη ανίχνευση απειλών και ασφάλεια βάσει AI**:

   - **Ασφαλές πλαίσιο API:** Δημιουργήστε ένα ασφαλές πλαίσιο API υιοθετώντας τυποποιημένα πρωτόκολλα ασφαλείας του κλάδου, όπως το OAuth 2.0 και το OpenID Connect, για τη διαχείριση του ελέγχου ταυτότητας και της εξουσιοδότησης σε όλο το σύστημα. Το πλαίσιο αυτό θα πρέπει να περιλαμβάνει περιορισμό ρυθμού, κρυπτογράφηση και τακτικές αξιολογήσεις ασφάλειας για την πρόληψη καταχρήσεων API και παραβιάσεων δεδομένων.

   - **Εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) στο iNicosia**: Η μετάβαση από τον έλεγχο ταυτότητας ενός παράγοντα (SFA) στον έλεγχο ταυτότητας πολλαπλών παραγόντων είναι ζωτικής σημασίας για την ενίσχυση της ασφάλειας σε ολόκληρη την ψηφιακή υποδομή της iNicosia. Το MFA προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας από τους χρήστες να επαληθεύουν την ταυτότητά τους χρησιμοποιώντας δύο ή περισσότερα ανεξάρτητα credentials, γεγονός που μειώνει σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης και πιθανών παραβιάσεων ασφαλείας, ειδικά σε ένα εξελιγμένο περιβάλλον ψηφιακού δίδυμου όπως το iNicosia. Αυτή η εφαρμογή όχι μόνο ενισχύει τους μηχανισμούς ελέγχου πρόσβασης, αλλά ευθυγραμμίζεται επίσης με τις βέλτιστες πρακτικές για την προστασία ευαίσθητων δεδομένων και υποδομών.

   - **Συστήματα ασφαλείας με τεχνητή νοημοσύνη**: Αναπτύξτε συστήματα ασφαλείας με τεχνητή νοημοσύνη που χρησιμοποιούν αλγόριθμους μηχανικής μάθησης για να μαθαίνουν συνεχώς από την κυκλοφορία δικτύου, τη συμπεριφορά των χρηστών και την εξωτερική ευφυΐα απειλών. Αυτά τα συστήματα μπορούν να ανιχνεύσουν ανωμαλίες που αποκλίνουν από τα κανονικά πρότυπα, να εντοπίσουν πιθανές απειλές σε πραγματικό χρόνο και να ξεκινήσουν αυτοματοποιημένες απαντήσεις για τον μετριασμό των κινδύνων.

- **Προγνωστική ανάλυση**: Η ενσωμάτωση εξελιγμένων εργαλείων προγνωστικής ανάλυσης μπορεί να μετατρέψει τεράστιες ποσότητες ιστορικών δεδομένων και δεδομένων της πόλης σε πραγματικό χρόνο σε αξιοποιήσιμες πληροφορίες. Με την εφαρμογή αλγορίθμων machine learning, η iNicosia μπορεί να προβλέψει μελλοντικές συνθήκες και σενάρια, όπως η πρόβλεψη κυκλοφοριακής συμφόρησης κατά τη διάρκεια εκδηλώσεων ή η βελτιστοποίηση διαδρομών συλλογής απορριμμάτων. Αυτή η προορατική προσέγγιση θα διευκόλυνε την καλύτερη διαχείριση των πόρων και τον πολεοδομικό σχεδιασμό.

- **Επεξεργασία δεδομένων σε πραγματικό χρόνο**: Η αξιοποίηση προηγμένων πλαισίων επεξεργασίας δεδομένων θα επιτρέψει στην iNicosia να χειρίζεται αποτελεσματικά μεγάλες ροές δεδομένων σε πραγματικό χρόνο. Εργαλεία όπως το Apache Flink ή το Apache Spark μπορούν να επεξεργαστούν δεδομένα κατά την άφιξή τους, κάτι που είναι ζωτικής σημασίας για εφαρμογές όπως η διαχείριση της κυκλοφορίας σε πραγματικό χρόνο ή τα συστήματα αντιμετώπισης έκτακτης ανάγκης, διασφαλίζοντας ότι το ψηφιακό δίδυμο αντικατοπτρίζει τις τρέχουσες συνθήκες της πόλης με ακρίβεια και ταχύτητα.

- **Ανάλυση συμπεριφοράς**: Χρησιμοποιήστε αναλύσεις συμπεριφοράς για να παρακολουθείτε τις δραστηριότητες των χρηστών και να εντοπίζετε ύποπτες ενέργειες που θα μπορούσαν να υποδηλώνουν απειλή για την ασφάλεια, όπως ασυνήθιστα μοτίβα πρόσβασης ή συναλλαγές. Αυτή η προληπτική επιτήρηση βοηθά στην έγκαιρη ανίχνευση πιθανών παραβιάσεων ασφαλείας, μειώνοντας σημαντικά τον αντίκτυπό τους.

2. Ολοκληρωμένη κρυπτογράφηση δεδομένων:

- **Κρυπτογράφηση από άκρο σε άκρο**: Εφαρμογή κρυπτογράφησης end to end σε όλα τα δεδομένα κατά τη μεταφορά και την ηρεμία εντός του οικοσυστήματος ψηφιακών διδύμων. Χρησιμοποιήστε ισχυρά πρότυπα κρυπτογράφησης όπως το AES-128 ή AES-256 για να διασφαλίσετε ότι όλα τα δεδομένα, ανεξάρτητα από την κατάστασή τους, δεν είναι αναγνώσιμα από μη εξουσιοδοτημένους χρήστες.

- **Διαχείριση κλειδιών κρυπτογράφησης**: Ανάπτυξη ενός ισχυρού συστήματος διαχείρισης κλειδιών κρυπτογράφησης που αυτοματοποιεί τη δημιουργία, τη διανομή, την αποθήκευση και την ανάκληση κλειδιών κρυπτογράφησης. Το σύστημα αυτό θα πρέπει επίσης να υποστηρίζει στρατηγικές εναλλαγής κλειδιών και αρχειοθέτησης για την ενίσχυση της ασφάλειας των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής του.

3. **Τακτικοί έλεγχοι ασφαλείας και έλεγχοι συμμόρφωσης**:

- **Automated Compliance Tools**: Εφαρμογή αυτοματοποιημένων εργαλείων για τη συνεχή παρακολούθηση της συμμόρφωσης με τα πρότυπα ασφαλείας όπως το GDPR, το ISO 27001 και το NIST. Τα εργαλεία αυτά θα πρέπει να παρέχουν ειδοποιήσεις και αναφορές σε πραγματικό χρόνο σχετικά με την κατάσταση συμμόρφωσης, συμβάλλοντας στην άμεση αντιμετώπιση τυχόν αποκλίσεων ή τρωτών σημείων.

- **Δοκιμές διείσδυσης**: Προγραμματισμός τακτικών δοκιμών διείσδυσης που διενεργούνται από εξωτερικούς εμπειρογνώμονες ασφαλείας για την προσομοίωση επιθέσεων στον κυβερνοχώρο και τον εντοπισμό τρωτών σημείων στην υποδομή ψηφιακού διδύμου. Αυτή η άσκηση βοηθά στην κατανόηση των αδυναμιών του συστήματος και στη βελτίωση των μέτρων ασφαλείας για την άμυνα έναντι πραγματικών επιθέσεων.

4. **Ισχυρά σχέδια αντιμετώπισης συμβάντων και αποκατάστασης**:

- **Ομάδα Αντιμετώπισης Περιστατικών**: Δημιουργία μιας ειδικής ομάδας αντιμετώπισης περιστατικών εκπαιδευμένη στον αποτελεσματικό χειρισμό περιστατικών στον κυβερνοχώρο. Αυτή η ομάδα θα είναι υπεύθυνη για την εκτέλεση του σχεδίου αντιμετώπισης περιστατικών, τον συντονισμό των ενεργειών σε ολόκληρο τον οργανισμό και την επικοινωνία με τους ενδιαφερόμενους κατά τη διάρκεια και μετά από ένα συμβάν ασφαλείας.

- **Λύσεις αποκατάστασης καταστροφών**: Ανάπτυξη ολοκληρωμένων λύσεων αποκατάστασης καταστροφών που περιλαμβάνουν τακτικά αντίγραφα ασφαλείας, μηχανισμούς ανακατεύθυνσης και ασκήσεις αποκατάστασης καταστροφών. Αυτές οι λύσεις διασφαλίζουν ότι το ψηφιακό δίδυμο σύστημα μπορεί να ανακάμψει γρήγορα από επιθέσεις στον κυβερνοχώρο, αποτυχίες υλικού ή άλλα ενοχλητικά συμβάντα, ελαχιστοποιώντας το χρόνο διακοπής λειτουργίας και την απώλεια δεδομένων.

- **Κατανεμημένη αποθήκευση**: Κατανεμημένη αποθήκευση για τη διασπορά δεδομένων σε πολλές τοποθεσίες, μειώνοντας τους κινδύνους που σχετίζονται με την κεντρική αποθήκευση δεδομένων. Αυτή η προσέγγιση όχι μόνο ενισχύει την ασφάλεια των δεδομένων, αλλά βελτιώνει επίσης τη διαθεσιμότητα των δεδομένων και την εξισορρόπηση φόρτου σε όλο το δίκτυο.

4.2. Συστάσεις ως προς την εφαρμογή πρακτικών ασφαλείας

OAuth and OpenID Connect [2]

API Security αναφέρεται στην πρακτική πρόληψης ή μετριασμού επιθέσεων σε API. Τα API λειτουργούν ως πλαίσιο backend για εφαρμογές για κινητά και web. Ως εκ τούτου, είναι κρίσιμο να προστατεύονται τα ευαίσθητα δεδομένα που μεταφέρουν. **Open authorization** (OAuth) υπαγορεύει τον τρόπο με τον οποίο η εφαρμογή από την πλευρά του πελάτη αποκτά credentials πρόσβασης. Το OpenID Connect (OIDC) είναι ένα επίπεδο ελέγχου ταυτότητας που βρίσκεται στο OAuth και επιτρέπει στους υπολογιστές-πελάτες να ελέγχουν την ταυτότητα του τελικού χρήστη. Και τα δύο αυτά λειτουργούν για την ενίσχυση του ελέγχου ταυτότητας και της εξουσιοδότησης, περιορίζοντας τη μεταφορά πληροφοριών ώστε να περιλαμβάνει μόνο εκείνους που διαθέτουν είτε το κατάλληλο, επαληθεύσιμο διακριτικό είτε τα κατάλληλα διαπιστευτήρια αναγνώρισης.

Εφαρμογή AI Security στην αρχιτεκτονική iNicosia Digital Twin

Για να ενσωματώσουμε αποτελεσματικά ένα σύστημα ασφαλείας που λειτουργεί με AI στην αρχιτεκτονική iNicosia Digital Twin, είναι ζωτικής σημασίας να ακολουθήσουμε μια ολοκληρωμένη και δομημένη προσέγγιση. Ξεκινώντας πρέπει να αξιολογήσουμε διεξοδικά την αρχιτεκτονική του δικτύου και τις ροές δεδομένων του ψηφιακού δίδυμου. Η αξιολόγηση αυτή θα πρέπει να περιλαμβάνει όλες τις συσκευές IoT, τους αισθητήρες, τα δίκτυα επικοινωνίας και τα σημεία αποθήκευσης δεδομένων που αποτελούν το οικοσύστημα ψηφιακού διδύμου. Η κατανόηση αυτών των στοιχείων είναι απαραίτητη για τον προσδιορισμό των πιο στρατηγικών σημείων για εφαρμογή λύσεων ασφάλειας AI, όπως σημεία συγκέντρωσης δεδομένων, πύλες δικτύου ή απευθείας σε κρίσιμες συσκευές.

Μόλις δημιουργηθούν τα σημεία ενοποίησης, θα ενσωματωθούν οι λύσεις ασφάλειας που βασίζονται σε AI ικανές να διαχειριστούν την κλίμακα και την πολυπλοκότητα του δικτύου του ψηφιακού δίδυμου. Ανάλογα με την ευαισθησία των δεδομένων και την απαιτούμενη επεκτασιμότητα, αυτό μπορεί να περιλαμβάνει την επιλογή είτε λύσεων on-premise είτε επιλογών που βασίζονται στο cloud. Είναι επίσης σημαντικό να εξοπλιστεί το σύστημα με δυνατότητες παρακολούθησης σε πραγματικό χρόνο (real time monitoring) που επιτρέπουν συνεχείς ενημερώσεις στα μοντέλα ανίχνευσης απειλών, ελαχιστοποιώντας έτσι το χρόνο διακοπής λειτουργίας και διατηρώντας την ακεραιότητα των λειτουργιών του ψηφιακού δίδυμου.

Κρυπτογράφηση δεδομένων

Για να την εφαρμογή αποτελεσματικής κρυπτογράφησης από άκρο σε άκρο στην αρχιτεκτονική iNicosia Digital Twin, πρέπει να ξεκινήσουμε με την ολοκληρωμένη χαρτογράφηση της ροής δεδομένων. Αυτό περιλαμβάνει τον εντοπισμό κρίσιμων σημείων δεδομένων που χρειάζονται κρυπτογράφηση, τα οποία περιλαμβάνουν δεδομένα σε κατάσταση ηρεμίας και κατά τη μεταφορά. Βασικοί τομείς στους οποίους πρέπει να επικεντρωθούμε είναι τα δεδομένα από συσκευές IoT, έξοδοι αισθητήρων, επικοινωνίες μεταξύ μικροϋπηρεσιών, και τυχόν ανταλλαγές μεταξύ του ψηφιακού δίδυμου και των εξωτερικών συστημάτων.

Μόλις εντοπιστούν τα κρίσιμα σημεία δεδομένων, επιλέγουμε ισχυρά πρωτόκολλα κρυπτογράφησης κατάλληλα για την ασφάλεια και των δύο τύπων δεδομένων. Για δεδομένα κατά τη μεταφορά, χρησιμοποιήστε Transport Layer Security (TLS) για να κρυπτογραφήσουμε τα δεδομένα που μεταφέρονται μέσω του δικτύου και για την διασφάλιση όλων των API και τα τελικά σημεία δεδομένων χρησιμοποιούν HTTPS για ασφαλείς ανταλλαγές δεδομένων. Για δεδομένα σε κατάσταση ηρεμίας, θα εφαρμόσουμε ισχυρούς αλγόριθμους κρυπτογράφησης, όπως το AES (Advanced Encryption Standard) με μήκος κλειδιού 128 / 256 bit, για την προστασία των αποθηκευμένων δεδομένων είτε βρίσκονται σε χώρο αποθήκευσης στο cloud είτε σε τοπικές βάσεις δεδομένων.

Η διαχείριση κλειδιών διαδραματίζει κρίσιμο ρόλο στη διατήρηση της ακεραιότητας της ασφάλειας του συστήματος κρυπτογράφησης. Θα χρησιμοποιήσουμε ένα κεντρικό σύστημα διαχείρισης κλειδιών (KMS) για τον χειρισμό κλειδιών κρυπτογράφησης, διασφαλίζοντας την τακτική εναλλαγή κλειδιών και την ασφαλή απόσυρση παλαιών κλειδιών για να αποτρέψουμε τη μη εξουσιοδοτημένη αποκρυπτογράφηση δεδομένων.

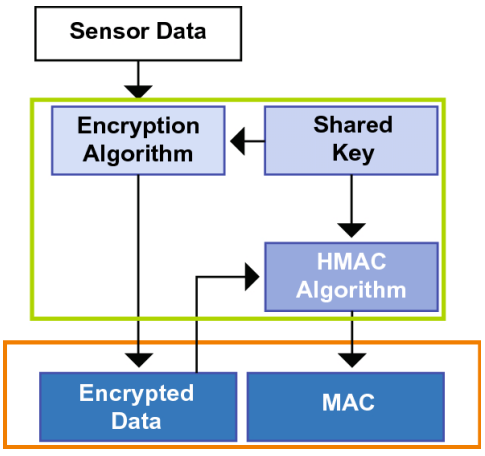

Figure 9: Αναπαράσταση Ασφάλειας Δεδομένων

Ταυτοποιηση πολλαπλων παραγόντων (MFA)

Σε αυτό το έγγραφο, παρουσιάζουμε εν συντομία διάφορα πρωτόκολλα ελέγχου ταυτότητας κλειδιών που ενισχύουν την ασφάλεια του δικτύου με διάφορα μέσα, με λεπτομερή ανασκόπηση και σύγκριση που θα ακολουθήσει αργότερα. Το Kerberos χρησιμοποιεί κρυπτογραφημένα δελτία για να επιτρέψει τον ασφαλή αμοιβαίο έλεγχο ταυτότητας μεταξύ κόμβων σε ένα μη ασφαλές δίκτυο, αποτρέποντας αποτελεσματικά την εξαπάτηση και μειώνοντας τον κίνδυνο επιθέσεων επανάληψης. Το Extensible Authentication Protocol (EAP) παρέχει ένα ευέλικτο πλαίσιο που υποστηρίζει πολλαπλούς μηχανισμούς ελέγχου ταυτότητας για δίκτυα, που χρησιμοποιούνται συνήθως για την ασφάλεια ασύρματων δικτύων και συνδέσεων από σημείο σε σημείο, προσαρμόζοντας διάφορους τύπους ελέγχου ταυτότητας, όπως κωδικούς πρόσβασης, ψηφιακά πιστοποιητικά ή βιομετρική επικύρωση. Το πρωτόκολλο IEEE 802.1X προσφέρει ισχυρό έλεγχο πρόσβασης βάσει ταυτότητας για συσκευές που προσπαθούν να συνδεθούν σε δίκτυα LAN ή WLAN, χρησιμοποιώντας ένα κεντρικό σημείο ελέγχου ταυτότητας για την ασφαλή διαχείριση της πρόσβασης στο δίκτυο, κάτι που είναι ιδιαίτερα επωφελές σε εταιρικές ρυθμίσεις. Η υπηρεσία χρήστη με κλήση σύνδεσης απομακρυσμένου ελέγχου ταυτότητας (RADIUS) χρησιμοποιείται εκτενώς για έλεγχο ταυτότητας χρήστη και εκχώρηση δικαιωμάτων πρόσβασης σε δίκτυα, υποστηρίζοντας ένα ευρύ φάσμα επιλογών ελέγχου ταυτότητας και κεντρική διαχείριση ταυτότητας για απομακρυσμένους χρήστες. Τέλος, το Terminal Access Controller Access-Control System (TACACS) παρέχει λεπτομερή έλεγχο του ελέγχου ταυτότητας, της εξουσιοδότησης και της λογιστικής για διακομιστές πρόσβασης δικτύου και άλλες δικτυωμένες συσκευές, με την πιο ασφαλή και ευέλικτη εξέλιξή του, το TACACS+, προσφέροντας βελτιωμένα χαρακτηριστικά ασφαλείας. Μια πιο λεπτομερής ανασκόπηση και σύγκριση αυτών των πρωτοκόλλων θα παρουσιαστεί αργότερα στο έγγραφο για να παρέχει βαθύτερες πληροφορίες σχετικά με τις λειτουργίες και τις εφαρμογές τους στην ασφάλεια δικτύου.

Σχέδια αντιμετώπισης συμβάντων και αποκατάστασης

Ομάδα Αντιμετώπισης Περιστατικών

Η δημιουργία μιας εξειδικευμένης ομάδας αντιμετώπισης περιστατικών είναι απαραίτητη για την αποτελεσματική διαχείριση και επίλυση περιστατικών κυβερνοασφάλειας εντός ενός οργανισμού. Αυτή η ομάδα διαδραματίζει κρίσιμο ρόλο και πρέπει να είναι καλά εκπαιδευμένη και πλήρως εξοπλισμένη για να χειριστεί την πολυπλοκότητα των απειλών

στον κυβερνοχώρο. Τα μέλη της ομάδας θα πρέπει να λαμβάνουν συνεχή εκπαίδευση στην αναγνώριση απειλών στον κυβερνοχώρο, την εκτέλεση στρατηγικών αντιμετώπισης περιστατικών και την εφαρμογή διαδικασιών αποκατάστασης για τον μετριασμό των ζημιών.

Η επικοινωνία αποτελεί σημαντικό κομμάτι της αποτελεσματικής διαχείρισης συμβάντων. Θα πρέπει να θεσπιστούν πρωτόκολλα για αποτελεσματική ενδοοργανωτική επικοινωνία κατά τη διάρκεια ενός συμβάντος, διασφαλίζοντας ότι όλα τα σχετικά μέρη ενημερώνονται και εμπλέκονται ανάλογα με τις ανάγκες. Επιπλέον, πρέπει να υπάρχουν διαδικασίες για την εξωτερική επικοινωνία με τα ενδιαφερόμενα μέρη, τις αρχές επιβολής του νόμου και, ενδεχομένως, το κοινό, για τη διαχείριση της κατάστασης με διαφάνεια και επαγγελματισμό.

Για να διασφαλιστεί η ετοιμότητα, η ομάδα αντιμετώπισης συμβάντων θα πρέπει να συμμετέχει τακτικά σε ασκήσεις προσομοίωσης. Αυτές οι ασκήσεις είναι χρήσιμες για τη δοκιμή της πρακτικής εφαρμογής του σχεδίου αντιμετώπισης περιστατικών και παρέχουν την ευκαιρία για τη βελτίωση των στρατηγικών και των απαντήσεων βάσει ρεαλιστικών σεναρίων. Αυτή η τακτική πρακτική βοηθά την ομάδα να αντιδρά γρήγορα και αποτελεσματικά, μειώνοντας σημαντικά τις πιθανές επιπτώσεις στον οργανισμό κατά τη διάρκεια πραγματικών περιστατικών στον κυβερνοχώρο.

Λύσεις αποκατάστασης καταστροφών

Η ανάπτυξη ολοκληρωμένων λύσεων αποκατάστασης καταστροφών είναι πάρα πολύ σημαντικά για να διασφαλιστεί ότι ένας οργανισμός μπορεί να ανακάμψει αμέσως από κυβερνοεπιθέσεις, αποτυχίες υλικού ή άλλα συμβάντα που προκαλούν αναστάτωση. Αυτές οι λύσεις είναι θεμελιώδεις για την ανθεκτικότητα και τη λειτουργική συνέχεια ενός οργανισμού.

Ένα από τα βασικά συστατικά της αποτελεσματικής αποκατάστασης καταστροφών είναι η εφαρμογή αυτοματοποιημένων και τακτικών διαδικασιών δημιουργίας αντιγράφων ασφαλείας. Είναι σημαντικό να συμπεριλάβετε όλα τα κρίσιμα δεδομένα σε αυτά τα αντίγραφα ασφαλείας και να διασφαλίσετε ότι αποθηκεύονται τόσο σε επιτόπιες όσο και σε μη επιτόπιες τοποθεσίες. Αυτή η στρατηγική αποθήκευσης διπλής τοποθεσίας προστατεύει από την απώλεια δεδομένων σε περίπτωση φυσικής καταστροφής ή βλάβης συγκεκριμένης τοποθεσίας.

Για να διασφαλιστεί ότι αυτά τα συστήματα λειτουργούν όπως αναμένεται υπό πίεση, είναι σημαντικό να διεξάγονται τακτικά προγραμματισμένες ασκήσεις αποκατάστασης καταστροφών. Αυτές οι ασκήσεις δοκιμάζουν την αποτελεσματικότητα των σχεδίων αποκατάστασης και την επιχειρησιακή ικανότητα γρήγορης αποκατάστασης συστημάτων και δεδομένων από αντίγραφα ασφαλείας. Οι ασκήσεις αυτές όχι μόνο επισημαίνουν πιθανές αδυναμίες στα σχέδια ανάκαμψης, αλλά βοηθούν επίσης στην κατάρτιση του προσωπικού ώστε να ανταποκρίνεται αποτελεσματικά.

Κατανεμημένη αποθήκευση

Η υλοποίηση κατανεμημένης αποθήκευσης αποτελεί μια κρίσιμη στρατηγική για την ενίσχυση της ασφάλειας και διαθεσιμότητας των δεδομένων, μειώνοντας τους κινδύνους που συνδέονται με την κεντρική αποθήκευση. Η διασπορά των δεδομένων σε πολλαπλές γεωγραφικές τοποθεσίες βοηθά στην αντιμετώπιση προβλημάτων όπως οι τοπικές αποτυχίες υλικού, οι φυσικές καταστροφές ή οι στοχευμένες κυβερνοεπιθέσεις. Η χρήση κρυπτογράφησης τόσο για τα δεδομένα που βρίσκονται σε αδράνεια όσο και για εκείνα σε μεταφορά ενισχύει την ασφάλεια σε όλο το κατανεμημένο δίκτυο. Η εφαρμογή της κατανεμημένης αποθήκευσης επιτρέπει επίσης την ισορροπία φόρτου στο δίκτυο, βελτιώνοντας την απόδοση του συστήματος και μειώνοντας τα σημεία συμφόρησης. Τέλος, η αποτελεσματική διαχείριση της αναπαραγωγής δεδομένων εξασφαλίζει ότι σε περίπτωση αποτυχίας ενός κόμβου, τα δεδομένα παραμένουν προσβάσιμα από άλλους κόμβους χωρίς σημαντική καθυστέρηση, διασφαλίζοντας τη συνεχή διαθεσιμότητα και πρόσβαση.

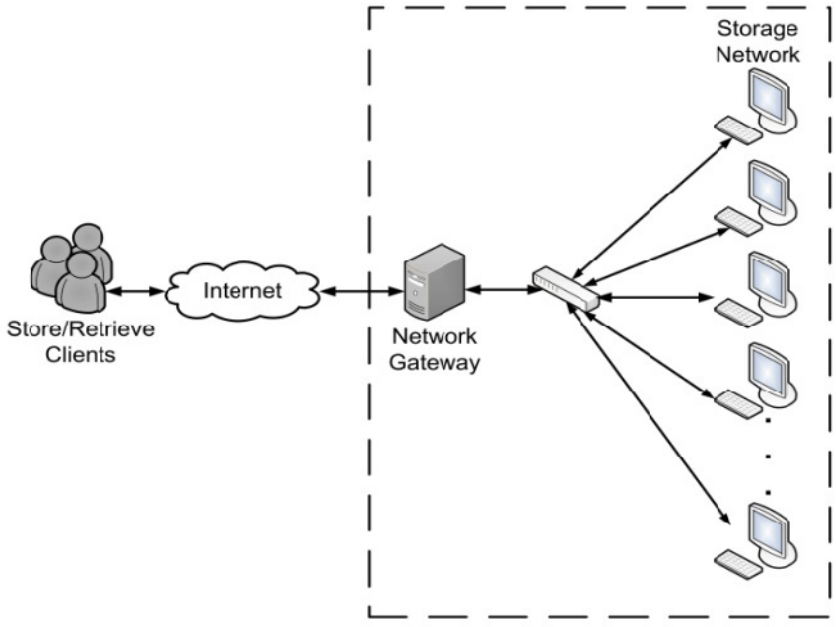

Figure 10: Example of Distributed Storage

Κεφάλαιο 5

5. Ανάλυση ασφάλειας

5.1. Ζητήματα ελέγχου ταυτότητας χρήστη

5.2. Σύγκριση και πρόταση λύσης

5.3. Δοκιμές διείσδυσης σε ιστότοπους με μεθόδους PortSwigger

---

5.1. Ζητήματα ελέγχου ταυτότητας χρήστη

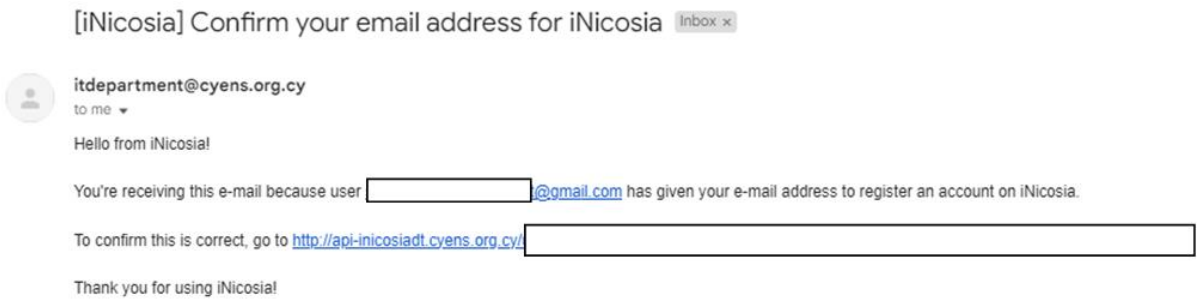

Figure 11: Example of Email Confirmation Request from iNicosia Platform

Στην περίπτωση του iNicosia, η πλατφόρμα digital twin χρησιμοποιεί κυρίως Single Factor Authentication (SFA) για συνδέσεις χρηστών μετά την αρχική ρύθμιση λογαριασμού. Το SFA, το οποίο συνήθως περιλαμβάνει μόνο έναν κωδικό πρόσβασης, είναι μια απλή μέθοδος ελέγχου ταυτότητας που ευνοείται για την απλότητα και την ταχύτητά της, η οποία μπορεί να βελτιώσει σημαντικά την εμπειρία του χρήστη ελαχιστοποιώντας τον χρόνο σύνδεσης και την πολυπλοκότητα. Αυτή η ευκολία πρόσβασης είναι ιδιαίτερα επωφελής για τις πλατφόρμες που στοχεύουν στην ενθάρρυνση της ευρείας συμμετοχής των χρηστών και της προσβασιμότητας.

Ωστόσο, η εξάρτηση από το SFA εγείρει ορισμένες ανησυχίες για την ασφάλεια, ιδίως δεδομένης της ευαισθησίας και του εύρους των δεδομένων που διαχειρίζεται η iNicosia. Μόνο οι κωδικοί πρόσβασης θεωρούνται όλο και περισσότερο ευάλωτοι σε μια ποικιλία απειλών στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων Brute Force, credential stuffing and phishing schemes.. Οι πιθανές συνέπειες της παραβίασης της ασφάλειας είναι

σημαντικές στο πλαίσιο μιας Digital Twin platform, όπου η μη εξουσιοδοτημένη πρόσβαση θα μπορούσε να οδηγήσει σε χειραγώγηση ή κλοπή κρίσιμων δεδομένων πολεοδομικού σχεδιασμού, κατάχρηση προσωπικών πληροφοριών και ευρύτερη υπονόμευση της εμπιστοσύνης των χρηστών και της ακεραιότητας της πλατφόρμας. Τέτοια κενά ασφαλείας θα μπορούσαν όχι μόνο να θέσουν σε κίνδυνο μεμονωμένα δεδομένα χρηστών, αλλά θα μπορούσαν επίσης να επηρεάσουν την ευρύτερη κοινότητα, επηρεάζοντας την ακρίβεια και την αξιοπιστία των αστικών μοντέλων και προσομοιώσεων που παρέχει το iNicosia.

Για να μετριαστούν αυτοί οι κίνδυνοι, είναι επιτακτική ανάγκη για πλατφόρμες όπως το iNicosia να εξετάσουν το ενδεχόμενο ενσωμάτωσης πρόσθετων επιπέδων ασφάλειας. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA), που περιλαμβάνει έναν συνδυασμό κάτι που γνωρίζει ο χρήστης (κωδικός πρόσβασης), κάτι που έχει ο χρήστης (διακριτικό ασφαλείας ή κινητή συσκευή) και κάτι που είναι ο χρήστης (biometric authentication), αντιπροσωπεύει μια πιο ασφαλή εναλλακτική λύση στο SFA. Η εφαρμογή MFA θα μπορούσε να μειώσει σημαντικά την πιθανότητα μη εξουσιοδοτημένης πρόσβασης, ενισχύοντας τη συνολική ασφάλεια της πλατφόρμας, διατηρώντας παράλληλα την εμπιστοσύνη των χρηστών. Ενώ αυτό μπορεί να προσθέσει ένα βήμα στη διαδικασία σύνδεσης, ο συμβιβασμός για αυξημένη ασφάλεια μπορεί να αξίζει τη μικρή ταλαιπωρία, ειδικά για τη διασφάλιση δεδομένων υψηλού ρίσκου σε πολεοδομικά πλαίσια. Στη συνέχεια θα αναφερθουν οι περισσοτεροι τυποι επαληθευσης όπως το Two – Factor Authentication (2FA), Three – Factor Authentication (3FA), Four-factor authentication (4FA) όπως και άλλοι τρόποι.

5.2. Σύγκριση και πρόταση λύσης

Οι πολιτικές ελέγχου ταυτότητας χρήστη (User Authentication) είναι απαραίτητοι μηχανισμοί για την επαλήθευση της ταυτότητας κάποιου, διασφαλίζοντας ότι τα άτομα που έχουν πρόσβαση σε υπηρεσίες και εφαρμογές είναι πράγματι αυτά που ισχυρίζονται ότι είναι. Ο βασικός σκοπός του ελέγχου ταυτότητας είναι να επιβεβαιώσει την ταυτότητα του χρήστη και, στη συνέχεια, να χρησιμοποιήσει αυτήν την επαληθευμένη ταυτότητα για να εκχωρήσει κατάλληλα δικαιώματα πρόσβασης στο δίκτυο ενός οργανισμού. Το σύστημα αυτό αποτελεί αναπόσπαστο μέρος της διατήρησης της ασφάλειας τόσο των φυσικών όσο και των ολοένα και περισσότερο ψηφιακών πόρων.

Τύποι ελέγχου ταυτότητας χρήστη

- **Έλεγχος ταυτότητας ενός παράγοντα (SFA)**: Αυτή η μέθοδος εξαρτάται από ένα μόνο παράγοντα – συνήθως έναν κωδικό πρόσβασης – για την επιβεβαίωση της ταυτότητας του χρήστη. Αν και είναι η πιο απλή και γρήγορη μέθοδος ελέγχου ταυτότητας, τείνει να είναι λιγότερο ασφαλής σε σύγκριση με τις πολυπαραγοντικές μεθόδους επειδή εξαρτάται από ένα μόνο στοιχείο που μπορεί να κλαπεί ή να μαντευτεί εύκολα.
- **Έλεγχος ταυτότητας δύο παραγόντων (2FA)**: Αυτή η μέθοδος προσθέτει ένα δεύτερο επίπεδο ασφάλειας στην τυπική διαδικασία σύνδεσης, απαιτώντας δύο ξεχωριστούς παράγοντες ελέγχου ταυτότητας, γεγονός που μειώνει σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης.
- **Έλεγχος ταυτότητας τριών παραγόντων (3FA)**: Αυτό ενσωματώνει ένα τρίτο επίπεδο, συνήθως έναν βιομετρικό παράγοντα, προσθέτοντας ένα σημαντικό επίπεδο ασφάλειας συνδυάζοντας κάτι που γνωρίζετε (κωδικός πρόσβασης), κάτι που έχετε (κινητή συσκευή ή διακριτικό), και κάτι που είστε (βιομετρική επαλήθευση).
- **Έλεγχος ταυτότητας τεσσάρων παραγόντων (4FA)**: Αυτή η μέθοδος περιλαμβάνει γνώση (κωδικός πρόσβασης), κατοχή (διακριτικό), εγγενής (βιομετρική), και επαλήθευση τοποθεσίας, προσφέροντας το υψηλότερο επίπεδο ασφάλειας απαιτώντας τέσσερις ξεχωριστές μορφές επαλήθευσης.

Όλοι αυτοί οι τύποι ελέγχου ταυτότητας ανήκουν στην κατηγορία του Multi-Factor Authentication (MFA), εξαιρουμένης της μεθόδου SFA, η οποία χρησιμοποιείται για βασική πρόσβαση και προσφέρει μια βασική στρώση ασφαλείας

	1st or Type 1 Factor	2nd or Type 2 Factor	3rd or Type 3 Factor
Also known as	*Knowledge* factor	*Possession* factor	*Inherence* factor
Is about	"What you *know*"	"What you *have*"	"What you *are*"
Examples of authentication techniques	Password, passphrase, PIN, lock combination, security questions	OTP, hardware/software token, smart card, key, ID card	Fingerprints, face topography, retina pattern, iris pattern, typing rhythm

Figure 12: Overview of Authentication Factors and Techniques

Πρωτόκολλα ελέγχου ταυτότητας

- **Kerberos**: Το πρωτόκολλο Kerberos είναι μία σταθερή τεχνολογία που βασίζεται στη χρήση εισιτηρίων (tickets) για να επιτρέψει ασφαλή αμοιβαία ταυτοποίηση μεταξύ κόμβων σε ένα μη ασφαλές δίκτυο. Κάθε εισιτήριο είναι κρυπτογραφημένο και περιέχει τα διαπιστευτήρια του χρήστη, παρέχοντας μια ασφαλή μέθοδο για την αποφυγή εξαπάτησης και τη μείωση της απειλής των επιθέσεων replay.
- **Extensible Authentication Protocol (EAP)**: Το EAP είναι ένα πλαίσιο που υποστηρίζει πολλαπλούς μηχανισμούς ταυτοποίησης για δίκτυα. Χρησιμοποιείται συχνά για την ασφάλεια των ασύρματων δικτύων και των συνδέσεων point-to-point, παρέχοντας ένα ευέλικτο σύστημα που μπορεί να προσαρμόζεται για να υποστηρίξει διάφορους τύπους ταυτοποίησης, όπως κωδικούς πρόσβασης, ταυτότητες ψηφιακών πιστοποιητικών ή άλλες μορφές βιομετρικής ταυτοποίησης.
- **IEEE 802.1X**: Αυτό το πρωτόκολλο παρέχει έλεγχο πρόσβασης βασισμένος σε έλεγχο ταυτότητας για συσκευές που επιθυμούν να συνδεθούν σε LAN ή WLAN. Χρησιμοποιεί ένα κεντρικό σημείο αυθεντικοποίησης για να επιτρέψει ή να απαγορεύσει την πρόσβαση στο δίκτυο, αυξάνοντας την ασφάλεια σε εταιρικά περιβάλλοντα.
- **Remote Authentication Dial-In User Service (RADIUS)**: Χρησιμοποιείται ευρέως για την ταυτοποίηση και άδεια πρόσβασης χρηστών σε δίκτυα, το RADIUS υποστηρίζει μια ευρεία ποικιλία επιλογών ταυτοποίησης και παρέχει κεντρική διαχείριση ταυτοτήτων για απομακρυσμένους χρήστες.
- **Terminal Access Controller Access-Control System (TACACS)**: Προσφέρει πιο λεπτομερή έλεγχο ταυτοποίησης, εξουσιοδότησης και λογοδοσίας για διακομιστές πρόσβασης δικτύου και άλλες δικτυωμένες συσκευές. Η εκδοχή TACACS+, μια εξέλιξη του αρχικού πρωτοκόλλου, προσφέρει υψηλότερα επίπεδα ασφαλείας και ευελιξίας.

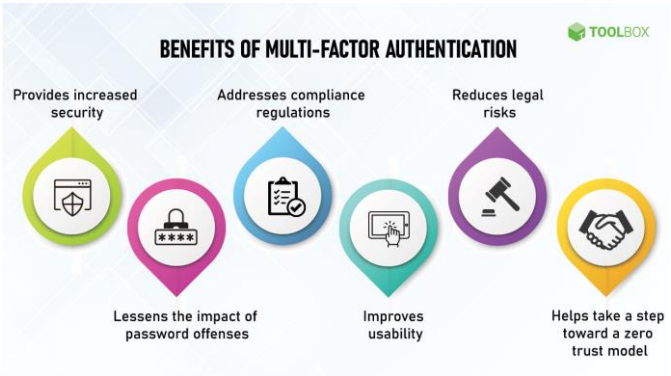

Figure 13: Benefits of MFA image from TOOLBOX

Πίνακας Πρωτοκόλλων Ελέγχου Ταυτότητας

Attribute	Kerberos	EAP	IEEE 802.1X	RADIUS	TACACS	MFA Methods	iNicosia Authentication
Functionality	Uses tickets for secure mutual authentication over an insecure network	Framework supporting multiple authentication mechanisms	Authentication mechanism for LAN/WLAN access control	Manages remote access with AAA services	Provides detailed authentication, authorization, and accounting	Requires multiple verification factors for access.	Uses email for initial setup; password-only for subsequent logins.
Security Features	Strong mutual authentication; reduces replay attack risks with time-stamped tickets	Flexible; can integrate with MFA for enhanced security	Controls network access based on device authentication	Supports various authentication methods; integrates with network equipment	Separates authentication and authorization for granular control	Significantly enhances security by requiring multiple identity proofs	Email verification adds initial security layer; subsequent security minimal
Typical Use Case	Used in secure internal networks like corporate intranets	Common in wireless networks and point-to-point connections	Used in environments like campuses or corporate buildings for network access control	Widely used for network access and VPN connections	Used in environments with complex security needs	Broadly used across online and offline platforms to protect sensitive data	Suitable where ease of access is prioritized; low-risk environments
Ease of Use	Moderately complex; requires setup of a ticketing system	Varies with chosen method; potentially complex setup	Requires network configuration for access control	Requires setup and maintenance of a centralized server	Complex; requires configuration of AAA protocols	Can be complex but increasingly user-friendly with new technologies	Simple post-setup but minimal security for access control
Integration and Flexibility	Integrates well in secure environments needing mutual authentication	Highly adaptable with support for various authentication types	Integrates with existing network infrastructure for access control	Compatible with standard network equipment for flexible AAA management	High flexibility with granular security controls	Integrates with various user devices and systems for robust security	Limited to email verification; lacks integration with robust security measures

Προτεινόμενες Λύσεις και Σύγκριση

Κατά τη σύγκριση των επιπέδων ασφαλείας διαφόρων μεθόδων ελέγχου ταυτότητας, τα πρωτόκολλα δικτύου όπως το Kerberos και το TACACS ξεχωρίζουν για τα ισχυρά χαρακτηριστικά ασφαλείας τους, καθιστώντας τα ιδανικά για την προστασία ευαίσθητων λειτουργιών δικτύου. Από την άλλη, ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) ενισχύει σημαντικά την ασφάλεια για τους λογαριασμούς χρηστών, απαιτώντας πολλαπλές αποδείξεις ταυτότητας, γεγονός που ελαχιστοποιεί σημαντικά την πιθανότητα μη εξουσιοδοτημένης πρόσβασης. Αυτό έρχεται σε πλήρη αντίθεση με απλούστερες μεθόδους ενός παράγοντα, όπως αυτές που χρησιμοποιούνται από την iNicosia, οι οποίες βασίζονται κυρίως σε ένα μόνο επίπεδο ασφάλειας μετά από μια αρχική επαλήθευση email.

Όσον αφορά την ευελιξία και την ενσωμάτωση, πρωτόκολλα όπως το Extensible Authentication Protocol (EAP) και το IEEE 802.1X δείχνουν μεγάλη προσαρμοστικότητα. Έχουν σχεδιαστεί για να λειτουργούν καλά με άλλα πλαίσια ασφαλείας, συμπεριλαμβανομένου του MFA, επιτρέποντάς τους να ενσωματώνονται απρόσκοπτα σε μια ποικιλία περιβαλλόντων δικτύου. Αυτή η προσαρμοστικότητα είναι ζωτικής σημασίας για οργανισμούς που επιθυμούν να διατηρήσουν ισχυρά πρότυπα ασφαλείας σε διαφορετικά συστήματα. Αντίθετα, η μέθοδος ελέγχου ταυτότητας που χρησιμοποιεί η iNicosia, η οποία εξαρτάται κυρίως από τους κωδικούς πρόσβασης μετά από μια αρχική επαλήθευση ηλεκτρονικού ταχυδρομείου, δεν προσφέρει το ίδιο επίπεδο ευελιξίας ή τα ολοκληρωμένα οφέλη ασφάλειας που συνοδεύουν την ενσωμάτωση πρόσθετων παραγόντων ελέγχου ταυτότητας.

Όσον αφορά την ευκολία χρήσης, οι μέθοδοι ελέγχου ταυτότητας ενός παράγοντα, οι οποίες συνήθως περιλαμβάνουν μόνο έναν κωδικό πρόσβασης, είναι γενικά απλούστερες για τους τελικούς χρήστες, αλλά προσφέρουν λιγότερη ασφάλεια. Το MFA, αν και εγγενώς πιο περίπλοκο λόγω της συμμετοχής πολλαπλών επιπέδων ελέγχου ταυτότητας, εξελίσσεται για να γίνει πιο φιλικό προς το χρήστη. Χάρη στις τεχνολογικές εξελίξεις σε τομείς όπως τα biometrics και η ενσωμάτωση κινητών συσκευών, το MFA είναι όλο και πιο προσβάσιμο και πρακτικό, ακόμη και για όσους μπορεί να μην είναι εξοικειωμένοι με την τεχνολογία. Αυτή η ισορροπία ενισχυμένης ασφάλειας χωρίς σημαντικό συμβιβασμό στην εμπειρία χρήστη καθιστά το MFA μια όλο και πιο προτιμώμενη επιλογή στα σύγχρονα ψηφιακά περιβάλλοντα.

5.3. Δοκιμές διείσδυσης σε ιστότοπους με μεθόδους PortSwigger

- **SQL injection[2]**

Τι είναι το SQL Injection (SQLi);

SQL injection (SQLi) είναι ένα web security vulnerability που επιτρέπει σε έναν εισβολέα να παρεμβαίνει στα queries που κάνει μια εφαρμογή στη βάση δεδομένων της. Αυτό μπορεί να επιτρέψει σε έναν εισβολέα να προβάλει δεδομένα που κανονικά δεν είναι σε θέση να ανακτήσει. Αυτό μπορεί να περιλαμβάνει δεδομένα που ανήκουν σε άλλους χρήστες ή οποιαδήποτε άλλα δεδομένα στα οποία μπορεί να έχει πρόσβαση η εφαρμογή. Σε πολλές περιπτώσεις, ένας εισβολέας μπορεί να τροποποιήσει ή να διαγράψει αυτά τα δεδομένα, προκαλώντας μόνιμες αλλαγές στο περιεχόμενο ή τη συμπεριφορά της εφαρμογής. Σε ορισμένες περιπτώσεις, ένας εισβολέας μπορεί να κλιμακώσει μια επίθεση SQL injection για να θέσει σε κίνδυνο τον υποκείμενο διακομιστή ή άλλη υποδομή υποστήριξης. Μπορεί επίσης να τους επιτρέψει να εκτελούν επιθέσεις άρνησης υπηρεσίας.

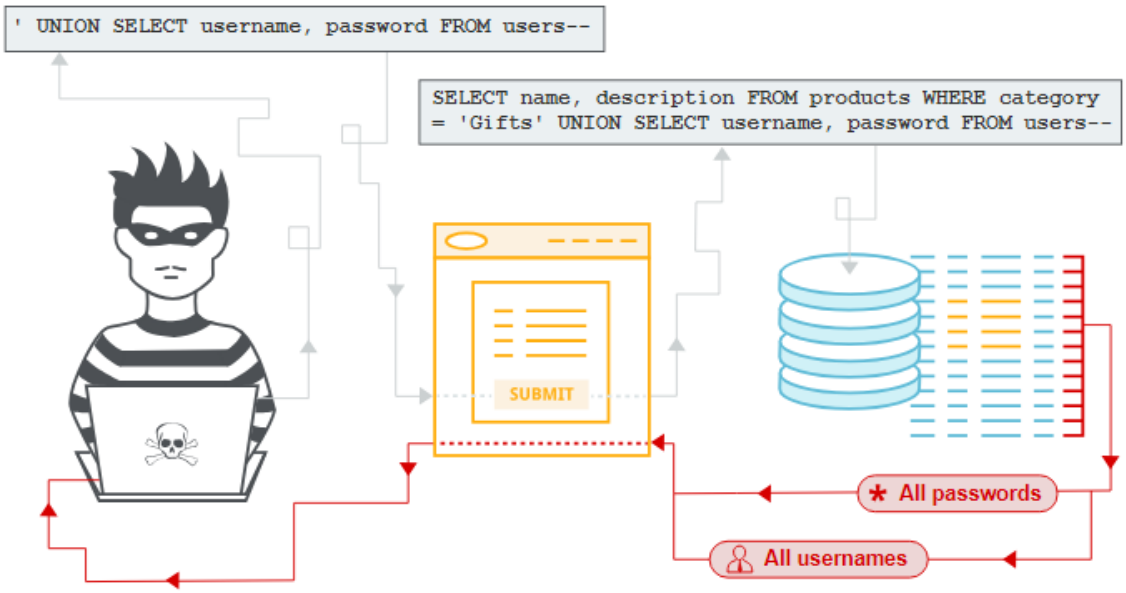

Figure 14: Representation of SQL Injection image from PortSwigger

Ποιος είναι το αντίκτυπο μιας επιτυχημένης επίθεσης SQL injection;

Μια επιτυχημένη επίθεση SQL injection μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα, όπως:

1. Κωδικούς πρόσβασης.
2. Στοιχεία πιστωτικής κάρτας.
3. Προσωπικές πληροφορίες χρήστη.

Οι επιθέσεις SQL injection έχουν χρησιμοποιηθεί σε πολλές παραβιάσεις δεδομένων υψηλού προφίλ όλα αυτά τα χρόνια. Αυτά έχουν προκαλέσει ζημιά στη φήμη και ρυθμιστικά πρόστιμα. Σε ορισμένες περιπτώσεις, ένας εισβολέας μπορεί να αποκτήσει μια persistent backdoor στα συστήματα ενός οργανισμού, οδηγώντας σε μια μακροπρόθεσμη παραβίαση που μπορεί να περάσει απαρατήρητη για μεγάλο χρονικό διάστημα.

Μέθοδοι Penetration Testing για SQL Injection

1. **Identifying Injection Points:** Εντοπίσαμε πιθανά πεδία εισαγωγής στην πλατφόρμα iNicosia που θα μπορούσαν να αλληλοεπιδράσουν με τη βάση δεδομένων, όπως γραμμές αναζήτησης και log in forms. Όλες οι δοκιμές διενεργήθηκαν για να εξακριβωθούν τα τρωτά σημεία, ωστόσο, όπως αναμενόταν, δεν αποκαλύφθηκαν άμεσες παρατυπίες, γεγονός που υποδηλώνει ισχυρές πρακτικές επικύρωσης εισροών.

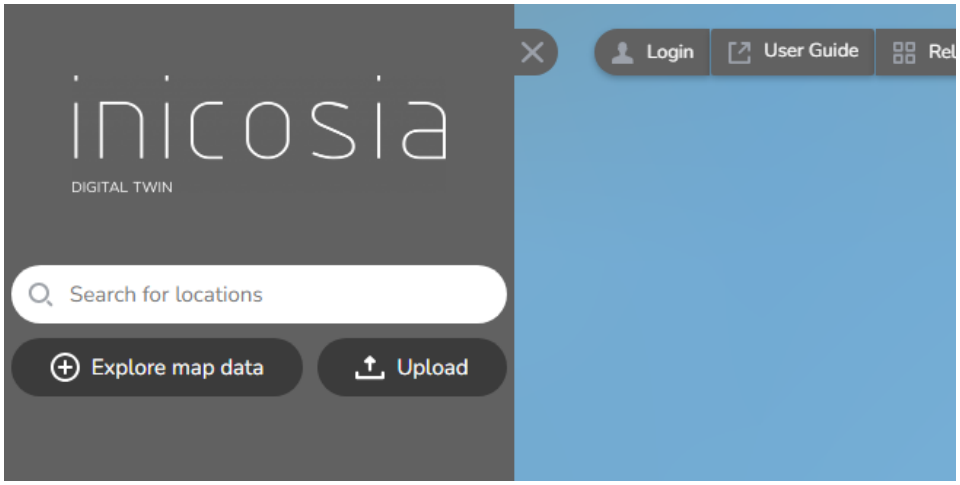

Figure 15: User Interaction Interface image iNicosia Digital Twin Platform

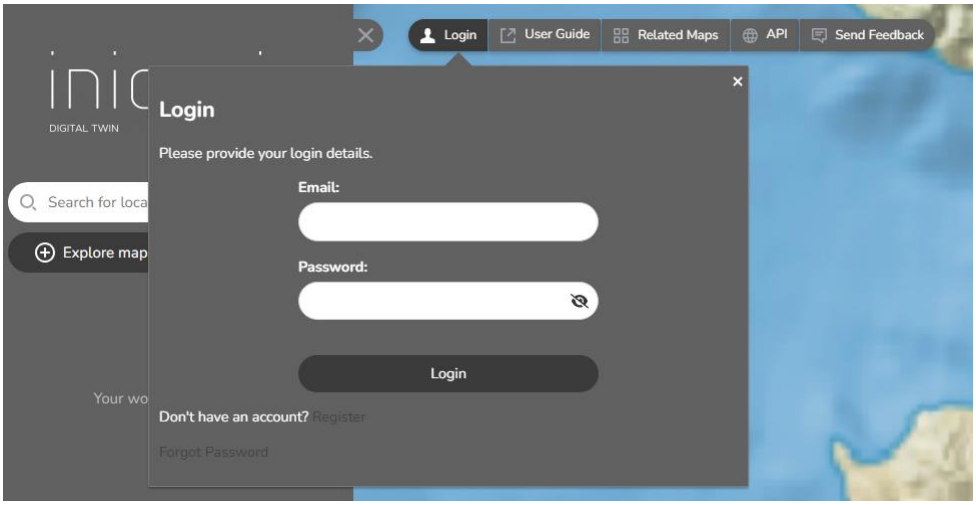

Figure 16: User Log In Interface image iNicosia Digital Twin Platform

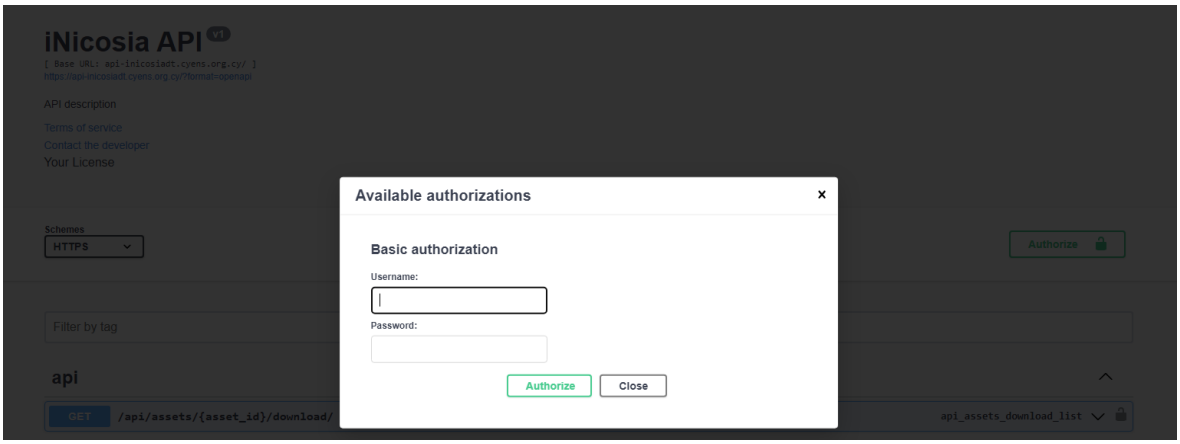

Figure 17: User Interaction for Data Authorization image iNicosia Digital Twin Platform

2. **Crafting Injection Queries:**: Τα ερωτήματα έγχυσης δημιουργήθηκαν και εκτελέστηκαν σχολαστικά, ενσωματώνοντας SQL querries όπως 'OR '1' ='1. Η άσκηση αυτή αποσκοπούσε στην ενεργοποίηση γνωστοποιήσεων σφαλμάτων. Ωστόσο, σύμφωνα με τα υψηλά πρότυπα ασφαλείας που διατηρεί η πλατφόρμα, αυτές οι προσπάθειες δεν απέδωσαν απαντήσεις ούτε εξέθεσαν τρωτά σημεία.
3. **Observing Responses and Refining Techniques:**: Έγιναν παρατηρήσεις για τυχόν αποκλίσεις στην απόκριση της πλατφόρμας στις ενέσεις μας, ιδιαίτερα αναζητώντας μηνύματα σφάλματος που ενδέχεται να αποκαλύψουν λεπτομέρειες της βάσης δεδομένων. Παρά τις αρκετές βελτιώσεις στην προσέγγισή μας για βαθύτερη διερεύνηση, οι απαντήσεις της πλατφόρμας παρέμειναν ασφαλώς μη περιγραφικές, υπογραμμίζοντας την αποτελεσματικότητα των διασφαλίσεών της έναντι των ενέσεων SQL.

Συγκεκριμένα για τα βήματα 2 και 3 χρησιμοποιήθηκαν οι εξής τεχνικές

1. **Error based SQL Injections**: Ξεκινήσαμε δοκιμές που προσπάθησαν να προκαλέσουν μηνύματα σφάλματος που θα μπορούσαν να αποκαλύψουν λεπτομέρειες δομής βάσης δεδομένων. Το σύστημα, ωστόσο, δεν εμφάνισε τέτοια τρωτά σημεία, αντανακλώντας τον προηγμένο χειρισμό σφαλμάτων και τα πρωτόκολλα ασφαλείας που ισχύουν.

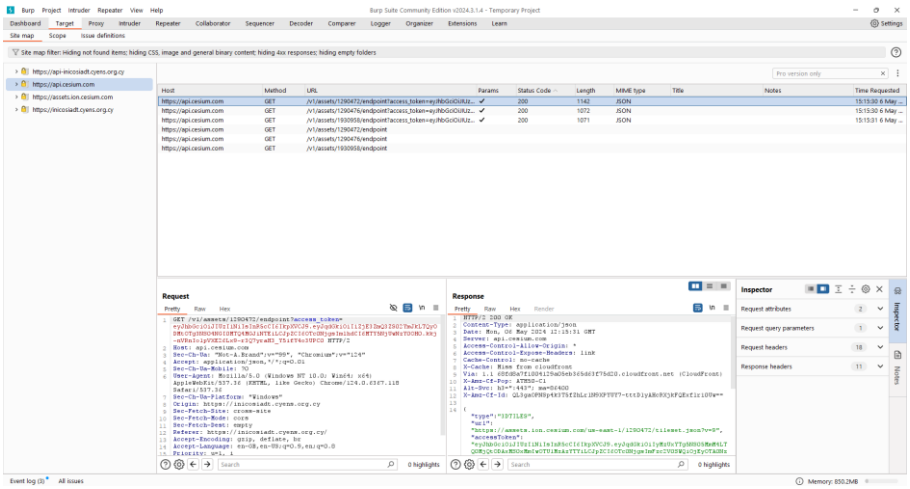

Figure 18: Interface Interactions for Database Vulnerability Testing on iNicosia Digital Twin

2. **Blind SQL Injection**: Έγιναν προσπάθειες για την εκτέλεση τόσο χειρισμών απόκρισης υπό όρους όσο και ερωτημάτων βάσει χρόνου για την αξιολόγηση των δυνατοτήτων αθόρυβης εξαγωγής δεδομένων. Το σύστημα δεν έδειξε αποκλίσεις στον χρόνο απόκρισης ή διαρροή δεδομένων, υποδεικνύοντας ασφαλείς μηχανισμούς επικύρωσης και εκτέλεσης ερωτημάτων.

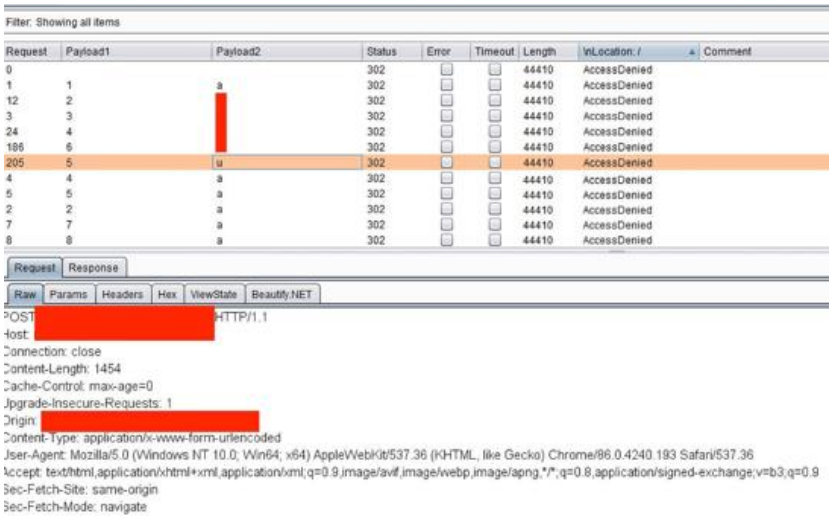

Figure 19: Blind SQL Injection Attempt

3. **Union-Based and Out-of-Band SQL Injection**: Αυτές οι μέθοδοι δοκιμάστηκαν για να ελέγξουν για μη εξουσιοδοτημένη πρόσβαση σε δεδομένα από διαφορετικούς πίνακες βάσης δεδομένων και εξωτερικά κανάλια. Η πλατφόρμα διατήρησε την ακεραιότητά της σε αυτές τις δοκιμές χωρίς να εκθέσει ευαίσθητες πληροφορίες.

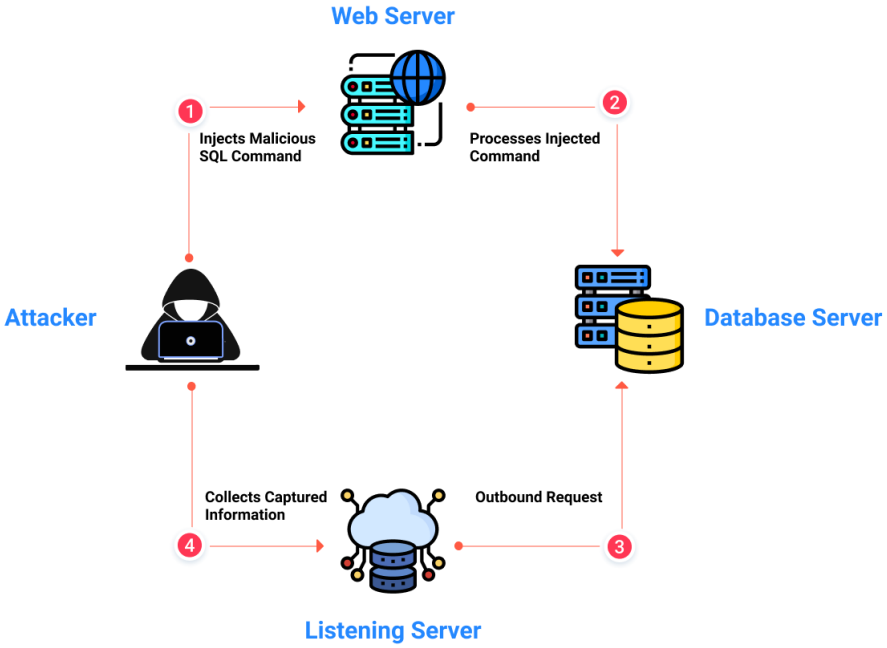

Figure 20: Injection image from PortSwigger

Συνολικά, οι αυστηρές άμυνες του iNicosia <u>απέτρεψαν με επιτυχία</u> όλες τις SQL injection attacks, υπογραμμίζοντας την αποτελεσματικότητα των μέτρων ασφαλείας που εφαρμόστηκαν από την επαγγελματική ομάδα που διαχειρίζεται την πλατφόρμα. Αυτό αποδεικνύει τη δέσμευσή τους να προστατεύουν από τέτοιες διαδεδομένες απειλές στον κυβερνοχώρο.

- ## Cross-Site Scripting (XSS): [2]

Τι είναι το Cross-Site Scripting (XSS)

Το Cross-Site Scripting (γνωστό και ως XSS) είναι μια web Security vulnerability που επιτρέπει σε έναν εισβολέα να υπονομεύσει τις αλληλεπιδράσεις που έχουν οι χρήστες με μια ευάλωτη εφαρμογή. Επιτρέπει σε έναν εισβολέα να παρακάμψει την ίδια πολιτική προέλευσης, η οποία έχει σχεδιαστεί για να διαχωρίζει διαφορετικούς ιστότοπους μεταξύ τους. Το Cross-Site Scripting συνήθως επιτρέπει σε έναν εισβολέα να μεταμφιεστεί ως χρήστης-θύμα, να εκτελέσει οποιεσδήποτε ενέργειες μπορεί να εκτελέσει ο χρήστης και να αποκτήσει πρόσβαση σε οποιοδήποτε από τα δεδομένα του χρήστη. Εάν ο χρήστης θύμα έχει

προνομιακή πρόσβαση εντός της εφαρμογής, τότε ο εισβολέας ενδέχεται να είναι σε θέση να αποκτήσει τον πλήρη έλεγχο όλων των λειτουργιών και των δεδομένων της εφαρμογής.

Πώς λειτουργεί το XSS;

Το Cross-Site Scripting λειτουργεί χειραγωγώντας μια ευάλωτη ιστοσελίδα, ώστε να επιστρέφει κακόβουλο JavaScript στους χρήστες. Όταν ο κακόβουλος κώδικας εκτελείται μέσα στο πρόγραμμα περιήγησης ενός θύματος, ο εισβολέας μπορεί να θέσει σε πλήρη κίνδυνο την αλληλεπίδρασή του με την εφαρμογή.

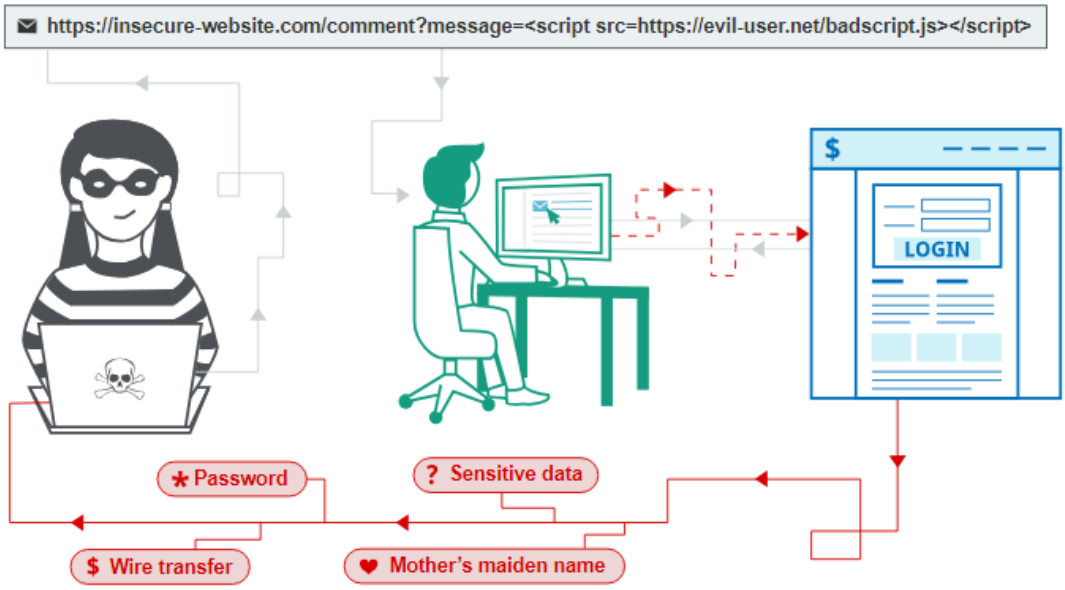

Figure 21: Representation of XSS Scripting image from PortSwigger

Κατά τη διάρκεια της δοκιμής της πλατφόρμας iNicosia για ευπάθειες ασφαλείας, εξετάστηκαν διάφορα συγκεκριμένα σενάρια επίθεσης Cross-Site Scripting (XSS) για να διασφαλιστεί ότι εφαρμόζονται ισχυρά μέτρα ασφαλείας:

1. **Reflected and Stored XSS in HTML Context:** Αυτές οι θεμελιώδεις δοκιμές ελέγχουν για unencoded user inputπου εκτελείται στο browser. Δεν εντοπίστηκαν τρωτά σημεία, υποδεικνύοντας αποτελεσματικές πρακτικές απολύμανσης και κωδικοποίησης.
2. **DOM XSS in Document.Write Sink:** Αυτή η δοκιμή σχεδιάστηκε για να διερευνήσει τις ευπάθειες XSS που βασίζονται σε DOM μέσω της μεθόδου document.write της JavaScript, χρησιμοποιώντας δυναμικά αποδιδόμενες εισόδους χρήστη. Η πλατφόρμα δεν εμφάνισε τέτοια τρωτά σημεία, επιδεικνύοντας την ανθεκτικότητά της έναντι του DOM XSS.

3. **Reflected XSS in JavaScript Strings**: Αυτή η δοκιμή επικεντρώθηκε στον χειρισμό των κωδικοποιήσεων συμβολοσειρών JavaScript από την πλατφόρμα. Επιβεβαίωσε ότι ειδικοί χαρακτήρες όπως γωνιακές αγκύλες κωδικοποιούνται σωστά (angle brackets are correctly encoded), εμποδίζοντας την εκτέλεση οποιασδήποτε μορφής εκτελέσιμου σεναρίου.

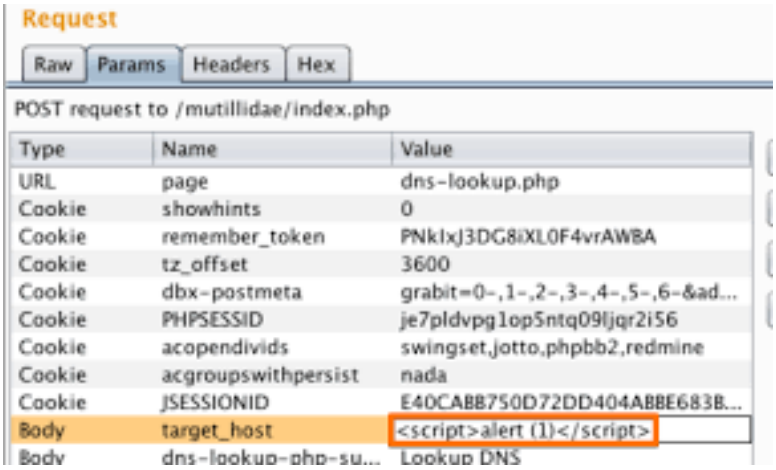

Figure 22: Cross-site Scripting Attack via POST Request

4. **Exploiting XSS to Steal Cookies and Capture Passwords:** Αυτές οι κρίσιμες δοκιμές στοχεύουν στην αποκάλυψη πιθανών επιπτώσεων του XSS στον πραγματικό κόσμο, όπως η μη εξουσιοδοτημένη πρόσβαση σε cookies ή κωδικούς πρόσβασης. Η πλατφόρμα βρέθηκε ασφαλής έναντι τέτοιων εκμεταλλεύσεων, επιβεβαιώνοντας περαιτέρω την ευρωστία των μέτρων προστασίας XSS.

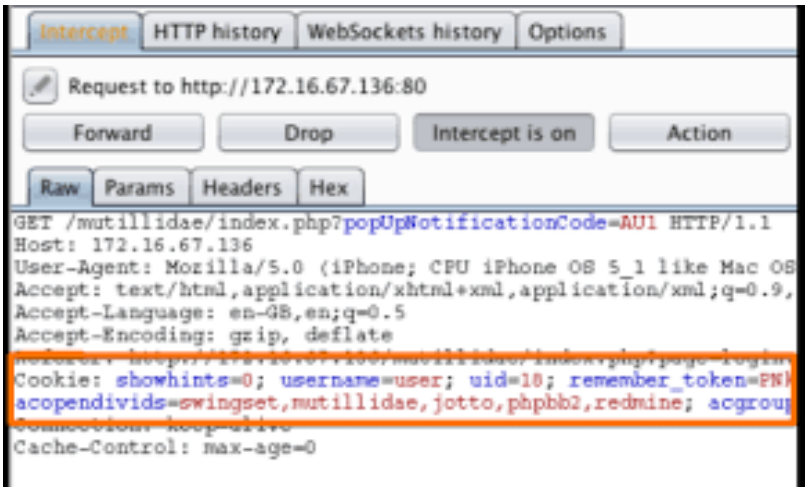

Figure 23: Cross-Site Scripting (XSS) Attack Demonstration for Cookie Theft and Password Capture

Αυτά τα ευρήματα <u>αντικατοπτρίζουν τα ολοκληρωμένα και αποτελεσματικά μέτρα ασφαλείας της πλατφόρμας</u> κατά των επιθέσεων XSS, υποστηρίζοντας ένα ασφαλές περιβάλλον για τους χρήστες της.

1. Έλεγχος ταυτότητας

1. **Username Enumeration**: Η πλατφόρμα δοκιμάστηκε για διαφορετικές αποκρίσεις ή παραλλαγές χρονισμού που θα μπορούσαν να επιτρέψουν σε έναν εισβολέα να συναγάγει έγκυρα ονόματα χρήστη. Δεν βρέθηκαν τέτοιες ευπάθειες, υποδεικνύοντας ισχυρά μέτρα απορρήτου και ασφάλειας των χρηστών. Η πλατφόρμα iNicosia, η οποία δεν διαθέτει έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA), χρησιμοποιεί μόνο έλεγχο ταυτότητας ενός παράγοντα (SFA) που περιλαμβάνει κυρίως διαπιστευτήρια χρήστη όπως email και κωδικό πρόσβασης. Η εξέταση μέσω του Burp Suite αποκαλύπτει ότι το email και ο κωδικός πρόσβασης είναι ορατά στην κυκλοφορία, γεγονός που αποτελεί σημαντικό κίνδυνο για την ασφάλεια. Αυτή η ορατότητα θα μπορούσε ενδεχομένως να επιτρέψει μια επίθεση man-in-the-middle, όπου ένας εισβολέας θα μπορούσε να υποκλέψει αυτά τα credentials. Επιπλέον, χωρίς MFA, η πλατφόρμα είναι πιο ευάλωτη σε επιθέσεις brute force. Ένας εισβολέας θα μπορούσε να δοκιμάσει πολλούς κοινούς κωδικούς πρόσβασης έναντι ενός έγκυρου για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση, αυξάνοντας τον κίνδυνο κλοπής δεδομένων.

Figure 24 & 25: Successful Username Enumeration Example Client and Sever Response Respectively

2. **Password Reset Flaws**: Η λογική πίσω από την επαναφορά κωδικού πρόσβασης εξετάστηκε εξονυχιστικά για τον εντοπισμό τυχόν τρωτών σημείων που θα μπορούσαν να επιτρέψουν σε έναν εισβολέα να παρακάμψει ή να χειριστεί την ανάκτηση κωδικού πρόσβασης. Η διαδικασία επαναφοράς κωδικού πρόσβασης στην πλατφόρμα iNicosia Digital Twin περιλαμβάνει μια ασφαλή μέθοδο που τηρεί καλές πρακτικές ασφαλείας. Όταν επιχειρούν να επαναφέρουν έναν κωδικό πρόσβασης, οι χρήστες πρέπει να εισάγουν έναν νέο κωδικό πρόσβασης που συμμορφώνεται με συγκεκριμένες απαιτήσεις πολυπλοκότητας. Αυτό είναι εμφανές από τα μηνύματα σφάλματος που επιβάλλουν τη χρήση ισχυρών, μη κοινών κωδικών πρόσβασης, οι οποίοι πρέπει να περιέχουν ένα ελάχιστο μήκος και δεν μπορούν να είναι εντελώς αριθμητικοί.

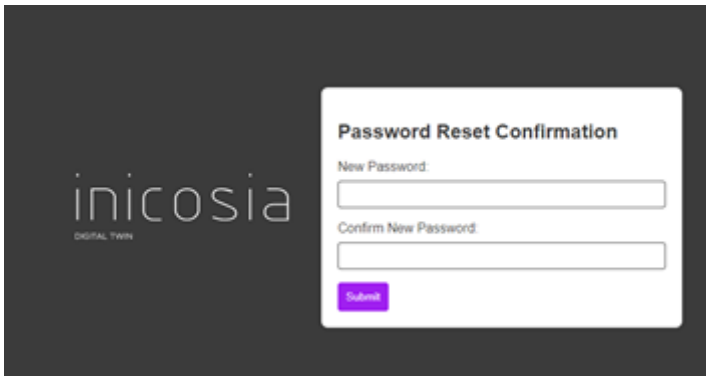

Figure 26: Password Reset Confirmation Page of iNicosia Digital Twin

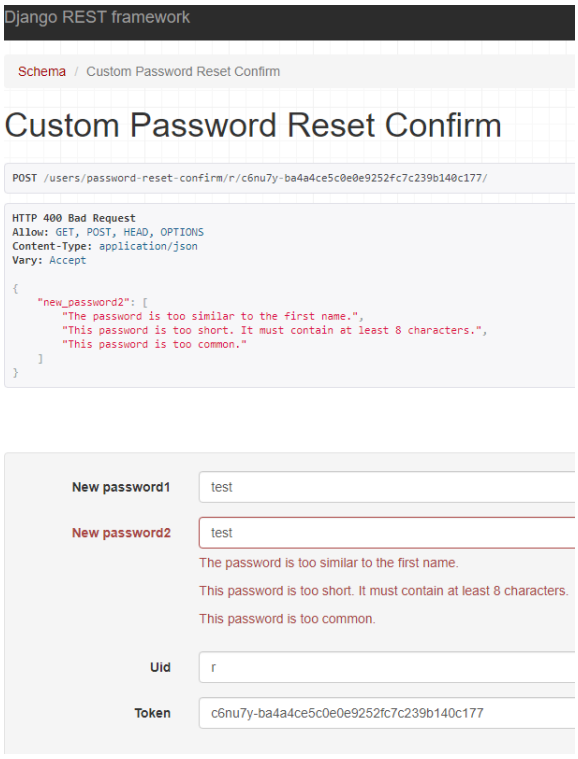

Figure 27: Password Reset Validation Response in iNicosia Platform

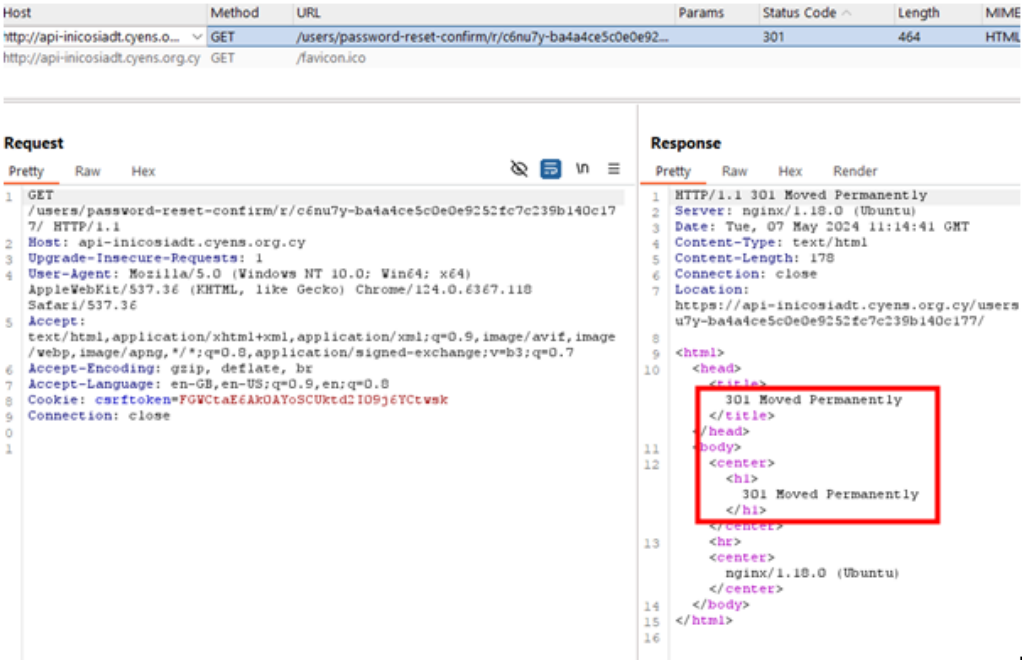

Figure 28: Redirect Response 301 During Password Reset Attempt

Επιπλέον, η διαδικασία ανακατεύθυνσης που διαχειρίζεται μέσω HTTP status codes, όπως μια ανακατεύθυνση 301 που παρατηρείται στο sever response, υποδηλώνει μια καλά διαχειριζόμενη και ασφαλή ροή επαναφοράς κωδικού πρόσβασης.

- **API testing**

Τα API (Application Programming Interfaces) επιτρέπουν σε συστήματα λογισμικού και εφαρμογές να επικοινωνούν και να μοιράζονται δεδομένα. Οι δοκιμές API είναι σημαντικές, καθώς οι ευπάθειες στα API ενδέχεται να υπονομεύσουν βασικές πτυχές της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας ενός ιστότοπου.
Όλα τα dynamic websites αποτελούνται από API, επομένως οι κλασικές ευπάθειες ιστού όπως το SQL injection θα μπορούσαν να ταξινομηθούν ως δοκιμές API. Στη συνέχεια παρουσιάζονται οι δοκιμές API που δεν χρησιμοποιούνται πλήρως από το front-end του ιστότοπου, με έμφαση στα API RESTful και JSON που χρησιμοποιεί η πλατφόρμα iNicosia.

1. **Exploiting an API endpoint using documentation**

Κατά την προσπάθεια πρόσβασης στη λίστα χρηστών τους πλατφόρμας iNicosia μέσω του API τους, παρουσιάστηκε σφάλμα «403 Forbidden» που υποδεικνύει αποτυχία επαλήθευσης CSRF. Αυτό υποδεικνύει ότι η πλατφόρμα εφαρμόζει μέτρα προστασίας CSRF, καθώς ελέγχει την προέλευση των αιτημάτων για να διασφαλίσει ότι προέρχονται από αξιόπιστες πηγές. Το μήνυμα σφάλματος υποδεικνύει την ανάγκη για CSRF tokens στα POST requests, τα οποία αποτελούν μέρος των πρακτικών ασφαλείας του Django για την αποτροπή του Cross-Site Request Forgery. Η πλατφόρμα του iNicosia απέτρεψε με επιτυχία την προσπάθεια αυτή.

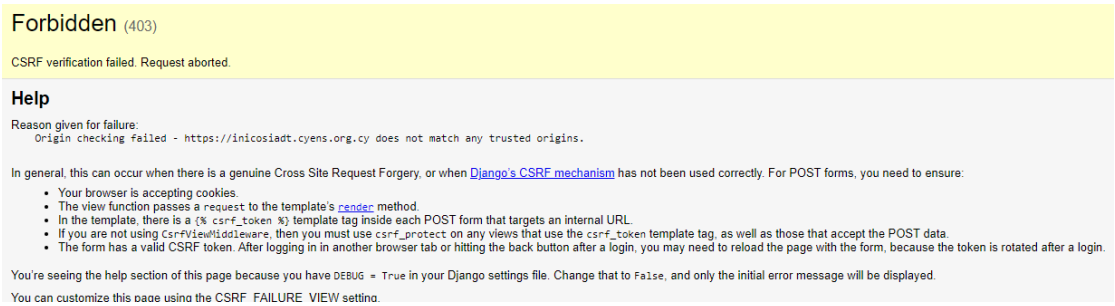

Figure 29: CSRF Protection Error on iNicosia Platform of API Expoloit attempt

2. **Finding and Exploiting an Unused API Endpoint**: Αναζήτησα και προσπάθησα να εκμεταλλευτώ τυχόν ανενεργά ή παλιά API endpoints που ενδέχεται να εξακολουθούν να είναι προσβάσιμα, θέτοντας πιθανούς κινδύνους ασφαλείας. Μέσα από την έρευνα δεν εντοπίστηκαν ανενεργά API endpoints, ως εκ τούτου να καθιστούν ασφαλή την πλατφόρμα

Όλες οι δοκιμές που πραγματοποιήθηκαν στην πλατφόρμα ήταν για ερευνητικούς σκοπούς για την υποστήριξη της ασφάλειάς της. Για τις δοκιμές χρησιμοποιήθηκε το λογισμικό BurpSuite v.2024.3.1.4 από το PortSwigger, ένα καλά αναγνωρισμένο εργαλείο στην ασφάλεια στον κυβερνοχώρο. Αυτό το λογισμικό έχει σχεδιαστεί για δοκιμές ασφάλειας εφαρμογών ιστού, επιτρέποντας στους ερευνητές να εκτελούν δομημένες επιθέσεις όπως SQL injection ή cross-site scripting (XSS) για τον εντοπισμό τρωτών σημείων. Η χρήση τέτοιων προηγμένων εργαλείων βοηθά να διασφαλιστεί ότι οι μηχανισμοί ασφαλείας της πλατφόρμας είναι ισχυροί έναντι πραγματικών επιθέσεων, επισημαίνοντας πιθανά ζητήματα ασφάλειας που πρέπει να αντιμετωπιστούν για την αποτελεσματική προστασία των δεδομένων των χρηστών.

Κεφάλαιο 6

6. Συμπεράσματα και μελλοντικές εργασίες

6.1. Προτεινόμενες Βελτιώσεις Ασφαλείας

Συνοπτικά οι προτεινόμενες βελτιώσεις ασφαλείας μεσα από την διατριβή και την έρευνα που πραγματοποήθηκε είναι|:

- **Έλεγχος ταυτότητας πολλαπλών παραγόντων** Η δημιουργία ενός ασφαλούς πλαισίου API είναι θεμελιώδης. Με την υιοθέτηση τυποποιημένων πρωτοκόλλων ασφαλείας όπως το OAuth 2.0 και το OpenID Connect, το σύστημα μπορεί να διαχειριστεί τον έλεγχο ταυτότητας και την εξουσιοδότηση με ασφάλεια σε ολόκληρο το δίκτυό του. Το πλαίσιο αυτό θα πρέπει να περιλαμβάνει περιορισμό ρυθμού, κρυπτογράφηση και τακτικούς ελέγχους ασφαλείας για την πρόληψη καταχρήσεων API και παραβιάσεων δεδομένων, ενισχύοντας έτσι την πύλη μέσω της οποίας εξωτερικές εφαρμογές και υπηρεσίες αλληλεπιδρούν με το ψηφιακό δίδυμο.

- **Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA):** Η μετάβαση από τον έλεγχο ταυτότητας ενός παράγοντα (SFA) στον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) είναι εξαιρετικά σημαντική για την ενίσχυση της ασφάλειας σε ολόκληρη την ψηφιακή υποδομή της iNicosia. Το MFA εισάγει ένα πρόσθετο επίπεδο ασφάλειας, απαιτώντας από τους χρήστες να επαληθεύουν την ταυτότητά τους χρησιμοποιώντας δύο ή περισσότερα ανεξάρτητα credentials, μειώνοντας σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης και πιθανών παραβιάσεων ασφαλείας. Αυτό είναι ιδιαίτερα ζωτικής σημασίας σε ένα εξελιγμένο περιβάλλον ψηφιακού διδύμου, όπου οι ενισχυμένοι μηχανισμοί ελέγχου πρόσβασης ευθυγραμμίζονται με τις βέλτιστες πρακτικές για την προστασία ευαίσθητων δεδομένων και υποδομών.

- **Διαχείριση κλειδιών κρυπτογράφησης**: : Αναπτύξτε συστήματα ασφαλείας που τροφοδοτούνται από τεχνητή νοημοσύνη, χρησιμοποιώντας αλγόριθμους μηχανικής μάθησης για να μαθαίνετε συνεχώς από την κυκλοφορία δικτύου, τη συμπεριφορά των χρηστών και την εξωτερική νοημοσύνη απειλών. Αυτά τα συστήματα είναι ικανά να ανιχνεύουν ανωμαλίες που αποκλίνουν από τα κανονικά πρότυπα, να εντοπίζουν πιθανές απειλές σε πραγματικό χρόνο και να ξεκινούν αυτοματοποιημένες απαντήσεις για τον μετριασμό των κινδύνων. Αυτά τα προληπτικά μέτρα ασφαλείας μπορούν να ανταποκριθούν προσαρμοστικά στις νέες απειλές που προκύπτουν.

- **Προγνωστική ανάλυση**: Η ενσωμάτωση προηγμένων εργαλείων προγνωστικής ανάλυσης μπορεί να μετατρέψει τεράστιες ποσότητες ιστορικών δεδομένων και δεδομένων πόλης σε πραγματικό χρόνο σε αξιοποιήσιμες πληροφορίες. Με την εφαρμογή αλγορίθμων μηχανικής μάθησης, το iNicosia μπορεί να προβλέψει μελλοντικές συνθήκες και σενάρια, όπως η πρόβλεψη κυκλοφοριακής συμφόρησης κατά τη διάρκεια εκδηλώσεων ή η βελτιστοποίηση διαδρομών συλλογής απορριμμάτων. Αυτή η μελλοντοστραφής προσέγγιση διευκολύνει την καλύτερη διαχείριση των πόρων και τον πολεοδομικό σχεδιασμό.

- **Επεξεργασία δεδομένων σε πραγματικό χρόνο**: Η αξιοποίηση προηγμένων πλαισίων επεξεργασίας δεδομένων επιτρέπει στο iNicosia να χειρίζεται αποτελεσματικά μεγάλες ροές δεδομένων σε πραγματικό χρόνο. Εργαλεία όπως **το Apache Flink ή το Apache Spark** μπορούν να επεξεργαστούν δεδομένα κατά την άφιξή τους, κάτι που είναι ζωτικής σημασίας για εφαρμογές όπως η διαχείριση της κυκλοφορίας σε πραγματικό χρόνο ή τα συστήματα αντιμετώπισης έκτακτης ανάγκης, διασφαλίζοντας ότι το ψηφιακό δίδυμο αντικατοπτρίζει με ακρίβεια και άμεσα τις τρέχουσες συνθήκες της πόλης.

- **Ανάλυση συμπεριφοράς**: Η χρήση αναλύσεων συμπεριφοράς για την παρακολούθηση των δραστηριοτήτων των χρηστών και τον εντοπισμό ύποπτων ενεργειών μπορεί να υποδεικνύει απειλή για την ασφάλεια, όπως ασυνήθιστα μοτίβα πρόσβασης ή συναλλαγές. Αυτή η προληπτική επιτήρηση βοηθά στον έγκαιρο εντοπισμό πιθανών παραβιάσεων ασφαλείας, μειώνοντας σημαντικά τον αντίκτυπό τους.

- **Ολοκληρωμένη κρυπτογράφηση δεδομένων**: Η εφαρμογή κρυπτογράφησης από άκρο σε άκρο για όλα τα δεδομένα κατά τη μεταφορά και την ηρεμία εντός του οικοσυστήματος ψηφιακών διδύμων είναι κρίσιμη. Η χρήση ισχυρών προτύπων κρυπτογράφησης όπως το AES-128 ή το AES-256 διασφαλίζει ότι όλα τα δεδομένα, ανεξάρτητα από την κατάστασή τους, παραμένουν δυσανάγνωστα σε μη εξουσιοδοτημένους χρήστες.

- **Διαχείριση κλειδιών κρυπτογράφησης**: Η ανάπτυξη ενός ισχυρού συστήματος διαχείρισης κλειδιών κρυπτογράφησης αυτοματοποιεί τη δημιουργία, τη διανομή, την αποθήκευση και την ανάκληση κλειδιών κρυπτογράφησης. Το σύστημα αυτό θα πρέπει επίσης να υποστηρίζει στρατηγικές εναλλαγής κλειδιών και αρχειοθέτησης για την ενίσχυση της ασφάλειας των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής.

6.2. Σύνοψη των πορισμάτων

Από μια σύντομη έρευνα, δεν υπήρχαν ευρέως δημοσιευμένες ή συγκεκριμένες αναφορές που να περιγράφουν λεπτομερώς επιτυχημένες επιθέσεις στον κυβερνοχώρο που στοχεύουν αποκλειστικά σε τεχνολογίες ψηφιακών διδύμων. Ωστόσο, δεδομένου ότι τα ψηφιακά δίδυμα ενσωματώνονται στενά με συσκευές IoT, πλατφόρμες cloud, και άλλα δικτυωμένα συστήματα, μοιράζονται κοινά τρωτά σημεία και απειλές που επηρεάζουν αυτές τις τεχνολογίες. Οι μέθοδοι που προϋπάρχουν στην πλατφόρμα του iNicosia σε συνδυασμό με τις εισηγήσεις που έχω αναφέρει και αναλύσει προηγουμένως θα καθιστούν την πλατφόρμα ασφαλή σε ένα πολύπλευρο βαθμό και θωρακισμένη από οποιαδήποτε επίθεση.

Το εξελισσόμενο τοπίο της κυβερνοασφάλειας παρουσιάζει νέες προκλήσεις και τρωτά σημεία, ιδίως σε πολύπλοκα συστήματα όπως τα ψηφιακά δίδυμα. Μια σημαντική ανησυχία είναι η έλλειψη ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) και η ευαισθησία σε επιθέσεις Man-In-The-Middle (MITM). Αυτές οι επιθέσεις, όπου ένας μη εξουσιοδοτημένος παράγοντας υποκλέπτει την επικοινωνία μεταξύ δύο μερών, είναι ιδιαίτερα επικίνδυνες καθώς μπορούν να οδηγήσουν σε κλοπή ταυτότητας και μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα συστήματα.

Πρόσφατες μελέτες δείχνουν μια ανησυχητική αύξηση της συχνότητας και της πολυπλοκότητας των επιθέσεων MITM. Σύμφωνα με έρευνα της Symantec, οι επιθέσεις MITM έχουν σημειώσει αύξηση περίπου 35% μόνο τον τελευταίο χρόνο. Αυτή η αύξηση

υπογραμμίζει την ευκολία με την οποία μπορούν να εκτελεστούν αυτές οι επιθέσεις, ειδικά καθώς οι επιτιθέμενοι εκμεταλλεύονται μη ασφαλείς ή ασθενώς κρυπτογραφημένες συνδέσεις. Στο πλαίσιο των ψηφιακών διδύμων, όπου η συνεχής ανταλλαγή δεδομένων αποτελεί θεμελιώδες στοιχείο, ο αντίκτυπος τέτοιων επιθέσεων μπορεί να είναι καταστροφικός, θέτοντας σε κίνδυνο την ακεραιότητα και την εμπιστευτικότητα των δεδομένων των διδύμων.

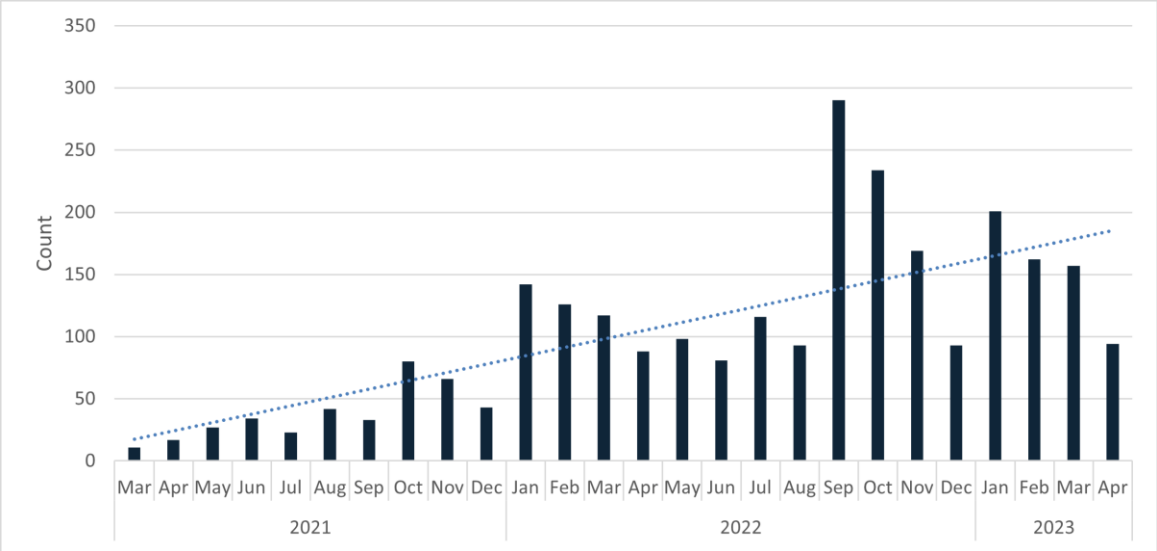

Figure 30: Symantec Study about MITM Attacks attempts over the months

Η εφαρμογή του MFA είναι ένα κρίσιμο μέτρο ασφαλείας που μετριάζει σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης. Απαιτώντας περισσότερες από μία μεθόδους επαλήθευσης, το MFA διασφαλίζει ότι η κλοπή ή η παραβίαση ενός μεμονωμένου διαπιστευτηρίου—όπως ενός κωδικού πρόσβασης—δεν θα επαρκεί για την απόκτηση πρόσβασης. Αυτό το επίπεδο ασφάλειας καθίσταται απαραίτητο για την προστασία από κλοπή ταυτότητας και μη εξουσιοδοτημένες προσπάθειες πρόσβασης, οι οποίες είναι κοινές σε σενάρια MITM.

Επιπλέον, η ενσωμάτωση συστημάτων ανίχνευσης που βασίζονται στην τεχνητή νοημοσύνη στην πλατφόρμα iNicosia είναι υπερ. σημαντικά για την παρακολούθηση και την αντιμετώπιση απειλών σε πραγματικό χρόνο. Αυτά τα συστήματα αξιοποιούν αλγόριθμους μηχανικής μάθησης για να αναλύσουν μοτίβα συμπεριφοράς και να εντοπίσουν ανωμαλίες που μπορεί να υποδηλώνουν απειλή για την ασφάλεια, συμπεριλαμβανομένων πιθανών επιθέσεων MITM. Παρέχοντας αυτοματοποιημένη και έξυπνη ανίχνευση απειλών, αυτά τα συστήματα μπορούν να ειδοποιούν τους διαχειριστές για ύποπτες δραστηριότητες καθώς

συμβαίνουν, επιτρέποντας άμεσες και αποτελεσματικές απαντήσεις για τον μετριασμό τυχόν ζημιών.

Η εφαρμογή ισχυρών μέτρων ασφαλείας, όπως το MFA και τα συστήματα ανίχνευσης που βασίζονται στην τεχνητή νοημοσύνη, δεν είναι απλώς μια βελτίωση αλλά μια αναγκαιότητα για την πλατφόρμα iNicosia. Καθώς τα ψηφιακά δίδυμα εξακολουθούν να διαδραματίζουν κεντρικό ρόλο στη διαχείριση των αστικών περιοχών και των υποδομών, η διασφάλιση της ασφάλειάς τους έναντι ολοένα και πιο κοινών και εξελιγμένων απειλών στον κυβερνοχώρο είναι υψίστης σημασίας. Η υιοθέτηση αυτών των τεχνολογιών θα παράσχει ισχυρότερη στάση ασφαλείας, διασφαλίζοντας τις κρίσιμες υποδομές και τα ευαίσθητα δεδομένα που διαχειρίζονται και αλληλεπιδρούν καθημερινά τα ψηφιακά δίδυμα.

6.3. Μελλοντικές Ερευνητικές Κατευθύνσεις

Προηγμένες τεχνικές κρυπτογράφησης

Καθώς τα ψηφιακά δίδυμα γίνονται όλο και περισσότερο αναπόσπαστο μέρος των υποδομών ζωτικής σημασίας και των περιβαλλόντων υψηλού ρίσκου, η διασφάλιση της ασφάλειας των μεταδιδόμενων και αποθηκευμένων δεδομένων είναι υψίστης σημασίας. Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στην ανάπτυξη προηγμένων μεθόδων κρυπτογράφησης που μπορούν να αντέξουν τις δυνητικές απειλές που θέτει η κβαντική υπολογιστική. Οι κβαντικοί αλγόριθμοι θα είναι ύψιστης σημασίας για την προστασία των ψηφιακών διδύμων από μελλοντικές κρυπτογραφικές προκλήσεις. Αυτή η έρευνα δεν θα πρέπει μόνο να διερευνήσει νέα μοντέλα κρυπτογράφησης, αλλά και να αξιολογήσει την απόδοση και τη σκοπιμότητα της ενσωμάτωσης αυτών των μοντέλων σε υπάρχουσες αρχιτεκτονικές ψηφιακών διδύμων χωρίς να διακυβεύεται η αποτελεσματικότητα του συστήματος.

Τακτικοί έλεγχοι ασφαλείας και έλεγχοι συμμόρφωσης

Για να ευθυγραμμιστούν με τα διεθνή πρότυπα και κανονισμούς, τα ψηφιακά δίδυμα απαιτούν συνεχή έλεγχο και ενημερώσεις. Μελλοντικές μελέτες θα πρέπει να διερευνήσουν μεθοδολογίες για την αυτοματοποίηση αυτών των ελέγχων ώστε να διασφαλιστεί η συνεχής συμμόρφωση και η ακεραιότητα της ασφάλειας. Η έρευνα θα μπορούσε να διερευνήσει συστήματα ελέγχου που βασίζονται στην τεχνητή νοημοσύνη και μαθαίνουν συνεχώς και προσαρμόζονται σε νέες απειλές, παρέχοντας βοήθεια συμμόρφωσης σε πραγματικό χρόνο και ανίχνευση ανωμαλιών. Επιπλέον, η καθιέρωση σημείων αναφοράς για ελέγχους ασφαλείας σε ψηφιακά δίδυμα μπορεί να τυποποιήσει τις πρακτικές σε όλους τους κλάδους,

προωθώντας μια ενοποιημένη προσέγγιση ασφάλειας που θα μπορούσε να διευκολύνει την ευρύτερη υιοθέτηση αυτής της τεχνολογίας.

Δοκιμές ανθεκτικότητας

Καθώς τα ψηφιακά δίδυμα συστήματα χειρίζονται όλο και πιο ευαίσθητα και πολύτιμα δεδομένα, γίνονται πρωταρχικοί στόχοι για εξελιγμένες επιθέσεις στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κλιμάκωσης προνομίων. Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στην ανάπτυξη και βελτίωση μοντέλων προσομοίωσης που μπορούν να μιμηθούν προηγμένες απειλές στον κυβερνοχώρο, παρέχοντας πληροφορίες σχετικά με πιθανές ευπάθειες εντός ψηφιακών δίδυμων συστημάτων. Αυτό περιλαμβάνει όχι μόνο τον εντοπισμό τυπικών τρωτών σημείων, αλλά και την πρόβλεψη μελλοντικών απειλών που θα μπορούσαν να εξελιχθούν καθώς αναπτύσσεται η τεχνολογία και οι εφαρμογές της. Επιπλέον, η διερεύνηση του αντίκτυπου των διαφόρων φορέων επίθεσης, συμπεριλαμβανομένων εκείνων που εκμεταλλεύονται εσωτερικές απειλές ή επιθέσεις που δημιουργούνται από AI, θα μπορούσε να παράσχει μια ολοκληρωμένη εικόνα των πιθανών κενών ασφαλείας.

Πρόληψη επίθεσης ανύψωσης ρόλου

Ένας συγκεκριμένος τομέας ανησυχίας είναι οι επιθέσεις ανύψωσης ρόλων, όπου μη εξουσιοδοτημένοι χρήστες αποκτούν υψηλότερα δικαιώματα πρόσβασης. Η έρευνα θα πρέπει να εμβαθύνει σε στρατηγικές ανίχνευσης και τεχνικές μετριασμού για την πρόληψη τέτοιων κλιμακώσεων. Αυτό θα μπορούσε να περιλαμβάνει την ανάπτυξη πιο εξελιγμένων πλαισίων ελέγχου πρόσβασης που χρησιμοποιούν μηχανική μάθηση για την κατανόηση των κανονικών προτύπων συμπεριφοράς των χρηστών και τον εντοπισμό ανωμαλιών ενδεικτικών τέτοιων επιθέσεων. Επιπλέον, η ενσωμάτωση αυτών των πλαισίων με τα υπάρχοντα εργαλεία διαχείρισης ψηφιακών διδύμων θα ενισχύσει τη συνολική στάση ασφαλείας.

Ενσωμάτωση συστημάτων ασφαλείας που βασίζονται στην τεχνητή νοημοσύνη

Η ενσωμάτωση της τεχνητής νοημοσύνης και της μηχανικής μάθησης στην ασφάλεια των ψηφιακών διδύμων προσφέρει μια προληπτική προσέγγιση για την ανίχνευση και την αντιμετώπιση απειλών. Η μελλοντική έρευνα θα πρέπει να διερευνήσει την ενσωμάτωση συστημάτων που βασίζονται στην τεχνητή νοημοσύνη και μπορούν να αναλύουν συνεχώς δεδομένα από ψηφιακά δίδυμα, να ανιχνεύουν αποκλίσεις από τις κανονικές λειτουργίες και να ξεκινούν αυτόματα αντίμετρα. Η δυνατότητα αυτών των συστημάτων να μαθαίνουν και

να προσαρμόζονται σε νέες απειλές σε πραγματικό χρόνο παρουσιάζει σημαντική πρόοδο στις στρατηγικές ασφάλειας ψηφιακών διδύμων.

Κεφάλαιο 7

Βιβλιογραφία

[0] iNicosia Digital Twin Platform User guide https://inicosia.gitbook.io/inicosia-digital-twin-user-guide

[1] TM Forum Digital Twin Architecture https://inform.tmforum.org/research-and-analysis/proofs-of-concept/digital-twin-network-operations-can-ease-the-burden-of-oam-in-the-5g-era

[2] API Security Details https://www.fortinet.com/resources/cyberglossary/api-security#:~:text=Application%20programming%20interface%20(API)%20security,the%20sensitive%20data%20they%20transfer.

[3] Cisco Stealth Watch AI Security System https://www.cisco.com/site/us/en/products/security/security-analytics/secure-network-analytics/index.html

[4] Configuration Examples and Technotes https://www.cisco.com/c/en/us/tech/security-vpn/authentication-protocols/tech-configuration-examples-list.html

[5] SQL Injection Attacks Simulation Attacks https://portswigger.net/web-security/sql-injection#retrieving-hidden-data

[6] Man in the Middle Attacks: Analysis, Motivation and Prevention https://www.researchgate.net/publication/347006863_Man_in_the_Middle_Attacks_Analysis_Motivation_and_Prevention