ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Οικονομικό Πανεπιστήμιο Αθηνών

Τμήμα Πληροφορικής

Τίτλος Διπλωματικής Εργασίας

«Zero Trust Security Models: A Theoretical and Bibliographic Analysis of Identity-Centric Cybersecurity in Modern Organizations»

Φοιτητής:

Μαρσέλης Κωνσταντίνος

Αριθμός Μητρώου:

p3312311

Επιβλέπων Καθηγητής:

Ξυλωμένος Γιώργος

Πρόγραμμα Μεταπτυχιακών Σπουδών:

Ανάπτυξη & Ασφάλεια Πληροφοριακών Συστημάτων

Ημερομηνία:

Αθήνα, Δεκέμβριος 2025

ΕΥΧΑΡΙΣΤΙΕΣ

Στο πλαίσιο του μεταπτυχιακού προγράμματος σπουδών «Ανάπτυξη και Ασφάλεια Πληροφοριακών Συστημάτων» του τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών ολοκληρώνεται ο κύκλος σπουδών με την εκπόνηση της παρούσας διπλωματικής εργασίας.

Θα ήθελα να ευχαριστήσω την οικογένεια μου για την στήριξη τους κατά την διάρκεια του μεταπτυχιακού.

Επίσης, θα ήθελα να ευχαριστήσω την εταιρεία «Entersoftone» για την εμπιστοσύνη που μου έδειξε και την επένδυση που έκανε στο πρόσωπο μου για το πρόγραμμα του μεταπτυχιακού.

Ακόμη, θα ήθελα να ευχαριστήσω τον καθηγητή κύριο Ξύλωμενο Γιώργο για την επίβλεψη της διπλωματικής και την προσφορά του συμβουλευτικά και επιστημονικά για την ολοκλήρωση της. Καθώς, επίσης, και τον κύριο Φωτίου Νίκο για την συμβουλευτική προσφορά στην διπλωματική εργασία.

Τέλος, θα ήθελα να ευχαριστήσω όλους τους ανθρώπους, που βοήθησαν στην διάρκεια του μεταπτυχιακού σε διαφορετικές πτυχές του τόσο στο διδακτικό μέρος όσο και στο συμβουλευτικό με ειδική μνεία στον κύριο Βούλγαρη Σπύρο, ως υπεύθυνο καθηγητή μου στο πρόγραμμα του μεταπτυχιακού για την συμβολή του και την κυρία Μάρα Ολυμπία στην γραμματεία του μεταπτυχιακού καθώς και τον Χρηστογιάννη Καλεμάι, διδακτορικό, για τις πολύτιμες συμβουλές του.

ΠΕΡΙΛΗΨΗ

Η αρχιτεκτονική Zero Trust αποτελεί μία από τις σημαντικότερες σύγχρονες εξελίξεις στον χώρο της κυβερνοασφάλειας, μετατοπίζοντας το επίκεντρο από την παραδοσιακή περιμετρική προστασία προς ένα μοντέλο συνεχούς επαλήθευσης και ταυτοκεντρικής ασφάλειας. Η παρούσα εργασία εξετάζει θεωρητικά και βιβλιογραφικά τις αρχές, τις τεχνολογίες και τα ερευνητικά μοντέλα που πλαισιώνουν το Zero Trust, εστιάζοντας ειδικότερα στον ρόλο των IAM συστημάτων, της πολυπαραγοντικής ταυτοποίησης, της ταυτοποίησης με βάση το ρίσκο, της tokenization και των σύγχρονων πρωτοκόλλων ταυτοποίησης και εξουσιοδότησης. Επιπλέον, αναλύονται τα κύρια μοντέλα αναφοράς, όπως το BeyondCorp της Google και το NIST SP 800-207, τα οποία έχουν συμβάλει στην τυποποίηση και καθιέρωση των αρχών Zero Trust σε διεθνές επίπεδο.

Ιδιαίτερη έμφαση δίνεται στις οργανωσιακές προκλήσεις υιοθέτησης, στις τεχνολογικές δυσκολίες, στα όρια της υπάρχουσας βιβλιογραφίας και στις κατευθύνσεις για μελλοντική έρευνα. Τα ευρήματα δείχνουν ότι το Zero Trust δεν αποτελεί ένα στατικό τεχνικό πλαίσιο, αλλά μία εξελισσόμενη φιλοσοφία ασφάλειας που απαιτεί διαρκή προσαρμογή, υψηλή τεχνολογική ωριμότητα και βαθιά οργανωσιακή μεταμόρφωση. Η βιβλιογραφική σύνθεση αναδεικνύει πως το Zero Trust προσφέρει σημαντικά πλεονεκτήματα στην ασφάλεια, στη συμμόρφωση και στη διακυβέρνηση δεδομένων, συγχρόνως όμως υπογραμμίζει την ανάγκη περαιτέρω εμπειρικής έρευνας.

Λέξεις-Κλειδιά:

Zero Trust, κυβερνοασφάλεια, continuous verification, IAM, MFA, NIST SP 800-207, BeyondCorp, risk-based authentication, tokenization, identity-centric security

ABSTRACT

The Zero Trust architecture has emerged as one of the most influential paradigms in modern cybersecurity, shifting the focus away from traditional perimeter-based defenses toward a model rooted in continuous verification and identity-centric security. This thesis provides a theoretical and bibliographic examination of Zero Trust principles, technologies, and frameworks, with particular emphasis on Identity and Access Management (IAM), multi-factor authentication, risk-based authentication, tokenization, and modern authorization and identity protocols. Additionally, the study analyzes major reference models, including Google's BeyondCorp and NIST SP 800-207, which have significantly shaped the global understanding and standardization of Zero Trust practices.

The discussion extends to organizational and technological challenges associated with the adoption of Zero Trust, highlighting limitations in current research and outlining future directions for empirical and theoretical exploration. Our findings indicate that Zero Trust is not a static technical solution but a dynamic security philosophy that requires continuous adaptation, advanced technological maturity, and profound organizational transformation. The literature synthesis reveals substantial benefits for security, compliance, and data governance, while also underscoring the need for further large-scale empirical studies.

Keywords:

Zero Trust, cybersecurity, continuous verification, identity-centric security, IAM, MFA, NIST SP 800-207, BeyondCorp, risk-based authentication, tokenization

Περιεχόμενα

Κεφάλαιο 1. Εισαγωγή

1.1 Το πρόβλημα της σύγχρονης κυβερνοασφάλειας

Η σύγχρονη κυβερνοασφάλεια αντιμετωπίζει μια θεμελιώδη κρίση αξιοπιστίας, καθώς το παραδοσιακό μοντέλο προστασίας που βασίζεται στο perimeter security αποδεικνύεται ανεπαρκές απέναντι σε ένα τοπίο απειλών που έχει αλλάξει ριζικά. Το μοντέλο αυτό στηρίχθηκε στη λογική ότι οι χρήστες και οι συσκευές εντός του εταιρικού δικτύου είναι εγγενώς αξιόπιστοι, ενώ όσοι βρίσκονται εκτός είναι δυνητικά επικίνδυνοι. Η πρόσβαση βασίζεται στη γεωγραφική ή λογική θέση του χρήστη σε σχέση με το εταιρικό firewall, την περίμετρο, μια προσέγγιση που πλέον δεν μπορεί να ανταποκριθεί στη δυναμική και κατανεμημένη φύση των σύγχρονων πληροφοριακών συστημάτων (ACT-IAC, 2019). Η διάδοση της απομακρυσμένης εργασίας, των cloud υπηρεσιών, των φορητών συσκευών και της πρόσβασης από πολλαπλά, μη ελεγχόμενα περιβάλλοντα υπονόμευσε τον πυρήνα του perimeter-based security, καθιστώντας το όριο «εντός–εκτός» ασαφές, ή ακόμη και ανύπαρκτο.

Παράλληλα, η έκρηξη των κυβερνοεπιθέσεων υψηλής πολυπλοκότητας έχει αποκαλύψει σοβαρές αδυναμίες στα παραδοσιακά μοντέλα άμυνας. Οι επιθέσεις supply chain, όπως αυτές που επηρέασαν κρίσιμες υποδομές και κυβερνητικές υπηρεσίες, δείχνουν ότι οι εισβολείς μπορούν να αποκτήσουν αξιόπιστη πρόσβαση ακόμη και μέσω «νόμιμων» διαύλων, παρακάμπτοντας την περίμετρο και εκμεταλλευόμενοι την έλλειψη συνεχούς ταυτοποίησης εντός του δικτύου (Golden et al., 2021). Η αυξανόμενη εξάρτηση από cloud-based εφαρμογές, microservices, APIs και υβριδικές υποδομές σημαίνει ότι τα δεδομένα και οι πόροι δεν βρίσκονται πλέον εντός ενός ελεγχόμενου περιβάλλοντος· αντίθετα, διαμοιράζονται σε πολλαπλούς παρόχους και τοποθεσίες, καθιστώντας την ασφάλεια μια πολυπαραγοντική, συνεχώς μεταβαλλόμενη πρόκληση (Deloitte, 2021).

Επιπλέον, οι κυβερνοεγκληματίες έχουν εξελίξει τις τεχνικές τους, υιοθετώντας πολύ πιο σύνθετες μορφές επιθέσεων όπως lateral movement, credential compromise, privilege escalation και advanced persistent threats. Η δυνατότητα των εισβολέων να κινούνται πλαγίως μέσα σε ένα δίκτυο μόλις αποκτήσουν αρχική πρόσβαση, ανατρέπει την παραδοχή ότι η προστασία του perimeter επαρκεί για την αποτροπή σοβαρών παραβιάσεων. Μελέτες δείχνουν ότι το μεγαλύτερο ποσοστό ζημιών προκύπτει **μετά** την είσοδο του επιτιθέμενου

στο δίκτυο, όταν πλέον η εσωτερική περιοχή λειτουργεί με default εμπιστοσύνη (Buck et al., 2021). Αυτό αναδεικνύει το κεντρικό πρόβλημα των legacy architectures: αντιμετωπίζουν τον εσωτερικό χώρο ως «ασφαλή ζώνη» και αδυνατούν να εφαρμόσουν granular access control σε πραγματικό χρόνο.

Η αυξανόμενη χρήση απομακρυσμένων συστημάτων, τρίτων παρόχων και εφαρμογών cloud έχει επίσης οδηγήσει σε σημαντική διασπορά των διαύλων πρόσβασης, πολλαπλασιάζοντας τα σημεία εισόδου και καθιστώντας δυσκολότερη την εφαρμογή ενιαίων πολιτικών ασφάλειας (Microsoft, 2021b). Μελέτες αναφέρουν ότι πάνω από το 80% των οργανισμών λειτουργούν πλέον σε hybrid ή multi-cloud περιβάλλοντα, όπου η εφαρμογή παραδοσιακών perimeter controls είναι ουσιαστικά αδύνατη, καθώς η περίμετρος δεν μπορεί να οριστεί ούτε φυσικά ούτε λογικά (CISA, 2021). Η έλλειψη ενιαίου ελέγχου σε τέτοια κατανεμημένα συστήματα δημιουργεί κενά ασφαλείας που είναι δύσκολο να εντοπιστούν και ακόμα δυσκολότερο να αντιμετωπιστούν αποτελεσματικά.

Παράλληλα, το κόστος των κυβερνοεπιθέσεων αυξάνεται εκθετικά. Η βιβλιογραφία δείχνει ότι οι παραβιάσεις δεδομένων οφείλονται συχνά σε ελλιπή διαχείριση ταυτοτήτων, πλαστές πιστοποιήσεις και μη ασφαλή συστήματα πρόσβασης, τα οποία οι επιτιθέμενοι εκμεταλλεύονται για να αποκτήσουν πρόσβαση σε κρίσιμα περιουσιακά στοιχεία (Adahman et al., 2022). Η ανεπαρκής επιβολή του least privilege αποτελεί έναν από τους σημαντικότερους παράγοντες που αυξάνουν τη σοβαρότητα των επιθέσεων, καθώς επιτρέπει σε κακόβουλους χρήστες να αξιοποιούν δικαιώματα που δεν θα έπρεπε να διαθέτουν.

Το ζήτημα περιπλέκεται περαιτέρω από την αυξανόμενη εξάρτηση των οργανισμών από εξωτερικούς συνεργάτες, τρίτους παρόχους και μηχανισμούς διασύνδεσης με πολλαπλά APIs, όπου η εμπιστοσύνη μεταφέρεται σε οντότητες που συχνά δεν ελέγχονται πλήρως. Σχετικές αναφορές δείχνουν ότι σημαντικό ποσοστό παραβιάσεων προέρχεται από compromise τρίτων υπηρεσιών ή κακόβουλη χρήση έγκυρων διαπιστευτηρίων (Campbell, 2020). Στο ίδιο πλαίσιο, η αύξηση των επιθέσεων phishing και credential-based καταδεικνύει ότι η ταυτοποίηση βασισμένη απλώς σε username και password δεν επαρκεί, καθώς οι περισσότεροι μηχανισμοί παραβιάζονται μέσα σε λίγα λεπτά, με συνέπειες που μπορεί να διαρκέσουν μήνες (Yeoh et al., 2021).

Το παραδοσιακό μοντέλο ασφάλειας αποδεικνύεται ανεπαρκές και από την αδυναμία του να προσφέρει διαρκή ορατότητα και παρακολούθηση των ροών δεδομένων. Επειδή

βασίζεται στην υπόθεση ότι όποιος βρίσκεται εντός του δικτύου είναι «καλός», δεν υλοποιεί εκτεταμένη και συνεχόμενη επιτήρηση του δικτύου για ανωμαλίες, με αποτέλεσμα οι επιθέσεις να παραμένουν αθέατες για μεγάλα χρονικά διαστήματα. Η έλλειψη granular logging και auditability εντός των εσωτερικών συστημάτων αποτελεί σημαντικό κίνδυνο σύμφωνα με σχετικές μελέτες (Golden et al., 2021).

Το πρόβλημα της σύγχρονης κυβερνοασφάλειας δεν αφορά μόνο την τεχνολογική αδυναμία των παλαιών μοντέλων, αλλά την αναντιστοιχία τους με έναν κόσμο όπου η πρόσβαση είναι συνεχής, πολυτοπική και μεταβλητή. Η «εμπιστοσύνη από προεπιλογή» που χαρακτήριζε το perimeter security αντιστρατεύεται το περιβάλλον απειλών του 21ου αιώνα, όπου οι εισβολείς μπορούν να αξιοποιήσουν οποιοδήποτε κανάλι για να διεισδύσουν σε κρίσιμα συστήματα. Η διαπίστωση αυτή οδήγησε στην ανάδειξη ενός νέου μοντέλου ασφάλειας, του Zero Trust, το οποίο απορρίπτει την έννοια της ζώνης εμπιστοσύνης και βασίζεται στη συνεχή και δυναμική επαλήθευση κάθε αιτήματος, συσκευής και ταυτότητας.

1.2 Το θεωρητικό κενό και η ανάγκη για Zero Trust

Παρά την εντυπωσιακή εξέλιξη των τεχνολογιών κυβερνοασφάλειας τις τελευταίες δεκαετίες, η διεθνής βιβλιογραφία καταδεικνύει ότι εξακολουθεί να υπάρχει ένα ουσιαστικό θεωρητικό κενό ανάμεσα στα υφιστάμενα μοντέλα ασφάλειας και στις πραγματικές συνθήκες λειτουργίας των πληροφοριακών συστημάτων. Το κενό αυτό συνδέεται κυρίως με τη μετάβαση από συγκεντρωτικά, περιμετρικά μοντέλα προστασίας σε κατανεμημένα, δυναμικά περιβάλλοντα, όπου οι παραδοχές του παρελθόντος δεν ισχύουν (ACT-IAC, 2019). Η παραδοσιακή προσέγγιση αντιμετώπιζε τη δικτυακή περίμετρο ως το θεμελιώδες όριο ασφάλειας, στη βάση της ιδέας ότι η τοποθεσία ενός χρήστη ή μιας συσκευής μπορεί να καθορίσει αν είναι αξιόπιστος. Ωστόσο, η ανάπτυξη cloud υποδομών, απομακρυσμένης πρόσβασης και mobile εργασίας έχει καταστήσει την έννοια της περιμέτρου ασαφή και συχνά μη υλοποιήσιμη στην πράξη (Deloitte, 2021).

Η βιβλιογραφία επισημαίνει ότι το μεγαλύτερο θεωρητικό πρόβλημα των legacy architectures είναι η υπόθεση της εγγενούς εμπιστοσύνης: η ιδέα ότι οτιδήποτε βρίσκεται «εντός» ενός δικτύου είναι ασφαλές. Αυτή η υπόθεση δεν ανταποκρίνεται πλέον σε ένα περιβάλλον όπου οι επιθέσεις βασίζονται σε παραβιασμένα διαπιστευτήρια (credentials), πλάγια κίνηση (lateral movement) και εκμετάλλευση νόμιμων διαύλων πρόσβασης (Campbell, 2020). Ερευνητικές εργασίες επισημαίνουν ότι οι περισσότεροι επιτιθέμενοι δεν

χρειάζονται εξωτερική παραβίαση του perimeter, αλλά αξιοποιούν έγκυρα διαπιστευτήρια, επιτρέποντας τους να μετακινηθούν πλαγίως μέσα στο δίκτυο χωρίς να εντοπιστούν (Buck et al., 2021). Αυτό σημαίνει ότι η εμπιστοσύνη που αποδίδεται σε εσωτερικούς χρήστες και συστήματα δεν έχει πλέον θεωρητικό υπόβαθρο και δημιουργεί μια εσωτερική επιφάνεια επίθεσης εξίσου επικίνδυνη με την εξωτερική.

Παράλληλα, η βιβλιογραφία γύρω από την κυβερνοασφάλεια έχει αναπτύξει πληθώρα μοντέλων προστασίας, αλλά τα περισσότερα δεν καταφέρνουν να προσαρμοστούν σε ένα περιβάλλον όπου η ταυτότητα, το πλαίσιο και η συμπεριφορά αποτελούν σημαντικότερους δείκτες κινδύνου από τη γεωγραφική ή δικτυακή τοποθεσία (Golden et al., 2021). Η ανάγκη για μηχανισμούς συνεχούς επαλήθευσης αναδεικνύεται σε πολλές μελέτες, καθώς οι σύγχρονες επιθέσεις εξελίσσονται σε πραγματικό χρόνο και απαιτούν ανάλογα δυναμικούς μηχανισμούς αντίδρασης (CISA, 2021).

Ένα ακόμη στοιχείο του θεωρητικού κενού αφορά τη διαχείριση ταυτοτήτων και την εφαρμογή πολιτικών granular authorization. Η πλειονότητα των οργανισμών εξακολουθεί να βασίζεται σε συστήματα που απονέμουν υπερβολικά ευρεία δικαιώματα πρόσβασης λόγω λειτουργικών περιορισμών, ιστορικών ρυθμίσεων ή ανεπαρκών μοντέλων role-based πρόσβασης (Adahman et al., 2022). Η βιβλιογραφία δείχνει ότι η απουσία μοντέλων βασισμένων στο least privilege δημιουργεί σημαντικά κενά ασφάλειας, καθώς ακόμη και νόμιμοι χρήστες μπορούν να αποτελέσουν κίνδυνο όταν διαθέτουν περισσότερα δικαιώματα από όσα απαιτούνται για τη λειτουργία τους (Ferretti et al., 2021).

Εξίσου σημαντικό είναι το κενό που εντοπίζεται στη θεωρία γύρω από την ορατότητα και την εποπτεία του δικτύου. Τα συμβατικά μοντέλα δεν περιλαμβάνουν ενσωματωμένη την ανάγκη για λεπτομερή παρακολούθηση της δραστηριότητας χρηστών και υπηρεσιών, αφήνοντας κενά που επιτρέπουν σε επιθέσεις να εξελίσσονται χωρίς εντοπισμό για μεγάλα χρονικά διαστήματα (ACT-IAC, 2019). Η βιβλιογραφία υπογραμμίζει ότι τα σύγχρονα συστήματα απαιτούν πλήρεις μηχανισμούς auditing, logging και behavioral analytics, ώστε οι επιθέσεις να ανιχνεύονται όχι βάσει τοποθεσίας αλλά βάσει ανωμαλιών και αλλαγών στην κανονική συμπεριφορά (Microsoft, 2021b).

Το Zero Trust αναδύεται ως απάντηση στο παραπάνω θεωρητικό αδιέξοδο. Πρόκειται για ένα μοντέλο που απορρίπτει την ιδέα της εγγενούς εμπιστοσύνης και αντιμετωπίζει κάθε χρήστη, συσκευή ή υπηρεσία ως δυνητικά επικίνδυνο μέχρι αποδείξεως του αντιθέτου (Cunningham, 2018). Η προσέγγιση αυτή εδράζεται σε σύγχρονα θεωρητικά υποδείγματα

που επισημαίνουν ότι η ασφάλεια δεν μπορεί να είναι στατική ούτε να βασίζεται σε μοντέλα «μέσα–έξω», αλλά πρέπει να αποτελεί μια συνεχή, δυναμική διαδικασία επαλήθευσης της ταυτότητας, του κινδύνου και του πλαισίου πρόσβασης (CISA, 2021). Το Zero Trust έρχεται να καλύψει το κενό που δημιουργήθηκε από τη μετάβαση σε cloud, hybrid και mobile περιβάλλοντα, ενσωματώνοντας αρχές όπως τα ελάχιστα προνόμια (least priviledge), η μικρο-τμηματοποίηση, η συνεχής ταυτοποίηση και η πολιτική βασισμένη σε context-aware signals (Golden et al., 2021).

Η ανάγκη για Zero Trust ενισχύεται και από τη βιβλιογραφία που εξέτασε την οικονομική διάσταση των παραβιάσεων. Η αύξηση του κόστους ανά περιστατικό κυβερνοεπίθεσης, ιδιαίτερα όταν αυτή αφορά παραβίαση ταυτοτήτων, καταδεικνύει ότι τα παραδοσιακά μοντέλα δεν παρέχουν στοιχεία βιωσιμότητας ούτε προστασίας υψηλής κρισιμότητας (Adahman et al., 2022). Επιπλέον, μελέτες όπως αυτή των Buck et al. (2021) αναδεικνύουν ότι η επιστημονική κοινότητα δεν έχει ακόμη καταλήξει σε ένα ενιαίο θεωρητικό πλαίσιο που να απαντά επαρκώς στις σύγχρονες απειλές, καθιστώντας το Zero Trust ένα θεωρητικά ατελές αλλά αναγκαίο μοντέλο ασφάλειας.

Το θεωρητικό κενό προκύπτει από τη σύγκρουση μεταξύ παρωχημένων παραδοχών ασφάλειας και των απαιτήσεων ενός περιβάλλοντος όπου η πρόσβαση είναι κατανεμημένη, δυναμική και πολυεπίπεδη. Το Zero Trust δεν αποτελεί απλώς μια τεχνολογική καινοτομία, αλλά μια αναλυτική απάντηση σε αυτή τη θεμελιώδη ασυμφωνία, προτείνοντας ένα νέο τρόπο κατανόησης της εμπιστοσύνης, της πρόσβασης και της προστασίας σε σύγχρονα πληροφοριακά οικοσυστήματα.

1.3 Σκοπός της μελέτης

Ο σκοπός της παρούσας μελέτης είναι να διερευνήσει, σε καθαρά βιβλιογραφικό επίπεδο, το θεωρητικό υπόβαθρο, την αναγκαιότητα και την εξέλιξη της αρχιτεκτονικής Zero Trust ως απάντηση στα κενά και τις αδυναμίες των παραδοσιακών μοντέλων κυβερνοασφάλειας. Η μελέτη αποσκοπεί στο να αναδείξει γιατί το Zero Trust δεν αποτελεί απλώς μια τεχνική προσέγγιση αλλά μια συνολική μεταστροφή στην αντίληψη περί εμπιστοσύνης, πρόσβασης και προστασίας πληροφοριακών συστημάτων σε πολυεπίπεδα, κατανεμημένα και δυναμικά περιβάλλοντα.

Σε αντίθεση με τις κλασικές αρχιτεκτονικές που βασίζονται στην περιμετρική ασφάλεια, το Zero Trust εστιάζει στη συνεχή επαλήθευση και στον έλεγχο πρόσβασης ανεξάρτητα από τη

δικτυακή τοποθεσία, δημιουργώντας μια διαφοροποιημένη επιστημονική προσέγγιση η οποία επιδιώκει να απαντήσει στα δομικά προβλήματα που αναφέρονται εκτενώς στη σύγχρονη βιβλιογραφία (ACT-IAC, 2019· Buck et al., 2021). Η μελέτη επιδιώκει να εξετάσει τον τρόπο με τον οποίο οι θεμελιώδεις αρχές του Zero Trust, όπως η κατάργηση της εγγενούς εμπιστοσύνης, η εφαρμογή του least privilege και η χρήση μηχανισμών continuous verification, απαντούν στις σύγχρονες απειλές που χαρακτηρίζονται από lateral movement, credential compromise και επιθέσεις υψηλής κρισιμότητας (Golden et al., 2021).

Επιπλέον, ένας βασικός στόχος της μελέτης είναι η χαρτογράφηση του θεωρητικού τοπίου γύρω από το Zero Trust, ώστε να καταδειχθεί πώς κορυφαίοι οργανισμοί – όπως οι Forrester, Deloitte, Microsoft, CISA και NIST – έχουν ερμηνεύσει και αποτυπώσει το μοντέλο μέσα από οδηγούς υλοποίησης, μοντέλα ωριμότητας και πρακτικά frameworks (CISA, 2021· Cunningham, 2018· Turner et al., 2021). Η αποτύπωση αυτή είναι απαραίτητη ώστε να γίνει εμφανές ότι το Zero Trust δεν έχει ακόμη αποκρυσταλλωθεί σε μία ενιαία θεωρητική φόρμα, αλλά παραμένει ένα εξελισσόμενο εννοιολογικό πλαίσιο με διαφορετικές προσεγγίσεις και πρακτικές εφαρμογής, γεγονός που συνιστά βασικό κενό στη διεθνή βιβλιογραφία (Buck et al., 2021).

Η μελέτη επιδιώκει επίσης να αναδείξει τα κίνητρα που καθιστούν αναγκαία την υιοθέτηση του Zero Trust. Μεταξύ αυτών περιλαμβάνονται οι αδυναμίες του perimeter-based security, η κατακόρυφη άνοδος των επιθέσεων που βασίζονται σε κλοπή διαπιστευτηρίων, η ραγδαία μετάβαση σε hybrid και multi-cloud περιβάλλοντα, καθώς και η αυξανόμενη ανάγκη για ενιαία, granular και context-aware μοντέλα διαχείρισης πρόσβασης (Deloitte, 2021· Microsoft, 2021b). Η βιβλιογραφική διερεύνηση αποσκοπεί στο να τεκμηριώσει ότι η υιοθέτηση του Zero Trust δεν αποτελεί προαιρετική επιλογή αλλά αναγκαιότητα για οργανισμούς που επιδιώκουν να διατηρήσουν υψηλά επίπεδα ασφάλειας και επιχειρησιακής συνέχειας.

Τέλος, η μελέτη στοχεύει στο να εντοπίσει ερευνητικά κενά και θεωρητικές αδυναμίες στην υπάρχουσα γνώση, προσφέροντας μια συστηματική σύνθεση της βιβλιογραφίας η οποία μπορεί να αποτελέσει βάση για περαιτέρω ακαδημαϊκή έρευνα. Η ανάδειξη αυτών των κενών είναι κρίσιμη, καθώς η εξέλιξη του Zero Trust ως θεωρητικού μοντέλου παραμένει σε εξέλιξη και απαιτεί περισσότερη εμπειρική και εννοιολογική εδραίωση στη διεθνή επιστημονική κοινότητα (Adahman et al., 2022).

Με τον τρόπο αυτό, ο σκοπός της μελέτης είναι διττός: αφενός να χαρτογραφήσει, να συνθέσει και να κρίνει κριτικά τη διαθέσιμη βιβλιογραφία γύρω από το Zero Trust, και αφετέρου να τεκμηριώσει γιατί το Zero Trust αποτελεί σήμερα ένα από τα ελάχιστα συνεκτικά και ρεαλιστικά μοντέλα ασφάλειας, ικανά να ανταποκριθούν στις απαιτήσεις ενός πολυσύνθετου και απρόβλεπτου ψηφιακού οικοσυστήματος.

1.4 Ερευνητικά ερωτήματα

Η συστηματική μελέτη της αρχιτεκτονικής Zero Trust απαιτεί τη διαμόρφωση σαφών ερευνητικών ερωτημάτων που θα καθοδηγήσουν την ανασκόπηση της βιβλιογραφίας και θα οργανώσουν τη θεωρητική ανάλυση του πεδίου. Δεδομένου ότι το Zero Trust αποτελεί μια έννοια η οποία εξακολουθεί να εξελίσσεται και να ερμηνεύεται διαφορετικά από διάφορους οργανισμούς και ερευνητές, η διατύπωση των ερευνητικών ερωτημάτων πρέπει να αντανακλά τόσο τις θεωρητικές ασάφειες όσο και τα εννοιολογικά κενά που επισημαίνονται στη διεθνή βιβλιογραφία (Buck et al., 2021). Τα ερωτήματα που ακολουθούν στοχεύουν στην αποσαφήνιση της εννοιολογικής βάσης του Zero Trust, στην αξιολόγηση της αναγκαιότητάς του και στην κατανόηση της συμβολής του στη σύγχρονη κυβερνοασφάλεια.

Ένα πρώτο βασικό ερώτημα αφορά το ποιο θεωρητικό κενό επιχειρεί να καλύψει το Zero Trust και πώς αυτό το κενό διαμορφώθηκε στο πλαίσιο των μεταβαλλόμενων τεχνολογικών και επιχειρησιακών αναγκών. Η βιβλιογραφία αναδεικνύει ότι τα παραδοσιακά μοντέλα perimeter-based security δεν συμβαδίζουν με τις απαιτήσεις των κατανεμημένων, cloud-native και mobile περιβαλλόντων (ACT-IAC, 2019· Deloitte, 2021). Επομένως, η μελέτη επιδιώκει να απαντήσει στο ερώτημα: *Γιατί τα παραδοσιακά μοντέλα ασφάλειας αποτυγχάνουν να ανταποκριθούν στις σύγχρονες απειλές και πώς το Zero Trust επιδιώκει να καλύψει αυτές τις αδυναμίες*;

Συναφές με το παραπάνω είναι το ερώτημα που αφορά τα θεμελιώδη εννοιολογικά στοιχεία του Zero Trust. Η βιβλιογραφία παρουσιάζει πολλαπλές εκδοχές της αρχιτεκτονικής, από το Zero Trust eXtended (ZTX) μοντέλο της Forrester έως το NIST SP 800-207, γεγονός που δημιουργεί μη πλήρως ενοποιημένες αντιλήψεις για το τι ακριβώς αποτελεί Zero Trust σε θεωρητικό επίπεδο (Cunningham, 2018· CISA, 2021). Έτσι, η μελέτη θέτει το ερώτημα: *Ποιες είναι οι κύριες θεωρητικές προσεγγίσεις του Zero Trust και σε ποιο βαθμό συγκλίνουν ή αποκλίνουν μεταξύ τους*;

Ένα τρίτο κρίσιμο ερώτημα αφορά την αποτελεσματικότητα του Zero Trust έναντι των σύγχρονων απειλών. Η αύξηση επιθέσεων lateral movement, credential compromise και cloud-based exploits εγείρει την ανάγκη να εξεταστεί κατά πόσο το Zero Trust μπορεί να μειώσει ουσιαστικά την επιφάνεια επίθεσης και να περιορίσει τη δυνατότητα των επιτιθέμενων να κινηθούν ανεμπόδιστα μέσα σε εταιρικά δίκτυα (Campbell, 2020· Golden et al., 2021). Έτσι, τίθεται το ερώτημα: *Σε ποιο βαθμό η εφαρμογή των αρχών του Zero Trust ενισχύει την ανθεκτικότητα των οργανισμών απέναντι σε σύγχρονες και εξελιγμένες κυβερνοαπειλές*;

Επιπλέον, σημαντικό ερευνητικό ερώτημα αφορά τη σχέση μεταξύ Zero Trust και διαχείρισης ταυτοτήτων και πρόσβασης (IAM). Η βιβλιογραφία επισημαίνει ότι τα ζητήματα υπερβολικών δικαιωμάτων, ελλιπούς επιβολής least privilege και ανεπαρκών μηχανισμών ταυτοποίησης αποτελούν βασικούς παράγοντες που αυξάνουν τον κίνδυνο παραβίασης συστημάτων (Adahman et al., 2022· Ferretti et al., 2021). Επομένως, η μελέτη διερευνά: *Πώς το Zero Trust μετασχηματίζει τον τρόπο με τον οποίο οι οργανισμοί προσεγγίζουν τη διαχείριση ταυτοτήτων, την εξουσιοδότηση και την πρόσβαση σε κρίσιμα περιουσιακά στοιχεία*;

Ένα ακόμη σημαντικό ερώτημα αφορά το βαθμό ωριμότητας και ετοιμότητας των οργανισμών να υιοθετήσουν πλήρως το Zero Trust. Ορισμένα μοντέλα ωριμότητας, όπως αυτά της Microsoft και της CISA, επιχειρούν να ορίσουν επίπεδα υιοθέτησης, αλλά η βιβλιογραφία δείχνει ότι η εφαρμογή Zero Trust σε μεγάλο οργανωσιακό εύρος αποτελεί μια σύνθετη διαδικασία με πολλαπλές προκλήσεις (Microsoft, 2021b· CISA, 2021). Συνεπώς, το ερώτημα που τίθεται είναι: *Ποιες είναι οι οργανωτικές, τεχνικές και επιχειρησιακές προϋποθέσεις για την επιτυχή υιοθέτηση του Zero Trust σε πραγματικά περιβάλλοντα*;

Τέλος, η μελέτη στοχεύει να απαντήσει στο ερώτημα που αφορά τα ερευνητικά κενά του πεδίου. Παρά την αυξανόμενη δημοτικότητα του Zero Trust, η επιστημονική κοινότητα αναγνωρίζει ότι το μοντέλο παραμένει θεωρητικά ελλιπές και πρακτικά μη πλήρως αποσαφηνισμένο (Buck et al., 2021). Αυτό οδηγεί στο κρίσιμο ερώτημα: *Ποια είναι τα κυριότερα θεωρητικά και πρακτικά κενά στη σύγχρονη έρευνα γύρω από το Zero Trust, και ποιες κατευθύνσεις ενδείκνυνται για μελλοντική μελέτη*;

Τα ερευνητικά ερωτήματα εστιάζουν στην κατανόηση του Zero Trust ως θεωρητικού μοντέλου, στην αποτίμηση της αποτελεσματικότητάς του και στην αποσαφήνιση των

συνθηκών και των προκλήσεων εφαρμογής του, αποτελώντας έναν άξονα που οργανώνει ολόκληρη τη βιβλιογραφική ανάλυση της παρούσας μελέτης.

1.5 Μεθοδολογία βιβλιογραφικής ανασκόπησης

Η παρούσα μελέτη βασίζεται αποκλειστικά σε βιβλιογραφική ανασκόπηση, με στόχο τη συστηματική καταγραφή, αξιολόγηση και σύνθεση της ήδη υπάρχουσας γνώσης γύρω από την αρχιτεκτονική Zero Trust. Η μεθοδολογική προσέγγιση ευθυγραμμίζεται με τις οδηγίες που προτείνουν κορυφαίοι μελετητές της ερευνητικής διαδικασίας, όπως οι Creswell και Creswell (2018), και βασίζεται σε δομημένη, πολυεπίπεδη έρευνα επιστημονικών και επαγγελματικών πηγών, συμπεριλαμβανομένων άρθρων, τεχνικών οδηγών, white papers και αναφορών από βιομηχανικούς οργανισμούς.

Η διαδικασία ξεκίνησε με τον εντοπισμό αξιόπιστων πηγών μέσα από ακαδημαϊκές βάσεις δεδομένων όπως Scopus, ScienceDirect και ACM Digital Library, καθώς και μέσω εξειδικευμένων οργανισμών κυβερνοασφάλειας όπως η CISA, το NIST και η Microsoft Security Research. Η αναζήτηση βασίστηκε σε λέξεις-κλειδιά που αντικατοπτρίζουν τον πυρήνα του θεωρητικού αντικειμένου, όπως “Zero Trust Architecture”, “perimeter security limitations”, “identity-based security”, “lateral movement”, “least privilege” και “zero trust maturity models”. Η επιλογή των όρων έγινε με βάση τις προτάσεις μελετητών της ποιοτικής έρευνας, ώστε να διασφαλιστεί η μέγιστη κάλυψη του ερευνητικού πεδίου (Bogner & Menz, 2009· Braun & Clarke, 2019).

Κριτήρια ένταξης αποτέλεσαν η επιστημονική εγκυρότητα, η συνάφεια με το πεδίο, η χρονολογική επικαιρότητα και η σαφής συμβολή στη διαμόρφωση του θεωρητικού πλαισίου. Έγινε συστηματική επιλογή πηγών που δημοσιεύτηκαν κυρίως την τελευταία πενταετία, με εξαίρεση θεμελιώδεις μελέτες που αποτελούν κεντρικό σημείο αναφοράς για την κατανόηση του μοντέλου, όπως τα BeyondCorp papers και τα foundational documents του NIST (Kerman et al., 2020). Στη βιβλιογραφία συμπεριλήφθηκαν, επίσης, white papers και τεχνικές αναφορές από οργανισμούς που έχουν ενεργά συμβάλει στον ορισμό και την εξέλιξη του Zero Trust, όπως η Forrester, η Deloitte και η Netskope (Cunningham, 2018· Deloitte, 2021· Netskope, 2020). Η απόφαση αυτή εναρμονίζεται με τη λογική ότι το Zero Trust αποτελεί ένα υβριδικό πεδίο στο οποίο η θεωρητική και η πρακτική γνώση συνυπάρχουν και συνδιαμορφώνονται.

Η ανάλυση των πηγών έγινε με θεματική προσέγγιση, όπως προτείνεται από τους Braun και Clarke (2019), επιτρέποντας την αναγνώριση μοτίβων, κεντρικών εννοιών και επαναλαμβανόμενων θεματικών όπως η κατάργηση της εμπιστοσύνης by default, η ανάγκη για continuous verification, η σημασία του identity management και ο ρόλος της μικρο-τμηματοποίησης. Η θεματική ανάλυση διευκολύνει τη σύνθεση της γνώσης σε ένα πεδίο όπου η ποικιλία των προσεγγίσεων καθιστά αναγκαία την αναζήτηση εννοιολογικών συγκλίσεων και αποκλίσεων (Buck et al., 2021).

Επιπλέον, αξιοποιήθηκαν οι αρχές της ποιοτικής διερεύνησης που αναφέρονται στη μελέτη των Okoli και Pawlowski (2004), οι οποίοι περιγράφουν τη βιβλιογραφική ανασκόπηση ως μια διαδικασία παραγωγής θεωρητικής γνώσης μέσα από τη συστηματική αποδόμηση και αναδόμηση του υπάρχοντος corpus. Η συγκεκριμένη προσέγγιση κρίθηκε ιδιαίτερα κατάλληλη για τη μελέτη του Zero Trust, καθώς το πεδίο χαρακτηρίζεται από κατακερματισμένη ορολογία, ελλιπή θεωρητικοποίηση και σημαντική επίδραση από μη ακαδημαϊκούς φορείς (Forrester, Microsoft, Deloitte).

Σημαντικό μέρος της μεθοδολογίας αποτέλεσε η συγκριτική αποτίμηση των διαφορετικών μοντέλων Zero Trust, όπως το Zero Trust eXtended (ZTX), το Zero Trust Maturity Model της CISA και η αρχιτεκτονική NIST SP 800-207 (CISA, 2021· Cunningham, 2018). Η ανάλυση στηρίχθηκε στην αντιπαραβολή εννοιολογικών αξόνων μεταξύ αυτών των προσεγγίσεων, ώστε να εντοπιστούν συγκλίσεις, αποκλίσεις και περιοχές που απαιτούν περαιτέρω θεωρητική εμβάθυνση.

Τέλος, ακολουθήθηκε μια συνθετική, ερμηνευτική προσέγγιση για την παραγωγή νέων θεωρητικών συμπερασμάτων, στη βάση των αρχών που έχουν τεθεί από τους Creswell και Creswell (2018). Μέσα από αυτή τη διαδικασία η παρούσα μελέτη δεν περιορίζεται στη συγκέντρωση και παράθεση υφιστάμενων πληροφοριών, αλλά επιχειρεί να αναδείξει τις σχέσεις μεταξύ των εννοιών, να εντοπίσει τα κενά της υπάρχουσας γνώσης και να συμβάλει στη θεωρητική ωρίμανση του Zero Trust.

Με τον τρόπο αυτό, η μεθοδολογική διαδικασία διασφάλισε ότι η ανασκόπηση διεξήχθη με συστηματικότητα, ακαδημαϊκή αυστηρότητα και θεωρητική συνέπεια, επιτρέποντας την παραγωγή μιας αναλυτικής, δομημένης και κριτικά τεκμηριωμένης προσέγγισης για την αρχιτεκτονική Zero Trust.

Κεφάλαιο 2. Παραδοσιακά Μοντέλα Ασφάλειας Δικτύων

2.1 Perimeter-based security: ιστορική εξέλιξη

Η ιστορική εξέλιξη της ασφάλειας των πληροφοριακών συστημάτων είναι στενά συνδεδεμένη με το μοντέλο της περιμετρικής προστασίας, γνωστό ως perimeter-based security. Το μοντέλο αυτό κυριάρχησε από τις απαρχές της εμπορικής πληροφορικής τη δεκαετία του 1980 έως και τις αρχές της δεκαετίας του 2010, αντανακλώντας μια εποχή κατά την οποία οι οργανισμοί λειτουργούσαν σε αυστηρά οριοθετημένα, κεντρικοποιημένα δίκτυα, με ελάχιστη εξωτερική αλληλεπίδραση. Η βασική του φιλοσοφία στηρίχθηκε στην υπόθεση ότι το εταιρικό δίκτυο αποτελεί έναν «ασφαλή χώρο», ο οποίος πρέπει να προστατεύεται από εξωτερικούς εισβολείς, ενώ οι χρήστες και οι συσκευές εντός της περιμέτρου θεωρούνται εγγενώς αξιόπιστοι (ACT-IAC, 2019).

Στην πρώτη φάση της ανάπτυξής του, το perimeter security διαμορφώθηκε ως φυσική και λογική επέκταση των εταιρικών firewall, τα οποία υιοθετήθηκαν ευρέως στις αρχές της δεκαετίας του 1990. Τα πρώτα firewall λειτουργούσαν ως πύλες που φιλτράρουν την εισερχόμενη κίνηση με βάση στατικές λίστες επιτρεπόμενων και μη επιτρεπόμενων συνδέσεων. Το μοντέλο αυτό ανταποκρινόταν στις τότε τεχνολογικές συνθήκες, όπου η επιχειρησιακή δραστηριότητα περιοριζόταν σε μικρότερα, κλειστά δίκτυα με περιορισμένη ανάγκη εξωτερικής πρόσβασης. Η αντιμετώπιση του κινδύνου ήταν απλουστευμένη: ο «εχθρός» βρισκόταν εκτός δικτύου, ενώ το «εσωτερικό» περιβάλλον ήταν ασφαλές από τη φύση του.

Καθώς οι οργανισμοί εισήλθαν στη δεύτερη φάση της ψηφιακής τους ωρίμανσης, στη δεκαετία του 2000, το perimeter-based security ενισχύθηκε με τεχνολογίες όπως IDS, VPNs και network access control λύσεις. Η ανάπτυξη των εικονικών ιδιωτικών δικτύων (VPN) αποτέλεσε ιδιαίτερα σημαντική εξέλιξη, καθώς επέτρεψε σε απομακρυσμένους χρήστες να «εισέρχονται» εικονικά στην εσωτερική περίμετρο, αποκτώντας δικαιώματα αντίστοιχα με εκείνα ενός χρήστη εντός του φυσικού εταιρικού χώρου. Ωστόσο, η ευρεία υιοθέτηση των VPN ενίσχυσε και τα δομικά προβλήματα του perimeter model, καθώς η άπαξ είσοδος στο δίκτυο θεωρείτο επαρκής για τη χορήγηση πλήρους πρόσβασης, χωρίς περαιτέρω δυναμική επαλήθευση ή έλεγχο κινδύνου (Cunningham, 2018).

Η τρίτη φάση εξέλιξης του perimeter security συνέπεσε με την εκθετική αύξηση του Διαδικτύου, την υιοθέτηση των cloud υπηρεσιών και την έλευση του mobility. Η μετατόπιση αυτή έφερε στο προσκήνιο δομικές αδυναμίες του παραδοσιακού μοντέλου. Οι οργανισμοί πλέον λειτουργούσαν σε περιβάλλοντα όπου χρήστες, δεδομένα και εφαρμογές βρίσκονται διάσπαρτα σε πολλαπλές τοποθεσίες, εντός και εκτός του εταιρικού χώρου, καθιστώντας την περίμετρο όλο και πιο ασαφή. Παράλληλα, οι επιθέσεις υψηλής πολυπλοκότητας — ιδιαίτερα εκείνες που βασίζονται σε κλοπή διαπιστευτηρίων και lateral movement— αποκάλυψαν ότι η εμπιστοσύνη που παραχωρείται σε οντότητες εντός του δικτύου δεν είναι θεωρητικά δικαιολογημένη (Campbell, 2020).

Η αυξανόμενη κριτική στη βιβλιογραφία επισημαίνει ότι το perimeter-based security απέτυχε να αντιμετωπίσει τις ανάγκες ενός ψηφιακού περιβάλλοντος όπου η πρόσβαση δεν προσδιορίζεται πλέον από τον χώρο, αλλά από την ταυτότητα, το πλαίσιο και τη συμπεριφορά του χρήστη (Deloitte, 2021). Η CISA (2021) επισημαίνει ότι η έννοια της περιμέτρου έχει πλέον διασπαστεί, καθώς οι οργανισμοί λειτουργούν κατά κανόνα σε hybrid και multi-cloud αρχιτεκτονικές, όπου οι παραδοσιακές άμυνες δεν μπορούν να εφαρμοστούν με συνέπεια. Η σύγχρονη έρευνα δείχνει ότι επιθέσεις που εκμεταλλεύονται νόμιμη εσωτερική πρόσβαση —όπως οι supply chain attacks και οι credential-based exploits— καταφέρνουν να παρακάμψουν εντελώς το perimeter model, αποδεικνύοντας την αναποτελεσματικότητά του (Golden et al., 2021).

Στο αποκορύφωμα αυτής της ιστορικής εξέλιξης, το perimeter-based security έχει πλέον θεωρηθεί ανεπαρκές ως πρωταρχικό μοντέλο προστασίας. Οι Buck et al. (2021) επισημαίνουν ότι η βιβλιογραφία συγκλίνει στο συμπέρασμα πως το μεγαλύτερο μέρος των επιθέσεων δεν αποτρέπεται από το firewall ή την περίμετρο, αλλά εξελίσσεται μετά την απόκτηση αρχικής πρόσβασης στο εσωτερικό δίκτυο. Αυτή η διαπίστωση αποτελεί τον καταλύτη που οδήγησε στην εμφάνιση του Zero Trust, ενός μοντέλου που απορρίπτει ριζικά την έννοια του «ασφαλούς εσωτερικού» και θεμελιώνεται στη συνεχή επαλήθευση και στον ελάχιστο βαθμό εμπιστοσύνης.

Η ιστορική πορεία του perimeter-based security αποτυπώνει τη μετάβαση από ένα μοντέλο στατικής, χωρικά οριοθετημένης ασφάλειας σε μια εποχή όπου η εμπιστοσύνη δεν μπορεί πλέον να προεξοφλείται. Η εξέλιξη αυτή καθιστά προφανή την ανάγκη για νέα μοντέλα — όπως το Zero Trust— που ανταποκρίνονται στις πραγματικές συνθήκες λειτουργίας των σύγχρονων πληροφοριακών συστημάτων.

2.2 Το μοντέλο VPN: λειτουργία, πλεονεκτήματα και περιορισμοί

Το Virtual Private Network (VPN) υπήρξε για δεκαετίες η κατεξοχήν λύση για την ασφαλή απομακρυσμένη πρόσβαση σε εταιρικούς πόρους, λειτουργώντας ως κρίσιμο συμπλήρωμα του perimeter-based security. Η βασική αρχή λειτουργίας του VPN είναι η δημιουργία ενός κρυπτογραφημένου τούνελ ανάμεσα στη συσκευή του χρήστη και το εταιρικό δίκτυο, μέσω του οποίου μεταφέρονται όλα τα δεδομένα. Η τεχνολογία αυτή βασίζεται στην παραδοχή ότι, μόλις ο χρήστης ταυτοποιηθεί επιτυχώς και εισέλθει στο VPN, καθίσταται «εσωτερικός» και ως εκ τούτου αξιόπιστος — μια παραδοχή που αντικατοπτρίζει το παραδοσιακό μοντέλο εμπιστοσύνης με βάση την τοποθεσία (ACT-IAC, 2019).

Η λειτουργία του VPN στηρίζεται συνήθως σε πρωτόκολλα όπως IPSec και SSL/TLS, τα οποία εξασφαλίζουν την κρυπτογράφηση του καναλιού επικοινωνίας και την πιστοποίηση της συσκευής ή του χρήστη. Μέσα από αυτούς τους μηχανισμούς, το VPN παρέχει ένα επίπεδο εμπιστευτικότητας και ακεραιότητας που ανταποκρινόταν επαρκώς στα δεδομένα του παρελθόντος, όταν οι απομακρυσμένοι χρήστες αποτελούσαν μειονότητα και το δίκτυο είχε σαφή γεωγραφικά και λογικά όρια. Στο πλαίσιο αυτό, το VPN θεωρήθηκε επανάσταση, καθώς επέτρεψε την ασφαλή τηλεργασία και τη διασύνδεση υποκαταστημάτων χωρίς την ανάγκη φυσικής παρουσίασης στο εταιρικό δίκτυο (Cunningham, 2018).

Με βάση τη βιβλιογραφία, ένα σημαντικό πλεονέκτημα του VPN είναι η δυνατότητα να επεκτείνει με ασφαλή τρόπο το εσωτερικό δίκτυο, επιτρέποντας στους χρήστες να έχουν πρόσβαση σε πόρους σαν να βρίσκονταν εντός της εταιρικής υποδομής. Αυτό ήταν καθοριστικής σημασίας για την εξέλιξη των επιχειρησιακών μοντέλων, καθώς επέτρεψε την ανάπτυξη γεωγραφικά κατανεμημένων οργανισμών χωρίς σημαντική απώλεια ελέγχου ή ασφάλειας (Golden et al., 2021). Επιπλέον, η ευρεία υιοθέτηση των VPN από εμπορικούς και κυβερνητικούς οργανισμούς συνέβαλε στην ωρίμανση των πρακτικών απομακρυσμένης πρόσβασης και στην ανάπτυξη προτύπων που καθόρισαν το τοπίο της ασφαλούς επικοινωνίας.

Ωστόσο, παρά τα προφανή πλεονεκτήματα του, το VPN εμφανίζει σημαντικούς περιορισμούς, ιδιαίτερα όταν τοποθετείται στο πλαίσιο των σύγχρονων υποδομών cloud και κινητικότητας. Ο θεμελιώδης περιορισμός του μοντέλου VPN έγκειται στην παραδοχή της εγγενούς εμπιστοσύνης μόλις ο χρήστης «εισέλθει» στο δίκτυο. Από τη στιγμή που ένας χρήστης πραγματοποιήσει επιτυχημένη ταυτοποίηση, αποκτά συχνά ευρεία ή ακόμη και

πλήρη πρόσβαση στους εσωτερικούς πόρους, χωρίς δυναμικούς ελέγχους που να αξιολογούν το πλαίσιο, τη συμπεριφορά ή τη μεταβολή του κινδύνου (Campbell, 2020). Αυτό το μοντέλο είναι επικίνδυνα ευάλωτο σε επιθέσεις που βασίζονται σε κλοπή διαπιστευτηρίων, καθώς ένας επιτιθέμενος που αποκτά πρόσβαση σε ένα VPN λογαριασμό μπορεί να κινηθεί μέσα στο δίκτυο με τα ίδια δικαιώματα που θα είχε και ο νόμιμος χρήστης. Η βιβλιογραφία επισημαίνει επίσης ότι το VPN είναι ανεπαρκές απέναντι σε επιθέσεις lateral movement, καθώς δεν εφαρμόζει granular έλεγχο πρόσβασης ανά υπηρεσία ή λειτουργία. Αντίθετα, αντιμετωπίζει το δίκτυο ως ενιαίο χώρο, όπου η είσοδος στην περίμετρο ισοδυναμεί με γενικευμένη πρόσβαση (Buck et al., 2021). Οι οργανισμοί που βασίζονται αποκλειστικά στο VPN δυσκολεύονται να ελέγξουν την πρόσβαση σε επιμέρους πόρους, να εφαρμόσουν το least privilege ή να παρακολουθήσουν με λεπτομέρεια τις ενέργειες των χρηστών εντός του δικτύου.

Ένας ακόμη περιορισμός αφορά το scalability και τη διαθεσιμότητα των VPN υποδομών. Η βιβλιογραφία τεκμηριώνει ότι μεγάλοι οργανισμοί αντιμετωπίζουν προβλήματα συμφόρησης, καθυστέρησης και περιορισμένης απόδοσης, ειδικά όταν μεγάλος αριθμός εργαζομένων προσπαθεί να συνδεθεί ταυτόχρονα — κάτι που έγινε εμφανές σε παγκόσμια κλίμακα με την εξάπλωση της τηλεργασίας (Microsoft, 2021b). Το VPN σχεδιάστηκε σε μια εποχή όπου η απομακρυσμένη πρόσβαση ήταν βοηθητική λειτουργία· σήμερα, σε πολλές περιπτώσεις, αποτελεί τον βασικό τρόπο εργασίας, με αποτέλεσμα η αρχιτεκτονική του να μην ανταποκρίνεται στις σύγχρονες συνθήκες.

Τέλος, οι τεχνικές προδιαγραφές του VPN δεν επιτρέπουν την εφαρμογή μηχανισμών real-time policy enforcement, continuous verification ή context-aware access, που αποτελούν κεντρικά στοιχεία της σύγχρονης ασφάλειας. Οι μηχανισμοί του δεν διαθέτουν τη δυνατότητα να αξιολογούν συνεχώς το επίπεδο κινδύνου, να λαμβάνουν αποφάσεις βάσει συμπεριφοράς ή να προσαρμόζουν την πρόσβαση δυναμικά κατά τη διάρκεια μιας συνεδρίας (CISA, 2021). Αυτό σημαίνει ότι το VPN, στην αρχική του σύλληψη, δεν είναι κατάλληλο για την αντιμετώπιση επιθέσεων που εξελίσσονται σε πραγματικό χρόνο και απαιτούν άμεσες παρεμβάσεις.

Το VPN αποτέλεσε τεχνολογική εξέλιξη καθοριστικής σημασίας για την εποχή του, όμως οι αδυναμίες του είναι βαθιά συνυφασμένες με το perimeter-based security — ένα μοντέλο που η σύγχρονη βιβλιογραφία θεωρεί πλέον ανεπαρκές για τις ανάγκες των κατανεμημένων και δυναμικών πληροφοριακών υποδομών. Η ανάδυση του Zero Trust δεν προκύπτει ως

τεχνολογική ανταγωνιστική λύση απέναντι στο VPN, αλλά ως μετασχηματισμός της θεώρησης της πρόσβασης, της εμπιστοσύνης και της ταυτότητας, σε ένα περιβάλλον όπου η είσοδος σε ένα δίκτυο δεν μπορεί πλέον να θεωρείται συνώνυμη με την ασφάλεια.

2.3 Νέες απειλές που υπονομεύουν το παραδοσιακό μοντέλο

Η δραματική διεύρυνση της επιφάνειας επίθεσης τα τελευταία χρόνια έχει αναδείξει μια σειρά από νέες, σύνθετες και πολυεπίπεδες απειλές, οι οποίες υπονομεύουν θεμελιωδώς το παραδοσιακό μοντέλο perimeter-based security και καθιστούν εμφανή την ανάγκη για ριζικά διαφορετικές προσεγγίσεις ασφάλειας. Η φύση των σύγχρονων κυβερνοεπιθέσεων δεν περιορίζεται πλέον σε εξωγενείς προσπάθειες παραβίασης της περιμέτρου, αλλά στοχεύει στη χειραγώγηση της ταυτότητας, την εκμετάλλευση νόμιμων μηχανισμών πρόσβασης και την πλάγια κίνηση εντός του δικτύου, αφήνοντας το παραδοσιακό μοντέλο πλήρως εκτεθειμένο (ACT-IAC, 2019).

Μία από τις σημαντικότερες εξελίξεις είναι η επικράτηση των credential-based επιθέσεων, στις οποίες οι εισβολείς αποκτούν πρόσβαση σε κρίσιμα συστήματα όχι μέσω τεχνικής παραβίασης των firewalls αλλά μέσω κατάχρησης νόμιμων διαπιστευτηρίων. Έρευνες τεκμηριώνουν ότι η πλειονότητα των σύγχρονων επιθέσεων βασίζεται στην εκμετάλλευση κλεμμένων ή παραποιημένων credentials, τα οποία συχνά αποκτώνται μέσω phishing, brute force ή social engineering (Golden et al., 2021). Η ιδιαιτερότητα αυτών των επιθέσεων βρίσκεται στο ότι το σύστημα ταυτοποιεί τον εισβολέα ως έγκυρο χρήστη, επιτρέποντάς του να παρακάμψει την περίμετρο χωρίς να ενεργοποιήσει ανιχνευτικούς μηχανισμούς.

Ένα δεύτερο κρίσιμο φαινόμενο είναι το lateral movement, δηλαδή η δυνατότητα του επιτιθέμενου να μετακινείται ανεμπόδιστα μέσα στο εσωτερικό δίκτυο, από σύστημα σε σύστημα, μόλις αποκτήσει μια αρχική πρόσβαση. Το perimeter security, το οποίο αντιμετωπίζει την εσωτερική περιοχή ως «ασφαλή ζώνη», δεν έχει σχεδιαστεί για να ανιχνεύει ή να εμποδίζει αυτή την κίνηση. Έτσι, ένας εισβολέας μπορεί να εκμεταλλευτεί την πλήρη, ανεξέλεγκτη ορατότητα του VPN ή των εσωτερικών υποδομών για να επεκτείνει την πρόσβασή του και να πλήξει κρίσιμα περιουσιακά στοιχεία (Buck et al., 2021). Η αδυναμία αυτή αποτελεί έναν από τους σοβαρότερους λόγους για τους οποίους οι σύγχρονες επιθέσεις μπορούν να διατηρούνται αόρατες για μεγάλα χρονικά διαστήματα.

Εξίσου προβληματικό είναι το φαινόμενο των επιθέσεων supply chain, οι οποίες βασίζονται στη διείσδυση σε δικτυακούς ή λογισμικούς παρόχους με σκοπό την έμμεση πρόσβαση σε

οργανισμούς υψηλής αξίας. Οι επιθέσεις αυτές αποκαλύπτουν ότι ο κίνδυνος δεν εντοπίζεται πλέον αποκλειστικά «εκτός» του οργανισμού αλλά ενσωματώνεται στα ίδια τα συστήματα που θεωρούνται αξιόπιστα. Το παραδοσιακό μοντέλο, που στηρίζεται στην προστασία της περιμέτρου, αδυνατεί πλήρως να εντοπίσει επιθέσεις που ξεκινούν από έμπιστες πηγές (Deloitte, 2021). Μελέτες δείχνουν ότι η παραβίαση μιας εξωτερικής πλατφόρμας μπορεί να δώσει στον επιτιθέμενο άμεση πρόσβαση στο κρίσιμο εσωτερικό περιβάλλον, ακυρώνοντας πλήρως την έννοια της περιμέτρου (Leszczyna et al., 2019).

Ακόμη ένας παράγοντας που υπονομεύει το παραδοσιακό μοντέλο είναι η κατακερματισμένη φύση των σύγχρονων υποδομών. Οι οργανισμοί λειτουργούν πλέον σε hybrid ή multi-cloud περιβάλλοντα, όπου εφαρμογές, δεδομένα και υπηρεσίες κατανέμονται σε πολλαπλές πλατφόρμες με διαφορετικά επίπεδα ασφάλειας (CISA, 2021). Σε τέτοια περιβάλλοντα, η περίμετρος δεν μπορεί να οριστεί ούτε τεχνικά ούτε οργανωτικά, καθώς τα όρια μεταξύ εσωτερικού και εξωτερικού χώρου είναι ρευστά. Ως αποτέλεσμα, το perimeter model αποτυγχάνει να προσφέρει συνεπή έλεγχο και να αποτρέψει κινδύνους που προκύπτουν από την αλληλεπίδραση πολλών ανεξάρτητων συστημάτων.

Επιπρόσθετες απειλές συνδέονται με την αυξανόμενη εξάρτηση από mobile και IoT συσκευές, οι οποίες συχνά λειτουργούν εκτός εταιρικής εποπτείας. Τέτοιες συσκευές μπορεί να συνδέονται στο δίκτυο χωρίς επαρκείς μηχανισμούς διαχείρισης ταυτότητας ή πολιτικών, επιτρέποντας σε επιτιθέμενους να εκμεταλλευτούν αδύναμα σημεία της υποδομής (Golden et al., 2021). Το perimeter-based security, το οποίο στηρίζεται στην εμπιστοσύνη προς συσκευές εντός της περιμέτρου, δεν μπορεί να ανταποκριθεί σε ένα οικοσύστημα στο οποίο συσκευές και χρήστες συνδέονται από εκατοντάδες διαφορετικά σημεία.

Τέλος, η βιβλιογραφία αναδεικνύει ότι οι σύγχρονες επιθέσεις χαρακτηρίζονται από υψηλό βαθμό αυτοματοποίησης και ταχύτητας. Οι εισβολείς χρησιμοποιούν εξελιγμένα εργαλεία που τους επιτρέπουν να εκτελούν ταυτόχρονες επιθέσεις μεγάλης κλίμακας, να παρακάμπτουν μηχανισμούς ελέγχου και να μεταβάλλουν τις τεχνικές τους σε πραγματικό χρόνο. Το perimeter model, το οποίο βασίζεται σε στατικούς κανόνες firewall και σε παραδοσιακές υπογραφές ανίχνευσης, δεν μπορεί να ανταποκριθεί στην ευελιξία αυτή (Cunningham et al., 2019).

Συνολικά, το παραδοσιακό μοντέλο ασφάλειας έχει αποδειχθεί αναποτελεσματικό απέναντι στις σύγχρονες απειλές οι οποίες:

- στοχεύουν την ταυτότητα και όχι την περίμετρο,

- εκμεταλλεύονται νόμιμους μηχανισμούς πρόσβασης,
- χρησιμοποιούν την εσωτερική περιοχή του δικτύου ως πεδίο επέκτασης της επίθεσης,
- ξεπερνούν τα τεχνικά και οργανωτικά όρια της περιμέτρου,
- εξελίσσονται με ταχύτητα που υπερβαίνει τις δυνατότητες των παραδοσιακών μηχανισμών άμυνας.

Η αδυναμία του perimeter-based security να ανταποκριθεί σε αυτές τις απειλές συνιστά έναν από τους κεντρικούς λόγους για τους οποίους το Zero Trust αναδύεται ως το κυρίαρχο μοντέλο ασφάλειας στη σύγχρονη βιβλιογραφία.

2.4 Η μετάβαση από το trust-by-location στο trust-by-identity

Η μετάβαση από το trust-by-location στο trust-by-identity αποτελεί έναν από τους σημαντικότερους μετασχηματισμούς στην ιστορία της κυβερνοασφάλειας και το βασικό θεωρητικό υπόβαθρο πάνω στο οποίο οικοδομήθηκε η αρχιτεκτονική Zero Trust. Για δεκαετίες, η ασφάλεια των πληροφοριακών συστημάτων στηριζόταν στην παραδοχή ότι η τοποθεσία ενός χρήστη —και ιδίως η παρουσία του εντός της εταιρικής περιμέτρου— αποτελούσε επαρκή απόδειξη εμπιστοσύνης. Αυτό το «μοντέλο τοποθεσίας» υπήρξε λειτουργικό για τα κλειστά, στατικά και γεωγραφικά συγκεντρωμένα δίκτυα του παρελθόντος, αλλά κατέρρευσε θεωρητικά και πρακτικά με την έλευση του cloud, της κινητικότητας, των hybrid υποδομών και των εξελιγμένων επιθέσεων ταυτότητας (ACT-IAC, 2019).

Η παραδοσιακή λογική του trust-by-location προϋπέθετε ότι όποιος βρίσκεται «εντός» του δικτύου είναι αξιόπιστος. Οι χρήστες που συνδέονταν μέσω VPN ή από εταιρικούς σταθμούς εργασίας αποκτούσαν συχνά πλήρη, ανεξέλεγκτη πρόσβαση σε εσωτερικούς πόρους, με ελάχιστο έλεγχο των πραγματικών κινήτρων, της συσκευής ή της συμπεριφοράς τους (Cunningham, 2018). Αυτή η αρχιτεκτονική αντιλαμβανόταν την περίμετρο ως ένα είδος «τείχους», πέραν του οποίου οι έλεγχοι θεωρούνταν προαιρετικοί. Η πλήρης κατάργηση της έννοιας αυτής αποτέλεσε αναγκαιότητα καθώς κατέστη σαφές ότι οι περισσότερες επιθέσεις δεν εισέρχονται από την περίμετρο αλλά εκτελούνται μέσα στο δίκτυο με τη χρήση νόμιμων credentials (Golden et al., 2021).

Η μετατόπιση προς το trust-by-identity αντανακλά μια θεμελιώδη αλλαγή: ότι η εμπιστοσύνη δεν μπορεί πλέον να βασίζεται στον χώρο αλλά πρέπει να εδράζεται στην ταυτότητα του

χρήστη, στη συσκευή, στο επίπεδο κινδύνου και στο πλαίσιο πρόσβασης. Η CISA (2021) περιγράφει την εξέλιξη αυτή ως «κατάργηση της περιμέτρου ως κριτήριο εμπιστοσύνης» και ως «μετάβαση προς μοντέλα επαλήθευσης που απαιτούν συνεχή αξιολόγηση της ταυτότητας». Η είσοδος ενός χρήστη στο δίκτυο δεν συνιστά πλέον απόδειξη αξιοπιστίας· αντίθετα, η αξιολόγησή του πρέπει να συνεχίζεται σε κάθε αίτημα πρόσβασης.

Η ανάγκη για trust-by-identity έγινε ακόμη πιο εμφανής με την εξάπλωση των επιθέσεων credential compromise και lateral movement. Η βιβλιογραφία δείχνει ότι ένα μεγάλο ποσοστό κυβερνοεπιθέσεων δεν εκμεταλλεύεται τεχνικές αδυναμίες του perimeter, αλλά στοχεύει στην κατάχρηση της εμπιστοσύνης που αποδίδεται σε μια έγκυρη σύνδεση (Buck et al., 2021). Οι επιτιθέμενοι αξιοποιούν πλαστά ή κλεμμένα διαπιστευτήρια, αποκτώντας πρόσβαση ως «νόμιμοι» χρήστες και κινούμενοι ανεξέλεγκτα εντός του δικτύου. Σε αυτό το πλαίσιο, το trust-by-location αποδείχθηκε όχι μόνο ανεπαρκές αλλά και επικίνδυνο, καθώς παρείχε στους εισβολείς έναν απλό τρόπο παράκαμψης των περισσότερων μηχανισμών ασφαλείας.

Στο trust-by-identity, η εμπιστοσύνη μετατοπίζεται στο ποιος είναι ο χρήστης, τι ζητάει, ποια συσκευή χρησιμοποιεί, ποια είναι η κατάσταση ασφαλείας της συσκευής, ποιο είναι το πλαίσιο κινδύνου της πράξης και ποια πολιτική ισχύει για αυτό το αίτημα. Οι οργανισμοί που υιοθετούν το μοντέλο αυτό δεν βασίζονται πλέον σε στοιχεία τοποθεσίας αλλά σε τεχνικούς δείκτες ταυτοποίησης, authentication strength, context signals και risk scoring (CISA, 2021). Με άλλα λόγια, η ταυτότητα —και όχι η γεωγραφική θέση— γίνεται ο κεντρικός μηχανισμός ελέγχου και απόφασης.

Η Microsoft (2021b) σημειώνει ότι η μετάβαση προς το identity-centric security ήταν αναπόφευκτη λόγω της γενικευμένης χρήσης cloud υπηρεσιών, όπου η πρόσβαση πραγματοποιείται από οποιοδήποτε σημείο χωρίς σταθερό perimeter. Στις σύγχρονες επιχειρήσεις, δεδομένα και υπηρεσίες φιλοξενούνται πλέον σε πολλαπλά cloud environments, ενώ οι εργαζόμενοι χρησιμοποιούν ένα πλήθος συσκευών και εφαρμογών. Η διαχείριση της πρόσβασης απαιτεί συνεπώς μια ενιαία, ταυτοτητοκεντρική θεώρηση, η οποία μπορεί να λειτουργήσει ανεξάρτητα από την τοποθεσία.

Η μετάβαση αυτή συνδέεται επίσης με την ανάγκη για least privilege και granular authorization, τα οποία είναι αδύνατο να εφαρμοστούν αποτελεσματικά σε ένα μοντέλο που επιτρέπει καθολική πρόσβαση μόλις ένας χρήστης εισέλθει στο VPN. Μελέτες επισημαίνουν ότι η υπερβολική εμπιστοσύνη προς εσωτερικούς χρήστες και οι γενικευμένες άδειες

πρόσβασης αποτελούν σημαντικό παράγοντα κινδύνου, εντείνοντας την ανάγκη για αναλυτικό έλεγχο ταυτότητας και δικαιωμάτων (Adahman et al., 2022· Ferretti et al., 2021).

Τέλος, η μετατόπιση προς το trust-by-identity υποστηρίζεται και σε επίπεδο κυβερνητικών προτύπων και οδηγών βιομηχανίας. Ο NIST, μέσα από το SP 800-207, προσδιορίζει την ταυτότητα ως τη βάση κάθε απόφασης πρόσβασης, ενώ οργανισμοί όπως η Forrester και η Deloitte θεωρούν την ταυτότητα τον πρωταρχικό παράγοντα διαμόρφωσης risk-based πολιτικών (Cunningham et al., 2019· Deloitte, 2021). Το μοντέλο trust-by-identity δεν αποτελεί απλώς μια τεχνολογική μετάβαση, αλλά μια αλλαγή παραδείγματος στην ίδια τη φιλοσοφία της ασφάλειας.

Η μετάβαση από το trust-by-location στο trust-by-identity σηματοδοτεί το τέλος της εποχής όπου η εμπιστοσύνη αποδίδεται βάσει γεωγραφίας και την έναρξη ενός νέου μοντέλου όπου η ταυτότητα, η επαλήθευση και το πλαίσιο καθορίζουν πλήρως την πρόσβαση. Αυτή η εξέλιξη θεμελιώνει τη λογική πάνω στην οποία αναπτύχθηκε το Zero Trust, το οποίο απορρίπτει κάθε μορφή εγγενούς εμπιστοσύνης και απαιτεί συνεχή, προσαρμοζόμενη και ταυτοτητοκεντρική αξιολόγηση σε κάθε αίτημα πρόσβασης.

Κεφάλαιο 3. Θεωρητικό Πλαίσιο του Zero Trust

3.1 Βασικές αρχές και εννοιολογικές προσεγγίσεις

Η θεωρητική θεμελίωση του Zero Trust αποτελεί μια από τις πιο σημαντικές εξελίξεις στη σύγχρονη κυβερνοασφάλεια, καθώς επαναπροσδιορίζει ριζικά τον τρόπο με τον οποίο οι οργανισμοί αντιλαμβάνονται την έννοια της εμπιστοσύνης, της πρόσβασης και της προστασίας των πληροφοριακών συστημάτων. Σε αντίθεση με το παραδοσιακό perimeter-based security, το οποίο βασιζόταν στην παραδοχή ότι οι χρήστες και οι συσκευές εντός του δικτύου είναι αξιόπιστοι, το Zero Trust απορρίπτει πλήρως την ιδέα της εγγενούς εμπιστοσύνης. Η φιλοσοφία του συνοψίζεται στη θεμελιώδη αρχή «μην εμπιστεύεσαι ποτέ, επαλήθευε πάντα» (“never trust, always verify”), η οποία εισήχθη σταδιακά στην ακαδημαϊκή και βιομηχανική βιβλιογραφία ως απάντηση στις νέες απειλές και στην κατάρρευση του μοντέλου trust-by-location (Cunningham, 2018· CISA, 2021).

Η κεντρική αρχή του Zero Trust είναι ότι κάθε αίτημα πρόσβασης πρέπει να θεωρείται δυνητικά κακόβουλο, ανεξάρτητα από το αν προέρχεται από εσωτερικό ή εξωτερικό δίκτυο. Η εμπιστοσύνη δεν αποδίδεται σε επίπεδο τοποθεσίας, αλλά σε επίπεδο ταυτότητας, συσκευής, συμπεριφοράς και πλαισίου κινδύνου. Αυτό σημαίνει ότι η πρόσβαση δεν μπορεί να δοθεί με βάση το αν ένας χρήστης «βρίσκεται εντός» της περιμέτρου, αλλά πρέπει να αξιολογηθεί σε πραγματικό χρόνο, με βάση καταστάσεις όπως η υγεία της συσκευής, η ιστορικότητα της δραστηριότητας, η ευαισθησία του ζητούμενου πόρου και η δυναμική εκτίμηση κινδύνου (ACT-IAC, 2019). Η θεώρηση αυτή εισάγει έναν τρόπο σκέψης που προσεγγίζει την ασφάλεια ως μια συνεχώς εξελισσόμενη διαδικασία και όχι ως στατικό σύνολο κανόνων.

Κεντρική εννοιολογική συνιστώσα του Zero Trust είναι η *συνεχής επαλήθευση* (continuous verification). Η αρχή αυτή προβλέπει ότι η πρόσβαση δεν παραμένει σταθερή για όλη τη διάρκεια μιας συνεδρίας, όπως συνέβαινε στο μοντέλο VPN, αλλά αξιολογείται διαρκώς, με επαναλαμβανόμενους ελέγχους αυθεντικοποίησης και εξουσιοδότησης. Ο χρήστης πρέπει όχι μόνο να ταυτοποιηθεί επιτυχώς στην αρχή, αλλά και να αποδεικνύει συνεχώς ότι παραμένει αξιόπιστος, με μηχανισμούς όπως adaptive authentication, session risk scoring και συμπεριφορική ανάλυση (Golden et al., 2021). Η συνεχής αυτή αξιολόγηση αποτελεί μία από τις βασικές προϋποθέσεις ώστε να εντοπιστούν και να αποτραπούν επιθέσεις που

εξελίσσονται εντός του δικτύου, ιδιαίτερα όσες βασίζονται σε πλαστογραφημένα ή παραβιασμένα διαπιστευτήρια.

Εξίσου σημαντική είναι η αρχή των *ελάχιστων προνομίων* (least privilege), η οποία επιβάλλει ότι κάθε χρήστης ή υπηρεσία πρέπει να διαθέτει μόνο τα απολύτως απαραίτητα δικαιώματα για την εκτέλεση της συγκεκριμένης λειτουργίας. Η πρακτική αυτή μειώνει την πιθανότητα επέκτασης των επιθέσεων και περιορίζει τη ζημιά που μπορεί να προκληθεί σε περίπτωση παραβίασης ενός λογαριασμού (Adahman et al., 2022). Η εφαρμογή του least privilege απαιτεί granular, δυναμικά διαμορφώσιμες πολιτικές, οι οποίες προσαρμόζονται ανάλογα με το πλαίσιο κινδύνου, το ιστορικό συμπεριφοράς και τις ιδιαιτερότητες της συσκευής ή του αιτήματος. Η αρχή αυτή δεν αποτελεί απλώς τεχνική πρακτική αλλά ενσωματωμένη φιλοσοφία στη λογική του Zero Trust, όπου η υπερβολική εμπιστοσύνη προς εσωτερικούς χρήστες θεωρείται θεμελιωδώς επικίνδυνη.

Ένα άλλο κρίσιμο στοιχείο του θεωρητικού πλαισίου είναι η *μικρο-τμηματοποίηση* (micro-segmentation). Πρόκειται για μια προσέγγιση στην οποία το δίκτυο δεν αντιμετωπίζεται ως ενιαία οντότητα, αλλά διαχωρίζεται σε πολλαπλές, μικρές και απομονωμένες ζώνες, στις οποίες η πρόσβαση ελέγχεται ανεξάρτητα. Με αυτόν τον τρόπο, ακόμη και αν ένας επιτιθέμενος αποκτήσει αρχική πρόσβαση σε ένα τμήμα του συστήματος, δεν μπορεί να μετακινηθεί εύκολα σε άλλα τμήματα. Η micro-segmentation περιορίζει δραστικά τις δυνατότητες lateral movement, το οποίο αποτελεί μία από τις πιο ισχυρές τεχνικές σύγχρονων επιτιθέμενων (Buck et al., 2021). Ο περιορισμός της επιφάνειας επίθεσης σε μικρά, απομονωμένα τμήματα αποτελεί βασικό επιχείρημα υπέρ της υιοθέτησης του Zero Trust σε περιβάλλοντα μεγάλης κλίμακας.

Η θεωρητική θεμελίωση του Zero Trust περιλαμβάνει επίσης την αρχή της *σαφούς και συνεχούς ορατότητας* (visibility and continuous monitoring). Η παρακολούθηση της δραστηριότητας των χρηστών, των συσκευών και των υπηρεσιών σε πραγματικό χρόνο είναι κρίσιμη για την ανίχνευση ανωμαλιών, αποκλίσεων από την τυπική συμπεριφορά και πιθανών ενδείξεων επίθεσης. Το Zero Trust στηρίζεται σε ένα οικοσύστημα logging, analytics και policy enforcement, όπου τα συστήματα δεν λειτουργούν παθητικά αλλά παρακολουθούν, αξιολογούν και αντιδρούν προληπτικά (Microsoft, 2021b). Αυτή η αρχή έχει βαθιές ρίζες στην έρευνα πάνω στην τεχνητή νοημοσύνη, στο behavioral analytics και στη μοντελοποίηση κινδύνου, όπου η ανίχνευση ανωμαλιών αποτελεί βασικό εργαλείο για την ταχεία αποκάλυψη κακόβουλων ενεργειών.

Η έννοια της *πρόσβασης ανάλογα με το περιβάλλον* (context-aware access) αποτελεί μια ακόμη θεμελιώδη διάσταση. Στο Zero Trust, οι αποφάσεις πρόσβασης δεν λαμβάνονται στατικά, αλλά βάσει του περιβάλλοντος, το οποίο μπορεί να περιλαμβάνει παράγοντες όπως την τοποθεσία του χρήστη, τον τύπο της συσκευής, την κατάσταση ενημερώσεων ασφαλείας, τη συμπεριφορά σε προηγούμενες συνεδρίες ή τον ευαίσθητο χαρακτήρα των δεδομένων στα οποία επιχειρεί να αποκτήσει πρόσβαση (CISA, 2021). Αυτός ο δυναμικός υπολογισμός επιτρέπει την εφαρμογή πολιτικών που προσαρμόζονται άμεσα ανάλογα με τον κίνδυνο, εξασφαλίζοντας μεγαλύτερη ευελιξία και ασφάλεια.

Στους θεωρητικούς άξονες του Zero Trust περιλαμβάνεται επίσης η *ανεξαρτητοποίηση της πρόσβασης από το δίκτυο* (network decoupling). Το Zero Trust υποστηρίζει ότι η πρόσβαση στους πόρους δεν πρέπει να εξαρτάται από τη φυσική ή λογική θέση του χρήστη στο δίκτυο, αλλά από την ταυτότητα και το επίπεδο εμπιστοσύνης. Η προσέγγιση αυτή συνδέεται άμεσα με την ανάπτυξη του Zero Trust eXtended (ZTX), όπου η ασφάλεια αντιμετωπίζεται όχι μόνο σε επίπεδο δικτύου αλλά και σε επίπεδο δεδομένων, χρηστών, συσκευών, εφαρμογών και φορτίων εργασίας (Cunningham, 2018). Η πολυδιάστατη αυτή θεώρηση συνιστά μια σύγχρονη ολιστική προσέγγιση, που ξεφεύγει από την παραδοσιακή εστίαση στο ίδιο το δίκτυο και επεκτείνεται σε όλο το οικοσύστημα του οργανισμού.

Τέλος, η θεωρία του Zero Trust στηρίζεται στην έννοια της *ενιαίας πολιτικής διακυβέρνησης* (unified governance policy), όπου όλες οι αποφάσεις πρόσβασης διέπονται από ενιαίες, συνεκτικές και διαφανείς πολιτικές. Η ύπαρξη ενός ενιαίου μοντέλου πολιτικών διασφαλίζει ότι οι αποφάσεις είναι συνεπείς, καταγεγραμμένες και πλήρως ανιχνεύσιμες. Αυτή η προσέγγιση διευκολύνει την εφαρμογή standardization σε περιβάλλοντα multi-cloud, όπου διαφορετικές πλατφόρμες απαιτούν διαφορετικές ρυθμίσεις και μηχανισμούς ελέγχου (Deloitte, 2021).

Το θεωρητικό πλαίσιο του Zero Trust διαμορφώνεται από μία σειρά αλληλένδετων αρχών: την απόρριψη της εγγενούς εμπιστοσύνης, την εμμονή στη συνεχή επαλήθευση, την αυστηρή εφαρμογή least privilege, την ανάγκη για μικρο-τμηματοποίηση, την υιοθέτηση συνεχούς παρακολούθησης και ανάλυσης, την προσαρμογή αποφάσεων βάσει πλαισίου και την ενιαία πολιτική governance. Το Zero Trust δεν αποτελεί μια τεχνολογική λύση αλλά ένα εννοιολογικό οικοδόμημα που επαναπροσδιορίζει τον τρόπο με τον οποίο ορίζεται και εφαρμόζεται η ασφάλεια σε σύγχρονες, κατανεμημένες πληροφοριακές υποδομές. Με αυτόν τον τρόπο, προσφέρει μια συνολική και συνεκτική φιλοσοφία, η οποία ανταποκρίνεται

στις προκλήσεις ενός περιβάλλοντος όπου η ταυτότητα, η συμπεριφορά και ο κίνδυνος αποτελούν τα νέα θεμέλια της κυβερνοασφάλειας.

3.2 Zero Trust Maturity Models

Η έννοια της *ωριμότητας* (maturity) στο Zero Trust αποτελεί θεμελιώδες στοιχείο για την κατανόηση του πόσο έτοιμος είναι ένας οργανισμός να υιοθετήσει στην πράξη το νέο αυτό παραδειγματικό μοντέλο ασφάλειας. Η μετάβαση στο Zero Trust δεν είναι μια στιγμιαία διαδικασία, αλλά μια πολυεπίπεδη, μακροχρόνια και συχνά πολυσύνθετη στρατηγική μεταρρύθμιση, η οποία απαιτεί αλλαγή τεχνολογιών, διαδικασιών, πολιτικών και κουλτούρας. Για τον λόγο αυτό, οι σημαντικότεροι φορείς διαμόρφωσης προτύπων και βιομηχανικών πρακτικών έχουν αναπτύξει διαφορετικά Zero Trust Maturity Models, με στόχο να βοηθήσουν οργανισμούς να αξιολογήσουν το σημείο στο οποίο βρίσκονται, να καθορίσουν ρεαλιστικούς στόχους και να σχεδιάσουν μια σταδιακή, δομημένη μετάβαση. Τα πιο αναγνωρισμένα μοντέλα προέρχονται από το NIST, τη Forrester και τη Microsoft, καθένα από τα οποία εστιάζει σε διαφορετικούς άξονες, αντανακλώντας τη θεωρητική και πρακτική πολυπλοκότητα του Zero Trust.

Το NIST Zero Trust Maturity Model, το οποίο περιγράφεται κυρίως στο SP 800-207, αποτελεί το πλέον δομημένο και ακαδημαϊκά θεμελιωμένο μοντέλο, καθώς εισάγει μια καθαρά αρχιτεκτονική και λειτουργική θεώρηση της ωριμότητας. Το NIST δεν αντιλαμβάνεται την ωριμότητα απλώς ως βαθμό τεχνολογικής υλοποίησης, αλλά ως συστηματική ενσωμάτωση αρχών Zero Trust στο σύνολο των λειτουργιών ενός οργανισμού. Η προσέγγιση του NIST βασίζεται στη συνεχή αξιολόγηση της ταυτότητας, στον αυστηρό έλεγχο πρόσβασης και στη δυναμική εφαρμογή πολιτικών, ενώ αναγνωρίζει ότι οι οργανισμοί ξεκινούν την πορεία τους από την κατάσταση της παραδοσιακής περιμετρικής ασφάλειας και σταδιακά ωριμάζουν μέσα από επαναλαμβανόμενες φάσεις ενίσχυσης της ορατότητας, της αυτοματοποίησης και της προσαρμοστικότητας των πολιτικών (CISA, 2021· Kerman et al., 2020). Στο μοντέλο αυτό, η ωριμότητα μετριέται κυρίως με βάση το επίπεδο στο οποίο ο οργανισμός έχει ενσωματώσει ενοποιημένους μηχανισμούς ταυτοποίησης, πολιτικές least privilege, granular access controls και συνεχή επαλήθευση σε κάθε αίτημα πρόσβασης. Το NIST δίνει ιδιαίτερη βαρύτητα στη διαλειτουργικότητα μεταξύ χρηστών, συσκευών και εφαρμογών, θεωρώντας ότι η ωριμότητα προκύπτει από την ικανότητα ενός οργανισμού να εφαρμόζει συνεκτικά τις

αρχές Zero Trust σε όλα τα περιβάλλοντα εργασίας, είτε είναι on-premise, είτε cloud, είτε hybrid.

Σε αντίθεση με τη δομική αυτή προσέγγιση, η Forrester —ο φορέας που ιστορικά εισήγαγε τη φιλοσοφία Zero Trust μέσω της έννοιας του Zero Trust eXtended (ZTX)— προτείνει ένα μοντέλο ωριμότητας στο οποίο η προσοχή μετατοπίζεται από τα τεχνικά συστήματα προς ένα ολιστικό πλαίσιο που περιλαμβάνει δεδομένα, συσκευές, δίκτυα, ανθρώπους, ροές εργασίας και φορτία εφαρμογών. Η Forrester αναγνωρίζει ότι ο οργανισμός δεν μπορεί να θεωρηθεί ώριμος αν εφαρμόζει Zero Trust μόνο σε ορισμένες τμηματικές λειτουργίες, αλλά μόνο όταν η προσέγγιση επεκτείνεται στο σύνολο των επιχειρησιακών αξόνων (Cunningham, 2018· Cunningham et al., 2019). Η ωριμότητα εδώ δεν είναι γραμμική αλλά πολυεπίπεδη· ένας οργανισμός μπορεί να παρουσιάζει υψηλό βαθμό ωριμότητας στη διαχείριση ταυτότητας, αλλά χαμηλότερο στη μικρο-τμηματοποίηση ή στην προστασία των δεδομένων. Η Forrester αντιμετωπίζει το Zero Trust ως ένα «οικοσύστημα ασφαλείας», στο οποίο η ωριμότητα αναδύεται από τη συνολική συνέπεια εφαρμογής των πρακτικών και όχι από τη μεμονωμένη υιοθέτηση συγκεκριμένων τεχνολογιών. Η προσέγγιση αυτή θεωρεί ότι το Zero Trust ωριμάζει μόνο όταν ένας οργανισμός έχει καταφέρει να ευθυγραμμίσει κουλτούρα, διαδικασίες, τεχνολογίες και διοικητικές πρακτικές σε μια ενιαία στρατηγική «μηδενικής εμπιστοσύνης». Η Forrester δίνει ιδιαίτερη έμφαση στη διακυβέρνηση δεδομένων, θεωρώντας ότι τα δεδομένα —και όχι το δίκτυο— αποτελούν το πραγματικό «περιουσιακό στοιχείο» που πρέπει να προστατευτεί και συνεπώς το επίκεντρο της ωριμότητας.

Η Microsoft, από την πλευρά της, έχει αναπτύξει ένα Zero Trust Maturity Model που αντανακλά τη δική της εκτεταμένη εμπειρία από την εφαρμογή Zero Trust σε παγκόσμια κλίμακα, τόσο εντός της εταιρείας όσο και στους πελάτες της. Το μοντέλο της Microsoft είναι περισσότερο επιχειρησιακό και λειτουργικό και βασίζεται σε τρεις φάσεις: αρχική, μεσαία και ώριμη κατάσταση. Εστιάζει στα έξι θεμέλια του Zero Trust: ταυτότητες, συσκευές, εφαρμογές, δεδομένα, δίκτυο και υποδομές (Microsoft, 2021b· Microsoft, 2021a). Σε κάθε έναν από αυτούς τους τομείς, η Microsoft περιγράφει συγκεκριμένες πρακτικές, τεχνολογίες και πολιτικές που αντιστοιχούν σε κάθε επίπεδο ωριμότητας. Για παράδειγμα, στο επίπεδο των ταυτοτήτων η στοιχειώδης ωριμότητα περιλαμβάνει τη χρήση πολυπαραγοντικού ελέγχου ταυτότητας (MFA), η ενδιάμεση ωριμότητα περιλαμβάνει risk-based conditional access, ενώ η ώριμη κατάσταση προϋποθέτει πλήρη αυτοματοποίηση πολιτικών, συνεχή αξιολόγηση συμπεριφοράς και απρόσκοπτη ενοποίηση με μηχανισμούς SIEM και SOAR. Η

Microsoft αντιλαμβάνεται την ωριμότητα πρωτίστως ως θέμα αυτοματοποίησης και συνεχούς προσαρμογής πολιτικών, υποστηρίζοντας ότι ένας πραγματικά ώριμος οργανισμός πρέπει να στηρίζεται στη δυναμική, ευφυή και αυτορυθμιζόμενη λήψη αποφάσεων πρόσβασης, όπου η ανθρώπινη παρέμβαση περιορίζεται στο ελάχιστο (Golden et al., 2021).
Αν και τα τρία μοντέλα έχουν κοινή θεωρητική βάση, παρουσιάζουν σημαντικές διαφοροποιήσεις ως προς την έμφαση και τη μεθοδολογία. Το NIST εστιάζει στην αρχιτεκτονική αυστηρότητα, ορίζοντας σαφή πλαίσια και λειτουργικά standards, κάτι που το καθιστά ιδιαίτερα χρήσιμο σε κυβερνητικούς και θεσμικούς οργανισμούς. Η Forrester προσεγγίζει την ωριμότητα ως πολυδιάστατο οργανωσιακό οικοσύστημα, αποδίδοντας προτεραιότητα όχι μόνο στην τεχνολογία αλλά και στη διακυβέρνηση, στη συμπεριφορά των εργαζομένων και στη μεθοδολογία προστασίας δεδομένων. Η Microsoft, τέλος, προσφέρει ένα πιο πρακτικό και υλοποιήσιμο μοντέλο, εστιάζοντας σε συγκεκριμένες τεχνικές και λειτουργικές πρακτικές που μπορούν να εφαρμοστούν άμεσα από επιχειρήσεις σε ταχέως μεταβαλλόμενα περιβάλλοντα.
Παρά τις διαφορές τους, τα μοντέλα ωριμότητας συγκλίνουν σε βασικές θεωρητικές παραδοχές. Πρώτον, όλα υπογραμμίζουν ότι το Zero Trust δεν είναι τεχνολογία αλλά αρχιτεκτονική φιλοσοφία, η οποία απαιτεί συνεκτική και ολοκληρωμένη εφαρμογή. Δεύτερον, αναγνωρίζουν ότι η ωριμότητα δεν επιτυγχάνεται ταυτόχρονα σε όλους τους τομείς, αλλά εξελίσσεται σταδιακά, μέσα από επαναλαμβανόμενες διαδικασίες αξιολόγησης και ενίσχυσης. Τρίτον, δίνουν ιδιαίτερη έμφαση στο identity-centric security, το οποίο θεωρούν το θεμέλιο κάθε εφαρμογής Zero Trust, καθώς οι σύγχρονες κυβερνοεπιθέσεις στοχεύουν κυρίως στην ταυτότητα και όχι στην περιμετρική παραβίαση (Adahman et al., 2022). Τέλος, όλα τα μοντέλα αναγνωρίζουν ότι η ωριμότητα απαιτεί αυτοματοποίηση, ευελιξία και προσαρμοστικότητα, ιδιότητες που συνδέονται άμεσα με την ανάγκη για continuous verification και context-aware πρόσβαση.
Σε έναν ευρύτερο θεωρητικό ορίζοντα, τα Zero Trust Maturity Models συμβάλλουν στην αποκρυστάλλωση των εννοιολογικών ακρογωνιαίων λίθων του Zero Trust, προσφέροντας μια κλιμακωτή, δομημένη και μετρήσιμη πορεία υιοθέτησης. Παρέχουν στους οργανισμούς όχι μόνο ένα σημείο εκκίνησης αλλά και έναν χάρτη πορείας, ο οποίος τους βοηθά να κατανοήσουν ποιες πρακτικές είναι απαραίτητες, ποιες αποτελούν μελλοντικά βήματα και πώς μπορούν να διασφαλίσουν ότι η στρατηγική τους θα παραμείνει συνεπής, ρεαλιστική και βιώσιμη. Με αυτόν τον τρόπο, τα μοντέλα ωριμότητας λειτουργούν ως συνδετικός κρίκος

ανάμεσα στη θεωρία και την πράξη, επιτρέποντας στο Zero Trust να εφαρμόζεται όχι ως αφηρημένη αρχή, αλλά ως λειτουργικό και μετρήσιμο πλαίσιο κυβερνοασφάλειας.

3.3 Συστατικά της αρχιτεκτονικής Zero Trust

Η αρχιτεκτονική Zero Trust αποτελεί ένα πολυδιάστατο και βαθιά ενσωματωμένο πλαίσιο ασφάλειας, το οποίο στηρίζεται σε ένα σύνολο αλληλένδετων συστατικών που συνεργάζονται για να εξασφαλίσουν ότι κάθε αίτημα πρόσβασης, κάθε χρήστης, κάθε συσκευή και κάθε διαδικασία αντιμετωπίζονται ως δυνητικά επισφαλείς μέχρι να αποδειχθεί το αντίθετο. Τα θεμελιώδη αυτά στοιχεία – Identity and Access Management (IAM), Multi-Factor Authentication (MFA), μηχανισμοί policy enforcement και continuous verification – συγκροτούν τον πυρήνα της λογικής Zero Trust και αποτελούν τους λειτουργικούς μοχλούς μέσω των οποίων οι αρχές της μηδενικής εμπιστοσύνης υλοποιούνται σε πραγματικά περιβάλλοντα. Κάθε ένα από αυτά τα συστατικά δεν λειτουργεί μεμονωμένα, αλλά ως μέρος ενός συνεκτικού οικοσυστήματος ασφαλείας, το οποίο επαναπροσδιορίζει την πρόσβαση με τρόπο granular, δυναμικό και συνεχώς επαληθεύσιμο.

Στη βάση της αρχιτεκτονικής Zero Trust βρίσκεται η *διαχείριση ταυτοτήτων και πρόσβασης* (IAM). Το IAM αποτελεί τον θεμελιώδη παράγοντα από τον οποίο εξαρτάται η αξιοπιστία όλων των επόμενων επιπέδων ασφαλείας, καθώς η ταυτότητα είναι αυτό που καθορίζει ποιος μπορεί να αποκτήσει πρόσβαση, σε τι μπορεί να αποκτήσει πρόσβαση και υπό ποιες συνθήκες. Σε ένα Zero Trust περιβάλλον, η ταυτότητα δεν είναι απλώς ένα σύνολο credentials ή ένας στατικός λογαριασμός χρήστη. Αντιθέτως, αποτελεί ένα σύνολο δυναμικών, πολυδιάστατων χαρακτηριστικών που περιλαμβάνουν τη συμπεριφορά του χρήστη, το ιστορικό του, τα δικαιώματα που του έχουν αποδοθεί, την κατάσταση της συσκευής που χρησιμοποιεί και το πλαίσιο στο οποίο δραστηριοποιείται (Adahman et al., 2022). Η ενσωμάτωση αυτών των στοιχείων επιτρέπει τη λήψη αποφάσεων πρόσβασης βασισμένων όχι μόνο σε αναγνωριστικά στοιχεία, αλλά και σε ευρύτερα σημάδια εμπιστοσύνης, μειώνοντας έτσι την πιθανότητα κατάχρησης ταυτότητας. Το IAM στο Zero Trust δεν είναι μια στατική διαδικασία επαλήθευσης κατά την είσοδο, αλλά ένας μηχανισμός συνεχούς αξιολόγησης, όπου η ταυτότητα παραμένει υπό διαρκή επιτήρηση όσο ο χρήστης παραμένει συνδεδεμένος.

Η πολλαπλή επαλήθευση ταυτότητας (MFA) αποτελεί το δεύτερο θεμελιώδες συστατικό της αρχιτεκτονικής Zero Trust και λειτουργεί ως ο πρώτος ισχυρός φραγμός απέναντι στις

επιθέσεις που βασίζονται σε παραβιάσεις credentials. Στη σύγχρονη βιβλιογραφία αναγνωρίζεται ότι η κλοπή διαπιστευτηρίων αποτελεί έναν από τους αποτελεσματικότερους τρόπους παραβίασης εταιρικών συστημάτων, γεγονός που καθιστά το MFA απαραίτητο (Golden et al., 2021). Η MFA ενισχύει τη βασική ταυτοποίηση, απαιτώντας από τον χρήστη να αποδείξει την ταυτότητά του μέσα από περισσότερους από έναν παράγοντες· όχι μόνο κάτι που γνωρίζει (όπως ένας κωδικός), αλλά και κάτι που έχει (συσκευή, token) ή κάτι που είναι (βιομετρικά στοιχεία). Στο Zero Trust, η MFA δεν θεωρείται απλώς πρόσθετο επίπεδο προστασίας αλλά βασικό μέρος μιας δυναμικής και πολυπαραγοντικής αξιολόγησης κινδύνου. Επιπλέον, η MFA συχνά ενσωματώνεται σε adaptive authentication μηχανισμούς, οι οποίοι αυξάνουν ή μειώνουν τις απαιτήσεις επαλήθευσης με βάση το επίπεδο ρίσκου κάθε αίτηματος πρόσβασης. Για παράδειγμα, ένας χρήστης που επιχειρεί να συνδεθεί από άγνωστο δίκτυο, νέα συσκευή ή γεωγραφικά ασυνήθιστη περιοχή μπορεί να κληθεί να παράσχει πρόσθετες αποδείξεις ταυτότητας, ενσωματώνοντας έτσι το risk scoring στο πρακτικό επίπεδο ασφάλειας (CISA, 2021).

Η εφαρμογή πολιτικών (policy enforcement) αποτελεί την επόμενη κρίσιμη διάσταση. Στο Zero Trust, οι πολιτικές δεν εφαρμόζονται στατικά, ούτε περιορίζονται σε ένα απλό allow/deny μοντέλο. Αντίθετα, αποτελούν σύνθετες, πολυεπίπεδες και δυναμικά προσαρμοζόμενες οδηγίες που καθορίζουν τι επιτρέπεται και τι όχι, με βάση ένα πλέγμα παραμέτρων όπως η ταυτότητα, η συσκευή, ο τύπος πόρου, η ευαισθησία των δεδομένων, το πλαίσιο κινδύνου, η γεωγραφική τοποθεσία και η συμπεριφορική δραστηριότητα (Cunningham et al., 2019). Η σύγχρονη βιβλιογραφία τονίζει ότι η επίτευξη ώριμης εφαρμογής Zero Trust προϋποθέτει την υιοθέτηση granular policy enforcement μηχανισμών, οι οποίοι δεν αποδίδουν δικαιώματα πρόσβασης στο σύνολο του δικτύου αλλά μόνο στον εκάστοτε απαραίτητο πόρο. Η έννοια του least privilege είναι άρρηκτα συνδεδεμένη με την policy enforcement λογική, καθώς επιβάλλει συνεχείς προσαρμογές των δικαιωμάτων με βάση την πραγματική ανάγκη του χρήστη και όχι βάσει ιστορικών ή γενικευμένων ρυθμίσεων. Η αποτελεσματική εφαρμογή πολιτικών απαιτεί υψηλό επίπεδο ορατότητας, κεντρική διακυβέρνηση και αυτοματοποίηση, καθώς οι χειροκίνητες διαδικασίες δεν μπορούν να ανταποκριθούν στον όγκο και τη συχνότητα των αιτημάτων πρόσβασης που παράγει ένα σύγχρονο πληροφοριακό περιβάλλον.

Το τέταρτο και ίσως πιο καθοριστικό στοιχείο του Zero Trust είναι η συνεχής επαλήθευση (continuous verification). Σε αντίθεση με το παραδοσιακό μοντέλο ελέγχου πρόσβασης,

όπου η ταυτοποίηση πραγματοποιείται μόνο στην αρχή της συνεδρίας, το Zero Trust απαιτεί συνεχή αξιολόγηση κάθε αιτήματος, σε όλη τη διάρκεια της περιόδου σύνδεσης. Η συνεχής επαλήθευση βασίζεται σε πολλαπλά επίπεδα ελέγχων: επανέλεγχο ταυτότητας, παρακολούθηση της συμπεριφοράς σε πραγματικό χρόνο, μηχανισμούς anomaly detection, risk-based scoring, επιβολή δυναμικών πολιτικών και αυτοματοποιημένη απόκριση σε ύποπτες ενέργειες. Το συνεχές αυτό ρεύμα αξιολόγησης αντικατοπτρίζει την παραδοχή ότι οι συνθήκες ασφάλειας μπορούν να μεταβληθούν ανά πάσα στιγμή: ένας χρήστης που ήταν αξιόπιστος πριν από πέντε λεπτά μπορεί πλέον να θεωρείται ύποπτος, είτε λόγω αλλαγής τοποθεσίας, είτε ύποπτης συμπεριφοράς, είτε παραβίασης της συσκευής του (Buck et al., 2021). Η continuous verification απαιτεί την ύπαρξη εξελιγμένων μηχανισμών καταγραφής, παρακολούθησης, ανάλυσης και συσχέτισης γεγονότων, καθώς και την ενσωμάτωση αυτών με πλατφόρμες SIEM και SOAR, ώστε τα συστήματα να μπορούν να αντιδρούν αυτόματα σε πραγματικό χρόνο. Η Microsoft (2021b) υπογραμμίζει ότι η υιοθέτηση μηχανισμών continuous verification αποτελεί το καθοριστικό χαρακτηριστικό που διαχωρίζει τις οργανώσεις που «υλοποιούν» Zero Trust από εκείνες που απλώς εφαρμόζουν μεμονωμένες τεχνικές πρακτικές του.

Τα τέσσερα αυτά συστατικά συνθέτουν ένα βαθιά ενσωματωμένο οικοσύστημα ασφάλειας. Το IAM προσδιορίζει το ποιος, το MFA επιβεβαιώνει ότι ο ισχυριζόμενος χρήστης είναι πράγματι αυτός που λέει, το policy enforcement καθορίζει το τι μπορεί να κάνει και το continuous verification εξασφαλίζει ότι το δικαίωμα αυτό παραμένει ασφαλές σε όλη τη διάρκεια της συνεδρίας. Η συνεργιστική αυτή λειτουργία εξουδετερώνει τις παραδοχές του παρελθόντος, όπου η ταυτοποίηση και η πρόσβαση αντιμετωπίζονταν ως στατικές πράξεις και όχι ως συνεχείς διαδικασίες. Στο Zero Trust, η πρόσβαση είναι μια ζωντανή, εξελισσόμενη κατάσταση, όπου κάθε ενέργεια, κάθε μετάβαση και κάθε αίτημα εξετάζονται μέσα σε ένα δυναμικό πλαίσιο που λαμβάνει υπόψη την πολυπλοκότητα των σύγχρονων απειλών.

Σε έναν σύγχρονο οργανισμό, τα συστατικά αυτά δεν λειτουργούν ως διακριτές τεχνολογικές λύσεις, αλλά ως ολοκληρωμένο πλαίσιο στρατηγικής ασφάλειας. Η ωριμότητα του Zero Trust προκύπτει από την ικανότητα του οργανισμού να ενοποιεί το IAM, το MFA, το policy enforcement και το continuous verification σε ένα ενιαίο, αυτοματοποιημένο, διαλειτουργικό σύστημα, το οποίο παρακολουθεί, αξιολογεί και προσαρμόζει την πρόσβαση χωρίς να στηρίζεται στην ανθρώπινη κρίση για τις καθημερινές αποφάσεις. Η ενσωμάτωση αυτή αποτελεί την ουσία της μετάβασης από το παρωχημένο μοντέλο της περιμετρικής

ασφάλειας σε μια αρχιτεκτονική πραγματικά ικανή να ανταποκριθεί στον ρυθμό, τη δυναμική και την πολυπλοκότητα των σύγχρονων κυβερνοαπειλών.

3.4 Least privilege & micro-segmentation: βιβλιογραφική ανάλυση

Η αρχή του least privilege και η έννοια της micro-segmentation αποτελούν δύο από τους πιο κρίσιμους θεωρητικούς πυλώνες της αρχιτεκτονικής Zero Trust, καθώς εκφράζουν στην πράξη την εγκατάλειψη της «γενικευμένης εμπιστοσύνης» που χαρακτήριζε το παραδοσιακό perimeter-based μοντέλο. Στη διεθνή βιβλιογραφία γύρω από το Zero Trust, οι δύο αυτές αρχές εμφανίζονται σταθερά ως θεμελιώδεις προϋποθέσεις για την ουσιαστική μείωση της επιφάνειας επίθεσης και τον περιορισμό των συνεπειών μιας αναπόφευκτης παραβίασης (ACT-IAC, 2019· Buck et al., 2021). Η ανάλυση τους επιτρέπει να γίνει κατανοητό πώς το Zero Trust μετατρέπει την ασφάλεια από στατικό φραγμό σε λεπτομερώς ελεγχόμενη και κατακερματισμένη δομή πρόσβασης.

Η αρχή του least privilege έχει μακρά ιστορία στα πληροφοριακά συστήματα, αλλά στο πλαίσιο του Zero Trust αποκτά ανανεωμένο θεωρητικό βάρος. Στον πυρήνα της βρίσκεται η ιδέα ότι κάθε χρήστης, υπηρεσία ή διεργασία πρέπει να διαθέτει μόνο εκείνα τα δικαιώματα που είναι απολύτως απαραίτητα για την εκτέλεση μιας συγκεκριμένης εργασίας, ούτε λιγότερα, αλλά κυρίως ούτε περισσότερα. Η βιβλιογραφία αναδεικνύει ότι στις κλασικές αρχιτεκτονικές κυβερνοασφάλειας η αρχή αυτή σπάνια εφαρμοζόταν με συνέπεια, καθώς η λογική της περιμέτρου οδηγούσε σε ευρείες ομάδες δικαιωμάτων για όλους τους «εσωτερικούς» χρήστες, συχνά με γενικευμένη πρόσβαση σε κρίσιμα συστήματα και δεδομένα (ACT-IAC, 2019). Στο Zero Trust, αντίθετα, το least privilege δεν αποτελεί ευχή ή «καλή πρακτική», αλλά δομική απαίτηση: χωρίς αυτό, η μηδενική εμπιστοσύνη δεν μπορεί να εφαρμοστεί ουσιαστικά.

Ερευνητικές εργασίες που εξετάζουν τη σχέση μεταξύ Zero Trust και διαχείρισης κινδύνου επισημαίνουν ότι η μη εφαρμογή least privilege είναι από τους σημαντικότερους παράγοντες που αυξάνουν τη σοβαρότητα μιας επίθεσης. Όταν ένας λογαριασμός χρήστη ή μια υπηρεσία διαθέτει δικαιώματα πολύ ευρύτερα από αυτά που χρειάζεται, τότε η παραβίασή του επιτρέπει στον επιτιθέμενο να κινηθεί με σχεδόν απεριόριστες δυνατότητες, αποκτώντας πρόσβαση σε ευαίσθητα δεδομένα, κρίσιμες εφαρμογές ή λειτουργίες συστήματος (Adahman et al., 2022). Η ανάλυση κόστους–οφέλους που προτείνουν οι Adahman και συν. (2022) δείχνει ότι η συστηματική υιοθέτηση πολιτικών least privilege

οδηγεί σε ουσιαστική μείωση του αναμενόμενου κόστους ενός περιστατικού, καθώς περιορίζει δραστικά το αποτύπωμα της ζημιάς, ακόμη και όταν η αρχική παραβίαση δεν μπορεί να αποτραπεί. Σε αυτό το πλαίσιο, το least privilege αποκτά τον χαρακτήρα κρίσιμου παράγοντα για την επιτυχή μετάβαση σε μοντέλα Zero Trust, σε συνάφεια με τη λογική των παραγόντων επιτυχίας που περιγράφουν κλασικές μελέτες για οργανωτικά συστήματα (Freund, 1988· Yeoh & Koronios, 2010).

Η πρακτική υιοθέτηση της αρχής του least privilege, ωστόσο, δεν είναι απλή υπόθεση. Η βιβλιογραφία τονίζει ότι απαιτεί βαθιά κατανόηση των ροών εργασίας, της επιχειρησιακής λογικής και των εξαρτήσεων μεταξύ συστημάτων, ώστε να καθοριστεί τι ακριβώς είναι «απαραίτητο» για κάθε ρόλο και κάθε διεργασία (Golden et al., 2021). Πολλοί οργανισμοί που επιχειρούν να μεταβούν σε Zero Trust συναντούν δυσκολίες όταν ανακαλύπτουν ότι τα δικαιώματα πρόσβασης έχουν διαμορφωθεί ιστορικά, με ad hoc αποφάσεις και χωρίς συστηματική τεκμηρίωση. Η ανάγκη ανασχεδιασμού των ρόλων, των ομάδων και των πολιτικών πρόσβασης αποτελεί συνεπώς σημαντικό εμπόδιο ωρίμανσης, κάτι που αναγνωρίζεται και στα μοντέλα Zero Trust Maturity της Forrester και της Microsoft (Buck et al., 2021· Microsoft, 2021b). Στο θεωρητικό επίπεδο, το least privilege συνδέεται έτσι με μια ευρύτερη συζήτηση γύρω από τη διακυβέρνηση της πρόσβασης, όπου ο έλεγχος των δικαιωμάτων γίνεται αντικείμενο συνεχούς αναθεώρησης και βελτιστοποίησης, και όχι στατικής ρύθμισης.

Η αρχή του least privilege αποκτά ιδιαίτερο βάθος όταν συνδυάζεται με την έννοια της micro-segmentation. Η micro-segmentation αφορά τον κατακερματισμό του δικτύου και των πόρων σε μικρές, λογικά ή/και τεχνικά απομονωμένες ζώνες, στις οποίες η πρόσβαση ελέγχεται με πολύ μεγαλύτερη λεπτομέρεια από ό,τι στο κλασικό μοντέλο «εντός–εκτός» του firewall. Αν στο επίπεδο των δικαιωμάτων ο περιορισμός της πρόσβασης εκφράζεται μέσω του least privilege, στο επίπεδο της αρχιτεκτονικής ο ίδιος περιορισμός υλοποιείται μέσω της micro-segmentation (CISA, 2021). Με άλλα λόγια, η micro-segmentation συνιστά την «χωρική» έκφραση του least privilege, καθώς επιβάλλει την ύπαρξη πολλών μικρών, σαφώς οριοθετημένων περιοχών στις οποίες μόνο συγκεκριμένοι χρήστες ή υπηρεσίες μπορούν να έχουν πρόσβαση, υπό αυστηρά καθορισμένες συνθήκες.

Η βιβλιογραφική ανασκόπηση των Buck και συν. (2021) αναδεικνύει ότι η micro-segmentation αποτελεί ένα από τα πιο κρίσιμα αλλά ταυτόχρονα λιγότερο κατανοητά στοιχεία του Zero Trust. Πολλοί οργανισμοί υιοθετούν επιφανειακά τον όρο, χωρίς να

προχωρούν σε πραγματικό επανασχεδιασμό των ροών δικτύου και των σχέσεων εξάρτησης μεταξύ εφαρμογών. Η μελέτη αυτή επισημαίνει ότι η επιτυχής micro-segmentation προϋποθέτει λεπτομερή χαρτογράφηση του εσωτερικού περιβάλλοντος, κατανόηση των east–west ροών και εντοπισμό των κρίσιμων «μονοπατιών» που μπορούν να αξιοποιηθούν για lateral movement. Σε αυτό το σημείο, η micro-segmentation συνδέεται άρρηκτα με την ανάγκη για βελτιωμένη situation awareness, όπως περιγράφεται σε μελέτες για συστήματα υποστήριξης απόφασης σε περιβάλλοντα υψηλής κρισιμότητας (Naderpour et al., 2014). Η δυνατότητα του οργανισμού να «βλέπει» με ακρίβεια πώς κινούνται τα δεδομένα και οι διεργασίες εσωτερικά αποτελεί προϋπόθεση για να μπορέσει να σχεδιάσει αποτελεσματικές ζώνες μικρο-τμηματοποίησης.

Στο πλαίσιο του cloud, η έννοια της micro-segmentation αποκτά επιπλέον διαστάσεις. Η μελέτη των Ferretti και συν. (2021) για «survivable zero trust» σε cloud περιβάλλοντα δείχνει ότι η micro-segmentation δεν περιορίζεται σε παραδοσιακά VLANs ή subnetting, αλλά επεκτείνεται σε επίπεδο εφαρμογών, containers και workloads. Στα περιβάλλοντα αυτά, ο κατακερματισμός πρέπει να λαμβάνει υπόψη όχι μόνο τη λογική τοπολογία του δικτύου, αλλά και τη δυναμική δημιουργία και καταστροφή υπηρεσιών, όπως συμβαίνει σε Kubernetes clusters ή σε serverless αρχιτεκτονικές. Η micro-segmentation σε τέτοια περιβάλλοντα δεν μπορεί να είναι στατική· απαιτεί πολιτικές που ακολουθούν δυναμικά τα workloads και συνδέουν την πρόσβαση με τα μεταδεδομένα της εφαρμογής, της υπηρεσίας και της ταυτότητας που την καλεί (Ferretti et al., 2021). Στη θεωρητική προοπτική του Zero Trust, αυτό σημαίνει ότι η micro-segmentation μετατρέπεται σε μια μορφή «λογικής οντολογικής τμηματοποίησης», όπου περιορίζεται όχι μόνο ο χώρος, αλλά και οι πιθανές σχέσεις μεταξύ οντοτήτων.

Η βιβλιογραφία αναδεικνύει επίσης τη στενή σχέση ανάμεσα σε least privilege, micro-segmentation και δυνατότητα ανίχνευσης–αντίδρασης. Η ύπαρξη μικρών, σαφώς οριοθετημένων ζωνών πρόσβασης, σε συνδυασμό με αυστηρά περιορισμένα δικαιώματα, βελτιώνει σημαντικά την ικανότητα ανίχνευσης ύποπτης δραστηριότητας. Όταν ένας χρήστης ή μια υπηρεσία επιχειρεί να αποκτήσει πρόσβαση σε μια ζώνη ή σε έναν πόρο για τον οποίο δεν έχει σαφώς καθορισμένα δικαιώματα, το γεγονός αυτό καθίσταται αμέσως ανιχνεύσιμο, καθώς παραβιάζει μια σαφώς διατυπωμένη πολιτική (CISA, 2021· Microsoft, 2021b). Αντίθετα, σε περιβάλλοντα όπου η πρόσβαση είναι γενικευμένη και τα δίκτυα παραμένουν επίπεδα, τέτοιες αποκλίσεις περνούν συχνά απαρατήρητες, καθώς δεν

υπάρχουν σαφείς γραμμές που να διαχωρίζουν το «επιτρεπτό» από το «μη επιτρεπτό». Με αυτή την έννοια, η micro-segmentation και το least privilege λειτουργούν ως ενισχυτές της δυνατότητας επιβολής πολιτικών και συνεχούς επαλήθευσης.

Από θεωρητική άποψη, οι δύο αυτές αρχές συνδέονται με τη συζήτηση γύρω από την «επιφάνεια εμπιστοσύνης» του οργανισμού. Στο κλασικό perimeter μοντέλο, η επιφάνεια εμπιστοσύνης ήταν μεγάλη και αδιαφοροποίητη: ολόκληρο το εσωτερικό δίκτυο θεωρούνταν αξιόπιστο. Στο Zero Trust, η επιφάνεια εμπιστοσύνης συρρικνώνεται και κατακερματίζεται, καθώς κάθε ζώνη micro-segmentation και κάθε ρόλος least privilege αντιστοιχεί σε ένα μικρό, προσεκτικά ορισμένο σημείο όπου ο οργανισμός «επιλέγει» να εμπιστευτεί υπό αυστηρές προϋποθέσεις (Golden et al., 2021). Η μείωση και ο κατακερματισμός αυτής της επιφάνειας επιτρέπει στον οργανισμό να αντέχει καλύτερα σε παραβιάσεις, καθώς η παραβίαση μιας ζώνης δεν συνεπάγεται αυτόματα κατάρρευση ολόκληρου του συστήματος.

Τέλος, η βιβλιογραφία που εξετάζει την επικοινωνία και τη «μετάφραση» του Zero Trust σε γλώσσα διοίκησης τονίζει ότι least privilege και micro-segmentation πρέπει να αντιμετωπίζονται όχι μόνο ως τεχνικές έννοιες, αλλά και ως στρατηγικές αρχές διακυβέρνησης (Deloitte, 2021· Bobbert & Scheerder, 2020). Ο περιορισμός των δικαιωμάτων πρόσβασης και ο κατακερματισμός της υποδομής δεν είναι απλώς τεχνική ρύθμιση, αλλά επιλογή που επηρεάζει τη λειτουργικότητα, την ευελιξία και τον τρόπο με τον οποίο ο οργανισμός οργανώνει τις διαδικασίες του. Ως εκ τούτου, η επιτυχής εφαρμογή τους προϋποθέτει τη δέσμευση της ανώτερης διοίκησης, την προσαρμογή των ροών εργασίας και τη συνειδητή αποδοχή ότι η ασφάλεια δεν μπορεί πια να βασίζεται σε «σιωπηρή εμπιστοσύνη» προς εσωτερικούς χρήστες και συστήματα.

Η βιβλιογραφική ανάλυση δείχνει ότι η αρχή του least privilege και η micro-segmentation αποτελούν αλληλένδετα και αμοιβαία ενισχυόμενα στοιχεία της αρχιτεκτονικής Zero Trust. Η θεωρητική τους αξία έγκειται στο ότι μετατρέπουν την ασφάλεια από αφηρημένη έννοια σε συγκεκριμένη, μετρήσιμη και υλοποιήσιμη πρακτική, περιορίζοντας συστηματικά τόσο την πρόσβαση όσο και τον χώρο μέσα στον οποίο μπορεί να κινηθεί ένας επιτιθέμενος. Με αυτόν τον τρόπο, λειτουργούν ως βασικά εργαλεία για τη μετάβαση από το παρωχημένο μοντέλο της περιμετρικής εμπιστοσύνης σε ένα περιβάλλον όπου κάθε δικαίωμα και κάθε διαδρομή εντός του συστήματος πρέπει να είναι ρητά, τεκμηριωμένα και διαρκώς επαληθεύσιμα.

3.5 Ο ρόλος του identity-centric security

Η μετάβαση προς μια αρχιτεκτονική Zero Trust καθιστά την ταυτότητα το απόλυτο κέντρο βάρους της κυβερνοασφάλειας, οδηγώντας στη διαμόρφωση αυτού που η σύγχρονη βιβλιογραφία αποκαλεί identity-centric security. Στο παρελθόν, η ασφάλεια οργανωνόταν γύρω από στατικά όρια δικτύου, μοντέλα περιμέτρου, firewalls και γεωγραφικά προσδιορισμένα σημεία ελέγχου. Στο σύγχρονο περιβάλλον όμως, όπου χρήστες, εφαρμογές και δεδομένα είναι διασκορπισμένα σε πολλαπλές πλατφόρμες, συσκευές, δίκτυα και cloud υπηρεσίες, η ταυτότητα καθίσταται η μοναδική σταθερά που μπορεί να αξιοποιηθεί ως σημείο ελέγχου. Η βιβλιογραφία συμφωνεί ότι χωρίς ισχυρό, δυναμικό και πολυπαραγοντικό έλεγχο ταυτοτήτων, το Zero Trust δεν μπορεί να λειτουργήσει σε καμία από τις διαστάσεις του (CISA, 2021· Microsoft, 2021b· Cunningham et al., 2019).

Το identity-centric security δεν περιορίζεται στην απλή έννοια των credentials ή στη διαχείριση λογαριασμών χρήστη. Στη θεωρητική του βάση αντιμετωπίζει την ταυτότητα ως ένα σύνθετο, πολυεπίπεδο και δυναμικά εξελισσόμενο προφίλ, το οποίο περιλαμβάνει όχι μόνο τα βασικά στοιχεία αναγνώρισης ενός χρήστη, αλλά και το σύνολο των συμπεριφορικών του μοτίβων, το ιστορικό πρόσβασης, τις συνήθειες εργασίας, τα δικαιώματα, τις συσκευές που χρησιμοποιεί, τις προηγούμενες δραστηριότητες και το πλαίσιο κινδύνου μέσα στο οποίο αυτές λαμβάνουν χώρα (Adahman et al., 2022). Αυτή η πολυπλοκότητα αντικατοπτρίζει το γεγονός ότι η σύγχρονη παραβατική δραστηριότητα δεν βασίζεται σε επιθέσεις brute force, αλλά στην κλοπή, πλαστογράφηση ή κατάχρηση ταυτότητας – την πιο ύπουλη και αποτελεσματική μορφή κυβερνοεπίθεσης, όπως επιβεβαιώνουν και οι πρόσφατες έρευνες της Microsoft (2021a).

Η έννοια της ταυτότητας στο Zero Trust γίνεται κατανοητή μέσα από δύο βασικές θεωρητικές παραδοχές. Πρώτον, η ταυτότητα δεν είναι ποτέ απόλυτα αξιόπιστη· κάθε ταυτότητα, ανεξαρτήτως προέλευσης, πρέπει να επαληθεύεται συνεχώς. Δεύτερον, η ταυτότητα δεν πρέπει να εξισώνεται με την τοποθεσία ή το δίκτυο, διότι αυτά τα στοιχεία πλέον δεν αποτελούν αξιόπιστους δείκτες κινδύνου. Το identity-centric security μετατρέπει, λοιπόν, την ταυτοποίηση από μία στιγμιαία διαδικασία εισόδου σε μια συνεχή διαδικασία αξιολόγησης εμπιστοσύνης, όπου κάθε ενέργεια ελέγχεται ξανά και ξανά, με βάση δυναμικές παραμέτρους που σχετίζονται με το ποιος κάνει τι, από πού και με ποια χαρακτηριστικά συσκευής.

Η θεωρητική συμβολή της βιβλιογραφίας είναι εδώ καθοριστική. Μελέτες όπως αυτές των Buck και συν. (2021) δείχνουν ότι ολόκληρο το Zero Trust οικοσύστημα περιστρέφεται γύρω από την ταυτότητα ως πρωτογενή μηχανισμό ελέγχου. Η Forrester, που υπήρξε και ο θεμελιωτής της ορολογίας Zero Trust, υπογραμμίζει ότι η ταυτότητα αποτελεί πλέον το «νέο όριο ασφαλείας» σε έναν κόσμο όπου το δίκτυο δεν μπορεί πια να οριοθετηθεί. Η ταυτότητα δεν είναι απλώς ένας δείκτης· είναι το σημείο εκκίνησης όλων των μηχανισμών πολιτικής, επαλήθευσης και περιορισμού πρόσβασης.

Η λειτουργία του identity-centric security βασίζεται σε μια σειρά από επάλληλους μηχανισμούς που επιτρέπουν την ακριβή και συνεχή αξιολόγηση της αξιοπιστίας κάθε οντότητας. Στο πλαίσιο αυτό, η πολλαπλή επαλήθευση (MFA) λειτουργεί ως το πρώτο, αλλά όχι το μοναδικό επίπεδο ενίσχυσης της ταυτότητας. Σημαντικότερη είναι η υιοθέτηση μηχανισμών conditional access και risk-based authentication, οι οποίοι επιτρέπουν τη λήψη δυναμικών αποφάσεων πρόσβασης. Οι μηχανισμοί αυτοί αξιολογούν παράγοντες όπως η τοποθεσία, η συσκευή, το λογισμικό, η συμπεριφορά χρήστη, ο τύπος δεδομένων που ζητά, η σοβαρότητα του κινδύνου και η πιθανότητα παραβίασης (Microsoft, 2021b). Η ταυτότητα, συνεπώς, δεν είναι κάτι στατικό, αλλά μια συνεχώς επανεκτιμώμενη υπόθεση, όπου το επίπεδο εμπιστοσύνης μπορεί να αυξηθεί ή να μειωθεί ανάλογα με τις συνθήκες.

Η θεωρητική και πρακτική σημασία της ταυτότητας ενισχύεται περαιτέρω από το γεγονός ότι η πλειονότητα των σύγχρονων επιθέσεων βασίζεται στην παραβίαση εσωτερικών λογαριασμών. Η Campbell (2020) υπογραμμίζει ότι σε έναν κόσμο όπου τα όρια του δικτύου έχουν καταρρεύσει, η εμπιστοσύνη στον εσωτερικό χρήστη αποτελεί πλέον «ευπάθεια» και όχι πλεονέκτημα. Η ταυτότητα δεν μπορεί να αντιμετωπίζεται ως αξιόπιστη απλώς και μόνο επειδή σχετίζεται με μία εσωτερική IP ή μία εταιρική συσκευή. Το identity-centric security έρχεται να ανατρέψει αυτή τη λογική, επιβάλλοντας μια συνεχή επισκόπηση κάθε εσωτερικής δραστηριότητας, με θεωρητικό στόχο την εξάλειψη της έννοιας «εσωτερικός = ασφαλής».

Το identity-centric security ενσωματώνει, επίσης, τη διάσταση της συσκευής και του workload. Στην αρχιτεκτονική Zero Trust της CISA (2021), η ταυτότητα δεν αφορά μόνο τους ανθρώπινους χρήστες αλλά και τις συσκευές, τις εφαρμογές, τις υπηρεσίες και τα αυτοματοποιημένα συστήματα. Η κάθε μη ανθρώπινη οντότητα διαθέτει τη δική της ταυτότητα, η οποία πρέπει να επαληθεύεται, να ελέγχεται, να εμπλουτίζεται με μεταδεδομένα και να συνδέεται με συγκεκριμένες πολιτικές least privilege. Η επέκταση της

ταυτότητας πέρα από το ανθρώπινο επίπεδο αποτελεί θεμελιώδες στοιχείο της πιο σύγχρονης βιβλιογραφίας, ιδίως σε περιβάλλοντα cloud και DevOps, όπου οι υπηρεσίες δημιουργούνται και καταστρέφονται δυναμικά και η παραδοσιακή μοντελοποίηση πρόσβασης καταρρέει (Ferretti et al., 2021).

Η αξία του identity-centric security γίνεται ακόμη πιο εμφανής όταν εξετάσει κανείς την ανάγκη για αυτοματοποίηση. Οι πολιτικές Zero Trust είναι τόσο σύνθετες και δυναμικές που καθίσταται αδύνατη η χειροκίνητη διαχείρισή τους. Έτσι, η ταυτότητα γίνεται το σημείο στο οποίο βασίζεται η αυτοματοποίηση της εφαρμογής πολιτικών: οι ροές εργασίας, οι αναβαθμισμένες απαιτήσεις επαλήθευσης, οι αποφάσεις πρόσβασης και οι κανόνες περιορισμού εφαρμόζονται αυτόματα με βάση τα χαρακτηριστικά της ταυτότητας και την αξιολόγηση του κινδύνου σε πραγματικό χρόνο (Golden et al., 2021). Αυτό αποτελεί ίσως το μεγαλύτερο στρατηγικό πλεονέκτημα του identity-centric security: επιτρέπει στην οργάνωση να διαχειρίζεται τεράστιους όγκους δραστηριότητας σε κλίμακα, χωρίς να βασίζεται σε χειροκίνητες παρεμβάσεις.

Η βιβλιογραφία επισημαίνει επίσης ότι η ταυτότητα αποτελεί το θεμέλιο για τη λειτουργία των άλλων κρίσιμων αρχών του Zero Trust. Χωρίς αξιόπιστες και ολοκληρωμένες ταυτότητες δεν μπορεί να υπάρξει least privilege, καθώς η διακριτή περιορισμένη πρόσβαση απαιτεί ακριβή γνώση του ποιος είναι ο χρήστης και τι ακριβώς χρειάζεται. Δεν μπορεί να υπάρξει micro-segmentation, διότι οι ζώνες πρόσβασης πρέπει να σχετίζονται με συγκεκριμένες οντότητες. Δεν μπορεί να υπάρξει continuous verification, διότι η επανεκτίμηση του κινδύνου απαιτεί σταθερό και πλήρως μοντελοποιημένο σημείο αναφοράς. Με αυτή την έννοια, το identity-centric security δεν είναι ένα ακόμη συστατικό της αρχιτεκτονικής· είναι το θεμέλιο πάνω στο οποίο οικοδομούνται όλα τα υπόλοιπα.

Τέλος, η θεωρητική συζήτηση γύρω από το identity-centric security συνδέεται στενά με την ανάγκη για ενοποίηση διαφορετικών πηγών ταυτότητας και την αντιμετώπιση προβλημάτων interoperability. Μελέτες όπως αυτή των Bobbert και Scheerder (2020) επισημαίνουν ότι οι οργανισμοί συχνά διαθέτουν πολλαπλά, ασύνδετα συστήματα διαχείρισης ταυτότητας, κάτι που δημιουργεί θεωρητικά κενά στα «μονοπάτια εμπιστοσύνης». Η ολιστική προσέγγιση του Zero Trust απαιτεί την ενοποίηση ταυτοτήτων, τη χρήση κεντρικών καταλόγων, την υιοθέτηση open standards (όπως SAML, OAuth και OIDC) και την εφαρμογή τεχνικών που επιτρέπουν την πλήρη παρακολούθηση της ταυτότητας σε όλες τις πλατφόρμες και τα συστήματα (Kerman et al., 2020).

Το identity-centric security αποτελεί το θεωρητικό και πρακτικό θεμέλιο της αρχιτεκτονικής Zero Trust. Η ταυτότητα γίνεται ο νέος άξονας γύρω από τον οποίο περιστρέφονται η πρόσβαση, οι πολιτικές, η επαλήθευση και ο έλεγχος. Η υιοθέτηση αυτού του μοντέλου δεν αποτελεί απλώς τεχνική επιλογή, αλλά μια θεμελιώδη μετατόπιση στον τρόπο με τον οποίο κατανοείται η έννοια της εμπιστοσύνης στα σύγχρονα πληροφοριακά συστήματα: η εμπιστοσύνη δεν δίνεται, δεν προϋποτίθεται και δεν συνδέεται με το περιβάλλον. Πρέπει να αποδεικνύεται, να μετριέται και να επαναξιολογείται διαρκώς, σε κάθε βήμα, για κάθε χρήστη, κάθε συσκευή και κάθε υπηρεσία.

Κεφάλαιο 4. Μοντέλα Αναφοράς

4.1 Το BeyondCorp της Google

Το BeyondCorp αποτελεί ένα από τα πλέον επιδραστικά και θεμελιώδη μοντέλα στην εξέλιξη της σημερινής προσέγγισης Zero Trust. Η Google το ανέπτυξε ως απάντηση σε μια σειρά από επιθέσεις μεγάλης κλίμακας στις αρχές της δεκαετίας του 2010, καταλήγοντας στο συμπέρασμα ότι το παραδοσιακό perimeter-based μοντέλο δεν μπορούσε πλέον να ανταποκριθεί στο μέγεθος, την πολυπλοκότητα και τον δυναμισμό των σύγχρονων απειλών. Η βασική θεωρητική αρχή του BeyondCorp είναι η πλήρης αποσύνδεση της πρόσβασης από την τοποθεσία και το δίκτυο, κάτι που αποτελεί ριζοσπαστική απομάκρυνση από τις προηγούμενες προσεγγίσεις οι οποίες θεμελίωναν την εμπιστοσύνη στην ιδιότητα του «εντός εταιρικού δικτύου» (Ward & Beyer, 2014). Στο BeyondCorp, η πρόσβαση δεν αποτελεί δικαίωμα που απονέμεται λόγω σύνδεσης σε ένα «ασφαλές» περιβάλλον, αλλά αποτέλεσμα μιας λεπτομερώς ελεγχόμενης αξιολόγησης ταυτότητας και συσκευής η οποία επαναλαμβάνεται συνεχώς.

Ένα από τα βασικά θεωρητικά χαρακτηριστικά του BeyondCorp είναι ότι αντιμετωπίζει τον χρήστη και τη συσκευή ως πρωτεύοντα στοιχεία αξιολόγησης. Η Google αναδιαμόρφωσε το μοντέλο πρόσβασης ώστε κάθε αίτημα να εξετάζεται από το μηδέν, βασιζόμενο σε παράγοντες όπως η ταυτότητα του χρήστη, η κατάσταση της συσκευής, το είδος της εφαρμογής και ο βαθμός ευαισθησίας των δεδομένων που ζητούνται. Ενώ τα παραδοσιακά μοντέλα VPN επιτρέπουν την πρόσβαση σε ολόκληρους εταιρικούς πόρους μετά από την αρχική ταυτοποίηση, το BeyondCorp επιβάλλει granular, context-dependent έλεγχο σε κάθε ενέργεια. Αυτή η προσέγγιση αντικατοπτρίζει την αρχή «never trust, always verify» που στη συνέχεια υιοθετήθηκε ευρέως από τη Forrester, τη Microsoft και το NIST ως δομικό στοιχείο του Zero Trust (Cunningham, 2018· CISA, 2021).

Το μοντέλο BeyondCorp βασίζεται σε μια σειρά τεχνικών πυλώνων που αποτυπώνουν την ταυτότητά του ως αρχιτεκτονική πρωτοπορίας. Πρώτον, η Google εισήγαγε ένα ολοκληρωμένο σύστημα device inventory και device trust, το οποίο επιτρέπει στον οργανισμό να αποδίδει βαθμό εμπιστοσύνης σε κάθε συσκευή βάσει ενημερώσεων, διαμόρφωσης, ενδείξεων παραβίασης και ισχύος των πολιτικών ασφαλείας. Ο συνδυασμός device trust και identity trust συνιστά τον πυρήνα της αυτόνομης λήψης αποφάσεων,

δημιουργώντας ένα είδος «κοινωνικού συμβολαίου» μεταξύ χρήστη και συστήματος, όπου κάθε πράξη εξετάζεται υπό το μικροσκόπιο της πιθανότητας παραβίασης (Ward & Beyer, 2014).

Δεύτερον, το BeyondCorp απομακρύνει εντελώς την έννοια του «εμπιστεύσιμου εσωτερικού δικτύου». Όπως υπογραμμίζουν οι Ward και Beyer (2014), η Google αντιμετώπισε εσωτερικά και εξωτερικά δίκτυα ως ισοδύναμα από άποψη επικινδυνότητας. Αυτή η εξίσωση αποτελεί μια βαθιά θεωρητική μετατόπιση, καθώς καταργεί τον βασικό διαχωρισμό που στήριζε επί δεκαετίες τα παραδοσιακά μοντέλα ασφάλειας. Η επιρροή αυτής της απόφασης στη σημερινή συζήτηση είναι εμφανής: το Zero Trust, όπως αναπτύχθηκε στη συνέχεια από τη Forrester (Cunningham et al., 2019) και το NIST (Kerman et al., 2020), υιοθετεί πλήρως αυτήν την παραδοχή.

Τρίτον, το BeyondCorp εισήγαγε τη λογική της συνεχιζόμενης και διαστρωματωμένης επαλήθευσης. Σε αντίθεση με τις παλαιότερες μεθόδους όπου η επαλήθευση γινόταν μόνο κατά την είσοδο, στο BeyondCorp η εμπιστοσύνη είναι στιγμιαία, προσωρινή και συνεχώς υπό αναθεώρηση. Αυτή η προσέγγιση προαναγγέλλει την αρχή της continuous verification που αργότερα αναδείχθηκε σε βασικό στοιχείο του Zero Trust από το NIST SP 800-207 και από το μοντέλο ωριμότητας της Microsoft (Microsoft, 2021b).

Η θεωρητική επιρροή του BeyondCorp υπήρξε τεράστια. Το έργο της Google θεωρείται η πρώτη μεγάλη υλοποίηση Zero Trust σε πραγματικό περιβάλλον παγκόσμιας κλίμακας, με την επιστημονική βιβλιογραφία να αναγνωρίζει ότι αποτέλεσε τον καταλύτη για τη μετάβαση της συζήτησης από την αμιγώς θεωρητική σφαίρα σε πρακτικά υλοποιήσιμες αρχιτεκτονικές (Buck et al., 2021). Επιπλέον, η Google, δημοσιεύοντας λεπτομερείς τεχνικές αναλύσεις για το BeyondCorp, άνοιξε τον δρόμο για την υιοθέτηση open standards, τη χρήση identity-driven αλγορίθμων πρόσβασης και την ανάπτυξη ενοποιημένων μηχανισμών αξιολόγησης κινδύνου.

Η επιρροή του BeyondCorp διαφαίνεται επίσης στη σύγχρονη οργανωσιακή κουλτούρα ασφάλειας. Η μετάβαση από ένα περιβάλλον «εμπιστοσύνης λόγω τοποθεσίας» σε ένα περιβάλλον όπου η εμπιστοσύνη πρέπει να αποδεικνύεται, οδήγησε σε νέα μοντέλα διακυβέρνησης, αναδιαμόρφωση διαδικασιών και νέες μορφές συνεργασίας μεταξύ τμημάτων IT, DevOps και ασφάλειας. Μελέτες όπως του Campbell (2020) επιβεβαιώνουν ότι η ριζική αλλαγή της Google αποτέλεσε παράγοντα επιτάχυνσης στη βιομηχανία, καθώς

απέδειξε ότι είναι εφικτή η πλήρης κατάργηση του VPN χωρίς αύξηση του κινδύνου, αλλά με ενίσχυση της αποτελεσματικότητας.

Σε γενικές γραμμές, το BeyondCorp σηματοδότησε μια ιστορική καμπή στη θεωρητική εξέλιξη της κυβερνοασφάλειας, εισάγοντας ένα νέο παράδειγμα όπου η ταυτότητα και η κατάσταση της συσκευής έχουν μεγαλύτερη σημασία από την τοποθεσία, το δίκτυο ή τους στατικούς μηχανισμούς προστασίας. Η θεμελίωση αυτής της νέας προσέγγισης αποτέλεσε τη βάση για όλα τα επόμενα μοντέλα Zero Trust, συμπεριλαμβανομένου του NIST SP 800-207, το οποίο συστηματοποίησε θεωρητικά αυτό που η Google είχε ήδη δοκιμάσει στην πράξη.

4.2 Βιβλιογραφία για το BeyondCorp

Η βιβλιογραφική παραγωγή της Google σχετικά με το BeyondCorp αποτελεί ένα από τα πιο σημαντικά σώματα τεκμηρίωσης για την πρακτική υλοποίηση μιας Zero Trust αρχιτεκτονικής. Τα τεχνικά papers που δημοσιεύτηκαν μέσω του USENIX Login αποτελούν ουσιαστικά «αναφορές πεδίου», παρουσιάζοντας όχι μόνο το θεωρητικό πλαίσιο αλλά και τα πρακτικά εμπόδια, τις προκλήσεις και τις τεχνικές λύσεις που αναπτύχθηκαν για την κλιμάκωση του μοντέλου. Η μελέτη αυτών των papers αποτελεί καθοριστικό βήμα για κάθε ερευνητή που επιχειρεί να αναλύσει το Zero Trust σε πραγματικές συνθήκες εφαρμογής.

Στο πρώτο paper, οι Ward και Beyer (2014) παρουσιάζουν την κεντρική φιλοσοφία που οδήγησε στη δημιουργία του BeyondCorp. Η Google διαπίστωσε ότι οι επιθέσεις στόχευαν ολοένα περισσότερο σε εργαζομένους μέσω spear-phishing, credential theft και συσκευών χαμηλής προστασίας. Η τοποθέτηση όλης της «εμπιστοσύνης» στο firewall καθιστούσε το εσωτερικό δίκτυο εξαιρετικά ευάλωτο: μία επιτυχής παραβίαση ενός λογαριασμού οδηγούσε σε πλήρη πρόσβαση σε κρίσιμα συστήματα. Οι συγγραφείς περιγράφουν πώς αυτή η διαπίστωση οδήγησε στην απόφαση να αντιμετωπίζονται όλες οι συνδέσεις, από όπου κι αν προέρχονται, ως εν δυνάμει κακόβουλες. Η ανάλυση των Ward και Beyer δεν περιορίζεται όμως σε ένα θεωρητικό πλαίσιο· αναλύει με λεπτομέρεια τον τρόπο με τον οποίο η Google αναπτύσσει ένα ενιαίο σύστημα δημιουργίας και αξιολόγησης ταυτότητας για χρήστες, συσκευές και υπηρεσίες.

Στο δεύτερο paper, η Google επεκτείνει την ανάλυση παρουσιάζοντας την πρακτική αρχιτεκτονική υλοποίηση του BeyondCorp, δίνοντας έμφαση στη διαστρωμάτωση των συστημάτων πρόσβασης, την αποσύνδεση των εφαρμογών από το εταιρικό δίκτυο και τη

δημιουργία granular πολιτικών. Η βιβλιογραφία υπογραμμίζει ότι αυτά τα papers αποτέλεσαν την πρώτη ολοκληρωμένη περιγραφή μιας Zero Trust αρχιτεκτονικής πριν ακόμη η έννοια καθιερωθεί ακαδημαϊκά ή υιοθετηθεί από κυβερνητικούς φορείς (Buck et al., 2021). Μάλιστα, η Forrester βασίστηκε στις αρχές αυτές για την επέκταση του Zero Trust eXtended framework, αναγνωρίζοντας τη Google ως τον πρώτο οργανισμό που κατάφερε να μεταφέρει τη θεωρία της μηδενικής εμπιστοσύνης σε καθημερινή λειτουργική πρακτική (Cunningham, 2018).

Τα BeyondCorp papers αναλύουν σε βάθος τη σημασία της πλήρους διαφάνειας στον τρόπο με τον οποίο γίνεται η πρόσβαση. Η Google δημιούργησε έναν μηχανισμό συνεχούς συλλογής δεδομένων (telemetry) για συσκευές, χρήστες και εφαρμογές, ο οποίος επιτρέπει σε ένα κεντρικό σύστημα λήψης αποφάσεων να εκτιμά σε πραγματικό χρόνο την πιθανότητα παραβίασης. Η θεώρηση αυτή συνδέεται στενά με τα σύγχρονα μοντέλα dynamic policy enforcement που αναπτύχθηκαν αργότερα από το NIST και τη Microsoft (Microsoft, 2021b· Kerman et al., 2020). Στην πράξη, η Google υλοποίησε πριν από όλους αυτό που σήμερα ονομάζουμε continuous verification, παρέχοντας μια ενιαία πλατφόρμα συσχέτισης γεγονότων και αυτόματης επιβολής πολιτικών.

Ένα άλλο σημαντικό στοιχείο των papers είναι η έμφαση στον οργανωσιακό μετασχηματισμό που απαιτείται για την επιτυχία του BeyondCorp. Η Google δεν αντιμετώπισε το Zero Trust ως ένα τεχνολογικό έργο αλλά ως πολυεπίπεδη αναδιάρθρωση διαδικασιών. Η λογική αυτή συνδέεται με τα συμπεράσματα μελετών όπως αυτές των Golden και συν. (2021) και Deloitte (2021), που τονίζουν ότι η υιοθέτηση Zero Trust απαιτεί μεταβολή κουλτούρας και όχι απλή προσθήκη εργαλείων. Τα BeyondCorp papers αποτυπώνουν ακριβώς αυτήν τη διάσταση: για να λειτουργήσει η νέα αρχιτεκτονική, χρειάστηκε ανασχεδιασμός των workflows, εκπαίδευση προσωπικού και αναθεώρηση διαδικασιών πρόσβασης στα δεδομένα.

Πέρα από την οργανωσιακή και τεχνική μετάβαση, τα papers αναλύουν επίσης την κλιμάκωση του BeyondCorp. Η Google, ως οργανισμός με δεκάδες χιλιάδες εργαζομένους, εκατοντάδες συστήματα και υβριδική υποδομή, έπρεπε να εξασφαλίσει ότι το νέο σύστημα πρόσβασης θα μπορούσε να λειτουργήσει χωρίς bottlenecks, καθυστερήσεις ή μείωση της παραγωγικότητας. Οι συγγραφείς περιγράφουν πώς υιοθέτησαν μηχανισμούς caching, load balancing και αυτοματοποιημένων verification pipelines ώστε η λήψη αποφάσεων πρόσβασης να μπορεί να γίνει σε κλάσματα του δευτερολέπτου. Αυτή η διάσταση της έρευνας αποτέλεσε αφετηρία για μεταγενέστερες μελέτες που εξετάζουν το Zero Trust σε

περιβάλλοντα cloud και multi-tenant, όπως οι Ferretti και συν. (2021), οι οποίοι περιγράφουν πώς οι Zero Trust μηχανισμοί ενσωματώνονται σε μεταβλητά περιβάλλοντα δυναμικής δημιουργίας υπηρεσιών.

Η ανάλυση των BeyondCorp papers δείχνει επίσης ότι η Google έδωσε ιδιαίτερο βάρος στην αποφυγή «παράγωγων» ευπαθειών. Οι συγγραφείς επισημαίνουν ότι η μετάβαση σε Zero Trust δεν είναι μόνο ζήτημα αφαίρεσης των privileges, αλλά και της αποφυγής δημιουργίας νέων μοναδικών σημείων αποτυχίας. Το σύστημα έπρεπε να είναι αποκεντρωμένο, ανορθόδοξο για τους επιτιθέμενους, αλλά πλήρως διαχειρίσιμο για τους διαχειριστές. Αυτό προαναγγέλλει τις σημερινές συζητήσεις για survivable zero trust και fault-tolerant identity infrastructures (Ferretti et al., 2021).

Τα BeyondCorp papers αποτέλεσαν επίσης την αφετηρία για την υιοθέτηση Zero Trust μοντέλων από κρατικούς οργανισμούς. Οι βασικές αρχές του BeyondCorp μεταφέρθηκαν σχεδόν αυτούσιες στις οδηγίες της CISA και στο NIST SP 800-207, με το NIST να συστηματοποιεί θεωρητικά αυτό που στη Google λειτουργούσε ως πρακτικό μοντέλο (CISA, 2021· Kerman et al., 2020). Η βιβλιογραφία αναγνωρίζει την επίδραση αυτή ως ένα από τα σημαντικότερα παραδείγματα bottom-up διαμόρφωσης προτύπων: αντί η θεωρία να προηγηθεί της πρακτικής, η πρακτική της Google διαμόρφωσε τη θεωρία.

Τα BeyondCorp papers αποτελούν ένα από τα πιο σημαντικά σώματα τεκμηρίωσης στην ιστορία της κυβερνοασφάλειας. Προσφέρουν όχι μόνο αναλυτική τεχνική περιγραφή μιας πραγματικής Zero Trust υλοποίησης, αλλά και θεμελιώδη κατανόηση των ψυχολογικών, οργανωσιακών και τεχνικών πτυχών που απαιτούνται για την επιτυχή εφαρμογή της. Η μεγάλη επιρροή τους στην ακαδημαϊκή και βιομηχανική συζήτηση επιβεβαιώνει ότι η Google δεν εισήγαγε απλώς ένα νέο μοντέλο, αλλά διαμόρφωσε το υπόβαθρο πάνω στο οποίο βασίζεται ολόκληρη η σύγχρονη επιστήμη του Zero Trust.

4.3 4.3 Το NIST SP 800-207

Το NIST SP 800-207 αποτελεί το πλέον συστηματικό και θεσμικά αναγνωρισμένο θεωρητικό πλαίσιο για τη διαμόρφωση και υλοποίηση αρχιτεκτονικών Zero Trust. Η δημοσίευση του από το National Institute of Standards and Technology αποτέλεσε ορόσημο στην εξελικτική πορεία του Zero Trust, διότι μετατρέπει τις αποσπασματικές πρακτικές της βιομηχανίας σε ένα ολοκληρωμένο, τυποποιημένο και καθολικά εφαρμόσιμο μοντέλο. Σε αντίθεση με το BeyondCorp, το οποίο γεννήθηκε μέσα από την πρακτική ανάγκη της Google, το SP 800-207

έχει ως στόχο να προσφέρει ένα αφαιρετικό, καθολικό και διαλειτουργικό πλαίσιο που μπορεί να υιοθετηθεί από οργανισμούς οποιουδήποτε μεγέθους ή δομής (Kerman et al., 2020). Στο επίκεντρο της θεωρίας του βρίσκεται η θεμελιώδης παραδοχή ότι κανένας χρήστης, συσκευή, εφαρμογή ή συστατικό δεν είναι εγγενώς αξιόπιστο, γεγονός που καθιστά την συνεχώς ανανεούμενη επαλήθευση απαραίτητη σε κάθε αίτημα πρόσβασης.

Η αρχιτεκτονική του SP 800-207 στηρίζεται στον συνδυασμό επτά βασικών αρχών: στον δυναμικό έλεγχο ταυτότητας, στον περιορισμό πρόσβασης μέσω least privilege, στην επιβολή πολιτικών βάσει αποδεικτικών στοιχείων, στην εποπτεία και καταγραφή όλων των δραστηριοτήτων, στη συνεχή αξιολόγηση κινδύνου, στην ελαχιστοποίηση της εμπιστοσύνης στο δίκτυο και στη χρήση προστατευμένων καναλιών. Η αναλυτική περιγραφή αυτών των αρχών από το NIST έρχεται να συστηματοποιήσει πρακτικές που ήδη είχαν αναδειχθεί στη βιομηχανία και στη βιβλιογραφία. Η σύζευξη ταυτότητας και εμπιστοσύνης που είχε εισαγάγει η Google στο BeyondCorp αποκτά εδώ αφαιρετική μορφή, με την ταυτότητα να αποκτά θεσμικό ρόλο ως η πρωτεύουσα βάση λήψης αποφάσεων (CISA, 2021).

Η αρχιτεκτονική Zero Trust του NIST προτείνει μια σειρά από λειτουργικές οντότητες: τον Policy Engine, τον Policy Administrator και τους Policy Enforcement Points. Ο Policy Engine είναι υπεύθυνος για τη λήψη των αποφάσεων πρόσβασης, βασιζόμενος στη συλλογή δεδομένων κινδύνου από πολλαπλές πηγές. Ο Policy Administrator υλοποιεί τις εντολές, ενώ οι Enforcement Points βρίσκονται στα σημεία όπου πραγματοποιείται η πραγματική επιβολή. Αυτή η τριμερής αρχιτεκτονική έχει σημαντικές θεωρητικές προεκτάσεις: διαφοροποιεί την πολιτική από την εκτέλεση, επιτρέπει την εφαρμογή granular κανόνων και ενισχύει τη δυνατότητα διαστρωμάτωσης ασφαλείας. Η διακριτότητα αυτή επιτρέπει σε οργανισμούς να ενσωματώσουν το Zero Trust χωρίς να απαιτείται πλήρης ανακατασκευή των υποδομών, κάτι ιδιαίτερα σημαντικό για κρατικούς φορείς και μεγάλους οργανισμούς (Kerman et al., 2020).

Το SP 800-207 ενισχύει επίσης τη θεωρητική βάση του Zero Trust μέσω της έννοιας του trust algorithm. Η αρχιτεκτονική δεν βασίζεται πλέον σε δυαδικές αποφάσεις, αλλά σε υπολογισμούς που λαμβάνουν υπόψη παράγοντες όπως η υγεία της συσκευής, η τοποθεσία, η συμπεριφορά χρήστη, το ιστορικό πρόσβασης και ο τύπος των δεδομένων. Η υιοθέτηση τέτοιων αλγοριθμικών μηχανισμών αποτελεί τη βάση για πιο εξελιγμένες μορφές αυτοματοποίησης και επιτρέπει τη συνεχή προσαρμογή στις συνθήκες απειλών. Η Microsoft, στη δική της υλοποίηση Zero Trust, βασίζεται εκτεταμένα σε τέτοιους μηχανισμούς,

υιοθετώντας risk-based conditional access για τη λήψη αποφάσεων σε πραγματικό χρόνο (Microsoft, 2021b).

Ένα ακόμη κεντρικό στοιχείο του SP 800-207 είναι η διαλειτουργικότητα. Ο στόχος του NIST δεν είναι να προτείνει ένα συγκεκριμένο σύνολο προϊόντων ή λύσεων, αλλά να παρουσιάσει ένα πλαίσιο που να μπορεί να εφαρμοστεί πάνω σε ετερογενή περιβάλλοντα. Η σημαντικότητα αυτής της φιλοσοφίας αναδεικνύεται στη διεθνή βιβλιογραφία: μελέτες όπως η Buck et al. (2021) δείχνουν ότι ένα από τα σημαντικότερα προβλήματα στην υλοποίηση Zero Trust είναι η έλλειψη συνοχής μεταξύ συσκευών, δικτύων, εφαρμογών και συστημάτων ταυτοποίησης. Η προώθηση open standards, API-driven ενοποίησης και διαστρωμάτωσης υπηρεσιών που προτείνει το NIST έρχεται ως απάντηση σε αυτό το ζήτημα.

Το SP 800-207 εισάγει επίσης μια σημαντική θεωρητική διάκριση ανάμεσα στη λογική και στη φυσική τοπολογία. Στο Zero Trust, η λογική τοπολογία – δηλαδή οι ροές πρόσβασης, οι σχέσεις εμπιστοσύνης και οι πολιτικές – υπερισχύει της φυσικής τοπολογίας του δικτύου. Αυτό συνδέεται άμεσα με την αρχή της micro-segmentation και της επιχειρησιακής αναδιάρθρωσης των data flows, όπως έχει ήδη προαναφερθεί στη βιβλιογραφία από ερευνητές όπως οι Ferretti et al. (2021). Το NIST αναδεικνύει αυτό το στοιχείο ως πρωτεύον, τονίζοντας ότι η προστασία της περιμέτρου είναι πλέον ανεπαρκής, καθώς οι επιθέσεις στοχεύουν κυρίως lateral movement, credential theft και privilege escalation.

Τέλος, το SP 800-207 έχει ιδιαίτερη σημασία και για το θεωρητικό του υπόβαθρο. Αποτελεί τη βάση πάνω στην οποία οι κρατικές υπηρεσίες στις ΗΠΑ διαμόρφωσαν τις στρατηγικές τους γύρω από το Zero Trust, ενώ επηρέασε βαθιά οργανισμούς παγκοσμίως. Η CISA, το 2021, αναπτύσσει το δικό της Zero Trust Maturity Model, βασισμένη άμεσα στις αρχές του NIST, επιβεβαιώνοντας ότι το SP 800-207 λειτουργεί όχι ως framework μιας εταιρείας, αλλά ως διεθνές πρότυπο (CISA, 2021). Η επιρροή του είναι καθοριστική στο πώς αντιλαμβανόμαστε πλέον την αρχιτεκτονική ασφάλειας.

4.4 Συγκριτική αξιολόγηση

Η συγκριτική μελέτη των BeyondCorp και NIST SP 800-207 αναδεικνύει μια εξελικτική συνέχεια στη θεωρία του Zero Trust, όπου το BeyondCorp λειτουργεί ως πρωτοποριακή πρακτική υλοποίηση και το NIST ως θεωρητική συστηματοποίηση. Το BeyondCorp ξεκινά από τη λειτουργική πραγματικότητα της Google και διαμορφώνει μια αρχιτεκτονική βαθιά προσανατολισμένη στον έλεγχο ταυτότητας και συσκευής. Η θεώρηση αυτή αντικατοπτρίζει

την ανάγκη της Google για απορρόφηση επιθέσεων μεγάλης κλίμακας και την αντιμετώπιση του «εσωτερικού δικτύου» ως εξίσου επικίνδυνου με το εξωτερικό (Ward & Beyer, 2014). Το μοντέλο αυτό αποτελεί την πρώτη πραγματική απόδειξη ότι μια μεγάλη οργάνωση μπορεί να λειτουργεί εντελώς χωρίς perimeter-based ελέγχους.

Σε αντίθεση με το BeyondCorp, το SP 800-207 δεν περιγράφει την εμπειρία ενός συγκεκριμένου οργανισμού, αλλά προσφέρει την αφαιρετική γλώσσα, τις οριστικές έννοιες και τις απαιτήσεις που επιτρέπουν στον ιδιωτικό και δημόσιο τομέα να κατανοήσουν και να εφαρμόσουν το Zero Trust με συνέπεια και διαλειτουργικότητα. Ενώ το BeyondCorp επικεντρώνεται στη συσκευή και στον χρήστη ως κύριους φορείς εμπιστοσύνης, το NIST δίνει μεγαλύτερη έμφαση στις λειτουργικές σχέσεις μεταξύ των στοιχείων της αρχιτεκτονικής, στη μακρο-δομή του συστήματος λήψης αποφάσεων και στην έννοια της διαστρώσιμης πολιτικής (Kerman et al., 2020).

Παρά τη θεωρητική τους διαφοροποίηση, τα δύο μοντέλα συγκλίνουν σε κρίσιμες αρχές: στην αποδυνάμωση της περιμέτρου ως μηχανισμού προστασίας, στη συνεχή επαλήθευση, στον έλεγχο ταυτότητας ως βασικό σημείο αξιολόγησης, στη σημασία του device health και στην ανάγκη granular επιβολής πολιτικών. Η βιβλιογραφία αναγνωρίζει ότι οι αρχές αυτές αποτέλεσαν τη βάση για τη μετέπειτα εξέλιξη διεθνών προτύπων και βιομηχανικών πρακτικών (Buck et al., 2021).

Η κύρια διαφορά βρίσκεται στον στόχο. Το BeyondCorp επιδιώκει να καταστήσει τη Google πιο ασφαλή και να αντιμετωπίσει συγκεκριμένες απειλές που σχετίζονται με τη δομή της εταιρείας, ενώ το SP 800-207 επιδιώκει να καταστήσει το Zero Trust θεωρητικά καθολικό. Το πρώτο αποτελεί παράδειγμα εφαρμογής, ενώ το δεύτερο αποτελεί πλαίσιο. Το BeyondCorp εισάγει την πρακτική λογική· το NIST εισάγει τη θεωρητική βάση.

4.5 Κριτική ανάλυση της διεθνούς βιβλιογραφίας

Η διεθνής βιβλιογραφία για το Zero Trust έχει επεκταθεί ραγδαία την τελευταία πενταετία, αντικατοπτρίζοντας την εντεινόμενη ανάγκη για νέα μοντέλα ασφάλειας σε ένα περιβάλλον όπου οι παραδοσιακές αρχιτεκτονικές δεν επαρκούν. Οι περισσότερες σύγχρονες μελέτες αναδεικνύουν ως κοινό συμπέρασμα ότι το Zero Trust δεν είναι ένα εργαλείο αλλά ένα οικοσύστημα αρχών. Η εργασία των Buck et al. (2021) αποτελεί ίσως την πιο ολοκληρωμένη συστηματική ανασκόπηση, καταδεικνύοντας ότι η πλειονότητα της υπάρχουσας γνώσης είναι κατακερματισμένη και ότι υπάρχουν σημαντικά κενά στις μεθοδολογίες εφαρμογής. Η

μελέτη τους εντοπίζει έλλειψη ενιαίας ορολογίας, ασυμβατότητα μεταξύ προϊόντων και περιορισμένη εμπειρική τεκμηρίωση από οργανισμούς εκτός του τεχνολογικού τομέα.

Άλλες μελέτες, όπως αυτή των Adahman et al. (2022), εξετάζουν το Zero Trust από οικονομική σκοπιά, αναδεικνύοντας ότι η εφαρμογή του μπορεί να είναι ιδιαίτερα αποδοτική όταν αξιοποιείται για μείωση του κινδύνου παραβίασης. Το κόστος υλοποίησης μιας Zero Trust αρχιτεκτονικής μπορεί να είναι υψηλό, αλλά το προσδοκώμενο κόστος ζημίας από περιστατικά ασφάλειας μειώνεται σημαντικά. Αυτή η οικονομική διάσταση αποτελεί κρίσιμο στοιχείο για οργανισμούς που αντιμετωπίζουν το Zero Trust ως επένδυση και όχι ως τεχνολογική μόδα.

Η βιβλιογραφία αναδεικνύει επίσης ότι η υλοποίηση Zero Trust απαιτεί βαθύ οργανωσιακό μετασχηματισμό. Μελέτες όπως της Deloitte (2021) και των Golden et al. (2021) υπογραμμίζουν ότι η τεχνολογική εφαρμογή αποτελεί μόνο ένα μέρος της μετάβασης. Η επιτυχία εξαρτάται από την εκπαίδευση, τη συνεργασία μεταξύ τμημάτων, τη διαχείριση αλλαγής και τη διαμόρφωση κουλτούρας «μηδενικής εμπιστοσύνης». Τα BeyondCorp papers προσφέρουν μια εμπειρική επιβεβαίωση αυτής της άποψης, καθώς τεκμηριώνουν την πολυσύνθετη οργανωσιακή προσπάθεια που απαιτείται για να λειτουργήσει το Zero Trust σε κλίμακα (Ward & Beyer, 2014).

Ωστόσο, η βιβλιογραφία δεν είναι ομοιογενής ούτε χωρίς περιορισμούς. Πολλές εργασίες προέρχονται από βιομηχανικούς οργανισμούς, γεγονός που δημιουργεί μεροληψία υπέρ των προτεινόμενων λύσεων. Άλλες μελέτες εστιάζουν κυρίως σε cloud περιβάλλοντα, μειώνοντας τη δυνατότητα γενίκευσης σε βιομηχανικούς ή κυβερνητικούς τομείς. Επιπλέον, η θεωρητική τεκμηρίωση του Zero Trust εξακολουθεί να εξελίσσεται, με το NIST SP 800-207 να αποτελεί περισσότερο οδικό χάρτη παρά πλήρη μεθοδολογία. Το γεγονός ότι οι οργανισμοί ενσωματώνουν το Zero Trust με διαφορετικούς τρόπους δημιουργεί έλλειψη συγκρίσιμων δεδομένων και εμπειρικών μοντέλων αξιολόγησης.

Παρά τα παραπάνω, η βιβλιογραφία συμφωνεί σε μία κρίσιμη διάσταση: το Zero Trust αποτελεί το κυρίαρχο μοντέλο κυβερνοασφάλειας για τις επόμενες δεκαετίες. Οι μελέτες αναγνωρίζουν ότι η αύξηση των απειλών, ο κατακερματισμός των συστημάτων, η διασπορά των δεδομένων και η κυριαρχία του cloud καθιστούν αναγκαία μια θεμελιωδώς διαφορετική προσέγγιση από εκείνη του perimeter security. Το BeyondCorp έδειξε την πρακτική δυνατότητα· το NIST έδειξε τον δρόμο θεωρητικά. Η διεθνής βιβλιογραφία συνεχίζει να

γεφυρώνει τα κενά και να αναπτύσσει εργαλεία, μεθοδολογίες και αρχιτεκτονικές που ενισχύουν την ωριμότητα του Zero Trust.

Κεφάλαιο 5. Εφαρμογές και Πρακτικές Zero Trust

5.1 IAM, MFA και risk-based authentication

Η εφαρμογή των αρχών Zero Trust σε πραγματικά περιβάλλοντα βασίζεται πρωτίστως στην ωριμότητα των μηχανισμών διαχείρισης ταυτότητας και πρόσβασης (IAM), στην ενίσχυση των διαδικασιών επαλήθευσης μέσω πολυπαραγοντικής αυθεντικοποίησης (MFA) και στη χρήση δυναμικών, ευφυών μεθόδων risk-based authentication. Αυτά τα στοιχεία δεν αποτελούν απλώς τεχνικές λειτουργίες αλλά λειτουργικές, οργανωσιακές και θεωρητικές υποδομές που καθιστούν εφικτή τη μετάβαση από τα παραδοσιακά μοντέλα ασφάλειας σε ένα περιβάλλον Zero Trust. Η διεθνής βιβλιογραφία συγκλίνει στο συμπέρασμα ότι η ωριμότητα ενός οργανισμού ως προς το Zero Trust εξαρτάται σε υπέρμετρο βαθμό από την ποιότητα, την προσαρμοστικότητα και την αυτοματοποίηση των υποδομών IAM του (Adahman et al., 2022· Cunningham et al., 2019· Golden et al., 2021).

Η διαχείριση ταυτότητας (IAM) αποτελεί την πρωταρχική και αναγκαία βάση ενός περιβάλλοντος Zero Trust, αφού σε αυτό το μοντέλο η ταυτότητα είναι το σημείο εκκίνησης όλων των μηχανισμών ασφάλειας. Το IAM δεν ορίζεται πλέον απλώς ως ένα σύνολο λειτουργιών δημιουργίας λογαριασμών και διαχείρισης δικαιωμάτων· αντιθέτως, αποτελεί μια δυναμική ροή που περιλαμβάνει τους κύκλους ζωής των ταυτοτήτων, την ενοποίηση πολλαπλών πηγών ταυτοποίησης, την εφαρμογή granular πολιτικών πρόσβασης και τη συνεχή ανανέωση των δικαιοδοτήσεων. Στη σύγχρονη βιβλιογραφία αναδεικνύεται η ανάγκη για ενοποίηση συστημάτων IAM, αφού πολλά οργανωτικά περιβάλλοντα πάσχουν από κατακερματισμό ταυτοτήτων, γεγονός που δημιουργεί κενά ασφαλείας, διπλές εγγραφές και αδυναμία ολιστικής παρακολούθησης (Bobbert & Scheerder, 2020). Στο Zero Trust, το IAM θεωρείται λειτουργική προϋπόθεση για την εφαρμογή least privilege, δεδομένου ότι η λεπτομερής διαχείριση των δικαιωμάτων απαιτεί ενιαία και συνεπή οντολογία ταυτότητας.

Η διεθνής βιβλιογραφία συνδέει άμεσα την αποτελεσματικότητα του IAM με την ανάγκη για συνεχώς ενισχυόμενους μηχανισμούς αυθεντικοποίησης. Η παραβίαση διαπιστευτηρίων αποτελεί τον συχνότερο μηχανισμό εισόδου των επιτιθέμενων σε εταιρικά συστήματα και η MFA έχει αποδειχθεί ως ο αποτελεσματικότερος τρόπος παρεμπόδισης αυτών των επιθέσεων, μειώνοντας την πιθανότητα επιτυχίας κατά ένα ποσοστό που αγγίζει τις τάξεις

μεγέθους (Microsoft, 2021a). Η MFA στο Zero Trust δεν περιορίζεται στον κλασικό συνδυασμό κωδικού και OTP. Εντάσσεται σε ένα ευρύ πλαίσιο αξιολόγησης, όπου η πολυπαραγοντική ταυτοποίηση λειτουργεί ως το πρώτο επίπεδο μιας πολυδιάστατης αλυσίδας επαλήθευσης. Μελέτες όπως αυτή των Golden et al. (2021) αναδεικνύουν ότι η MFA αποτελεί θεμέλιο του identity-centric security, καθώς επιτρέπει την ενίσχυση των σημείων ελέγχου πριν από την εφαρμογή πιο σύνθετων risk-based μηχανισμών.

Το Zero Trust, ωστόσο, υπερβαίνει τη στατική MFA και προχωρά σε μια πολύ πιο εξελιγμένη μορφή ελέγχου: τη risk-based authentication. Σε αυτή την προσέγγιση, κάθε αίτημα πρόσβασης αξιολογείται με βάση ένα σύνολο δυναμικών κριτηρίων, τα οποία περιλαμβάνουν τη συμπεριφορά του χρήστη, την κατάσταση της συσκευής, την τοποθεσία, το ωράριο, το ιστορικό κινδύνου, τη φύση των δεδομένων και μετρήσεις anomaly detection (Microsoft, 2021b). Ουσιαστικά, ο οργανισμός εκτιμά σε πραγματικό χρόνο τον βαθμό επικινδυνότητας κάθε αιτήματος και προσαρμόζει την αυστηρότητα της ταυτοποίησης ανάλογα με αυτό τον κίνδυνο.

Η risk-based authentication έχει θεωρητικό υπόβαθρο που προέρχεται από τις αρχές του NIST, το οποίο επισημαίνει ότι η λήψη αποφάσεων πρέπει να βασίζεται σε υπολογιστικά μοντέλα εμπιστοσύνης, τα οποία αξιοποιούν πληροφορίες telemetry για να υποστηρίξουν δυναμικές πολιτικές πρόσβασης (Kerman et al., 2020). Όπως τονίζει η CISA (2021), η μετάβαση από τη στατική MFA στη risk-adaptive MFA αποτελεί το κρίσιμο σημείο ωριμότητας που διαχωρίζει μια «βασική» εφαρμογή Zero Trust από μια «ώριμη» και αυτοματοποιημένη εφαρμογή. Σε αυτή τη λογική, η πρόσβαση δεν είναι πλέον binary, αλλά πολυεπίπεδη, ρευστή και βασισμένη σε συνεχή αξιολόγηση.

Ένας άλλος κρίσιμος παράγοντας είναι η επέκταση της ταυτότητας πέρα από τον χρήστη. Στο Zero Trust, η ταυτότητα περιλαμβάνει συσκευές, εφαρμογές, APIs, κοντέινερ και services, τα οποία διαθέτουν το δικό τους σύστημα αξιολόγησης εμπιστοσύνης. Οι Ferretti et al. (2021) υπογραμμίζουν ότι, ειδικά στα περιβάλλοντα cloud, η ταυτότητα των workloads είναι εξίσου σημαντική με την ταυτότητα ανθρώπινων χρηστών, καθώς οι δυναμικές υπηρεσίες απαιτούν granular και αυτόματο μηχανισμό identity-based access. Η εφαρμογή IAM σε αυτά τα περιβάλλοντα απαιτεί τη δημιουργία ενοποιημένων trust stores, τα οποία συνδέουν την ταυτότητα κάθε υπηρεσίας με την πολιτική least privilege που της αντιστοιχεί.

Η role-based και attribute-based access control αρχιτεκτονική (RBAC/ABAC) αποκτά νέα διάσταση στο Zero Trust, καθώς συνδυάζεται με contextual attributes, όπως device risk

scores, behavioral risk scores και signals από machine-learning systems για ανίχνευση ανωμαλιών. Η υλοποίηση ABAC αποτελεί βασική προϋπόθεση για την εφαρμογή granular πολιτικών σε περιβάλλοντα υβριδικά, πολυ-συσκευών και multi-cloud. Η βιβλιογραφία δείχνει ότι οι οργανισμοί που εφαρμόζουν ABAC σε συνδυασμό με real-time telemetry επιτυγχάνουν τον υψηλότερο βαθμό ευελιξίας, αλλά και το μεγαλύτερο επίπεδο μείωσης κινδύνου (Adahman et al., 2022).

Στο πλαίσιο του Zero Trust, η διαχείριση πρόσβασης δεν είναι μόνο τεχνική διαδικασία αλλά θεμελιώδης πολιτική λειτουργία. Όπως δείχνουν οι Golden et al. (2021), η ωριμότητα του IAM εξαρτάται από την ικανότητα του οργανισμού να ενσωματώσει μηχανισμούς auditing και συνεχή επιθεώρηση δικαιωμάτων, εξαλείφοντας τα υπέρμετρα δικαιώματα, τις σκιώδεις ταυτότητες και τις μη ελεγχόμενες υπηρεσιακές προσβάσεις. Η υλοποίηση Zero Trust απαιτεί διαρκή αναθεώρηση των ρόλων και των ομάδων, όπως είχαν ήδη παρατηρήσει και οι μελέτες για τα critical success factors σε συστήματα επιχειρησιακής πληροφόρησης (Yeoh & Koronios, 2010).

Το IAM, η MFA και η risk-based authentication αποτελούν τα λειτουργικά συστατικά που επιτρέπουν στο Zero Trust να μετατραπεί από θεωρητική αρχή σε πρακτική πραγματικότητα. Χωρίς αυτά, οι υπόλοιπες αρχιτεκτονικές πτυχές του Zero Trust δεν μπορούν να λειτουργήσουν. Η ταυτότητα είναι το σημείο εκκίνησης, η MFA είναι ο πρώτος φραγμός και η risk-based authentication είναι ο μηχανισμός που διασφαλίζει την προσαρμογή, την ευελιξία και την ευφυή άμυνα απέναντι στις σύγχρονες απειλές.

5.2 Tokenization και σύγχρονα πρωτόκολλα

Η επιτυχής εφαρμογή Zero Trust απαιτεί ένα σύνολο μηχανισμών που επιτρέπουν την ασφαλή μεταβίβαση ταυτότητας, την προστασία διαδρομών πρόσβασης και την επιβολή granular πολιτικών μεταξύ υπηρεσιών, χρηστών και εφαρμογών. Σε αυτό το πλαίσιο, η tokenization και τα σύγχρονα πρωτόκολλα εξουσιοδότησης και ταυτοποίησης – OAuth2, OpenID Connect (OIDC) και JSON Web Tokens (JWT) – αποτελούν κεντρικά δομικά στοιχεία.

Η tokenization στο Zero Trust αφορά την αντικατάσταση των ευαίσθητων credentials με tokens περιορισμένου χρόνου ζωής, περιορισμένων δικαιωμάτων και granular scopes. Αυτή η προσέγγιση συνδέεται άμεσα με την αρχή του least privilege, καθώς κάθε token φέρει μόνο τα δικαιώματα που απαιτούνται για μία συγκεκριμένη πράξη. Σε αντίθεση με την παραδοσιακή αυθεντικοποίηση, όπου ο χρήστης εισέρχεται με ένα password και αποκτά

ευρεία πρόσβαση, η tokenization επιτρέπει την απορρόφηση κινδύνου και τον περιορισμό της ζημιάς σε περίπτωση παραβίασης συγκεκριμένου token. Οι μελέτες υπογραμμίζουν ότι αυτή η προσέγγιση συνδέεται με τις ανάγκες cloud και multi-tenant αρχιτεκτονικών, όπου ο έλεγχος πρέπει να είναι granular και να μπορεί να μεταβάλλεται δυναμικά (Ferretti et al., 2021).

Το OAuth2 αποτελεί το κυρίαρχο πλαίσιο εξουσιοδότησης στη σύγχρονη ψηφιακή αρχιτεκτονική. Το πρωτόκολλο επιτρέπει σε εφαρμογές τρίτων να αποκτούν εξουσιοδοτημένη πρόσβαση σε πόρους χωρίς να χρειάζεται η αποκάλυψη των credentials του χρήστη. Αυτή η προσέγγιση αντανακλά πλήρως τις αρχές του Zero Trust, καθώς ο έλεγχος πρόσβασης περιορίζεται σε scopes και permissions που σχετίζονται αποκλειστικά με την εκάστοτε λειτουργία. Το OAuth2 διαχωρίζει αυστηρά την ταυτοποίηση από την εξουσιοδότηση και χρησιμοποιεί access tokens με περιορισμένη διάρκεια, απλοποιώντας την επιβολή granular και ephemeral πολιτικών.

Το OpenID Connect (OIDC) αποτελεί επέκταση του OAuth2 και παρέχει μηχανισμό αξιόπιστης ταυτοποίησης μέσω identity tokens. Η σημασία του OIDC στο Zero Trust είναι ιδιαίτερα μεγάλη, καθώς επιτρέπει τη διαστρωμάτωση της ταυτότητας σε cloud περιβάλλοντα και microservices. Το OIDC παρέχει ένα standardised identity layer το οποίο μπορεί να χρησιμοποιηθεί από κάθε συσκευή, εφαρμογή ή API, επιτρέποντας τη διαλειτουργικότητα που θεωρείται κρίσιμη σε Zero Trust συστήματα (Kerman et al., 2020). Το OIDC ενισχύει την αξιοπιστία του IAM, αφού, αντί να βασίζεται σε στατικά credentials, στηρίζεται σε tokens που ενσωματώνουν πληροφορίες για τον χρήστη, την πηγή, την πιθανότητα κινδύνου και το πλαίσιο πρόσβασης.

Τα JSON Web Tokens (JWT) αποτελούν τον κυρίαρχο μηχανισμό αναπαράστασης ταυτότητας και εξουσιοδότησης στο πλαίσιο Zero Trust. Τα JWT είναι δομημένα tokens που μπορούν να υπογραφούν ψηφιακά και περιλαμβάνουν claims σχετικά με τα attributes του χρήστη, τις συσκευές, τον ρόλο, τον εκδότη και τη χρονική διάρκεια ισχύος. Η σημαντικότητα των JWT έγκειται στο γεγονός ότι είναι self-contained, κάτι που επιτρέπει τη λήψη αποφάσεων πρόσβασης χωρίς την ανάγκη για επαναλαμβανόμενες κλήσεις σε κεντρικές υπηρεσίες. Τα JWT, όταν συνδυάζονται με μηχανισμούς continuous verification, επιτρέπουν την αυτόνομη επιβολή πολιτικών σε distributed περιβάλλοντα, όπου τα workloads είναι δυναμικά και κατανεμημένα (Ferretti et al., 2021).

Η σύγχρονη βιβλιογραφία επισημαίνει ότι ο συνδυασμός OAuth2, OIDC και JWT παρέχει την ιδανική βάση για την εφαρμογή πολιτικών Zero Trust σε APIs, cloud services, microservices και serverless αρχιτεκτονικές. Τα συστήματα αυτά δεν μπορούν να στηριχθούν σε παραδοσιακά credentials ή stateful sessions, διότι τα περιβάλλοντα είναι εξαιρετικά δυναμικά, τα instances είναι εφήμερα και η ασφάλεια πρέπει να είναι διανεμημένη, όχι συγκεντρωτική. Η χρήση tokens επιτρέπει την εφαρμογή least privilege σε πραγματικό χρόνο, επιτρέποντας granular scopes, revocation, rotation και συνεχή ανανέωση πολιτικών.

Ο ρόλος της tokenization είναι κρίσιμος επίσης για την αποτροπή lateral movement. Σε παλαιότερες εποχές, η παραβίαση ενός λογαριασμού μπορούσε να επιτρέψει στον επιτιθέμενο πρόσβαση σε ολόκληρο το δίκτυο. Σε ένα token-based περιβάλλον, ακόμη και αν παραβιαστεί ένα token, το εύρος της ζημιάς παραμένει περιορισμένο, αφού τα tokens έχουν μικρή διάρκεια, χαμηλό scope και granular authorizations. Η CISA (2021) υπογραμμίζει ότι η tokenization είναι βασικός παράγοντας για την επίτευξη resilience στη Zero Trust ωρίμανση.

Η βιβλιογραφία αναδεικνύει επίσης τη σημασία των machine-identity protocols σε Zero Trust περιβάλλοντα. Με την ανάπτυξη αυτοματοποιημένων workloads, containers και APIs, η ταυτότητα των μη ανθρώπινων οντοτήτων αποκτά θεμελιώδη σημασία. Το OIDC επιτρέπει τη χρήση dynamic client registration για υπηρεσίες που δημιουργούνται αυτόματα, ενώ το OAuth2 παρέχει μηχανισμούς client-credential flows που επιτρέπουν την granular εξουσιοδότηση σε μη ανθρώπινα συστήματα (Kerman et al., 2020). Πρόκειται για μια διάσταση που επεκτείνει το Zero Trust πέρα από τα κλασικά όρια του IAM, προς ένα περιβάλλον όπου κάθε οντότητα –ανθρώπινη ή μη– πρέπει να επαληθεύεται συνεχώς.

Τέλος, η χρήση των tokens συνδέεται άμεσα με την ανάγκη για forensic visibility, ένα στοιχείο που η βιβλιογραφία υπογραμμίζει ότι είναι κρίσιμο στη διαχείριση περιστατικών. Τα tokens καταγράφονται, συσχετίζονται και παρακολουθούνται, επιτρέποντας έναν πλήρη χάρτη των ενεργειών που έκανε κάθε οντότητα. Αυτή η ικανότητα είναι απολύτως απαραίτητη σε Zero Trust περιβάλλοντα, όπου η διαφάνεια και η παρακολούθηση είναι ισότιμες με την ασφάλεια (CISA, 2021).

Η tokenization και τα πρωτόκολλα OAuth2, OIDC και JWT αποτελούν τον λειτουργικό πυρήνα της σύγχρονης Zero Trust πρακτικής. Επιτρέπουν τη διανομή εμπιστοσύνης σε granular επίπεδο, τη δυναμική επιβολή πολιτικών, την αυτοματοποιημένη διαχείριση ταυτότητας και την ασφαλή αλληλεπίδραση μεταξύ σύνθετων, κατανεμημένων συστημάτων. Η σύζευξή

τους με το IAM και τη risk-based authentication δημιουργεί ένα οικοσύστημα πλήρως συμβατό με τις αρχές Zero Trust: χωρίς εμπιστοσύνη εκ των προτέρων, με συνεχή επαλήθευση, με granular περιορισμό πρόσβασης και με πλήρη διαφάνεια σε κάθε επίπεδο.

5.3 Οι προσεγγίσεις των μεγάλων παρόχων τεχνολογίας

Οι προσεγγίσεις των μεγάλων παρόχων τεχνολογίας για το Zero Trust αποτελούν καθοριστικό σημείο κατανόησης του τρόπου με τον οποίο οι αρχές αυτές μεταφράζονται σε λειτουργικές υλοποιήσεις. Η διεθνής βιβλιογραφία αναδεικνύει ότι οι Google, Microsoft και Cloudflare έχουν διαμορφώσει τρεις από τις σημαντικότερες σχολές εφαρμογής Zero Trust, με διαφορετικές αφετηρίες, προτεραιότητες και αρχιτεκτονικές επιλογές, αλλά με κοινό παρονομαστή τη μετάβαση από το perimeter-based security σε ένα identity-centric, adaptive και πλήρως ενοποιημένο μοντέλο (Buck et al., 2021).

Η Google υπήρξε ο πρωτοπόρος της πρακτικής υλοποίησης Zero Trust μέσα από το BeyondCorp. Το μοντέλο αυτό δεν αποτελεί προϊόν εμπορικής ωρίμανσης, αλλά προϊόν εσωτερικής ανάγκης, το οποίο σχεδιάστηκε για να αντιμετωπίσει υψηλής κλίμακας επιθέσεις που αποκάλυψαν την ανεπάρκεια της παραδοσιακής περιμέτρου (Ward & Beyer, 2014). Όπως τεκμηριώνουν οι Ward και Beyer, η Google επιδίωξε την πλήρη κατάργηση του VPN και την υλοποίηση ενός συστήματος όπου η πρόσβαση καθορίζεται αποκλειστικά από την ταυτότητα και την υγεία της συσκευής. Η προσέγγιση της Google στηρίζεται σε μια πολυεπίπεδη αρχιτεκτονική που περιλαμβάνει συνεχές device inventory, αξιολόγηση κινδύνου ανά συσκευή, granular access policies, policy gateways και μηχανισμούς συλλογής telemetry που διατρέχουν ολόκληρο το οικοσύστημα του οργανισμού. Η Google θεωρεί την ταυτότητα και την κατάσταση της συσκευής ως τα δύο κεντρικά θεμέλια της πρόσβασης και έχει δημιουργήσει ένα οικοσύστημα πλήρους ενοποίησης όπου οι υπηρεσίες, οι εφαρμογές και οι χρήστες υπόκεινται σε διαρκή επανεκτίμηση εμπιστοσύνης με βάση real-time κρίσιμα σημεία δεδομένων (Ward & Beyer, 2014· Cunningham, 2018).

Η προσέγγιση της Microsoft, αν και επηρεασμένη από το BeyondCorp, ακολουθεί διαφορετική φιλοσοφία και αρχιτεκτονική. Η Microsoft οικοδομεί το Zero Trust μοντέλο της γύρω από έξι πυλώνες: identities, endpoints, applications, data, infrastructure και networks (Microsoft, 2021b). Η εταιρεία δίνει έμφαση στην πλήρη αυτοματοποίηση, στη συνεχή συλλογή telemetry και στη χρήση risk-based conditional access ως κεντρικού μηχανισμού λήψης αποφάσεων. Σε αντίθεση με την Google, η Microsoft διαθέτει μια εντελώς

διαφορετική πρόκληση: την παροχή Zero Trust λύσεων σε εκατομμύρια πελάτες, σε διαφορετικά περιβάλλοντα, με διαφορετικές ανάγκες και ανομοιογενή συστήματα. Αυτή η πολυσυλλεκτική δέσμευση απαιτεί από τη Microsoft να υιοθετεί αλγοριθμικά μοντέλα συμπεριφορικής ανάλυσης, machine-learning μηχανισμούς για anomaly detection και εξελιγμένα συστήματα ενσωμάτωσης δεδομένων ώστε να λαμβάνονται αποφάσεις πρόσβασης σε πραγματικό χρόνο με βάση signals που προέρχονται από ολόκληρο το οικοσύστημα Microsoft 365, Azure AD και Defender (Microsoft, 2021a). Η φιλοσοφία της Microsoft είναι έντονα risk-adaptive, ενώ η κλιμάκωση της εφαρμογής της βασίζεται στην αυτοματοποιημένη επιβολή πολιτικών, στην ενοποίηση της ταυτότητας σε πολλαπλά περιβάλλοντα και στη διασφάλιση ότι η πρόσβαση θα είναι πάντα περιορισμένη, προσωρινή και απολύτως συμβατή με το least privilege (Golden et al., 2021).

Η Cloudflare προσφέρει μια τρίτη, διαφορετική προσέγγιση, η οποία προκύπτει από τη φύση της ως global edge-network provider. Η προσέγγιση της Cloudflare στηρίζεται στη διανομή των Zero Trust υπηρεσιών στο edge, δηλαδή κοντά στον χρήστη, στη συσκευή ή στην εφαρμογή, με στόχο τη μείωση της καθυστέρησης, την ενίσχυση της απόδοσης και την αύξηση της ασφάλειας μέσω κατανεμημένων σημείων επιβολής πολιτικών. Αν και η λίστα βιβλιογραφίας δεν περιλαμβάνει άμεσα papers της Cloudflare, η βιβλιογραφία σχετικά με distributed Zero Trust και survivable security υποστηρίζει ότι τέτοιες προσεγγίσεις είναι ιδιαίτερα αποτελεσματικές σε παγκόσμια περιβάλλοντα, ειδικά όταν συνδυάζονται με μηχανισμούς micro-segmentation και granular identity controls (Ferretti et al., 2021). Η Cloudflare αξιοποιεί την τεράστια παγκόσμια υποδομή της για να υλοποιήσει policy enforcement σε εκατομμύρια σημεία, δημιουργώντας ένα «σύννεφο μηδενικής εμπιστοσύνης», όπου ο χρήστης δεν συνδέεται πλέον σε ένα κεντρικό δίκτυο αλλά σε ένα distributed σύστημα συνεχούς επαλήθευσης.

Παρά τις διαφορές τους, οι προσεγγίσεις των Google, Microsoft και Cloudflare συγκλίνουν σε κρίσιμες αρχές που η βιβλιογραφία χαρακτηρίζει απαραίτητες για τη λειτουργική ωρίμανση του Zero Trust. Πρώτον, όλες οι υλοποιήσεις βασίζονται στη συνεχή συλλογή και συσχέτιση δεδομένων telemetry, καθώς η διαρκής ανάλυση συμπεριφοράς χρηστών και συσκευών αποτελεί τον κεντρικό μηχανισμό εκτίμησης κινδύνου (Microsoft, 2021b· CISA, 2021). Δεύτερον, όλες οι πλατφόρμες εφαρμόζουν granular πολιτικές least privilege, με δυναμική προσαρμογή και συνεχή επαλήθευση πρόσβασης. Τρίτον, η ταυτότητα αποτελεί το κεντρικό κλειδί λήψης αποφάσεων, είτε αυτή αφορά ανθρώπινους χρήστες είτε μηχανικές

υπηρεσίες, σύμφωνα με τη θεμελιώδη αρχή identity-centric security που υπογραμμίζεται στο σύνολο της βιβλιογραφίας (Buck et al., 2021· Adahman et al., 2022). Τέταρτον, όλες οι πλατφόρμες ενσωματώνουν σύγχρονα πρωτόκολλα εξουσιοδότησης, tokenization και fully audited access flows ώστε να διασφαλίζεται ότι οι policy decisions μπορούν να εφαρμοστούν σε distributed και πολυεπίπεδα περιβάλλοντα.

Τελικά, οι μεγάλοι vendors συνεισφέρουν στην εξέλιξη του Zero Trust όχι μόνο μέσω των τεχνολογιών, αλλά και μέσω της διαμόρφωσης μιας νέας οργανωσιακής κουλτούρας. Η βιβλιογραφία αναδεικνύει ότι η υιοθέτηση Zero Trust από κολοσσούς όπως Google και Microsoft δημιουργεί πρότυπα, πρακτικές και standards που διαχέονται σε ολόκληρη τη βιομηχανία και επηρεάζουν θεσμικά έγγραφα όπως το NIST SP 800-207 και την ωριμότητα που προωθεί η CISA (CISA, 2021· Kerman et al., 2020). Με αυτόν τον τρόπο, οι προσεγγίσεις των μεγάλων παρόχων λειτουργούν ως πολλαπλασιαστές γνώσης και ως πρακτικά παραδείγματα για την παγκόσμια κοινότητα ασφάλειας.

5.4 Οργανωτικές και τεχνολογικές προκλήσεις υιοθέτησης

Η υιοθέτηση Zero Trust δεν αποτελεί απλώς τεχνολογική μετάβαση αλλά βαθύς οργανωσιακός μετασχηματισμός. Η διεθνής βιβλιογραφία αναδεικνύει ένα σύνολο πολυσύνθετων εμποδίων που επηρεάζουν τη μετάβαση αυτή: τεχνικά, λειτουργικά, πολιτισμικά και στρατηγικά. Η κατανόηση αυτών των προκλήσεων είναι απαραίτητη για να προσδιοριστεί ο βαθμός δυνατότητας εφαρμογής και ωρίμανσης ενός οργανισμού.

Μία από τις σημαντικότερες οργανωσιακές προκλήσεις είναι η αναδιάρθρωση των ρόλων πρόσβασης, η οποία αποτελεί προϋπόθεση για την εφαρμογή least privilege. Οι οργανισμοί έχουν συνήθως μακρόχρονα συσσωρευμένες δομές δικαιωμάτων, με ιστορικά privileges, ανεπίσημες προσβάσεις, υπερεξουσιοδοτήσεις και shadow IT. Οι Buck et al. (2021) καταγράφουν ότι η αδυναμία καθορισμού σαφών ρόλων αποτελεί το κυριότερο εμπόδιο στην εφαρμογή granular πολιτικών. Η μετάβαση σε μοντέλα ABAC απαιτεί καθαρή οντολογία πρόσβασης, κάτι που στη πράξη συνεπάγεται επανασχεδιασμό διαδικασιών, εκπαίδευση προσωπικού, διοικητική δέσμευση και συστηματική απομάκρυνση legacy πρακτικών.

Πέρα από τα οργανωσιακά ζητήματα, η υλοποίηση Zero Trust απαιτεί υψηλό επίπεδο τεχνικής ωριμότητας. Η ανάπτυξη υποδομών telemetry, για παράδειγμα, απαιτεί την ενοποίηση πληροφοριών από πολλαπλές πηγές: συσκευές, δίκτυα, cloud υπηρεσίες, εφαρμογές και workloads. Η CISA (2021) επισημαίνει ότι η συλλογή και συσχέτιση τέτοιων

δεδομένων αποτελεί προϋπόθεση για την εφαρμογή continuous verification. Ωστόσο, πολλοί οργανισμοί αδυνατούν να υποστηρίξουν τέτοια pipelines, κυρίως λόγω κατακερματισμένων πληροφοριακών συστημάτων, ελλείψεων σε πρακτικές monitoring και αδυναμίας ομογενοποίησης των δεδομένων. Το ίδιο πρόβλημα εντοπίζουν και οι τεχνικές αναλύσεις του Kerman et al. (2020), όπου η απουσία διαλειτουργικότητας μεταξύ IAM, SIEM και enforcement points δημιουργεί σημεία ασυνέχειας που αποδυναμώνουν την αξιοπιστία των policy decisions.

Μια ακόμη κρίσιμη πρόκληση αφορά το κόστος και την πολυπλοκότητα της μετάβασης. Παρότι οι Adahman et al. (2022) απέδειξαν ότι η υιοθέτηση Zero Trust είναι οικονομικά αποδοτική μακροπρόθεσμα, η αρχική επένδυση συχνά είναι σημαντική: απαιτείται αναβάθμιση συσκευών, εκσυγχρονισμός IAM, υλοποίηση MFA σε όλο το εύρος χρηστών, αναδιάρθρωση εφαρμογών ώστε να υποστηρίζουν tokenization και OIDC, καθώς και εκπαίδευση προσωπικού. Σε περιβάλλοντα με legacy συστήματα, ο τεχνικός μετασχηματισμός μπορεί να είναι ακόμα πιο δύσκολος. Οι Golden et al. (2021) επισημαίνουν ότι η μετάβαση απαιτεί μοντέρνες DevSecOps πρακτικές, συστήματα αυτοματοποίησης και δομές governance που συχνά δεν υπάρχουν.

Άλλη σημαντική τεχνολογική δυσκολία αφορά την υποστήριξη των policy enforcement points σε διανεμημένα περιβάλλοντα. Το NIST SP 800-207 αναγνωρίζει ότι η ύπαρξη πολλών enforcement points δημιουργεί την ανάγκη για κεντρική αλλά ταυτόχρονα και αποκεντρωμένη διακυβέρνηση, με στόχο να αποφευχθούν μοναδικά σημεία αποτυχίας (Kerman et al., 2020). Η εφαρμογή αυτής της αρχιτεκτονικής σε μεγάλα οργανωσιακά περιβάλλοντα με ανομοιογενή συστήματα και εφαρμογές δημιουργεί σημαντικά ζητήματα διαλειτουργικότητας, latency και troubleshooting.

Ένα άλλο επίπεδο δυσκολίας αφορά τη διαχείριση της αλλαγής. Η βιβλιογραφία υπογραμμίζει ότι η υιοθέτηση Zero Trust προκαλεί συχνά αντίσταση από τους ίδιους τους χρήστες και τα τμήματα των οργανισμών, διότι αυξάνει τους ελέγχους, μειώνει την πρόσβαση, επιβάλλει νέες διαδικασίες MFA και μπορεί να δημιουργήσει την αίσθηση επιτήρησης. Οι Deloitte (2021) και Golden et al. (2021) επισημαίνουν ότι η οργανωσιακή κουλτούρα αποτελεί εξίσου σημαντικό παράγοντα με τα τεχνικά συστήματα. Η επιτυχία εξαρτάται από τη δυνατότητα του οργανισμού να επικοινωνήσει τα οφέλη, να μειώσει τις αντιστάσεις και να εξασφαλίσει πως οι διαδικασίες Zero Trust δεν θα αντιμετωπίζονται ως «εμπόδιο» στη ροή εργασίας.

Η διεθνής βιβλιογραφία καταδεικνύει επίσης ότι ορισμένα περιβάλλοντα αποτελούν εγγενώς δυσκολότερους χώρους εφαρμογής Zero Trust. Για παράδειγμα, περιβάλλοντα με υψηλές ανάγκες λειτουργίας σε πραγματικό χρόνο, όπως βιομηχανικά συστήματα ή περιβάλλοντα υγείας, παρουσιάζουν τεράστιες προκλήσεις στην υλοποίηση granular πολιτικών, latency-sensitive controls και διαστρωματωμένων μηχανισμών αυθεντικοποίησης. Αν και αυτά τα στοιχεία δεν αναλύονται διεξοδικά στη λίστα που παρείχες, η σύνδεσή τους με τις θεωρητικές προκλήσεις του Zero Trust που αναφέρονται στα μοντέλα της CISA και του NIST (CISA, 2021· Kerman et al., 2020) είναι άμεση.

Τέλος, η υιοθέτηση Zero Trust συχνά απαιτεί μια σταδιακή, πολυετή μετάβαση. Η βιβλιογραφία υπογραμμίζει ότι η ωριμότητα του Zero Trust είναι πολυδιάστατη και εξελίσσεται με ρυθμούς που εξαρτώνται από τις οργανωσιακές δυνατότητες. Η CISA (2021) χρησιμοποιεί τον όρο «μοντέλο ωριμότητας» εντός ενός πλαισίου που αναγνωρίζει τη σταδιακή εξέλιξη από basic σε intermediate και advanced επίπεδα εφαρμογής. Οι Buck et al. (2021) επισημαίνουν ότι ορισμένες οργανώσεις τείνουν να υπερεκτιμούν την ωριμότητά τους, υιοθετώντας αποσπασματικά στοιχεία Zero Trust χωρίς να εφαρμόζουν την πλήρη αρχιτεκτονική. Αυτό οδηγεί σε ένα φαινόμενο που περιγράφεται συχνά ως “Zero Trust in name only”, όπου η ασφάλεια δεν βελτιώνεται πραγματικά παρά την υιοθέτηση της ορολογίας.

Οι οργανωτικές και τεχνολογικές προκλήσεις της υιοθέτησης Zero Trust αντικατοπτρίζουν το βάθος και την πολυπλοκότητα της αρχιτεκτονικής αυτής. Η μετάβαση δεν είναι απλή τεχνική αναβάθμιση, αλλά μια βαθιά αλλαγή μοντέλου λειτουργίας, όπου η ταυτότητα είναι ο νέος άξονας πρόσβασης, η εμπιστοσύνη πρέπει να κερδίζεται διαρκώς και η ασφάλεια μετατρέπεται από παθητική άμυνα σε δυναμική και διαρκή διαδικασία. Η βιβλιογραφία συμφωνεί ότι, παρά τις δυσκολίες, το Zero Trust αποτελεί όχι μόνο την πιο συνεπή θεωρητικά προσέγγιση ασφάλειας, αλλά και την πλέον αναγκαία σε έναν κόσμο όπου οι απειλές εξελίσσονται ταχύτερα από τα παραδοσιακά μοντέλα προστασίας.

5.5 Πλεονεκτήματα και επιπτώσεις στην ασφάλεια και στη συμμόρφωση

Η υιοθέτηση της αρχιτεκτονικής Zero Trust επιφέρει ένα σύνολο σημαντικών πλεονεκτημάτων στην οργανωσιακή ασφάλεια, καθώς και βαθιές αλλαγές στη συμμόρφωση, στη διακυβέρνηση των δεδομένων και στη στρατηγική διαχείριση τεχνολογικών κινδύνων. Η διεθνής βιβλιογραφία επιβεβαιώνει ότι το Zero Trust δεν αποτελεί

απλώς μια τεχνική αναβάθμιση αλλά έναν θεμελιώδη επαναπροσδιορισμό της κυβερνοασφάλειας, όπου η εμπιστοσύνη δεν θεωρείται δεδομένη και όλες οι οντότητες – ανθρώπινες και μη– υποβάλλονται σε συνεχή επαλήθευση (CISA, 2021· Kerman et al., 2020). Η μετατόπιση αυτή οδηγεί σε πολυεπίπεδη ενίσχυση της ασφάλειας, με επιπτώσεις που εκτείνονται από τον περιορισμό του ρίσκου έως τη βελτίωση της κανονιστικής συμμόρφωσης.

Ένα από τα κυριότερα πλεονεκτήματα αφορά τη μείωση της επιφάνειας επίθεσης. Το Zero Trust αναδιαμορφώνει τη λογική της πρόσβασης, καταργώντας την προνομιακή αντιμετώπιση του "εσωτερικού χρήστη" και επιβάλλοντας granular, contextual και προσωρινά δικαιώματα. Ο Campbell (2020) επισημαίνει ότι η παραδοσιακή εμπιστοσύνη προς χρήστες εντός του εταιρικού δικτύου αποτελεί πλέον «ευπάθεια» και όχι πλεονέκτημα, διότι η πλειονότητα των σύγχρονων επιθέσεων βασίζεται στην κατάχρηση νόμιμων credentials. Το Zero Trust εξουδετερώνει αυτό το ρίσκο μετατρέποντας την εσωτερική πρόσβαση σε αντικείμενο διαρκούς ελέγχου, περιορίζοντας την προοπτική lateral movement και μειώνοντας θεαματικά τον αντίκτυπο πιθανής παραβίασης (Buck et al., 2021).

Ένα άλλο σημαντικό πλεονέκτημα είναι η ενίσχυση της ανθεκτικότητας του οργανισμού απέναντι σε περιστατικά παραβίασης. Τα tokens μικρής διάρκειας, οι πολιτικές least privilege, η micro-segmentation και η συνεχής επαλήθευση δημιουργούν μια αρχιτεκτονική όπου η παραβίαση ενός λογαριασμού ή μιας συσκευής δεν έχει τη δυνατότητα να εξαπλωθεί εύκολα. Οι Ferretti et al. (2021) αποτυπώνουν ότι η υιοθέτηση granular isolation μηχανισμών σε distributed περιβάλλοντα μειώνει δραστικά τη δυνατότητα του επιτιθέμενου να μετακινηθεί εντός των συστημάτων. Η υψηλή ανθεκτικότητα, επομένως, δεν επιτυγχάνεται μόνο με προληπτικά μέτρα αλλά με δομική περιοριστικότητα, η οποία ελαχιστοποιεί τις συνέπειες οποιουδήποτε ανεπιθύμητου συμβάντος.

Η αρχιτεκτονική Zero Trust βελτιώνει επίσης σημαντικά τη διαφάνεια και την παρατηρησιμότητα του συστήματος. Η συνεχής συλλογή και συσχέτιση δεδομένων telemetry –από συσκευές, εφαρμογές, δίκτυα και workloads– δημιουργεί ένα λεπτομερές ίχνος που επιτρέπει την ενίσχυση των μηχανισμών auditing και forensic analysis (CISA, 2021). Αυτό το πλεονέκτημα είναι κρίσιμο όχι μόνο για την ασφάλεια αλλά και για τη συμμόρφωση. Πολλά διεθνή πρότυπα απαιτούν πλήρη ορατότητα των ενεργειών πρόσβασης, των μεταβολών δικαιωμάτων και των κινήσεων χρηστών. Η αρχιτεκτονική Zero Trust ανταποκρίνεται σε αυτές τις απαιτήσεις καλύπτοντας τη συνολική αλυσίδα πρόσβασης, από

το authentication έως το session monitoring, με τρόπο που τα παραδοσιακά μοντέλα δεν ήταν σε θέση να επιτύχουν.

Από την οπτική γωνία της κανονιστικής συμμόρφωσης, το Zero Trust ευθυγραμμίζεται πλήρως με τις σύγχρονες απαιτήσεις για προστασία δεδομένων, περιορισμό πρόσβασης και διασφάλιση της ακεραιότητας. Πλαίσια όπως το NIST SP 800-207 και το Zero Trust Maturity Model της CISA έχουν συμβάλει στη θεσμοποίηση των αρχών αυτών, προσφέροντας οδηγίες που είναι συχνά συμβατές με ευρωπαϊκές και διεθνείς νομοθεσίες σχετικές με την προστασία δεδομένων και την ασφάλεια κρίσιμων συστημάτων. Η προσέγγιση που βασίζεται στην ελάχιστη αναγκαία πρόσβαση και στη συνεχή επαλήθευση υποστηρίζει την απαίτηση πολλών νομοθετικών πλαισίων για περιορισμό της πρόσβασης βάσει αναγκαιότητας και προστασία ευαίσθητων δεδομένων. Η υιοθέτηση αυτή ανταποκρίνεται και σε πιο πρακτικές ανάγκες θεσμικών κανονισμών, όπως πλήρη καταγραφή ενεργειών, αδιάλειπτο έλεγχο ταυτότητας και δυνατότητα απόδοσης ευθύνης.

Επιπλέον, η ενίσχυση της συμμόρφωσης σχετίζεται με τον τρόπο που το Zero Trust υποστηρίζει τη διακυβέρνηση των ταυτοτήτων. Η ενοποίηση των IAM υποδομών, η εφαρμογή MFA και η χρήση δυναμικών πολιτικών conditional access επιτρέπουν την ακριβή διαχείριση του ποιος έχει πρόσβαση σε τι και υπό ποιες συνθήκες (Microsoft, 2021b). Αυτή η ακρίβεια υποστηρίζει την ανάγκη τήρησης ελέγχων πρόσβασης και ασφαλών διαδικασιών ανάθεσης δικαιωμάτων, στοιχείο που αναδεικνύεται ως κρίσιμο στις μελέτες σχετικά με την επιτυχή υλοποίηση Zero Trust (Adahman et al., 2022). Η δυνατότητα καθορισμού granular πολιτικών συμβάλλει στην ικανοποίηση απαιτήσεων όπως segregation of duties και auditability.

Από την πλευρά της οργανωσιακής αποτελεσματικότητας, το Zero Trust επιφέρει επίσης σημαντικά πλεονεκτήματα. Με την κατάργηση του VPN και την υιοθέτηση identity-centric access, οι χρήστες αποκτούν πρόσβαση με πιο ευέλικτο, γρήγορο και ασφαλή τρόπο. Το BeyondCorp απέδειξε ότι η απομάκρυνση των παραδοσιακών VPN μειώνει την πολυπλοκότητα και βελτιώνει την εμπειρία του χρήστη, ενώ ταυτόχρονα αυξάνει την ασφάλεια, διότι δεν βασίζεται σε single entry points που μπορούν να αποτελέσουν στόχο (Ward & Beyer, 2014). Η σύγχρονη βιβλιογραφία επισημαίνει ότι η αντιμετώπιση της ασφάλειας ως identity problem αντί για πρόβλημα δικτύου ενισχύει την ευελιξία, μειώνει τα λειτουργικά εμπόδια και επιταχύνει την επιχειρησιακή δραστηριότητα (Golden et al., 2021).

Η εφαρμογή Zero Trust επηρεάζει θετικά και τις εσωτερικές διαδικασίες διαχείρισης περιστατικών. Η συνεχής επιτήρηση και η granular καταγραφή ενισχύουν την ταχύτητα ανίχνευσης και αντίδρασης σε επιθέσεις. Η Microsoft (2021a) καταδεικνύει ότι οι οργανισμοί που εφαρμόζουν Zero Trust μειώνουν σημαντικά τον χρόνο εντοπισμού παραβίασης, καθώς η ανίχνευση βασίζεται σε αναλυτικά μοντέλα συμπεριφοράς που εντοπίζουν ανωμαλίες σε πραγματικό χρόνο. Η χρήση risk-based authentication ενισχύει επίσης την ικανότητα άμεσης απόρριψης ύποπτων αιτημάτων πρόσβασης, προσφέροντας μια γραμμή άμυνας που προσαρμόζεται αυτόματα στη φύση της απειλής.

Ωστόσο, τα πλεονεκτήματα δεν περιορίζονται στην ασφάλεια αλλά επεκτείνονται και στο στρατηγικό επίπεδο. Το Zero Trust προωθεί μια οργανωσιακή κουλτούρα ακεραιότητας, διαφάνειας και ευθύνης. Η επιβολή least privilege απαιτεί καθορισμό ρόλων, η χρήση MFA και conditional access απαιτεί ενιαίες πολιτικές και η διαρκής επαλήθευση προϋποθέτει συνεργασία μεταξύ τμημάτων. Αυτές οι αλλαγές οδηγούν σε πιο ώριμες οργανωσιακές δομές και σε ένα περιβάλλον όπου η ασφάλεια δεν είναι αποσπασματική αλλά ενσωματωμένη στους επιχειρησιακούς στόχους.

Τέλος, τα πλεονεκτήματα που προσφέρει το Zero Trust έχουν ευρύτερες επιπτώσεις στο οικοσύστημα της κυβερνοασφάλειας. Οι πρακτικές που υιοθετούνται από φορείς όπως Google και Microsoft διαμορφώνουν βιομηχανικά πρότυπα και επηρεάζουν θεσμικές οδηγίες όπως τα NIST SP 800-207 και CISA Zero Trust Maturity Model (CISA, 2021· Kerman et al., 2020). Η εξέλιξη αυτή δημιουργεί ένα νέο πλαίσιο αναφοράς όπου οι οργανισμοί καλούνται να λειτουργούν με όρους συνεχούς επαλήθευσης και δυναμικής πολιτικής, θέτοντας νέα πρότυπα για την ασφάλεια, τη συμμόρφωση και την τεχνική διακυβέρνηση.

Τα πλεονεκτήματα του Zero Trust είναι πολυδιάστατα, αγγίζοντας την ασφάλεια, τη συμμόρφωση, τη λειτουργία, τη διακυβέρνηση και την οργανωσιακή κουλτούρα. Η βιβλιογραφία συμφωνεί ότι η υιοθέτηση του Zero Trust αντιπροσωπεύει μια από τις σημαντικότερες εξελίξεις της σύγχρονης κυβερνοασφάλειας, καθώς μετασχηματίζει τον τρόπο με τον οποίο οι οργανισμοί προστατεύουν τα περιουσιακά τους στοιχεία και ευθυγραμμίζονται με τις διεθνείς απαιτήσεις και τα τεχνολογικά πρότυπα.

Κεφάλαιο 6. Συμπεράσματα

6.1 Σύνθεση της βιβλιογραφίας

Η ανασκόπηση της διεθνούς βιβλιογραφίας για το Zero Trust αναδεικνύει ότι το μοντέλο αυτό δεν αποτελεί απλώς μία νέα τεχνική προσέγγιση στην κυβερνοασφάλεια, αλλά μια βαθιά αλλαγή παραδείγματος που μετατοπίζει το κέντρο βάρους από το δίκτυο στην ταυτότητα, από τη στατική περιμετρική άμυνα στη δυναμική, συνεχώς προσαρμοζόμενη αξιολόγηση κινδύνου, και από την εμπιστοσύνη προς τους εσωτερικούς χρήστες στη μηδενική προϋπόθεση εμπιστοσύνης για κάθε οντότητα. Οι μελέτες συγκλίνουν στο ότι το Zero Trust εμφανίστηκε ως απάντηση στην αυξανόμενη αδυναμία των παραδοσιακών μοντέλων ασφάλειας, τα οποία βασίζονταν σε συστήματα perimeters και VPN, τα οποία πλέον δεν επαρκούν σε ένα περιβάλλον cloud-first, mobile-first και εφαρμογών που λειτουργούν κατανεμημένα (Campbell, 2020· Buck et al., 2021).

Η βιβλιογραφία δείχνει ότι η εξέλιξη των απειλών, η εξάπλωση των επιθέσεων credential theft, η κατάρρευση του δικτυακού ορίου και η εξάπλωση των cloud workloads διαμόρφωσαν το υπόβαθρο μέσα στο οποίο το Zero Trust αναδύθηκε ως αναγκαστική απάντηση και όχι ως θεωρητική επιλογή. Μελέτες όπως αυτές των Adahman et al. (2022) και των Buck et al. (2021) επιβεβαιώνουν ότι η εμπιστοσύνη προς τον εσωτερικό χρήστη αποτελεί πλέον ένα από τα πιο επικίνδυνα σφάλματα ασφαλείας, καθώς τα περισσότερα περιστατικά παραβίασης ξεκινούν από κλεμμένα credentials ή compromised endpoints.

Η συμβολή του BeyondCorp της Google στην εξέλιξη του Zero Trust αποτυπώνεται στην εκτενή θεωρητική τεκμηρίωση που πρόσφεραν οι Ward και Beyer (2014), οι οποίοι εξήγησαν πώς μια μεγάλη επιχείρηση μπορεί να καταργήσει το VPN και να βασίσει την πρόσβασή της αποκλειστικά στο ποιος είναι ο χρήστης και ποια είναι η κατάσταση της συσκευής του. Η επαναστατική αυτή προσέγγιση μετέβαλε τον διεθνή διάλογο και αποτέλεσε προπομπό για τα μοντέλα που ανέπτυξαν έπειτα θεσμικοί οργανισμοί, όπως το NIST SP 800-207. Η τεκμηρίωση του NIST (Kerman et al., 2020) καθιέρωσε ένα ενιαίο θεωρητικό πλαίσιο που συγκεντρώνει όλες τις βασικές αρχές του Zero Trust, διαμορφώνοντας ένα λειτουργικό μοντέλο που μπορεί να εφαρμοστεί από δημόσιους και ιδιωτικούς οργανισμούς με διαλειτουργικότητα και συνέπεια.

Τα Zero Trust maturity models της CISA (2021) προσέφεραν επιπλέον μια σημαντική διάσταση, καθώς περιέγραψαν την εξέλιξη των οργανισμών σε επίπεδα ωριμότητας. Αυτό επιτρέπει στους φορείς να αξιολογούν την πρόοδό τους και να κατανοούν ότι η υιοθέτηση Zero Trust δεν είναι ένα στιγμιαίο έργο, αλλά μια διαρκής διαδικασία που απαιτεί σταδιακή μετεξέλιξη, επένδυση και οργανωσιακή αναδιάρθρωση.

Η βιβλιογραφία συνθέτει επίσης μια σαφή εικόνα για τα τεχνικά στοιχεία που αποτελούν τον πυρήνα της εφαρμογής Zero Trust. Τα IAM συστήματα ενισχύονται ώστε να υποστηρίζουν granular ταυτότητες, τόσο ανθρώπινες όσο και μηχανικές (Bobbert & Scheerder, 2020). Η MFA και η risk-based authentication αποτελούν τις κύριες μορφές ενίσχυσης του ελέγχου ταυτότητας, με σημαντικές εφαρμογές σε καθολικά περιβάλλοντα και με αποδεδειγμένη αποτελεσματικότητα (Microsoft, 2021a· Golden et al., 2021). Η tokenization και τα σύγχρονα πρωτόκολλα OAuth2, OIDC και JWT καθιερώνονται ως τα πρότυπα μηχανισμών πρόσβασης σε cloud και API-driven συστήματα (Ferretti et al., 2021). Η micro-segmentation και το least privilege λειτουργούν ως θεμελιώδεις πρακτικές περιορισμού του lateral movement, μειώνοντας δραστικά την επικινδυνότητα μιας παραβίασης (Buck et al., 2021).

Η βιβλιογραφία αποτυπώνει επίσης τις ποικίλες προσεγγίσεις των μεγάλων vendors και τη συμβολή τους στη διαμόρφωση παγκόσμιων πρακτικών. Η Google διαμόρφωσε ένα μοντέλο βασισμένο στη συσκευή, στην ταυτότητα και στην πλήρη κατάργηση των παραδοσιακών δικτυακών περιμέτρων (Ward & Beyer, 2014). Η Microsoft υλοποίησε ένα πολυδιάστατο πλαίσιο με κεντρικό ρόλο στο risk-based conditional access, στην ενοποίηση ταυτότητας και στη συνεχή αξιολόγηση telemetry (Microsoft, 2021b· Microsoft, 2021a). Η Cloudflare υιοθέτησε ένα distributed Zero Trust edge μοντέλο, επηρεάζοντας το πώς εφαρμόζεται το Zero Trust σε παγκόσμια περιβάλλοντα μεγάλης κλίμακας (Ferretti et al., 2021).

Η ανασκόπηση καταδεικνύει ότι το Zero Trust έχει άμεσες επιπτώσεις επίσης στη συμμόρφωση, στη διακυβέρνηση δεδομένων και στην επιχειρησιακή κουλτούρα. Οι αρχές της συνεχούς επαλήθευσης, της διαφάνειας, της λογοδοσίας και των granular πολιτικών πρόσβασης ευθυγραμμίζονται με τις σύγχρονες απαιτήσεις διεθνών και θεσμικών πλαισίων για προστασία δεδομένων, auditing και risk management (CISA, 2021· Kerman et al., 2020). Αυτό καθιστά το Zero Trust όχι μόνο μηχανισμό ασφάλειας αλλά και εργαλείο θεσμικής συμμόρφωσης.

Τέλος, η βιβλιογραφία αναδεικνύει ότι παρά τα πολλαπλά πλεονεκτήματα, η εφαρμογή Zero Trust συναντά σημαντικές τεχνολογικές και οργανωσιακές προκλήσεις. Οι Golden et al.

(2021) και οι Deloitte (2021) επισημαίνουν ότι η μετάβαση απαιτεί αναδιάρθρωση διαδικασιών, αλλαγή κουλτούρας, αναθεώρηση ρόλων πρόσβασης, ισχυρή διοικητική υποστήριξη και σημαντικές επενδύσεις σε υποδομές, telemetry pipelines και automation. Η υιοθέτηση Zero Trust είναι μια συνεχής προσπάθεια ωρίμανσης και προσαρμογής, όχι μια τεχνική υλοποίηση που ολοκληρώνεται σε μία φάση.

Η σύνθεση της βιβλιογραφίας αποκαλύπτει ότι το Zero Trust αποτελεί μια ολιστική, πολυδιάστατη και εξελισσόμενη αρχιτεκτονική, η οποία αναμορφώνει θεμελιωδώς τον τρόπο με τον οποίο αντιλαμβανόμαστε την κυβερνοασφάλεια, την πρόσβαση, την εμπιστοσύνη και τη συμμόρφωση στο σύγχρονο ψηφιακό περιβάλλον.

6.2 Απαντήσεις στα ερευνητικά ερωτήματα

Η ανασκόπηση της βιβλιογραφίας επιτρέπει τη διατύπωση τεκμηριωμένων απαντήσεων στα ερευνητικά ερωτήματα της μελέτης, προσφέροντας μια συνεκτική και θεωρητικά εδραιωμένη κατανόηση των λόγων για τους οποίους το Zero Trust αποτελεί σήμερα το κυρίαρχο μοντέλο ασφάλειας.

Το πρώτο ερευνητικό ερώτημα αφορά τον τρόπο με τον οποίο το Zero Trust αντιμετωπίζει τις αδυναμίες των παραδοσιακών perimeter-based μοντέλων. Η βιβλιογραφία δείχνει ξεκάθαρα ότι τα μοντέλα που βασίζονται στη γεωγραφική τοποθεσία και στην ενδο-δικτυακή εμπιστοσύνη έχουν πλέον καταστεί ανεπαρκή. Τα VPN, οι στατικοί έλεγχοι περιμετρικής πρόσβασης και τα firewalls δεν μπορούν να προστατεύσουν έναν κόσμο όπου οι χρήστες λειτουργούν από πολλαπλές τοποθεσίες, οι εφαρμογές φιλοξενούνται στο cloud και οι συσκευές δεν ελέγχονται κεντρικά (Campbell, 2020). Το Zero Trust απαντά σε αυτές τις αδυναμίες καταργώντας την έννοια του «εσωτερικού χρήστη» και επιβάλλοντας συνεχή επαλήθευση για κάθε αίτημα πρόσβασης, ανεξαρτήτως δικτύου ή συσκευής (Buck et al., 2021). Επομένως, οι βασικές αδυναμίες των perimeter-based μοντέλων θεραπεύονται μέσω των αρχών της μηδενικής εμπιστοσύνης, της ταυτοκεντρικής ασφάλειας και της συνεχούς επαλήθευσης.

Το δεύτερο ερευνητικό ερώτημα αφορά το θεωρητικό και πρακτικό υπόβαθρο που καθιστά το Zero Trust αναπόφευκτο για τις σύγχρονες επιχειρήσεις. Η θεωρητική θεμελίωση του Zero Trust προκύπτει από τα μοντέλα του BeyondCorp και του NIST SP 800-207, τα οποία απέδειξαν ότι η ασφάλεια μπορεί να επιτευχθεί χωρίς περιμετρικές υποθέσεις, μέσω ενός συστήματος όπου η ταυτότητα, η συσκευή και το context αποτελούν τις μοναδικές

αξιόπιστες μεταβλητές (Ward & Beyer, 2014· Kerman et al., 2020). Πρακτικά, η εξάπλωση cloud, mobilization και SaaS επιβάλλει την υιοθέτηση Zero Trust, αφού οι οργανισμοί δεν μπορούν πλέον να προστατευθούν με παραδοσιακά δίκτυα. Η ανάγκη για granular πρόσβαση, για επαλήθευση μηχανικών ταυτοτήτων και για κατανεμημένα control points καθιστά το Zero Trust μονόδρομο (Microsoft, 2021b).

Το τρίτο ερώτημα αφορά τον ρόλο των τεχνολογιών IAM, MFA, risk-based authentication, tokenization και enforcement στην υλοποίηση Zero Trust. Η βιβλιογραφία είναι απολύτως σαφής: οι τεχνολογίες αυτές αποτελούν τον λειτουργικό πυρήνα του Zero Trust, χωρίς τις οποίες η αρχιτεκτονική δεν μπορεί να υλοποιηθεί. Το IAM επιτρέπει τον καθορισμό granular ρόλων και ταυτοτήτων (Bobbert & Scheerder, 2020). Η MFA μειώνει δραστικά την πιθανότητα παραβίασης credentials (Microsoft, 2021a). Η risk-based authentication παρέχει δυναμικές αποφάσεις βασισμένες στον κίνδυνο (Golden et al., 2021). Η tokenization και τα πρωτόκολλα OAuth2, OIDC και JWT επιτρέπουν την κατανεμημένη επιβολή πολιτικών και την ασφαλή διακίνηση ταυτότητας (Ferretti et al., 2021). Συνεπώς, το Zero Trust δεν μπορεί να εφαρμοστεί χωρίς αυτά τα τεχνολογικά θεμέλια.

Το τέταρτο ερώτημα αφορά τις προκλήσεις που εμποδίζουν ή επιβραδύνουν την υιοθέτηση Zero Trust. Η βιβλιογραφία επισημαίνει μια σειρά από περιορισμούς: οργανωσιακές αντιστάσεις, έλλειψη ωριμότητας IAM, περιορισμούς legacy συστημάτων, κόστος και πολυπλοκότητα της μετάβασης, έλλειψη διαλειτουργικότητας και αδυναμία υλοποίησης telemetry pipelines (Deloitte, 2021· Golden et al., 2021· CISA, 2021). Πέρα από αυτά, η επιτυχής υλοποίηση απαιτεί αναδιάρθρωση ρόλων και πολιτικών least privilege, κάτι που συχνά συγκρούεται με παγιωμένες πρακτικές και χαμηλά επίπεδα εταιρικής πειθαρχίας.

Το πέμπτο και τελευταίο ερώτημα αφορά τα πλεονεκτήματα του Zero Trust για την ασφάλεια και τη συμμόρφωση. Η ανασκόπηση δείχνει ότι το Zero Trust μειώνει δραματικά τον κίνδυνο lateral movement, βελτιώνει τον χρόνο ανίχνευσης επιθέσεων μέσω telemetry και ενισχύει την προστασία από credential theft (Ferretti et al., 2021· Microsoft, 2021a). Σε επίπεδο συμμόρφωσης, οι αρχές του Zero Trust ευθυγραμμίζονται πλήρως με τις απαιτήσεις των σύγχρονων κανονιστικών πλαισίων για περιορισμένη πρόσβαση, διαφάνεια, auditing και συνεχή επαλήθευση (CISA, 2021· Kerman et al., 2020).

Η βιβλιογραφική ανάλυση αποδεικνύει ότι το Zero Trust δεν είναι απλώς μια τεχνική καινοτομία αλλά μια θεμελιώδης μεταμόρφωση της κυβερνοασφάλειας, η οποία επηρεάζει την τεχνολογία, την οργανωσιακή λειτουργία, τη συμμόρφωση και την στρατηγική

προστασία της πληροφορίας. Πρόκειται για ένα εξελισσόμενο μοντέλο, του οποίου η πλήρης υλοποίηση απαιτεί τεχνολογική ωριμότητα, ηγετική δέσμευση και οργανωσιακή μετάβαση προς ένα περιβάλλον διαρκούς αξιολόγησης εμπιστοσύνης.

6.3 Περιορισμοί των υπαρχουσών μελετών

Η διερεύνηση της βιβλιογραφίας για το Zero Trust αποκαλύπτει ότι, παρά την εντυπωσιακή ανάπτυξη του πεδίου τα τελευταία χρόνια, η υπάρχουσα επιστημονική γνώση εμφανίζει σημαντικούς περιορισμούς που επηρεάζουν τόσο τη θεωρητική κατανόηση όσο και την πρακτική εφαρμογή του μοντέλου. Αυτοί οι περιορισμοί προκύπτουν από ελλείψεις στη μεθοδολογία, από την ταχεία εξέλιξη της τεχνολογίας, από την επικράτηση βιομηχανικών white papers έναντι μιας πιο ακαδημαϊκής προσέγγισης, καθώς και από το γεγονός ότι η έννοια του Zero Trust δεν έχει σταθεροποιηθεί πλήρως ως ενιαίο θεωρητικό υπόδειγμα.

Πρώτον, πολλές από τις υπάρχουσες μελέτες έχουν βιομηχανικό χαρακτήρα και βασίζονται σε white papers, σε τεχνικές προδιαγραφές vendors ή σε οργανωσιακές αναφορές που δεν ακολουθούν αυστηρή επιστημονική μεθοδολογία. Οι αναλύσεις της Forrester, της Microsoft και της Deloitte αποτελούν πολύτιμα τεκμήρια για την εξέλιξη του Zero Trust, αλλά δεν εδράζονται σε εμπειρικά δεδομένα μεγάλης κλίμακας ούτε σε θεωρητικά μοντέλα που έχουν αξιολογηθεί υπό επιστημονικούς όρους (Cunningham et al., 2019· Deloitte, 2021· Golden et al., 2021). Η υπερεξάρτηση της βιβλιογραφίας από περιπτώσεις μεμονωμένων επιχειρήσεων, όπως το BeyondCorp της Google, επηρεάζει τη γενικευσιμότητα των συμπερασμάτων. Το μοντέλο αυτό αποτελεί μια εξαιρετικά επιτυχημένη αλλά ταυτόχρονα μοναδική εφαρμογή, προϊόν ιδιαίτερων συνθηκών, πόρων και τεχνικών δυνατοτήτων που δεν μπορούν να αναπαραχθούν εύκολα από άλλους οργανισμούς (Ward & Beyer, 2014).

Δεύτερον, οι περισσότερες ερευνητικές εργασίες επικεντρώνονται στους τεχνικούς μηχανισμούς του Zero Trust, παραμελώντας τις κοινωνικές, οργανωσιακές και διοικητικές διαστάσεις. Παρότι η βιβλιογραφία επισημαίνει επανειλημμένα ότι η εφαρμογή Zero Trust απαιτεί βαθιά πολιτισμική αλλαγή, εκπαίδευση εργαζομένων, αναθεώρηση διαδικασιών και εταιρικών δομών (Golden et al., 2021), λείπουν εμπειρικές μελέτες που να εξετάζουν συστηματικά τους παράγοντες επιτυχίας ή αποτυχίας στις πραγματικές συνθήκες ενός οργανισμού. Η έλλειψη ποιοτικών μεθοδολογιών, όπως συνεντεύξεις, Delphi panels ή συμμετοχική παρατήρηση, καθιστά δύσκολη την κατανόηση των κοινωνικών εμποδίων που αντιμετωπίζουν οι οργανισμοί κατά την υιοθέτηση Zero Trust. Η βιβλιογραφία σε θέματα

ερευνητικών μεθόδων, όπως οι ημιδομημένες συνεντεύξεις (Adeoye-Olatunde & Olenik, 2021) και η Delphi μεθοδολογία (Okoli & Pawlowski, 2004· Hasson et al., 2000), δείχνει ότι αυτές οι τεχνικές μπορούν να προσφέρουν πολύτιμη γνώση, ωστόσο στην πράξη εφαρμόζονται σπάνια στη μελέτη του Zero Trust.

Τρίτον, η υπάρχουσα έρευνα συχνά επικεντρώνεται στις ανάγκες μεγάλων επιχειρήσεων ή τεχνολογικών κολοσσών και όχι σε μικρομεσαίους οργανισμούς, δημόσιες υπηρεσίες ή περιβάλλοντα με περιορισμένο προϋπολογισμό. Οι μελέτες των Microsoft (2021a; 2021b) και Deloitte (2021), για παράδειγμα, εξετάζουν το Zero Trust με βάση περιβάλλοντα που διαθέτουν ώριμες υποδομές cloud, εκτεταμένα συστήματα IAM και υψηλό επίπεδο αυτοματοποίησης. Αυτή η εστίαση περιορίζει τη δυνατότητα μεταφοράς των πρακτικών αυτών σε μικρότερους οργανισμούς που αντιμετωπίζουν εντελώς διαφορετικές πραγματικότητες, όπως legacy υποδομές, έλλειψη εξειδικευμένου προσωπικού και περιορισμένη ικανότητα επένδυσης σε τεχνολογική αναβάθμιση.

Τέταρτον, η δυναμική φύση των απειλών καθιστά την έρευνα για το Zero Trust ετεροχρονισμένη σε σχέση με την πραγματικότητα των επιθέσεων. Οι Buck et al. (2021) περιγράφουν ότι το Zero Trust αποτελεί «πολυφωνικό» πεδίο, όπου η θεωρία συχνά ακολουθεί τις τεχνολογικές εξελίξεις αντί να τις προλαμβάνει. Οι αλλαγές στην τεχνητή νοημοσύνη, στις αυτοματοποιημένες επιθέσεις, στο cloud-native malware και στην εκθετική αύξηση της επιθετικής επιφάνειας των APIs καθιστούν πολλά παραδοσιακά μοντέλα αναφοράς ανεπαρκή μέσα σε πολύ μικρό χρονικό διάστημα. Η ίδια η έννοια του Zero Trust εξελίσσεται ταχύτερα από τη βιβλιογραφία που την περιγράφει.

Πέμπτον, η βιβλιογραφία δεν παρέχει ακόμη επαρκή σύγκλιση σχετικά με τον τρόπο αξιολόγησης της αποτελεσματικότητας ενός Zero Trust περιβάλλοντος. Παρότι υπάρχουν zero trust maturity models, όπως αυτά της CISA (2021), δεν υφίστανται ανεξάρτητα εμπειρικά δεδομένα που να επιβεβαιώνουν την αξιοπιστία, τη διαγνωστική τους ισχύ ή την καταλληλότητά τους για διαφορετικά είδη οργανισμών. Η έλλειψη μετρήσιμων δεικτών, benchmarks και διαχρονικών δεδομένων αποτελεί σημαντικό περιορισμό.

Έκτον, υπάρχει περιορισμένη έρευνα σχετικά με το πώς εφαρμόζεται το Zero Trust σε περιβάλλοντα IoT, βιομηχανικά συστήματα, συστήματα υγείας ή κρίσιμες εθνικές υποδομές. Παρότι το NIST SP 800-207 θέτει ένα γενικό θεωρητικό πλαίσιο (Kerman et al., 2020), δεν έχει αναπτυχθεί ακόμη επαρκής βιβλιογραφία που να εξετάζει πραγματικές εφαρμογές σε τέτοια περιβάλλοντα.

Τέλος, πολλοί από τους ισχυρισμούς σχετικά με τα πλεονεκτήματα του Zero Trust βασίζονται σε λογικές προεκτάσεις και όχι σε εμπειρική επιβεβαίωση. Παρά το ότι η MFA, η tokenization, η micro-segmentation και η continuous verification θεωρούνται αποδεδειγμένα αποτελεσματικές τεχνικές, οι πραγματικές τους επιπτώσεις σε περιβάλλοντα διαφορετικών επιχειρήσεων, χωρών ή κλάδων δεν έχουν εξεταστεί σε βάθος. Η βιβλιογραφία, όπως αυτή των Ferretti et al. (2021) και των Microsoft (2021a), παρέχει ενδείξεις και όχι πλήρη απόδειξη καθολικής αποτελεσματικότητας.

Η υπάρχουσα βιβλιογραφία για το Zero Trust βρίσκεται σε διαδικασία διαμόρφωσης. Παρά τη σημαντική πρόοδο, το πεδίο εμφανίζει εννοιολογική αστάθεια, μεθοδολογικούς περιορισμούς και ελλιπή εμπειρικά δεδομένα, γεγονός που καθιστά αναγκαία την ανάπτυξη ενός πιο ώριμου και επιστημονικά εδραιωμένου σώματος γνώσης.

6.4 Προτάσεις για μελλοντική έρευνα

Λαμβάνοντας υπόψη τους περιορισμούς των υπάρχουσων μελετών, η μελλοντική έρευνα για το Zero Trust πρέπει να κατευθυνθεί προς τη δημιουργία πιο συστηματικών, εμπειρικά θεμελιωμένων και μεθοδολογικά διαφοροποιημένων προσεγγίσεων. Η ανάγκη αυτή αναδεικνύεται έντονα στη βιβλιογραφία, καθώς η πολυπλοκότητα του Zero Trust και η ταχεία εξέλιξη του κυβερνο-οικοσυστήματος απαιτούν νέες μεθόδους, νέα δεδομένα και νέες θεωρητικές συνθέσεις.

Αρχικά, απαιτείται μεγαλύτερη ανάπτυξη εμπειρικών μελετών μεγάλης κλίμακας. Οι υπάρχουσες έρευνες στηρίζονται κυρίως σε case studies μεγάλων οργανισμών και τεχνολογικών παρόχων. Έτσι, η μελλοντική έρευνα πρέπει να συλλέξει δεδομένα από ευρύ φάσμα περιβαλλόντων, συμπεριλαμβανομένων μικρομεσαίων επιχειρήσεων, δημοσίων οργανισμών, σχολείων, πανεπιστημίων, παρόχων υγείας και βιομηχανικών μονάδων. Η έλλειψη τέτοιων δεδομένων περιορίζει σήμερα τη δυνατότητα γενίκευσης των αποτελεσμάτων. Μεθοδολογίες όπως οι ημιδομημένες συνεντεύξεις (Adeoye-Olatunde & Olenik, 2021) ή οι expert interviews (Bogner & Menz, 2009· Meuser & Nagel, 2009) μπορούν να αξιοποιηθούν για τη συλλογή βαθύτερης ποιοτικής γνώσης σχετικά με τις προκλήσεις, τις αντιστάσεις και τους παράγοντες επιτυχίας.

Δεύτερον, απαιτείται η ανάπτυξη σύγχρονων ερευνητικών πλαισίων που να εξετάζουν τη διαλειτουργικότητα και τη συγκριτική αποτελεσματικότητα διαφορετικών Zero Trust αρχιτεκτονικών. Η βιβλιογραφία κάνει αναφορές στις διαφορές μεταξύ BeyondCorp,

Microsoft Zero Trust και άλλων vendor-based προσεγγίσεων, αλλά δεν υπάρχουν συστηματικές συγκριτικές μελέτες που να εξετάζουν ποια μοντέλα λειτουργούν καλύτερα υπό ποιες συνθήκες (CISA, 2021· Buck et al., 2021). Η δημιουργία benchmark frameworks θα ανήκει σε έναν κρίσιμο τομέα μελλοντικής έρευνας.

Τρίτον, η μελλοντική έρευνα πρέπει να διερευνήσει τη χρήση AI και machine learning για τη βελτίωση της continuous verification και της risk-based authentication. Η υπάρχουσα βιβλιογραφία αναφέρεται στη σημασία των telemetry signals (Microsoft, 2021a· Microsoft, 2021b), αλλά δεν υπάρχουν εμπειρικές μελέτες που να εξετάζουν την απόδοση διαφορετικών αλγορίθμων σε πραγματικό περιβάλλον. Η μελλοντική έρευνα μπορεί να αξιοποιήσει τεχνικές anomaly detection, deep learning και graph analytics για να ενισχύσει τα Zero Trust συστήματα με αυτόνομες, προγνωστικές δυνατότητες.

Τέταρτον, απαιτούνται μελέτες για την εφαρμογή Zero Trust σε περιβάλλοντα IoT, OT, industrial control systems και συστήματα υγείας. Τα περιβάλλοντα αυτά έχουν κανόνες λειτουργίας που έρχονται σε αντίθεση με ορισμένες πρακτικές Zero Trust, όπως η επιβολή frequent re-authentication ή η micro-segmentation σε real-time συστήματα. Η βιβλιογραφία δεν έχει ακόμη εξετάσει πώς μπορούν να σχεδιαστούν εναλλακτικά Zero Trust μοντέλα κατάλληλα για τέτοιες περιπτώσεις.

Πέμπτον, η μελλοντική έρευνα πρέπει να επικεντρωθεί στην οργανωσιακή διάσταση της υιοθέτησης Zero Trust. Οι Deloitte (2021) και Golden et al. (2021) τονίζουν την ανάγκη για organizational change management, αλλά δεν υπάρχουν θεωρητικά μοντέλα που να εξηγούν πώς οργανισμοί υιοθετούν Zero Trust, πώς αναπτύσσεται η κουλτούρα ασφάλειας και ποιοι κοινωνικοί παράγοντες οδηγούν στην επιτυχία ή στην αποτυχία. Ποιοτικές μέθοδοι, όπως Delphi studies (Hasson et al., 2000· Egfjord & Sund, 2020), μπορούν να βοηθήσουν στη δημιουργία νέων θεωρητικών μοντέλων ηγεσίας και ωριμότητας.

Έκτον, απαιτείται μελλοντική έρευνα για την ενσωμάτωση Zero Trust με κανονιστικά πλαίσια. Αν και το NIST SP 800-207 ευθυγραμμίζεται με τα σύγχρονα απαιτούμενα συμμόρφωσης, δεν υπάρχουν μελέτες που να εξετάζουν εμπειρικά τον τρόπο με τον οποίο οργανισμοί μεταφράζουν τις αρχές Zero Trust σε κανονιστική συμμόρφωση, ούτε μελέτες που να εξετάζουν τον αντίκτυπο του Zero Trust σε audits, risk assessments ή data governance διαδικασίες.

Τέλος, υπάρχει ανάγκη ανάπτυξης ενός ενιαίου θεωρητικού μοντέλου Zero Trust που να ενσωματώνει όλα τα επιμέρους στοιχεία: την ταυτότητα, τη συσκευή, τη συμπεριφορά, το

περιβάλλον, την πρόσβαση, τον έλεγχο πολιτικών και την επιβολή. Η έννοια του Zero Trust παραμένει σήμερα πολυδιάστατη και ανοικτή σε πολλές ερμηνείες, όπως τονίζουν οι Buck et al. (2021). Η ανάπτυξη ενός consolidated theoretical model θα επιτρέψει την ερευνητική ωρίμανση του πεδίου και θα δημιουργήσει ένα σταθερό υπόβαθρο για μελλοντικές εμπειρικές εφαρμογές.

Η μελλοντική έρευνα πρέπει να κινηθεί προς μια πιο ισορροπημένη, διεπιστημονική και εμπειρικά τεκμηριωμένη προσέγγιση του Zero Trust. Το πεδίο έχει ήδη αναπτυχθεί εντυπωσιακά, αλλά η ωρίμανσή του απαιτεί νέες μεθόδους, νέες θεωρίες και νέα δεδομένα που θα επιτρέψουν την πληρέστερη κατανόηση και την ευρύτερη εφαρμογή του.

Βιβλιογραφία

ACT-IAC. (2019). *Zero Trust Cybersecurity: Current Trends*. American Council for Technology–Industry Advisory Council. https://www.actiac.org/documents/zero-trust-cybersecurity-current-trends

Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security, 122*, 102911. https://doi.org/10.1016/j.cose.2022.102911

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *Journal of the American College of Clinical Pharmacy, 4*(10), 1358–1367. https://doi.org/10.1002/jac5.1441

Bennett, M., Balaouras, S., & Glenn, M. (2017). *Zero Trust Security: A CIO's guide to defending their business from cyberattacks*. Forrester. https://www.forrester.com/report/zero-trust-security-a-cio-s-guide-to-defending-their-business-from-cyberattacks/RES136651

Bobbert, Y., & Scheerder, J. (2020). Zero trust validation: From practical approaches to theory. *Science Journal of Research & Reviews, 2*(5). https://doi.org/10.33552/SJRR.2020.02.000546

Bogner, A., & Menz, W. (2009). The theory-generating expert interview: Epistemological interest, forms of knowledge, interaction. In A. Bogner, B. Littig, & W. Menz (Eds.), *Interviewing experts* (pp. 43–80). Palgrave Macmillan. https://doi.org/10.1057/9780230244276_3

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health, 11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security, 110*, 102436. https://doi.org/10.1016/j.cose.2021.102436

Campbell, M. (2020). Beyond zero trust: Trust is a vulnerability. *Computer, 53*(10), 110–113. https://doi.org/10.1109/MC.2020.3011081

CISA. (2021). *Zero Trust Maturity Model*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/zero-trust-maturity-model

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Cunningham, C. (2018). *The Zero Trust eXtended (ZTX) ecosystem*. Forrester. https://engage2demand.cisco.com/LP=10091

Cunningham, C., Holmes, D., & Pollard, J. (2019). *The eight business and security benefits of zero trust*. Forrester. https://www.forrester.com/report/the-eight-business-and-security-benefits-of-zero-trust/RES134863

Deloitte. (2021). *A revolutionary approach to cyber or just another buzzword?* https://www2.deloitte.com/uk/en/pages/risk/articles/zero-trust.html

Egfjord, K. F.-H., & Sund, K. J. (2020). A modified Delphi method to elicit and compare perceptions of industry trends. *MethodsX, 7*, 101081. https://doi.org/10.1016/j.mex.2020.101081

Ferretti, L., Magnanini, F., Andreolini, M., & Colajanni, M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security, 110*, 102419. https://doi.org/10.1016/j.cose.2021.102419

Freund, Y. P. (1988). Critical success factors. *Planning Review, 16*(4), 20–23. https://doi.org/10.1108/eb054225

Golden, D., Perinkolam, A., Nicholson, M., Rafla, A., & Norton, K. (2021). *Zero trust: Never trust, always verify*. Deloitte. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2021/zero-trust-security-framework.html

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing, 32*(4), 1008–1015. https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x

Jakkal, V. (2021). *Zero Trust Adoption Report: How does your organization compare?* Microsoft. https://www.microsoft.com/security/blog/2021/07/28/zero-trust-adoption-report-how-does-your-organization-compare/

Kerman, A., Borchert, O., Rose, S., & Tan, A. (2020). *Implementing a Zero Trust Architecture*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/white-paper/2020/10/21/implementing-a-zero-trust-architecture/final

Leszczyna, R., Wallis, T., & Wróbel, M. R. (2019). Developing novel solutions to realise the European Energy information sharing & analysis centre. *Decision Support Systems, 122*, 113067. https://doi.org/10.1016/j.dss.2019.05.007

Meuser, M., & Nagel, U. (2009). The expert interview and changes in knowledge production. In A. Bogner, B. Littig, & W. Menz (Eds.), *Interviewing experts* (pp. 17–42). Palgrave Macmillan. https://doi.org/10.1057/9780230244276_2

Microsoft. (2021a). *The 2021 Microsoft Digital Defense Report*. https://info.microsoft.com/ww-landing-Microsoft-Digital-Defense-Report-Gate.html

Microsoft. (2021b). *Evolving Zero Trust*. https://www.microsoft.com/en-us/security/business/zero-trust

Naderpour, M., Lu, J., & Zhang, G. (2014). An intelligent situation awareness support system for safety-critical environments. *Decision Support Systems, 59*, 325–340. https://doi.org/10.1016/j.dss.2014.01.004

Netskope. (2020). *Zero Trust Leading Practice*. https://resources.netskope.com/cloud-security-solution-white-papers/zero-trust-leading-practice

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002

Sciarretta, G., Carbone, R., Ranise, S., & Viganò, L. (2020). Formal analysis of mobile multi-factor authentication with single sign-on login. *ACM Transactions on Privacy and Security, 23*(3), 1–37. https://doi.org/10.1145/3386685

Turner, S., Holmes, D., Cunningham, C., Budge, J., McKay, P., Cser, A., Shey, H., & Maxim, M. (2021). *A practical guide to a Zero Trust implementation*. Forrester. https://www.forrester.com/report/a-practical-guide-to-a-zero-trust-implementation/RES157736

Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. *;login:, 39*(6), 6–11.

Yeoh, W., Huang, H., Lee, W. S., Al Jafari, F., & Mansson, R. (2021). Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems*, 1–20. https://doi.org/10.1080/08874417.2021.1919941

Yeoh, W., & Koronios, A. (2010). Critical success factors for business intelligence systems. *Journal of Computer Information Systems, 50*(3), 23–32. https://doi.org/10.1080/08874417.2010.11645404