ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Ασφάλεια και Ιδιωτικότητα σε Παρόχους Επικοινωνιών. Μια σύγχρονη οπτική της Αρχής

Βασίλης Σταθόπουλος

Infocom Security– Αθήνα – 18 Απριλίου 2019

Ασφάλεια και Ιδωτικότητα

- Ιδιωτικότητα: (privacy)
  - Αποτελεί θεμελιώδες ατομικό δικαίωμα

- Υποστηρίζεται από διεθνείς και ευρωπαϊκούς νόμους
  - Οδηγία 2002/58/EC (Directive on Privacy and Electronic Communications)

- Οι Αρμόδιες Αρχές είναι υπεύθυνες για τον έλεγχο και τη παρακολούθηση της εφαρμογής της νομοθεσίας
  - ΑΔΑΕ για την Ελλάδα

Διασφάλιση του Απορρήτου των Επικοινωνιών

- Πώς επιτυγχάνεται η ασφάλεια:
  - Προστασία **δικτυακών και πληροφοριακών** πόρων και **όλων των δεδομένων επικοινωνίας** που υποβάλλονται σε **επεξεργασία** (αποθήκευση και μετάδοση)

- Δύο τύποι δεδομένων επικοινωνίας

1. **Content data:** Το πραγματικό περιεχόμενο της επικοινωνίας
2. **Context data or metadata:** Εξωτερικά δεδομένα που χρησιμοποιούνται για την παροχή επικοινωνίας, π.χ.
   - IP address
   - e-mail address
   - MAC address
   - date/time of call/connection/ disconnection etc
   - Cell-id

Διασφάλιση του Απορρήτου των Επικοινωνιών

- Σημαντική η προστασία των metadata
  - Πληροφορίες για τον αποστολέα και παραλήπτη (π.χ. μέσω IP address)
  - Πληροφορίες με ποιόν ανταλλάσω την πληροφορία (π.χ. e-mails)
  - Πληροφορίες για το περιεχόμενο της επικοινωνίας
    - Η IP του παραλήπτη (target IP) αποκαλύπτει το είδος της ιστοσελίδας και μερικώς το περιεχόμενό της

Απειλές ασφάλειας σε δίκτυα επικοινωνιών

- **Κακή χρήση πιστοποιητικών** αυθεντικοποίησης/ εξουσιοδότησης (Identity misuse/abuse)
  - Οι διαχειριστές μοιράζονται κοινά passwords δικτυακών ή IT συστημάτων
- **Μη εξουσιοδοτημένη χρήση** (Unauthorized use) των συστημάτων/εφαρμογών/data
  - Χρήστες ή διαχειριστές χωρίς καταγεγραμμένη αρμοδιότητα πρόσβασης σε ένα σύστημα, τελικά το προσπελαύνουν
    - Π.χ. Agent τηλεφωνικού κέντρου αποκτά πρόσβαση σε CDRs συνδρομητή χωρίς τη συγκατάθεσή του
- **Ενσωμάτωση κακόβουλου λογισμικού**
  - Π.χ. Ένα παθητικό εργαλείο παρακολούθησης (passive interception tool) σε email servers
  - **Φιλτράρισμα/χειραγώγηση επικοινωνίας** Communication infiltration /manipulation
  - Π.χ. Αλλαγές στο configuration file δικτυακών συσκευών (routers / switches) (π.χ. Port mirroring)

Συνήθεις Αδυναμίες Ασφάλειας και Αντίμετρα

- Διαχείριση Λογαριασμών Χρήστη
- Logging and (internal) auditing
- Συνεργάτες και 3α μέρη
- Perimeter/Network Security
- Συντήρηση Συστημάτων /Δικτύου

- **personalized passwords**
- **password/identity management tools**
- **Εκτέλεση συχνών εσωτερικών ελέγχων**
- **Συνεχής ενεργοποίηση του access logging**
- **Επιλεγμένη ενεργοποίηση του command and application logging**
- **Χρήση αυστηρών διμερών συμφωνιών**
- **Χρήση centralized malware management**
- **Χρήση automated lock-out των χρηστών μετά από ένα αριθμό ανεπιτυχών προσπαθειών login**
- **Χρήση ticketing system για την παρακολούθηση και τη διαχείριση ενεργειών**
- **Χρήση secure protocols (e.g. SSH-2) και περιορισμός απομακρυσμένης πρόσβασης**

Συμπεράσματα για την Ασφάλεια

- Οι **Πάροχοι** παίζουν **σημαντικό ρόλο** στην προστασία του απορρήτου και της ιδιωτικότητας των επικοινωνιών.

- **Παρατηρούνται τεχνικές και διαδικαστικές ευπάθειες** των Παρόχων που μπορεί να οδηγήσουν στην πραγματοποίηση των απειλών

- Τα μέτρα Ασφάλειας πρέπει να **εφαρμόζονται με οργανωμένο τρόπο**, να υπάρχει **συνεχής επίβλεψη** και **διαδικασία αναθεώρησής** τους

- Σημαντικός ο ρόλος των χρηστών (the other key player)

Ευρύτερα Ζητήματα Ασφάλειας

Ασφάλεια GSM – 2G

- Σχεδιάστηκε ως **ασφαλές ασύρματο δίκτυο**
  - Υποστηρίζει αυθεντικοποίηση και ανωνυμία του χρήστη (TMSI) καθώς και κρυπτογράφηση στο ασύρματο τμήμα (ciphering),
    - Χρήση των **A3/A8 κρυπτογραφικών αλγορίθμων** για την αυθεντικοποίηση του χρήστη στο δίκτυο και
    - την παραγωγή session key για την κρυπτογράφησης της πληροφορίας.
  - Πλην όμως, είναι **ευάλωτο σε πολλές επιθέσεις.**

Ευρύτερα Ζητήματα Ασφάλειας

- **Αδυναμίες 2G:**
- Authentication functions A3, A5, A8 (not published)
  - Ελαττώματα στην υλοποίηση των A3/A8 αλγορίθμων
  - Ελαττώματα στους αλγορίθμους A5/1 and A5/2
- Μονομερής αυθεντικοποίηση (Unilateral authentication) - Man in the middle attack
- SIM card cloning (αδυναμία στην συνάρτηση COMP128 με αποτέλεσμα την αποκάλυψη του κλειδιού αυθεντικοποίησης Ki)
- Χωρίς κρυπτογράφηση στα σταθερά σημεία του δικτύου (Short range of protection)
- Η κρυπτογράφηση ελέγχεται από το BTS. Ο χρήστης δεν ειδοποιείται κατά την απενεργοποίηση της κρυπτογράφησης. Συνδυάζεται με ss7 αδυναμίες.
- Απώλεια της ανωνυμίας του χρήστη - Identity catching
  - Το IMSI μεταφέρεται σε plaintext (το δίκτυο ζητά από το συνδρομητή να δηλώσει το IMSI του σε κάθε νέο location area)
- Απουσία προστασίας ακεραιότητας (integrity protection)

Ευρύτερα Ζητήματα Ασφάλειας

- **Ασφάλεια 3G – UMTS**
  - **Authentication and Key Agreement (AKA)**
    - **Αμφίδρομο Authentication** για τη πρόληψη της απάτης
    - Δημιουργεί κλειδιά (keys) for **ciphering** (Προστασία δεδομένων) και **integrity protection (**Προστασία σηματοδοσίας για αποτροπή από επιθέσεις με False Base Stations**)**

- **Αδυναμίες 3G - UMTS:**
  - Απώλεια της ανωνυμίας του χρήστη- Identity catching
    - Το IMSI μεταφέρεται σε plaintext σε κάθε νέα διανομή TMSI
  - Unencrypted επικοινωνία είναι δυνατή και αποδεκτή (GEA0)
  - Είναι πιθανό μια κινητή συσκευή να συνδεθεί με GPRS/EDGE αν οι υπηρεσίες UMTS/HSPA δεν είναι διαθέσιμες. (SN impersonation and eavesdropping)

Ευρύτερα Ζητήματα Ασφάλειας

Security στο 4G – LTE

- Το LTE χρησιμοποιεί αποκλειστικά packet switched τεχνολογία, IP-based τεχνολογία.
- Στο LTE εισάγεται νέους αλγορίθμους κρυπτογράφησης και ουσιαστικά διαφορετική δομή κλειδιών σε σύγκριση με τα GSM και UMTS
- Πολλά κλειδιά στο LTE είναι 256-bits, σε διάφορες όμως υλοποιήσεις μόνο τα 128 least significant bits χρησιμοποιούνται.

› **Authentication and Key Agreement (AKA)**

- **Bidirectional Authentication**

› Δημιουργεί κλειδιά (keys) για **ciphering και integrity protection**

› **Signaling integrity protection** υποστηρίζεται

› User plane integrity protection δεν υποστηρίζεται

› **User plane confidentiality** (αφορά τον operator)

Ευρύτερα Ζητήματα Ασφάλειας

- **Αδυναμίες 4G - LTE:**
  - Ένα **IP-based δίκτυο** εισάγει συγκεκριμένα ζητήματα ασφάλειας (κυρίως backhaul security) τα οποία δεν απασχολούσαν παλιότερα non-IP δίκτυα (2G και 3G)
  - **Εντοπισμός της συσκευής και της ταυτότητας χρήστη**. Τα δεδομένα (IMSI) μεταφέρονται μέσω καναλιών σηματοδοσίας κατά τη διάρκεια του handset attach και της αυθεντικοποίησης.
  - **Downgrade Attacks με rogue base stations**.
    - Downgrade σε GSM. Ισχύουν σημαντικές αδυναμίες ασφάλειας (A5/1 και A5/2)

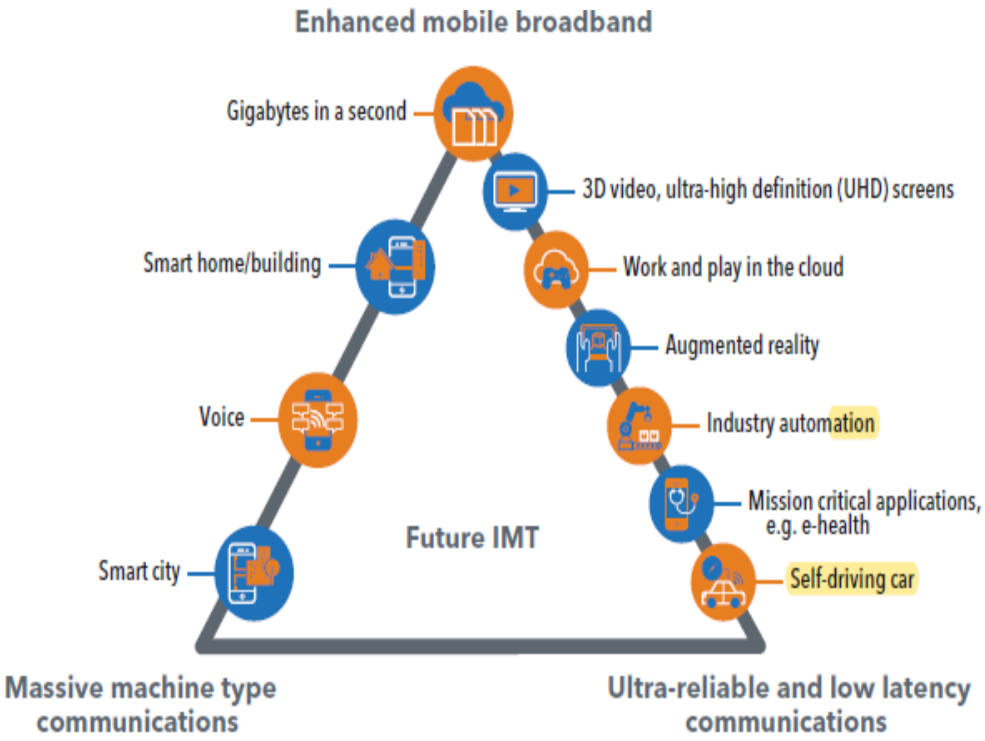
Ευρύτερα Ζητήματα Ασφάλειας

Γενικά για το 5G

- Οι προδιαγραφές του 5G δίνονται από διάφορους φορείς
  - NGMN, **3GPP**, ETSI (ETSI NFV SEC), ITU-T Security Study Group 17, IETF net-slicing, GSMA, 5GPPP
- Αποτελεί πλατφόρμα ενεργοποίησης για διαφορετικές υπηρεσίες
  - Mission Critical Communications (MCC) / Internet of Things (IoT)
  - Automotive and Railways (i.e. Vehicle to Everything (V2X))
  - Energy Providers / Broadcast agencies e.t.c
- Προβλέπονται
  - Αλλαγές στο radio interface (massive MIMO, dense deployment of small cell base stations, and larger bandwidths)
  - Αλλαγές στο Core network
  - Νέες υπηρεσίες για διαφορετικούς φορείς με ποικίλες απαιτήσεις σε latency, reliability κ.α.

Ευρύτερα Ζητήματα Ασφάλειας

Use cases in 5G



ITU News Magazine

eMBB: Data-driven use cases - *Απαιτούν high data rates σε μια ευρεία περιοχή κάλυψης.*

mMTC: Υποστηρίζει έναν πολύ μεγάλο αριθμό συσκευών σε μια μικρή περιοχή (στέλνει δεδομένα, σποραδικά –IoT).

URLLC: αυστηρές απαιτήσεις σχετικά με την καθυστέρηση και αξιοπιστία για κρίσιμες επικοινωνίες, π.χ. απομακρυσμένη χειρουργική επέμβαση, αυτόνομα οχήματα

Ευρύτερα Ζητήματα Ασφάλειας

Πώς θα υλοποιηθούν - Τι απαιτήσεις ασφάλειας δημιουργούνται στο 5G;

- "Network Slicing", SDN και VNF θα ενσωματωθούν στο 5G
  - Οι φυσικοί πόροι του δικτύου θα μπορούν να κατανεμηθούν – διανεμηθούν ως πολλαπλοί λογικοί πόροι σε τρίτες εταιρείες ή ενδιαφερόμενα μέρη
  - Ορισμό διαφορετικού επιπέδου ασφάλειας για κάθε υπηρεσία/slice
  - Διασφάλιση slice isolation
- Multi-access Edge Computing (MEC)
  - ETSI standardized
  - Η υπολογιστική ισχύς και ευφυΐα προσεγγίζει τα άκρα του δικτύου (radio access network ή aggregation point).
- Ασφάλεια και ευελιξία σε Non-3GPP access interworking

Ευρύτερα Ζητήματα Ασφάλειας

Συμπέρασμα για το 5G

- Το 5G θέτει πολλαπλά ζητήματα ασφάλειας και επιβάλλει την επανεξέταση τους (3GPP standardization activity)
  - Authentication and Authorization (μαζί με identity management)
  - Unified authentication framework for 3GPP and non-3GPP access
  - RAN (multi-access) security
  - User Equipment (including IoT) confidentiality and key management,
  - Network Slicing security.
  - Extended key hierarchy for later security services
  - Security of the interconnect network between operators
- Η Ευρωπαϊκή Ένωση έχει πρόσφατα ζητήσει από τα Κ.Μ. τη δημιουργία εκτίμησης κινδύνου (risk assessment) για το 5G

Ευρύτερα Ζητήματα Ασφάλειας

SS7 suite - Ζητήματα ασφάλειας

- Το SS7 suite χρησιμοποιήθηκε αρχικά σε PSTN και αργότερα σε GSM δίκτυα
- Χρησιμοποιείται από τους περισσότερους παρόχους δικτύων επικοινωνιών
- Σχεδιάστηκε όταν η ασφάλεια δεν ήταν πρωταρχική μέριμνα
- Την δεκαετία 1990 και 2000 προστέθηκαν νέα πρωτόκολλα επίσης χωρίς μέριμνα ασφάλειας
  - Mobile Application Part (MAP) για τις κινητές επικοινωνίες
  - CAMEL Application Part (CAP) για την δημιουργία νέων custom services

Ευρύτερα Ζητήματα Ασφάλειας

SS7 suite – Ζητήματα ασφάλειας

- **Η πρόσβαση μπορεί να αγοραστεί εύκολα από τους Παρόχους ή από roaming hubs**
- Αρκετοί Πάροχοι διαθέτουν τον εξοπλισμό τους χωρίς ασφάλεια
- Οι κυριότερες απειλές είναι:
  - **Εντοπισμός θέσης** (user location tracking),
  - **Παρακολούθηση** κλήσεων, SMS ή internet κίνησης,
  - **Denial of Service (DoS) επιθέσεις** σε συνδρομητές του δικτύου,
  - Πραγματοποίηση **μη νόμιμων κλήσεων αποφεύγοντας τις χρεώσεις** και στέλνοντας ανεπιθύμητα μηνύματα

Ευρύτερα Ζητήματα Ασφάλειας

- **Πώς προστατευόμαστε στο SS7;**
  - Υλοποίηση νέου πρωτοκόλλου με εγγενή ασφάλεια (authentication, encryption).
    - Diameter χρησιμοποιείται σε δίκτυα LTE (μεταφέρει αρκετές από τις αδυναμίες ασφάλειας του SS7)
  - Παρεμβάσεις και αλλαγές στην υπάρχουσα υποδομή
    - SMS Home Routing
    - Optimal parameter configuration,
    - **Logging, examining, assessing ύποπτης SS7 κίνησης,**
    - **Signalling firewalling based on message type, source address**
  - **Η ΑΔΑΕ έχει εκδώσει «Τεχνική Σύσταση για την Αντιμετώπιση Ευπαθειών των Δικτύων Κινητής Τηλεφωνίας»**
  - Σε Ευρωπαϊκό επίπεδο δεν έχει υπάρξει ακόμα κάποια Γενική Οδηγία

Ευρύτερα Ζητήματα Ασφάλειας

Ζητήματα Ασφάλειας στο Border Gateway Protocol (BGP)

- **Αποτελεί πρωτόκολλο δρομολόγησης. Δηλαδή:**
  - επιτρέπει «ανεξάρτητα δίκτυα», γνωστά ως “Autonomous Systems - AS” να επικοινωνούν μεταξύ τους.
  - Στέλνουν IP prefixes
  - **Τι μπορεί να πάει λάθος;**
  - **BGP route manipulation**: Μία κακόβουλη συσκευή μετατρέπει το περιεχόμενο του BGP table, εμποδίζοντας την κίνηση να φτάσει στον προορισμό της.
  - **BGP route hijacking:** Μια κακόβουλη συσκευή αναγγέλλει κακόβουλα τα prefixes του θύματος για να ανακατευθύνει την κυκλοφορία προς ή μέσω του ίδιου.
  - **BGP denial-of-service (DoS):** Μια κακόβουλη συσκευή αποστέλλει ανεπιθύμητη ή μη αναμενόμενη κίνηση BGP σε ένα AS εξαντλώντας όλους τους πόρους και καθιστώντας το ανίκανο να επεξεργάζεται έγκυρη κίνηση BGP

Ευρύτερα Ζητήματα Ασφάλειας

- **Τα περιστατικά BGP μπορεί να είναι**
  - Σκόπιμα
  - Ακούσια: Misconfigurations **π.χ. BGP route leaks .**

- **Ένα πρόσφατο παράδειγμα BGP hijacks στη βιβλιογραφία**
  - «**China has been 'hijacking the vital internet backbone of western countries**»

    https://www.zdnet.com/

Ασφάλεια και σύγχρονες Τεχνολογικές Εξελίξεις

- **Ερώτημα:** Η Ευρώπη μπορεί να ενσωματώσει τις τεχνολογικές εξελίξεις και αν ναι πώς προστατεύεται από τις νέες απειλές που δημιουργούνται ;
  - Κεντρικό ρόλο έχει η υλοποίηση της πολιτικής Digital Single Market (DSM). Η στρατηγική της πολιτικής απαιτεί μεταξύ άλλων:
    - Την ενσωμάτωση των τεχνολογικών εξελίξεων (π.χ. 5G/NFV) στις ψηφιακές υπηρεσίες
    - η ενίσχυση της **εμπιστοσύνης** και της **ασφάλειας** στις ψηφιακές υπηρεσίες

- Βασική συνιστώσα προς αυτή τη κατεύθυνση είναι η **αναθεώρηση** της Οδηγίας 2002/58/EU με την εφαρμογή του **σχεδίου του e-privacy regulation**.
  - Το σχέδιο κανονισμού προτάθηκε αρχές του 2017 και συζητείται ακόμη μεταξύ των Κρατών-Μελών στο Συμβούλιο της Ευρωπαϊκής Ένωσης.

Ασφάλεια και σύγχρονες Τεχνολογικές Εξελίξεις

- Πιο συγκεκριμένα, το **σχέδιο του e-privacy regulation:**
- **Διευρύνει** το πεδίο των υπηρεσιών
  - Νέες μορφές υπηρεσιών (**OTT** τεχνολογίες - Skype, Viber, WhatsApp, Facebook, Gmail και άλλες).
  - **Θέτει τον όρο "Interpersonal Communication"**: περιλαμβάνει και υπηρεσίες που επιτρέπουν τη διαπροσωπική και διαδραστική επικοινωνία.
    - Οι υπηρεσίες αυτές δεν είναι απαραίτητο να λειτουργούν αυτόνομα αλλά και ως **δευτερεύον βοηθητικό χαρακτηριστικό** άλλης υπηρεσίας.
- Επεκτείνει το «**γεωγραφικό πεδίο**» εφαρμογής του κανονισμού
  - Παροχή υπηρεσιών σε τελικούς χρήστες εγκατεστημένους στην ΕΕ, ακόμη και αν ο πάροχος είναι εγκατεστημένος εκτός της ΕΕ.
- Επιβάλλει **υψηλό επίπεδο διασφάλισης της ασφάλειας** όλων των δεδομένων επικοινωνιών
  - content και metadata

Ασφάλεια και σύγχρονες Τεχνολογικές Εξελίξεις

- Η επεξεργασία των δεδομένων επικοινωνίας από τον Πάροχο **επιτρέπεται μόνο** για τεχνικούς λόγους δηλαδή,
  - μετάδοση μιας επικοινωνίας ή παροχής μιας υπηρεσίας,
  - διατήρηση της ασφάλειας,
  - τιμολόγηση
  - ή με προηγούμενη συγκατάθεση των χρηστών.
  - **Επιβάλλει** κανόνες ασφάλειας για **Machine to Machine (M2M)** μεταδόσεις. Αυτό περιλαμβάνει όλα τα δεδομένα που διακινούνται μεταξύ συσκευών (IoT)
- **Data breach notification:**
  - επί του παρόντος υπάρχει ο κανονισμός 611/2013 .
  - Το σχέδιο κανονισμού δεν περιλαμβάνει ειδικές διατάξεις, αλλά βασίζεται στις σχετικές διατάξεις του GDPR.

Ασφάλεια και σύγχρονες Τεχνολογικές Εξελίξεις

- Μία δεύτερη συνιστώσα της Digital Single Market στρατηγικής είναι ο **European Electronic Communications Code (EECC)**
- Ο κώδικας θέτει ***νέο Ορισμό για Electronic Communication Services***
- Επίσης διευρύνει το πεδίο των υπηρεσιών, η ασφάλεια των οποίων πρέπει να διασφαλίζεται, ως ακολούθως:
  - **Interpersonal communication services (ICS)**
    - Number based ICS
    - Number Independent ICS
  - **Internet Access Services (IAS)**
  - **Services consisting wholly or mainly of conveyance of signals**
    - Transmission of broadcasting signals
    - **Transmission of M2M services**

Ασφάλεια και σύγχρονες Τεχνολογικές Εξελίξεις

- Θέτει νέο και ευρύτερο ορισμό για "**security** of networks and services" Art 2(21) και για "περιστατικά ασφάλειας (security incidents) Art 2(42)
  - **Η ασφάλεια περιλαμβάνει availability, authenticity, integrity and confidentiality**
  - **Προτείνει τη λήψη μέτρων** (κρυπτογράφηση όταν είναι απαραίτητο) που θα μετριάζουν τις επιπτώσεις
  - τα περιστατικά ασφάλειας ορίζονται ευρύτερα
    - Οι πάροχοι ECN/ECS γνωστοποιούν σε ανεξάρτητες αρχές ένα **περιστατικό ασφάλειας με σημαντική επίπτωση**

Ασφάλεια και σύγχρονες Τεχνολογικές Εξελίξεις

- Τρίτο συνιστώσα είναι η Οδηγία για την **ασφάλεια Network and Information Systems (NIS directive)**
  - αποτελεί το πρώτο τμήμα πανευρωπαϊκής νομοθεσίας για την ασφάλεια στον κυβερνοχώρο.
  - Επιβάλλει κουλτούρα ασφάλειας σε **διάφορους τομείς που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία** και εξαρτώνται σε μεγάλο βαθμό από τεχνολογία ICT.
    - Ενέργεια, μεταφορές, νερό, τραπεζικός τομέας, οικονομικές υποδομές, υποδομές υγείας και ψηφιακές
    - Ουσιαστικά επικεντρώνεται στην ενίσχυση της ασφάλειας και επιχειρησιακής ανθεκτικότητας (operational resilience) των οργανισμών αυτών.

Ασφάλεια και σύγχρονες Τεχνολογικές Εξελίξεις

- Πρόσφατα η Ευρωπαϊκή Ένωση εξέδωσε ένα Recommendation με τίτλο “Cybersecurity of 5G networks”
  - Προτρέπει τα Κ.Μ. για την δημιουργία εκτίμησης κινδύνου (risk assessment) που αφορά τα δίκτυα 5G
  - Απώτερο στόχο έχει τον ορισμό ενός συνόλου πιθανών μέτρων για το μετριασμό των κινδύνων και των ρίσκων
  - **Θέτει ως πλαίσιο διαχείρισης το NIS**
  - Η συγκεκριμένη πρωτοβουλία απαιτεί:
  - **Τη συνεργασία όλων των Αρμοδίων Αρχών για κάθε Κ. Μ.**
    - Ποιες Αρχές; Οι αρμόδιες για την ασφάλεια των επικοινωνιών, την ασφάλεια δικτύων και πληροφοριών και την ασφάλεια δικτύων και υπηρεσιών επικοινωνιών.

Συμπεράσματα και Προκλήσεις

- **Προκλήσεις:**
  - Συνεργασία όλων των Αρμοδίων Αρχών σε εθνικό επίπεδο.
    - Μεμονωμένη αντιμετώπιση δεν μπορεί πλέον να φέρει κανένα αποτέλεσμα
  - Συνεργασία όλων των Κ.Μ. της Ε.Ε. για τη επιτυχή διαχείριση της ασφάλειας
    - **Ανταλλαγή γνώσεων** (ανάλυση συμβάντων ασφάλειας, απειλών, αδυναμιών ασφάλειας, νέων τεχνολογιών) σε θεσμοθετημένες Ομάδες Εργασίας
      - αυτή τη στιγμή οι συζητήσεις είναι αρκετά περιορισμένες μεταξύ των Αρχών των Κ.Μ.
    - **Κοινή αντιμετώπιση των προβλημάτων** σε θεσμοθετημένες Ομάδες Εργασίας (Εναρμόνιση πλαισίου ασφάλειας)
- Κανάλι επικοινωνίας μεταξύ των Κ.Μ. σε διμερές επίπεδο για τη διαχείριση των περιστατικών ασφάλειας **(cross border collaboration)**
  - Επικοινωνία βάσει συγκεκριμένων πρωτοκόλλων επικοινωνίας