Υποδομή Ασφαλούς Απομακρυσμένης Πρόσβασης

Απαιτήσεις και Παράδειγμα Ανάπτυξης

*Άρθρο του **Σταύρου Καραγκιούλογλου**, Dipl.-Ing*
Managing Partner United-Telecom AE-
Partner Juniper Networks
e-mail: s.kara@united-telecom.gr

Η ασφαλής απομακρυσμένη πρόσβαση είναι σήμερα η ικανή και απαραίτητη συνθήκη για παραγωγική τηλε-εργασία χωρίς κινδύνους για τους πόρους της επιχείρησης που την υλοποιεί.

Παρατίθενται στη συνέχεια τα τεχνικά χαρακτηριστικά ενός συστήματος που θα εξασφάλιζε περιβάλλον ασφαλούς απομακρυσμένης πρόσβασης, λαμβάνοντας υπόψη και υλοποιώντας πρακτικές Zero Trust (Μηδενική Εμπιστοσύνη):

- Απομακρυσμένη πρόσβαση VPN
- Host checking (Health-Check πριν την σύνδεση)
- Πολλαπλή Πιστοποίηση ταυτότητας (Multi-factor Authentication - MFA)
- Single Sign On (SSO)
- Secure-Access to Cloud App's
- Bring Your Own Device - BYOD
- Enterprise Mobility & Device Management - EMM/MDM
- WorkSpace/Containerization/Cryptographie
- Profiling (Αξιολόγηση & κατάταξη συσκευών)
- Μηδενική Εμπιστοσύνη προς όλους και όλα
- Ενιαία συμπεριφορά, λειτουργία και επίπεδο ασφάλειας σε όλα τα λειτουργικά (OS) των συσκευών των χρηστών
- Δυνατότητα συγκρότησης σε Non-Stop λειτουργία (High Availability)
- Ευέλικτα σχήματα χρέωσης με Ονοματισμένους (Named) χρήστες ή Ανώνυμους χρήστες (Concurrent)
- Κεντρική εποπτεία, διαχείριση και έλεγχο της υποδομής και των χρηστών.

Οι παραπάνω απαιτήσεις ομαδοποιούνται σε τέσσερεις τομείς έλεγχου μηδενικής εμπιστοσύνης: User, Device, Acess, Data (Εικόνα 1).

Το πιο ευαίσθητο σημείο της απομακρυσμένης πρόσβασης:

Οι συσκευές των χρηστών

Απαιτούνται οι κάτωθι λειτουργικές δυνατότητες για την εξασφάλιση του επιπέδου προστασίας, συνδυασμένη και με εργονομία:

1-Self-Service Provisioning:

Αυτόματη διαμόρφωση των ρυθμίσεων email, VPN και Wi-Fi χρήστη με σύστημα Onboarding και Management Portal.

2-Identity Management:

Αξιοποίηση του υπάρχοντος Active Directory ή άλλων εσωτερικών ή εξωτερικών μηχανισμών ελέγχου ταυτότητας για την πιστοποίηση της πρόσβασης σε Cloud εφαρμογές και υπηρεσίες όπως π.χ. το Office 365, BOX, DropBox, Salesforce, FB, Spotify, Slack, YouTube και άλλες υπηρεσίες cloud (SaaS).

3-BYOD Container:

Ασφαλές Container σε συσκευές Android και iOS, το οποίο θα κρυπτογραφεί τα δεδομένα, θα ελέγχει την κοινή χρήση δεδομένων εφαρμογών, θα διαγράφει επιλεκτικά δεδομένα και θα μπορεί να υποστηρίξει πολιτικές συνδεσιμότητας ανά εφαρμογή. Η συσκευή να μπορεί να έχει 2 προσωπικότητες: Work & Life ή Private/ Public κλπ.

4-Πρόσβαση SSO:

Έλεγχος ταυτότητας βάσει πιστοποιητικών και SSO που παρέχει στους χρήστες εύκολη πρόσβαση δίχως επαναλαμβανόμενες αυθεντικοποιήσεις στις εφαρμογές και υπηρεσίες στο cloud (Security Assertion Markup Language - SAML).

5-Ενιαία εμπειρία χρηστών:

Ενιαίο Client software με ίδια λειτουργικότητα του Client software ανεξάρτητα από το λειτουργικό πρόγραμμα της συσκευής του χρήστη (Windows, Android, iOS, MAC, Linux, κ.α.).

Ενοποιημένη πολιτική ελέγχου πρόσβασης, ανεξάρτητα από τη γεωγραφική θέση του χρήστη και της συσκευής.

Κεντρική διαχείριση όλων των συσκευών και χρηστών έτσι ώστε να επιτρέπεται ορατότητα και διαχείριση χρηστών / συσκευών.

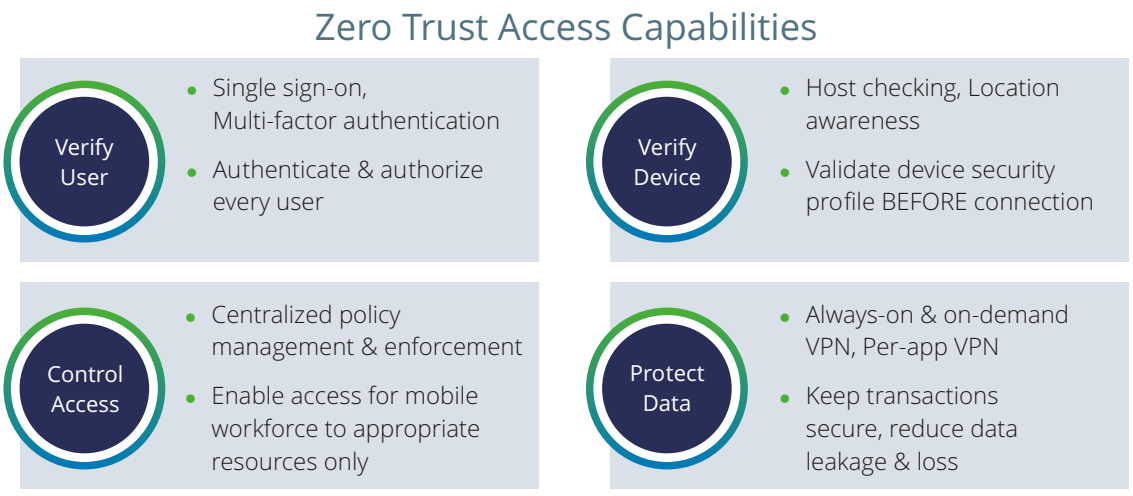
6-Hostchecking:

Η επιβολή συμμόρφωσης διασφαλίζει ότι μόνο οι ασφαλείς συσκευές θα έχουν πρόσβαση στις εφαρμογές και υπηρεσίες στο cloud. Το Hostchecking θα εφαρμόζεται σε όλα τα λειτουργικά των συσκευών. Να είναι δυνατή η χειροκίνητη ή αυτόματη αποκατάσταση.

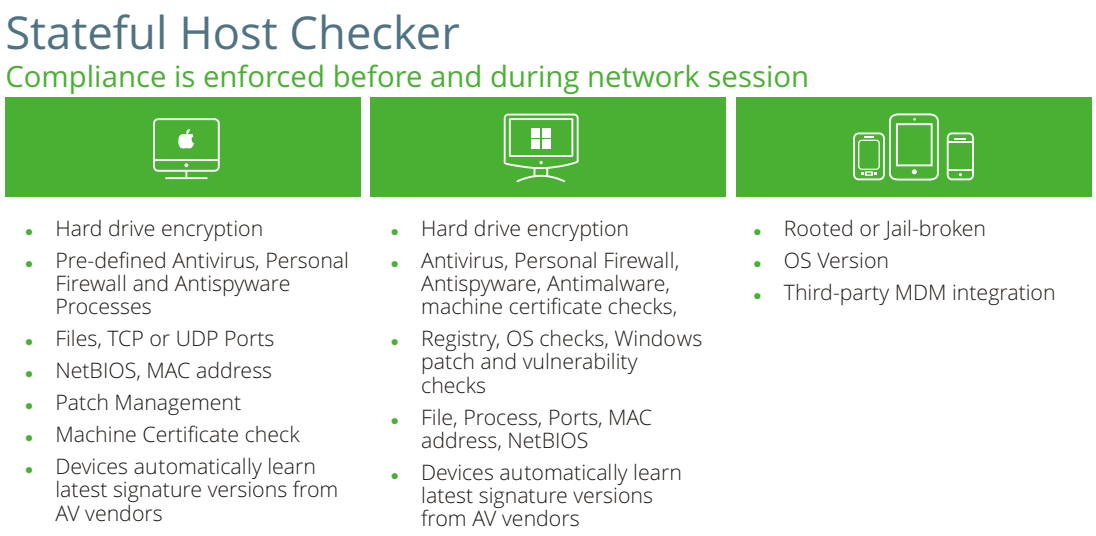
Παράμετροι τεχνικής διοίκησης απομακρυσμένων χρηστών με το σύστημα Μηδενικής Εμπιστοσύνης (Zero Trust)

Παράμετροι προστασίας για απομακρυσμένους χρήστες:

- Πολιτικές HostChecking (χειροκίνητες / αυτόματες)



Εικόνα 1. Οι τέσσερεις τομείς ελέγχου λόγω μηδενικής εμπιστοσύνης: User, Device, Access, Data



Εικόνα 2. Το Hostchecking αναλαμβάνει να ελέγχει διαρκώς και εξονυχιστικά όλους τους τύπους συσκευών

- Antivirus
- Antimalware
- Κρυπτογράφηση δίσκου
- Προσωπικό τείχος προστασίας
- Πιθανός έλεγχος ταυτότητας πιστοποιητικού
- Διαχείριση Patch
- Πιστοποίηση τεχνικής "υγείας" των συσκευών των χρηστών, Statement of Health (SoH)
- Ζώνες αποκατάστασης (χειροκίνητες / αυτόματες).

Παράμετροι πιστοποίησης απομακρυσμένων χρηστών (επιλέγουμε μία ή περισσότερες):

- Τοπικός έλεγχος ταυτότητας
- Έλεγχος ταυτότητας μέσω Radius
- Έλεγχος ταυτότητας μέσω Ldap
- Έλεγχος ταυτότητας μέσω Active Directory
- Έλεγχος ταυτότητας SAML
- MFA με One-Time-Password - OTP (όπως RSA, Vasco, Google, SMS κλπ)
- MFA με Προσωπικό Πιστοποιητικό
- Πιστοποιητικό επιχείρησης.

Παράμετροι διοίκησης απομακρυσμένων χρηστών:

- Αυτοματισμός onboarding χρήστη
- Μέθοδοι σύνδεσης χρήστη:
  - Clientless [Web]
  - Client Software (Windows, Mac, Linux)
  - Mobile Client
- Ενιαία εμπειρία/ευκολία χρήστη σε σταθερά και Mobile
- Λίστες ελέγχου πρόσβασης (ACL) μέσω VPN
- RDP (HTML5) μέσω VPN
- Windows File Share μέσω VPN
- Bookmarks για χρήστες VPN
- Split Tunneling μέσω FQDN ή IP-based
- SSO χρησιμοποιώντας SAML 2.0
- Διαχείριση χρηστών στην κεντρική κονσόλα διαχείρισης
- BYOD / WorkSpace για Containerization & Έλεγχο
- Mobile Device Management (EMM/MDM) ή διασύνδεση με τρίτους κατασκευαστές.

Παράμετροι τύπων VPN για απομακρυσμένους χρήστες:

- Δυνατότητα επιλογής τύπων VPN που θα εφαρμοστούν:
  - VPN ανά εφαρμογή
  - On-demand VPN
  - Πάντα ενεργό VPN (Always On VPN)
- Δυνατότητα ορισμού REALMS εισόδου, δηλαδή κατηγοριών αυστηρότητας των αυθεντικοποιήσεων βάσει της Πολιτικής Ασφάλειας της Επιχείρησης:

- CertAUTH
- 2FAAUTH
- AD, άλλα

- Να γίνεται αντιστοίχιση των τύπων VPN στα REALMS εισόδου
- Δυνατότητα ορισμού σελίδων για Sign-In
- Να γίνεται η αντιστοίχιση των σελίδων εισόδου (Sign-In) στα REALMS εισόδου.

Παράμετροι Επιπέδων πρόσβασης (μέσω επιλεγμένων Ρόλων) για τους απομακρυσμένους χρήστες, ορίζοντας:

- Ρόλους χρηστών όπως π.χ.: υπάλληλος, διευθυντής, τηλεργαζόμενος, ασκούμενος, επισκέπτης, ανάδοχος, συνεργάτης, IoT, άλλος
- Ρόλους Διαχειριστών όπως πχ: Master-admin, άλλοι
- Αντιστοίχιση των χρηστών ατομικά σε ρόλους χρηστών, ομοίως και για τους διαχειριστές.

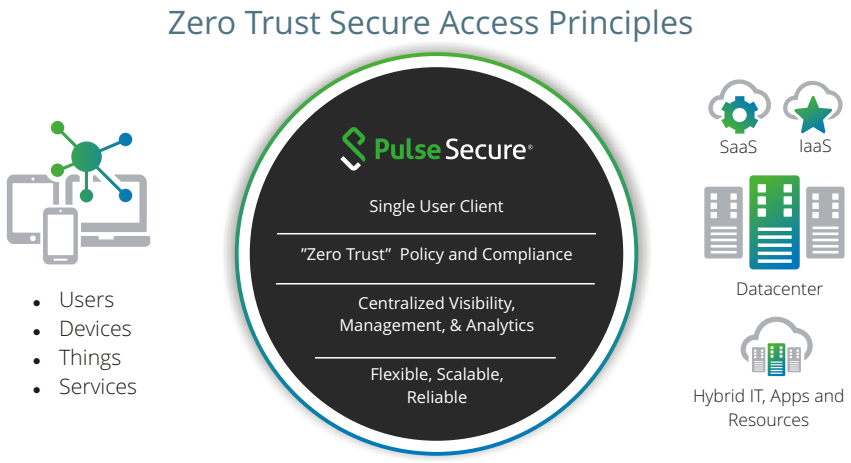
Παράδειγμα συστήματος Ασφαλούς Πρόσβασης

Για την καλύτερη κατανόηση της παραπάνω μεθοδολογίας θα χρησιμοποιηθεί ως παράδειγμα ένα σύστημα που υλοποιεί το σετ λειτουργιών και δυνατοτήτων που αναφέρθηκαν.

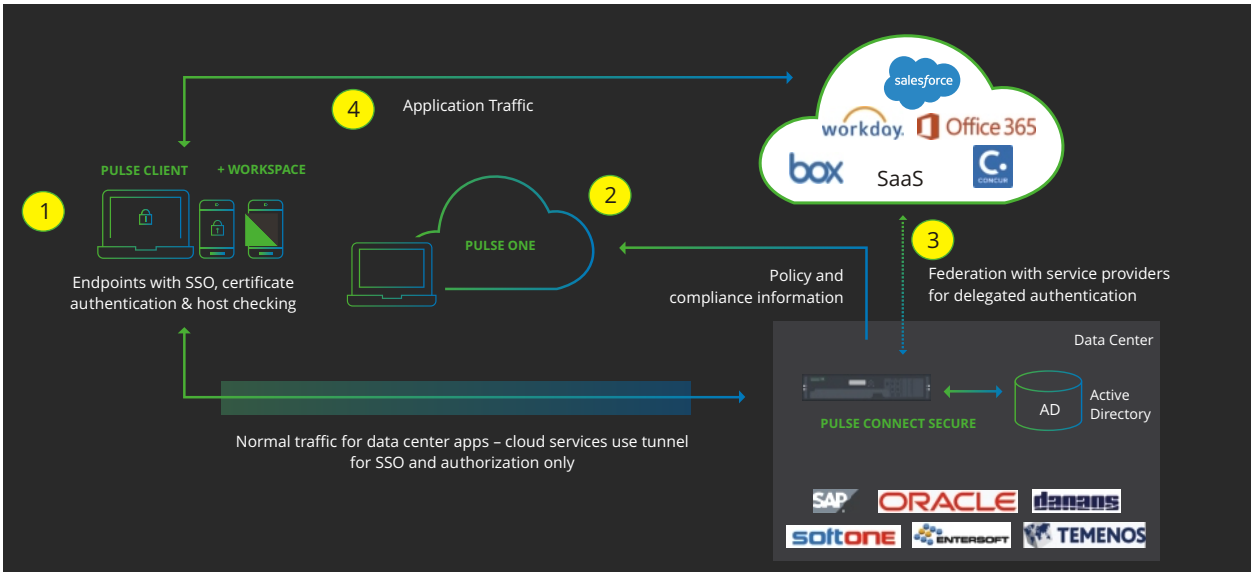
Σήμερα που σχεδόν όλες οι επιχειρήσεις βρίσκονται σε ένα υβριδικό IT περιβάλλον, το σύστημα αυτό μπορεί να εφαρμόσει ασφαλή πρόσβαση με διαδικασίες μηδενικής εμπιστοσύνης (Zero Trust).

Οι λειτουργίες μηδενικής εμπιστοσύνης μεταξύ άλλων είναι:

- Αρχική επαλήθευση του χρήστη. Επιπλέον, οι λειτουργίες Multi-Factor Authentication (MFA) και Single Sign-On (SSO) μπορούν να βελτιώσουν την ασφάλεια και τη λειτουργικότητα. Γίνεται έλεγχος ταυτότητας για κάθε χρήστη, όχι μόνο κάθε φορά που συνδέεται αλλά και κατά τη διάρκεια της σύνδεσης.
- Δευτερευόντως επαληθεύεται η ίδια συσκευή. Δεδομένης της ποικιλίας των συσκευών που χρησιμοποιούνται συνήθως σε κάθε οργανισμό, το σύστημα διασφαλίζει ότι κάθε συσκευή έχει τις πιο πρόσφατες ενημερώσεις λειτουργικού OS, έχει το σωστό λογισμικό προστασίας από ιούς, το λογισμικό εκτίμησης ευπάθειας και τις λειτουργίες τείχους προστασίας κ.λπ, ΠΡΙΝ πραγματοποιηθεί η σύνδεση (δηλαδή πριν δοθεί διεύθυνση IP).
- Εφαρμόζεται μια κεντρική λειτουργία για τη διανομή πολιτικών ασφαλούς πρόσβασης σε όλες τις συσκευές που έχουν πρόσβαση σε εφαρμογές και πόρους, μειώνοντας έτσι την πολυπλοκότητα της ενσωμάτωσης και τη διατήρηση πολιτικών σε ολόκληρη την υποδομή.
- Μέθοδοι επιβολής πολιτικής όπως μόνιμες



Εικόνα 3. Οι διαδικασίες μηδενικής εμπιστοσύνης εφαρμόζονται απ' άκρου εις άκρον



Εικόνα 4. Η πρόσβαση στο Data Center και στα SaaS ελέγχεται εξ ίσου στη βάση μηδενικής εμπιστοσύνης

συνδέσεις συνεχούς λειτουργίας, συνδέσεις ανά εφαρμογή και ούτω καθεξής χρησιμοποιούνται για να διασφαλιστεί ότι τα δεδομένα στα οποία γίνεται πρόσβαση προστατεύονται επίσης κατά τη μεταφορά. Με αυτόν τον τρόπο οι συναλλαγές είναι πάντα ασφαλείς και δεν υπάρχει περίπτωση οι χρήστες να μπορέσουν να παρακάμψουν τους μηχανισμούς ασφαλείας.

- Το σύστημα αυτό συνδυάζεται αρμονικά με τις υπόλοιπες υποδομές ασφάλειας και τα υπόλοιπα συστήματα του της επιχείρησης τόσο σε επίπεδο Data Center όσο και στις υποδομές των χρηστών. Επιπλέον διασφαλίζει ότι εφαρμόζονται παντού συμφωνημένοι και εγκεκριμένοι κανόνες πρόσβασης και επιπλέον δίνεται η δυνατότητα εποπτείας και απόδειξης της τήρησης των κανόνων με χρήση του δικού του cloud portal διαχείρισης.

Βήματα λειτουργίας συστήματος Ασφαλούς Πρόσβασης

Το παρακάτω λογικό διάγραμμα δικτύου μας δείχνει ενδεικτικά το σύστημα καθώς και την αλληλεπίδρασή του με το περιβάλλον ΤΠΕ της επιχείρησης στο Data Center.

Το σύστημα αυτό μπορεί να παρέχει τις ίδιες δυνατότητες ασφάλειας και ελέγχου πρόσβασης στα δεδομένα του Data Center καθώς και στις εφαρμογές στο cloud (SaaS). Οι χρήστες και των δύο περιβαλλόντων πιστοποιούνται εξ ίσου, οι συσκευές τους είναι host checked και παρέχεται κρυπτογραφημένη σύνδεση στο Data Center ή στους πόρους που βρίσκονται στο cloud.

Επιπροσθέτως:

(1) Το περιβάλλον Workspace παρέχει ένα ασφαλές εταιρικό Container BYOD για τις εγκεκριμένες εφαρμογές και δεδομένα της Επιχείρησης επάνω στις συσκευές των χρηστών.

(2) Το Workspace διαμορφώνεται χρησιμοποιώντας την κονσόλα του cloud portal και εφαρμόζονται οι πολιτικές ασφαλείας. Δίδεται πλήρης οπτική των συνδέσεων του χρήστη συμπεριλαμβανομένης της κατάστασης συμμόρφωσης των συσκευών του.

(3) Η ασφάλεια στο cloud ενεργοποιείται μέσω της ενοποίησης των παρόχων εφαρμογών και υπηρεσιών cloud (SaaS) με το χρησιμοποιούμενο σύστημα. Στην πραγματικότητα αυτό που συμβαίνει είναι ότι οι πάροχοι των εφαρμογών και υπηρεσιών μεταβιβάζουν τον έλεγχο ταυτότητας των χρηστών στο σύστημα μέσω IF-MAP Federation, το οποίο μπορεί και εφαρμόζει την εταιρική Πολιτική Ασφάλειας της Επιχείρη-

σης. Αυτό με τη σειρά του επιτρέπει την πρόσβαση στο cloud και στο Data Center μόνο όταν ο χρήστης έχει ελεγχθεί μέσω AD ή άλλων μηχανισμών ελέγχου ταυτότητας της επιχείρησης και το hostchecking επιβεβαιώνει ότι η συσκευή του είναι ασφαλής.

(4) Μόλις ολοκληρωθεί ο έλεγχος ταυτότητας ενός χρήστη για πρόσβαση στο cloud και πιστοποιηθεί επίσης και η επαρκής ασφάλεια του τερματικού του, το PCS συνδέει τον χρήστη απ' ευθείας με την εφαρμογή ή υπηρεσία στο cloud.

Εναλλακτικά, οι επιχειρήσεις έχουν την επιλογή να προγραμματίσουν η κίνηση των χρηστών να περνάει σε κάθε περίπτωση από το σύστημα PCS έτσι ώστε να μπορεί να γίνεται πρόσθετη επεξεργασία στο Data Center (π.χ. φιλτράρισμα περιεχομένου κλπ).

Μέσα από αυτή την αναλυτική παρουσίαση ενός τελευταίας γενιάς συστήματος τηλεργασίας γίνονται προφανείς οι πλήρεις δυνατότητες ενός πλέγματος λειτουργιών που πρακτικά είναι πολύ υπερκείμενες της τηλεργασίας και μπορεί να υλοποιηθεί όχι μόνο από ανάγκη λόγω των υγειονομικών συνθηκών που επικρατούν παγκοσμίως, αλλά ως στρατηγική για μία πραγματικά ενοποιημένη υποδομή που αφ' ενός επιτρέπει σημαντική βελτιστοποίηση των λειτουργικών εξόδων της επιχείρησης - με εξόχως σημαντικό τη μείωση του φυσικού χώρου και της φιλοξενίας του προσωπικού σε αυτόν, και αφ' ετέρου μία πλατφόρμα συνεργασίας για όλο το οικοσύστημα της επιχείρησης που περιλαμβάνει πέρα από το προσωπικό της τους εξωτερικούς της συμβούλους, τους συνεργάτες, τις θυγατρικές και τα υποκαταστήματά της.

Η τηλεργασία είναι χωρίς αμφιβολία ο τρόπος συνεργασίας του μέλλοντος και ειδικά στην Ελλάδα, που συνεχίζει να έχει σημαντικά χαμηλότερη διείσδυση, αναμένεται να ακολουθήσει γοργότερο ρυθμό έχοντας ως αρωγό και τις σημαντικές επενδύσεις και εξελίξεις στο τηλεπικοινωνιακό περιβάλλον.

Λίγα λόγια για τον αρθρογράφο

Ο κ. **Σταύρος Καραγκιούλογλου** κατάγεται από την Κωνσταντινούπολη και αποφοίτησε από το Γερμανο-Αυστριακό Κολλέγιο St.Georg. Στη συνέχεια σπούδασε Διπλ. Ηλεκτρολόγος-Μηχανολόγος Μηχανικός με ειδικότητα στα δίκτυα τηλεπικοινωνιών στο Technical University RWTH AACHEN Γερμανίας, όπου πήρε και το μεταπτυχιακό του με εργασία την εφαρμογή real-time τηλεματικής στον έλεγχο οδικής κυκλοφορίας. Είναι παντρεμένος και πατέρας δύο παιδιών. Στην τηλεπικοινωνιακή αγορά έχει εμπειρία 30 χρόνια, εκ των οποίων τα περισσότερα στη SIEMENS - στους τομείς εφαρμογής, πωλήσεων και marketing τηλεπικοινωνιακών προϊόντων και υπηρεσιών, όπου κατείχε καίριες θέσεις, μεταξύ αυτών και τη θέση του Διευθυντή Πωλήσεων Τηλεπικοινωνιακών Συστημάτων, Προϊόντων και Εφαρμογών. Το 2003 ίδρυσε και μετέχει ενεργά ως Διευθύνων Σύμβουλος στην διοίκηση της UNITED TELECOM AE, μία εταιρία που δραστηριοποιείται εντατικά στην παροχή και την ασφάλεια των κινητών, ασύρματων και σταθερών επιχειρησιακών δικτύων υπολογιστών, τηλεφωνίας και πολυμέσων δημόσιας και ιδιωτικής χρήσης καθώς και στην ασφάλεια των ηλεκτρονικών συναλλαγών, των δεδομένων και του Cloud.