
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ


# ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΑ ΔΙΚΤΥΑ ΔΙΑΝΟΜΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ


της

Ζαρκαλή Βασίλως ΜΤΕ2206

Επιβλέπων: Γκρίτζαλης Στέφανος



ΑΘΗΝΑ, ΝΟΕΜΒΡΙΟΣ 2024

Η σελίδα αυτή είναι σκόπιμα λευκή

# Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει την ασφάλεια και την προστασία της ιδιωτικότητας στα Content Delivery Networks (CDN), αναδεικνύοντας τις βασικές αρχιτεκτονικές τους, τις προκλήσεις που αντιμετωπίζουν και τις τεχνολογίες που χρησιμοποιούνται για την προστασία των δεδομένων και των χρηστών.

Αρχικά, γίνεται ανάλυση της λειτουργίας των CDN, τα οποία αποτελούν κατανεμημένα δίκτυα διακομιστών που επιταχύνουν την παράδοση περιεχομένου στο διαδίκτυο. Παρουσιάζονται οι βασικές συνιστώσες τους, όπως οι Edge Servers, οι μηχανισμοί caching και οι τεχνικές δρομολόγησης αιτημάτων, καθώς και οι διαφορετικοί τύποι των CDN (Public, Private, P2P, Hybrid).

Στη συνέχεια, η εργασία εστιάζει στις απειλές ασφάλειας που σχετίζονται με τα CDN, όπως οι επιθέσεις DDoS, η εκμετάλλευση αδυναμιών σε επίπεδο εφαρμογής, η υποκλοπή δεδομένων και η αποκάλυψη του Origin Server. Αναλύονται οι μηχανισμοί προστασίας, όπως τα Web Application Firewalls (WAF), τα συστήματα ανίχνευσης εισβολών (IDS), οι τεχνικές anti-bot και η χρήση κρυπτογράφησης δεδομένων.

Επιπλέον, δίνεται έμφαση στο ζήτημα της ιδιωτικότητας, καθώς τα CDN συχνά συλλέγουν και αποθηκεύουν δεδομένα χρηστών. Γίνεται αναφορά σε κανονιστικά πλαίσια, όπως ο GDPR και η οδηγία NIS-2, και εξετάζονται τεχνολογίες που ενισχύουν την προστασία προσωπικών δεδομένων, όπως η ανωνυμοποίηση, το Privacy by Design και η χρήση ασφαλών πρωτοκόλλων επικοινωνίας.

Ως μελέτη περίπτωσης, αναλύεται το Akamai CDN, ένα από τα μεγαλύτερα και πιο διαδεδομένα δίκτυα παγκοσμίως, και εξετάζονται οι στρατηγικές που χρησιμοποιεί για την ασφάλεια και τη συμμόρφωση με τα κανονιστικά πρότυπα.

Η εργασία καταλήγει στο συμπέρασμα ότι τα CDN αποτελούν βασικό εργαλείο για την απόδοση και την ασφάλεια του διαδικτύου, ωστόσο απαιτούν διαρκή προσαρμογή σε νέες απειλές. Η χρήση τεχνολογιών όπως η τεχνητή νοημοσύνη, η αυτοματοποιημένη ανίχνευση επιθέσεων και οι αποκεντρωμένες λύσεις προστασίας δεδομένων αναμένεται να παίξουν καθοριστικό ρόλο στο μέλλον.

# Πίνακας Περιεχομένων

# Λίστα Εικόνων



# Λίστα Πινάκων

# Κεφάλαιο 1ο: Content Delivery Network (CDN)

## 1.1 Εισαγωγή στο Content Delivery Network (CDN)

Το Content Delivery Network (CDN) αποτελεί μια εξαιρετικά κατανεμημένη πλατφόρμα διακομιστών που ελαττώνει τη γεωγραφική απόσταση μεταξύ ενός διακομιστή και ενός χρήστη, ελαχιστοποιώντας με αυτόν τον τρόπο τις καθυστερήσεις κατά τη φόρτωση ιστοσελίδων [2]. Βασισμένο στη διαδικασία Caching, το CDN αποθηκεύει περιεχόμενο στα πλησιέστερα για τους τελικούς χρήστες κέντρα δεδομένων παγκοσμίως. Στη συνέχεια, δρομολογεί τα αιτήματα των τελικών χρηστών προς αυτά τα κέντρα και διανέμει το περιεχόμενο στους τελικούς χρήστες, με αποτέλεσμα να εξασφαλίζει ταχύτερη και αποδοτικότερη διαδικτυακή εμπειρία [1].

## 1.2 Ιστορική Αναδρομή

Η ιδέα των CDN εμφανίστηκε πριν από περίπου 20 έτη με σκοπό την αντιμετώπιση της πρόκλησης της ταχείας διανομής μεγάλων όγκων δεδομένων μέσω του διαδικτύου. Σήμερα, τα CDNs αποτελούν την κινητήρια δύναμη της διαδικτυακής εμπειρίας. Τα πρώτα CDN εμφανίστηκαν στα τέλη της δεκαετίας του 90’ και εξακολουθούν μέχρι και σήμερα να διαδραματίζουν σημαντικό ρόλο, διανέμοντας περίπου το 15%-30% της παγκόσμιας κίνησης. Η ανάπτυξη του ευρυζωνικού περιεχομένου καθώς και η αυξανόμενη ζήτηση για μετάδοση περιεχομένου, όπως ήχου, βίντεο και δεδομένων, οδήγησαν στη δημιουργία μίας πληθώρας τύπων CDN [2,3].

Η εξέλιξη των CDN μπορεί να διακριθεί σε τέσσερις φάσεις:

**Περίοδος Προ-Διαμόρφωσης**: πριν από την ουσιαστική καινοτομία του CDN, η τεχνολογία καθώς και οι υποδομές βρισκόταν στο στάδιο ανάπτυξης. Κατά την περίοδο αυτή, σημειώθηκαν σημαντικές πρόοδοι, όπως η άνοδος των φαρμών διακομιστών, το ιεραρχικό Caching, οι βελτιώσεις στους διακομιστές ιστού καθώς και η δημιουργία των Caching Proxy Servers. Επιπλέον, τεχνολογίες όπως το Mirroring, το Caching και το Multihoming αποτέλεσαν θεμέλια για την ανάπτυξη των πρώτων CDN [3].

**1η γενιά:** Η πρώτη γενιά CDN ασχολήθηκε κυρίως με τη διανομή στατικού και δυναμικού περιεχομένου, τους δύο κύριους τύπους δεδομένων στο διαδίκτυο εκείνη την εποχή. Ο βασικός μηχανισμός λειτουργίας βασίζονταν στην υλοποίηση αντιγράφων, στην ευφυή δρομολόγηση καθώς και στην εφαρμογή τεχνικών Edge Computing. Αυτά τα συστήματα επέτρεπαν τη διανομή εφαρμογών και πληροφοριών μεταξύ των διακομιστών [2,3]

**2η γενιά:** Στην δεύτερη φάση, τα CDN επικεντρώθηκαν στην μετάδοση περιεχομένου βίντεο και ήχου ή υπηρεσιών Video on Demand (VOD). Παράλληλα, εισήχθησαν και τεχνολογίες

Peer-to-Peer (P2P), Cloud Computing, καθώς και υποστήριξη για περιεχόμενο ιστότοπων που προοριζόταν για κινητές συσκευές.

3η γενιά: Η τρίτη γενιά CDN ανταποκρίνεται στις απαιτήσεις της σύγχρονης επιστημονικής έρευνας και ανάπτυξης Τα σύγχρονα CDN χαρακτηρίζονται από υψηλό επίπεδο αυτοματοποίησης, δυναμική προσαρμογή στις συνθήκες δικτύου και χρήση τεχνητής νοημοσύνης για τη βελτίωση της εμπειρίας του τελικού χρήστη. Στο μέλλον, τα CDN αναμένεται να εξελιχθούν περαιτέρω, καθοδηγούμενα από τις ανάγκες των χρηστών, με την ποιότητα της εμπειρίας του τελικού χρήστη να αποτελεί καθοριστικό παράγοντα [2,3].

Τα CDN δημιουργήθηκαν αρχικά για να ανταποκριθούν στις αυξανόμενες απαιτήσεις σε εύρος ζώνης, καθώς η δημοτικότητα της μετάδοσης βίντεο οδήγησε σε αύξηση της ζήτησης για υπηρεσίες από παρόχους CDN. Με την πρόοδο της συνδεσιμότητας και τις αλλαγές στις καταναλωτικές τάσεις, το κόστος των υπηρεσιών CDN μειώθηκε, επιτρέποντας τη διάδοσή τους σε μαζική κλίμακα. Επιπλέον, η ανάπτυξη της νεφουπολογιστικής έχει καταστήσει τα CDN αναπόσπαστο μέρος των επιχειρησιακών λειτουργιών σε παγκόσμιο επίπεδο [2,3].

Πέρα από τη βελτίωση της απόδοσης και της διαθεσιμότητας των ιστοσελίδων, τα CDN σήμερα προσφέρουν μια σειρά από λειτουργίες ασφαλείας, όπως η προστασία από επιθέσεις DDoS, η ανίχνευση και η αποτροπή κακόβουλου λογισμικού, καθώς και η κρυπτογράφηση των δεδομένων. Ωστόσο, η αυξανόμενη πολυπλοκότητα των CDN και η συγκέντρωση δεδομένων σε μεγάλους παρόχους δημιουργούν προκλήσεις, όπως η αυξημένη εξάρτηση από συγκεκριμένους παρόχους και η δυνατότητα καταχρηστικής εκμετάλλευσης δεδομένων.

## 1.3 Προκλήσεις στο Content Delivery μέσω του Διαδικτύου

Αν και συχνά αναφέρεται ως μια ενιαία οντότητα, το διαδίκτυο στην πραγματικότητα αποτελείται από χιλιάδες διαφορετικά δίκτυα, το καθένα εκ των οποίων εξυπηρετεί ένα μικρό ποσοστό χρηστών. Αξίζει να σημειωθεί πώς ακόμα και το μεγαλύτερο δίκτυο εξυπηρετεί μόνο ένα 5% περίπου της παγκόσμιας κίνησης στο διαδίκτυο, με τα ποσοστά να μειώνονται ραγδαία στην συνέχεια (Εικόνα 1). Στην πραγματικότητα, παραπάνω από 650 δίκτυα είναι απαραίτητα για να φτάσουν το 90% της συνολικής κίνησης. Αυτό σημαίνει πώς το περιεχόμενο που φιλοξενείται κεντρικά πρέπει να διασχίσει πολλά δίκτυα προκειμένου να φτάσει στους τελικούς χρήστες [4].

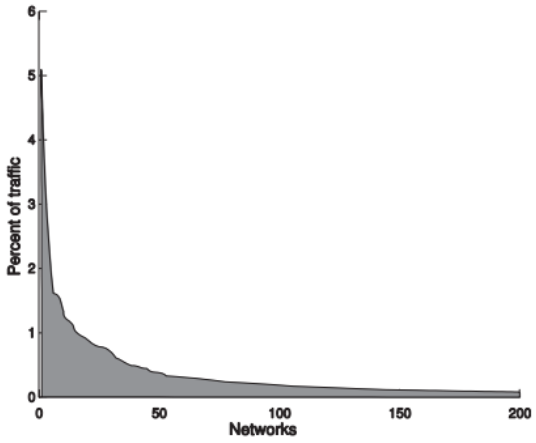


*Figure 1: Ποσοστό κίνησης από τα κορυφαία δίκτυα - The Akamai Network: A Platform for High-Performance Internet Applications, E.Nygren, K.Sitamaran, J.Sun*

Δυστυχώς, η διασύνδεση δεδομένων μέσω διαφορετικών δικτύων δεν είναι ούτε αποδοτική, ούτε αξιόπιστη και μπορεί να επηρεαστεί αρνητικά από πληθώρα παραγόντων, οι σημαντικότεροι εκ των οποίων είναι οι κάτωθι:

**Συμφόρηση στα Σημεία Σύνδεσης (Peering Point Congestion):** Η χωρητικότητα στα σημεία σύνδεσης όπου τα δίκτυα ανταλλάσσουν κίνηση, συνήθως δεν επαρκεί για να καλύψει την ζήτηση, κυρίως λόγω της οικονομικής δομής του διαδικτύου. Αυτό οφείλεται κυρίως στη σύσταση της οικονομίας του διαδικτύου, όπου οι επενδύσεις επικεντρώνονται στην αρχή (φιλοξενία ιστοσελίδων) και στο τέλος της διαδρομής (τελικοί χρήστες). Αντίθετα, τα μεσαία σημεία σύνδεσης, τα οποία είναι υψηλού κόστους και χωρίς άμεσα έσοδα, παραμελούνται. Αυτή η ανισορροπία δημιουργεί "στενά σημεία" (Bottlenecks), που οδηγούν σε απώλειες πακέτων και αυξημένες καθυστερήσεις.

**Αναποτελεσματικά Πρωτόκολλα Δρομολόγησης:** Το BGP, αν και διαχειρίζεται ικανοποιητικά την κλιμάκωση του διαδικτύου, έχει γνωστούς περιορισμούς. Το BGP δεν σχεδιάστηκε με γνώμονα την απόδοση, συγκεκριμένα βασίζει τους υπολογισμούς των διαδρομών του κυρίως στον αριθμό των hops, χωρίς να λαμβάνει υπόψιν του τοπολογίες, καθυστερήσεις ή την συμφόρηση των δικτύων. Το BGP συχνά χρησιμοποιείται για να υποστηρίξει επιχειρηματικές συμφωνίες παρά για βέλτιστη απόδοση από άκρο σε άκρο. Αξίζει επίσης να σημειωθεί πώς, το PGP είναι ευάλωτο σε ανθρώπινα λάθη καθώς και σε κακόβουλες ενέργειες, όπως λανθασμένες ή κακώς διαμορφωμένες διαδρομές, που μπορούν να προκαλέσουν σοβαρές διακοπές συνδεσιμότητας.

**Αναξιόπιστα Δίκτυα:** Στο διαδίκτυο, οι διακοπές είναι συχνές και οφείλονται σε ποικίλους λόγους, όπως κοπές καλωδίων, κακώς διαμορφωμένους δρομολογητές, επιθέσεις DDoS και φυσικές καταστροφές. Μεγάλης κλίμακας διακοπές, όπως η αποσύνδεση των δικτύων Sprint και Cogent το 2008, μπορούν να επηρεάσουν χιλιάδες δίκτυα, ενώ περιστατικά BGP

Hijacking, όπως και το παγκόσμιο blackout του YouTube το 2008, υπογραμμίζουν την ευπάθεια των συστημάτων.

**Αναποτελεσματικά Δίκτυα Δρομολόγησης:** Αν και το TCP σχεδιάστηκε για αξιοπιστία και αποφυγή συμφόρησης, φέρει σημαντικό επιπλέον φόρτο και μπορεί να έχει χαμηλή απόδοση για συνδέσεις με υψηλή καθυστέρηση ή απώλεια πακέτων, και τα δυο εκ των οποίων είναι κοινά στο ευρύ διαδίκτυο. Επιπλέον, για εφαρμογές αλληλεπίδρασης (Interactive Applications), οι πολλαπλοί γύροι που απαιτούνται για τα αιτήματα HTTP μπορούν γρήγορα να συσσωρευτούν, επηρεάζοντας την απόδοση της εφαρμογής. Το TCP επίσης γίνεται σοβαρό σημείο συμφόρησης για την απόδοση της μετάδοσης των βίντεο και άλλων μεγάλων αρχείων. Επειδή απαιτεί επιβεβαιώσεις από τον παραλήπτη για κάθε παράθυρο δεδομένων που αποστέλλεται, η ταχύτητα μετάδοσης σχετίζεται με την καθυστέρηση του δικτύου ή τον χρόνο γύρου (RTT). Έτσι, η απόσταση μεταξύ διακομιστή και τελικού χρήστη μπορεί να γίνει το κύριο σημείο συμφόρησης για τις ταχύτητες λήψης και την ποιότητα θέασης βίντεο.

**Κλιμάκωση (Scalability):** η κλιμάκωση των εφαρμογών του διαδικτύου σημαίνει ότι πρέπει να υπάρχουν αρκετοί πόροι διαθέσιμοι για να ανταποκριθούν στις αυξημένες ανάγκες που υπάρχουν σε περιόδους αιχμής. Η διαχείριση αυτών των αιχμών είναι δαπανηρή και απαιτεί λεπτομερή πρόβλεψη, η οποία συχνά αποδεικνύεται δύσκολη. Εάν οι διαθέσιμοι πόροι είναι δεν είναι αρκετοί, υπάρχει κίνδυνος απώλειας ευκαιριών, ενώ η υπερβολική παροχή οδηγεί σε σπατάλη και αυξημένο κόστος. Παράλληλα, η ανάγκη για διαρκή διαθεσιμότητα πόρων έχει και περιβαλλοντικές συνέπειες, λόγω της ενέργειας που καταναλώνουν οι υποδομές που μένουν ανεκμετάλλευτες.

**Περιορισμοί σε επίπεδο εφαρμογής και ο αργός ρυθμός υιοθέτησης αλλαγών:** Αν και ορισμένες από τις προκλήσεις που αντιμετωπίζει το διαδίκτυο μπορούν να αντιμετωπιστούν εν μέρει με αλλαγές στα πρωτόκολλα και/ή στο λογισμικό του πελάτη, η ιστορία δείχνει ότι αυτές οι αλλαγές πραγματοποιούνται αργά. Ενώ οι επιχειρήσεις επιθυμούν να παρέχουν την καλύτερη απόδοση στους τελικούς χρήστες τους, συχνά έχουν λίγο ή καθόλου έλεγχο πάνω στο λογισμικό των τελικών χρηστών [4].

## 1.4 Αρχιτεκτονική του Content Delivery Network (CDN)

Οι προκλήσεις που αναφέρθηκαν στο προηγούμενο υποκεφάλαιο, αναδεικνύουν πόσο δύσκολο μπορεί να είναι για τις επιχειρήσεις να επιτύχουν αποδεκτά επίπεδα απόδοσης, αξιοπιστίας και οικονομικά αποδοτικής κλιμάκωσης στις διαδικτυακές δραστηριότητες. Τα περισσότερα σημεία συμφόρησης βρίσκονται εκτός του ελέγχου οποιουδήποτε μεμονωμένου φορέα και είναι εγγενή στον τρόπο λειτουργίας του διαδικτύου, ως ένα χαλαρά συντονισμένο μωσαϊκό από ετερογενή, αυτόνομα δίκτυα [4].

Ένα CDN έχει ως στόχο την βελτίωση της εμπειρίας των τελικών χρηστών κατά την διανομή ψηφιακού περιεχομένου, ενώ παράλληλα αξιοποιεί πιο αποτελεσματικά τους δικτυακούς πόρους. Το CDN αποθηκεύει προσωρινά περιεχόμενο σε τοποθεσίες κοντινές στους τελικούς χρήστες, δρομολογεί τα αιτήματα των χρηστών για το περιεχόμενο προς σε αυτές τις τοποθεσίες και διανέμει το περιεχόμενο στους τελικούς χρήστες.

Οι κύριοι βασικοί παράγοντες της διαδικασίας διανομής περιεχομένου είναι οι πάροχοι CDN, οι κάτοχοι περιεχομένου και οι τελικοί χρήστες. Ο πάροχος CDN διαχειρίζεται και λειτουργεί την υποδομή του CDN. Ο κάτοχος περιεχομένου διαθέτει ψηφιακό περιεχόμενο και είναι πελάτης του CDN. Οι κάτοχοι περιεχομένου αναθέτουν την διανομή του περιεχομένου τους στα CDN. Ο τελικός χρήστης καταναλώνει το περιεχόμενο χρησιμοποιώντας ψηφιακές συσκευές, όπως τηλεοράσεις, tablet και έξυπνα τηλέφωνα [5].

### 1.4.1 Delivery Networks ως Εικονικά Δίκτυα

Γενικά, ένα Delivery Network σε θεωρητικό επίπεδο, είναι ένα εικονικό δίκτυο που δημιουργείται ως ένα επίπεδο λογισμικού πάνω από το υπάρχον διαδίκτυο και εγκαθίσταται σε ευρέως κατανεμημένες υποδομές ενώ σχεδιάζεται ειδικά για να καλύπτει τις ανάγκες κατανεμημένων εφαρμογών και υπηρεσιών. Ένα τέτοιο δίκτυο προσφέρει βελτιωμένη αξιοπιστία, απόδοση, επεκτασιμότητα και ασφάλεια, χαρακτηριστικά που δεν μπορούν να επιτευχθούν με την απευθείας χρήση του βασικού διαδικτύου. Ένα παραδοσιακό CDN, που χρησιμοποιείται για την παράδοση στατικού περιεχομένου ιστού, αποτελεί έναν από τους τύπους αυτών των δικτύων. Το πλεονέκτημα της προσέγγισης του εικονικού δικτύου είναι ότι λειτουργεί πάνω στο υπάρχον διαδίκτυο χωρίς την ανάγκη για ειδικό λογισμικό από την πλευρά του χρήστη ή αλλαγές στα υποκείμενα δίκτυα. Επιπλέον, επειδή βασίζεται κυρίως σε λογισμικό, μπορεί εύκολα να προσαρμοστεί σε μελλοντικές απαιτήσεις, καθώς το διαδίκτυο συνεχίζει να εξελίσσεται. [4]

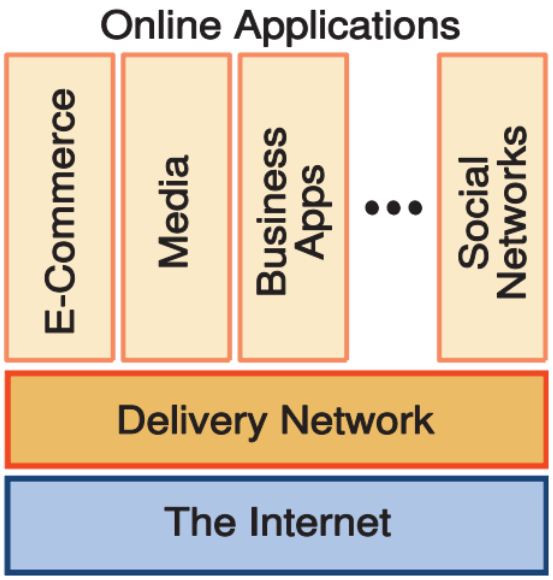


*Figure 2: Το Delivery Network ως εικονικό δίκτυο πάνω από το διαδίκτυο - The Akamai Network: A Platform for High-Performance Internet Applications, E.Nygren, K.Sitamaran, J.Sun*

### 1.4.2 Διαδικασία του Content Delivery

Η διαδικασία του Content Delivery ξεκινάει από τον ιδιοκτήτη του περιεχομένου, ο οποίος αποθηκεύει τα ψηφιακά δεδομένα στους Origin Servers. Το CDN διανέμει και αναπαράγει το περιεχόμενο από τους Origin Servers σε πληθώρα Edge Servers, οι οποίοι μπορεί να αριθμούν από εκατοντάδες έως και χιλιάδες. Αυτοί οι Edge Servers είναι κατανεμημένοι σε όλο το Διαδίκτυο, παρέχοντας υψηλή αποθηκευτική ικανότητα με σκοπό το Caching περιεχομένου σε κοντινή απόσταση από τους τελικούς χρήστες.

Στην Εικόνα 3 φαίνεται η διαδικασία διανομής περιεχομένου μέσω ενός CDN. Το CDN λαμβάνει και εξυπηρετεί αιτήματα τελικών χρηστών για λογαριασμό απομακρυσμένων ιδιοκτητών περιεχομένου (βήμα 1). Κάνοντας χρήση ενός μηχανισμού δρομολόγησης αιτημάτων, το CDN επιλέγει και ανακατευθύνει το Request σε έναν Edge Server (βήμα 2). Ο επιλεγμένος Edge Server πραγματοποιεί στην συνέχεια έναν έλεγχο αποδοχής και αν το αίτημα γίνει δεκτό, τότε ο Edge Server διανέμει το περιεχόμενο από την Cache του (βήμα 3). Στην περίπτωση που το περιεχόμενο δεν είναι διαθέσιμο στην Cache, ο Edge Server ανακτά και αποθηκεύει το περιεχόμενο είτε από έναν άλλο Edge Server, είτε απευθείας από τον Origin Server (βήμα 4) [5].

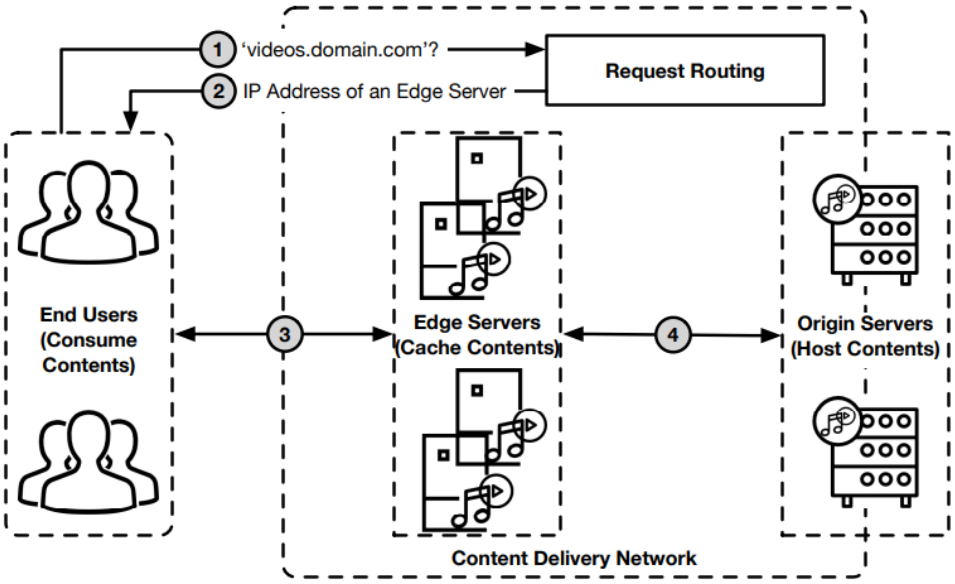


*Figure 3: Η υποδομή ενός Content Delivery Network - Content Delivery Network Security: A Survey, M. Ghaznavi, E. Jalalpour, A. Salahuddin, R. Boutaba, D. Migault, S. Preda*

### 1.4.3 Κύριες Λειτουργικές Μονάδες του Content Delivery Network (CDN)

Όλες οι λειτουργικές μονάδες ενός CDN, συμπεριλαμβανομένων των Edge Servers, του μηχανισμού δρομολόγησης αιτημάτων καθώς και οι Origin Servers, συμμετέχουν στην διαδικασία διανομής του περιεχομένου [4]. Ακολούθως, αναλύεται καθένα από τα συστατικά στοιχεία του CDN:

**Edge Servers:** οι Edge Servers λειτουργούν ως προστατευτική ασπίδα και κασάρουν το περιεχόμενο, ώστε να διατηρείται σε χαμηλά επίπεδα η κίνηση που φτάνει στους Origin

Server. Οι Edge Servers τοποθετούνται στρατηγικά σε Points of Presence (PoPs) του CDN, κοντά στους τελικούς χρήστες, συνήθως σε απόσταση ενός ή δύο δικτυακών hops. Παραδείγματα τέτοιων PoPs είναι τα σημεία ανταλλαγής διαδικτυακής κίνησης (Internet Exchange Points), τα δίκτυα παρόχων υπηρεσιών διαδικτύου (ISPs) και τα κέντρα δεδομένων. Κάθε PoP μπορεί να περιλαμβάνει πολλούς Edge Servers.

Οι Edge Servers μπορούν επίσης να συνεργάζονται μεταξύ τους εξυπηρετώντας ο ένας τα αιτήματα του άλλου. Αυτή η συνεργασία δημιουργεί ένα δεύτερο επίπεδο Caching, καθώς ο τελευταίος Edge Server αποθηκεύει απαντήσεις από τους Origin Servers. Επιπλέον, οι Edge Servers χρησιμοποιούν μια ιεραρχική Caching μέθοδο, η οποία είναι βασισμένη στην δημοτικότητα του περιεχομένου. Τα πιο δημοφιλή περιεχόμενα αποθηκεύονται στη μνήμη RAM, ενώ τα λιγότερο δημοφιλή διατηρούνται στους σκληρούς δίσκους [5]. Ένας αλγόριθμος αντικατάστασης, όπως ο Least Recently Used (LRU) ή ο Least Frequently Used (LFU) διαχειρίζεται ποιο περιεχόμενο θα διατηρηθεί στην Cache [6].

Υπάρχουν τρία κύρια μοντέλα για τη διανομή περιεχομένου από τους Origin Servers στους Edge Servers [7][8]. Αρχικά, το **Push model**, στο οποίο το περιεχόμενο διανέμεται εάν, το συγκεκριμένο request αναμένεται σε έναν Edge Server [9]. Δεύτερον, το **Pull model**, όπου ένας Edge Server ανακτά το περιεχόμενο μόνο όταν λάβει σχετικό αίτημα από τον τελικό χρήστη. Το τελευταίο μοντέλο είναι το **Hybrid Push-Pull model**, το οποίο προσαρμόζεται δυναμικά στις μεταβαλλόμενες απαιτήσεις των χρηστών, διανέμοντας ορισμένα περιεχόμενα προληπτικά (Push) και ανακτώντας άλλα κατόπιν αιτήματος (Pull) [10].

Οι Edge Servers χρησιμοποιούν Web Caching Proxies για την υλοποίηση του Caching. Τα Caching Proxies μπορούν εύκολα να αποθηκεύσουν στατικό περιεχόμενο για να εξυπηρετήσουν μελλοντικά αιτήματα, καθώς το στατικό περιεχόμενο δεν αλλάζει με την πάροδο του χρόνου. Αντίθετα, το Caching δυναμικού περιεχομένου είναι πιο περίπλοκο. Για παράδειγμα, το Edge Side Includes (ESI) είναι μια γλώσσα σήμανσης που επιτρέπει τον καθορισμό των δυναμικών τμημάτων ενός web περιεχομένου, δίνοντας τη δυνατότητα σε ένα Caching Proxy να ανακτήσει μόνο τα δυναμικά τμήματα (π.χ. τα τελευταία νέα σε μια ιστοσελίδα μίας εταιρείας, ενώ διατηρεί στη μνήμη τα στατικά τμήματα (π.χ. το λογότυπο της εταιρείας). Επιπλέον, οι Edge Servers μπορούν να εκτελούν Scripts για τη δημιουργία δυναμικού περιεχομένου με βάση διάφορα γεγονότα και εισόδους, όπως την ώρα της ημέρας, τον τύπο της συσκευής και την τοποθεσία του τελικού χρήστη.

**Request Routing**: Ο request routing μηχανισμός παρακολουθεί την κατάσταση του δικτύου, το φορτίο στους Edge Servers και διανέμει τα αιτήματα μεταξύ τους βάσει των δεδομένων που συλλέγει [4]. Η δρομολόγηση ενός αιτήματος βασίζεται σε διάφορες μετρήσεις όπως η απόσταση από τον τελικό χρήστη, ο αριθμός των hops, η καθυστέρηση και ο φόρτος του διακομιστή[6].

Οι βασικές τεχνικές Request Routing μπορούν να διαχωριστούν σε 4 βασικές κατηγορίες [6]:

- DNS based Routing:
  Με το DNS based Routing, ένας τελικός χρήστης στέλνει ένα DNS request για το domain (π.χ. youtube.com) στον τοπικό Name Server του. Ο τοπικός Name Server προωθεί το αίτημα στον Authoritative Name Server του CDN, ο οποίος απαντά με τη διεύθυνση IP ενός Edge Server. Οι Authoritative Name Servers του CDN εκτελούν επίσης Load Balancing, διαχειριζόμενοι τα αιτήματα για το ίδιο domain, ανακατευθύνοντάς τα σε διαφορετικές διευθύνσεις IP των Edge Servers.

- Anycast Routing:
  Η Anycast Routing απλοποιεί το Request Routing αναθέτοντας τη δρομολόγηση στο ίδιο το διαδίκτυο. Στην Anycast Routing, ο Authoritative Name Server του CDN επιστρέφει επίσης μια διεύθυνση IP. Η διαφορά σε σχέση με τη DNS-based Routing είναι ότι πολλοί Edge Servers χρησιμοποιούν την ίδια διεύθυνση IP, ενώ το Border Gateway Protocol (BGP) δρομολογεί το αίτημα προς τον πλησιέστερο Edge Server. Συγκεκριμένα, πολλοί Edge Servers σε μια συγκεκριμένη γεωγραφική περιοχή ανακοινώνουν την ίδια IP διεύθυνση, και το BGP επιλέγει τη συντομότερη διαδρομή μέσω αυτόνομων συστημάτων (AS) για να φτάσει στον κοντινότερο Edge Server.

  Για παράδειγμα, το Open Connect , το CDN του Netflix, χρησιμοποιεί BGP Routing. Το Open Connect περιλαμβάνει μια σειρά από ειδικά σχεδιασμένους Edge Servers, γνωστούς ως Open Connect Appliances (OCAs), για τη διανομή περιεχομένου βίντεο. Το Open Connect αναπτύσσει τα OCAs σε δίκτυα ISP και σημεία ανταλλαγής διαδικτυακής κίνησης (Internet Exchange Points) και χρησιμοποιεί το Multi Exit Discriminator (MED) για να δώσει προτεραιότητα στα OCAs έναντι εναλλακτικών BGP διαδρομών. Αυτό επιτρέπει στο Netflix να τοπικοποιεί την κίνησή της όσο το δυνατόν πιο κοντά στους τελικούς χρήστες, ελαχιστοποιώντας τις αποστάσεις του δικτύου και τις γεωγραφικές αποστάσεις για την παράδοση του περιεχομένου.

- Application Layer Routing:
  Το Application Layer Request Routing βασίζεται στο πρωτόκολλο HTTP και μπορεί να κατευθύνει αιτήματα με ακρίβεια σε επίπεδο αντικειμένων περιεχομένου. Χρησιμοποιώντας URL rewriting, οι αρχικές διευθύνσεις URL των ιστοσελίδων αντικαθίστανται με υποτομείς του CDN, οι οποίοι κάνουν resolve σε Edge Servers του CDN. Για παράδειγμα, ο ιδιοκτήτης του ονόματος τομέα «ww.test.com» μπορεί να δημοσιεύσει το περιεχόμενο μέσω του «www.test.com.cdn.net», το οποίο ανήκει στο CDN.

- Ένας συνδυασμός των παραπάνω:
  Τα CDNs μπορούν να συνδυάσουν τις παραπάνω τεχνικές για να βελτιώσουν την ακρίβεια και την απόδοση του Request Routing. Για παράδειγμα, το YouTube, η Google, η Akamai και η Microsoft χρησιμοποιούν συνδυασμό DNS-based και Application Layer Redirection. Από την άλλη, το Bing και το LinkedIn συνδυάζουν τη DNS-based με την Anycast Routing.

**Origin Server:** Οι Origin Servers φιλοξενούν το αρχικό περιεχόμενο, όπως τις ιστοσελίδες ενός ιστότοπου. Έναν Origin Server μπορεί να διαχειριστεί είτε ο ιδιοκτήτης του περιεχομένου είτε ο πάροχος του CDN [4]. Ο ιδιοκτήτης του περιεχομένου μπορεί να αποθηκεύσει το περιεχόμενο είτε τοπικά είτε σε ένα Cloud.

Οι Origin Servers συνήθως χρησιμοποιούν Web Servers, όπως το NGINX και το Microsoft IIS, για τη φιλοξενία και την εξυπηρέτηση του web περιεχομένου. Ακόμα και με τη χρήση υπηρεσιών CDN, οι Origin Servers συνεχίζουν να εξυπηρετούν τα περισσότερα αιτήματα για δυναμικό web περιεχόμενο (π.χ. κοινωνικά δίκτυα και προσωπικές ιστοσελίδες). Αυτό συμβαίνει επειδή το δυναμικό περιεχόμενο δημιουργείται για κάθε request και βασίζεται σε δεδομένα που ο ιδιοκτήτης του περιεχομένου δεν μπορεί να μοιραστεί με το CDN (π.χ. πληροφορίες των τελικών χρηστών)[6].

## 1.5 Βασικοί Στόχοι του Content Delivery Network (CDN)

Το Content Delivery Network (CDN) αποτελεί βασικό εργαλείο για τη βελτίωση της εμπειρίας των τελικών χρηστών κατά την διανομή ψηφιακού περιεχομένου, ενώ παράλληλα επιτρέπει την πιο αποτελεσματική αξιοποίηση των πόρων του δικτύου. Οι βασικοί στόχοι ενός CDN επικεντρώνονται στη βελτιστοποίηση της ταχύτητας, της απόδοσης, της ασφάλειας και της αξιοπιστίας του διαδικτύου [12].

**Στόχος #1: Μείωση της καθυστέρησης:**
Ένας από τους κύριους στόχους ενός CDN είναι η ελαχιστοποίηση του χρόνου καθυστέρησης που απαιτείται για τη φόρτωση περιεχομένου. Αυτό επιτυγχάνεται μέσω Caching του περιεχομένου στους Edge Servers που βρίσκονται γεωγραφικά κοντά στους τελικούς χρήστες, μειώνοντας τη φυσική απόσταση που πρέπει να διανύσουν τα δεδομένα. Ως αποτέλεσμα, οι χρόνοι απόκρισης βελτιώνονται, προσφέροντας μια ταχύτερη και πιο ομαλή εμπειρία περιήγησης.

**Στόχος #2: Βελτίωση της απόδοσης:**
Τα CDN βελτιώνουν την απόδοση παρέχοντας άμεση και γρήγορη πρόσβαση στο περιεχόμενο. Με τη διανομή προσωρινά αποθηκευμένων αντιγράφων δεδομένων σε διάφορες τοποθεσίες παγκοσμίως, οι χρήστες μπορούν να έχουν πρόσβαση στο περιεχόμενο

από τον πλησιέστερο διακομιστή. Αυτό μειώνει τους χρόνους φόρτωσης ιστοσελίδων, αυξάνει την εμπλοκή των χρηστών και βελτιστοποιεί τη συνολική εμπειρία χρήσης.

**Στόχος #3: Αύξηση της διαθεσιμότητας:**
Τα CDN διασφαλίζουν τη διαθεσιμότητα των διαδικτυακών υπηρεσιών, ακόμη και σε περιόδους υψηλής ζήτησης ή σε περιπτώσεις αστοχίας διακομιστών. Εάν ένας διακομιστής αποτύχει, το CDN ανακατευθύνει αυτόματα την κίνηση στο πλησιέστερο Edge Server, αποτρέποντας έτσι τη διακοπή λειτουργίας. Επιπλέον, η αποθήκευση προσωρινών δεδομένων σε διάφορες τοποθεσίες επιτρέπει τη συνέχιση της παροχής υπηρεσιών ακόμη και σε περιπτώσεις βλάβης του Origin Server.

**Στόχος #4: Αποφόρτιση των Origin Servers (Load Offloading):**
Τα CDN μειώνουν το φορτίο στους Origin Servers, καθώς τα αιτήματα των χρηστών εξυπηρετούνται από Edge Servers που έχουν κρατήσει στην Cache τους το περιεχόμενο. Έτσι, αποφεύγεται η υπερφόρτωση των κεντρικών υποδομών, διασφαλίζοντας την ομαλή και γρήγορη παροχή περιεχομένου σε μεγάλους όγκους επισκεψιμότητας.

**Στόχος #5: Κλιμάκωση(Scalability):**
Τα σύγχρονα CDN προσφέρουν υψηλή κλιμάκωση, διαχειριζόμενα τις αυξομειώσεις της εισερχόμενης κίνησης μέσω της προσθήκης διακομιστών Cloud On-Demand. Αυτό επιτρέπει στις επιχειρήσεις να διαχειρίζονται αιφνίδιες αυξήσεις επισκεψιμότητας, όπως κατά τη διάρκεια μεγάλων εκδηλώσεων ή προωθητικών ενεργειών, χωρίς να επηρεάζεται η απόδοση του δικτύου.

**Στόχος #6: Ασφάλεια:**
Η ασφάλεια αποτελεί έναν από τους σημαντικότερους στόχους ενός CDN, καθώς προστατεύει τα διαδικτυακά δεδομένα και τις εφαρμογές από διάφορες απειλές. Τα CDN ενσωματώνουν προηγμένες λειτουργίες ασφαλείας, όπως:

- Web Application Firewalls (WAF) για την προστασία από κακόβουλες επιθέσεις,
- Intrusion Detection Systems (IDS) και Intrusion Prevention Systems (IPS) για την αποτροπή μη εξουσιοδοτημένης πρόσβασης,
- DDoS mitigation, το οποίο αποτρέπει επιθέσεις άρνησης υπηρεσίας, αξιοποιώντας την υπολογιστική ισχύ των διακομιστών αιχμής του CDN.

**Στόχος #7: Μείωση του κόστους:**
Τα CDN βοηθούν στη μείωση του κόστους, ελαχιστοποιώντας την ανάγκη για μεταφορά δεδομένων σε μεγάλες αποστάσεις και μειώνοντας την πίεση στις κεντρικές υποδομές. Αυτό οδηγεί σε εξοικονόμηση κόστους τόσο σε επίπεδο υποδομής όσο και σε κόστος εύρους ζώνης ενώ παράλληλα αυξάνεται η απόδοση των εφαρμογών.

**Στόχος #8: Βελτίωση της ικανοποίησης των πελατών:**
Με την παροχή γρήγορης και αξιόπιστης πρόσβασης στο περιεχόμενο, τα CDN συμβάλλουν στη βελτίωση της ικανοποίησης των πελατών. Οι χρήστες μπορούν να απολαμβάνουν ταχύτερες και πιο ομαλές εμπειρίες περιήγησης, κάτι που οδηγεί σε αυξημένη αφοσίωση και παραμονή στον ιστότοπο.

## 1.6 Βασικοί Τύποι Content Delivery Network (CDN)

Τα CDN μπορούν να ταξινομηθούν ποικιλοτρόπως με βάση τα κάτωθι κριτήρια:

- η αρχιτεκτονική τους
- η λειτουργικότητα τους

Συγκεκριμένα, οι βασικότεροι τύποι των CDNs είναι οι κάτωθι [4]:

**Δημόσια CDNs (Public CDNs):** κάθε CDN το οποίο είναι προσβάσιμο σε όλους στο διαδίκτυο ονομάζεται Δημόσιο CDN (Public CDN). Τα συγκεκριμένα CDN χρησιμοποιούνται για την ταχεία και αποτελεσματική παροχή περιεχομένου όπως εικόνες, βίντεο και άλλα στατικά αρχεία στους χρήστες. Συνήθως αποτελούνται από ένα μεγάλο παγκόσμιο δίκτυο διακομιστών. Τα βασικότερα παραδείγματα Δημόσιων CDNs [4]: Akamai, Cloudflare, Amazon CloudFront.

**Ιδιωτικά CDNs (Private CDNs):** ένα CDN το οποίο χρησιμοποιείται αποκλειστικά από μία εταιρεία ή έναν οργανισμό καλείται Ιδιωτικό CDN (Private CDN). Ο συγκεκριμένος τύπος CDN χρησιμοποιείται για την διανομή περιεχομένου σε εσωτερικούς χρήστες ή πελάτες και συνήθως εγκαθίσταται σε ένα ιδιωτικό Cloud ή στο εσωτερικό της υποδομής του ίδιου του οργανισμού. Τα Ιδιωτικά CDN (Private CDNs) παρέχουν περισσότερο έλεγχο στην διανομή περιεχόμενου ενώ υπάρχει δυνατότητα προσαρμογής ώστε να καλύπτουν συγκεκριμένες ανάγκες απόδοσης και ασφάλειας. Τα βασικότερα παραδείγματα των Ιδιωτικών CDNs: Google Cloud CDN, Netflix Open Connect.

**Peer-to-Peer (P2P) CDNs:** ο συγκεκριμένος τύπος CDN κάνει χρήση της τεχνολογίας peer-to-peer για την διανομή περιεχομένου μεταξύ χρηστών, μειώνοντας με αυτόν τον τρόπο την εξάρτηση από κεντρικούς διακομιστές. Τα βασικότερα παραδείγματα των P2P CDNs: BitTorrent, webTorrent.

**Υβριδικά CDNs (Hybrid CDNs):** ένα υβριδικό CDN συνδυάζει στοιχεία δημόσιων και ιδιωτικών CDNs. Σε ένα υβριδικό περιβάλλον, ορισμένο περιεχόμενο διανέμεται μέσω ενός δημοσίου CDN, ενώ άλλο περιεχόμενο διανέμεται κάνοντας χρήση ενός ιδιωτικού CDN. Αυτή η προσέγγιση επιτρέπει στους οργανισμούς να βελτιστοποιούν την διανομή περιεχομένου βάσει παραγόντων όπως το κόστος, η απόδοση και οι απαιτήσεις ασφάλειας. Το βασικότερο παράδειγμα ενός Hybrid CDN: Microsoft Azure CDN.

**Push CDNs:** σε ένα Push CDN, το περιεχόμενο προωθείται στους διακομιστές του CDN προτού χρειαστεί. Αυτό μπορεί να βελτιώσει την απόδοση, διασφαλίζοντας ότι το περιεχόμενο θα είναι διαθέσιμο κοντά στους τελικούς χρήστες όταν αυτοί το ζητήσουν. Τα Push CDN χρησιμοποιούνται συχνά για την προσωρινή αποθήκευση μεγάλων αρχείων ή περιεχομένου που δεν ενημερώνεται συχνά. Τα βασικότερα παραδείγματα των Push CDNs: KeyCDN, CDN77.

**Pull CDN:** σε ένα Pull CDN, το περιεχόμενο ζητείται ή τραβιέται από τους διακομιστές του CDN αποκλειστικά και μόνο όταν αυτό είναι απαραίτητο. Αυτή η προσέγγιση είναι πιο αποδοτική για την διανομή περιεχόμενου που δεν ενημερώνεται συχνά ή δημιουργείται δυναμικά. Τα Pull CDNs χρησιμοποιούνται συχνά για την διανομή δυναμικού περιεχομένου όπως ιστοσελίδες ή απαντήσεις API. Τα βασικότερα παραδείγματα των Pull CDNs: Amazon CloudFront, Cloudflare.

**Hybrid Push-Pull CDN:** ένα Υβριδικό Push-Pull μοντέλο προσαρμόζεται δυναμικά στις μεταβαλλόμενες απαιτήσεις των τελικών χρηστών, προωθώντας (pushing) ορισμένα περιεχόμενα εκ των προτέρων και ανακτώντας (pulling) άλλα περιεχόμενα αντιδραστικά. Το συγκεκριμένο μοντέλο συνδυάζει τα χαρακτηριστικά των δυο προηγούμενων τύπων CDN, Push και Pull CDNs, εξισορροπώντας με αυτόν τον τρόπο την αποδοτικότητα και την ευελιξία. Τα βασικότερα παραδείγματα Hybrid Push-Pull CDNs: Microsoft Azure CDN, Akamai Intelligent Platform.

## 1.7 Αναγνώριση του Content Delivery Network (CDN)

Για την αναγνώριση του CDN που βρίσκεται πίσω από ένα hostname, έχουν προταθεί διάφορες μέθοδοι, ωστόσο μέχρι σήμερα είναι ελάχιστες οι μελέτες οι οποίες να εστιάζουν στην ανίχνευση ρυθμίσεων προστασίας των CDNs ή στην διάκριση μεταξύ ιστοτόπων που χρησιμοποιούν δωρεάν ή επί πληρωμή CDN.

**Μέθοδος #1: MultiFinder - Αναγνώριση μέσω DNS και HTTP-Based Μετρήσεων [15]**
Η MultiFinder μέθοδος αναγνωρίζει τα CDNs, συμπεριλαμβανομένων των περιπτώσεων όπου ένας ιστότοπος χρησιμοποιεί multiple-CDN deployments. Η μέθοδος αυτή βασίζεται σε συνδυασμό DNS και HTTP-based μετρήσεων.

Τα βασικά στοιχεία του MultiFinder περιλαμβάνουν:

- Αποστολή DNS queries με EDNS0 Client Subnet prefixes σε open DNS resolvers.
- Ανάλυση των CNAME records, των HTTP(S) headers, των TLS certificates και των πληροφοριών RDAP (ipwhois).

**Μέθοδος #2: Αναγνώριση CDNs μέσω IP Mapping και Regular Expressions [20] [16]**
Μια άλλη μέθοδος για την αναγνώριση των CDNs που βρίσκονται πίσω από ένα hostname είναι η αντιστοίχιση των IPs σε AS (Autonomous Systems) και στη συνέχεια η υλοποίηση regular expression searches στο πεδίο "name" της AS2Org database για τον εντοπισμό του CDN. Αυτή η μέθοδος χρησιμοποιείται ευρέως σε ακαδημαϊκές μελέτες.

**Μέθοδος #3: Αναγνώριση CDNs μέσω Transport Layer Security (TLS) Fingerprinting**
Η συγκεκριμένη μέθοδος είναι μια active measurement-based methodology για τη συλλογή Transport Layer Security (TLS) metadata από διακομιστές και την αξιοποίησή τους για fingerprinting. Τα fingerprints καταγράφουν τη χαρακτηριστική συμπεριφορά του TLS stack, η οποία επηρεάζεται κυρίως από την υλοποίηση, τη διαμόρφωση και την υποστήριξη hardware του διακομιστή. Χρησιμοποιώντας μια empirical optimization strategy, οι ερευνητές ανέπτυξαν 10 general-purpose Client Hellos ως scanning probes, δημιουργώντας μια μεγάλη βάση δεδομένων με TLS configurations που χρησιμοποιούνται για την ταξινόμηση διακομιστών. Αυτή η προσέγγιση είναι ιδιαίτερα χρήσιμη για την αναγνώριση των CDNs, καθώς αυτά παρέχουν μεγάλο αριθμό επαληθεύσιμων δειγμάτων δεδομένων. Στη μελέτη τους, οι ερευνητές συνδύασαν Autonomous System (AS), HTTP headers και x509 certificate data για την δημιουργία μίας ground truth. Στη συνέχεια, ένας διακομιστής ταξινομήθηκε ως μέρος ενός CDN εάν είχε ένα fingerprint που είχε ήδη παρατηρηθεί. Αυτό το μοντέλο ήταν ιδιαίτερα αξιόπιστο, καθώς τα fingerprints δεν επικαλύπτονταν [17].

**Μέθοδος #4: Ανίχνευση CDNs μέσω Feature Extraction**
Η συγκεκριμένη μέθοδος για την αναγνώριση των CDN μέσω feature extraction περιλαμβάνει τα κάτωθι [12]:

- Reverse DNS lookups
- Ανάλυση HTTP headers
- Εξέταση CNAME records
- TLS certificate analysis

Η συγκεκριμένη μέθοδος είχε χρησιμοποιηθεί και σε προηγούμενες μελέτες [18],[19]. Λόγω των συνεχών αλλαγών στις επεκτάσεις των πιστοποιητικών, τις πολιτικές απορρήτου και τις ανησυχίες για την ασφάλεια, έγιναν τροποποιήσεις και ενημερώσεις στα σύνολα χαρακτηριστικών που χρησιμοποιήθηκαν. Οι ερευνητές ανέπτυξαν Python scripts για την εξαγωγή χαρακτηριστικών από ιστότοπους που περιλαμβάνονται στη λίστα Alexa Top 1 Million, αποθηκεύοντας τα δεδομένα για περαιτέρω ανάλυση. Γνωστά χαρακτηριστικά CDNs χρησιμοποιήθηκαν για την ταυτοποίηση τους, ενώ άγνωστα CDNs αναγνωρίστηκαν μέσω feature clustering και χειροκίνητης επαλήθευσης. Διάφορες τεχνικές, όπως reverse DNS queries και εξέταση των HTTP headers και των CNAME records, χρησιμοποιήθηκαν για την αναγνώριση της παρουσίας ενός CDN. Αξίζει να σημειώθει πώς, η χρήση TLS certificates δεν κρίθηκε τόσο αποτελεσματική, καθώς η ευρεία υιοθέτηση του Server Name Indication (SNI)

από τους περισσότερους CDN providers έχει περιορίσει τη χρησιμότητα των πιστοποιητικών στη front-end ανίχνευση.

### 1.7.1 Αναγνώριση των Κορυφαίων CDNs

Ο παρακάτω πίνακας παρουσιάζει την κατάταξη των παρόχων CDN με βάση τη χρήση τους στους Top 1 Million ιστότοπους παγκοσμίως [21].

Top In Verified CDN Usage Distribution in the Top 1 Million Sites

| Technology | Websites | % |
|---|---|---|
| Cloudflare CDN | 406,162 | 40.62 |
| Amazon CloudFront | 115,506 | 11.55 |
| Amazon S3 CDN | 42,941 | 4.29 |
| Google Cloud CDN | 41,921 | 4.19 |
| Akamai Edge | 25,447 | 2.54 |
| Microsoft Azure Verified CDN | 14,972 | 1.5 |
| Akamai EdgeWorkers | 11,694 | 1.17 |
| BunnyCDN | 6,003 | 0.6 |

*Figure 4: Top in Verified CDN Usage Distribution in the Top 1 Million Sites - builtWith*

Στην Ελλάδα η κατανομή είναι η ακόλουθη με την Cloudflare να καταλαμβάνει την πρωτιά ξεπερνώντας το Google Cloud CDN κατά 70 ποσοστιαίες μονάδες περίπου [22].

Top In Verified CDN Usage Distribution in Greece

| Technology | Websites | % |
|---|---|---|
| Cloudflare CDN | 58,307 * | 80.52 |
| Google Cloud CDN | 8,396 | 11.6 |
| Amazon S3 CDN | 2,569 | 3.55 |
| Amazon CloudFront | 1,959 | 2.71 |
| Akamai Edge | 394 | 0.54 |
| Hummingbird Cache | 263 | 0.36 |
| BunnyCDN | 180 | 0.25 |

*Figure 5:Verified CDN Usage Distribution in Greece*

Όπως αναφέρθηκε και παραπάνω, οι πιο δημοφιλείς μέθοδοι αναγνώρισης των CDN περιλαμβάνουν την ανάλυση των DNS records (CNAME, PTR κ.λπ.), των HTTP Headers και την αντιστοίχιση IP addresses με Autonomous System Numbers (ASNs). Ορισμένες έρευνες έχουν επίσης χρησιμοποιήσει TLS Certificates και TLS Fingerprint Data, ωστόσο, αυτές οι μέθοδοι παρουσιάζουν συγκεκριμένους περιορισμούς και ως εκ τούτου, εφαρμόζονται λιγότερο συχνά.

Βασισμένοι στις μεθόδους αναγνώρισης που έχουν χρησιμοποιηθεί και σε προηγούμενες έρευνες, διαπιστώθηκε πώς οι κάτωθι βελτιωμένες μέθοδοι παρέχουν αποτελέσματα μεγαλύτερης ακρίβειας και εξαλείφουν τους περιορισμούς των παραπάνω μεθόδων.

**CNAME:**
Ορισμένοι CDN providers χρησιμοποιούν CNAME records για να ανακατευθύνουν αιτήματα από τον Origin Server σε ένα Edge Hostname που έχει καθοριστεί από το CDN. Για παράδειγμα, ιστότοποι που χρησιμοποιούν Akamai διαθέτουν CNAME records που καταλήγουν σε “edgekey.net".

**ASN:**
Οι Edge Servers που χρησιμοποιούνται από τους CDN providers βρίσκονται συνήθως εντός των αντίστοιχων Autonomous Systems (AS) τους. Ως αποτέλεσμα, τα Edge Hostnames που χρησιμοποιούν τα CDN διαθέτουν IP addresses που σχετίζονται με τα AS Numbers των CDN παρόχων. Για παράδειγμα, ιστότοποι που χρησιμοποιούν Akamai συχνά έχουν IP addresses που σχετίζονται με τα ASN "16625" ή "20940".

**PTR:**
Τα PTR records παρέχουν πληροφορίες για το Domain που αντιστοιχεί σε μια IP διεύθυνση. Ορισμένοι CDN πάροχοι επιλέγουν να αποκαλύπτουν τα Reverse Domain Name Resolution Records για να προσδιορίσουν τον κάτοχο της IP. Για παράδειγμα, ιστότοποι που χρησιμοποιούν Amazon CloudFront διαθέτουν συχνά Reverse Resolution Records που καταλήγουν σε "cloudfront.net".

**HTTP Headers:**
Πολλά CDN επιστρέφουν μοναδικά HTTP headers στις απαντήσεις τους, επιτρέποντας την εύκολη αναγνώριση της παρουσίας τους. Για παράδειγμα, ιστότοποι που χρησιμοποιούν Cloudflare περιλαμβάνουν συχνά headers όπως "Server: Cloudflare".

| CDN | CNAME | ASN | PTR | HEADERS |
|---|---|---|---|---|
| **Cloudflare** | cdn.cloudflare.net | 13335, 209242 | / | Server: Cloudflare CF-Cache-Status CF-RAY |
| **Amazon CloudFront** | cloudfront.net | / | cloudfront.net | Server: CloudFront Via: CloudFront x-amz-cf-id x-amz-cf-pop |
| **Akamai** | edgekey.net edgesuite.net akamaized.net akamaihd.net | 16625, 20940 | akamaitechnologies.com | Server: AkamaiGHost X-Akamai-Transformed X-Akam-SW-Version Akamai-GRN X-Akamai-Request-ID Akamai-Mon-Iucid-Del Akamai-True-TTL |

| | | | | |
|---|---|---|---|---|
| **Google Cloud CDN** | / | / | googleusercontent.com | / |
| **Microsoft Azure CDN** | azureedge.net azurefd.net | / | / | X-Azure-Ref x-fd-int-roxy-purgeid X-Azure-Ref-OriginShield |
| **Fastly** | fastly.net | 54113 | / | X-Fastly-Request-ID Fastly-Restarts Fastly-Client-IP fastly-request-id Fastly-Drupal-Html |

*Table 1:CDN Identifiers*

### 1.7.2 Αναγνώριση των Βασικών Χαρακτηριστικών των CDN

Τα σημαντικότερα στοιχεία για την αναγνώριση των CDN χαρακτηριστικών που χρησιμοποιούνται από ιστοτόπους, με βάση τόσο τις τεχνικές προδιαγραφές του εκάστοτε παρόχου όσο και τις διαθέσιμες πληροφορίες τεκμηρίωσης, είναι τα εξής [14]:

**CNAME:**
Τα CNAME records μπορούν να σηματοδοτήσουν τα CDN χαρακτηριστικά που χρησιμοποιεί ένας ιστότοπος. Για παράδειγμα ιστότοποι με CNAME records που καταλήγουν σε "elb.amazonaws.com" υποδηλώνουν τη χρήση του Amazon Classic Load Balancer.

**PTR:**
Τα PTR Records μπορούν επίσης να αποκαλύψουν συγκεκριμένα CDN χαρακτηριστικά που χρησιμοποιεί ένας ιστότοπος. Για παράδειγμα, ιστότοποι με Reverse Domain Name Resolution Results που καταλήγουν σε "awsglobalaccelerator.com" υποδεικνύουν τη χρήση του Amazon Global Accelerator.

**Autonomous System Description/Number (ASD/ASN):**
Ορισμένα χαρακτηριστικά των CDN διαθέτουν συγκεκριμένα ASD/ASN στοιχεία. Για παράδειγμα, οι IP διευθύνσεις που χρησιμοποιούνται από το Cloudflare Spectrum αντιστοιχούν στο AS CLOUDFLARESPECTRUM.

**HTTP Response Headers:**
Τα HTTP Response Headers μπορούν επίσης να προσφέρουν ενδείξεις για τις επί πληρωμή CDN υπηρεσίες που χρησιμοποιεί ένας ιστότοπος. Για παράδειγμα, το header "X-Azure-Ref-OriginShield" υποδηλώνει τη χρήση του Azure Origin Shield.

**Name Server Records (NS):**
Τα NS Records δείχνουν τους Authoritative Name Servers που χρησιμοποιούνται από ένα Domain. Πολλοί CDN πάροχοι προσφέρουν επί πληρωμή DNS υπηρεσίες. Για παράδειγμα,

ιστότοποι που χρησιμοποιούν Akamai Edge DNS διαθέτουν συχνά NS records που περιέχουν το "akam.net".

**TLS Certificate Issuer (CERT-issuer):**
Πολλοί CDN providers περιορίζουν τις Certificate Authorities (CAs) από τις οποίες ένας ιστότοπος μπορεί να λάβει TLS certificates. Για παράδειγμα, μόνο οι επί πληρωμή χρήστες του Fastly μπορούν να χρησιμοποιούν CAs διαφορετικές από το Let's Encrypt και το Certainly.

**TLS Certificate Subject Alternative Name – SAN (CERT-san):**
Το SAN προσδιορίζει τα Domains, IP addresses και Email Addresses που καλύπτονται από ένα TLS certificate. Πολλοί CDN πάροχοι περιορίζουν το scope των TLS certificates, αλλά προσφέρουν επί πληρωμή προηγμένα certificates. Για παράδειγμα, το Amazon CloudFront παρέχει επι πληρωμή certificates ανά IP.

## 1.8 Akamai Content Delivery Network (CDN)

Αποτελούμενη από περισσότερους από 365.000 διακομιστές που βρίσκονται σε σχεδόν 1.500 δίκτυα σε 135 χώρες παγκοσμίως, η πλατφόρμα της Akamai διαχειρίζεται καθημερινά εκατοντάδες δισεκατομμύρια διαδικτυακών συναλλαγών, βοηθώντας χιλιάδες επιχειρήσεις να βελτιώσουν την απόδοση και την αξιοπιστία των διαδικτυακών τους εφαρμογών [4].

### 1.8.1 Λειτουργικά Στοιχεία της Akamai

Το δίκτυο της Akamai είναι ένα εξαιρετικά μεγάλο κατανεμημένο σύστημα, το οποίο αποτελείται από δεκάδες χιλιάδες διακομιστές εγκατεστημένους παγκοσμίως. Αυτοί οι διακομιστές χρησιμοποιούν προηγμένους αλγόριθμους για να επιτρέψουν την διανομή εφαρμογών μεγάλης κλίμακας και υψηλής απόδοσης. Στην πραγματικότητα αποτελεί ένα σύνολο από επιμέρους δίκτυα διανομής, το καθένα προσαρμοσμένο σε διαφορετικούς τύπους περιεχομένου, όπως στατικό περιεχόμενο, πολυμέσα συνεχούς ροής ή δυναμικές εφαρμογές. Σε γενικές γραμμές, αυτά τα δίκτυα διανομής ακολουθούν παρόμοια αρχιτεκτονική ωστόσο η τεχνολογία και η υλοποίηση κάθε επιμέρους συστήματος μπορεί να διαφέρει, προκειμένου να ανταποκρίνεται καλύτερα στον συγκεκριμένο τύπο περιεχομένου, πολυμέσων ή εφαρμογών που εξυπηρετεί [4].

Τα βασικά συστατικά του Akamai CDN είναι τα ακόλουθα:

- Όταν ο χρήστης πληκτρολογεί ένα URL στον περιηγητή του, το domain name του URL μεταφράζεται από το Mapping System στη διεύθυνση IP ενός Edge Server, προκειμένου να εξυπηρετηθεί το περιεχόμενο. Για να αντιστοιχίσει τον χρήστη σε έναν διακομιστή, το Mapping System βασίζεται σε μεγάλες ποσότητες ιστορικών και τρεχόντων δεδομένων, τα οποία έχουν συλλεχθεί και επεξεργαστεί σχετικά με τις συνθήκες του παγκόσμιου δικτύου και των διακομιστών. Αυτά τα δεδομένα

χρησιμοποιούνται για την επιλογή ενός Edge Server που βρίσκεται κοντά στον τελικό χρήστη.

- Κάθε Edge Server αποτελεί μέρος της Edge Server Platform, μιας μεγάλης παγκόσμιας δομής διακομιστών που βρίσκονται σε χιλιάδες σημεία σε όλο τον κόσμο. Αυτοί οι διακομιστές είναι υπεύθυνοι για την επεξεργασία των αιτημάτων από κοντινούς χρήστες και την παροχή του ζητούμενου περιεχομένου.

- Για να ανταποκριθεί σε ένα αίτημα χρήστη, ένας Edge Server ενδέχεται να χρειαστεί να ζητήσει περιεχόμενο από έναν Origin Server. Για παράδειγμα, το δυναμικό περιεχόμενο μιας ιστοσελίδας που είναι εξατομικευμένο για κάθε χρήστη δεν μπορεί να αποθηκευτεί πλήρως στην Edge Platform και πρέπει να ανακτηθεί από τον Origin. Το Transport System χρησιμοποιείται για τη λήψη των απαιτούμενων δεδομένων με αξιόπιστο και αποδοτικό τρόπο. Γενικότερα, το Transport System είναι υπεύθυνο για τη μεταφορά δεδομένων και περιεχομένου μέσω του ευρύτερου Internet με υψηλή αξιοπιστία και απόδοση. Σε πολλές περιπτώσεις, το Transport System μπορεί επίσης να αποθηκεύσει προσωρινά στατικό περιεχόμενο.

- Το Communications and Control System χρησιμοποιείται για τη διάδοση πληροφοριών κατάστασης, μηνυμάτων ελέγχου και ενημερώσεων διαμόρφωσης με ανθεκτικότητα σε σφάλματα και έγκαιρο τρόπο.

- Το Data Collection and Analysis System είναι υπεύθυνο για τη συλλογή και επεξεργασία δεδομένων από διάφορες πηγές, όπως server logs, client logs, καθώς και πληροφορίες σχετικά με το δίκτυο και τους διακομιστές. Τα συλλεγμένα δεδομένα μπορούν να χρησιμοποιηθούν για παρακολούθηση, ειδοποιήσεις, ανάλυση, δημιουργία αναφορών και τιμολόγηση.

- Τέλος, το Management Portal επιτελεί δύο βασικές λειτουργίες. Πρώτον, παρέχει μια πλατφόρμα διαχείρισης διαμόρφωσης που επιτρέπει στον enterprise πελάτη να έχει λεπτομερή έλεγχο σχετικά με το πώς το περιεχόμενο και οι εφαρμογές του διανέμονται στον τελικό χρήστη. Αυτές οι ρυθμίσεις ενημερώνονται σε όλη την Edge Platform μέσω του Management Portal, χρησιμοποιώντας το Communications and Control System. Επιπλέον, το Management Portal παρέχει στις επιχειρήσεις ορατότητα σχετικά με τον τρόπο που οι χρήστες αλληλεπιδρούν με τις εφαρμογές και το περιεχόμενό τους, προσφέροντας αναφορές για τα δημογραφικά στοιχεία του κοινού και τις μετρήσεις κίνησης.

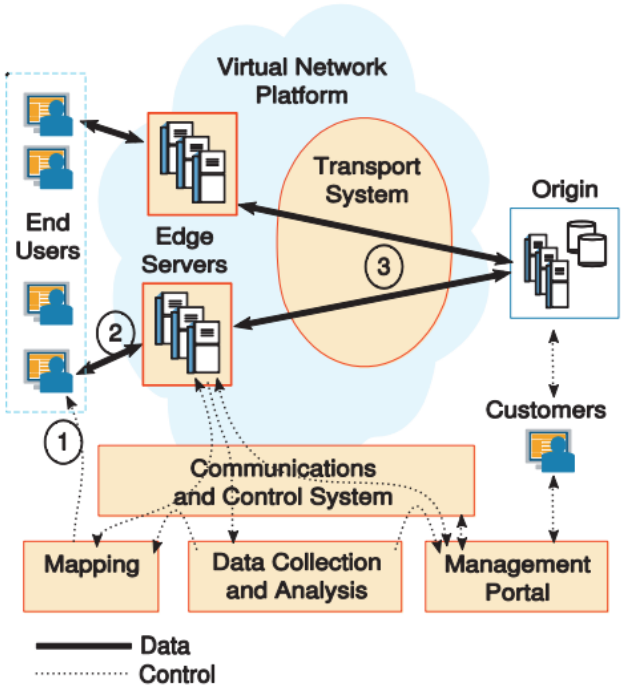


*Figure 6:Τα συστεμικά συστατικά του Akamai CDN - The Akamai Network: A Platform for High-Performance Internet Applications, E.Nygren, K.Sitamaran, J.Sun*

Αν και όλα τα delivery networks της Akamai ενσωματώνουν τα παραπάνω συστήματα, ο συγκεκριμένος σχεδιασμός του κάθε συστήματος επηρεάζεται από τις απαιτήσεις της εκάστοτε εφαρμογής. Για παράδειγμα, το Transport System ενός Application Delivery Network θα έχει διαφορετικές απαιτήσεις και αρχιτεκτονική σε σύγκριση με εκείνο ενός Content Delivery Network.

### 1.8.2 Βασικές Αρχές Συστημικού Σχεδιασμού στην Akamai

Η πολυπλοκότητα ενός παγκοσμίως κατανεμημένου CDN επιφέρει μια μοναδική σειρά προκλήσεων στην αρχιτεκτονική, τη λειτουργία και τη διαχείριση, ιδιαίτερα σε ένα περιβάλλον τόσο ετερογενές και απρόβλεπτο όπως το Διαδίκτυο. Για παράδειγμα, η διαχείριση του δικτύου και η συλλογή δεδομένων πρέπει να είναι επεκτάσιμες και γρήγορες σε χιλιάδες συστοιχίες διακομιστών, πολλές από τις οποίες βρίσκονται σε μη στελεχωμένα κέντρα δεδομένων τρίτων, ενώ οποιοσδήποτε αριθμός από αυτές μπορεί να είναι εκτός σύνδεσης ή να αντιμετωπίζει προβλήματα συνδεσιμότητας ανά πάσα στιγμή. Οι αλλαγές διαμόρφωσης και οι ενημερώσεις λογισμικού πρέπει να εφαρμόζονται στο δίκτυο με ασφαλή, γρήγορο και συνεπή τρόπο, χωρίς να διαταράσσεται η υπηρεσία, ενώ οι επιχειρήσεις πρέπει επίσης να διατηρούν ορατότητα και λεπτομερή έλεγχο του περιεχομένου τους σε ολόκληρη την κατανεμημένη πλατφόρμα.

Η βασικότερη παραδοχή που διέπει τις σχεδιαστικές επιλογές του Akamai CDN είναι ότι στην πραγματικότητα ένας σημαντικός αριθμός αποτυχιών (σε επίπεδο μηχανής, rack, συστοιχίας, συνδεσιμότητας ή δικτύου) είναι αναμενόμενος και συμβαίνει συνεχώς στο δίκτυο. Αν και αυτή η προσέγγιση δεν είναι τυπική στον σχεδιασμό συστημάτων, θεωρείται

φυσική στο πλαίσιο του Διαδικτύου. Αυτό σημαίνει ότι το Akamai CDN έχει σχεδιαστεί με τη φιλοσοφία ότι οι αποτυχίες είναι φυσιολογικές και το δίκτυο πρέπει να λειτουργεί ομαλά παρά την παρουσία τους, ενώ παρατηρείται μεγάλη προσπάθεια στον σχεδιασμό μηχανισμών ανάκαμψης από όλα τα είδη σφαλμάτων, συμπεριλαμβανομένων των ταυτόχρονων αποτυχιών [4].

Ακολουθούν οι βασικές αρχές σχεδιασμού της Akamai πλατφόρμας:

**Design for Reliability:** Λόγω της φύσης της δραστηριότητας της Akamai, ο στόχος είναι η επίτευξη σχεδόν 100% διαθεσιμότητας. Αυτό απαιτεί σημαντική προσπάθεια, δεδομένης της θεμελιώδους παραδοχής ότι τα συστατικά στοιχεία ενός συστήματος θα αποτυγχάνουν συχνά και με απρόβλεπτους τρόπους. Είναι απαραίτητο να διασφαλιστεί η πλήρης Redundancy των Components (χωρίς Single Points of Failure), να ενσωματωθούν πολλαπλά επίπεδα Fault Tolerance και να χρησιμοποιηθούν πρωτόκολλα όπως το PAXOS και μηχανισμοί Decentralized Leader Election, ώστε να αντιμετωπιστεί η πιθανότητα αποτυχιών.

**Design for Scalability:** Με περισσότερες από 365.000 μηχανές παγκοσμίως, όλα τα συστατικά στοιχεία της πλατφόρμας πρέπει να είναι εξαιρετικά επεκτάσιμα. Σε ένα βασικό επίπεδο, επεκτασιμότητα σημαίνει διαχείριση μεγαλύτερου όγκου κίνησης, περιεχομένου και πελάτων. Αυτό περιλαμβάνει επίσης τη διαχείριση ολοένα και μεγαλύτερων ποσοτήτων δεδομένων που πρέπει να συλλέγονται και να αναλύονται, καθώς και την ανάπτυξη των Communications, Control και Mapping Systems, τα οποία πρέπει να υποστηρίζουν έναν συνεχώς αυξανόμενο αριθμό κατανεμημένων μηχανών.

**Limit the Necessity for Human Management:** Σε πολύ μεγάλο βαθμό, το σύστημα έχει σχεδιαστεί ώστε να είναι αυτόνομο. Αυτό αποτελεί συνέπεια της φιλοσοφίας ότι οι αποτυχίες είναι συχνές και το σύστημα πρέπει να είναι σε θέση να λειτουργεί παρά την ύπαρξή τους. Επιπλέον, η αυτονομία είναι απαραίτητη για την επεκτασιμότητα, διαφορετικά το λειτουργικό κόστος ανθρώπινου δυναμικού θα γίνει υπερβολικά υψηλό. Συνεπώς, το σύστημα πρέπει να μπορεί να ανταποκρίνεται σε λάθη, να διαχειρίζεται μεταβολές σε φόρτο και χωρητικότητα, να αυτορυθμίζεται για βέλτιστη απόδοση και να αναπτύσσει με ασφάλεια Software και Configuration Updates με ελάχιστη ανθρώπινη παρέμβαση.

**Design for Performance:** Συνεχής προσπάθεια καταβάλλεται επίσης για τη βελτίωση της απόδοσης των κρίσιμων διαδρομών του συστήματος, όχι μόνο από την άποψη της βελτίωσης των End User Response Times, αλλά και για πολλούς άλλους δείκτες σε όλη την πλατφόρμα, όπως τα Cache Hit Rates και η Network Resource Utilization. Ένα επιπλέον όφελος αυτών των βελτιώσεων είναι η ενεργειακή απόδοση. Για παράδειγμα, οι βελτιστοποιήσεις σε Kernel και άλλο Software επιτρέπουν μεγαλύτερη χωρητικότητα και διαχείριση περισσότερης κίνησης με λιγότερες μηχανές.

### 1.8.3 Βασικά Συστατικά Στοιχεία της Akamai Πλατφόρμας

Η πλατφόρμα της Akamai επιτρέπει την παράδοση και ανάπτυξη εξαιρετικά επεκτάσιμων διαδικτυακών εφαρμογών. Το Σχήμα 7 παρουσιάζει μια αρχιτεκτονική επισκόπηση των βασικών συστατικών της πλατφόρμας. Ωστόσο, η λίστα αυτή δεν είναι εξαντλητική, καθώς η πλατφόρμα περιλαμβάνει επιπλέον υποσυστήματα και λειτουργίες που διασφαλίζουν την αποδοτική και ασφαλή λειτουργία του δικτύου. Στα επόμενα υποκεφάλαια, περιλαμβάνεται μία ανάλυση των βασικότερων δομικών συστημάτων της Akamai Πλατφόρμας, το Transport System και το Edge Server System.

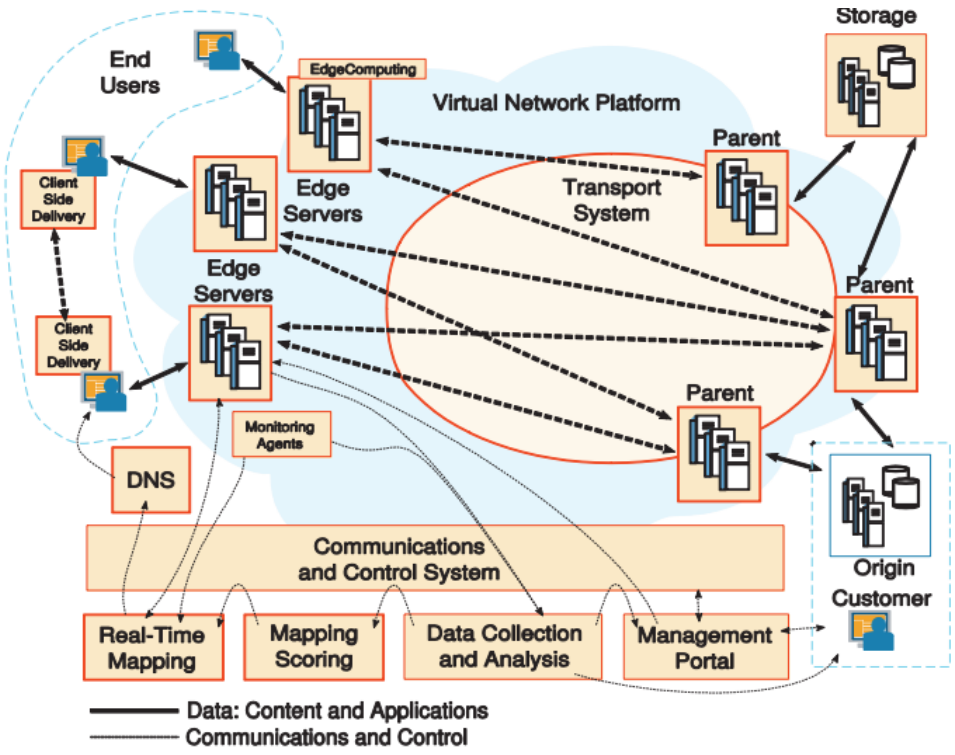


*Figure 7: Τα Βασικά Συστατικά Στοιχεία της Akamai Πλατφόρμας*

#### 1.8.3.1 Transport Σύστημα

Το Transport System αποτελεί θεμελιώδες στοιχείο της πλατφόρμας της Akamai, καθώς εξασφαλίζει την αξιόπιστη και αποδοτική μεταφορά δεδομένων από τους Origin Servers στους Edge Servers. Η λειτουργία του προσαρμόζεται ανάλογα με τον τύπο των δεδομένων που μεταφέρονται, με εξειδικευμένες προσεγγίσεις για web περιεχόμενο, streaming media και εφαρμογές [4].

**Διαχείριση web περιεχομένου και Streaming Media:**
Για τη διανομή **web περιεχομένου** και **streaming media**, το **Transport System** χρησιμοποιεί προηγμένες τεχνικές βελτιστοποίησης, όπως:

- Tiered Distribution: η συγκεκριμένη αρχιτεκτονική βελτιστοποιεί την διανομή περιεχομένου μέσω μιας πολυεπίπεδης ιεραρχίας διακομιστών. Όταν ένας Edge Server δεν διαθέτει το ζητούμενο περιεχόμενο στην Cache, δεν επικοινωνεί

απευθείας με τον Origin Server, αλλά αντλεί το περιεχόμενο από ένα πιο κοντινό Parent Cluster. Τα Parent Clusters λειτουργούν ως ενδιάμεσοι, αποτελώντας ισχυρά συνδεδεμένους κόμβους που μειώνουν το φορτίο στους Origin Servers, βελτιώνοντας έτσι την απόδοση, τη διαθεσιμότητα και την ταχύτητα διανομής του περιεχομένου στους τελικούς χρήστες.

- Overlay Network για Live Streaming: η συγκεκριμένη αρχιτεκτονική στοχεύει στη μείωση της συμφόρησης και των καθυστερήσεων κατά τη μετάδοση ζωντανού βίντεο. Η ροή αρχικά αποστέλλεται σε ένα Entrypoint Cluster, το οποίο τη διανέμει σε πολλαπλά Entrypoints, εξαλείφοντας έτσι μοναδικά σημεία αποτυχίας (single points of failure). Στη συνέχεια, οι Reflectors δημιουργούν πολλαπλά αντίγραφα της ροής, παρέχοντας εναλλακτικές διαδρομές μετάδοσης. Το σύστημα επιλέγει δυναμικά την καλύτερη διαδρομή για κάθε ροή και, όταν δεν υπάρχει διαθέσιμη διαδρομή υψηλής ποιότητας, συνδυάζει πολλαπλές εναλλακτικές για τη βελτίωση της απόδοσης.

**Διαχείριση Εφαρμογών:**
Για τη βελτίωση της ταχύτητας και αξιοπιστίας των εφαρμογών, η Akamai χρησιμοποιεί ένα υψηλής απόδοσης Overlay Network, το οποίο περιλαμβάνει τις ακόλουθες τεχνικές:

- Βελτιστοποίηση Διαδρομής (Route Optimization): Λόγω των περιορισμών του πρωτοκόλλου BGP στην επιλογή της βέλτιστης διαδρομής, η Akamai αξιοποιεί εναλλακτικές διαδρομές μέσω ενδιάμεσων διακομιστών για τη βελτιστοποίηση της δρομολόγησης. Συγκεκριμένα, το δίκτυό επιλέγει δυναμικά τις πιο αποδοτικές διαδρομές, βασιζόμενο σε τοπολογικά δεδομένα και μετρήσεις απόδοσης, επιτυγχάνοντας βελτίωση 30-50%, ιδιαίτερα σε περιοχές με περίπλοκες δικτυακές συνθήκες, όπως η Ασία.

- Μείωση Απώλειας Πακέτων (Packet Loss Reduction): Η Akamai χρησιμοποιεί πολλαπλές διαδρομές και τεχνικές διόρθωσης σφαλμάτων για να μειώσει την απώλεια πακέτων και την καθυστέρηση.

- Βελτιστοποιήσεις Πρωτοκόλλου Μεταφοράς (Transport Protocol Optimization): Για τις επικοινωνίες μεταξύ των Akamai servers, εφαρμόζονται βελτιστοποιήσεις στο TCP πχ. Persistent Connections, Smart Reconnections.

- Βελτιστοποιήσεις Εφαρμογών (Application Optimization): Τα βασικότερα παραδείγματα των βελτιστοποιήσεων που υλοποιούνται από την Akamai είναι το pre-fetching, η συμπίεση δεδομένων, το Edge Side Includes (ESI).

### 1.8.3.2 Edge Server Σύστημα

Το Edge Server System της Akamai αποτελεί ένα θεμελιώδες στοιχείο της πλατφόρμας, καθώς είναι υπεύθυνο για την επεξεργασία των αιτημάτων των χρηστών, την διανομή περιεχομένου, αλλά και τη λειτουργία ως ενδιάμεσος κόμβος στο Overlay Network.

Το συγκεκριμένο σύστημα αποτελείται από μεγάλο αριθμό διακομιστών που είναι κατανεμημένοι σε χιλιάδες τοποθεσίες παγκοσμίως, προσφέροντας υψηλή απόδοση, ευελιξία και δυνατότητες διαχείρισης περιεχομένου.

| **Βασικές Λειτουργίες Edge Server Συστήματος** | **Περιγραφή** |
|---|---|
| Επεξεργασία αιτημάτων χρηστών | Οι Edge Servers λαμβάνουν και επεξεργάζονται αιτήματα, επιστρέφοντας το ζητούμενο περιεχόμενο. |
| Ενδιάμεσοι κόμβοι στο Overlay Network | Βελτιώνουν την απόδοση επικοινωνιών μεγάλων αποστάσεων στο Overlay Network. |
| Caching περιεχομένου | Διατηρούν προσωρινά αποθηκευμένο περιεχόμενο κοντά στους χρήστες, μειώνοντας την ανάγκη επικοινωνίας με τους Origin Servers. |
| Εκτέλεση εφαρμογών (Edge Computing) | Επιτρέπουν την εκτέλεση εφαρμογών στους Edge Servers, μειώνοντας την καθυστέρηση και βελτιώνοντας την απόδοση. |
| Προσαρμογή περιεχομένου | Προσαρμόζουν το περιεχόμενο ανάλογα με τα χαρακτηριστικά του χρήστη (τοποθεσία, ταχύτητα σύνδεσης). |
| Διαχείριση προέλευσης περιεχομένου | Οι Edge Servers μπορούν να ανακτούν δεδομένα από διαφορετικούς Origin Servers ή Data Centers |
| Έλεγχος πρόσβασης | Υποστηρίζουν επικύρωση cookies, πιστοποιητικά πελατών και authentication servers. |
| Δυναμική διαμόρφωση σελίδων (ESI) | Επιτρέπουν συναρμολόγηση ιστοσελίδων από δυναμικά fragments για ταχύτερη απόδοση. |

*Table 2: Βασικές Λειτουργίες του Edge Server Συστήματος της Akamai*

## 1.9 Θέση του CDN στην Παγκόσμια Αγορά

Το παγκόσμιο μέγεθος της αγοράς CDN εκτιμάται ότι θα ανέλθει στα 32,70 δισεκατομμύρια USD το 2025 ενώ προβλέπεται να φτάσει περίπου τα 144,91 δισεκατομμύρια USD έως το 2034. Στις Ηνωμένες Πολιτείες η αγορά του CDN εκτιμήθηκε στα 6,06 δισεκατομμύρια USD το 2024 και προβλέπεται να φτάσει περίπου τα 33,79 δισεκατομμύρια USD έως το 2034 [23].


*Figure 8: U.S CDN Market Size 2024 to 2034 (USD Billion) - Precedence Reasearch*

Η Βόρεια Αμερική κυριάρχησε στην αγορά το 2024, καταλαμβάνοντας πάνω από το 31,14% του συνολικού μεριδίου εσόδων. Ωστόσο, η περιοχή Ασίας-Ειρηνικού (APAC) αναμένεται να καταγράψει υψηλότερο ρυθμό ανάπτυξης, λόγω της ραγδαίας βελτίωσης των IT υποδομών και της ανάγκης υιοθέτησης των τελευταίων τεχνολογιών. Η Κίνα επίσης ξεχωρίζει ως ένα δυναμικό οικοσύστημα για το διαδικτυακό βίντεο περιεχόμενο. Η αυξανόμενη ζήτηση για streaming αποτελεί έναν από τους σημαντικότερους παράγοντες που οδηγούν την ανάπτυξη της βιομηχανίας video streaming στην Κίνα. Παράλληλα, οι χρήστες στην περιοχή Ασίας-Ειρηνικού παρακολουθούν ολοένα και περισσότερα σύντομα βίντεο, λόγω της ευρύτερης πρόσβασης στο διαδίκτυο και των πολυμέσων, γεγονός που έχει οδηγήσει σε εκρηκτική αύξηση της διαδικτυακής κίνησης βίντεο. Με τις αναπτυσσόμενες οικονομίες της Ιαπωνίας, Κίνας, Ινδίας και Νότιας Κορέας, η περιοχή APAC αναμένεται να σημειώσει υψηλή ανάπτυξη στην αγορά CDN. Ο ταχύτατος ρυθμός ανάπτυξης του CDN στην APAC οφείλεται κυρίως στη συνεχή αύξηση της κατανάλωσης ψηφιακού περιεχομένου σε αυτές τις χώρες. Στις Ηνωμένες Πολιτείες, η κατανάλωση συνδρομητικής τηλεόρασης μειώνεται σταδιακά, με τους χρήστες να στρέφονται όλο και περισσότερο στο διαδικτυακό περιεχόμενο αντί της συνδρομητικής τηλεόρασης. Αυτή η εξέλιξη αναμένεται να ενισχύσει περαιτέρω την αγορά CDN, καθώς η ζήτηση για on-demand ψυχαγωγία συνεχίζει να αυξάνεται.

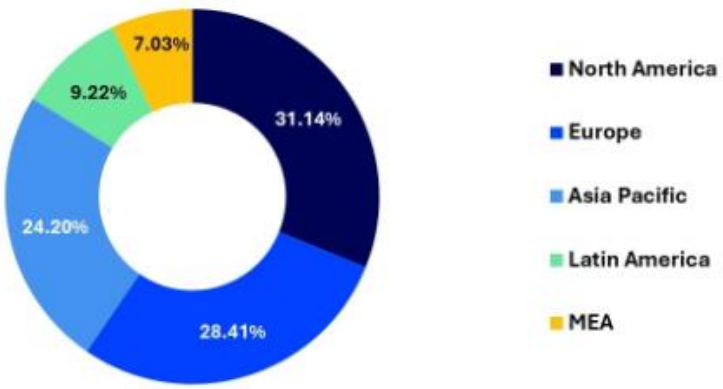


*Figure 9: CDN Market Share by Region, 2024 - Precedence Research*

### 1.9.1 Δυναμική της Αγοράς του Content Delivery Network (CDN)

Η αυξανόμενη υιοθέτηση κινητών συσκευών και η εισχώρηση του διαδικτύου σε όλες τις πτυχές του βίου δημιουργούν σημαντικές ευκαιρίες ανάπτυξης για το mobile CDN. Σύμφωνα με το Cisco Annual Internet Report, ο αριθμός των χρηστών διαδικτύου προβλέπεται να φτάσει τα 5,3 δισεκατομμύρια, 66% του παγκόσμιου πληθυσμού, το 2024, από 3,9 δισεκατομμύρια, 51% του παγκόσμιου πληθυσμού, το 2018. Επιπλέον, σύμφωνα με το Oberlo, τον Οκτώβριο του 2020, σχεδόν 48,62% της παγκόσμιας διαδικτυακής κίνησης προερχόταν από κινητά τηλέφωνα. Η αυξανόμενη κίνηση δικτύου οδηγεί σε αυξημένη ζήτηση για λύσεις CDN, ώστε να διασφαλιστεί η αποτελεσματική διανομή περιεχομένου στους τελικούς χρήστες [23].

Το mobile CDN έχει συμβάλει σημαντικά στη μείωση της κίνησης δεδομένων κινητής τηλεφωνίας και στη βελτίωση της εμπειρίας των χρηστών κινητών συσκευών. Η ραγδαία εξέλιξη των φορητών συσκευών με πρόσβαση στο διαδίκτυο, όπως tablets, smartphones και phablets, αποτελεί έναν από τους βασικούς παράγοντες που αναμένεται να ενισχύσουν τη συνολική κατανάλωση διαδικτυακού περιεχομένου. Η αυξανόμενη χρήση υπηρεσιών διαδικτύου σε κινητές συσκευές αυξάνει τη ζήτηση για mobile CDN, το οποίο προσφέρει βελτιωμένο περιεχόμενο και καλύτερη εμπειρία τελικού χρήστη. Δεδομένου ότι τα υφιστάμενα CDN απαιτούν αυξημένες δυνατότητες και καινοτομία για τη βελτίωση της εμπειρίας χρήστη, υπάρχει σημαντικό περιθώριο για τους CDN providers να προσφέρουν υψηλής ποιότητας mobile CDN λύσεις.

Η χρήση cloud υπηρεσιών από πολλές επιχειρήσεις έχει μειώσει τα έξοδα και τις προσπάθειες συντήρησης, εξαλείφοντας την πολυπλοκότητα του Hardware Installation. Το cloud CDN αναμένεται να μεταμορφώσει το τοπίο της αγοράς CDN και cloud υποδομών, καθώς η ζήτηση για cloud λύσεις αυξάνεται δραματικά στις αναπτυσσόμενες οικονομίες.

Οι Communications Service Providers (CSPs) έχουν ήδη αρχίσει να αναπτύσσουν CDNs για τη διανομή εφαρμογών, λογισμικού και υποδομών. Η διαδικασία αυτή θα προσφέρει στους χρήστες υψηλότερη ποιότητα υπηρεσίας και εμπειρίας. Επιπλέον, οι CSPs διαχειρίζονται τα CDN στα data centers τους και παρέχουν αυτές τις υπηρεσίες με δική τους εμπορική επωνυμία.

Η τάση χρήσης CDN για προσωπική χρήση προβλέπεται να αυξηθεί επίσης, παράλληλα με τη ζήτηση για cloud υπηρεσίες. Επιπλέον, οι CSPs χρησιμοποιούν τα CDN για την ασφάλεια δεδομένων των πελατών, την αποθήκευση και την παροχή υποδομών, ενισχύοντας περαιτέρω την ανάπτυξη της αγοράς CDN.

Η συνδυασμένη εξάπλωση των mobile και cloud CDN αναμένεται να διαδραματίσει καθοριστικό ρόλο στην παγκόσμια αγορά CDN, οδηγώντας σε νέες επιχειρηματικές ευκαιρίες και τεχνολογικές καινοτομίες.

### 1.9.2 Επίδραση της Πανδημίας COVID-19 στην αγορά του Content Delivery Network (CDN)

Η πανδημία του COVID-19 είχε θετικό αντίκτυπο στις επιχειρήσεις που αξιοποίησαν την τεχνολογία CDN. Τα CDN βοήθησαν τους οργανισμούς να ανταποκριθούν στην αυξημένη ζήτηση για μεταφορά δεδομένων υψηλής χωρητικότητας μέσω του διαδικτύου.

Επιπλέον, κατά τη διάρκεια της πανδημίας, πολλές επιχειρήσεις παγκοσμίως υιοθέτησαν μοντέλα τηλεργασίας, γεγονός που δημιούργησε μεγάλες ευκαιρίες για την αγορά των CDN, καθώς η ανάγκη για αξιόπιστη και αποδοτική διανομή περιεχομένου αυξήθηκε σημαντικά.

Παράλληλα, η πανδημία ενίσχυσε τη ζήτηση για Over-the-Top (OTT) πλατφόρμες, οι οποίες αξιοποιούν CDN τεχνολογίες για τη διάθεση περιεχομένου υψηλής ποιότητας στους τελικούς χρήστες.

Η αγορά των Content Delivery Networks αναμένεται να συνεχίσει την ανοδική της πορεία, καθώς η διακίνηση δεδομένων μέσω του διαδικτύου συνεχώς αυξάνεται, ακολουθώντας την ανάπτυξη και την ευρεία υιοθέτηση δικτύων υψηλής ταχύτητας.

# Κεφάλαιο 2ο: Ανάλυση της Αλληλεπίδρασης Ασφάλειας και Content Delivery Network (CDN)

## 2.1 Κυβερνοσφάλεια

Δεν υπάρχει τυποποιημένος και καθολικά αποδεκτός ορισμός της Κυβερνοασφάλειας. Η έννοια σε γενικές γραμμές καλύπτει το σύνολο των διασφαλίσεων και μέτρων που υιοθετούνται για την προστασία συστημάτων, πληροφοριών και των χρηστών τους απέναντι στην μη εξουσιοδοτημένη πρόσβαση, επίθεση και ζημιά, ώστε να εξασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα δεδομένων.

Η κυβερνοασφάλεια περιλαμβάνει την πρόληψη και ανίχνευση κυβερνοπεριστατικών, καθώς και την ανάκαμψη από αυτά. Τα περιστατικά μπορεί να είναι εσκεμμένα και μη και κυμαίνονται από την τυχαία κοινολόγηση πληροφοριών έως επιθέσεις κατά επιχειρήσεων και υποδομών ζωτικής σημασίας και την κλοπή δεδομένων προσωπικού χαρακτήρα, ή ακόμη και έως την παρέμβαση σε δημοκρατικές διαδικασίες. Όλα τα συμβάντα μπορούν να έχουν πολυποίκιλες επιζήμιες επιδράσεις σε πρόσωπα, οργανισμούς και κοινότητες.

Στο εσωτερικό της Ευρώπης, ο όρος καλύπτει και κάθε παράνομη δραστηριότητα με τη χρήση ψηφιακών τεχνολογιών στον κυβερνοχώρο. Με βάση αυτό, μπορεί να περιλαμβάνονται εγκλήματα εξαπόλυσης επιθέσεων με ιούς υπολογιστών ή απάτες με ψηφιακά μέσα πληρωμής καθώς επίσης και εγκλήματα που αφορούν τόσο τα συστήματα όσο και το περιεχόμενο. Δραστηριότητες της μορφής διάδοσης κακοποιητικού υλικού στο διαδίκτυο, εκστρατείες παραπληροφόρησης για την άσκηση επιρροής στον διαδικτυακό διάλογο και υπόνοιες για παρέμβαση σε εκλογικές διαδικασίες συμπεριλαμβάνονται στα κυβερνοεγκλήματα.

Η ασφάλεια στον κυβερνοχώρο αποτελεί προτεραιότητα τόσο για τους οργανισμούς, όσο και για τις παγκόσμιες κυβερνήσεις. Συγκεκριμένα, η ασφάλεια δεδομένων δίνει άλλη οπτική σε όλες τις πρακτικές ασφάλειας, είτε αφορά τη προστασία από επιτιθέμενους, είτε αφορά τη προστασία από εταιρείες που διαχειρίζονται δεδομένα χρηστών. Στην πρώτη περίπτωση απαιτείται η ανάλυση απειλών, που αφορά την αξιολόγηση ύποπτων ενεργειών στον κυβερνοχώρο, ενώ στην δεύτερη, απαιτείται η υιοθέτηση κατάλληλων πολιτικών ασφάλειας.

### 2.1.1 Βασικές Αρχές Κυβερνοσφάλειας

Οι βασικές αρχές της Κυβερνοασφάλειας είναι οι ακόλουθες [24]:

**Αρχή της Αναλογικότητας (Proportionality Principle):** Πρόκειται για την αρχή που καθοδηγεί την ορθολογική λήψη αποφάσεων στην ασφάλεια, σύμφωνα με την οποία τα μέτρα προστασίας πρέπει να είναι αντίστοιχα των κινδύνων που απειλούν ένα σύστημα, της

πιθανότητας υλοποίησης των απειλών και της σοβαρότητας των αντίστοιχων συνεπειών. Συνεπώς, οι πόροι και τα μέτρα ασφάλειας που εφαρμόζονται για τη προστασία των ψηφιακών αγαθών πρέπει να είναι ανάλογα της αξίας τους.

**Απόλυτη Ασφάλεια:** Η επίτευξη της απόλυτης ασφάλειας δεν είναι υλοποιήσιμος στόχος στον πραγματικό κόσμο, συνεπώς πάντα υπάρχει απόπειρα προσδιορισμού του επιπέδου ή του ποσοστού ασφάλειας που είμαστε διατεθειμένοι να αποδεχτούμε, εφαρμόζοντας την αρχή της αναλογικότητας.

**Αρχή Ελαχίστου Προνομίου:** Η αρχή αυτή δηλώνει πως κάθε χρήστης πρέπει να έχει ελάχιστα δικαιώματα πρόσβασης στα δεδομένα και στους πόρους που απαιτούνται για την εκπλήρωση των καθηκόντων του, δηλαδή τις ενέργειες για τις οποίες έχει εξουσιοδότηση. Η αρχή του ελάχιστου προνομίου προστατεύει από εσωτερικές και εξωτερικές επιθέσεις μη εξουσιοδοτημένης πρόσβασης. Οι τακτικές που ακολουθούν συνήθως οι επιτιθέμενοι είναι να αποκτούν πρόσβαση στα πληροφοριακά συστήματα ή σε δίκτυα και στη συνέχεια να αναβαθμίζουν τα δικαιώματα αυτά από απλού χρήστη σε διαχειριστή, αποκτώντας τον έλεγχο του συστήματος.

**Ασφάλεια εκ Σχεδιασμού (Security by Design):** Η αρχή αυτή σημαίνει ότι ένα ψηφιακό σύστημα θα πρέπει να υλοποιείται ενσωματώνοντας στις προδιαγραφές σχεδίασης όλες τις απαιτήσεις ασφάλειας που είναι αναγκαίες για την σωστή λειτουργία του.

**Ασφάλεια εξ Ορισμού (Security by Default):** Πρόκειται για την αρχή που διατυπώνει ότι όλες οι ρυθμίσεις προστασίας πρέπει να είναι εξ ορισμού ενεργοποιημένες και μόνο εφόσον απαιτείται να απενεργοποιούνται.

**Κανόνας Ασθενέστερου Κρίκου:** Το επίπεδο της ασφάλειας ενός συστήματος εξαρτάται από την ασφάλεια του ασθενέστερου σημείου, άρα για την αποτελεσματική θωράκιση ενός ψηφιακού συστήματος απαιτείται μία ολιστική προσέγγιση και η χάραξη μίας ενιαίας πολιτικής ασφάλειας σε επίπεδο οργανισμού.

**Μείωση Επιφάνειας Επίθεσης:** Αξιοσημείωτο είναι να υπάρχει μείωση της επιφάνειας επίθεσης, η οποία αποτελείται από το εύρος των λειτουργικών πόρων που είναι προσπελάσιμοι από έναν επιτιθέμενο, καθώς όσες περισσότερες εφαρμογές λειτουργούν σε ένα πληροφοριακό σύστημα, τόσο μεγαλύτερη είναι η επιφάνεια επίθεσης.

**Αρχή Kerckhoffs:** Στην κρυπτογραφία εφαρμόζεται η αρχή αυτή και διατυπώνει πώς η ασφάλεια ενός κρυπτοσυστήματος δεν εξαρτάται από τη μυστικότητα του αλγορίθμου κρυπτογράφησης, αλλά μόνο από τη διατήρηση της μυστικότητας του κλειδιού που έχει χρησιμοποιηθεί για τη κρυπτογράφηση.

### 2.1.2 Βασικές Απαιτήσεις Ασφάλειας

Η Κυβερνοασφάλεια στηρίζεται σε τρία βασικά χαρακτηριστικά, αυτά είναι εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Η σημασία τους γίνεται κατανοητή από το γεγονός ότι οι ειδικοί του τομέα της Κυβερνοασφάλειας αξιολογούν τις απειλές με βάση το αντίκτυπο που έχουν στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, των εφαρμογών και των συστημάτων ενός οργανισμού [24].

- Η **εμπιστευτικότητά (confidentiality)** διασφαλίζει ότι οι πληροφορίες δε γίνονται διαθέσιμες και δεν αποκαλύπτονται σε μη εξουσιοδοτημένους χρήστες, οντότητες και διαδικασίες.

- Η **ακεραιότητα (integrity)** διασφαλίζει τη προστασία της ορθότητας και της πληρότητας ενός αγαθού και της αποφυγής της μη εξουσιοδοτημένης τροποποίησης του.

- Η **διαθεσιμότητα (availability)** διασφαλίζει πώς ένα αγαθό είναι διαθέσιμο προς χρήση όταν ζητείται από μία εξουσιοδοτημένη οντότητα. Οι επιθέσεις που μπορούν να σημειωθούν κατά της διαθεσιμότητα είναι γνωστές ως επιθέσεις άρνησης υπηρεσιών.

Πρόσθετες θεωρούνται οι ακόλουθες απαιτήσεις:

- **Μη-άρνηση της ευθύνης (Non-Repudiation)** καλείται η αδυναμία αποποίησης της ευθύνης για την εκτέλεση μίας πράξης.

- **Ανθεκτικότητα (Resilience)** αναφέρεται η ικανότητα ενός συστήματος να παράγει συνεχώς το επιδιωκόμενο αποτέλεσμα παρά τα όποια αντίξοα περιστατικά.

- **Ασφάλεια Πληροφορίας (information Security)** καλείται η προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας μιας πληροφορίας.

- **Αυθεντικότητα (Authenticity)** ονομάζεται η ιδιότητα ότι η ταυτότητα μίας οντότητας είναι αυτή που εκείνη έχει ισχυριστεί.

- **Λογοδοσία – Απόδοση Ευθύνης (accountability)** καλείται η υπευθυνότητα μίας οντότητας για τις ενέργειες και αποφάσεις της.

### 2.1.3. Σημασία της Ασφάλειας της Πληροφορίας στους Οργανισμούς

Η κατάλληλη εφαρμογή ελέγχων ασφάλειας πληροφοριών είναι ζωτικής σημασίας για την προστασία ενός οργανισμού, καθώς και της νομικής θέσης, του προσωπικού και άλλων υλικών ή άυλων περιουσιακών στοιχείων. Η αδυναμία ενός οργανισμού να διαλέξει και

υλοποιήσει κατάλληλους κανόνες και διαδικασίες ασφάλειας ενδέχεται να έχει καταστροφικές συνέπειες στην λειτουργία του. Ειδικότερα στη σύγχρονη εποχή που χαρακτηρίζεται από έντονη δραστηριότητα κακόβουλου κώδικα, παραβιάσεων συστημάτων και απειλών εσωτερικών πληροφοριών, τα δημοσιευμένα αλλά και τα αδημοσίευτα ζητήματα ασφάλειας έχουν αρνητικές συνέπειες στην λειτουργία, κερδοφορία και φήμη του οργανισμού.

Στις περιπτώσεις που τα δεδομένα και τα συστήματα ενός οργανισμού συνδέονται με άλλα συστήματα εξωτερικά, οι ευθύνες εκτείνονται πέρα από τα όρια της οργάνωσης. Αυτό μπορεί να απαιτήσει από τη διοίκηση να γνωρίζει τους μηχανισμούς και τις πολιτικές ασφάλειας που 34 χρησιμοποιούν τα εξωτερικά συστήματα ή να ζητήσει διασφάλιση ότι το εξωτερικό σύστημα παρέχει ένα καλό επίπεδο ασφάλειας για τις πληροφορίες και το σύστημα του οργανισμού.

Η παροχή ενός αξιοπρεπούς επιπέδου ασφάλειας πληροφοριών απαιτεί μία ολοκληρωμένη προσέγγιση που λαμβάνει υπόψιν μία ποικιλία τομέων τόσο εντός, όσο και εκτός του πεδίου ασφάλειας πληροφοριών. Η προσέγγιση αυτή βρίσκει εφαρμογή σε ολόκληρο τον κύκλο ζωής του συστήματος.

Η ασφάλεια των πληροφοριών δεν είναι μία διαδικασία που θεωρείται στατική, αλλά απαιτεί συνεχή παρακολούθηση και διαχείριση για τη προστασία της εμπιστευτικότητας, ακεραιότητας και της διαθεσιμότητας των πληροφοριών καθώς και για να διασφαλιστεί ότι οι νέες ευπάθειες και οι εξελισσόμενες απειλές εντοπίζονται σε σύντομο χρονικό διάστημα και υπάρχει η ανάλογη ανταπόκριση για την αντιμετώπιση τους.

## 2.2 Ασφάλεια και Content Delivery Network (CDN)

Η ασφάλεια στο CDN αποτελεί έναν από τους πιο κρίσιμους παράγοντες για τη διατήρηση της ομαλής και ασφαλής λειτουργίας του διαδικτύου. Η σχέση μεταξύ του CDN και της ασφάλειας είναι αμοιβαία: από τη μία, το ίδιο το CDN πρέπει να διαθέτει ισχυρούς μηχανισμούς προστασίας ώστε να μην αποτελεί ευάλωτο σημείο σε κυβερνοεπιθέσεις, και από την άλλη, το CDN λειτουργεί ως βασικός πυλώνας ενίσχυσης της ασφάλειας για τις ιστοσελίδες και τις διαδικτυακές υπηρεσίες που εξυπηρετεί. Αξίζει να υπογραμμιστούν τα ακόλουθα σημεία:

**Προστασία από Επιθέσεις και διασφάλιση της διαθεσιμότητας:** Τα CDN διανέμουν περιεχόμενο μέσω ενός παγκόσμιου δικτύου διακομιστών, μετριάζοντας έτσι τον κίνδυνο μην διαθεσιμότητας λόγω επιθέσεων DDoS και εξασφαλίζοντας χαμηλή καθυστέρηση. Απορροφώντας την επισκεψιμότητα και μέσω μηχανισμών όπως τα Web Application Firewalls (WAF) προστατεύουν τις ιστοσελίδες από απειλές που θα μπορούσαν να τις θέσουν εκτός λειτουργίας, εξασφαλίζοντας με αυτό τον τρόπο την διαθεσιμότητα. Αυτή η συνεχής

διαθεσιμότητα είναι ζωτικής σημασίας για επιχειρήσεις και χρήστες που βασίζονται στις διαδικτυακές υπηρεσίες.

**Ακεραιότητα και εμπιστευτικότητα δεδομένων:** Τα CDN αποθηκεύουν προσωρινά αντίγραφα του περιεχομένου, και ως εκ τούτου, η ασφάλεια του περιεχομένου αυτού είναι πρωταρχικής σημασίας. Η παραβίαση ενός CDN μπορεί να οδηγήσει σε τροποποίηση περιεχομένου, διαρροή ευαίσθητων δεδομένων ή διανομή κακόβουλου λογισμικού στους χρήστες. Σημειώνεται επίσης πώς το πρωτόκολλο TLS/HTTPS εξασφαλίζει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων που μεταφέρονται μεταξύ των χρηστών και των διακομιστών του CDN.

**Απόκρυψη του Origin Server:** Ένα σημαντικό πλεονέκτημα των CDN είναι ότι αποτρέπουν την άμεση πρόσβαση στον Origin Server, κρύβοντας την πραγματική IP του από κακόβουλους χρήστες. Ωστόσο, εάν η IP του Origin Server διαρρεύσει, για παράδειγμα με την υλοποίηση λανθασμένων ρυθμίσεων ή κάποιων headers, ο Origin Server γίνεται ευάλωτος. Η ασφαλής διαχείριση αυτής της πληροφορίας είναι ζωτικής σημασίας.

**Προστασία της φήμης**: Ένα περιστατικό ασφαλείας σε ένα CDN μπορεί να βλάψει τη φήμη των ιστοσελίδων που το χρησιμοποιούν και να οδηγήσει σε απώλεια εμπιστοσύνης από τους χρήστες, ενώ παράλληλα βλάπτει και το ίδιο το CDN. Η ασφάλεια του CDN είναι συνεπώς κρίσιμη για τη διατήρηση της εμπιστοσύνης και της αξιοπιστίας των τελικών χρηστών στον εκάστοτε οργανισμό που επιλέγει να χρησιμοποιήσει το CDN.

**Αποτροπή κατάχρησης:** Εκτός από την παροχή προστασίας από επιθέσεις, ένα CDN πρέπει επίσης να διασφαλίζει ότι δεν θα χρησιμοποιηθεί από κακόβουλους παράγοντες για τη διενέργεια επιθέσεων, όπως η εκτέλεση DDoS επιθέσεων ή η σάρωση θυρών TCP. Η διασφάλιση ότι τα CDN δεν μπορούν να χρησιμοποιηθούν για τέτοιες δραστηριότητες είναι σημαντική για την ασφάλεια του διαδικτύου.

**Διασφάλιση των συναλλαγών:** Τα CDN εξυπηρετούν επίσης εφαρμογές ηλεκτρονικού εμπορίου, οπότε η διασφάλιση της ασφάλειας των συναλλαγών και των προσωπικών πληροφοριών των χρηστών είναι απαραίτητη. Χρησιμοποιώντας προηγμένα πρωτόκολλα ασφαλείας και εργαλεία ανίχνευσης απάτης, τα CDN συμβάλλουν στην ασφάλεια των ηλεκτρονικών συναλλαγών, μειώνοντας τους κινδύνους παραβίασης δεδομένων.

Η ασφάλεια στο CDN δεν αποτελεί απλώς μια τεχνική λεπτομέρεια, αλλά βασικό στοιχεία για την διασφάλιση ενός ασφαλούς και αξιόπιστου διαδικτυακού περιβάλλοντος. Η αμοιβαία σχέση μεταξύ CDN και ασφάλειας σημαίνει ότι η προστασία του ίδιου του CDN είναι εξίσου σημαντική με την προστασία που παρέχει στις υπηρεσίες που υποστηρίζει. Για να διατηρηθεί αυτή η ισορροπία, απαιτείται συνεχής παρακολούθηση, ενημέρωση των

μηχανισμών προστασίας και συνεργασία μεταξύ των παρόχων CDN και των οργανισμών που τα χρησιμοποιούν.

## 2.3 Κύριες Προκλήσεις Ασφάλειας στο Content Delivery Network (CDN) και Αντίμετρα

Οι κύριες προκλήσεις ασφάλειας που αντιμετωπίζουν τα CDN μπορούν να ταξινομηθούν με βάση τα βασικά συστατικά στοιχεία της αρχιτεκτονικής ενός CDN. Συγκεκριμένα, προκλήσεις ασφάλειας στα CDN αναλύονται στις προκλήσεις ασφάλειας σε επίπεδο Edge Servers, στις προκλήσεις ασφάλειας σε επίπεδο Origin Server και στις προκλήσεις ασφάλειας σε επίπεδο δρομολόγησης αιτημάτων (request routing). [5]

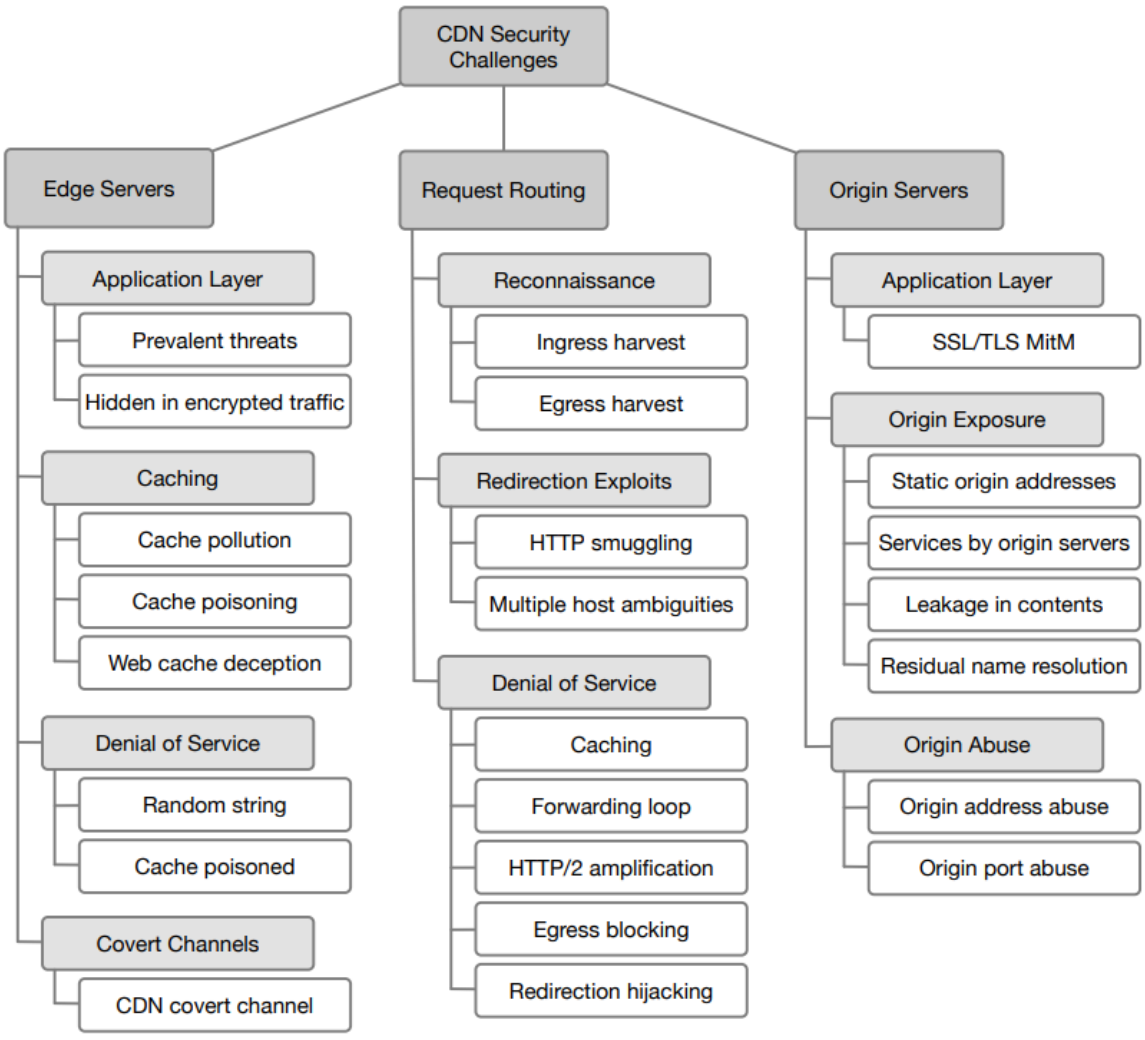


*Figure 10: Κατηγοριοποίηση των Προκλήσεων Ασφάλειας - Content Delivery Network Security: A Survey, M. Ghaznavi, E. Jalalpour, A. Salahuddin, R. Boutaba, D. Migault, S. Preda*

### 2.3.1 Προκλήσεις Ασφάλειας σε Επίπεδο Edge Servers και Αντίμετρα

Οι Edge Servers αποτελούν ένα από τα βασικά δομικά στοιχεία των CDN, γεγονός που τους καθιστά στόχους για κακόβουλες ενέργειες, απαιτώντας παράλληλα προσεκτική διαχείριση και εφαρμογή αντιμέτρων για την αντιμετώπιση ευπαθειών. Τα CDN διαχειρίζονται

διαδικτυακά αιτήματα γεγονός που καθιστά τους Edge Servers ευάλωτους σε επιθέσεις που λαμβάνουν χώρα σε επίπεδο εφαρμογής. Παράλληλα, οι Edge Servers είναι εκτεθειμένοι σε απειλές που σχετίζονται με το Caching. Αξίζει επίσης να σημειωθεί πώς, επιτιθέμενοι μπορούν να στείλουν κακόβουλα requests, τα οποία εκμεταλλεύονται ευπάθειες των Edge Servers, με σκοπό να ξεκινήσουν επιθέσεις τύπου Denial of Service (DoS). Τέλος, οι Edge Servers μπορούν να χρησιμοποιηθούν ως κρυφό κανάλι επικοινωνίας για την μετάδοση ευαίσθητων πληροφοριών.

#### 2.3.1.1 Προκλήσεις στο Application Layer – Επίπεδο 7 και Αντίμετρα

Οι προκλήσεις ασφάλειας σε επίπεδο Application Layer των Edge Servers αποτελούν κρίσιμο ζήτημα, λόγω της θέσης και των αρμοδιοτήτων που έχουν οι Edge Servers, δηλαδή του διαμεσολαβητή μεταξύ του Origin Server και των τελικών χρηστών. Συγκεκριμένα, οι Edge Servers διανέμουν μεγάλους όγκους διαδικτυακής κίνησης και παράλληλα αποθηκεύουν περιεχόμενο, γεγονός που τους καθιστά ευάλωτους σε επιθέσεις σε επίπεδο 7. Οι προκλήσεις που αντιμετωπίζονται σε αυτό το επίπεδο μπορούν να διακριθούν σε δυο βασικές κατηγορίες, τις Prevalent Threats (διαδεδομένες απειλές) και τις Hidden in Encrypted Traffic (κρυμμένες σε κρυπτογραφημένη κίνηση). Ακολούθως, φαίνεται μια συνοπτική περιγραφή των απειλών αυτών, των ευπαθειών που εκμεταλλεύονται, των αντιμέτρων που μπορούν να ληφθούν και των επιπτώσεων τους.

**Prevalent Threats (Διαδεδομένες Απειλές):**
Οι Edge Servers είναι ευάλωτοι σε πληθώρα επιθέσεων που εκμεταλλεύονται ευπάθειες στα web applications. Οι  πιο συνηθισμένες επιθέσεις αυτού του τύπου είναι οι SQL Injection, Cross-Site Scripting (XSS), File Inclusion, Remote Command Execution, Dictionary επίθεση κτλ. Αυτές οι επιθέσεις μπορούν να προκαλέσουν σοβαρές συνέπειες για την λειτουργία ενός οργανισμού όπως διαρροή ευαίσθητων δεδομένων, απάτη ή δυσλειτουργία του οργανισμού, όπως και διακοπή των παρεχόμενων υπηρεσιών. Για την αντιμετώπιση αυτών των απειλών, οι Edge Servers χρησιμοποιούν μία σειρά από αντίμετρα, όπως η ανάλυση του πηγαίου κώδικα της εφαρμογής για την ανεύρεση ευπαθειών, κάτι το οποίο δεν είναι δυνατό να αποκλείσει κάθε πιθανή απειλή. Ένα ακόμα αντίμετρο είναι ο περιορισμός συγκεκριμένων τύπων requests πχ. τα POST requests, κάτι το οποίο από την μία ελαχιστοποιεί την υλοποίηση επιθέσεων με κάνουν χρήση αυτής της μεθόδου, αλλά από την άλλη περιορίζουν τις δυνατότητες του CDN. Τέλος, το βασικότερο αντίμετρο για τις επιθέσεις αυτού του τύπου είναι η εγκατάσταση Web Application Firewalls μπροστά από τους Edge Servers, με σκοπό να υλοποιούν deep inspection της κίνησης και να φιλτράρουν την κακόβουλη από τους πραγματικούς χρήστες.  Πολλά από τα WAFs αυτού του τύπου, είναι ειδικά διαμορφωμένα ώστε να φιλτράρουν την κίνηση με βάση τις απειλές που έχουν καθοριστεί από το OWASP [4][25].

**Hidden in Encrypted Traffic (Κρυμμένες σε Κρυπτογραφημένη Κίνηση):**
Η συγκεκριμένη κατηγορία προκλήσεων αναφέρεται στις επιθέσεις που εκμεταλλεύονται την κρυπτογραφημένη κίνηση, επιτρέποντας στους επιτιθέμενους να αποκρύψουν κακόβουλο περιεχόμενο, να παρακάμψουν τους μηχανισμούς ασφάλειας του CDN και να στοχεύσουν τους Origin Servers. Αν και πρωτόκολλα όπως το SSL/TLS εξασφαλίζουν την ασφαλή επικοινωνία, δυσχεραίνουν την επιθεώρηση της κίνησης από τους Edge Servers, καθώς το CDN δεν διαθέτει τα ιδιωτικά κλειδιά των κατόχων περιεχομένου. Αυτό δίνει στους

επιτιθέμενους τη δυνατότητα να αποφύγουν τους μηχανισμούς ασφάλειας του CDN και να στοχεύσουν απευθείας τους Origin Servers. Μια προφανής λύσης θα ήταν αποκρυπτογράφηση της κίνησης για ανάλυση, η οποία όμως θα απαιτούσε την κοινοποίηση των ιδιωτικών κλειδιών στο CDN, δημιουργώντας σοβαρούς κινδύνους για την ιδιωτικότητα των χρηστών και την εμπιστευτικότητα των δεδομένων. Για τον λόγο αυτό το CDN δεν μπορεί να κάνει inspect το traffic payload αλλά προχωράει σε διανομή της κίνησης στους Origin Servers. Αξίζει να σημειωθεί όμως, πώς για την αντιμετώπιση τέτοιων επιθέσεων, μπορούν να εφαρμόζονται τεχνικές όπως η ανάλυση συμπεριφοράς και η στατιστική εξέταση των χαρακτηριστικών της κίνησης, οι οποίες ωστόσο δεν αποτελούν μια πλήρως επαρκή λύση. Μια πιο καινοτόμος προσέγγιση θα ήταν η χρήση fully homomorphic encryption, που επιτρέπει την ανάλυση κρυπτογραφημένης κίνησης χωρίς την ανάγκη αποκρυπτογράφησης. Η πρακτική εφαρμογή της συγκεκριμένης λύσης παραμένει περιορισμένη έως σήμερα λόγω της υψηλής υπολογιστικής της πολυπλοκότητας [26][27][4].

#### 2.3.1.2 Προκλήσεις στο Caching και Αντίμετρα

Σχετικά με τις προκλήσεις ασφάλειας των Edge Servers σε επίπεδο Caching αξίζει αρχικά να υπογραμμιστεί πώς η δημοτικότητα του περιεχομένου αποτελεί βασικό παράγοντα που επηρεάζει την αποδοτική και ασφαλή αντικατάσταση του στους Edge Servers. Η συμπεριφορά που ακολουθείται είναι ότι οι Edge Servers κασάρουν τα πιο δημοφιλή περιεχόμενα αξιοποιώντας της αρχή τοπικότητας των αναφορών (Locality Reference Principle), δηλαδή το ότι στην ουσία ένα περιεχόμενο που έχει ζητηθεί πρόσφατα, έχει υψηλή πιθανότητα να ζητηθεί ξανά. Οι κακόβουλοι έρχονται να εκμεταλλευτούν αυτή την αρχή, εισάγοντας μη δημοφιλές περιεχόμενο, με σκοπό να υποβαθμίσουν την απόδοση του Caching. Επιπλέον, άλλο ένα κρίσιμο φαινόμενο είναι το Cache Poisoning, στο οποίο οι κακόβουλοι, αντικαθιστούν το περιεχόμενο, με ένα ψεύτικο περιεχόμενο, με σκοπό οι επόμενοι χρήστες να λαμβάνουν το ψεύτικο περιεχόμενο μέχρι την λήξη του σχετικού TTL. Παρόμοιες επίσης τεχνικές χρησιμοποιούνται και για την κλοπή ευαίσθητων δεδομένων, κάνοντας τους Edge Servers να κασάρουν πληροφορίες των τελικών χρηστών, κάτι το οποίο δημιουργεί μέγιστο κενό ασφάλειας.

**Cache Pollution:**
Μία σοβαρή απειλή για την ασφάλεια σε επίπεδο της Cache είναι η Cache pollution, όπου οι επιτιθέμενοι προκαλούν συχνές αστοχίες, δηλαδή Cache Misses, μειώνοντας την αποτελεσματικότητά της. Αυτό επιτυγχάνεται με την αποστολή μεγάλου αριθμού αιτημάτων για μη δημοφιλές περιεχόμενο, εκτοπίζοντας έτσι το πραγματικά δημοφιλές περιεχόμενο από την Cache. Το πρόβλημα με αυτές τις επιθέσεις είναι ότι είναι δύσκολο να ανιχνευθούν, καθώς τα αιτήματα για μη δημοφιλές περιεχόμενο δεν είναι απαραίτητα κακόβουλα. Για την αντιμετώπιση αυτού του κινδύνου, οι Edge Servers εφαρμόζουν μηχανισμούς που αναλύουν τη συμπεριφορά των χρηστών και τη δυναμική του περιεχομένου. Ένας τρόπος είναι η ανίχνευση επιθέσεων ψευδούς τοπικότητας (false locality attack), όπου ένας επιτιθέμενος ζητά επανειλημμένα το ίδιο μη δημοφιλές περιεχόμενο για να το διατηρήσει στην Cache. Μια άλλη μέθοδος είναι η ανίχνευση βάσει αντικειμένου, όπου περιεχόμενο που ζητείται συχνά από πολύ περιορισμένο αριθμό χρηστών θεωρείται ψευδώς δημοφιλές και απομακρύνεται από την Cache. Επιπλέον, υπάρχουν προσεγγίσεις που παρακολουθούν το ιστορικό επιτυχίας ή αποτυχίας ενός χρήστη στην Cache, επιτρέποντας τον εντοπισμό ύποπτων μοτίβων χρήσης και την προσαρμογή των πολιτικών αποθήκευσης για τη βελτίωση της απόδοσης και της ασφάλειας [28][28][4].

**Cache Poisoning:**
Μια ακόμη πρόκληση για την ασφάλεια των Edge Servers σε επίπεδο Caching είναι οι επιθέσεις τύπου Cache Poisoning, κατά τις οποίες οι επιτιθέμενοι αντικαθιστούν ένα νόμιμο αποθηκευμένο περιεχόμενο με ένα παραποιημένο. Αυτό επιτυγχάνεται μέσω της εκμετάλλευσης των "μη κλειδωμένων εισόδων" (Unkeyed Inputs) στους HTTP headers, δηλαδή στις περιπρώσεις όπου ορισμένες τιμές των headers δεν περιλαμβάνονται στο κλειδί της Cache. Με αυτή την τεχνική, ένας επιτιθέμενος μπορεί να στείλει ένα HTTP request με κακόβουλες τιμές στα headers, ενώ το κλειδί της Cache παραμένει αρκετά γενικό ώστε να ταιριάζει με μελλοντικά αιτήματα. Όταν ο Origin Server απαντήσει με το παραποιημένο περιεχόμενο, ο Edge Server το αποθηκεύει στην Cache, με αποτέλεσμα οι επόμενοι χρήστες να λαμβάνουν το ψεύτικο περιεχόμενο αντί του αυθεντικού. Για την αντιμετώπιση αυτής της απειλής, οι Origin Servers μπορούν να φιλτράρουν και να αποκλείουν μη ασφαλείς τιμές στα HTTP headers πριν απαντήσουν, ενώ οι Edge Servers μπορούν να ενισχύσουν την ασφάλεια της Cache, συμπεριλαμβάνοντας περισσότερα HTTP headers στο κλειδί της, ώστε να αποτρέπεται η αποθήκευση περιεχομένου που προέρχεται από κακόβουλες τροποποιήσεις [30][31].

**Web Cache Deception:**
Η συγκεκριμένη πρόκληση στο επίπεδο Caching, αφορά τις επιθέσεις κατά τις οποίες ένας επιτιθέμενος εξαπατά έναν Edge Server, ώστε να αποθηκεύσει ευαίσθητες πληροφορίες των χρηστών στην Cache, επιτρέποντάς του να τις ανακτήσει αργότερα. Αυτό επιτυγχάνεται παρασύροντας τον χρήστη να ζητήσει δυναμικό περιεχόμενο που περιέχει ευαίσθητα δεδομένα, το οποίο όμως αποθηκεύεται στην Cache σαν να ήταν στατικό. Στη συνέχεια, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε αυτές τις πληροφορίες απλώς ανακτώντας το αποθηκευμένο περιεχόμενο από την Cache, χωρίς να απαιτείται εξουσιοδότηση. Για την αποτροπή αυτής της επίθεσης, οι Origin Servers μπορούν να παραμετροποιηθούν ώστε να απαντούν κατάλληλα σε μη αναμενόμενες διευθύνσεις URL, αποτρέποντας το Caching ευαίσθητων δεδομένων. Παράλληλα, οι Edge Servers μπορούν να αποκλείουν το ευαίσθητο περιεχόμενο από την Cache, ελέγχοντας αν ο τύπος της απάντησης ταιριάζει με το αρχικό αίτημα. Με αυτόν τον τρόπο, μειώνεται ο κίνδυνος διαρροής πληροφοριών μέσω της Cache. Έρευνες έχουν δείξει πώς η Akamai, η Cloudflare, η Cloud-Front και η Fastly είναι ευάλωτες σε αυτού του τύπου τις επιθέσεις [32][33].

#### 2.3.1.3 Προκλήσεις Denial of Service και Αντίμετρα

Σε μια επίθεση Denial of Service (DoS), οι κακόβουλοι στοχεύουν στην μη διαθεσιμότητα των υπηρεσίων του CDN, με σκοπό οι τελικοί χρήστες να μην έχουν πρόσβαση στο περιεχόμενο που διανέμουν. Στην περίπτωση μιας Distributed Denial of Service (DDoS) επίθεσης, χρησιμοποιούνται πολλαπλοί επιτιθέμενοι ή μολυσμένα συστήματα για να επιτύχουν τον ίδιο στόχο. Για παράδειγμα, σε μία DoS επίθεση, ένας επιτιθέμενος μπορεί να κατακλύσει έναν Edge Server με τεράστιο όγκο requests, εξαντλώντας τους διαθέσιμους πόρους του και εμποδίζοντας τους τελικούς χρήστες από το να αποκτήσουν πρόσβαση στο περιεχόμενο. Αυτές οι επιθέσεις διαταράσσουν τη λειτουργία των υπηρεσιών CDN, προκαλώντας σημαντικές οικονομικές απώλειες στις επιχειρήσεις που βασίζονται σε αυτές και δημιουργώντας αμφιβολίες για την φήμη του ίδιου του CDN καθώς και των επιχειρήσεων που το έχουν επιλέξει. Επιπλέον, οι επιτιθέμενοι εκμεταλλεύονται την ευπάθεια των Edge Servers στη διαχείριση δυναμικού περιεχομένου, χρησιμοποιώντας το ίδιο το CDN για να ενισχύσουν τις επιθέσεις DoS εναντίον των Origin Servers. Παράλληλα, οι επιτιθέμενοι έχουν

την δυνατότητα να αξιοποιούν κενά ασφαλείας στα HTTP request headers για να δηλητηριάσουν την Cache, να υλοποιήσουν δηλαδή Cache Poisoning, αντικαθιστώντας το αυθεντικό περιεχόμενο με κακόβουλο [34][35][36].

**Random String DoS:**
Μία από τις σημαντικότερες επιθέσεις DoS σε Edge Servers είναι η επίθεση Random String DoS. Σε αυτή την επίθεση, οι επιτιθέμενοι παραποιούν διευθύνσεις URL προσθέτοντας τυχαίες συμβολοσειρές στις τιμές των query strings, πχ. ?test=12345, αναγκάζοντας τους Edge Servers να ζητούν συνεχώς περιεχόμενο από τους Origin Servers. Κάθε request με μια νέα τυχαία συμβολοσειρά στην τιμή του query string προκαλεί CACHE MISS στον Edge Server, ακόμα και αν το περιεχόμενο είναι στατικό. Ο Edge Server τότε ανακτά το περιεχόμενο από τον Origin Server και το παραδίδει στον επιτιθέμενο, μέσω δύο ξεχωριστών συνδέσεων TCP. Η πρώτη σύνδεση (Edge Server προς Origin Server) έχει υψηλή απόδοση, ενώ η δεύτερη (Edge Server προς επιτιθέμενο) έχει χαμηλή απόδοση. Αυτή η διαφορά στην απόδοση επιτρέπει στον επιτιθέμενο να ενισχύσει την κίνηση προς τον Origin Server, καταναλώνοντας περισσότερο bandwidth και πόρους. Για την αντιμετώπιση αυτής της επίθεσης, μπορούν να εφαρμοστούν πολλές τεχνικές όπως η αποκλειστική εξυπηρέτηση στατικού περιεχομένου από τους Edge Servers, η συνεργασία μεταξύ των Edge Servers και των Origin Servers για την ανίχνευση και τον περιορισμό της κίνησης από κακόβουλες IP διευθύνσεις, και η χρήση μηχανισμών ανίχνευσης ανωμαλιών για τον εντοπισμό ασυνήθιστων μοτίβων αιτημάτων. Επίσης, η επιβράδυνση της μεταφοράς περιεχομένου μεταξύ Origin Servers και Edge Servers και η διακοπή της μεταφοράς όταν ο χρήστης κλείνει τη σύνδεση μπορούν να μειώσουν τον αντίκτυπο της επίθεσης [28].

**Cache Poisoned DoS:**
Σε επίπεδο DoS, οι Edge Servers είναι ευάλωτοι και σε επιθέσεις Cache Poisoned DoS. Σε αυτή την περίπτωση, οι επιτιθέμενοι χρησιμοποιούν Cache Poisoning για να αναγκάσουν τους Edge Servers να αποθηκεύσουν κακόβουλο αντί για το πραγματικό περιεχόμενο. Αυτό γίνεται μέσω της αποστολής κακόβουλων αιτημάτων HTTP με headers που προκαλούν σφάλματα στους Origin Server. Οι Edge Servers, μη ανιχνεύοντας το κακόβουλο header, προωθούν το αίτημα στον Origin Server, ο οποίος απαντά με μια σελίδα σφάλματος, την οποία αποθηκεύει ο Edge Server. Έτσι, τα μελλοντικά requests για το ίδιο περιεχόμενο λαμβάνουν τη σελίδα σφάλματος, έως ότου λήξει το σχετικό TTL. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν διάφορες τεχνικές για να επιτύχουν Cache Poisoning όπως υπερμεγέθη HTTP headers, HTTP meta characters, και HTTP method override. Για την αντιμετώπιση αυτών των επιθέσεων, οι Edge Servers μπορούν να ρυθμιστούν ώστε να αποκλείουν τις σελίδες σφαλμάτων από την Cache. Ακόμα, ένας Origin Server μπορεί να στείλει τον header Cache-Control: no-store και οι Edge Servers να τηρήσουν την εντολή του Origin. Επίσης, η χρήση WAFs για το φιλτράρισμα των κακόβουλων headers μπορεί να προσφέρει επιπλέον προστασία [34][35].

#### 2.3.1.4 Προκλήσεις των Covert Channels και Αντίμετρα

Οι προκλήσεις ασφαλείας των Edge Servers που σχετίζονται με τα Covert Channels είναι ιδιαίτερα κρίσιμες, καθώς επιτρέπουν σε επιτιθέμενους να επικοινωνούν κρυφά και να εξάγουν ευαίσθητες πληροφορίες, παρακάμπτοντας τους μηχανισμούς ασφαλείας των CDN. Αυτή η μορφή επίθεσης, αν και πιο δύσκολο να εντοπιστεί, μπορεί να έχει σοβαρές

επιπτώσεις στην εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Μια από τις κύριες απειλές είναι το CDN Covert Channel, όπου ένας κακόβουλος χρήστης ή πάροχος περιεχομένου εκμεταλλεύεται την υποδομή του CDN για να δημιουργήσει ένα μυστικό κανάλι επικοινωνίας μεταξύ ενός κακόβουλου χρήστη και ενός κακόβουλου Origin Server. Αυτή η διαδικασία περιλαμβάνει την συλλογή των IP διευθύνσεων των Edge Servers, την ανάπτυξη ενός σχήματος κωδικοποίησης πληροφοριών, την κοινοποίηση αυτού του σχήματος και των IPs στους επιτιθέμενους, την κωδικοποίηση μυστικών μηνυμάτων σε αιτήματα διείσδυσης (δηλαδή requests που αναγκάζουν τον Edge Server να ανακτήσει περιεχόμενο από τον Origin Server, όπως URLs με τυχαίες συμβολοσειρές) και την αποκωδικοποίηση των αιτημάτων από τον κακόβουλο Origin Server. Η επιτυχία μιας τέτοιας επίθεσης εξαρτάται από τη δυνατότητα του επιτιθέμενου να επιλέξει και να στείλει requests διείσδυσης σε συγκεκριμένους Edge Servers, να παρακάμψει την Cache τους και να καθορίσει τη σχέση μεταξύ του πρώτου και τελευταίου Edge Server στην αλυσίδα μεταφοράς δεδομένων. Για την αντιμετώπιση αυτών των επιθέσεων, τα CDN μπορούν να εφαρμόσουν διάφορα μέτρα ασφαλείας, όπως η αποδοχή μόνο πιστοποιημένων αιτημάτων, η απενεργοποίηση των query strings στα HTTP requests για την αποφυγή παράκαμψης της Cache, και η τυχαιοποίηση της αντιστοίχισης μεταξύ των Edge Servers. Αυτές οι τεχνικές, αν και αποτελεσματικές, μπορεί να έχουν επιπτώσεις στην απόδοση και την ευελιξία του CDN. Επομένως, η ασφάλεια σε επίπεδο Covert Channel απαιτεί μια ισορροπημένη προσέγγιση που να λαμβάνει υπόψη τόσο την αποτελεσματικότητα των μέτρων ασφαλείας όσο και τις επιπτώσεις τους στη λειτουργία του CDN [28][4].

### 2.3.2 Προκλήσεις Ασφάλειας σε Επίπεδο Δρομολόγησης Αιτημάτων και Αντίμετρα

Το DNS αποτελεί αναπόσπαστο μέρος της δρομολόγησης αιτημάτων σε ένα CDN. Αξιοσημείωτος είναι ο τρόπος με τον οποίο οι επιτιθέμενοι εκμεταλλεύονται το request routing σύστημα για να συλλέξουν ευαίσθητες πληροφορίες σχετικά με ένα CDN, όπως οι IP διευθύνσεις των Edge Servers, και να χρησιμοποιήσουν αυτές τις πληροφορίες για την εκτέλεση σύνθετων επιθέσεων στα άλλα συστήματα του CDN. Οι επιτιθέμενοι επίσης μπορούν να παρέμβουν στο request routing σύστημα, ώστε να ανακατευθύνουν τα αιτήματα των τελικών χρηστών σε διευθύνσεις της επιλογής τους. Επιπλέον, οι κακόβουλοι μπορούν ακόμα, να υπερφορτώσουν το συγκεκριμένο σύστημα, εμποδίζοντας έτσι τους τελικούς χρήστες να αποκτήσουν πρόσβαση στις υπηρεσίες που παρέχει το CDN και οι ιδιοκτήτες περιεχομένου [4].

#### 2.3.2.1 Προκλήσεις Αναγνώρισης (Reconnaissance) και Αντίμετρα

Οι επιτιθέμενοι αλληλοεπιδρούν με το request routing σύστημα χρησιμοποιώντας επιθέσεις αναγνώρισης (reconnaissance attacks) για τη συλλογή πληροφοριών σχετικά με το περιεχόμενο, τους ιδιοκτήτες περιεχομένου και τα CDNs. Ύστερα, εκμεταλλεύονται τις πληροφορίες που συλλέγουν για να εκτελέσουν περαιτέρω ενεργές επιθέσεις, όπως επιθέσεις DoS, phishing και δηλητηρίαση της Cache (Cache Poisoning). Ιδιαίτερο ενδιαφέρον για τους επιτιθέμενους παρουσιάζει η συλλογή διευθύνσεων IP των CDNs μέσω αξιόπιστων

μεθόδων [37][38]. Τα CDNs διαθέτουν εύρη από IP διευθύνσεις, τα οποία κατανέμουν στους Edge Servers τους. Οι Edge Servers οργανώνονται σε δύο επίπεδα Caching, χρησιμοποιώντας τις IP διευθύνσεις ως Ingress και Egress διευθύνσεις. Στο πρώτο Caching επίπεδο, οι Edge Servers χρησιμοποιούν τις Ingress IP διευθύνσεις για την επικοινωνία τους με τους τελικούς χρήστες, ενώ στο δεύτερο Caching επίπεδο χρησιμοποιούν τις Egress IP διευθύνσεις για την επικοινωνία τους με τους Oigin Servers [38]. Οι επιτιθέμενοι επιδιώκουν αξιόπιστες μεθόδους συλλογής των διευθύνσεων IP των Edge Servers. Αξίζει να σημειωθεί ότι ορισμένα CDNs δημοσιεύουν τα εύρη των IP διευθύνσεών τους, επιτρέποντας στους επιτιθέμενους να στοχεύσουν άμεσα σε αυτές τις διευθύνσεις. Ωστόσο, υπάρχουν CDNs που δεν δημοσιεύουν τις IP διευθύνσεις τους. Μία εναλλακτική προσέγγιση είναι μία WHOIS αναζήτηση για το ιστορικό των IP διευθύνσεων ενός CDN. Ωστόσο, το WHOIS μπορεί να είναι ελλιπές ή μη ενημερωμένο, καθώς ο GDPR έχει περιορίσει τη συλλογή και αποθήκευση δεδομένων IP διευθύνσεων [39].

**Ingress Harvest:**

Οι επιθέσεις Ingress Harvest στοχεύουν στη συλλογή των διευθύνσεων IP εισόδου που χρησιμοποιούν οι Edge Servers για την επικοινωνία τους με τους τελικούς χρήστες. Εάν ένας επιτιθέμενος καταφέρει να εντοπίσει τη διεύθυνση IP ενός Edge Server, μπορεί να ξεκινήσει μια επίθεση DoS εναντίον του, επιδιώκοντας να τον καταστήσει μη διαθέσιμο. Αυτή η επίθεση βασίζεται στην τυχαιότητα με την οποία τα αιτήματα των χρηστών ανατίθενται στους Edge Servers, επιτρέποντας στον επιτιθέμενο να συλλέξει περισσότερες IP εισόδου. Η επιτυχία της συγκεκριμένης επίθεσης εξαρτάται από τον αριθμό των διευθύνσεων IP που καταφέρνει να εντοπίσει. Θεωρητικά, ο αριθμός των αιτημάτων που απαιτούνται για την ανακάλυψη n Edge Servers είναι της τάξης O(n log(n)) [37]. Ωστόσο, στην πράξη, ο ακριβής αριθμός των Edge Servers ενός CDN δεν είναι γνωστός, γεγονός που καθιστά δύσκολο για έναν επιτιθέμενο να εκτιμήσει πόσα αιτήματα πρέπει να υλοποιήσει. Αξίζει να σημειωθεί πώς τέτοια επίθεση δεν θα λειτουργήσει εάν το CDN χρησιμοποιεί request routing βασισμένη σε anycast. Στην περίπτωση αυτή, όλοι οι Edge Servers μοιράζονται την ίδια διεύθυνση IP, γεγονός που εμποδίζει τον επιτιθέμενο να συλλέξει μοναδικές IP και να στοχεύσει συγκεκριμένους Edge Servers. Δυο μέθοδοι αντιμετώπισης της παρούσας επίθεσης είναι η Bind-Split στρατηγική και η Proactive Proxy Migration. Η στρατηγική Bind-Split διατηρεί μια σταθερή αντιστοίχιση μεταξύ τελικών χρηστών και Edge Servers, ώστε να περιορίσει τον αριθμό των Edge Servers που μπορεί να εντοπίσει ένας κακόβουλος χρήστης. Ένας τελικός χρήστης παραμένει συνδεδεμένος σε έναν συγκεκριμένο edge server, εκτός εάν αυτός δεχθεί επίθεση. Στην περίπτωση επίθεσης, ο Edge Server τίθεται εκτός λειτουργίας και οι χρήστες του κατανέμονται ισόποσα σε δύο νέους Edge Servers. Αν ο server εξυπηρετούσε μόνο έναν χρήστη, τότε αυτός θεωρείται κακόβουλος εσωτερικός επιτιθέμενος. Ωστόσο, αυτή η προσέγγιση μπορεί να οδηγήσει σε μη ισορροπημένη κατανομή φορτίου μεταξύ των Edge Servers, αφού κάθε χρήστης παραμένει δεσμευμένος σε έναν συγκεκριμένο server. Για να βελτιώσει την κατανομή του φορτίου, η στρατηγική proactive proxy migration αναδιανέμει περιοδικά τους τελικούς χρήστες στους Edge Servers, ακόμη και όταν δεν

υπάρχει επίθεση. Παρόλα αυτά, αυτή η μέθοδος μπορεί να επιφέρει επιπλέον υπολογιστικό κόστος λόγω των συχνών μετακινήσεων των χρηστών μεταξύ των Edge Servers [37].

**Egress Harvest:**
Οι επιθέσεις αυτού του τύπου στοχεύουν στη συλλογή των IP διευθύνσεων που χρησιμοποιούν οι Edge Servers για την επικοινωνία τους με τους Origin Servers. Αποκτώντας αυτές τις πληροφορίες, ένας επιτιθέμενος μπορεί να διακόψει τη σύνδεση του CDN με τον Origin Server. Ένας τρόπος να επιτευχθεί αυτό είναι μέσω μιας crossfire επίθεσης, η οποία αποτελεί μια προηγμένη μορφή DoS επίθεσης. Σε αυτήν την περίπτωση, χιλιάδες bots στέλνουν ελεγχόμενα αιτήματα, προκαλώντας συμφόρηση στις δικτυακές συνδέσεις με την ανακαλυφθείσα διεύθυνση IP του Edge Server. Για να συλλέξει τις IP διευθύνσεις εξόδου, ο επιτιθέμενος πρέπει να προκαλέσει Cache Misses στους Edge Servers. Αυτό συμβαίνει επειδή οι Edge Servers επικοινωνούν με τους Origin Servers μέσω των διευθύνσεων IP εξόδου μόνο όταν δεν υπάρχει αποθηκευμένο περιεχόμενο στην Cache. Έτσι, ένας επιτιθέμενος μπορεί να πραγματοποιήσει την επίθεση λειτουργώντας ταυτόχρονα ως κακόβουλος τελικός χρήστης και ως κακόβουλος ιδιοκτήτης περιεχομένου. Συγκεκριμένα, ο επιτιθέμενος μπορεί να στήσει έναν δικό του Origin Server και να τον καταχωρήσει ώστε να λαμβάνει υπηρεσίες διανομής περιεχομένου από το στοχευμένο CDN. Έχοντας πλήρη έλεγχο του Origin Server, μπορεί να παρακολουθεί τις εισερχόμενες συνδέσεις από τους Edge Servers και να συλλέγει τις αντίστοιχες IP διευθύνσεις εξόδου. Για να προκαλέσει Cache Misses, ο επιτιθέμενος δημιουργεί συνεχώς HTTP αιτήματα με την χρήση query strings με τυχαία values, αναγκάζοντας τους Edge Servers να προωθήσουν τα αιτήματα στον κακόβουλο Origin Server, όπου αυτός καταγράφει τις IP διευθύνσεις εξόδου του CDN. Η αντιμετώπιση αυτής της επίθεσης είναι δύσκολη, καθώς όλες οι δραστηριότητές της θεωρούνται νόμιμες. Ένα CDN μπορεί να μειώσει τη σοβαρότητα της επίθεσης περιορίζοντας τα αιτήματα που περιέχουν query strings. Ωστόσο, αυτός ο περιορισμός μειώνει την ευελιξία του CDN στη διαχείριση δυναμικών αιτημάτων και την προσωρινή αποθήκευση των απαντήσεών τους για νόμιμες ιστοσελίδες. [38]

#### 2.3.2.2 Προκλήσεις Ανακατεύθυνσης και Αντίμετρα

Οι επιτιθέμενοι εκμεταλλεύονται τις ευπάθειες της HTTP-based δρομολόγησης αιτημάτων για να παρακάμψουν τους μηχανισμούς ασφαλείας του CDN και να ανακατευθύνουν τα αιτήματα των τελικών χρηστών σε προορισμούς της επιλογής τους. Η βασική αιτία αυτών των επιθέσεων είναι οι διαφορές στις υλοποιήσεις του HTTP όσον αφορά την ερμηνεία ενός αιτήματος. Ένα CDN χρησιμοποιεί πολλαπλές οντότητες HTTP, όπως Web Application Firewalls (WAFs), Reverse Proxies και Web Servers, για την επεξεργασία των HTTP αιτημάτων. Ωστόσο, όταν αυτές οι οντότητες βρίσκονται στην ίδια ροή δεδομένων, ενδέχεται να ερμηνεύουν το ίδιο αίτημα με διαφορετικούς τρόπους. Οι επιτιθέμενοι εκμεταλλεύονται αυτές τις ασυμβατότητες για να εκτελέσουν επιθέσεις όπως HTTP Smuggling, Multiple Hosts ambiguities και DoS. Μελέτες έχουν αναφέρει ότι CDNs όπως η Alibaba, το Cloudflare, το Cloudfront και το Level3 είναι ευάλωτα σε αυτού του τύπου επιθέσεις [40].

**HTTP Smuggling:**
Οι επιτιθέμενοι αξιοποιούν την τεχνική HTTP Smuggling για να παρακάμψουν τους μηχανισμούς φιλτραρίσματος της κυκλοφορίας και να εξαπολύσουν επιθέσεις όπως Cross-Site Scripting (XSS) και Session Hijacking. Για να εκτελέσουν μια τέτοια επίθεση, οι εισβολείς στέλνουν πολλαπλά HTTP αιτήματα που περνούν μέσα από διαφορετικές οντότητες HTTP. Αυτά τα αιτήματα είναι κατασκευασμένα με τέτοιο τρόπο ώστε, λόγω ασυνεπειών στον τρόπο που οι οντότητες HTTP επεξεργάζονται τα δεδομένα, κάθε οντότητα να αντιλαμβάνεται ένα διαφορετικό σύνολο αιτημάτων. Με αυτήν την προσέγγιση, ο εισβολέας εισάγει/ κρύβει ένα αίτημα HTTP σε μια οντότητα, ενώ οι υπόλοιπες δεν έχουν επίγνωση της ύπαρξής του. Για την αντιμετώπιση αυτής της απειλής, οι οντότητες HTTP πρέπει να εφαρμόζουν αυστηρότερους κανόνες ανάλυσης των HTTP αιτημάτων ώστε να αποφεύγονται οι ασάφειες στην ερμηνεία τους. Ένα αποτελεσματικό μέτρο προστασίας είναι η χρήση ενός WAF που εφαρμόζει αυστηρούς κανόνες ανάλυσης και φιλτράρει ύποπτα αιτήματα. Άλλες στρατηγικές αντιμετώπισης περιλαμβάνουν τη χρήση αποκλειστικά HTTPS για την επικοινωνία και την υποχρεωτική λήξη των συνεδριών των πελατών μετά από κάθε αίτημα, αποτρέποντας έτσι την εκμετάλλευση συνεχιζόμενων συνδέσεων από επιτιθέμενους [40].

**Multiple Host Ambiguities:**
Οι επιτιθέμενοι εκμεταλλεύονται τις ασυνέπειες στην ερμηνεία του header Host στα HTTP 1.1 αιτήματα, προκειμένου να εκτελέσουν επιθέσεις τύπου Multiple Host Ambiguities. Αυτή η τεχνική επιτρέπει σε έναν εισβολέα να παρακάμψει τους μηχανισμούς ασφαλείας και να πραγματοποιήσει περαιτέρω επιθέσεις, όπως Cache Poisoning [42].

Το Host header χρησιμοποιείται για την υποστήριξη Virtual Hosting, επιτρέποντας τη φιλοξενία πολλαπλών Domain Names σε μία μόνο διεύθυνση IP. Συγκεκριμένα, το Host header προσδιορίζει το Domain Name και προαιρετικά την πόρτα TCP του web server, πχ. Host: www.domain1.com:8080.

Υπάρχουν τρεις βασικοί τρόποι με τους οποίους οι επιτιθέμενοι κατασκευάζουν αιτήματα HTTP με ασάφειες στο πεδίο Host:

1. **Χρήση πολλαπλών Host headers:**
   Ένα κακόβουλο request σε αυτή την περιλαμβάνει πολλαπλά Host headers. Παρόλο που το RFC 7230 ορίζει ότι τέτοια αιτήματα πρέπει να απορρίπτονται, πολλές υλοποιήσεις εξακολουθούν να τα επεξεργάζονται, επιλέγοντας αυθαίρετα ένα από τα Host headers.

2. **Χρήση κενών χαρακτήρων στο Host header:**
   Οι επιτιθέμενοι εισάγουν κενά ή tabs μέσα στο πεδίο Host, προκαλώντας ασυνέπειες στην ερμηνεία του από διαφορετικές HTTP οντότητες. Ορισμένοι διακομιστές ενδέχεται να αντιμετωπίσουν ένα τέτοιο Host header ως πολλαπλά διαφορετικά

headers, επιτρέποντας στον επιτιθέμενο να παρακάμψει τους ελέγχους και να χειραγωγήσει τη συμπεριφορά του CDN.

3. **Χρήση απόλυτων URI στα HTTP requests:**
   Το RFC 7230 ορίζει ότι οι Web Servers μπορούν να αποδεχτούν αιτήματα που περιλαμβάνουν απόλυτα URI και να δίνουν προτεραιότητα στο hostname που περιλαμβάνεται στο απόλυτο URI, αντί για το Host header. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτήν τη δυνατότητα για να προκαλέσουν ασάφεια και να κατευθύνουν αιτήματα σε ανεπιθύμητους προορισμούς.

Για την αντιμετώπιση αυτών των επιθέσεων, μπορούν να εφαρμοστούν τα ίδια αντίμετρα που χρησιμοποιούνται και για το HTTP Smuggling.

#### 2.3.2.3 Προκλήσεις DoS και Αντίμετρα

Οι επιτιθέμενοι εκμεταλλεύονται ευπάθειες στο HTTP και το DNS για να μειώσουν την απόδοση του request routing και να εξαπολύσουν επιθέσεις άρνησης υπηρεσιών (DoS) σε επίπεδο εφαρμογής. Σε αυτήν την ενότητα, αναλύονται οι πέντε τύποι επιθέσεων που αξιοποιούν ευπάθειες του HTTP και του DNS για την υλοποίηση επιθέσεων άρνησης υπηρεσίας.

**Forwarding Loop Attack:**
Οι επιθέσεις Forwarding Loop κάνουν κατάχρηση του Host header, παρόμοια με την επίθεση Multiple Host Ambiguities, για να εξαντλήσουν τους πόρους ενός ή περισσότερων CDN. Ένας Edge Server μπορεί να ρυθμιστεί ώστε να προωθεί ένα αίτημα με βάση Host header. Ένας κακόβουλος μπορεί να εκμεταλλευτεί αυτή την ανακατεύθυνση των requests για να αναγκάσει τα CDN να επεξεργάζονται ένα αίτημα επανειλημμένα, ακόμη και επ' αόριστον, οδηγώντας με αυτόν το τρόπο σε DoS. Η επίθεση αρχικά ξεκινάει με τον επιτιθέμενο νοικιάζει και διαμορφώνει Edge Servers με forwarding rules βασισμένους σε Host headers. Στη συνέχεια, δημιουργεί κακόβουλα HTTP requests με τροποποιημένα Host headers, τα οποία ενεργοποιούν τα forwarding rules στους Edge Servers. Αυτό οδηγεί στη δημιουργία ατέρμονων βρόχων προώθησης (forwarding loops) μεταξύ των Edge Servers, προκαλώντας υπερφόρτωση του συστήματος και καταλήγοντας έτσι σε DoS [41] [44].

Υπάρχουν τέσσερις τύποι επιθέσεων Forwarding Loop:

- Self Loop μέσα σε έναν Edge Server
- Ενδο-CDN loop μεταξύ πολλαπλών Edge Servers μέσα σε ένα CDN
- Δια-CDN loop σε πολλαπλά CDN
- CDN Dam Flooding που μπορεί να προκαλέσει ταχύτερους βρόχους εναντίον CDN που υποστηρίζουν HTTP streaming

Τα βασικά αντίμετρα για αυτές τις επιθέσεις είναι τα ακόλουθα:

- **Περιορισμός του request rate με HOST headers:** ένα CDN μπορεί να παρακολουθεί τα HTTP headers και να εφαρμόζει rate limiting είτε με βάση την source IP είτε ανά τελικό χρήστη. Επιπλέον, το CDN μπορεί να εφαρμόσει rate limiting και στα forwarding destinations.

- **Χρήση του HTTP Via header:** με την συγκεκριμένη τεχνική μπορεί να υλοποιηθεί παρακολούθηση των Servers που έχουν ήδη επεξεργαστεί ένα HTTP request. Το πρότυπο HTTP 1.1 καθορίζει το Via Header, το οποία καταγράφει τα Web Proxies που έχουν διαχειριστεί το εκάστοτε request. Σε ένα CDN, κάθε Edge Server που προωθεί ένα request προσθέτει το αναγνωριστικό του στο Via header. Έτσι, ένας Edge Server μπορεί να ανιχνεύσει έναν βρόγχο εάν εντοπίσει το δικό του αναγνωριστικό στη λίστα. Για την αποφυγή εκτεταμένων βρόχων, ένα request απορρίπτεται όταν ο αριθμός των Edge Servers που αναφέρονται στο Via header υπερβαίνει ένα προκαθορισμένο όριο. Ωστόσο, το CDN πρέπει να αποτρέπει την αφαίρεση ή την τροποποίηση του Via header.

- Χρήση του HTTP CDN-Loop header:
  Η Akamai, Fastly και Cloudflare συνεργάστηκαν για να καθιερώσουν το HTTP CDN-Loop header με στόχο την επίλυση των προβλημάτων απόδοσης που σχετίζονται με τη χρήση του Via header για την ανίχνευση βρόγχων. Οι Servers μπορούν πλέον να χρησιμοποιούν το CDN-Loop header αποκλειστικά για την ανίχνευση βρόγχων, ενώ το Via header μπορεί να διατηρεί τη συμβατική του χρήση χωρίς τις επιπτώσεις απόδοσης. Η λειτουργία του CDN-Loop header είναι παρόμοια με αυτήν του Via header: κάθε edge server προσθέτει το αναγνωριστικό του CDN πριν προωθήσει το request, και αν ένας edge server εντοπίσει το δικό του αναγνωριστικό σε ένα HTTP αίτημα ανιχνεύει τον βρόγχο. Ωστόσο, το συγκεκριμένο header είναι αποτελεσματικό μόνο εάν εφαρμόζεται από όλα τα CDNs. Ένα CDN που δεν υιοθετεί αυτό το πρότυπο παραμένει ένα πιθανό σημείο επίθεσης, επιτρέποντας σε εισβολείς να εκμεταλλευτούν αδυναμίες ακόμη και σε CDNs που έχουν εφαρμόσει αυτό το μηχανισμό [44].

**HTTP/2 Amplification:**

Οι επιτιθέμενοι εκμεταλλεύονται την υποστήριξη του HTTP/2 από τα CDNs για να εξαπολύσουν επιθέσεις amplification DoS εναντίον των Origin Servers. Ορισμένα CDNs υποστηρίζουν το HTTP/2 μόνο για τις συνδέσεις μεταξύ των τελικών χρηστών και των Edge Servers, ενώ όλες οι συνδέσεις μεταξύ των Edge Servers και των Origin Servers εξακολουθούν να βασίζονται στο HTTP/1.1, ακόμη και όταν οι Origin Servers υποστηρίζουν το HTTP/2. Αυτό σημαίνει ότι το CDN αναλαμβάνει τη μετατροπή μεταξύ HTTP/2 και HTTP/1.1 προκειμένου να υποστηρίξει τις HTTP/2 συνδέσεις στην άκρη του δικτύου. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτή τη διαδικασία μετατροπής HTTP/2 σε HTTP/1.1 για να

πραγματοποιήσουν μια επίθεση Bandwidth Amplification εναντίον των Origin Servers. Επειδή οι συνδέσεις HTTP/1.1 καταναλώνουν πολλαπλάσιο εύρος ζώνης σε σχέση με τις αντίστοιχες συνδέσεις HTTP/2, ένας επιτιθέμενος μπορεί να αυξήσει σημαντικά τον όγκο της κυκλοφορίας που μεταφέρεται προς τον Oorigin Server, οδηγώντας σε υπερφόρτωση και πιθανή διακοπή της υπηρεσίας. Τα CDNs μπορούν να εξαλείψουν αυτήν την απειλή χρησιμοποιώντας την ίδια έκδοση του HTTP τόσο για την επικοινωνία με τους τελικούς χρήστες όσο και για τη σύνδεση με τους Origin Servers [38].

**Slow Pre-POST:**

Στην συγκεκριμένη επίθεση, οι κακόβουλοι μπορούν να εκμεταλλευτούν τον τρόπο με τον οποίο ορισμένα CDNs διαχειρίζονται την προώθηση POST αιτημάτων, προκειμένου να εκτελέσουν μια αργή επίθεση άρνησης υπηρεσίας (slow HTTP DoS) εναντίον των Origin Servers. Ορισμένα CDNs εφαρμόζουν μια προσέγγιση pre-POST forwarding, όπου προωθούν ένα HTTP POST αίτημα στον Origin Server αμέσως μόλις λάβουν το POST, χωρίς να περιμένουν την πλήρη παραλαβή του σώματος του request.Οι επιτιθέμενοι μπορούν να κάνουν κατάχρηση αυτής της συμπεριφοράς στέλνοντας αργά και εσκεμμένα ελλιπή σώματα POST, προκαλώντας σταδιακή συμφόρηση στον origin server και καταναλώνοντας τους διαθέσιμους πόρους του, με αποτέλεσμα την αδυναμία εξυπηρέτησης νόμιμων αιτημάτων.
Η επίθεση μπορεί να μετριαστεί τόσο στην πλευρά του Origin Server όσο και στην πλευρά του Edge Server. Οι Origin Servers μπορούν να μειώσουν το χρονικό όριο για τη λήψη του σώματος POST, ώστε να αποτρέψουν καθυστερημένες μεταδόσεις δεδομένων από επιτιθέμενους. Παράλληλα, οι Edge Servers μπορούν να αντιμετωπίσουν την επίθεση αποθηκεύοντας ολόκληρο το request προτού το προωθήσουν στον Origin Server, περιορίζοντας έτσι τη δυνατότητα εκμετάλλευσης αυτής της συμπεριφοράς [38].

**Egress Block:**

Οι επιτιθέμενοι μπορούν να απειλήσουν τη διαθεσιμότητα του περιεχομένου εκμεταλλευόμενοι το χαμηλό ρυθμό εναλλαγής διευθύνσεων IP (IP churning) που χρησιμοποιούν ορισμένα CDNs για τις επικοινωνίες τους με τους Origin Servers. Σε πολλές περιπτώσεις, τα CDNs αναθέτουν προβλέψιμες διευθύνσεις IP εξόδου για τη σύνδεση με τους Origin Σervers. Για παράδειγμα, ένα CDN μπορεί να χρησιμοποιεί μία και μόνο διεύθυνση IP εξόδου για το 96% της κυκλοφορίας του προς έναν συγκεκριμένο Origin Server. Ένας επιτιθέμενος μπορεί να συλλέξει αυτές τις στατικές διευθύνσεις IP εξόδου μέσω Harvesting επιθέσεων και στη συνέχεια να τις στοχεύσει με DoS επιθέσεις. Με αυτόν τον τρόπο, μπορεί να διακόψει την επικοινωνία του CDN με τον Origin Server, καθιστώντας το περιεχόμενό του μη διαθέσιμο στους τελικούς χρήστες [38] [45]. Τα CDN μπορούν να μετριάσουν αυτήν την επίθεση εφαρμόζοντας μια πιο απρόβλεπτη στρατηγική εκχώρησης egress IP διευθύνσεων. Για παράδειγμα, μπορούν να εκχωρούν μεγαλύτερο αριθμό egress διευθύνσεων IP σε έναν Origin Σerver και να τις αλλάζουν πιο συχνά, καθιστώντας πιο δύσκολη τη χαρτογράφηση και στόχευσή τους από τους επιτιθέμενους.

**Redirection Hijacking:**
Οι επιτιθέμενοι μπορούν να εισαγάγουν κατασκευασμένες εγγραφές DNS σε Name Σervers μέσω επίθεσης DNS Cache Poisoning, προκειμένου να ανακατευθύνουν τα αιτήματα των τελικών χρηστών προς έναν συγκεκριμένο Edge Server. Μια μαζική εισροή αυτών των requests μπορεί να οδηγήσει σε υπερφόρτωση του στοχευμένου Edge Server, καθιστώντας τον μη διαθέσιμο. Επιπλέον, ένας επιτιθέμενος μπορεί να ακυρώσει τα παραβιασμένα requests ανακατευθύνοντάς τα προς offline Edge Servers. Για να το πετύχει αυτό, συλλέγει τις διευθύνσεις IP των Edge Servers, παρακολουθεί τη διαθεσιμότητά τους, π.χ μέσω ping),και στη συνέχεια δηλητηριάζει τους Name Servers με κατασκευασμένες εγγραφές που κατευθύνουν τα αιτήματα σε μη διαθέσιμους Edge Servers. Αυτό έχει ως αποτέλεσμα την αποτυχία εξυπηρέτησης των χρηστών.

Η επίθεση DNS cache poisoning εκμεταλλεύεται μια ευπάθεια στην αυθεντικοποίηση της διαδικασίας DNS Name Resolution, επιτρέποντας την εισαγωγή ψευδών DNS εγγραφών στη μνήμη Cache ενός Name Server. Μέχρι να λήξουν αυτές οι δηλητηριασμένες εγγραφές, οι επιτιθέμενοι μπορούν να ανακατευθύνουν τα αιτήματα των τελικών χρηστών προς διευθύνσεις IP της επιλογής τους. Όταν ένας Resolving Name Server λαμβάνει ένα DNS query και δεν διαθέτει αποθηκευμένη απάντηση στη Cache του, ζητά την πληροφορία από έναν άλλο Name Server. Ο πρώτος Name Server χρησιμοποιεί έναν 16-bit Transaction Identifier για να επαληθεύσει την εγκυρότητα των απαντήσεων που λαμβάνει από τον δεύτερο Name Server. Εάν ένας επιτιθέμενος μαντέψει σωστά την τιμή αυτού του αναγνωριστικού και απαντήσει ταχύτερα από τον έγκυρο Name Server, μπορεί να δηλητηριάσει τη μνήμη Cache του Resolving Name Server, αποθηκεύοντας ψευδείς πληροφορίες και ανακατευθύνοντας έτσι την κυκλοφορία προς κακόβουλους προορισμούς [47].

Η επίθεση DNS cache poisoning αποτελεί τον βασικό μηχανισμό της απειλής Redirection Hijacking. Η πρόληψη του DNS Cache Poisoning συμβάλλει στην αντιμετώπιση αυτής της απειλής. Για τον περιορισμό του κινδύνου, μπορεί να χρησιμοποιηθεί η τεχνική Request Remapping στους Edge Servers. Τα βασικά αντίμετρα για την αντιμετώπιση του DNS Cache Poisoning είναι τα ακόλουθα [48][49][50]:

- **DNSSEC**: Το DNS Security Extension (DNSSEC) δημιουργεί μια αλυσίδα εμπιστοσύνης μεταξύ των Name Servers, η οποία τους επιτρέπει να αυθεντικοποιούν τις απάντήσεις DNS. Οι απαντήσεις DNS πρέπει να είναι ψηφιακά υπογεγραμμένες, δηλαδή, PKI, για να εγγυηθούν ότι οι αποκρίσεις DNS προέρχονται από νόμιμους Name Servers.

- **Wildcard DNS**: Ένας Name Server περιλαμβάνει μια τυχαία συμβολοσειρά στο ερώτημά του DNS για να αυξήσει την εντροπία των ερωτημάτων του DNS, καθιστώντας έτσι δύσκολη την εικασία έγκυρων DNS απαντήσεων.

Δεκαέξι δημοφιλή CDNs, συμπεριλαμβανομένων των Cloudflare, Akamai και Limelight, έχουν αναγνωριστεί ως ευάλωτα σε αυτήν την επίθεση[47].

### 2.3.3 Προκλήσεις Ασφάλειας σε Επίπεδο Origin Server και Αντίμετρα

Οι βασικότερες προκλήσεις ασφάλειας των Origin Server διαχωρίζονται στις απειλές σε επίπεδο εφαρμογής, σε αυτές που πηγάζουν από την αποκάλυψη των IP διευθύνσεων των Origin Servers καθώς και στις απειλές που προκύπτουν από την κατάχρηση των Origin Servers.

#### 2.3.3.1 Προκλήσεις σε Application Layer – Επίπεδο 7 και Αντίμετρα

Το Authentication στο διαδίκτυο βασίζεται στο SSL/TLS. Το SSL/TLS είναι συνδεδεμένο με μια υποδομή δημοσίου κλειδιού (Public Key Infrastructure - PKI), παρέχοντας ένα σαφές μοντέλο ταυτοποίησης: η Alice διαθέτει ένα πιστοποιητικό που συνδέει τον Bob με ένα δημόσιο κλειδί και η απομακρυσμένη οντότητα πρέπει να είναι πράγματι ο Bob και να αποδείξει ότι γνωρίζει το ιδιωτικό του κλειδί. Το SSL/TLS χρησιμοποιεί παρόμοιο μηχανισμό για να εξασφαλίσει την εμπιστευτικότητα των μηνυμάτων που ανταλλάσσονται μεταξύ της Alice και του Bob. Και οι δύο αυτές λειτουργίες, αυθεντικοποίηση και εμπιστευτικότητα, βασίζονται στην υπόθεση ότι ο Bob είναι ο μόνος που γνωρίζει το ιδιωτικό του κλειδί.

**SSL/TLS man-in-the-middle:**
Το πρόβλημα SSL/TLS Man-in-the-Middle αναφέρεται στο γεγονός ότι η παρουσία των Edge Servers στις συνδέσεις SSL/TLS μεταξύ των τελικών χρηστών και των Origin Servers διακόπτει την end-to-end εμπιστευτικότητα. Οι ιδιοκτήτες περιεχομένου συχνά μοιράζονται τα Private Keys τους με τα CDNs ώστε να μπορούν να επιθεωρούν την κίνηση και να λειτουργούν ως proxy για τις SSL/TLS συνδέσεις, γεγονός που παραβιάζει τη θεμελιώδη αρχή της μυστικότητας των κλειδιών και καθιστά τους Edge Servers δυνητικούς man-in-the-middle επιτιθέμενους. Για την αντιμετώπιση αυτής της απειλής, έχουν αναπτυχθεί τεχνικές όπως το Cloudflare Keyless SSL, το οποίο εισάγει έναν key server στην πλευρά του Origin Server για να επιτρέπει ασφαλή διαχείριση των κλειδιών χωρίς να τα εκθέτει στους Edge Servers. Ο Edge Server συνδέεται στον Key server, αυθεντικοποιείται μέσω πιστοποιητικού και λαμβάνει ένα αποκρυπτογραφημένο μυστικό, το οποίο επιτρέπει τη δημιουργία ενός κοινού session key με τον τελικό χρήστη. Παρόμοια, το Phoenix χρησιμοποιεί enclaves, δηλαδή απομονωμένες περιοχές μνήμης σε ένα Trusted Execution Environment μέσω του Intel SGX, ώστε να διασφαλίζει ασφαλείς TLS συνδέσεις χωρίς να εκθέτει τα private και session keys. Μια εναλλακτική προσέγγιση είναι η άμεση δημιουργία συνδέσεων SSL/TLS μεταξύ τελικών χρηστών και Edge Servers, παρακάμπτοντας πλήρως τους Origin Servers, με τους ιδιοκτήτες περιεχομένου να παρέχουν υπηρεσίες που επιτρέπουν στους τελικούς χρήστες να αυθεντικοποιούν τους Edge Servers, βελτιώνοντας έτσι την ασφάλεια και την εμπιστευτικότητα των συνδέσεων.

### 2.3.3.2 Προκλήσεις Αποκάλυψης του Origin Server και Αντίμετρα

Ένα CDN λειτουργεί ως προστατευτική ασπίδα για τους Origin Servers, απορροφώντας πολλές απειλές ασφαλείας που τους στοχεύουν. Ωστόσο, οι επιτιθέμενοι μπορούν να παρακάμψουν αυτήν την προστασία και να επιτεθούν απευθείας στους Origin Servers, εκμεταλλευόμενοι τις πραγματικές τους IP διευθύνσεις, για αυτό το λόγο είναι απαραίτητη η αντιμετώπιση των απειλών που θέτουν την μυστικότητα των IP διευθύνσεων αυτών σε κίνδυνο.

**Static origin addresses:**
Η χρήση στατικών διευθύνσεων IP για τους Origin Servers τους καθιστά ευάλωτους σε έκθεση. Όταν οι Origin Servers εκτίθενται προσωρινά στους τελικούς χρήστες, π.χ στις περιπτώσεις που ένα CDN διακόπτει την υπηρεσία του για συντήρηση, ένας κακόβουλος μπορεί να συλλέξει και να διατηρήσει τις διευθύνσεις IP του Origin Server. Επιπλέον, υπάρχουν οργανισμοί που διατηρούν βάσεις δεδομένων με εγγραφές DNS. Αντίστοιχα κακόβουλοι μπορούν να αναζητήσουν σε αυτές τις βάσεις δεδομένων ένα ιστορικό των Origin Domain Names και των διευθύνσεων IP τους και να εκμεταλλευτούν τις στατικές διευθύνσεις IP2 Η αλλαγή των διευθύνσεων IP των Origin Servers και των εγγραφών DNS μπορεί να προλάβει αυτήν την επίθεση. Όταν ένα CDN προστατεύει τους Origin Σervers, οι εγγραφές DNS πρέπει να αλλάξουν σε διευθύνσεις CDN και οι νέες εγγραφές DNS δεν πρέπει να εκθέτουν τις διευθύνσεις του εκάστοτε Origin Server. Οι Origin Server Ips πρέπει να αλλάξουν ώστε να διαφέρουν από το ιστορικό IP που συλλέχθηκε πριν προστατευτούν από ένα CDN ή κατά τη διάρκεια της προσωρινής αδράνειας ενός CDN [153][154][157].

**Services by origin servers:**
Οι IP διευθύνσεις των υπηρεσιών που παρέχονται απευθείας από τους Origin Servers μπορούν να εκθέσουν τις διευθύνσεις του. Συνήθως, οι Origin Servers εξυπηρετούν απευθείας υπηρεσίες, όπως mail, FTP και SSH χωρίς να χρησιμοποιούν CDN. Επομένως, οι κακόβουλοι μπορούν να συλλέξουν Origin IP διευθύνσεις από εγγραφές DNS αυτών των υπηρεσιών. Οι κάτοχοι περιεχομένου χρησιμοποιούν επίσης κρυφά sub-domains για ορισμένες υπηρεσίες, όπως το SSH. Χρησιμοποιώντας μια επίθεση λεξικού, ένας επιτιθέμενος μπορεί να μαντέψει και να υποβάλει ερωτήματα στα κρυφά sub-domains για να συλλέξει τις Origin Server IPs. Αυτή η ευπάθεια μπορεί να μετριαστεί χρησιμοποιώντας Port Forwarding. Για υπηρεσίες που εξυπηρετούνται απευθείας από τους Origin Servers, οι κάτοχοι περιεχομένου μπορούν να χρησιμοποιήσουν Edge Servers ως Proxies που λαμβάνουν και προωθούν αιτήματα. Οι εγγραφές DNS που σχετίζονται με αυτές τις υπηρεσίες πρέπει επίσης να δείχνουν στους Edge Servers. Κατά συνέπεια, οι Edge Servers λαμβάνουν πρώτα αιτήματα για αυτές τις υπηρεσίες και τα προωθούν στους Origin Servers χωρίς να εκθέτουν τις IP διευθύνσεις των Origin. Μια άλλη προσέγγιση που μπορεί να αξιοποιηθεί από τους Origin Servers είναι να εξυπηρετούν μόνο αιτήματα που προέρχονται από αξιόπιστες διευθύνσεις. Για να το εφαρμόσουν αυτό, οι κάτοχοι περιεχομένου

εγκαθιστούν Firewalls για να επιθεωρούν και να βάζουν σε whitelist την εισερχόμενη κίνηση στους Origin Servers [59].

**Leakage in contents:**
Η συγκεκριμένη πρόκληση σχετίζεται με τη διαρροή περιεχομένου και αφορά κυρίως την αποκάλυψη των διευθύνσεων IP των origin servers μέσω ευάλωτου Web Content και την εκμετάλλευση των Pingback services. Τα ευάλωτα Web Contents, όπως αρχεία ρυθμίσεων, verbose pages και αρχεία καταγραφής, μπορεί να περιέχουν τυχαία τις διευθύνσεις IP των κατόχων περιεχομένου μέσα σε HTML αρχεία, εκθέτοντάς τα σε πιθανές επιθέσεις. Επιπλέον, οι επιτιθέμενοι μπορούν να αξιοποιήσουν τις υπηρεσίες Pingback για να συλλέξουν τις IP των Origin Servers. Με την χρήση Pingback, οι κάτοχοι περιεχομένου μπορούν να ελέγξουν ένα third party σύνδεσμο προς το περιεχόμενο τους. Λαμβάνοντας την ειδοποίηση για το third party σύνδεσμο, ο Origin Server ξεκινάει μία επικοινωνία με το third party για να επαληθεύσει την εγκυρότητα αυτού του συνδέσμου. Ένας επιτιθέμενος μπορεί να εξάγει την IP του Origin Server από αυτή την διαδικασία. Για τη μείωση αυτών των κινδύνων, είναι κρίσιμη η επιθεώρηση ευαίσθητων αρχείων και του source code, ο περιορισμός της πρόσβασης σε αυτά και η εφαρμογή μέτρων όπως η απόρριψη των αιτημάτων Pingback στο Edge επίπεδο ή η πλήρης απενεργοποίηση της υπηρεσίας Pingback στους Origin Servers [56][59].

**Residual name resolution:**
Το συγκεκριμένο φαινόμενο αφορά τη διαρροή διευθύνσεων IP των Origin Servers κατά τη διάρκεια δυναμικών αλλαγών, όπως η παύση ή η τερματισμός των υπηρεσιών τους με CDN. Όταν οι υπηρεσίες είναι ενεργές, οι Name Servers είναι υπό την λειτουργία του CDN και ανακατευθύνουν τα αιτήματα περιεχομένου στους Edge Servers του CDN. Εάν η υπηρεσία διανομής περιεχομένου τεθεί σε παύση ή τερματιστεί, οι Name Servers ενδέχεται να διατηρήσουν ορισμένα σχετικά DNS records που αναλύουν τα requests στις διευθύνσεις IP του Origin Server αντί για τους Edge Servers. Για να αντιμετωπιστεί αυτή η απειλή, ένα CDN μπορεί να σταματήσει να ανταποκρίνεται σε αιτήματα περιεχομένου για υπηρεσίες που έχουν τεθεί σε παύση ή έχουν τερματιστεί. Εναλλακτικά, πριν από τον τερματισμό μιας υπηρεσίας, ο content owner μπορεί να ρυθμίσει το παλιό CDN ώστε να ανακατευθύνει τα αιτήματα σε ένα domain name που ανήκει στο νέο CDN, με σκοπό να μην αποκαλύπτεται κάποια Origin Server IP [55].

#### 2.3.3.3 Προκλήσεις Κατάχρησης του Origin Server

Τα CDN προσφέρουν ένα ευέλικτο σύνολο επιλογών που επιτρέπουν στους κατόχους περιεχομένου να διαμορφώσουν τη διαδικασία διανομής του περιεχομένου τους. Για παράδειγμα, οι κάτοχοι περιεχομένου μπορούν να καθορίσουν τους Origin Server, τα domain names, τις διευθύνσεις IP και τους αριθμούς θυρών των Origin Servers, καθώς και τις πολιτικές Caching και Forwarding. Ωστόσο, πολλά CDN δεν επαληθεύουν τις καθορισμένες ρυθμίσεις, όπως το αν ο κάτοχος περιεχομένου είναι ο πραγματικός

ιδιοκτήτης των Origin Servers. Αυτό το κενό επιτρέπει σε κακόβουλους χρήστες να διαμορφώσουν και να εκμεταλλευτούν τα CDNs για κακόβουλες δραστηριότητες [43][61]].

**Origin address abuse:**

Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί τις ρυθμίσεις των domain names και των διευθύνσεων των Origin Servers για να παρακάμψει γεωγραφικούς ή περιεχομενικούς περιορισμούς που επιβάλλουν οι ιδιοκτήτες περιεχομένου ή συγκεκριμένες περιοχές. Για παράδειγμα, πλατφόρμες όπως το Pandora Media και το Netflix επιβάλλουν γεωγραφικούς περιορισμούς στην παροχή των υπηρεσιών τους, προσφέροντας περιεχόμενο μόνο σε συγκεκριμένες χώρες ή παρέχοντας διαφορετικά σύνολα περιεχομένου ανάλογα με την τοποθεσία του χρήστη. Επιπλέον, σε ορισμένες χώρες, η πρόσβαση σε ευαίσθητο περιεχόμενο είναι περιορισμένη. Ένας κακόβουλος χρήστης, ενεργώντας ως ψευδής κάτοχος περιεχομένου, μπορεί να παρακάμψει αυτούς τους περιορισμούς εκμεταλλευόμενος τις ρυθμίσεις διαμόρφωσης των domain names και των διευθύνσεων IP των Origin Servers. Ο επιτιθέμενος μπορεί να ρυθμίσει Edge Servers ώστε να αιτούνται δεδομένα από Origin Servers που περιέχουν περιορισμένο περιεχόμενο. Παρά τους υφιστάμενους περιορισμούς, οι Edge Servers έχουν πρόσβαση στο περιεχόμενο των Origin Servers και μπορούν να το διανέμουν στους τελικούς χρήστες, παρακάμπτοντας έτσι τους γεωγραφικούς περιορισμούς. Για να αποτρέψουν αυτήν την ευπάθεια, τα CDNs μπορούν να εφαρμόσουν μηχανισμούς επικύρωσης της κυριότητας των Origin Servers. Μια προσέγγιση είναι η τεχνική Origin Pinning, όπου το CDN απαιτεί από τον ιδιοκτήτη περιεχομένου να παρέχει τόσο τη διεύθυνση IP όσο και το domain name του Origin Server και να ανεβάσει ένα ειδικό αρχείο σε αυτόν. Το CDN παρακολουθεί συνεχώς αυτό το IP-domain ζεύγος και την ύπαρξη του αρχείου, τερματίζοντας την υπηρεσία και απαιτώντας νέα διαδικασία επικύρωσης σε περίπτωση ανωμαλίας. Ωστόσο, η εφαρμογή του Origin Pinning απαιτεί περαιτέρω διερεύνηση ως προς τη χρηστικότητά του για τους ιδιοκτήτες περιεχομένου. Επιπλέον, η ανάγκη για ανέβασμα αρχείων στους Origin Servers μπορεί να δημιουργήσει νέες ευπάθειες και απειλές ασφαλείας, οι οποίες πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό των αντίμετρων.

**Origin port abuse:**

Η ρύθμιση για τον αριθμό των θυρών για τους origin servers μπορεί να επιτρέψει σε έναν επιτιθέμενο να εκτελέσει κρυφές επιθέσεις Port Scanning και DoS εναντίον νόμιμων Origin Servers. Ένας επιτιθέμενος μπορεί να ρυθμίσει ένα CDN ώστε να σαρώνει τις θύρες των Origin Servers. Σε περίπτωση σφάλματος, το CDN δημιουργεί μηνύματα σφάλματος που αποκαλύπτουν την κατάσταση των θυρών που σαρώθηκαν, δίνοντας πολύτιμες πληροφορίες στον επιτιθέμενο. Επιπλέον, το CDN μπορεί να ρυθμιστεί ώστε να εκτελέσει επίθεση DoS χρησιμοποιώντας Edge Servers που ανοίγουν πολλαπλές ταυτόχρονες συνδέσεις προς έναν Origin Server. Εάν ο αριθμός των συνδέσεων υπερβεί το μέγιστο όριο που μπορεί να διαχειριστεί ο Origin Server, αυτός καθίσταται μη διαθέσιμος. Οι στρατηγικές μετριασμού που εφαρμόζονται για την αποτροπή κατάχρησης των διευθύνσεων IP των Origin Servers είναι επίσης αποτελεσματικές για την αντιμετώπιση της κατάχρησης θυρών.

Επιπλέον, το whitelisting των επιτρεπόμενων θυρών για τους Origin Servers μπορεί να περιορίσει σημαντικά αυτήν την απειλή.

## 2.4 WAF και BOT Προστασία στο Content Delivery Network (CDN)

Τα Web Application Firewall (WAF) και τα συστήματα Bot προστασίας διαδραματίζουν κρίσιμο ρόλο στη σύγχρονη ασφάλεια δικτύων καθώς προστατεύουν τις διαδικτυακές εφαρμογές από επιθέσεις όπως SQL injection, Cross-Site Scripting (XSS), Distributed Denial of Service (DDoS) και κακόβουλη δραστηριότητα bots [62]. Με τη χρήση κατανεμημένων Edge Servers, τα CDNs όχι μόνο επιταχύνουν την διανομή περιεχομένου, αλλά φιλτράρουν και επιθεωρούν την εισερχόμενη κίνηση, αποκλείοντας κακόβουλα αιτήματα πριν φτάσουν στους Origin Servers[63].

Τα WAF των CDN χρησιμοποιούν πολλαπλές τεχνικές ανίχνευσης για την ανάλυση και αποκλεισμό κακόβουλης κίνησης, οι κύριες εκ των οποίων είναι οι κάτωθι:

- Η Signature Based Detection τεχνική, η οποία κάνει match την κίνηση με γνωστά μοτίβα επιθέσεων.
- Η Behavioral Analysis τεχνική, σύμφωνα με την οποία υλοποιείται ανάλυση συμπεριφοράς της κίνησης για την ανίχνευση ανωμαλιών.
- Η Machine Learning τεχνική, η οποία βελτιώνει συνεχώς τις δυνατότητες ανίχνευσης κακόβουλης κίνησης, μέσω της συνεχής βελτίωσης των μοντέλων ανίχνευσης, επιτρέποντας με αυτό τον τρόπο την ανίχνευση κακόβουλης κίνησης χωρίς κάποιο γνωστό μοτίβο επίθεσης.

Τα συστήματα προστασίας από Bots εστιάζουν στον εντοπισμό και τη διαχείριση της κίνησης από Bots, διακρίνοντας μεταξύ νόμιμων Bots (π.χ. search engine crawlers) και κακόβουλων Bots (π.χ. content scrapers και credential stuffing attacks). Αυτά τα συστήματα χρησιμοποιούν τεχνικές όπως Fingerprinting, Behavioral Analysis και CAPTCHA Challenges για την αναγνώριση και αποκλεισμό κακόβουλων Bots.

Τα WAF των CDN εφαρμόζουν πολυεπίπεδη προστασία, πραγματοποιώντας real-time ανάλυση HTTP/HTTPS κίνησης με τη χρήση προρυθμισμένων κανόνων ασφαλείας που ενημερώνονται συνεχώς βάσει των τελευταίων κυβερνοαπειλών. Οι κανόνες αυτοί καλύπτουν επιθέσεις όπως SQL injection, Cross Site Scripting (XSS) και Remote Code Execution (RCE). Ο συνδυασμός Machine Learning και Behavioral Analysis επιτρέπει την ανίχνευση ανώμαλων μοτίβων κίνησης, ακόμα και αγνώστων επιθέσεων, ενισχύοντας την αποτελεσματικότητα της άμυνας. Επιπλέον, τα WAF διαθέτουν προσαρμοστικές δυνατότητες μάθησης, μπορούν δηλαδή να προσαρμόζονται δυναμικά σε νέες απειλές και να βελτιστοποιούν συνεχώς τις στρατηγικές ασφαλείας τους[64].

Παρά τις προηγμένες δυνατότητες ασφαλείας που παρέχουν τα WAF, οι επιτιθέμενοι συνεχίζουν να αναπτύσσουν τεχνικές για να παρακάμπτουν αυτή την προστασία. Για παράδειγμα, οι επιτιθέμενοι μπορούν να διασπούν κακόβουλα requests σε μικρότερα τμήματα ώστε να αποφύγουν την ανίχνευση, να χρησιμοποιούν τεχνικές όπως Base64 encoding και URL encoding, καθώς και να προσομοιώνουν φυσιολογική συμπεριφορά χρήστη για να αποφύγουν τον εντοπισμό από τα WAF [65].

Τα συστήματα Bot προστασίας στα CDN, όπως αυτά που χρησιμοποιεί η Cloudflare, εφαρμόζουν προηγμένες μεθόδους ανίχνευσης για να διακρίνουν τους πραγματικούς χρήστες από τα Bots. Η ανάλυση διευθύνσεων IP είναι μια βασική τεχνική, καθώς επιτρέπει την απόδοση Trust Scores με βάση τη διαφοροποίηση μεταξύ Residential, Mobile και Data Center IP διευθύνσεων σχετικά με τα αιτήματα που παρατηρούνται σε υψηλή συχνότητα. Η τεχνική TLS Handshake Fingerprinting χρησιμοποιείται για την αναγνώριση των non-browser clients μέσω μοναδικών αποτυπωμάτων που παράγονται κατά τη διάρκεια της TLS χειραψίας. Η ανάλυση των HTTP headers εντοπίζει ασυνέπειες ή ανωμαλίες στους headers όπως User-Agent, Accept-Language και Cookie, που μπορεί να υποδηλώνουν δραστηριότητα Bots. Επιπλέον, το JavaScript Fingerprinting εκτελεί JavaScript challenges για τη συλλογή πληροφοριών σχετικά με το περιβάλλον του Client, τις δυνατότητες του Browser και το υλικό της συσκευής, βοηθώντας με αυτό τον τρόπο στον εντοπισμό αυτοματοποιημένων εργαλείων. Η Behavioral Analysis παρακολουθεί τα μοτίβα πλοήγησης και τη συχνότητα requests για τον εντοπισμό ανώμαλης συμπεριφοράς, καθώς η υπερβολική συχνότητα αιτημάτων μπορεί να μειώσει το Trust Score και να οδηγήσει σε Block.

Οι επιτιθέμενοι χρησιμοποιούν διάφορες τεχνικές για να παρακάμψουν αυτές τις μεθόδους ανίχνευσης. Η χρήση High-Trust Proxies είναι μια κοινή τακτική, όπου επιλέγονται αξιόπιστοι Residential ή Mobile Proxies που εναλλάσσονται τακτικά για να αποφεύγεται ο εντοπισμός μέσω διευθύνσεων IP. Η προσομοίωση της TLS χειραψίας και των HTTP headers δημοφιλών Browsers επίσης μειώνει την πιθανότητα ανίχνευσης. Αξίζει επίσης να σημειωθεί πώς, ως απάντηση στο JavaScript Fingerprinting, οι επιτιθέμενοι χρησιμοποιούν Headless Browsers (όπως Puppeteer και Selenium) για την αυτοματοποίηση των Browser λειτουργιών και την επίλυση JavaScript challenges, αξιοποιώντας plugins όπως το puppeteer-stealth για να αποκρύψουν τη συμπεριφορά αυτοματοποίησης. Οι τεχνικές διαχείρισης συνεδριών συνδυάζουν Headless Browsers με HTTP Clients (όπως το FlareSolverr), επιτρέποντας την επαναχρησιμοποίηση Session Values ώστε να μειωθεί η ανάγκη επίλυσης JavaScript προκλήσεων συνεχώς. Επιπλέον, οι επιτιθέμενοι προσομοιώνουν φυσιολογικά μοτίβα πλοήγησης, συμπεριλαμβανομένης της τυχαιοποίησης των χρονικών διαστημάτων μεταξύ requests, της αλλαγής viewport sizes και της μίμησης αλληλεπιδράσεων χρήστη με σκοπό της διατήρηση υψηλού Trust Score και την μείωση του κινδύνου ανίχνευσης [66].

## 2.5 Αναγνώριση της WAF και BOT Προστασίας στα Content Delivery Networks (CDNs)

Η ανιχνευσιμότητα των WAF και BOT μηχανισμών μπορεί να διαφέρει ανάλογα με τις ρυθμίσεις που έχουν υλοποιηθεί στο εκάστοτε hostname που εξυπηρετεί το κάθε CDN. Αξίζει επίσης να σημειωθεί πώς, οι WAF και BOT προστασίες επικαλύπτουν η μία την άλλη σε πολλές περιπτώσεις, συνεπώς δεν μπορούν να διακριθούν πλήρως από την πλευρά του Client [14].

**HTTP Title:**
Πολλοί πάροχοι CDN, όσον αφορά τις WAF και Bot προστασίες επιστρέφουν προεπιλεγμένες σελίδες σφαλμάτων. Για παράδειγμα, ιστοσελίδες που χρησιμοποιούν το Cloudflare εμφανίζουν σελίδες σφάλματος με τίτλους όπως "Attention Required!| Cloudflare", ενώ στις ιστοσελίδες που χρησιμοποιούν Akamai, επιστέφεται “Access Denied και ένα Error Code”.

**HTTP Body:**
Για την ακρίβεια της ανίχνευσης, εξετάζεται επίσης το περιεχόμενο του σώματος των σελίδων σφαλμάτων. Για παράδειγμα, ιστοσελίδες που χρησιμοποιούν Akamai ενδέχεται να επιστρέφουν σελίδες σφάλματος με τίτλο "Access Denied". Ωστόσο, επειδή αυτός ο τίτλος μπορεί να μοιάζει με εκείνον που επιστρέφουν ορισμένοι HTTP servers για σφάλματα 403, ελέγχεται και το περιεχόμενο του σώματος της σελίδας. Αν περιλαμβάνει τη φράση "errors.edgesuite.net" αυτό αποτελεί ένδειξη ότι η ιστοσελίδα χρησιμοποιεί Akamai WAF.

**HTTP Headers:**
Οι HTTP headers αποτελούν επίσης μέρος του μηχανισμού ανίχνευσης. Για παράδειγμα, αν η κεφαλίδα "x-amzn-waf-action" εμφανίζεται σε μια HTTP response, αυτό συνήθως υποδηλώνει τη χρήση του AWS.

Ακολουθούν αναγνωριστικά της WAF & BOT προστασίας σχετικά με τα TOP CDN σήμερα [14]:

| Title | Body | Headers | Features |
|---|---|---|---|
| Just a moment... | / | CF-RAY | Cloudflare WAF |
| Attention Required! \| Cloudflare | / | / | Cloudflare WAF |
| Access denied | Cloudflare Ray ID | CF-RAY | Cloudflare WAF |
| / | / | one of the following: cf-chl-out cf-mitigated | Cloudflare WAF |

*Table 3: Αναγνώριση WAF & BOT Προστασίας – Cloudflare*

| Title | Body | Headers | Features |
|---|---|---|---|
| ERROR: The request could not be satisfied | Generated by cloudfront (CloudFront) | / | AWS WAF |
| Human Verification | awswaf.com | / | AWS WAF |
| / | / | x-amzn-waf-action | AWS WAF |

*Table 4: Αναγνώριση WAF & BOT Προστασίας – CloudFront*

| Title | Body | Headers | Features |
|---|---|---|---|
| Access Denied | errors.edgesuite.net | / | Akamai WAF |

*Table 5: Αναγνώριση WAF & BOT Προστασίας – AKAMAI*

## 2.6 Akamai Content Delivery Network (CDN) και Παροχή Ασφάλειας

Η Akamai προσφέρει μια ευρεία γκάμα λύσεων για τη βελτιστοποίηση της απόδοσης, της διανομής περιεχομένου και της ασφάλειας στο διαδίκτυο. Στον τομέα της ασφάλειας, οι δύο βασικές λύσεις της είναι το Application and API Protector, το οποίο παρέχει προηγμένη προστασία επιπέδου Layer 7 για web applications και APIs, και το Prolexic, μια λύση Layer 3 που εξειδικεύεται στην προστασία από DDoS επιθέσεις μεγάλης κλίμακας. Το Application and API Protector αξιοποιεί μηχανισμούς όπως WAF, bot management και API security για την ανίχνευση και την αποτροπή κακόβουλων αιτημάτων, ενώ το Prolexic προσφέρει ισχυρή άμυνα ενάντια σε δικτυακές επιθέσεις (volumetric, protocol-based και application-layer DDoS attacks), διασφαλίζοντας τη διαθεσιμότητα κρίσιμων υπηρεσιών.

### 2.6.1 Application and API Protector (AAP) – Layer 7

Το Akamai App & API Protector είναι μια ολοκληρωμένη λύση ασφάλειας που παρέχεται από την Akamai και ενοποιεί προηγμένες τεχνολογίες προστασίας, συμπεριλαμβανομένων Web Application Firewall (WAF), προστασίας από κακόβουλων Bots, προστασίας των APIs και αντιμετώπισης επιθέσεων DDoS. Αναγνωρίζεται ως κορυφαία λύση WAAP και προσφέρει δυναμική ανίχνευση και εξουδετέρωση απειλών προστατεύοντας έτσι ολόκληρη την ψηφιακή υποδομή ενός οργανισμού από πολυδιάστατες επιθέσεις [67].

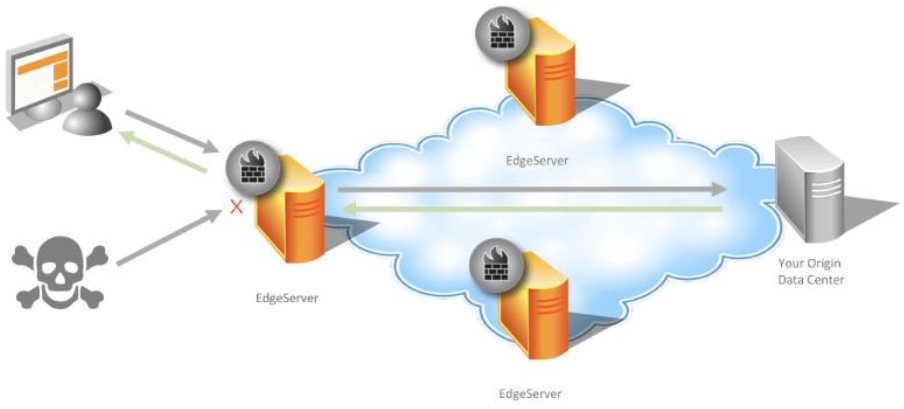


*Figure 11: Application and API Protector, https://techdocs.akamai.com/cloud-security/docs/app-api-protector*

Το Adaptive Security Engine της Akamai αποτελεί τον πυρήνα της προστασίας, επιτρέποντας την αυτόματη ενημέρωση των μηχανισμών ασφαλείας και την εφαρμογή προσαρμοσμένων πολιτικών. Χρησιμοποιεί Machine Learning, Real-Time Threat Intelligence και αυτοματοποιημένη ανάλυση για την ανίχνευση και το blocking επιθέσεων. Αξίζει να σημειωθεί πώς ξεχωρίζει για τη δυνατότητά του να:

- Αναλύει κάθε HTTP request σε πραγματικό χρόνο στο Edge για ταχύτερη ανίχνευση απειλών.
- Μαθαίνει μοτίβα επιθέσεων, χρησιμοποιώντας τοπικά και παγκόσμια δεδομένα για την προσαρμογή της προστασίας στις ανάγκες κάθε οργανισμού.
- Εξελίσσεται συνεχώς, διασφαλίζοντας ενημερωμένες άμυνες απέναντι σε νέες επιθέσεις.

Με zero-touch updates, το Adaptive Security Engine διπλασιάζει συνεχώς την ακρίβεια ανίχνευσης απειλών, ενώ διατηρεί το φαινόμενο των False – Positives στο ελάχιστο.

Το AAP ενσωματώνει επίσης την νεοεισαχθείσα τεχνολογία Behavioral DDoS Engine, η οποία χρησιμοποιεί αλγόριθμους Machine Learning για τον εντοπισμό και την προστασία από Layer 7 DDoS attacks. Ο μηχανισμός αυτός αναλύει χαρακτηριστικά κίνησης, όπως η χώρα προέλευσης, το Network Fingerprint και διάφορα HTTPS request attributes, δημιουργώντας αυτοματοποιημένες, προσαρμοσμένες άμυνες.

Συμπληρωματικά στο παραπάνω, σημειώνεται πώς το AAP προσφέρει πολυεπίπεδη προστασία από επιθέσεις DDoS, διασφαλίζοντας την αδιάλειπτη λειτουργία εφαρμογών και APIs. Χρησιμοποιεί Edge-Based άμυνα για το άμεσο Blocking επιθέσεων επιπέδου δικτύου Network-Layer DDoS, ενώ ταυτόχρονα ανιχνεύει και μετριάζει εξελιγμένες επιθέσεις Layer 7 DDoS σε πραγματικό χρόνο. Με τη χρήση Granular Rate Controls, η πλατφόρμα επιτρέπει τη διαμόρφωση προσαρμοσμένων κανόνων άμυνας βάσει του προφίλ κίνησης και των ειδικών αναγκών κάθε επιχείρησης, εξασφαλίζοντας προστασία χωρίς να επηρεάζεται η εμπειρία των πραγματικών χρηστών.

Το AAP διαθέτει ακόμα ισχυρά εργαλεία ανίχνευσης και διαχείρισης Bot κίνησης, παρέχοντας πλήρη έλεγχο και προστασία από κακόβουλα αυτοματοποιημένα requests. Συγκεκριμένα, παρέχει τα κάτωθι:

- Πραγματική ανάλυση bot traffic μέσω της καταλόγου 1.750+ γνωστών bots.
- Browser impersonation detection: Αναγνωρίζει bots που προσποιούνται ότι είναι νόμιμοι browsers.
- Crypto challenges: Προκαλεί τα Bots με προσαρμοσμένες δοκιμές για να επαληθεύσει αν είναι πραγματικοί χρήστες.
- Conditional actions: Δυνατότητα φιλτραρίσματος ή αποκλεισμού Bots με βάση συγκεκριμένα χαρακτηριστικά και συμπεριφορά.

- Ανάλυση Web Analytics: Εντοπίζει Bots που παραποιούν δεδομένα επισκεψιμότητας και προλαμβάνει την υπερφόρτωση των συστημάτων από ανεπιθύμητη κίνηση.
- Εύκολη δημιουργία προσαρμοσμένων bot κανόνων για αποδοχή τρίτων bots (π.χ. συνεργατών και APIs).

Με αυτές τις δυνατότητες, το AAP ελαχιστοποιεί τον κίνδυνο Bot-Driven επιθέσεων, όπως Credential Stuffing, Account Takeovers, Scraping και DDoS μέσω BotNets.

Αξίζει επίσης να σημειωθεί πώς, η API προστασία του AAP διασφαλίζει:

- Αυτόματη ανίχνευση API endpoints, ακόμα και άγνωστων ή μεταβαλλόμενων APIs.
- Προστασία από επιθέσεις σε API, όπως DDoS, SQL injections, credential abuse και API παραβιάσεις προδιαγραφών.
- Διαχείριση ευαίσθητων δεδομένων μέσω PII reporting για συμμόρφωση με κανονισμούς.

Με αυτές τις δυνατότητες, οι επιχειρήσεις διασφαλίζουν πλήρη ορατότητα στο API traffic και μειώνουν τον κίνδυνο επιθέσεων σε μη προστατευμένα APIs.

Ακόμα, ο μηχανισμός Malware Protector του AAP ανιχνεύει και αποκλείει κακόβουλα αρχεία πριν την αποστολή τους σε εταιρικά συστήματα, μειώνοντας έτσι τους κινδύνους από επιθέσεις μέσω αρχείων.

Παράλληλα, η πλατφόρμα της Akamai υποστηρίζει DevOps ενσωμάτωση με APIs, CLI και Terraform, επιτρέποντας την αυτοματοποίηση πολιτικών ασφαλείας.

### 2.6.2 Prolexic – Layer 3

Το Akamai Prolexic είναι μια προηγμένη λύση προστασίας από DDoS επιθέσεις σε Layer 3, σχεδιασμένη για να σταματά κακόβουλη κίνηση πριν φτάσει σε εφαρμογές, data centers και υβριδικές cloud υποδομές. Παρέχει πλήρη κάλυψη όλων των ports και πρωτοκόλλων, επιτρέποντας την προστασία σε on-prem, cloud ή υβριδικές εγκαταστάσεις. Σημειώνεται πώς το Prolexic δρα συμπληρωματικά στο AAP που αναφέρθηκε στην προηγούμενη υποενότητα καθώς αφορά προστασία σε διαφορετικό επίπεδο.

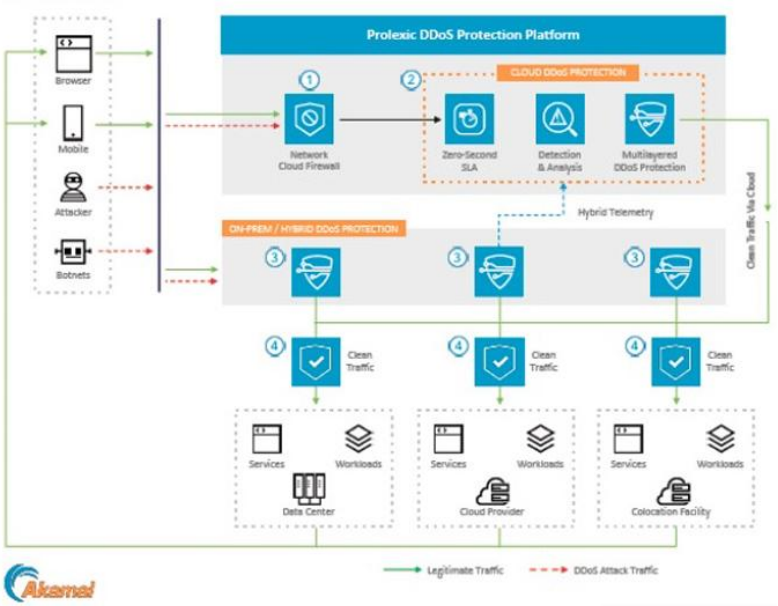


*Figure 12: Prolexic Προστασία,https://www.akamai.com/resources/product-brief/prolexic*

Το Prolexic Cloud αξιοποιεί 32 παγκόσμια Scrubbing Centers (κέντρα που φιλτράρουν την εισερχόμενη κίνηση) για τον εντοπισμό και την αποτροπή επιθέσεων πλησιέστερα στην πηγή από όπου ξεκινάνε. Η ομάδα ασφάλειας της Akamai (SOCC) εφαρμόζει προληπτικά και προσαρμοσμένα μέτρα blocking, εξασφαλίζοντας άμεση ανίχνευση επιθέσεων.

Η εισερχόμενη κίνηση που λαμβάνεται αναλύεται σε καθαρή και κακόβουλη, η οποία λαμβάνει Block από το Prolexic. Η καθαρή κίνηση επιστρέφεται στους Origin Servers με ασφαλείς συνδέσεις μέσω GRE tunnels, Layer 2 VLAN connections ή VIP-to-origin mapping, διατηρώντας την ακεραιότητα και την απόδοση του δικτύου.

Το Prolexic Network Cloud Firewall λειτουργεί ως πρώτη γραμμή άμυνας, παρέχοντας επιπλέον έλεγχο πρόσβασης στο Edge του δικτύου. Οι χρήστες μπορούν να διαχειρίζονται Firewall Rules, γεωγραφικό έλεγχο πρόσβασης και IP-based policies για αποτροπή κακόβουλης κίνησης και zero-day απειλών.

## 2.7 NIS-2

Η Οδηγία NIS2 (5160/2024) θεσπίζει ένα ενιαίο νομικό πλαίσιο για την κυβερνοασφάλεια σε 18 κρίσιμους τομείς εντός της Ευρωπαϊκής Ένωσης, αντικαθιστώντας την προηγούμενη οδηγία NIS1 (1148/2016). Στόχος της οδηγίας αυτής είναι η ενίσχυση της ανθεκτικότητας των κρατών-μελών απέναντι στις κυβερνοαπειλές μέσω αυστηρότερων κανόνων, ενισχυμένης εποπτείας και διασυνοριακής συνεργασίας [69].

Η οδηγία απαιτεί από κάθε κράτος-μέλος να υιοθετήσει εθνική στρατηγική κυβερνοασφάλειας, συμπεριλαμβάνοντας μέτρα για την ασφάλεια της εφοδιαστικής αλυσίδας, τη διαχείριση τρωτών σημείων και την εκπαίδευση. Οι εθνικές αρχές πρέπει να

διασφαλίζουν ότι οι οργανισμοί σε κρίσιμους τομείς εφαρμόζουν μέτρα διαχείρισης κινδύνων και υποβάλλουν αναφορές για σημαντικά συμβάντα που θα μπορούσαν να προκαλέσουν σοβαρές διαταραχές.

Το εύρος εφαρμογής της οδηγίας διευρύνεται, καλύπτοντας όχι μόνο τομείς όπως η ενέργεια, οι μεταφορές, η υγειονομική περίθαλψη και οι ψηφιακές υποδομές, αλλά και δημόσιες υπηρεσίες ηλεκτρονικών επικοινωνιών, κοινωνικές πλατφόρμες, υπηρεσίες ταχυμεταφορών, διαχείριση αποβλήτων, κατασκευή κρίσιμων προϊόντων και δημόσια διοίκηση.

Πιο συγκεκριμένα, τα βαικότερα σημεία της οδηγίας αυτής είναι τα ακόλουθα:

Ενίσχυση του ρόλου της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ), δίνοντάς της διευρυμένες αρμοδιότητες σχετικά με τον έλεγχο και την εποπτεία της εφαρμογής της Οδηγίας NIS2. Με την ψήφιση του νόμου, αναμένεται να αυξηθεί η ανάγκη για υπηρεσίες, προϊόντα και ειδικούς στην κυβερνοασφάλεια, γεγονός που θα οδηγήσει στη δημιουργία προγραμμάτων εκπαίδευσης και πιστοποίησης σε συνεργασία με σχετικούς φορείς, συμβάλλοντας έτσι στη διαμόρφωση ενός ισχυρού εγχώριου οικοσυστήματος κυβερνοασφάλειας.

Παράλληλα, η ΕΑΚ αναλαμβάνει τον ρόλο της ομάδας απόκρισης σε περιστατικά ασφάλειας υπολογιστών (CSIRT), ενώ προβλέπεται η σύσταση επιπλέον ομάδων απόκρισης, αν κριθεί απαραίτητο, για την ενίσχυση της κυβερνοασφάλειας. Σε κάθε περίπτωση, η ΕΑΚ θα έχει τον συντονιστικό ρόλο στη διαχείριση των περιστατικών.

Το πεδίο εφαρμογής της νομοθεσίας διευρύνεται, ώστε να περιλαμβάνει νέους τομείς που πρέπει να συμμορφωθούν με συγκεκριμένα μέτρα κυβερνοασφάλειας. Εκτός από τους ήδη υφιστάμενους κλάδους (όπως ενέργεια, μεταφορές, υγειονομική περίθαλψη και ψηφιακές υποδομές), πλέον καλύπτονται ταχυδρομικές υπηρεσίες, διαχείριση αποβλήτων, βιομηχανία τροφίμων, χημικά προϊόντα, κατασκευές, καθώς και η κεντρική κυβέρνηση, οι περιφέρειες και οι δήμοι.

Επιπλέον, εισάγεται υποχρέωση έγκαιρης αναφοράς σημαντικών περιστατικών, ακολουθώντας μια διαδικασία πολλαπλών σταδίων. Αρχικά, απαιτείται προειδοποίηση εντός 24 ωρών, ακολουθούμενη από μια πιο λεπτομερή ενημέρωση εντός 72 ωρών από τη στιγμή που θα διαπιστωθεί το περιστατικό. Στη συνέχεια, παρέχεται ενδιάμεση έκθεση με επικαιροποιημένα στοιχεία, ενώ η διαδικασία ολοκληρώνεται με την υποβολή τελικής έκθεσης εντός ενός μήνα.

Για τις περιπτώσεις μη συμμόρφωσης, προβλέπονται αυστηρές κυρώσεις και διοικητικά πρόστιμα, τα οποία μπορούν να φτάσουν έως 10 εκατομμύρια ευρώ ή 2% του παγκόσμιου ετήσιου κύκλου εργασιών μιας επιχείρησης, ανάλογα με το ποιο ποσό είναι μεγαλύτερο.

Οι νέες ρυθμίσεις αφορούν τόσο δημόσιους οργανισμούς όσο και ιδιωτικές επιχειρήσεις, οι οποίες πρέπει να εφαρμόσουν συγκεκριμένα μέτρα διαχείρισης κινδύνων για την προστασία των δικτύων και των πληροφοριακών τους συστημάτων. Ενδεικτικά, οι φορείς καλούνται να υιοθετήσουν:

- Πολιτικές και διαδικασίες για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων.
- Συστήματα διαχείρισης περιστατικών για έγκαιρη απόκριση σε κυβερνοεπιθέσεις.
- Μέτρα επιχειρησιακής συνέχειας, όπως δημιουργία αντιγράφων ασφαλείας και σχέδια αποκατάστασης σε περίπτωση καταστροφής.
- Ασφάλεια στην εφοδιαστική αλυσίδα, ώστε να ελέγχονται οι κίνδυνοι που προκύπτουν από συνεργασίες με προμηθευτές και παρόχους υπηρεσιών.
- Ασφάλεια στην ανάπτυξη και συντήρηση των συστημάτων πληροφορικής, περιλαμβάνοντας διαδικασίες για τη διαχείριση και γνωστοποίηση ευπαθειών.
- Πολιτικές και διαδικασίες αξιολόγησης της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων, διασφαλίζοντας τη διαρκή βελτίωση της κυβερνοασφάλειας.

Με την Οδηγία NIS2, η ΕΕ επιδιώκει να δημιουργήσει ένα πιο ανθεκτικό και συντονισμένο πλαίσιο κυβερνοασφάλειας, ενισχύοντας την πρόληψη, ανίχνευση και αντιμετώπιση κυβερνοαπειλών σε ευρωπαϊκό επίπεδο. Τα Content Delivery Networks (CDN) μπορούν να διαδραματίσουν κρίσιμο ρόλο στην εφαρμογή και ενίσχυση της κυβερνοασφάλειας, όπως απαιτείται από την Οδηγία NIS2. Δεδομένου ότι η NIS2 επιβάλλει αυστηρότερα μέτρα για την προστασία κρίσιμων ψηφιακών υποδομών, τα CDN μπορούν να βοηθήσουν τους οργανισμούς να συμμορφωθούν μέσω βελτιωμένης ασφάλειας, διαχείρισης κινδύνων και επιχειρησιακής συνέχειας.

# Κεφάλαιο 3ο: Προστασία της Ιδιωτικότητας σε Περιβάλλοντα Content Delivery Network (CDN)

## 3.1 Ιδιωτικότητα

Η πρώτη αναφορά στην Ιδιωτικότητα πραγματοποιήθηκε το 1890, από τους Brandeis και Warre, οι οποίοι αναφέρθηκαν σε αυτή ως «το δικαίωμα να μείνει κανείς μόνος του» και επισήμαναν την αναγκαιότητα της συνταγματικής κατοχύρωσης της. Το 1948, το Γενικό συμβούλιο των Ηνωμένων Εθνών στη Παγκόσμια Δήλωση των Ανθρωπίνων δικαιωμάτων αναφέρθηκε στο θέμα της Ιδιωτικότητας, ενώ λίγο αργότερα, το 1950, η Ευρώπη θέσπισε το δικαίωμα σεβασμού της Ιδιωτικής ζωής των πολιτών της [70].

Ο πιο κοινά αποδεκτός και κατανοητός ορισμός προτάθηκε από τον Westin το 1967, και υποστηρίζει πώς «η Ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων, των ιδρυμάτων, να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους».

Η έννοια της ιδιωτικότητας μπορεί να διαχωριστεί ως εξής:

➢ Η Ιδιωτικότητα Πληροφοριών (Informational Privacy) που αφορά τον έλεγχο του αν και πως οι προσωπικές πληροφορίες μπορούν να συγκεντρωθούν, να αποθηκευτούν, να επεξεργαστούν ή να διαδοθούν επιλεκτικά.

➢ Η Εδαφική Ιδιωτικότητα (Territorial Privacy) που ρυθμίζει τη προστασία της στενής φυσικής περιοχής που περιβάλλει ένα πρόσωπο.

➢ Η Σωματική Ιδιωτικότητα (Bodily Privacy) που σχετίζεται με τη προστασία ενός προσώπου από αδικαιολόγητη παρέμβαση, η οποία θίγει την ηθική αίσθηση του.

➢ Η Ιδιωτικότητα Επικοινωνίας (Communication Privacy) που αφορά την προστασία της επικοινωνίας ενός προσώπου από μη εξουσιοδοτημένη παρακολούθηση.

➢ Η Ψυχολογική Ιδιωτικότητα (Psychological Privacy) που ορίζεται ως ο έλεγχος κοινοποίησης ή παρακράτησης προσωπικών πληροφοριών για τη προστασία των πεποιθήσεων και της προσωπικότητας των ατόμων.

Αντίστοιχα, προκύπτει κατηγοριοποίηση των σύγχρονων ορισμών και προσεγγίσεων της έννοιας της ιδιωτικότητας στα παρακάτω θέματα:

➢ Δικαίωμα να παραμείνεις μόνος κατά βούληση.

➢ Δικαίωμα να περιορίζεις την πρόσβαση των άλλων στα προσωπικά σου δεδομένα.

➢ Δικαίωμα του απορρήτου και να αποκρύπτεις από τρίτους τα προσωπικά σου δεδομένα.
➢ Δικαίωμα να ελέγχεις πώς χρησιμοποιούνται τα προσωπικά σου δεδομένα από τρίτους.
➢ Δικαίωμα να ελέγχεις την ιδιωτική σου ζωή.
➢ Δικαίωμα του σεβασμού της προσωπικότητας και της αυτονομίας.
➢Δικαίωμα του αυτοπροσδιορισμού, της αυτοδιάθεσης και της δυνατότητας για προσωπική εξέλιξη.
➢ Δικαίωμα της προστασίας των ενεργειών και της ερωτικής ζωής.

### 3.1.1 Ιδιωτικότητα Εκ Σχεδιασμού (Privacy by Design)

Η έννοια της ιδιωτικότητας εκ σχεδιασμού, παρουσιάστηκε αρχικά από την Ann Cavoukian το 1990, και βασίζεται στην άποψη ότι για την προστασία της ιδιωτικής ζωής δεν αρκεί η συμμόρφωση με τα υφιστάμενα κανονιστικά πλαίσια. Συγκεκριμένα, η λειτουργία ενός πληροφοριακού συστήματος μιας επιχείρησης πρέπει ιδανικά να έχει σχεδιαστεί με γνώμονα τη διασφάλιση της προστασίας της ιδιωτικής ζωής. Στην περιγραφή της για το πώς είναι εφικτό να πραγματοποιηθεί η “Privacy by Design”, η Cavoukian, αναφέρθηκε σε επτά κατευθυντήριες αρχές:

➢ Η αρχή της πρόληψης (Proactive)
➢ Η αρχή της προεπιλογής (By Default)
➢ Η αρχή της Ενσωμάτωσης (Embedded)
➢ Η αρχή του θετικού αποτελέσματος (Positive Sum)
➢ Η αρχή της προστασίας ολόκληρου κύκλου ζωής (Life cycle protection)
➢ Η αρχή της διαφάνειας (Transparency)
➢ Η αρχή του σεβασμού προς τους χρήστες (Respect for User)

### 3.1.2 Βασικές Απαιτήσεις Ιδιωτικότητας

Οι βασικές απαιτήσεις ιδιωτικότητας είναι οι ακόλουθες [70]:

➢ Αυθεντικοποίηση (Authentication): είναι η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μίας οντότητας.

➢ Εξουσιοδότηση (Authorization): είναι η λειτουργία του καθορισμού δικαιωμάτων πρόσβασης σε διάφορους πόρους ενός συστήματος, που σχετίζεται με τη γενική ασφάλεια πληροφοριών και ειδικότερα με τον έλεγχο πρόσβασης.

➢ Ανωνυμία (Anonymity): η διαδικασία κατά την οποία ένα άτομο μπορεί να κάνει χρήση μιας υπηρεσίας, χωρίς να αποκαλυφθεί η ταυτότητά του.

➢ Ψευδωνυμία (Pseudonimity): η διαδικασία κατά την οποία η ταυτότητα ενός ατόμου προστατεύεται από αναγνώριση από μη εξουσιοδοτημένες οντότητες.

➢ Μη συνδεσιμότητα (Unlikability): η διαδικασία η οποία διασφαλίζει ότι οι επιτιθέμενοι δεν μπορούν να συνδέσουν σχετικές πληροφορίες που αφορούν ένα άτομο μεταξύ τους, προστατεύοντας έτσι την ιδιωτικότητά του ατόμου.

➢ Μη παρατηρησιμότητα (Unobservability): η διαδικασία κατά την οποία οι επιτιθέμενοι δεν μπορούν να παρατηρήσουν τα άτομα ή να εντοπίσουν ίχνη τους, με αποτέλεσμα να προστατεύεται η ιδιωτικότητά των ατόμων.

➢ Προστασία Δεδομένων (Data protection): σκοπός της συγκεκριμένης απαίτησης είναι η προστασία των προσωπικών δεδομένων από επεξεργασία. Οι βασικές αρχές ιδιωτικότητας που εκφράζονται από αντίστοιχους νόμους και την ισχύουσα νομοθεσία είναι οι ακόλουθες [70]:

- Αρχή της νομιμότητας και της δικαιοσύνης (Principle of Lawfulness and Fairness): τα προσωπικά δεδομένα πρέπει να συλλέγονται με νόμιμο και δίκαιο τρόπο.
- Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν (Principle of the Purpose Specification and Purpose Binding): ο σκοπός που συλλέγονται τα προσωπικά δεδομένα πρέπει να είναι σαφώς καθορισμένος και να συνάδει με τη νομοθεσία. Η επεξεργασία δεδομένων πρέπει να διεξάγεται μόνο για τον σκοπό για τον οποίο συγκεντρώθηκαν.
- Αρχή της αναγκαιότητας της συλλογής και της επεξεργασίας των δεδομένων (Principle of Necessity of Data Collection and Processing): η συλλογή και η επεξεργασία των προσωπικών δεδομένων πρέπει να επιτρέπονται μόνο στις περιπτώσεις όπου ο συλλέγων πράττει ενέργειες αντίστοιχες με το σκοπό συλλογής των δεδομένων, αποδεικνύοντας έτσι την αναγκαιότητα, αφού για την εκτέλεση των ενεργειών χρειάζεται τα δεδομένα αυτά.
- Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στα υποκείμενα των ευαίσθητων δεδομένων (Information, Notification and Access Rights of the Data Subjects): Τα υποκείμενα των δεδομένων πρέπει να έχουν το δικαίωμα της πληροφόρησης και της ενημέρωσης για τα προσωπικά τους δεδομένα, καθώς και το δικαίωμα πρόσβασης, της διόρθωσης, της διαγραφής ή και του αποκλεισμού των δεδομένων τους σε περιπτώσεις που εκείνα κρίνουν αναγκαίο.
- Αρχή της ασφάλειας και της ακρίβειας (Principle of Security and Accuracy): Επιβάλλει την ύπαρξη κατάλληλων μηχανισμών και τεχνολογιών για τη διασφάλιση της εμπιστευτικότητας, της ακρίβειας και της διαθεσιμότητας των προσωπικών δεδομένων, ούτως ώστε να παραμένουν ασφαλή , ενημερωμένα και ακέραια.

ο Εποπτεία και Κύρωση (Supervision and Sanctions): Προβλέπει τη σύσταση Ανεξάρτητης Αρχής Προστασίας Δεδομένων, με σκοπό την επίβλεψη και την παρατήρηση της εφαρμογής των κανόνων ιδιωτικότητας. Η ίδια Αρχή θα είναι υπεύθυνη και για την επιβολή κυρώσεων σε περιπτώσεις που σημειώνονται αποκλίσεις από την νομιμότητα.

### 3.1.3 Βασικές Απειλές Ιδιωτικότητας

Τα εξωτερικά δεδομένα επικοινωνίας περιλαμβάνουν πληροφορία η οποία σχετίζεται με την ταυτότητα και την τοποθεσία των μερών επικοινωνίας, την χρονική στιγμή και σε ορισμένες περιπτώσεις με το ίδιο το περιεχόμενο επικοινωνίας. Συνεπώς, η διατήρηση αυτών των δεδομένων ευνοεί την εκδήλωση διαφόρων απειλών ασφάλειας οι οποίες σχετίζονται με το απόρρητο της επικοινωνίας και την ιδιωτικότητά των συνδρομητών. Οι βασικότερες απειλές ιδιωτικότητας είναι οι ακόλουθες [70]:

➢ Αποκάλυψη Δεδομένων: Η αποκάλυψη των διατηρούμενων δεδομένων σε μη εξουσιοδοτημένους χρήστες, είτε αυτοί είναι εξωτερικοί είτε εσωτερικοί χρήστες του 73 παρόχου χωρίς τα απαιτούμενα δικαιώματα πρόσβασης, μπορεί να οδηγήσει σε άμεση ή έμμεση παραβίαση του απορρήτου.

➢ Τροποποίηση Δεδομένων: Μία τυχαία τροποποίηση στα δεδομένα ενδέχεται να επηρεάσει την αξιοπιστία τους. Όμως μία εσκεμμένη τροποποίηση ενδέχεται να οδηγήσει στην κατάχρηση των δεδομένων. Σε μία ακραία περίπτωση θα μπορούσαν να χρησιμοποιηθούν δεδομένα επικοινωνίας, τα οποία κακοβούλως έχουν τροποποιηθεί για τη νομική δίωξη κάποιου ανυποψίαστου συνδρομητή.

➢ Μη Εξουσιοδοτημένη Πρόσβαση: Η απειλή αυτή σχετίζεται με τις δύο προηγούμενες, εφόσον μία μη εξουσιοδοτημένη πρόσβαση ανάγνωσης θα οδηγούσε σε αποκάλυψη των δεδομένων, ενώ μία μη εξουσιοδοτημένη πρόσβαση εγγραφής θα μπορούσε να οδηγήσει σε τροποποίηση των δεδομένων.

➢ Παράνομη Καταγραφή Δεδομένων: Σχετίζεται με τη συλλογή δεδομένων πέρα από αυτά που έχουν καθοριστεί στις πολιτικές ιδιωτικότητας των παρόχων. Οι επικοινωνίες που εκτελούνται από τους συνδρομητές πραγματοποιούνται με βάση συγκεκριμένες πολιτικές ιδιωτικότητας, οι οποίες καθορίζουν το είδος των προς συλλογή δεδομένων. Η καταγραφή δεδομένων που δεν περιέχονται στις πολιτικές ιδιωτικότητας αποτελεί σημαντική παραβίαση της ιδιωτικότητας των συνδρομητών.

➢ Παράνομη Χρήση Δεδομένων: Περιλαμβάνει την επεξεργασία των δεδομένων για σκοπούς που δεν περιλαμβάνονται στους νόμιμους σκοπούς διατήρησης, όπως καθορίζονται στις πολιτικές ιδιωτικότητας. Για παράδειγμα, πρόσβαση σε δεδομένα

επικοινωνίας χρηστών διαδικτύου με σκοπό την κατηγοριοποίηση των αγοραστικών συνηθειών ή τη παρακολούθηση των δραστηριοτήτων τους.

➢ Παρατεταμένη Διατήρηση Δεδομένων: Αφορά τη διατήρηση δεδομένων για χρονικά διαστήματα μεγαλύτερα από αυτά που ορίζονται από τη νομοθεσία και αναφέρονται στις κοινοποιήσιμες πολιτικές ιδιωτικότητας. Παρόλο που η παρατεταμένη διατήρηση δεν αποτελεί από μόνη της άμεση παραβίαση του απορρήτου και της ιδιωτικότητας, παρατείνει την έκθεση των δεδομένων σε πιθανές επιθέσεις και αδυναμίες.

➢ Αδυναμία Καταλογισμού Ευθύνης: Σε περίπτωση που οι πράξεις των χρηστών με νόμιμα δικαιώματα πρόσβασης στα δεδομένα δεν είναι καταλογίσιμες σε αυτούς, πιθανοί κακόβουλοι εσωτερικοί χρήστες θα μπορούσαν να προβούν σε παράνομη χρήση ή κατάχρηση των δεδομένων. Για παράδειγμα, τα δεδομένα επικοινωνίας των συνδρομητών θα μπορούσαν να διαρρεύσουν σε μη εξουσιοδοτημένους χρήστες ή να αποτελέσουν αντικείμενο συναλλαγής ή εκβιασμού συνδρομητών. Επιπλέον, θα ήταν δυνατό να δοθεί πρόσβαση σε δεδομένα σε κάποια διωκτική αρχή, η οποία δεν θα είχε εξασφαλίσει την απαιτούμενη δικαστική άδεια.

## 3.2 Ρυθμιστικό και Κανονιστικό Πλαίσιο για την Προστασία της Ιδιωτικότητας

Το βασικότερο σημείο της Ιδιωτικότητας πληροφοριών είναι οι ίδιες οι πληροφορίες και ο διαχωρισμός τους σε δημόσιες πληροφορίες και σε ιδιωτικές πληροφορίες, που χρήζουν προστασίας. Ο διαχωρισμός αυτός πραγματοποιείται με βάση το ισχύον νομικό και κανονιστικό πλαίσιο.

### 3.2.1 Γενικά

#### 3.2.1.1 Προστασία της Ιδιωτικής Ζωής

Ως Ιδιωτικότητα ορίζεται το δικαίωμα του ατόμου να παραμείνει μόνο του. Συνεπώς, διαπιστώνεται πώς η έννοια αποτελεί έναν συνδυασμό των εννοιών «μοναξιά» και «μη εισβολή». Η πρώτη αναφέρεται στο απόρρητο της σκέψης, της ιδιοκτησίας και των ενεργειών του ατόμου, ενώ η τελευταία σχετίζεται με τα δεδομένα άλλων προσώπων και με τον τρόπο που αυτά το επηρεάζουν. Στη σύγχρονη καθημερινότητα, η ιδιωτική ζωή προστατεύεται από κοινωνικούς κανόνες, ενώ με τη διάσταση που αποκτά η προστασία της ιδιωτικότητας και στον ηλεκτρονικό κόσμο, δημιουργείται η ανάγκη για παρόμοιους κανόνες και σε αυτόν.

#### 3.2.1.2 Προστασία Προσωπικών Δεδομένων

Οι επιστήμονες της πληροφορικής ορίζουν την Ιδιωτικότητα ως το δικαίωμα του ατόμου να καθορίζει ποιες προσωπικές του πληροφορίες είναι διαθέσιμες, σε ποια άτομα και σε ποιο

βαθμό. Το άτομο έχει απόλυτο έλεγχο επί των προσωπικών του δεδομένων, των συνομιλιών και των ενεργειών του, ενώ είναι ο αποκλειστικός υπεύθυνος για τις πράξεις του. Συνεπώς, τα προσωπικά δεδομένα θεωρούνται ιδιοκτησία.

Οι παραπάνω προσεγγίσεις αλληλοσυμπληρώνονται, έτσι η προστασία της Ιδιωτικότητας στο ηλεκτρονικό περιβάλλον μπορεί να ταυτιστεί από τη μία με τη προστασία της ιδιωτικής ζωής στο ηλεκτρονικό περιβάλλον, που επιτυγχάνεται με τη προστασία των ηλεκτρονικών ταυτοτήτων που διαθέτει το άτομο, των ηλεκτρονικών ενεργειών του, της επικοινωνίας του, των πνευματικών δικαιωμάτων του και των συσκευών που κάνει χρήση για να εισέλθει σε αυτά τα περιβάλλοντα και από την άλλη, με τη προστασία των προσωπικών δεδομένων, ευαίσθητων και μη.

### 3.2.2 Νομικό Πλαίσιο στην Ευρώπη

Η Οδηγία 95/46/ΕΚ στοχεύει στην προστασία των ατομικών δικαιωμάτων και ελευθεριών, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία αυτών. Η παρούσα οδηγία καταργήθηκε με την έλευση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR).

➢ Η Οδηγία 2002/58/ΕΚ στοχεύει στη διασφάλιση ισοδύναμου επιπέδου προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, σε σχέση με την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Ακόμα, αποσκοπεί στην διασφάλιση ελεύθερης κυκλοφορίας των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στα κράτη μέλη της κοινότητας.

➢ Η Οδηγία 2006/24/ΕΚ παρέχει οδηγίες στα κράτη μέλη αναφορικά με τη διατήρηση των δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία, σε συνάρτηση με τη παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών. Αποβλέπει στην εναρμόνιση των διατάξεων των κρατών μελών σχετικά με τις υποχρεώσεις των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό ή δημοσίου δικτύου επικοινωνιών, όσον αφορά στη διατήρηση 75 ορισμένων δεδομένων που παράγονται ή υφίσταται επεξεργασία από αυτούς, ώστε να διασφαλιστεί ότι τα δεδομένα καθίσταται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων.

#### 3.2.2.1 Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ

Ο Γενικός Κανονισμός Προστασίας Δεδομένων καθορίζει τις απαιτήσεις για τη προστασία των φυσικών προσώπων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων και την ελεύθερη κυκλοφορία αυτών. Ο κανονισμός είναι υποχρεωτικός για όλους τους οργανισμούς που δραστηριοποιούνται στην Ευρώπη και στοχεύει σε [71]:

➢ Στην εξάλειψη των ασυνεπειών από τους εθνικούς νόμους, ανεβάζοντας το πήχη για τη καλύτερη προστασία της ιδιωτικότητας των φυσικών προσώπων.

➢ Στην αναθεώρηση του νόμου για τη καλύτερη αντιμετώπιση των σύγχρονων προκλήσεων που αφορούν την Ιδιωτικότητα, όπως αυτές δημιουργούνται από το διαδίκτυο, τα κοινωνικά μέσα, τα big data και το συμπεριφορικό μάρκετινγκ.

➢ Στην μείωση του δαπανηρού διοικητικού φόρτου για οργανισμούς που λογοδοτούν σε πολλαπλές Αρχές Προστασίας Δεδομένων.

Ο GDBR εφαρμόζεται:
➢ Στην επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στο πλαίσιο δραστηριοτήτων μιας εγκατάστασης ενός υπεύθυνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το αν η επεξεργασία πραγματοποιείται εντός της Ένωσης.

➢ Στην επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα υποκειμένων που βρίσκονται στην Ένωση από τον υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:

- ο Τη προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως αν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων.
- ο Τη παρακολούθηση της συμπεριφοράς τους, στο βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.

### 3.2.3 Νομικό Πλαίσιο στην Ελλάδα

Το νομοθετικό πλαίσιο στην Ελλάδα για τη προστασία των προσωπικών δεδομένων, συγκροτείται από το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων, όπως κατοχυρώνεται στο άρθρο 9 Α του Συντάγματος, τον νόμο 2472/97 για τη προστασία του ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, όπως ισχύει μετά τις τροποποιήσεις που εισήχθησαν, καθώς και τον νόμο 3471/06 που αφορά στην προστασία προσωπικών δεδομένων ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

## 3.3 Προστασία της Ιδιωτικότητας στο Content Delivery Network

Η ιδιωτικότητα στα CDN είναι ζωτικής σημασίας, καθώς αυτά τα δίκτυα διαχειρίζονται τεράστιο όγκο διαδικτυακής κίνησης, κάτι το οποίο τους δίνει τη δυνατότητα να συλλέγουν και να αναλύουν δεδομένα χρηστών, γεγονός που μπορεί να εγκυμονεί κινδύνους για την προστασία της ιδιωτικής ζωής. Η διασφάλιση ότι οι πληροφορίες των χρηστών δεν χρησιμοποιούνται καταχρηστικά ή δεν εκτίθενται σε μη εξουσιοδοτημένη πρόσβαση είναι καθοριστική τόσο για τη διατήρηση της εμπιστοσύνης των χρηστών όσο και για τη συμμόρφωση με τους κανονισμούς προστασίας δεδομένων.

Τα CDN έχουν τη δυνατότητα να παρακολουθούν τη δραστηριότητα των χρηστών, τις προτιμήσεις τους, ακόμη και τις γεωγραφικές τοποθεσίες τους, δημιουργώντας έτσι λεπτομερή προφίλ. Αν αυτά τα δεδομένα δεν προστατευτούν σωστά, υπάρχει σοβαρός κίνδυνος παραβίασης της ιδιωτικότητας και υλοποίησης επιθέσεων, όπως Inference επιθέσεις. Κατά τις επιθέσεις αυτού του τύπου, οι επιτιθέμενοι συλλέγουν πληροφορίες οι οποίες δεν είναι από μόνες τους ευαίσθητες, ωστόσο αν συνδυαστούν αποτελεσματικά, μπορούν να αποκαλύψουν ευαίσθητα δεδομένα. Ακόμα και με τη χρήση κρυπτογράφησης, οι επιθέσεις τύπου Inference μπορούν να αποκαλύψουν πληροφορίες σχετικά με το περιεχόμενο των αιτημάτων των χρηστών.

Αξίζει να αναφερθεί, πώς παρόλο που τα CDN μειώνουν την καθυστέρηση στη μεταφορά δεδομένων και βελτιώνουν την εμπειρία του χρήστη, η χρήση τους εγείρει και σημαντικά ζητήματα ασφαλείας τόσο για τους κατόχους περιεχομένου όσο και για τους τελικούς χρήστες. Επιπλέον, η δυνατότητα των CDN να παρακάμπτουν τη διαδικτυακή λογοκρισία δημιουργεί ηθικά και πολιτικά ζητήματα, ενισχύοντας την ανάγκη για σαφείς και ισχυρές πολιτικές προστασίας της ιδιωτικότητας.

Για την αντιμετώπιση αυτών των προκλήσεων, είναι απαραίτητη η εφαρμογή αυστηρών μέτρων ασφαλείας, όπως η ανώνυμη μετάδοση δεδομένων, η ελαχιστοποίηση της συλλογής πληροφοριών χρηστών και η υιοθέτηση ισχυρών μηχανισμών ελέγχου πρόσβασης. Μόνο μέσα από τέτοιες πρακτικές μπορεί να διασφαλιστεί ότι τα CDN προσφέρουν τα οφέλη τους χωρίς να θέτουν σε κίνδυνο την ασφάλεια και την ιδιωτικότητα των χρηστών.

### 3.3.1 Προκλήσεις Ιδιωτικότητας στο Content Delivery Network (CDN)

Οι προκλήσεις Ιδιωτικότητας που αναφέρονται στο υποκεφάλαιο 3.1.3 παρατηρούνται και στα περιβάλλοντα CDN. Σε συνέχεια, όσων αναφέρθηκαν στην συγκεκριμένη υποενότητα, αξίζει να προστεθούν και τα κάτωθι:

#### 3.3.1.1 Συλλογή και Ανάλυση Δεδομένων

Ένα από τα σημαντικότερα ζητήματα που σχετίζονται με την ιδιωτικότητα στα CDN είναι η δημιουργία λεπτομερών προφίλ χρηστών μέσω της παρακολούθησης της δραστηριότητάς τους στο διαδίκτυο. Αυτό εγείρει σημαντικές ανησυχίες σχετικά με το πώς χρησιμοποιούνται τα δεδομένα των χρηστών και ποιες πληροφορίες μπορούν να εξαχθούν από αυτά [75]. Παρακάτω παρουσιάζονται ορισμένες βασικές πτυχές αυτής της πρόκλησης [75]:

- Εκτεταμένη Συλλογή Δεδομένων
  Τα CDN συγκεντρώνουν μεγάλο όγκο πληροφοριών σχετικά με τις διαδικτυακές συνήθειες των χρηστών, όπως οι προτιμήσεις περιήγησης και η τοποθεσία τους. Αυτή η συλλογή μπορεί να είναι ιδιαίτερα λεπτομερής, καλύπτοντας σχεδόν κάθε αλληλεπίδραση ενός χρήστη με το περιεχόμενο που διανέμεται μέσω του CDN.

- Αποκάλυψη Προσωπικών Δεδομένων
  Μέσω της ανάλυσης της επισκεψιμότητας, τα CDN μπορούν να αποκαλύψουν κρίσιμες πληροφορίες για τους χρήστες, όπως τις πολιτικές τους πεποιθήσεις, τις θρησκευτικές τους απόψεις ή ακόμα και δεδομένα σχετικά με την υγεία τους. Αυτό ενδέχεται να δημιουργήσει κινδύνους τόσο για την ιδιωτικότητα των χρηστών όσο και για πιθανές στοχευμένες διαφημίσεις ή χειραγώγηση περιεχομένου.

- Επιθέσεις μέσω Web Page Fingerprinting (WPF)
  Μία από τις τεχνικές που μπορούν να απειλήσουν την ιδιωτικότητα είναι οι επιθέσεις Web Page Fingerprinting (WPF). Οι επιθέσεις αυτές επιτρέπουν σε έναν επιτιθέμενο να αναλύσει τα χαρακτηριστικά της επισκεψιμότητας και να καθορίσει ποιες συγκεκριμένες σελίδες έχει επισκεφθεί ένας χρήστης μέσα σε έναν ιστότοπο. Αυτό αυξάνει σημαντικά τον κίνδυνο παραβίασης της ιδιωτικότητας, ειδικά όταν η ανάλυση γίνεται σε κοινωνικά δίκτυα ή άλλες πλατφόρμες με ευαίσθητο περιεχόμενο.

- Ανάλυση επισκεψιμότητας και intra-domain WPF
  Οι επιθέσεις τύπου intra-domain WPF στοχεύουν στη σωστή ταξινόμηση των σελίδων που επισκέπτεται ένας χρήστης μέσω της ανάλυσης των μοτίβων επισκεψιμότητας. Ακόμα και όταν το περιεχόμενο είναι κρυπτογραφημένο, η δομή της επισκεψιμότητας μπορεί να αποκαλύψει στοιχεία για τις ενέργειες των χρηστών, δημιουργώντας νέες προκλήσεις για την προστασία της ιδιωτικότητας.

Η ανάγκη για αποτελεσματική προστασία των δεδομένων στα CDN είναι επιτακτική, καθώς η ανεξέλεγκτη συλλογή και ανάλυση δεδομένων μπορεί να οδηγήσει σε σοβαρές παραβιάσεις της ιδιωτικής ζωής των χρηστών. Η υιοθέτηση τεχνικών που ενισχύουν την ανωνυμία και μειώνουν την έκθεση των χρηστών σε τέτοιου είδους κινδύνους είναι απαραίτητη για τη διασφάλιση της ιδιωτικότητας στο σύγχρονο ψηφιακό περιβάλλον.

#### 3.3.1.2 Κατάχρηση δεδομένων

Μια από τις σημαντικότερες προκλήσεις που σχετίζονται με την ιδιωτικότητα στα CDN είναι ο κίνδυνος κατάχρησης των δεδομένων που συλλέγονται για φαινομενικά νόμιμους σκοπούς. Αν και τα CDN χρησιμοποιούν αυτά τα δεδομένα για τη βελτίωση της απόδοσης και της εμπειρίας του χρήστη, υπάρχει πάντα η πιθανότητα να αξιοποιηθούν με τρόπους που θέτουν σε κίνδυνο την ιδιωτικότητα των χρηστών ή ακόμη και να χρησιμοποιηθούν για κακόβουλες ενέργειες. Μερικοί από αυτούς τους τρόπους είναι οι κάτωθι [12] [75]:

- Αλλαγή σκοπού χρήσης δεδομένων
  Ένας κίνδυνος που αξίζει να σημειωθεί είναι η επαναχρησιμοποίηση των δεδομένων χωρίς τη συγκατάθεση των χρηστών. Για παράδειγμα, πληροφορίες που συλλέγονται

για τη βελτιστοποίηση της διανομής περιεχομένου μπορεί να αξιοποιηθούν για στοχευμένη διαφήμιση ή τη δημιουργία λεπτομερών προφίλ χρηστών. Αυτό μπορεί να οδηγήσει σε ανεπιθύμητη παρακολούθηση ή ακόμα και εμπορευματοποίηση των δεδομένων των χρηστών.

- Επιθέσεις και παραβιάσεις δεδομένων
  Τα CDN αποτελούν ελκυστικούς στόχους για επιθέσεις DDoS, καθώς χειρίζονται τεράστιο όγκο δεδομένων και δικτυακής κίνησης. Επιπλέον, είναι ευάλωτα σε επιθέσεις τύπου Cache poisoning (όπως διαπιστώθηκε στο προηγούμενο κεφάλαιο), όπου κακόβουλοι παράγοντες μπορούν να εισάγουν παραποιημένο περιεχόμενο, θέτοντας σε κίνδυνο την αξιοπιστία των δεδομένων. Αντίστοιχα, σε περίπτωση παραβίασης ενός CDN, υπάρχει ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες των χρηστών, γεγονός που μπορεί να έχει σοβαρές επιπτώσεις στην ιδιωτικότητα.

- Χρήση των CDN για λογοκρισία και επιτήρηση
  Παρόλο που τα CDN χρησιμοποιούνται για τη βελτίωση της προσβασιμότητας στο περιεχόμενο, μπορούν επίσης να αξιοποιηθούν για την επιβολή λογοκρισίας στο Διαδίκτυο. Αν κυβερνήσεις ή μεγάλες εταιρείες ελέγχουν τη διανομή περιεχομένου μέσω CDN, μπορούν να φιλτράρουν ή να αποκλείσουν συγκεκριμένες πληροφορίες, περιορίζοντας την ελεύθερη ροή δεδομένων.

- Forward και Backward Privacy
  Η έλλειψη διασφάλισης ιδιωτικότητας προς τα εμπρός (Forward Privacy) και προς τα πίσω (Backward Privacy) μπορεί να επιτρέψει σε έναν εισβολέα να συσχετίσει παλαιότερα αιτήματα με νέα, αποκαλύπτοντας ευαίσθητες πληροφορίες για τις συνήθειες περιήγησης των χρηστών και τη δημοτικότητα συγκεκριμένων αντικειμένων.

- Πολυπλοκότητα και κίνδυνοι στο DNS
  Το DNS παίζει πολύ σημαντικό ρόλο στην λειτουργία του CDN, κάτι το οποίο δημιουργεί αυξημένη πολυπλοκότητα στην διανομή περιεχομένου. Αυτό προκαλεί ευπάθειες που ενδέχεται να χρησιμοποιηθούν για την εκμετάλλευση δεδομένων, είτε μέσω επιθέσεων τύπου DNS hijacking είτε μέσω κακόβουλης ανακατεύθυνσης των χρηστών σε παραποιημένες σελίδες.

Για την προστασία της ιδιωτικότητας των χρηστών και την αποτροπή της κατάχρησης δεδομένων, είναι απαραίτητη η εφαρμογή ισχυρών μηχανισμών ασφαλείας, η διαφάνεια στις πολιτικές διαχείρισης δεδομένων και η ενίσχυση των μεθόδων κρυπτογράφησης στις επικοινωνίες μεταξύ χρηστών και CDN. Οι πάροχοι CDN θα πρέπει να διασφαλίζουν ότι τα

δεδομένα χρησιμοποιούνται μόνο για τον σκοπό που συλλέγονται και να υιοθετούν πρακτικές που προστατεύουν την ανωνυμία και την ασφάλεια των χρηστών.

#### 3.3.1.3 Inference Επιθέσεις

Ένα από τα προβλήματα που σχετίζονται με την ιδιωτικότητα στα CDN είναι η δυνατότητα εξαγωγής συμπερασμάτων, Inference επιθέσεων δηλαδή. Αυτό συμβαίνει όταν φαινομενικά αθώα ή μη ευαίσθητα δεδομένα συνδυάζονται και αναλύονται, οδηγώντας στην αποκάλυψη ευαίσθητων πληροφοριών για τους χρήστες. Παρόλο που τα δεδομένα μπορεί να μην είναι άμεσα προσωπικά, η διασταύρωση πληροφοριών μπορεί να αποκαλύψει στοιχεία όπως τα ενδιαφέροντα, τις πολιτικές απόψεις ή ακόμα και την υγεία ενός ατόμου [75].

- Συμπεράσματα από μη ευαίσθητα δεδομένα
  Ακόμα και αν τα CDN συλλέγουν μόνο πληροφορίες όπως η διεύθυνση IP, ο τύπος του browser ή η τοποθεσία του χρήστη, αυτά τα δεδομένα μπορούν να αναλυθούν για να εξαχθούν συμπεράσματα σχετικά με τη συμπεριφορά, τις συνήθειες ή ακόμη και την ψυχολογική κατάσταση των χρηστών. Η ανάλυση μοτίβων στη διαδικτυακή δραστηριότητα μπορεί να οδηγήσει στη δημιουργία ακριβών προφίλ χρηστών χωρίς τη συναίνεσή τους.

- Συνδυασμός δεδομένων από πολλαπλές πηγές
  Η δύναμη των CDN έγκειται στην εκτεταμένη συλλογή και επεξεργασία δεδομένων από πολλές διαφορετικές πηγές. Ο συνδυασμός δεδομένων από πλατφόρμες διαφήμισης, κοινωνικά δίκτυα και αρχεία επισκεψιμότητας μπορεί να δημιουργήσει ένα ολοκληρωμένο και εξαιρετικά ακριβές προφίλ ενός χρήστη, αποκαλύπτοντας πληροφορίες που κανένα μεμονωμένο σύστημα δεν θα μπορούσε να αντλήσει από μόνο του.

- Web Page Fingerprinting (WPF) και παρακολούθηση δραστηριότητας
  Μια τεχνική που εκμεταλλεύεται αυτή τη δυνατότητα είναι το Web Page Fingerprinting (WPF), το οποίο επιτρέπει σε εισβολείς να εντοπίζουν ποιες σελίδες επισκέπτεται ένας χρήστης μέσα σε έναν ιστότοπο. Με την παθητική συλλογή δεδομένων επισκεψιμότητας, ένας εισβολέας μπορεί να κατηγοριοποιήσει και να συσχετίσει ιστοσελίδες με συγκεκριμένα προφίλ χρηστών, θέτοντας σε κίνδυνο την ανωνυμία τους.

- Παραδείγματα εξαγωγής συμπερασμάτων
  Οι τεχνικές ανάλυσης δεδομένων των CDN μπορούν να οδηγήσουν σε εξαιρετικά ακριβή και ευαίσθητα συμπεράσματα. Για παράδειγμα, η ανάλυση των ιστοσελίδων που επισκέπτεται ένας χρήστης μπορεί να αποκαλύψει τη σεξουαλική του ταυτότητα, τις πολιτικές του πεποιθήσεις ή ακόμα και ιατρικές καταστάσεις από τις αναζητήσεις που πραγματοποιεί. Αυτές οι πληροφορίες, αν πέσουν σε λάθος χέρια, μπορούν να

χρησιμοποιηθούν για διακρίσεις, στοχευμένες επιθέσεις ή ανεπιθύμητη εκμετάλλευση των χρηστών.

- Πιθανοί κίνδυνοι από την εξαγωγή συμπερασμάτων
  Η ανεξέλεγκτη εξαγωγή συμπερασμάτων μπορεί να οδηγήσει σε σοβαρές συνέπειες για τους χρήστες, όπως αποκλεισμό από υπηρεσίες, δυναμική τιμολόγηση προϊόντων ή ακόμη και χειραγώγηση της πληροφόρησής τους. Για παράδειγμα, ένας χρήστης μπορεί να βλέπει υψηλότερες τιμές για συγκεκριμένα προϊόντα με βάση το προφίλ του ή να λαμβάνει στοχευμένες πολιτικές διαφημίσεις που ενισχύουν συγκεκριμένες απόψεις, περιορίζοντας έτσι την ελευθερία επιλογής του.

- Μετριασμός των κινδύνων
  Για την αντιμετώπιση αυτών των προβλημάτων, είναι απαραίτητη η εφαρμογή ισχυρών πολιτικών προστασίας δεδομένων, η διαφάνεια στις πρακτικές συλλογής πληροφοριών και η χρήση τεχνικών ανωνυμοποίησης ή ψευδωνυμοποίησης όπου είναι δυνατόν. Η περιορισμένη συλλογή δεδομένων και η υιοθέτηση τεχνικών που αποτρέπουν τη συσχέτιση πληροφοριών μπορούν να συμβάλουν σημαντικά στη μείωση των κινδύνων που προκύπτουν από την εξαγωγή συμπερασμάτων.

Η προστασία της ιδιωτικότητας στα CDN δεν αφορά μόνο την ασφάλεια των δεδομένων αλλά και την πρόληψη των έμμεσων απειλών που προκύπτουν από τη μαζική ανάλυση και επεξεργασία πληροφοριών. Η διασφάλιση των δικαιωμάτων των χρηστών απαιτεί συνεχή επαγρύπνηση και αυστηρότερες πολιτικές, ώστε η τεχνολογία να χρησιμοποιείται με τρόπο που σέβεται την ιδιωτική ζωή των ατόμων.

#### 3.3.1.4 Λογοκρισία στο Διαδίκτυο

Ένα από τα πιο ανησυχητικά ζητήματα που συνδέονται με τα CDN είναι η πιθανή χρήση τους για την επιβολή λογοκρισίας στο Διαδίκτυο. Παρόλο που τα CDN έχουν σχεδιαστεί για τη βελτίωση της ταχύτητας και της διαθεσιμότητας του διαδικτυακού περιεχομένου, μπορούν επίσης να χρησιμοποιηθούν για να ελέγχουν ή να περιορίζουν την πρόσβαση σε πληροφορίες, είτε μέσω κυβερνητικών πιέσεων είτε λόγω εταιρικών πολιτικών [19].

- Επιβολή κυβερνητικών πολιτικών λογοκρισίας
  Σε πολλές χώρες, οι κυβερνήσεις απαιτούν από τις εταιρείες CDN να συμμορφώνονται με πολιτικές λογοκρισίας, αποκλείοντας την πρόσβαση σε ιστότοπους που θεωρούνται παράνομοι ή επικίνδυνοι. Αυτό μπορεί να περιλαμβάνει ειδησεογραφικές ιστοσελίδες, πλατφόρμες κοινωνικής δικτύωσης ή ακόμα και ιστοσελίδες ακτιβισμού που αντιτίθενται στο εκάστοτε καθεστώς.

- Αποκλεισμός περιεχομένου
  Τα CDN μπορούν να μπλοκάρουν συγκεκριμένα είδη περιεχομένου είτε λόγω κυβερνητικών εντολών είτε στο πλαίσιο των εσωτερικών πολιτικών μιας εταιρείας. Για παράδειγμα, μπορεί να περιορίζεται η πρόσβαση σε ιστότοπους που φιλοξενούν περιεχόμενο το οποίο θεωρείται επιβλαβές, πολιτικά αμφιλεγόμενο ή αντίθετο με τα εμπορικά συμφέροντα της εταιρείας που διαχειρίζεται το CDN.

- Χειραγώγηση και φιλτράρισμα περιεχομένου
  Εκτός από τον αποκλεισμό ιστοσελίδων, τα CDN μπορούν να χρησιμοποιηθούν για την τροποποίηση του περιεχομένου που φτάνει στους χρήστες. Αυτό μπορεί να γίνει μέσω φιλτραρίσματος πληροφοριών, αλλοίωσης ειδησεογραφικών άρθρων ή ακόμη και αποκλεισμού συγκεκριμένων λέξεων-κλειδιών. Σε ορισμένες περιπτώσεις, οι χρήστες μπορεί να λαμβάνουν διαφορετική εκδοχή μιας ιστοσελίδας, ανάλογα με την τοποθεσία ή το προφίλ τους.

- Επιπτώσεις στην ελευθερία του λόγου
  Η χρήση των CDN για την επιβολή λογοκρισίας επηρεάζει άμεσα τη δημοκρατία και την ελευθερία του λόγου. Ο περιορισμός της πρόσβασης σε πληροφορίες μπορεί να οδηγήσει σε παραπληροφόρηση, χειραγώγηση της κοινής γνώμης και έλεγχο των αφηγήσεων που διαδίδονται στο Διαδίκτυο.

- Αντίσταση στη λογοκρισία
  Για την αντιμετώπιση της λογοκρισίας μέσω CDN, είναι απαραίτητο να αναπτυχθούν πολιτικές και τεχνολογίες που προωθούν την ελεύθερη ροή της πληροφορίας. Η διαφάνεια στις πολιτικές περιεχομένου των CDN, η χρήση κρυπτογραφημένων επικοινωνιών και η ανάπτυξη αποκεντρωμένων τεχνολογιών είναι μερικές από τις στρατηγικές που μπορούν να προστατεύσουν την πρόσβαση στην πληροφορία.

- Χρήση των CDN για την παράκαμψη λογοκρισίας
  Ενώ τα CDN μπορούν να χρησιμοποιηθούν για λογοκρισία, μπορούν επίσης να αξιοποιηθούν για την καταπολέμησή της. Κάποιες υπηρεσίες χρησιμοποιούν CDN για να διασφαλίσουν την απρόσκοπτη διανομή περιεχομένου σε περιοχές όπου εφαρμόζονται περιορισμοί. Ένα CDN μπορεί να λειτουργήσει ως μέσο εξισορρόπησης της διαδικτυακής λογοκρισίας, διανέμοντας πληροφορίες από ασφαλείς διακομιστές που βρίσκονται εκτός των περιοχών όπου ισχύουν περιορισμοί.

Η λογοκρισία στο Διαδίκτυο μέσω CDN αποτελεί μια πολυδιάστατη πρόκληση, καθώς μπορεί να επηρεάσει τόσο την ελευθερία του λόγου όσο και τη δυνατότητα των χρηστών να έχουν πρόσβαση σε ακριβή και ανεξάρτητη πληροφόρηση. Για να διασφαλιστεί ένα ελεύθερο και ανοιχτό Διαδίκτυο, είναι κρίσιμο να αναπτυχθούν μηχανισμοί που θα εξισορροπούν τη χρήση των CDN προς όφελος της πληροφόρησης και όχι προς τον έλεγχό της.

### 3.3.2 Κανονιστικό Πλαίσιο και Μέτρα για την Προστασία της Ιδιωτικότητας στο Content Delivery Network (CDN)

Κατά τη λειτουργία ενός CDN, η συμμόρφωση με τους κανονισμούς προστασίας δεδομένων είναι ζωτικής σημασίας. Βασικά παραδείγματα κανονισμών είναι τα κάτωθι:

- Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) ο οποίος ρυθμίζει την προστασία της ιδιωτικότητας στην Ευρωπαϊκή Ένωση.
- Ο California Consumer Privacy Act (CCPA) που ορίζει το πλαίσιο προστασίας ιδιωτικότητας σχετικά με τους κατοίκους της Καλιφόρνιας.
- Ο Health Insurance Portability and Accountability Act (HIPAA) ο οποίος καθορίζει κανόνες για την προστασία των ιατρικών δεδομένων.
- Το Payment Card Industry Data Security Standard (PCI-DSS), το οποίο διασφαλίζει την ασφάλεια των συναλλαγών με πιστωτικές κάρτες.

Δεδομένου ότι τα CDN αποθηκεύουν και επεξεργάζονται πληροφορίες χρηστών σε διάφορες γεωγραφικές τοποθεσίες, προκύπτουν υποχρεώσεις συμμόρφωσης με διαφορετικούς κανονισμούς προστασίας δεδομένων. Η κατανεμημένη φύση ενός CDN απαιτεί ιδιαίτερη προσοχή στη μεταφορά, την αποθήκευση και τη διατήρηση δεδομένων, ώστε να τηρούνται οι τοπικοί κανονισμοί. Για παράδειγμα, αν ένας διακομιστής CDN βρίσκεται εντός της Ευρωπαϊκής Ένωσης, η διαχείριση των δεδομένων πρέπει να είναι σύμφωνη με τις απαιτήσεις του GDPR.

Ένας πάροχος CDN επίσης πρέπει να λαμβάνει συγκεκριμένα μέτρα συμμόρφωσης, όπως η εφαρμογή ισχυρών ελέγχων πρόσβασης, η κρυπτογράφηση δεδομένων και η πραγματοποίηση τακτικών ελέγχων ασφαλείας, προκειμένου να προστατεύει τις προσωπικές και ευαίσθητες πληροφορίες που διαχειρίζεται. Παράλληλα, απαιτείται η διασφάλιση της συγκατάθεσης των χρηστών για τη συλλογή και επεξεργασία των δεδομένων τους, η ύπαρξη διαφανούς πολιτικής απορρήτου και η τήρηση των δικαιωμάτων των χρηστών, όπως η πρόσβαση και η δυνατότητα διαγραφής των δεδομένων τους.

Σε περίπτωση παραβίασης δεδομένων, οι πάροχοι CDN υποχρεούνται να ακολουθήσουν διαδικασίες ενημέρωσης, ειδοποιώντας τόσο τους επηρεαζόμενους χρήστες όσο και τις αρμόδιες αρχές, ενώ παράλληλα πρέπει να εφαρμόσουν άμεσα διορθωτικά μέτρα. Η υιοθέτηση αυτών των πρακτικών δεν αποσκοπεί μόνο στην αποφυγή νομικών κυρώσεων αλλά συμβάλλει καθοριστικά στη διατήρηση της εμπιστοσύνης των χρηστών, καθιστώντας τη συμμόρφωση αναπόσπαστο μέρος της λειτουργίας ενός CDN [76].

#### 3.3.2.1 Καλές Πρακτικές

Η προστασία της Ιδιωτικότητας στο CDN καθώς και η συμμόρφωση με τους ισχύοντες κανονισμούς απαιτεί την αντιμετώπιση προκλήσεων που σχετίζονται με την ιδιωτικότητα και

την ασφάλεια των δεδομένων καθώς επίσης την υιοθέτηση καλών πρακτικών. Υπογραμμίζονται επίσης τα ακόλουθα:

**Απαιτήσεις Data Localization**

Σε έναν διαρκώς συνδεδεμένο ψηφιακό κόσμο, η τοποθεσία όπου αποθηκεύονται τα δεδομένα έχει μεγάλη σημασία. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση, απαιτεί τα προσωπικά δεδομένα να παραμένουν εντός των συνόρων της περιοχής. Για να συμμορφωθεί ένα CDN με αυτούς τους κανονισμούς, πρέπει να έχει γεωγραφικά κατανεμημένη υποδομή. Η στρατηγική τοποθέτηση των διακομιστών του CDN σε περιοχές με συγκεκριμένες απαιτήσεις σχετικά την γεωγραφική αποθήκευση των δεδομένων αποτελεί βασικό βήμα για τη συμμόρφωση. Αυτό απαιτεί συνεργασία με νομικούς και ειδικούς συμμόρφωσης, ώστε να διασφαλιστεί ότι η αποθήκευση και η επεξεργασία των δεδομένων γίνονται με τρόπο που να πληροί τις σχετικές νομοθετικές απαιτήσεις.

**Σαφείς Συμβάσεις Επεξεργασίας Δεδομένων**

Η ύπαρξη ξεκάθαρων συμβάσεων επεξεργασίας δεδομένων (DPAs) με τους παρόχους CDN και τρίτους που εμπλέκονται στη διαχείριση δεδομένων είναι απαραίτητη. Αυτές οι συμφωνίες καθορίζουν τις υποχρεώσεις κάθε πλευράς ως προς την προστασία των δεδομένων και διασφαλίζουν τη δέσμευση όλων στη συμμόρφωση. Στα βασικά στοιχεία μιας τέτοιας συμφωνίας περιλαμβάνονται η διαδικασία ειδοποίησης σε περίπτωση παραβίασης δεδομένων, η διαγραφή τους όταν δεν είναι πλέον απαραίτητα και οι μηχανισμοί μεταφοράς τους. Αυτά τα μέτρα ενισχύουν τη διαφάνεια και τη λογοδοσία, που είναι κρίσιμα για τη συμμόρφωση με τους κανονισμούς ασφαλείας των CDN.

**Τακτικοί Έλεγχοι Ασφαλείας και Αξιολόγηση Ευπαθειών (Vulnerability Assessments)**

Ο εντοπισμός πιθανών κενών συμμόρφωσης στην υποδομή ενός CDN απαιτεί τακτικούς ελέγχους ασφαλείας και αξιολογήσεις ευπαθειών. Ειδικοί ασφαλείας, εσωτερικοί ή εξωτερικοί, μπορούν να αξιολογήσουν τα συστήματα, τις ρυθμίσεις και τα δικαιώματα πρόσβασης για να εντοπίσουν πιθανά προβλήματα. Τα όποια κενά ασφαλείας πρέπει να αντιμετωπίζονται άμεσα, ενώ οι απαραίτητες βελτιώσεις πρέπει να εφαρμόζονται χωρίς καθυστέρηση. Αυτή η προληπτική προσέγγιση συμβάλλει στη διατήρηση μιας ισχυρής συμμόρφωσης και εξασφαλίζει ότι το CDN πληροί τις κανονιστικές απαιτήσεις.

**Εκπαίδευση Προσωπικού για Θέματα Συμμόρφωσης**

Η συμμόρφωση καθώς και η διασφάλιση της Ιδιωτικότητας δεν εξαρτάται αποκλειστικά από τεχνολογικές λύσεις και διαδικασίες, αλλά και από τους ανθρώπους που διαχειρίζονται τα δεδομένα. Η εκπαίδευση του προσωπικού που εμπλέκεται στις λειτουργίες ενός CDN είναι ζωτικής σημασίας, ώστε να ακολουθείται σωστά το ρυθμιστικό πλαίσιο. Τα εκπαιδευτικά προγράμματα πρέπει να καλύπτουν τους κανονισμούς προστασίας προσωπικών δεδομένων, τις βέλτιστες πρακτικές ασφάλειας και τις διαδικασίες αντιμετώπισης περιστατικών.

### 3.3.2.2 Αξιοποίηση Τεχνολογιών CDN για την Ενίσχυση της Συμμόρφωσης με το Ισχύον Νομικό και Κανονιστικό Πλαίσιο και για την Διασφάλιση της Ιδιωτικότητα σε Περιβάλλοντα Content Delivery Network (CDN)

Η συμμόρφωση ενός CDN και κατ' επέκταση η διασφάλιση της Ιδιωτικότητας μπορεί να ενισχυθεί μέσα από τη σωστή αξιοποίηση των δυνατοτήτων του [76].

**Έλεγχος Πρόσβασης**

Οι λειτουργίες ελέγχου πρόσβασης, όπως το IP whitelisting, το geo-blocking και ο έλεγχος πρόσβασης μέσω tokens, μπορούν να περιορίσουν την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες.

- Το IP whitelisting επιτρέπει την πρόσβαση μόνο από έμπιστες διευθύνσεις IP, μειώνοντας σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης.
- Το geo-blocking μπορεί να περιορίσει την πρόσβαση σε περιεχόμενο βάσει τοποθεσίας, συμβάλλοντας στη συμμόρφωση με περιφερειακούς κανονισμούς προστασίας δεδομένων.
- Ο έλεγχος μέσω tokens προσθέτει ένα επιπλέον επίπεδο προστασίας, απαιτώντας έγκυρα διαπιστευτήρια πριν από την πρόσβαση σε ευαίσθητες πληροφορίες.

**Χρήση Edge Computing για την Διασφάλιση της Ιδιωτικότητας**

Η επεξεργασία δεδομένων στην άκρη του δικτύου (Edge) μπορεί να βελτιώσει σημαντικά την προστασία της ιδιωτικότητας. Με τη χρήση τεχνικών όπως η ανωνυμοποίηση, η κρυπτογράφηση και η τοκενοποίηση δεδομένων πριν από την αποθήκευση ή επεξεργασία τους, μειώνεται ο κίνδυνος διαρροής ή παραβίασης.

Επιπλέον, η κρυπτογράφηση δεδομένων στην άκρη του δικτύου (Edge) μειώνει την έκθεση των δεδομένων σε μη εξουσιοδοτημένη πρόσβαση τόσο κατά τη μεταφορά όσο και κατά την αποθήκευση.

**Real-Time Monitoring και Καταγραφή σε Πραγματικό Χρόνο**

Το Monitoring σε πραγματικό χρόνο επιτρέπει την άμεση ανίχνευση και αντιμετώπιση παραβιάσεων συμμόρφωσης ή περιστατικών ασφαλείας.

- Εξειδικευμένα εργαλεία μπορούν να αναλύσουν την κίνηση του CDN, τις απόπειρες πρόσβασης και τη συμπεριφορά των χρηστών, εντοπίζοντας ύποπτες δραστηριότητες.
- Αναλυτικά αρχεία καταγραφής διευκολύνουν την έρευνα περιστατικών και την αναφορά παραβάσεων.
- Η ενσωμάτωση των συστημάτων παρακολούθησης με διαδικασίες απόκρισης σε περιστατικά διασφαλίζει ότι οι απειλές αντιμετωπίζονται έγκαιρα και αποτελεσματικά.

**Ενημέρωση για Νέες Τεχνολογίες και Βέλτιστες Πρακτικές**

Η συνεχής ενημέρωση σχετικά με τις εξελίξεις στην ασφάλεια CDN και τις βέλτιστες πρακτικές της βιομηχανίας είναι ζωτικής σημασίας.

- Οι ρυθμίσεις ασφαλείας, οι αλγόριθμοι κρυπτογράφησης και οι μηχανισμοί ελέγχου πρόσβασης πρέπει να αναθεωρούνται και να ενημερώνονται τακτικά.
- Η συμμετοχή σε συνέδρια, ομάδες εργασίας και φόρουμ ασφαλείας παρέχει πολύτιμες γνώσεις για τις προκλήσεις συμμόρφωσης και τις αναδυόμενες λύσεις.
- Η συνεργασία με ειδικούς ασφαλείας και παρόχους CDN μπορεί να βελτιώσει διαρκώς την ασφάλεια του συστήματος και να διασφαλίσει τη συμμόρφωση με τα ισχύοντα πρότυπα.

Η συμμόρφωση ενός CDN με τους κανονισμούς περί προστασίας δεδομένων απαιτεί μια στρατηγική προσέγγιση, η οποία περιλαμβάνει ελέγχους πρόσβασης, αξιοποίηση edge computing, Monitoring σε πραγματικό χρόνο και συνεχή ενημέρωση. Η εφαρμογή αυτών των πρακτικών δεν είναι απλώς μια νομική υποχρέωση, αλλά και βασικός παράγοντας για την οικοδόμηση εμπιστοσύνης με τους χρήστες και την προστασία της ιδιωτικότητας.

## 3.4 Akamai Content Delivery Network (CDN) και Προστασία της Ιδιωτικότητας

Η Akamai δεσμεύεται για την προστασία της ιδιωτικότητας και τη συμμόρφωση με τους διεθνείς κανονισμούς προστασίας δεδομένων, εφαρμόζοντας ένα ολοκληρωμένο σύστημα πολιτικών και διαδικασιών. Η προσέγγισή της καλύπτει κάθε στάδιο επεξεργασίας δεδομένων, από τη συλλογή και αποθήκευση έως τη μεταφορά και διαχείρισή τους, με στόχο την ασφάλεια και τη διαφάνεια.

**Συμμόρφωση με τους Διεθνείς Νόμους Προστασίας Δεδομένων**

Η Akamai παρακολουθεί τις νομοθετικές εξελίξεις και συμμορφώνεται με σημαντικούς κανονισμούς προστασίας δεδομένων, όπως:

- GDPR (Γενικός Κανονισμός Προστασίας Δεδομένων) της Ευρωπαϊκής Ένωσης, που θέτει αυστηρές απαιτήσεις για τη διαχείριση των προσωπικών δεδομένων.
- CCPA (California Consumer Privacy Act), που προστατεύει τα προσωπικά δεδομένα των κατοίκων της Καλιφόρνιας.
- LGPD (Lei Geral de Proteção de Dados) της Βραζιλίας, που επιβάλλει κανόνες επεξεργασίας δεδομένων στο πλαίσιο των διεθνών προτύπων.
- PIPEDA (Personal Information Protection and Electronic Documents Act) του Καναδά, που ρυθμίζει τη χρήση προσωπικών πληροφοριών από οργανισμούς.

**Βασικές Αρχές Επεξεργασίας Δεδομένων**

Η Akamai ακολουθεί συγκεκριμένες αρχές στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα:

- Περιορισμένη συλλογή και επεξεργασία: Συλλέγονται μόνο τα απολύτως απαραίτητα δεδομένα, ανάλογα με τον σκοπό χρήσης τους.
- Δίκαιη και νόμιμη επεξεργασία: Όλες οι διαδικασίες συμμορφώνονται με τις νομικές απαιτήσεις και τα δικαιώματα των υποκειμένων των δεδομένων.
- Ασφάλεια και μείωση κινδύνων: Υιοθετούνται μέτρα για την ελαχιστοποίηση των επιπτώσεων της επεξεργασίας δεδομένων και την προστασία τους από παραβιάσεις.

**Ρόλος της Akamai στην Επεξεργασία Δεδομένων**

Η Akamai δραστηριοποιείται ως εκτελών την επεξεργασία ή ως υπεύθυνος επεξεργασίας, ανάλογα με τις συνθήκες:

- Ως εκτελών την επεξεργασία, χειρίζεται δεδομένα για λογαριασμό των πελατών της, σύμφωνα με τις οδηγίες τους.
- Ως υπεύθυνος επεξεργασίας, καθορίζει τον σκοπό και τα μέσα της επεξεργασίας δεδομένων, όπως τα αρχεία καταγραφής, τα στοιχεία επικοινωνίας και τις τηλεφωνικές συνομιλίες.

**Πολιτική Χειρισμού Διευθύνσεων IP**

Η Akamai αντιμετωπίζει τις διευθύνσεις IP ως δεδομένα προσωπικού χαρακτήρα, καθώς μπορούν να χρησιμοποιηθούν για την ταυτοποίηση χρηστών. Οι διευθύνσεις IP θεωρούνται ευαίσθητες, ιδίως όταν συνδυάζονται με άλλα δεδομένα, και υπόκεινται σε αυστηρές πολιτικές προστασίας.

**Διατήρηση Δεδομένων**

Τα δεδομένα διατηρούνται μόνο για όσο διάστημα είναι απαραίτητο, σύμφωνα με τις πολιτικές ασφαλείας και συμμόρφωσης της Akamai. Με αυτόν τον τρόπο, αποφεύγεται η άσκοπη διατήρηση πληροφοριών, ενώ μειώνονται οι κίνδυνοι παραβίασης.

**Διεθνείς Μεταφορές Δεδομένων**

Για τις διεθνείς μεταφορές δεδομένων, η Akamai διασφαλίζει ότι οι παραλήπτες τηρούν αυστηρά πρότυπα προστασίας. Οι μεταφορές δεδομένων γίνονται μέσω κατάλληλων νομικών και τεχνικών διασφαλίσεων, διατηρώντας το ίδιο επίπεδο προστασίας που απαιτούν οι κανονισμοί.

**Διαφάνεια και Συμφωνίες Επεξεργασίας**

Η Akamai δημοσιεύει δήλωση απορρήτου, στην οποία περιγράφονται αναλυτικά οι διαδικασίες επεξεργασίας δεδομένων. Παράλληλα, παρέχει στους πελάτες της συμφωνίες επεξεργασίας δεδομένων και τεχνικά μέτρα που διασφαλίζουν την προστασία των προσωπικών πληροφοριών.

**Επιλογές Ελέγχου για Πελάτες**

Οι πελάτες της Akamai έχουν στη διάθεσή τους εργαλεία που τους επιτρέπουν να διαμορφώνουν τις υπηρεσίες της, καθορίζοντας τον τρόπο με τον οποίο τα δεδομένα προσωπικού χαρακτήρα διέρχονται από το δίκτυό της. Ωστόσο, η ευθύνη συμμόρφωσης με τους κανονισμούς επεξεργασίας δεδομένων ανήκει στους ίδιους τους πελάτες.

**Μέτρα Ασφαλείας για την Προστασία Δεδομένων**

Για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη ή καταστροφή, η Akamai εφαρμόζει ένα σύνολο αυστηρών μέτρων ασφαλείας, τα οποία περιλαμβάνουν:

- Φυσική ασφάλεια, με προστατευμένες εγκαταστάσεις και ελεγχόμενη πρόσβαση στα κέντρα δεδομένων.
- Τεχνικές διασφαλίσεις, όπως κρυπτογράφηση, έλεγχος ταυτότητας και μηχανισμοί προστασίας από κυβερνοεπιθέσεις.
- Διοικητικά μέτρα, με πολιτικές ασφαλείας, εκπαίδευση προσωπικού και ελέγχους συμμόρφωσης.

Η Akamai εφαρμόζει ένα ολοκληρωμένο σύστημα προστασίας δεδομένων, προσαρμοσμένο στις διεθνείς απαιτήσεις συμμόρφωσης. Με σαφείς πολιτικές διαχείρισης, μέτρα ασφαλείας και διαφανείς διαδικασίες, διασφαλίζει ότι τα προσωπικά δεδομένα επεξεργάζονται με ασφάλεια, διατηρώντας υψηλό επίπεδο εμπιστοσύνης μεταξύ των χρηστών και των συνεργατών της.

# Συμπεράσματα

Η παρούσα εργασία ανέλυσε την ασφάλεια και την προστασία της ιδιωτικότητας στα Content Delivery Networks (CDN), τα οποία αποτελούν κρίσιμες υποδομές για την ταχεία και αποδοτική διανομή ψηφιακού περιεχομένου. Μέσα από την εξέταση της αρχιτεκτονικής τους, των προκλήσεων ασφάλειας και των μέτρων προστασίας, έγινε σαφές ότι τα CDN διαδραματίζουν σημαντικό ρόλο στη σύγχρονη διαδικτυακή εμπειρία, αλλά ταυτόχρονα είναι εκτεθειμένα σε πλήθος απειλών.

Οι κυριότεροι κίνδυνοι που αντιμετωπίζουν τα CDN περιλαμβάνουν επιθέσεις DDoS, επιθέσεις σε Edge Servers, αποκάλυψη του Origin Server, καθώς και παραβιάσεις ιδιωτικότητας μέσω ανεξέλεγκτης συλλογής και διαχείρισης δεδομένων χρηστών. Οι υφιστάμενοι μηχανισμοί άμυνας, όπως τα Web Application Firewalls (WAF), οι στρατηγικές Anti-DDoS και οι τεχνολογίες κρυπτογράφησης, αποτελούν ζωτικής σημασίας εργαλεία για την προστασία των δικτύων αυτών.

Παράλληλα, η συμμόρφωση με κανονιστικά πλαίσια όπως το GDPR και το NIS-2 καθίσταται επιτακτική, καθώς τα CDN διαχειρίζονται μεγάλο όγκο προσωπικών δεδομένων. Η εφαρμογή Privacy by Design, η υιοθέτηση ανώνυμων μηχανισμών μετάδοσης δεδομένων και η συνεχής παρακολούθηση των απειλών είναι καθοριστικοί παράγοντες για την προστασία της ιδιωτικότητας των χρηστών.

Μέσα από τη μελέτη περίπτωσης του Akamai CDN, διαπιστώθηκε ότι οι κορυφαίοι πάροχοι CDN επενδύουν σε καινοτόμες τεχνολογίες ασφάλειας, αναπτύσσοντας προηγμένες μεθόδους ανίχνευσης επιθέσεων, δυναμικής κρυπτογράφησης και αυτοματοποιημένης διαχείρισης κινδύνων.

Συμπερασματικά, η προστασία των CDN δεν είναι μια στατική διαδικασία, αλλά απαιτεί διαρκή προσαρμογή στις νέες απειλές, βελτιστοποίηση των υφιστάμενων μηχανισμών άμυνας και ευθυγράμμιση με τις σύγχρονες νομοθετικές απαιτήσεις. Η ενσωμάτωση τεχνητής νοημοσύνης και τεχνικών αυτοματοποιημένης ασφάλειας αναμένεται να διαδραματίσει καταλυτικό ρόλο στο μέλλον, επιτρέποντας στα CDN να παραμείνουν αξιόπιστα, ασφαλή και συμβατά με τις ανάγκες των χρηστών και των οργανισμών που τα αξιοποιούν.

# Βιβλιογραφία


[1] What Is a CDN (Content Delivery Network)? | How Do CDNs Work? | Akamai
[2] What Is A CDN? Content Delivery Networks Explained - CDNetworks
[3] Azure Content Delivery Network | Microsoft Azure
[4] The Akamai Network: A Platform for High-Performance Internet Applications, E.Nygren, K.Sitamaran, J.Sun
[5] Content Delivery Network Security: A Survey, M. Ghaznavi, E. Jalalpour, A. Salahuddin, R. Boutaba, D. Migault, S. Preda
[6] A survey of web cache replacement strategies: ASM Comput.Surv. S.Podlipinig, L. Boszormenyi
[7] A taxonomy of cdns, Content Delivery Networks, M.Pathan
[8] Request-routing trends and techniques in content distribution network, M.H Kabir, E.G.Manning, G.Shoja
[9] Social network analysis inspired content placement with QoS in cloud based content delivery networks, M. A. Salahuddin, H. Elbiaze, W. Ajib, and R. Glitho
[10] Push or pull? toward optimal content delivery using cloud storage, X. Guan and B. Choi
[11] Netflix, Netflix open connect https://openconnect.netflix.com/
[12] Cdn's dark side: Security Problems in cdn-to-origin connections, B. Shobiri
[13] International Journal of Advamced Research, Volume 10, Issue 7, July 2021
[14] Understanding and Characterizing CDN Services and Paid Features, Youwei Xu
[15] An efficient approach for (multi-) cdn identification, M.Zhou, J.Zheng, G.Chen, W.Dou
[16] CDNs meet CN an empirical study of CDN deployments in China, D.Choffnes, J.Wang
[17] Active tls stack fingerprinting: characterizing tls server deployments at scale, M/Sosnowski, J.Zirngibl, P.Sattler, G.Carle, C.Grohnfeldt, M.Russo, D.Sgandurra.
[18] Abusing cdns for fun and profit: Security issues in cdn's origin validation, R.Guo, J.Chen, B.Liu, C.Zhangm H.Duan, T.Wan, J.Jiang, S.Hao, Y.Jia.
[19] Cdn Judo: Breaking the cdn dos protection with itself, R.Guo, W.Li, B.Liu, S.Hao, J.Zhang, H.Duan, K.Sheng, J.Chen, Y.Liu.
[20] Characterizing the deployment and performance of multi-cdns, R.Singh, A.Runna, P.Gill.
[21] Verified CDN Usage Distribution in the Top 1 Million Sites https://trends.builtwith.com/cdns
[22] Verified CDN Usage Distribution in Greece, https://trends.builtwith.com/cdns/country/Greece
[23] Content Delivery Network (CDN) Market Size, Share, and Trends 2025 to 2034, S.Zoting, A.Shivarkar, https://www.precedenceresearch.com/content-delivery-network-market
[24] Ασφάλεια Πληροφοριακών Συστημάτων, Σ. Κάτσικας, Δ.Γκρίτζαλης, Σ. Γκρίτζαλης
[25] Anddromeda:Accurate and scalable security analysis of web applications, O.Tripp, M.Pistoia, P.Cousot, S.Guarnieri.
[26] Ssl/tls interception proxies and transitive trust, J.Jarmoc and D. Unit
[27] Reusable garbled circuits and succinct functional encryption, S. Goldwasser, Y. Kalai, R. A. Popa
[28] Content delivery networks: Protection or threat?, S. Triukose, Z. Al-Qudah, and M. Rabinovich
[29] Lightweight resource management for ddos traffic isolation in a cloud environment, I. Mubarok, K. Lee, S. Lee, and H. Lee
[30] Practical web cache poisoning, J.Kettle
[31] How cloudflare protects customers from cache poisoning, J.Levine
[32] Web cache deception attack, O.Gil
[33] Web cache deception attack revisited, K.Cheung

[34] Your cache has fallen: Cache-poisoned denial-of-service attack, V. Nguyen, L. L. Iacono, and H. Federrath
[35] Cpdos poisoning attack, AKAMAI, 2019
[36] Cloudflare response to cpdos exploits, R. Lalkak
[37] A moving target defense approach to mitigate ddos attacks against proxy-based architectures, S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, M. Wright
[38] Unveil the hidden presence: Characterizing the backend interface of content delivery networks, L. Jin, S. Hao, H. Wang, and C. Cotton
[39] General data protection regulation, https: //gdpr-info.eu
[40] Host of troubles: Multiple host ambiguities in http implementations, J. Chen, J. Jiang, H. Duan, N. Weaver, T. Wan, and V. Paxson
[41] Forwarding loop attacks in content delivery networks, J. Chen, J. Jiang, X. Zheng, H. Duan, J. Liang, K. Lik, T. Wan, and V. Paxson
[42] Hypertext transfer protocol (http/1.1): Message syntax and routing, R. Fielding and J. Reschke
[49] Abusing cdns for fun and profit: Security issues in cdns, R. Guo, J. Chen, B. Liu, J. Zhang, C. Zhang, H. Duan, T. Wan, J. Jiang, S. Hao
[44] Loop detection in content delivery networks (cdns), S. Ludin, M. Nottingham, and N. Sullivan
[45] Your state is not mine: A closer look at evading stateful internet censorship, Z. Wang, Y. Cao, Z. Qian, C. Song
[46] Fragmentation considered poisonous, or: One domain to rule them all?, A. Herzberg and H. Shulman
[47] Mapping the expansion of google's serving infrastructure, . Calder, X. Fan, Z. Hu, E. Katz-Bassett, J. Heidemann, R. Govindan
[48] Measures for making dns more resilient against forged answers, A. Hubert and R. van Mook
[49] Clarifications to the DNS specification, R. Elz, R. Bush
[50] Increased dns forgery resistance through 0x20-bit encoding: Security via leet queries, D. Dagon, M. Antonakakis, P. Vixie, T. Jinmei, and W. Lee
[51] Measurement and analysis of private key sharing in the https ecosystem, F. Cangialosi, T. Chung, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson
[52] When https meets cdn: A case of authentication in delegated service, J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu
[53] Keyless ssl: The nitty gritty technical details, N. Sullivan
[54] Achieving keyless cdns with conclaves, S. Herwig, C. Garman
[55] Your remnant tells secret: Residual resolution in ddos protection services, L. Jin, S. Hao, H. Wang
[56] Maneuvering around clouds: Bypassing cloud-based security providers, T. Vissers, T. Van Goethem, W. Joosen, N. Nikiforakis
[57] Dns history - largest archive of dns records - domain history, https://completedns.com/dns-history
[58] Catch me if you can: A cloud-enabled ddos defense, Q. Jia, H. Wang, D. Fleck, F. Li, A. Stavrou, and W. Powell
[59] The secure shell (ssh) connection protocol, T. Ylonen, C. Lonvick
[60] Analysis of a wordpress pingback ddos attack, T. Butler
[61] Wordpress default leaves millions of sites exploitable for ddos attacks, G. Shatz
[62]What are AWS WAF, AWS Shield Advanced, and AWS Firewall Manager? https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

[63]Cloudflare Web Application Firewall https://developers.cloudflare.com/waf/
[64] Break the wall from bottom: Automated discovery of protocol-level evasion vulnerabilities in web application firewalls, Qi Wang, Jianjun Chen, Zheyu Jiang, Run Guo, Ximeng Liu, Chao Zhang, Haixin Duan
[65] Web Application firewall evasion techniques, K Nagendran, S Balaji, B Akshay Raj, P Chanthrika, RG Amirthaa
[66]How to Bypass Cloudflare in 2025: The 9 Best Methods, https://www.zenrows.com/blog/bypass-cloudflare#cloudflare-bot-management
[67] App & API Protector Product Brief, https://www.akamai.com/resources/product-brief/app-and-api-protector
[68] Prolexic: Product Brief, https://www.akamai.com/resources/product-brief/prolexic
[69] NIS-2, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32022L2555
[70]Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Κ.Λαμπρινουδάκης, Σ.Γκρίτζαλης, Λ.Μήτρου, Σ.Κάτσικας
[71] Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Θ.Κ.Παπαχριστού, Λ.Μήτρου, Τ.Βιδάλης, Θ.Ξηρός
[72] ePrivacy Regulation, https://en.wikipedia.org/wiki/EPrivacy_Regulation
[73] Privacy Impact Assessment, https://en.wikipedia.org/wiki/Authorization
[74] Authorization, https://en.wikipedia.org/wiki/Authorization
[75] It's Not Just the Site, It's the Contents: Intra-domain Fingerprinting Social Media Websites Through CDN Bursts, K.Wang, J.Zhang
[76] Ensuring Compliance: A Comprehensive Guide to Navigating CDN Regulations, https://www.cachefly.com/news/ensuring-compliance-a-comprehensive-guide-to-navigating-cdn-regulations/
[77] Overview of Akamai's Personal Data Processing Activities and Roles in connection with Services Provisioning, This document is maintained by the Akamai Global Data Protection Office