ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Ασφάλεια από τη Σχεδίαση και εξ' Ορισμού»

Κυριάκος Δ. Φράγκος

ΑΘΗΝΑ 2020

ΕΠΙΒΛΕΠΟΝΤΕΣ: Λαμπρινουδάκης Κωνσταντίνος, Τίτλος (Καθηγητής)

Περίληψη

Οι περισσότεροι οργανισμοί υιοθετούν μια μεθοδολογία που ονομάζεται κύκλος ζωής ανάπτυξης συστημάτων (Systems Development Lifecycle SDLC) για την ανάπτυξη και εφαρμογή συστημάτων πληροφορικής. Η SDLC είναι μια διαδικασία πολλαπλών βημάτων κύκλου ζωής για την παροχή συστημάτων πληροφορικής και την εξασφάλιση καλής ποιότητας των συστημάτων τα οποία πληρούν τις προδιαγραφές και, εντός των εκτιμήσεων χρόνου και κόστους.

Ενώ οι περισσότεροι οργανισμοί αναγνωρίζουν ότι η ασφάλεια είναι ένα σημαντικό θέμα στην ανάπτυξη συστημάτων πληροφορικής, το κόστος και οι επιχειρηματικές επιδόσεις συχνά υπερισχύουν της ασφάλειας. Παρόλο που η ευαισθητοποίηση έχει αυξηθεί σε θέματα ασφάλειας, οι περισσότεροι οργανισμοί επικεντρώνονται στην εφαρμογή της ασφάλειας μόνο κατά το στάδιο της ανάθεσης της ανάπτυξης του συστήματος και προσπαθούν να εγκατασταθεί η ασφάλεια στην τελική φάση της σχεδίασης, με αποτέλεσμα την αναποτελεσματική εφαρμογή της ασφάλειας.

Ένας αποτελεσματικός τρόπος προστασίας των υπολογιστικών συστημάτων από τις απειλές στον κυβερνοχώρο είναι να ενσωματώσουμε την ασφάλεια σε κάθε βήμα του κύκλος ζωής ανάπτυξης των συστημάτων (SDLC), από την έναρξη, στην ανάπτυξη, στην εγκατάσταση και στην τελική διάθεση του συστήματος. Αυτή η προσέγγιση είναι η προσέγγιση Security by Design (SbD) και Security by Default (SbD) το οποίο και θα μελετήσουμε.

Το Security by Design είναι μια προσέγγιση για την ανάπτυξη λογισμικού και υλικού που επιδιώκει να ελαχιστοποιήσουν τα τρωτά σημεία των συστημάτων και να μειώσουν την επιφάνεια επίθεσης μέσω του σχεδιασμού και την ενσωμάτωση της ασφάλειας σε κάθε φάση του κύκλου ζωής ανάπτυξης (SDLC). Αυτό περιλαμβάνει την ενσωμάτωση των προδιαγραφών ασφαλείας στο σχεδιασμό, τη συνεχή αξιολόγηση της ασφάλειας σε κάθε φάση και την τήρηση των βέλτιστων πρακτικών. Οι αξίες της ενσωμάτωσης της ασφάλειας στην SDLC περιλαμβάνουν:

- Έγκαιρη ταυτοποίηση και μετριασμός των τρωτών σημείων ασφαλείας και των λανθασμένων ρυθμίσεων των συστημάτων.

- Προσδιορισμός κοινών υπηρεσιών ασφαλείας και εργαλείων για τη μείωση του κόστους, ενώ παράλληλα βελτιώνεται η στάση της ασφάλειας μέσω αποδεδειγμένων μεθόδων και τεχνικών.

- Διευκόλυνση των βασικών αποφάσεων των ενδιαφερομένων με ενημέρωση μέσω ενός risk management.

- Τεκμηρίωση σημαντικών αποφάσεων ασφαλείας καθ 'όλη τη διάρκεια του κύκλου ζωής του συστήματος, εξασφαλίζοντας ότι η ασφάλεια θα εξετάζεται ορθώς και πλήρως σε όλες τις φάσεις.

- Βελτιωμένη λειτουργικότητα συστημάτων που διαφορετικά θα παρεμποδίζεται από την απομονωμένη ασφάλεια των συστημάτων.

Ειδικά για την ασφάλεια του κυβερνοχώρου, το Security by Design καλύπτει τις ανησυχίες για την προστασία του κυβερνοχώρου καθ 'όλη τη διάρκεια του κύκλου ζωής ενός συστήματος. Αυτό περιλαμβάνει σχεδιασμό ασφάλειας ειδικά για την αναγνώριση, την προστασία, την ανίχνευση, την ανταπόκριση και τις δυνατότητες αποκατάστασης για να ενισχυθεί η ηλεκτρονική ανθεκτικότητα του συστήματος.

Ένας λιγότερο γνωστός όρος είναι το Security by Default, εφαρμόζει την ίδια αρχή στην εξασφάλιση δεδομένων στην πηγή. Αναφέρεται στην εξασφάλιση πληροφοριών. Το Security by Default η αλλιώς ασφάλεια από προεπιλογή στα δεδομένα μας, καθιστούν την υπόθεση ότι όλα τα δεδομένα πρέπει να έχουν ενσωματωμένη ασφάλεια. Τα συστήματα που επεξεργάζονται και αποθηκεύουν αυτά τα δεδομένα θα πρέπει να τηρούν αυστηρά τις πολιτικές ασφαλείας που είναι ενσωματωμένες σε αυτά. Αυτή η προσέγγιση δεν είναι τόσο γνωστή, διότι απλά δεν χρησιμοποιείται ευρέως. Μέχρι σήμερα, δεν έχουμε ενσωματώσει την ασφάλεια σε κάθε κομμάτι δεδομένων καθώς δημιουργείται, δημιουργώντας έτσι ένα σοβαρό πρόβλημα, ιδιαίτερα για τις κυβερνητικές υπηρεσίες.

Πριν από τη δημιουργία ενός νέου προϊόντος, πολλές ερωτήσεις περνούν από το κεφάλι ενός προγραμματιστή λογισμικού: Πως θα πρέπει να είναι οι νέες οθόνες εισαγωγής; Πόσο αποτελεσματικό θα έπρεπε να είναι το νέο λογισμικό; Ωστόσο, υπάρχει μια σημαντική πτυχή που εξακολουθεί να παραμελείτε πολύ συχνά και αυτό είναι η ασφάλεια. Και αυτό σε μια εποχή που ο αριθμός των επιθέσεων στον κυβερνοχώρο αυξάνεται ραγδαία, όπως αποκαλύπτεται στην έκθεση σχετικά με την κατάσταση από τη γερμανική Ομοσπονδιακή Υπηρεσία Ασφάλειας Πληροφοριών (BSI). Σύμφωνα με αυτό, οι ειδικοί ανακαλύπτουν περίπου 380.000 νέες εκδόσεις malware κάθε μέρα.

Το πρόβλημα είναι ότι το 95% των επιτυχημένων επιθέσεων οφείλεται σε κακό προγραμματισμένο, κακώς διατηρημένο ή κακώς διαμορφωμένο λογισμικό", λέει ο Διευθυντής Εσωτερικής Ασφάλειας και Cyber Defense στην Deutsche Telekom. Ωστόσο, αυτό το πρόβλημα θα μπορούσε να λυθεί λαμβάνοντας υπόψη την ασφάλεια απευθείας από την αρχή της ανάπτυξης του - "αντί να μπαλώνουμε τρύπες στο τελικό προϊόν".

Η παρούσα έρευνα πραγματεύεται και εμβαθύνει στο τι είναι το security by design - security by default, ποια τα οφέλη που θα επιφέρουν με την εφαρμογή τους και πως επιτυγχάνεται αυτό. Επίσης θα αναλύονται τα στάδια των βασικών αρχών σχεδιασμού για την εξασφάλιση της ασφάλειας σε κάθε στάδιο ανάπτυξης ενός συστήματος. Περαιτέρω θα αναλύσουμε πως θα διασφαλίσουμε την ιδιωτικότητα των πληροφοριών, ποια η φιλοσοφία αναπτύχθηκε στο τομέα αυτόν και πως θα καταφέρουμε να πετύχουμε μια ομαλή ενσωματώσει της προστασίας σε κάθε σκέλος του σχεδιασμού και της ανάπτυξης ενός προϊόντος η μιας υπηρεσίας. Επιπλέον θα δούμε τον ρόλο και των συσχετισμό της ασφάλειας από τον σχεδιασμό με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Παρέχεται μια εικόνα των κενών στην υιοθέτηση της προστασίας της ιδιωτικής ζωής από την βιομηχανία. Με βάση τα στοιχεία αυτά αναλύουμε εκτενέστερα τα κενά του ισχύον κανονισμού (όπως για παράδειγμα ασαφής

διατύπωση των υποχρεώσεων, αδυναμίες κυρώσεων, υποχρεώσεις διατήρησης ή από κάλυψης προσωπικών δεδομένων). Δίνεται μια έμφαση στο Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και ποιοι οι περιορισμοί στις υπάρχουσες τεχνολογίες και την μέθοδο σχεδιασμού, και ποια τα κίνητρα για την υιοθέτηση και την συμμόρφωση με τον κανονισμό. Τέλος έχει αναπτυχθεί ένας οδηγός - κατευθυντήριες γραμμές ώστε να γίνει πιο κατανοητό από την βιομηχανία το πώς θα συμμορφωθούν με την απαίτηση για την προστασία από τον σχεδιασμό και εξ' ορισμού σύμφωνα με το άρθρο 25 του γενικού κανονισμού και ποια τα οφέλη της συμμόρφωσης.

Λέξεις κλειδιά: Security by Design(SbD), Security by Default(SbD), Systems Development Lifecycle (SDLC), Privacy by Design(PbD), Privacy by Default(PbD), Privacy and Security by Design(PSbD), Data Protection by design(DPbD), General Data Protection Regulation(GDPR) Cybersecurity, Security, Privacy. Privacy Enhancing Technology(PET), Information Technologies(IT).

ABSTRACT

Most organisations adopt a Systems Development Lifecycle (SDLC) methodology for the development and implementation of computer systems. SDLC is a multi-step lifecycle process to deliver computer systems to ensure good-quality systems that meet specifications and, within time and cost estimates.

While most organisations acknowledge that security is an important consideration in developing computer systems, costs and business performance often take precedence over security. Even though awareness has been elevated on security issues, most organisations focus on applying security only at the commissioning stage of the system development and try to forced fit security into the final design, resulting in ineffective application of security

An effective way to protect computer systems against cyber threats is to integrate security into every step of the SDLC, from initiation, to development, to deployment and eventual disposal of the system. This approach is the Security-by-Design (SbD) approach, something that discussed in this research.

Security-by-Design is an approach to software and hardware development that seeks to minimise systems vulnerabilities and reduce the attack surface through designing and building security in every phase of the SDLC. This includes incorporating security specifications in the design, continuous security evaluation at each phase and adherence to best practices. The values of integrating security into SDLC include:

- Early identification and mitigation of security vulnerabilities and misconfigurations of systems.
- Identification of shared security services and tools to reduce cost, while
  improving security posture through proven methods and techniques.
- Facilitation of informed key stakeholder decisions through comprehensive risk
  management in a timely manner.
- Documentation of important security decisions throughout the lifecycle of the
  system, ensuring that security was full considered during all phases.

- Improved systems operability that would otherwise be hampered by isolated
  security of systems.

Specific to cybersecurity, Security-by-Design addresses the cyber protection considerations throughout a system's lifecycle. This includes security design specifically for the identification, protection, detection, response and recovery capabilities to strengthen the cyber resiliency of the system.

A lesser-known term, Security by Default applies the same principle to securing data at the source. It is referring to securing information. Secure by Default data makes the case that all data should have embedded security, and the systems that consume, process and store this data must adhere to the security policies embedded therein. This approach is not as well known because it's simply not widely employed, if at all. To date, we have failed to embed security into each piece of data as it is created, creating a serious problem, particularly for government agencies.

Before a new product is made, many questions go through a software developer's head: what should the new input screens look like? How efficient should the new software be? Yet there is one important aspect that is still neglected too often: security. And this at a time when the number of cyber-attacks is increasing rapidly, as is revealed in the status report by the German Federal Office for Information Security (BSI). According to this, experts discover around 380,000 new malware versions every day, for example.

It is said that "the problem is: that the 95 percent of successful attacks are due to poorly programmed, poorly maintained or poorly configured software," something that admitted by Head of Internal Security & Cyber Defense at Deutsche Telekom. Yet this problem could be solved by taking security into consideration directly from the outset – "instead of sticking a plaster over the product only once it already has been assembled"

This research addresses and deepens what security is by design - security by default, what benefits they will bring with their implementation and how that is achieved. It will also analyze the stages of the basic design principles to ensure security at each stage of development of a system. We will further analyze how we will ensure the privacy of information, what philosophy has developed in this field, and how we can achieve a smooth incorporation of protection into every aspect of the design and development of a product or service. In addition, we will see the role and correlation of security with design with the General Data Protection Regulation (GDPR).

Gap analysis in the adoption of privacy by industry is provided. On the basis of these data, we analyze more closely the gaps in the current regulation (such as imprecise wording, weaknesses in penalties, retention obligations or personal data coverage).An emphasis is placed on the General Data Protection Regulation (GDPR) and what limitations on existing technologies and design method, and what incentives to adopt and comply with the regulation. Finally, a guide - guidelines have been developed to make industry more understandable how they will comply with the requirement for protection from design and by definition in accordance with Article 25 of the General Regulation and what the benefits of compliance.

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Η ασφάλεια πρέπει να είναι στο μυαλό όλων σε κάθε φάση του κύκλου ζωής του λογισμικού. Ένα λάθος σε οποιαδήποτε φάση μπορεί να έχει σοβαρές συνέπειες. Ωστόσο, η εξεύρεση λύσης δεν είναι εύκολη. Τα προβλήματα που σχετίζονται με την ασφάλεια εφαρμογών επιδεινώνονται με το χρόνο. Το παλαιότερο λογισμικό, το οποίο ποτέ δεν αναπτύχθηκε για να είναι ασφαλές, είναι το θεμέλιο πάνω στο οποίο οι σύγχρονες, είναι υψηλά συνδεδεμένες και κρίσιμες για τις επιχειρήσεις στην οποία λειτουργεί. Η δυσκολία προσαρμογής αυτών των παλαιότερων συστημάτων και η ενσωμάτωση νεότερων εφαρμογών έχει επιδεινώσει το πρόβλημα. Η οικοδόμηση ασφάλειας κατά τη φάση σχεδιασμού μειώνει τις ενδεχόμενες διαταραχές και αποφεύγει την εξίσου πολύ πιο δύσκολη αλλά και συνάμα δαπανηρή διαδικασία τις προσπάθειας προσθήκης ασφάλειας στα προϊόντα κατά την διάρκεια σχεδιασμού τους, πόσο μάλλον αφού έχουν είδη αναπτυχθεί.

Το Security by Design & by Default είναι μια προσέγγιση διασφάλισης ασφάλειας που επιτρέπει στους πελάτες να τυποποιήσουν το σχεδιασμό ασφαλείας, να αυτοματοποιήσουν τους ελέγχους ασφαλείας και να απλοποιήσουν τον έλεγχο. Πρόκειται για συστηματική προσέγγιση για την εξασφάλιση της ασφάλειας. Το Security by Design παρέχει στους προγραμματιστές τη δυνατότητα να αναπτύξουν τον έλεγχο ασφάλειας σε όλη τη διαδικασία ανάπτυξης. Αρχίζει με μια πιο ενεργητική προσέγγιση στην ασφάλεια των υποδομών που δεν βασίζεται στα τυπικά εργαλεία ασφάλειας τρίτων συμβαλλόμενων μερών προστασίας, αλλά δημιουργεί ασφάλεια στην υποδομή μας από τα θεμέλια.

Είναι κρίσιμο το γεγονός ότι κάθε φάση της διαδικασίας ανάπτυξης λογισμικού περιλαμβάνει την κατάλληλη ανάλυση ασφαλείας, άμυνες και αντίμετρα που θα οδηγήσουν σε ασφαλέστερο κώδικα. Από τις απαιτήσεις μέσω του σχεδιασμού και της εφαρμογής μέχρι τη δοκιμή και την ανάπτυξη, η ασφάλεια πρέπει να ενσωματωθεί σε ολόκληρο τον κύκλο ανάπτυξης λογισμικού (SDLC), προκειμένου να παρέχεται στην κοινότητα των χρηστών οι καλύτερες και πιο ασφαλείς λύσεις που βασίζονται στο λογισμικό.

Το περιβάλλον απειλής ασφάλειας εξελίσσεται συνεχώς σε αυτήν την ψηφιακή εποχή και η αντιμετώπιση των προκλήσεων αυτών των απειλών απαιτεί τη σωστή εμπειρογνωμοσύνη. Μία από τις σημαντικότερες προκλήσεις του IT security είναι το γεγονός ότι η ασφάλεια δεν έχει παραδοσιακά εξεταστεί στο σχεδιασμό προϊόντων για συσκευές δικτύωσης και αντικείμενα που δεν έχουν, παραδοσιακά, συνδεθεί με το δίκτυο. Οι αυστηροί κανονισμοί προληπτικής εποπτείας, ασφάλειας και προστασίας της ιδιωτικής ζωής αποτελούν αναπόσπαστο μέρος του κανονιστικού πλαισίου εντός του οποίου πρέπει να λειτουργούν οι οργανισμοί και το οποίο έχει ενισχυθεί τα τελευταία χρόνια.

2. Ασφάλεια κατά τον σχεδιασμό (Security By Design)

2.1 Τι είναι η ασφάλεια κατά των σχεδιασμό (Security by Design)

Η ασφάλεια από το σχεδιασμό είναι μια προσέγγιση στην ανάπτυξη λογισμικού και υλικού που επιδιώκει να καταστήσει τα συστήματα ως απαλλαγμένα από τρωτά σημεία και αδιαπέραστα από την επίθεση μέσω μέτρων όπως οι συνεχείς έλεγχοι, οι έλεγχοι ταυτότητας και η τήρηση των βέλτιστων πρακτικών προγραμματισμού.

Η έμφαση στην οικοδόμηση της ασφάλειας στα προϊόντα αντισταθμίζει την πολύ συνηθισμένη τάση της ασφάλειας να είναι μια αφετηρία ανάπτυξης. Αντιμετώπιση τρωτών σημείων και βάζοντας κάποια ”μπαλώματα” σε τρύπες ασφαλείας που έχουν βρεθεί μπορεί να είναι μια διαδικασία όχι και τόσο ακριβής, πόσο μάλλον αποτελεσματικές, όσο το σχεδιασμό συστημάτων ώστε να είναι όσο το δυνατόν ασφαλέστερα από την αρχή της ανάπτυξής τους.

Η ασφάλεια από το σχεδιασμό ακόμα (SbD) αποκτά ταχύτατα ρόλο στο ταχέως αναπτυσσόμενο περιβάλλον του Internet Of Things (IoT), στο οποίο σχεδόν κάθε πιθανή συσκευή, αντικείμενο ή οντότητα μπορεί να έχει ένα μοναδικό αναγνωριστικό (UID) και να είναι δικτυωμένο ώστε να είναι διευθυνσιοδοτούμενο μέσω του διαδικτύου. Μία από τις μεγαλύτερες προκλήσεις της ασφάλειας του διαδικτύου είναι το γεγονός ότι η ασφάλεια δεν έχει παραδοσιακά εξεταστεί στο σχεδιασμό προϊόντων για συσκευές δικτύωσης και αντικείμενα που δεν έχουν παραδοσιακά συνδεθεί με το δίκτυο.

2.2 Ασφάλεια κατά των σχεδιασμό στην πράξη (Security by Design in practice)

Στην πράξη, το Security by Design (SbD) είναι για την κωδικοποίηση τυποποιημένων, επαναληπτικών, αυτοματοποιημένων αρχιτεκτονικών, έτσι ώστε η ασφάλεια μας και τα πρότυπα ελέγχου να παραμένουν συνεπή σε πολλαπλά περιβάλλοντα. Οι βασικοί μας στόχοι θα πρέπει να είναι:

i. **Ελεγχόμενη, τυποποιημένη διαδικασία κατασκευής**: Σχεδιασμός αρχιτεκτονικής κώδικα σε ένα πρότυπο που μπορεί να δημιουργήσει ένα περιβάλλον σύννεφου (cloud) . Στο Amazon AWS γίνεται με CloudFormation. Εν συνέχεια, κωδικοποιούμε τις διαμορφώσεις λειτουργικών συστημάτων σε ένα εργαλείο διαχείρισης παραμέτρων όπως το Puppet.

ii. **Ελεγχόμενη, τυποποιημένη διαδικασία ενημέρωσης:** Τοποθετούμαι τα πρότυπα CloudFormation και τα Puppet σε ένα εργαλείο διαχείρισης πηγαίου

κώδικα, όπως το GitHub, το οποίο μας επιτρέπει να εκτελούμαι πρότυπα έκδοσης, να κάνουμε αλλαγές, να βλέπουμε ποιος έκανε τι κλπ.

iii. **Αυτοματοποιημένη δοκιμή υποδομής και ασφάλειας κώδικα ως μέρος του αγωγού CI / CD:** Ενσωμάτωση τόσο των δοκιμών σε επίπεδο υποδομής όσο και σε επίπεδο κώδικα στη διαδικασία ανάπτυξης κώδικα καθώς και στη διαδικασία ενημέρωσης διαχείρισης διαμόρφωσης. Στο Logicworks, συχνά χρησιμοποιούμε το AWS CodeDeploy για τη δομή της διαδικασίας ανάπτυξης κώδικα. Μπορείτε επίσης να χρησιμοποιήσετε το Docker και το AWS ECS.

iv. **Επιβαλλόμενες ρυθμίσεις παραμέτρων στην παραγωγή**: Δημιουργήστε δέσμες ενεργειών διαχείρισης παραμέτρων που εκτελούνται συνεχώς ενάντια σε όλα τα περιβάλλοντά σας για να επιβάλλετε ρυθμίσεις. Συνήθως φιλοξενείται σε κεντρικό διαχειριστικό κόμβο και απαιτεί προσέγγιση VPC σχεδίασης με ακτίνες ομιλίας.

v. **Εργαλεία ώριμης παρακολούθησης με δεδομένα που υπόκεινται σε έξυπνη, καλά εκπαιδευμένη αξιολόγηση από τον άνθρωπο**: Σε συμβατά περιβάλλοντα, τα εργαλεία παρακολούθησής σας συνήθως έχουν εντολή και τα αρχεία καταγραφής πρέπει να υπόκεινται σε επανεξέταση από τον άνθρωπο. χρησιμοποιούμε τα εγγενή εργαλεία AWS όπως το CloudWatch, CloudTrail και Inspector AWS, καθώς και το Logic IDs Alert και το Log Manager και το SumoLogic για να καλύψουν τις περισσότερες απαιτήσεις. Το SumoLogic μας βοηθάει να χρησιμοποιήσουμε την εκμάθηση μηχανών για τη δημιουργία προσαρμοσμένων ειδοποιήσεων που ενημερώνουν το Κέντρο Λειτουργιών Δικτύου 24 × 7 όταν συμβαίνει ασυνήθιστη δραστηριότητα, ώστε οι μηχανικοί αυτοί να μπορούν να αναλάβουν τις κατάλληλες ενέργειες με ακριβέστερα δεδομένα σε πραγματικό χρόνο.

vi. **Μικρή έως καμία άμεση ανθρώπινη παρέμβαση στο περιβάλλον ... ποτέ**: Μόλις όλα αυτά τα εργαλεία είναι στη θέση τους, δεν θα πρέπει πλέον να τροποποιείτε άμεσα μεμονωμένες περιπτώσεις ή διαμορφώσεις. Θα πρέπει, αντίθετα, να τροποποιήσετε το πρότυπο ή το σενάριο για να ενημερώσετε (ή, ιδανικά, να επανεκκινήσετε) το περιβάλλον.

2.3 Γιατί είναι σημαντικό και γιατί το χρειαζόμαστε (Why it is important & Why do we need it?)

Φαίνεται λίγο προφανές, αλλά πολύ συχνά δημιουργούνται και παραδίδονται νέες λύσεις ή δυνατότητες και, στη συνέχεια, οι άνθρωποι σκέφτονται τον καλύτερο τρόπο για να το κάνουν ασφαλές και συμμορφούμενο. Και στην περίπτωση αυτή, είναι εκθετικά πιο δύσκολο να προσθέσετε ασφάλεια στο τέλος από το να το προσθέσετε από την αρχή του έργου και τις αναπτυξιακές προσπάθειες. Οι αξιολογήσεις επικινδυνότητας για την αντιμετώπιση πιθανών απειλών και στόχων επίθεσης θα πρέπει να εξετάζονται κατά τη διάρκεια της διαδικασίας σχεδιασμού.

Οι αρχιτέκτονες και οι πάροχοι λύσεων χρειάζονται καθοδήγηση για την παραγωγή ασφαλών εφαρμογών από το σχεδιασμό και μπορούν να το κάνουν αυτό όχι μόνο εφαρμόζοντας τους βασικούς ελέγχους που τεκμηριώνονται στο κύριο κείμενο αλλά και ανατρέχοντας στις υποκείμενες "γιατί" στις αρχές αυτές. Οι αρχές ασφαλείας, όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα, είναι σημαντικές για όλες τις εφαρμογές και τις συσκευές.

2.4 Επιπτώσεις του μη ασφαλούς περιβάλλοντος (Domino effects of insecurity)

Τώρα περισσότερο από ποτέ, η χρήση του μοντέλου Security by Design και του Secure by Default είναι κρίσιμη. Σκεφτείτε το ως ένα φαινόμενο ντόμινο. Εάν μια διαδικτυακή εταιρεία λιανικής επιλέξει έναν πάροχο υπηρεσιών που διαχειρίζεται να φιλοξενήσει την υποδομή και να παράσχει διαχειριζόμενες υπηρεσίες, ο σχεδιασμός και η ασφάλεια που χρησιμοποιούνται για την κατασκευή και την παροχή των υπηρεσιών αποτελούν κρίσιμο παράγοντα. Εάν υπάρχουν αδυναμίες ασφάλειας, η διαδικτυακή εταιρεία λιανικής πώλησης θα εκτεθεί σε αυτά τα ελαττώματα ασφαλείας, όπως και οι πελάτες τους, με τη σειρά τους - γεγονός που θα προκαλέσει την επιχειρηματική φήμη να υποφέρει.

Ο εμπειρογνώμονας στον τομέα της ασφάλειας στον κυβερνοχώρο Bruce Schneier ζήτησε κυβερνητική ρύθμιση του IoT, καταλήγοντας στο συμπέρασμα ότι τόσο οι κατασκευαστές του IoT όσο και οι πελάτες τους δεν ενδιαφέρονται για την ασφάλεια των 8,4 δισεκατομμυρίων συσκευών που έχουν συνδεθεί στο διαδίκτυο με τρέχουσα χρήση.

Η Forrester Research συζητά τις προοπτικές για τις 13 πιο σημαντικές και σημαντικές τεχνολογίες ασφάλειας του Διαδικτύου, προειδοποιώντας ότι "δεν υπάρχει ενιαία, μαγική κουκκίδα ασφαλείας που να μπορεί εύκολα να διορθώσει όλα τα θέματα ασφάλειας του Διαδικτύου". Ο Forrester παραθέτει τις ακόλουθες προκλήσεις για την επίτευξη ασφαλούς IoT: Πολλές συσκευές IoT δεν διαθέτουν βασικές απαιτήσεις ασφάλειας. Υπάρχει πληθώρα προτύπων και πρωτοκόλλων του Διαδικτύου, τα οποία δημιουργούν τυφλά σημεία ασφαλείας. Η κλίμακα και το πεδίο εφαρμογής των IoT παρεμποδίζουν την προβολή σε περιστατικά

ασφάλειας. Υπάρχει έλλειψη σαφήνειας της ευθύνης όσον αφορά την προστασία της ιδιωτικής ζωής και την ασφάλεια.

2.5 Θεμελιώδης Αρχές ασφάλειας από το σχεδιασμό (Principles of security by design)

Οι Αρχές Σχεδιασμού Ασφαλείας OWASP δημιουργήθηκαν για να βοηθήσουν τους προγραμματιστές να δημιουργήσουν εξαιρετικά ασφαλείς εφαρμογές ιστού. Οι αρχές σχεδιασμού ασφάλειας OWASP έχουν ως εξής:

Asset clarification (Αποσαφήνιση περιουσιακών στοιχείων):

Πριν από την ανάπτυξη στρατηγικών ασφαλείας, είναι σημαντικό να προσδιορίσετε και να ταξινομήσετε τα δεδομένα που θα χειριστεί η εφαρμογή. Το OWASP υποδεικνύει ότι οι προγραμματιστές δημιουργούν ελέγχους ασφάλειας που είναι κατάλληλοι για την αξία των δεδομένων που διαχειρίζονται. Για παράδειγμα, μια εφαρμογή επεξεργασίας οικονομικών πληροφοριών πρέπει να έχει πολύ αυστηρότερους περιορισμούς από ένα blog ή ένα φόρουμ στο διαδίκτυο.

Understanding attackers (Κατανόηση των επιτιθέμενων):

Οι προγραμματιστές θα πρέπει να σχεδιάζουν ελέγχους που αποτρέπουν την κατάχρηση της εφαρμογής από διάφορους τύπους κακόβουλων συμβαλλομένων, συμπεριλαμβανομένων (από τα περισσότερα έως τα λιγότερο επικίνδυνα):

- Δυσαρεστημένους υπαλλήλους και προγραμματιστές
- Οργανώσεις με κακόβουλη πρόθεση
- Παρακινούμενοι κυβερνοεγκληματίες
- Script kiddies (άτομα δηλαδή που χρησιμοποιούν σενάρια ή λογισμικό γραμμένο από κάποιον άλλο για να εκμεταλλευτεί ή να σπάσει ένα σύστημα υπολογιστή)

Ο πιο επικίνδυνος τύπος επιθέσεων που πρέπει να προστατεύουν οι προγραμματιστές είναι από τα δυσαρεστημένα μέλη του προσωπικού και τους προγραμματιστές. Αυτό συμβαίνει επειδή συνήθως έχουν υψηλό επίπεδο πρόσβασης σε ευαίσθητα συστήματα.

Οι προγραμματιστές μπορούν να χρησιμοποιήσουν τεχνικές αρχών OWASP για να προστατεύσουν αυτούς τους τύπους επιθέσεων.

Core pillars of information security(Βασικοί πυλώνες της ασφάλειας των πληροφοριών):

Το OWASP συνιστά να σχεδιάζονται όλοι οι έλεγχοι ασφάλειας με βάση τους πυλώνες της ασφάλειας των πληροφοριών:

- Εμπιστευτικότητα - επιτρέπουν μόνο την πρόσβαση σε δεδομένα για τα οποία επιτρέπεται ο χρήστης.
- Ακεραιότητα - Βεβαιωθείτε ότι τα δεδομένα δεν έχουν αλλοιωθεί ή αλλοιωθεί από μη εξουσιοδοτημένους χρήστες.
- Διαθεσιμότητα - εξασφαλίστε ότι τα συστήματα και τα δεδομένα είναι διαθέσιμα στους εξουσιοδοτημένους χρήστες όταν το χρειάζονται.

Security architecture(Αρχιτεκτονική ασφαλείας)

Το OWASP συνιστά κάθε εφαρμογή να έχει μέτρα ασφάλειας εφαρμογών σχεδιασμένα για να καλύπτουν κάθε είδους κινδύνους, που κυμαίνονται από τυπικούς κινδύνους χρήσης (ακούσια διαγραφή δεδομένων) έως ακραίες επιθέσεις (βίαιες επιθέσεις δυνάμεων, επιθέσεις ενέσεων κλπ.).

Συστήνουν στους προγραμματιστές να εξετάζουν κάθε στοιχείο σχετικά με την εφαρμογή που σχεδιάζουν και να θέτουν τις ακόλουθες ερωτήσεις:

- Είναι η διαδικασία που περιβάλλει αυτό το χαρακτηριστικό όσο το δυνατόν ασφαλέστερη; Με άλλα λόγια, είναι αυτή η λανθασμένη διαδικασία;
- Αν ήμουν κακός, πώς θα μπορούσα να καταχραστώ αυτό το χαρακτηριστικό;
- Απαιτείται η λειτουργία από προεπιλογή; Εάν ναι, υπάρχουν περιορισμοί ή επιλογές που θα μπορούσαν να συμβάλουν στη μείωση του κινδύνου από αυτό το χαρακτηριστικό;

2.5.1 Ελαχιστοποιήστε την περιοχή επίθεσης (Minimize attack surface area)

Κάθε δυνατότητα που προστίθεται σε μια εφαρμογή προσθέτει ένα ορισμένο βαθμό κινδύνου στη συνολική εφαρμογή. Ο στόχος για ασφαλή ανάπτυξη είναι να μειωθεί ο συνολικός κίνδυνος μειώνοντας την επιφάνεια επιθέσεων.

Κάθε φορά που οι προγραμματιστές προσθέτουν ένα χαρακτηριστικό στην εφαρμογή τους, αυξάνουν τον κίνδυνο μιας ευπάθειας ασφαλείας. Η αρχή της ελαχιστοποίησης της επιφάνειας επιθέσεων περιορίζει τις λειτουργίες στις οποίες επιτρέπεται στους χρήστες να έχουν πρόσβαση, για να μειώσουν τις πιθανές ευπάθειες.

Για παράδειγμα, μπορείτε να κωδικοποιήσετε μια λειτουργία αναζήτησης σε μια εφαρμογή. Αυτή η δυνατότητα αναζήτησης είναι ενδεχομένως ευάλωτη σε επιθέσεις ένταξης αρχείων και επιθέσεις SQL injection. Ο προγραμματιστής θα μπορούσε να περιορίσει την πρόσβαση στη λειτουργία αναζήτησης, επομένως μόνο οι εγγεγραμμένοι χρήστες θα μπορούσαν να το χρησιμοποιήσουν - μειώνοντας την επιφάνεια επίθεσης και τον κίνδυνο επιτυχούς επίθεσης.

2.5.2 θέσπιση ασφαλών προεπιλογών (Establish secure defaults)

Αυτή η αρχή δηλώνει ότι η εφαρμογή πρέπει να είναι ασφαλής από προεπιλογή(by default). Αυτό σημαίνει ότι ένας νέος χρήστης πρέπει να λάβει μέτρα για να αποκτήσει υψηλότερα προνόμια και να καταργήσει πρόσθετα μέτρα ασφαλείας (αν επιτρέπεται).

Η θέσπιση ασφαλών προεπιλογών σημαίνει ότι πρέπει να υπάρχουν ισχυροί κανόνες ασφαλείας για τον τρόπο χειρισμού των καταχωρήσεων των χρηστών, πόσο συχνά πρέπει να ενημερώνονται οι κωδικοί πρόσβασης, πόσο σύνθετοι είναι οι κωδικοί πρόσβασης και ούτω καθεξής. Οι χρήστες εφαρμογών ενδέχεται να είναι σε θέση να απενεργοποιήσουν ορισμένες από αυτές τις λειτουργίες, αλλά θα πρέπει να οριστούν από προεπιλογή σε επίπεδο υψηλής ασφάλειας.

2.5.3 Αρχή του ελάχιστου προνομίου (Principle of Least privilege(POLP))

Η αρχή του ελάχιστου προνομίου (POLP) δηλώνει ότι ο χρήστης πρέπει να έχει το ελάχιστο σύνολο προνομίων που απαιτούνται για την εκτέλεση μιας συγκεκριμένης εργασίας. Το POLP μπορεί να εφαρμοστεί σε όλες τις πτυχές μιας διαδικτυακής εφαρμογής, συμπεριλαμβανομένων των δικαιωμάτων των χρηστών και της πρόσβασης σε πόρους(όπως CPU, δικαιώματα μνήμης, δικτύου και αρχείων συστήματος).

Για παράδειγμα, ένας χρήστης που έχει εγγραφεί σε μια εφαρμογή ιστολογίου ως "συγγραφέας" δεν θα πρέπει να έχει δικαιώματα διαχειριστή που να του επιτρέπουν να προσθέτει ή να καταργεί χρήστες. Θα πρέπει να επιτρέπεται μόνο να δημοσιεύουν άρθρα στην εφαρμογή.

Επιπλέον εάν ένας client server απαιτεί μόνο πρόσβαση στο δίκτυο, να διαβάσει την πρόσβαση σε έναν πίνακα βάσης δεδομένων και τη δυνατότητα εγγραφής σε ένα αρχείο καταγραφής, αυτό περιγράφει όλα τα δικαιώματα που πρέπει να χορηγηθούν. Σε καμία περίπτωση δεν πρέπει να παρέχεται στο μεσολαβητή δικαιώματα διαχειριστή.

2.5.4 Αρχή υπεράσπισης σε βάθος (Principle of Defense in depth)

Η αρχή της υπεράσπισης σε βάθος δηλώνει ότι οι πολλαπλοί έλεγχοι ασφάλειας που προσεγγίζουν τους κινδύνους με διαφορετικούς τρόπους είναι η καλύτερη επιλογή για την εξασφάλιση μιας εφαρμογής. Έτσι, αντί να έχετε έναν έλεγχο ασφαλείας για την πρόσβαση των χρηστών, θα έχετε πολλαπλά επίπεδα επικύρωσης, πρόσθετα εργαλεία ελέγχου ασφαλείας και εργαλεία καταγραφής.

Για παράδειγμα, αντί να αφήσετε ένα χρήστη να συνδεθεί μόνο με ένα όνομα χρήστη και έναν κωδικό πρόσβασης, θα χρησιμοποιούσατε έλεγχο IP, σύστημα Captcha, καταγραφή των προσπαθειών σύνδεσης, ανίχνευση brute force attack και ούτω καθεξής.

2.5.5 Αποτυχία με ασφαλή τρόπο (Fail securely)

Υπάρχουν πολλοί λόγοι για τους οποίους μια εφαρμογή Ιστού θα αποτύχει να επεξεργαστεί μια συναλλαγή. Ίσως μια σύνδεση βάσης δεδομένων απέτυχε ή τα δεδομένα που εισήχθησαν από έναν χρήστη ήταν εσφαλμένα. Αυτή η αρχή αναφέρει ότι οι αιτήσεις πρέπει να αποτύχουν με ασφαλή τρόπο. Η αποτυχία δεν πρέπει να δίνει στο χρήστη πρόσθετα προνόμια και δεν πρέπει να εμφανίζει τις ευαίσθητες πληροφορίες του χρήστη, όπως ερωτήματα βάσης δεδομένων ή αρχεία καταγραφής.

Οι Εφαρμογές συχνά αποτυγχάνουν να επεξεργάζεται συναλλαγές για πολλούς λόγους. Το πώς αποτυγχάνουν μπορούν να καθορίσουν εάν μια εφαρμογή είναι ασφαλής ή όχι. Για παράδειγμα :

```
isAdmin = true;
try {
  codeWhichMayFail();
  isAdmin = isUserInRole( “Administrator” );
}
catch (Exception ex) {
```

```
    log.write(ex.toString());
}
```

Εάν η εντολή **codeWhichMayFail()** ή **isUserInRole** αποτυγχάνει, τότε ο χρήστης αυτομάτως είναι ένας διαχειριστής από προεπιλογή. Αυτός είναι προφανώς ένας κίνδυνος για την ασφάλεια

2.5.6 Μην εμπιστεύεστε τις υπηρεσίες (Don't trust services)

Πολλές εφαρμογές ιστού χρησιμοποιούν υπηρεσίες τρίτου μέρους για την πρόσβαση σε πρόσθετες λειτουργίες ή την απόκτηση πρόσθετων δεδομένων. Αυτή η αρχή δηλώνει ότι δεν πρέπει ποτέ να εμπιστεύεστε αυτές τις υπηρεσίες από την άποψη της ασφάλειας. Αυτό σημαίνει ότι η εφαρμογή θα πρέπει πάντα να ελέγχει την εγκυρότητα των δεδομένων που στέλνουν οι υπηρεσίες τρίτων και να μην παρέχουν στις υπηρεσίες αυτές δικαιώματα υψηλού επιπέδου εντός της εφαρμογής.

Επιπροσθέτως πολλοί είναι και οι οργανισμοί οι οποίοι χρησιμοποιούν τις δυνατότητες επεξεργασίας σε εξωτερικούς συνεργάτες (third party), οι οποίοι πιθανότατα θα έχουν διαφορετικές πολιτικές ασφάλειας από ό, τι έχουμε εμείς. Είναι απίθανο να μπορέσουμε να επηρεάσουμε ή να ελέγξουμε οποιοδήποτε εξωτερικό τρίτο μέρος, είτε είναι οικιακοί χρήστες είτε μεγάλοι προμηθευτές ή συνεργάτες Επομένως, η έμμεση εμπιστοσύνη των συστημάτων που λειτουργούν εξωτερικά δεν δικαιολογείται. Όλα τα εξωτερικά συστήματα θα πρέπει να αντιμετωπίζονται με παρόμοιο τρόπο.

Για παράδειγμα, ένας πάροχος προγράμματος πιστότητας παρέχει δεδομένα που χρησιμοποιούνται από το Internet Banking. Ωστόσο, τα δεδομένα θα πρέπει να ελέγχονται για να εξασφαλίζεται ότι είναι ασφαλές.

2.5.7 Διαχωρισμός των καθηκόντων (Separation of duties)

Ένας βασικός έλεγχος απάτης είναι ο διαχωρισμός των καθηκόντων. Ορισμένοι ρόλοι έχουν διαφορετικά επίπεδα εμπιστοσύνης από τους κανονικούς χρήστες. Συγκεκριμένα, οι διαχειριστές διαφέρουν από τους κανονικούς χρήστες. Σε γενικές γραμμές, οι διαχειριστές δεν πρέπει να είναι χρήστες της εφαρμογής.

Ο διαχωρισμός των καθηκόντων μπορεί να χρησιμοποιηθεί για την αποφυγή της άσκησης δόλιων ενεργειών. Για παράδειγμα, ένας χρήστης ενός ηλεκτρονικού καταστήματος δεν πρέπει να έχει δικαιώματα διαχειριστής, καθώς θα είναι σε θέση να αλλάξει τις παραγγελίες και πιθανόν να αγοράζει προϊόντα χωρίς να πληρώσει το αντίτιμο. Το αντίστροφο επίσης - ένας διαχειριστής δεν πρέπει να έχει τη δυνατότητα να κάνει πράγματα που κάνουν οι πελάτες, όπως επεμβαίνει στα στοιχεία παραγγελιών αλλά πρέπει να είναι σε θέση να ενεργοποιήσει ή να απενεργοποιήσει το σύστημα, να ορίσει την πολιτική για τον κωδικό πρόσβασης κτλπ.

2.5.8 Αποφύγετε την ασφάλεια από την ασάφεια (Avoid security by obscurity)

Αυτή η αρχή δηλώνει ότι δεν πρέπει ποτέ να στηριχθεί η ασφάλεια από την αφάνεια. Εάν η εφαρμογή σας απαιτεί τη διαγραφή της διεύθυνσης URL διαχείρισης, ώστε να μπορεί να παραμείνει ασφαλής, τότε δεν είναι καθόλου ασφαλής. Θα πρέπει να υπάρχουν αρκετοί έλεγχοι ασφαλείας για να διατηρείτε την εφαρμογή σας ασφαλή χωρίς να αποκρύπτετε τη βασική λειτουργικότητα ή τον πηγαίο κώδικα.

Ασφάλεια μέσω της αφύπνισης είναι ένας ασθενής έλεγχος ασφαλείας και σχεδόν πάντα αποτυγχάνει όταν είναι ο μοναδικός έλεγχος. Αυτό δεν σημαίνει ότι η διατήρηση μυστικών είναι μια κακή ιδέα, σημαίνει απλά ότι η ασφάλεια των βασικών συστημάτων δεν θα πρέπει να εξαρτάται από τη διατήρηση κρυμμένων στοιχείων.

Για παράδειγμα, η ασφάλεια μιας εφαρμογής δεν πρέπει να βασίζεται στη γνώση του πηγαίου κώδικα που κρατείται μυστική. Η ασφάλεια θα πρέπει να βασίζεται σε πολλούς άλλους παράγοντες, όπως λογικές πολιτικές κωδικού πρόσβασης, σε βάθος υπεράσπισης, όρια επιχειρηματικών συναλλαγών, σταθερή αρχιτεκτονική δικτύου και ελέγχους απάτης και ελέγχου.

Ένα πρακτικό παράδειγμα είναι το Linux. Ο πηγαίος κώδικας του Linux είναι ευρέως διαθέσιμος παρόλα αυτά έχει ασφαλιστεί σωστά, έτσι το καθιστά στο να είναι ένα ανθεκτικό και ασφαλές λειτουργικό σύστημα.

2.5.9 Μη χρησιμοποίηση πολύπλοκων αρχιτεκτονικών (Keep security simple)

Η επιφάνεια επίθεσης και η απλότητα είναι συνυφασμένα. Ορισμένες μηχανικές εφαρμογές λογισμικού προτιμούν υπερβολικά περίπλοκες προσεγγίσεις σε αυτό που διαφορετικά θα ήταν σχετικά απλό και με απλό κώδικα.

Οι προγραμματιστές θα πρέπει να αποφεύγουν τη χρήση πολύ εξελιγμένης αρχιτεκτονικής κατά την ανάπτυξη ελέγχων ασφαλείας για τις εφαρμογές τους. Η ύπαρξη πολύπλοκων μηχανισμών μπορεί να αυξήσει τον κίνδυνο σφαλμάτων.

2.5.10 Διόρθωση σφαλμάτων (Fix security issues correctly)

Εάν ένα ζήτημα ασφαλείας έχει εντοπιστεί σε μια εφαρμογή, οι προγραμματιστές θα πρέπει να καθορίσουν τη βασική αιτία του προβλήματος. Εάν η εφαρμογή χρησιμοποιεί μοτίβα σχεδίασης, είναι πιθανό το σφάλμα να υπάρχει σε πολλά συστήματα. Οι προγραμματιστές θα πρέπει να είναι προσεκτικοί για τον εντοπισμό όλων των επηρεαζόμενων συστημάτων.

Για παράδειγμα, εάν ένας χρήστης διαπιστώσει ότι μπορεί να δει στοιχεία ενός άλλου χρήστη προσαρμόζοντας το cookie του. Η διόρθωση φαίνεται να είναι σχετικά απλή, αλλά καθώς ο κώδικας επεξεργασίας των cookies μοιράζεται σε όλες τις εφαρμογές, μια αλλαγή σε μία μόνο εφαρμογή θα επηρεάσει και όλες τις άλλες εφαρμογές που συνδέονται με αυτή. Επομένως, η διόρθωση των σφαλμάτων πρέπει να δοκιμαστεί σε όλες τις εφαρμογές που επηρεάζονται.

2.7 Ασφαλές κατά τον σχεδιασμό: Διεξαγωγή στρατηγικής προσέγγισης στην κυβερνοασφάλεια (SECURE BY DESIGN: TAKING A STRATEGIC APPROACH TO CYBERSECURITY)

2.7.1 Οι απειλές των κυβερνοεπιθέσεων έχουν αναγνωριστεί (THE THREAT FROM CYBERATTACKS IS CLEAR AND ACKNOWLEDGED)

Σχεδόν όλες οι εταιρίες του Ηνωμένου Βασιλείου είδαν τους χάκερ να διεισδύσουν επιτυχώς στα συστήματα πληροφορικής τους σε μια προσπάθεια να κλέψουν, να αλλάξουν ή να δημοσιοποιήσουν τα ευαίσθητα δεδομένα τους. Οι κακόβουλοι - εγκληματίες δεν απευθύνονται μόνο σε χρηματοπιστωτικά ιδρύματα ή αναζητούν οικονομικά δεδομένα, αλλά αναζητούν τώρα προσωπικά δεδομένα των εργαζομένων και των πελατών , εταιρική νοημοσύνη και να πειραματιστεί με τις υποδομές των εταιρειών με εγκληματικό σκοπό.

Το Συμβούλιο Εθνικής Ασφάλειας του Ηνωμένου Βασιλείου ανακοίνωσε πρόσφατα ότι οι επιθέσεις σε δίκτυα υπολογιστών συγκαταλέγονται στις μεγαλύτερες αναδυόμενες απειλές για το Ηνωμένο Βασίλειο και γενικά στην σύγχρονη κοινωνία, κατατάσσοντάς τις παράλληλα με την τρομοκρατία και την πανδημία της γρίπης ως βασικούς παγκόσμιους κινδύνους για την ασφάλεια. Οι πρόσφατες επιθέσεις υψηλού προφίλ που αναφέρθηκαν σε διάφορες βιομηχανίες περιλαμβάνουν:

- Η Fiat Chrysler, που αναγκάστηκε να ανακαλέσει 1,4 εκατομμύρια οχήματα στις ΗΠΑ για αναβάθμιση στα συστήματα ηλεκτρονικών υπολογιστών, αφού οι ερευνητές της ασφάλειας απέδειξαν ότι θα μπορούσαν να αποκτήσουν τον πλήρη έλεγχο ενός Jeep Cherokee από απόσταση 10-20 μιλίων με την εισβολή στο ενσωματωμένο σύστημα που είναι τοποθετημένο μέσα στο εγκέφαλο του εν λόγω οχήματος.

- Η Carphone Warehouse, εταιρεία τηλεπικοινωνίων αναγνώρισε σοβαρή παραβίαση δεδομένων κατά την οποία ενδέχεται να έχουν υποκλαπεί τραπεζικές λεπτομέρειες για 2.4 εκατομμύρια πελάτες της.

- Επίσης τρεις από τις μεγαλύτερες φαρμακευτικές εταιρείες τους τελευταίους 18 μήνες είδαν παραβίαση και εκτενή πρόσβαση σε λεπτομέρειες στις χρηματοοικονομικές τους συναλλαγές.

- Η νεοαποκτηθείσα ασιατική θυγατρική της Telstra, η Pacnet, αναγνώρισε παράνομες δραστηριότητες στο δίκτυο πληροφορικής της, λίγο πριν από την τελική της εξαγορά.

Ενώ η πλειοψηφία των εταιρειών συμμετέχουν ενεργά στη θέσπιση πολιτικών διακυβέρνησης για την ασφάλεια και στη διενέργεια ελέγχων ασφαλείας με στόχο την προστασία τους από το έγκλημα στον κυβερνοχώρο, σχεδόν το ένα δέκατο των επιχειρήσεων του Ηνωμένου Βασιλείου δεν έχουν ενεργήσει καθόλου για να προστατευθούν από την πειρατεία.

Εκτός αυτού, η ασφάλεια στον κυβερνοχώρο αρχίζει να παίρνει το σωστό επίπεδο προσοχής στις μεγάλες επιχειρήσεις. Δεν θεωρείται πλέον ως πολιτικό ζήτημα, ζήτημα συμμόρφωσης ή θέμα πληροφορικής. Αντίθετα, θεωρείται τώρα περισσότερο ως θέμα στρατηγικού και εταιρικού κινδύνου, το οποίο πρέπει να εξεταστεί σε όλους τους εσωτερικούς κύκλους ζωής των έργων και ως μέρος της «συνήθους επιχειρηματικής δραστηριότητας», όχι μόνο ως εφάπαξ δραστηριότητα. Τα μέλη του διοικητικού συμβουλίου πολλών επιχειρήσεων κατέχουν πλέον τον CEO (chief executive officer) που είναι κυρίως υπεύθυνος για την ασφάλεια στον κυβερνοχώρο, με τον CIO (chief information officer,) ως το δεύτερο πιο υπεύθυνο στέλεχος, δείχνοντας τη σημασία της ασφάλειας στον κυβερνοχώρο μέσα στον οργανισμό.

2.7.2 Η κυβερνοασφάλεια ακόμα δεν έχει πραγματικά αποτελέσματα (THE ELEVATING PROFILE OF CYBERSECURITY HAS YET TO TAKE REAL EFFECT)

Σε μια πρόσφατη έρευνα για το Τμήμα Επιχειρηματικής Καινοτομίας και Δεξιοτήτων του Ηνωμένου Βασιλείου και η οποία συνέβαλε 200 εταιρικοί διευθυντές, μόλις πάνω από το ένα τρίτο δήλωσε ότι η ασφάλεια του κυβερνοχώρου με κάποια ιδιότητα συζητήθηκε σε κάθε συνεδρίαση του διοικητικού συμβουλίου και σχεδόν οι μισοί δήλωσαν ότι συζητήθηκε στις περισσότερες συνεδριάσεις. Αυτό είναι πιθανό να είναι μια σημαντική αύξηση από συγκρίσιμες απαντήσεις πριν από 12 μήνες. Ωστόσο, τα δύο τρίτα των μελών του διοικητικού συμβουλίου δεν είναι σίγουροι για την ικανότητα των εταιρειών τους να υπερασπίζονται πλήρως τους κυβερνοχώρους, ενώ μόνο το 4% είναι "πολύ" βέβαιοι για την άμυνα τους. Παρά την έλλειψη εμπιστοσύνης, η ενσωμάτωση της ασφάλειας στη σχεδίαση (security by design) νέων προϊόντων κατέλαβε την δεύτερη προτεραιότητα κατά την εξέταση της ανάπτυξης νέων προϊόντων και υπηρεσιών.

Η περιορισμένη ποσότητα νέων προϊόντων που κυκλοφορούν στο χώρο της ασφάλειας, καθώς και η ταχεία αύξηση του όγκου και της κρισιμότητας των απειλών των τελευταίων χρόνων, δείχνουν ότι το επίπεδο και η διαθεσιμότητα των τεχνικών γνώσεων του τομέα του κυβερνοχώρου συνολικά δεν έχει αυξηθεί σε σχέση με τον ρυθμό ζήτησης.

2.7.3 Στρατηγική προσέγγιση για την αποτελεσματική αντιμετώπιση απειλών

Το οικοσύστημα για την ασφάλεια του κυβερνοχώρου είναι διαφορετικό και περιλαμβάνει εταιρείες επαγγελματικών υπηρεσιών, προμηθευτές τεχνολογίας, παρόχους αμυντικού συστήματος συστημάτων πληροφορικής καθώς και εξειδικευμένους ειδικούς στον κυβερνοχώρο. Ωστόσο, στα περισσότερα παραδείγματα, η εστίαση αυτών των οργανώσεων μπορεί να εντοπιστεί στις ρίζες τους. Για παράδειγμα, πολλές από τις εταιρείες παροχής επαγγελματικών υπηρεσιών προσφέρουν υπηρεσίες ελέγχου ασφάλειας, βασιζόμενες στην εμπειρία του χρηματοοικονομικού ελέγχου τους σε μια νέα αγορά για την κάλυψη ενός αναδυόμενου χάσματος Ως αποτέλεσμα, πολλές υπηρεσίες στην αγορά παροχής συμβουλών στον κυβερνοχώρο τείνουν να βασίζονται σε λογιστικό έλεγχο και ελέγχους συμμόρφωσης με τη βιομηχανία και τα κυβερνητικά πρότυπα, συμπεριλαμβανομένων των ISO27001 και CESG Ασφαλισμένη Υπηρεσία (CAS).

Οι προμηθευτές τεχνολογίας και οι πάροχοι αμυντικού συστήματος έχουν επίσης τη δυνατότητα να προσφέρουν συμβουλές στον τομέα της ασφάλειας στον κυβερνοχώρο, αλλά αυτό επικεντρώθηκε κατά κύριο λόγο στο κατά πόσον το υλικό και το λογισμικό στο περιβάλλον πληροφορικής μιας εταιρείας και η αρχιτεκτονική ασφαλείας της είναι κατάλληλα για τον σκοπό αυτό εκείνη τη χρονική στιγμή ή στο σημείο εγκατάστασης. Μόνο λίγες έχουν αναπτύξει γνήσιες δημιουργικές δυνατότητες, αντιμετωπίζοντας τόσο τις επιχειρηματικές όσο και τις τεχνικές προοπτικές κινδύνου και κατά συνέπεια προσφέροντας συμβουλές με πιο σφαιρικό ολιστικό τρόπο. Αυτή η ολιστική προσέγγιση απαιτεί τη γνώση των επιχειρηματικών κινδύνων και των προτύπων ασφάλειας και τον τρόπο με τον οποίο μπορούν να εφαρμοστούν στην τεχνική αρχιτεκτονική και το επιχειρηματικό περιβάλλον των τελικών χρηστών. Αυτό πρέπει να υποστηρίζεται από τη γνώση και τη μάθηση που αποκτήθηκε από τις πρόσφατες κυβερνητικές επιθέσεις στον κλάδο για τον προσδιορισμό των καλύτερων στρατηγικών πρόληψης για τη διαχείριση του κινδύνου.

2.7.4 Μετριασμός του κίνδυνου σε επίπεδο επιχειρήσεων

Η αγορά του cybersecurity μπορεί να επικεντρωθεί υπερβολικά στον έλεγχο της συμμόρφωσης με την πολιτική και στην πραγματοποίηση δοκιμών αδυναμίας όταν ο βαθμός επιχειρηματικών κινδύνων απαιτεί μια πιο ολιστική αξιολόγηση κινδύνου σε ολόκληρη την περιουσία της και μια ευέλικτη αρχιτεκτονική ασφάλειας που θα αναπτυχθεί στην άμυνα, σε συνεχή βάση.

Ορισμένες εταιρείες πραγματοποίησαν ανεξάρτητους ελέγχους, οι οποίοι επιβεβαιώνουν ότι έχουν πλήρως συμμορφωθεί με τα πρότυπα συμμόρφωσης με την ασφάλεια. Μπορεί ακόμη και να έχουν επανασχεδιαστεί ή να αναβαθμιστεί το δίκτυο πληροφορικής τους για να καταστήσουν δυσκολότερη την εμφάνιση επιθέσεων στον κυβερνοχώρο. Ωστόσο, δεν είναι ασυνήθιστο να διαπιστώσουμε ότι λίγους μήνες αργότερα έχουν υποβληθεί σε cyberattack. Για να είναι ασφαλής στον κυβερνοχώρο απαιτεί την επίτευξη ενός κινούμενου στόχου: η αξιολόγηση και ο μετριασμός των επιθέσεων στον κυβερνοχώρο απαιτούν τη συνεχή και έτσι η προληπτική διαχείριση του κινδύνου να αποτελεί μέρος της στρατηγικής ασφάλειας.

Υποστηρίζουμε ότι οι οργανισμοί δεν θα πρέπει να κατασκευάζουν ένα κάστρο χωρίς εσωτερική προστασία μέσα στα τείχη του, αλλά θα πρέπει να οικοδομήσουν σύμφωνα με το μοντέλο του αεροδρομίου, δηλαδή με πολλαπλά επίπεδα ασφάλειας σε κάθε στάδιο ανάπτυξης, που παρακολουθούν και προσαρμόζονται στις απειλές, όπως απαιτείται. Επιβάλλεται το να αναζητήσουν εξειδικευμένη επαγγελματική υποστήριξη για να εξασφαλίσουν ότι οι λαμβάνονται υπόψιν οι αρχές της ασφαλείας κατά τον σχεδιασμό(security by design) και υιοθετούνται σε όλη την επιχείρηση και διαπερνούν όλες τις επιχειρηματικές διαδικασίες, προϊόντα και υπηρεσίες. Ο στόχος αυτής της προσέγγισης είναι να αναπτυχθεί προληπτικά η ασφάλεια στον σχεδιασμό των υπηρεσιών αντί να προστεθούν επίπεδα ασφάλειας σε μεταγενέστερο στάδιο.

2.7.5 Προσέγγιση της διαδικασίας της ασφάλειας κατά τον σχεδιασμό (Security by Design)

Για να αντιμετωπίσει την πρόκληση της ασφάλειας από το σχεδιασμό (security du design), ο υπεύθυνος ασφάλειας πληροφοριών (Chief Information Security Officer CISO) θα πρέπει να οργανώσει την ομάδα του ώστε να παρέχει εξειδικευμένη υποστήριξη σε όλα τα έργα και δραστηριότητες ανάπτυξης προϊόντων. Στόχος τους θα πρέπει να είναι η δημιουργία υπηρεσιών ασφαλείας και η αύξηση των ικανοτήτων ασφαλείας των διαχειριστών έργων, των προγραμματιστών και των αρχιτεκτόνων:

- Το πρώτο βήμα θα πρέπει να είναι να εξασφαλιστεί ότι οποιαδήποτε διαδικασία διαχείρισης έργου περιλαμβάνει μια αρχική "αξιολόγηση της ασφάλειας των πληροφοριών για να προσδιοριστεί εάν το έργο εμπλέκει ορισμένους τομείς κρίσιμης σημασίας για την ασφάλεια. Για παράδειγμα, το έργο απαιτεί τη χρήση προσωπικών δεδομένων, πληροφοριών πληρωμής, εμπιστευτικών δεδομένων ή άμεσης σύνδεσης στο Διαδίκτυο; Κάθε καταφατική απάντηση θα αυξήσει το επίπεδο προσοχής που απαιτείται από το έργο. Τα έργα που απαιτούν υψηλό επίπεδο εστίασης θα επωφελούνται συχνά από την συμπερίληψη ενός εμπειρογνώμονα ασφάλειας στην ομάδα του έργου.

- Έπειτα για να διευκολυνθεί η ενσωμάτωση της ασφάλειας στο έργο, ο υπεύθυνος ασφάλειας πληροφοριών, θα πρέπει επίσης να εξετάσει το ενδεχόμενο δημιουργίας βασικών προϊόντων ασφαλείας. Δυνατότητες όπως η

κρυπτογράφηση τις βάσης δεδομένων ή ο ισχυρός έλεγχος ταυτότητας. Η ικανότητα τυποποίησης των υπηρεσιών ασφαλείας αποτελεί βασικό στοιχείο για να εξασφαλιστεί ότι η ασφάλεια θα ενσωματωθεί πραγματικά όλα τα έργα.

- Τέλος, για την ενίσχυση η ασφάλεια από προεπιλογή (security by default SbD), απαιτεί την κατάρτιση των προγραμματιστών. Την σήμερον ημέρα ακόμα και επαγγελματίες - μέλη της ομάδας έργων έχουν περιορισμένη επίγνωση των απειλών ασφάλειας, κάτι που έχει ως αποτέλεσμα οι εφαρμογές να κατασκευάζονται χωρίς να έχουν ληφθεί μέτρα για ενσωματωμένη ασφάλεια. Έτσι λοιπόν λίγο πριν τεθεί σε παραγωγή, οι έλεγχοι δείχνουν πολυάριθμα ελαττώματα ασφαλείας, προσθέτοντας καθυστέρηση στο έργο και αύξηση του.

Η πλήρης εφαρμογή μιας παγκόσμιας, ολοκληρωμένης "ασφαλούς από το σχεδιασμό" (secure by design) κουλτούρας σε έναν μεγάλο οργανισμό είναι μια μακροπρόθεσμη στρατηγική δραστηριότητα και μπορεί να διαρκέσει από 3 έως 5 χρόνια. Ωστόσο, τα πρώτα κιόλας οφέλη μπορούν να επιτευχθούν σε περίπου 3 μήνες με την υποστήριξη ενός ειδικού στο τομέα της ασφάλειας στον κυβερνοχώρο .Κάτι το οποίο θα προσφέρει σημαντική εξοικονόμηση κόστους, καθώς το κόστος που σχετίζεται με την ασφάλεια των πληροφοριών μπορεί να κυμανθεί από 2% έως 20% του συνολικού κόστους του έργου.

2.8 Η ασφάλεια κατά τον σχεδιασμό προλαμβάνει συχνά λάθη από τα αρχικά ακόμα στάδια ανάπτυξης (Security by design prevents errors from an early stage)

Εάν ένας προγραμματιστής περιλαμβάνει χαρακτηριστικά ασφαλείας ως κριτήριο σχεδιασμού, τα σφάλματα του συστήματος μπορούν να αποφευχθούν από την αρχή. "Οι μηχανικοί λογισμικού εργάζονται παλαιότερα με εντελώς διαφορετικό τρόπο, καθώς εργάζονται μέσω προδιαγραφών. Εάν η ασφάλεια δεν είναι ένα από τα κριτήρια σχεδιασμού, δεν το αντιμετωπίζουν ", εξηγεί ο Tschersich. Στην περίπτωση αυτή, οι προγραμματιστές μπορούν μόνο να ελπίζουν ότι όλα πάνε καλά. "Αλλά η εμπειρία συνήθως δείχνει ότι το αντίθετο είναι αλήθεια."

Στην ιδανική περίπτωση, το ζήτημα της ασφάλειας είναι ήδη ένα σταθερό μέρος της φάσης της ιδέας: μπορεί η ιδέα να εφαρμοστεί ακόμη και στην πράξη όσον αφορά τις πτυχές ασφαλείας; Τι είδους λειτουργικές απαιτήσεις ασφαλείας χρειάζονται; Ως αποτέλεσμα, η πτυχή της ασφάλειας ενσωματώνεται στη δημιουργία του πρωτοτύπου - και διατηρείται σε όλα τα στάδια της παραγωγής. "Όταν το τελικό προϊόν υποβληθεί σε δοκιμές αποδοχής, μετατοπίζεται χωρίς περαιτέρω βήματα στο βέλτιστο σενάριο", λέει ο Tschersich.

Ο εμπειρογνώμονας ασφάλειας και ειδήμων Tschersich συμβουλεύει τις εταιρείες να εμείνουν σε επτά βασικούς κανόνες ώστε να μειώνετε την περιοχή επίθεσης κατά περισσότερο από 95 τοις εκατό."

Διατηρήστε μικρή επιφάνεια επίθεσης: Η επιφάνεια προσβολής μπορεί να ελαχιστοποιηθεί απενεργοποιώντας τα περιττά προγράμματα η εκείνα που δεν χρησιμοποιούνται. Απενεργοποιημένα, μη απαραίτητα προγράμματα λογισμικού και εξαρτήματα σε οποιαδήποτε συστήματα πληροφορικής τα κάνει αδύνατα ώστε να τους επιτεθούν.

Πιστοποιήστε κατάλληλα: Τα εμπιστευτικά συστήματα πληροφοριών και πληροφοριών πρέπει να είναι προσβάσιμα μόνο από τα άτομα με τα οποία θέλετε να επικοινωνήσετε. "Αν διασφαλίσετε ότι μόνο χρήστες ή συστήματα που έχουν πιστοποιηθεί μπορούν να έχουν πρόσβαση σε κάτι, αποκλείετε όλα τα μη αναγνωρισμένα άτομα με υψηλό βαθμό πιθανότητας.

Ελέγξτε τις εισόδους: Κάθε είσοδος θα πρέπει να ελέγχεται για τους επιτρεπόμενους χαρακτήρες - ιδιαίτερα τους ειδικούς χαρακτήρες - και για το μέγιστο επιτρεπόμενο μήκος. Ένα παράδειγμα: όταν ένας χρήστης παραγγείλει κάτι σε μια δικτυακή πύλη, απαιτούνται μόνο αριθμοί και ενδεχομένως περίοδοι στο πεδίο για την ημερομηνία γέννησης. "Μια επίθεση μπορεί να αποφευχθεί αγνοώντας τα πάντα εκτός από τους αριθμούς και τις περιόδους.

Ξεχωριστά συστήματα: Μετά από μια επιτυχημένη επίθεση σε ένα σύστημα, οι χάκερ προσπαθούν συχνά να αποκτήσουν σταδιακά πρόσβαση σε άλλα συστήματα από εκεί. Επομένως, τα συστήματα πρέπει να διαχωρίζονται μεταξύ τους. "Εάν ο διακομιστής ιστού, για παράδειγμα, έχει πειραχτεί, ο εισβολέας απέχει πολύ από το να μπαίνει στη βάση δεδομένων.

Κρυπτογράφηση εμπιστευτικών δεδομένων: Η πρόσβαση στα συστήματα αποθήκευσης, επεξεργασίας και μεταφοράς δεδομένων δεν βρίσκεται συνήθως στα χέρια της ίδιας της εταιρείας, όπως συμβαίνει στην περίπτωση που χρησιμοποιούνται υπηρεσίες cloud. Αυτό σημαίνει ότι είναι ακόμη πιο σημαντικό να προστατεύονται εμπιστευτικές πληροφορίες.

Ενημερώστε τακτικά: Τα συστήματα δεν προστατεύονται εάν η εκδοχή τους δεν είναι πάντοτε ενημερωμένη. Αυτός είναι ο μόνος τρόπος για να αποτρέψουμε τους επιτιθέμενους από την εκμετάλλευση γνωστών κενών ασφαλείας. Οι νέες εκδόσεις

έρχονται συχνά με μηχανισμούς για την προσάρτηση των κενών ασφαλείας που έχουν εντοπιστεί σε προηγούμενες εκδόσεις.

Ελέγξτε την ασφάλεια συνεχώς: Η κατάσταση ασφαλείας των συστημάτων και η ευπάθειά τους στις επιθέσεις πρέπει να επανεξετάζονται διαρκώς μέσω ελέγχων ασφαλείας. "Τα συστήματα είναι ζωντανά και συνεχίζουν να εξελίσσονται. Επιπλέον, ανακαλύπτονται όλο και περισσότερες νέες αδυναμίες

Η ασφάλεια από το σχεδιασμό μειώνει τον κίνδυνο ευθύνης, Σύμφωνα με τον διάσημο εμπειρογνώμονα ασφαλείας, μια εταιρεία μειώνει επίσης τον κίνδυνο ευθύνης της χρησιμοποιώντας ασφάλεια από το σχεδιασμό. "Στο μέλλον, οι κατασκευαστές μπορούν να αναμένουν να θεωρηθούν υπεύθυνοι εάν δεν έχουν δημιουργήσει από την αρχή λογικές εγγυήσεις." Εάν μια εταιρεία δεν μπορεί να αποδείξει ότι έχει εξασφαλίσει επαρκή ασφάλεια, σύντομα θα έχει "ένα σημαντικό οικονομικό πρόβλημα

3. Ιδιωτικότητα κατά των σχεδιασμό (Privacy By Design)

3.1 Τι είναι η Ιδιωτικότητα κατά των σχεδιασμό(What Privacy by design really is?)

Η προστασία της ιδιωτικής ζωής από το σχεδιασμό αποτελεί μια προσέγγιση για την ομαλή ενσωμάτωση της προστασίας σε κάθε σκέλος του σχεδιασμού και της ανάπτυξης ενός προϊόντος ή μιας υπηρεσίας. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) αγκαλιάζει τις αρχές της προστασίας της ιδιωτικής ζωής από το σχεδιασμό και τις θεωρεί ως τις σημαντικότερες πτυχές της προστασίας δεδομένων

Η προστασία προσωπικών δεδομένων από το σχεδιασμό (PbD) δεν είναι μια νέα έννοια στην προστασία δεδομένων. Είναι η φιλοσοφία που προτάθηκε και αναπτύχθηκε από την κυρία Ann Cavoukian, την Επίτροπο Πληροφοριών και Προστασίας Προσωπικών Δεδομένων του Οντάριο στη δεκαετία του 90 του περασμένου αιώνα, και εν συνέχεια υιοθετήθηκε σταδιακά από επαγγελματίες και οργανισμούς στον τομέα της ιδιωτικής ζωής σε ολόκληρο τον κόσμο

Το Privacy by Design χαρακτηρίζεται ως μια προσέγγιση στον σχεδιασμό τεχνολογίας κατά τον οποίο ενσωματώνουμε μέτρα ενίσχυσης της ιδιωτικής ζωής στην τεχνολογία, στο σημείο του σχεδιασμού και της παραγωγής. Έτσι έχουμε ένα τελικό προϊόν η μια υπηρεσία όπου έχουμε εξ αρχής ισχυρές προεπιλεγμένες ρυθμίσεις απορρήτου.

Η ασφάλεια των πληροφοριών επιδιώκει να επιτρέψει και να προστατεύσει τις δραστηριότητες και τα περιουσιακά στοιχεία τόσο των ανθρώπων όσο και των επιχειρήσεων. Σύμφωνα με τον NIST ως Βασικών Όρων Ασφάλειας Πληροφοριών ορίζει την "Ασφάλεια Πληροφοριών" ως εξής: "Η προστασία των πληροφοριών και των συστημάτων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή, προκειμένου να παρέχονται:

i. **Integrity (ακεραιότητα)**

Την προστασία από ακατάλληλη τροποποίηση των πληροφοριών ή καταστροφή, και περιλαμβάνει τη διασφάλιση της μη αναδημοσίευσης πληροφοριών και αυθεντικότητα;

ii. **Confidentiality (εμπιστευτικότητα)**

δηλαδή την διατήρηση των επιτρεπόμενων περιορισμών την πρόσβαση και τη γνωστοποίηση, συμπεριλαμβανομένων μέσων για την προστασία της ιδιωτικής ζωής και ιδιόκτητων πληροφοριών.

iii. **Availability (διαθεσιμότητα)**

Δηλαδή την εξασφάλιση έγκαιρης και αξιόπιστης πρόσβασης και χρήσης των πληροφοριών.

3.2 Οι επτά θεμελιώδεις αρχές της προστασίας της ιδιωτικής ζωής (Principles of Privacy by Design)

Οι επτά θεμελιώδεις αρχές προστασίας της ιδιωτικής ζωής (PbD) από το σχεδιασμό ακόμα, αντί να προσθέτουν την ασφάλεια των δεδομένων στο τέλος ενός έργου ή απλώς να το αγνοούν, οι οργανισμοί που υιοθετούν μια προσέγγιση απορρήτου από το σχεδιασμό θα εξετάσουν την αρχή της προστασίας της ιδιωτικής ζωής και των δεδομένων από την αρχή κατά την κατασκευή νέων συστημάτων, τα δεδομένα με τρίτους ή τη χρήση δεδομένων για νέους σκοπούς.

Οι οργανισμοί που πράττουν και έχουν έναν τέτοιο τρόπο σκέψης μόνο να κερδίσουν έχουν. Η εμπιστοσύνη, η φήμη του εμπορικού σήματος και τα εμπορικά οφέλη θα αυξάνονται ολοένα και σε μεγαλύτερο βαθμό σύμφωνα με αυτά που παρέχονται από μια καλά σχεδιασμένη Επιχειρησιακή Αρχιτεκτονική ασφάλειας (Enterprise Security Architecture, ESA) όπως είναι τα εξής:

i. Μειωμένος κίνδυνος σε περίπτωση μη ικανοποίησης δεδομένων συμμόρφωση προς την προστασία.

ii. Αυξημένη συνειδητοποίηση της ιδιωτικής ζωής και προστασία δεδομένων εντός του οργανισμού.

iii. Έγκαιρη αναγνώριση σε πιθανά ρίσκα απορρήτου μειώνοντας έτσι το χρόνο και τα χρήματα τα οποία θα πρέπει να δαπανηθούν ώστε να αποκατασταθεί το ζήτημα

Οι θεμελιώδεις αρχές του Privacy by Design ,οι οποίες έχουν μεταφερθεί σε μεγάλο βαθμό σε όλες τις σχετικές νομοθεσίες, επινοήθηκαν ως ένας τρόπος για να βοηθηθεί η προστασία της ιδιωτικής ζωής ακόμη και στη σύγχρονη οικονομία της γνώσης, όπου οι τεράστιες ροές δεδομένων είναι ο κανόνας. Ας ρίξουμε μια πιο εκτενέστερή ματιά στις επτά βασικές αρχές του Privacy by Design (PbD) και του πώς σχετίζονται με το γενικό κανονισμό προστασίας δεδομένων GDPR:

3.2 .1 Proactive not reactive

Η βιομηχανική προσέγγιση της ιδιωτικής ζωής πρέπει να είναι προληπτική. Οι οργανισμοί δεν θα πρέπει να περιμένουν έως ότου η παραβίαση της ιδιωτικής ζωής συμβεί ώστε να προσπαθήσει να μετριάσει τους κινδύνους ιδιωτικότητας ή ασφάλειας. Η αποφυγή ή η ελαχιστοποίηση της συλλογής προσωπικών μέσω Privacy Enhancing Technology PETs είναι ο πιο προφανής, αλλά όχι εύκολος και όχι πάντα δυνατός, τρόπος ελαχιστοποίησης των πιθανών παραβιάσεων της ιδιωτικής ζωής. Βεβαίως, η ελαχιστοποίηση των δεδομένων είναι επίσης η αρχή της ιδιωτικής ζωής για την οποία απαιτείται μεγάλη πρόοδος από τους οργανισμούς.

Ως παράδειγμα για το σημερινό κενό στο θέμα αυτό, το έργο της **Mobilitics**[1] που προκύπτει από τη συνεργασία της Inria και της CNIL, της γαλλικής Αρχής Προστασίας Δεδομένων, κατέδειξε ότι το 31% των εφαρμογών iPhone χρησιμοποιεί γεωγραφικές πληροφορίες (τις περισσότερες φορές χωρίς καμία σχέση με ο σκοπός της εφαρμογής), το 50% χρησιμοποιεί ένα μοναδικό αναγνωριστικό του κινητού τηλεφώνου (UDID) και πολλοί το στέλνουν με σαφήνεια (όλα αυτά χωρίς δικαιολογημένη ανάγκη).

Η μελέτη δείχνει επίσης ότι πολλοί ενδιαφερόμενοι (οι περισσότεροι εταιρείες παρακολούθησης που εργάζονται σε συνεργασία με διαμεσολαβητές διαφήμισης) που είναι εντελώς άγνωστοι από τους χρήστες λαμβάνουν αυτές τις πληροφορίες. Μια άλλη μελέτη δείχνει ότι το 43% των εφαρμογών Android απαιτούν υπερβολικά δικαιώματα, επιτρέποντας τη συλλογή προσωπικών δεδομένων (σύμφωνα με μια μελέτη που διεξήχθη από νότιο κορεατικό προμηθευτή antivirus AhnLab) και δείχνοντας την έλλειψη ανησυχιών που έχουν οι οργανισμοί όταν σέβονται το απόρρητο του χρήστη. Αυτές οι μελέτες δείχνουν σαφώς ότι μία από τις εξηγήσεις για αυτές τις παραβιάσεις της ιδιωτικής ζωής είναι η αναζήτηση οικονομικών οφελών που βασίζονται στην εκμετάλλευση προσωπικών δεδομένων. Αυτό το κενό συνδέεται συνεπώς με την

1 https://www.cnil.fr/fr/cybersecurite

έλλειψη (ή αδυναμία) αποτελεσματικών κυρώσεων (ή συμμετρικά, την έλλειψη κινήτρου για τη συμμόρφωση με τις αρχές της προστασίας της ιδιωτικής ζωής)

Εκτός από την προσέγγιση ελαχιστοποίησης, υπάρχουν πολλοί προληπτικοί έλεγχοι προστασίας της ιδιωτικής ζωής, οι οποίοι είναι καθοριστικοί για την επιτυχία στην προστασία των δεδομένων, οι οποίοι θα μπορούσαν στην πραγματικότητα να χρησιμοποιηθούν σήμερα στα περισσότερα συστήματα της βιομηχανίας, αλλά δεν είναι ακόμη διαδεδομένοι:

- Ανάλυση κινδύνου ιδιωτικού απορρήτου και εκτιμήσεις επιπτώσεων στην ιδιωτική ζωή.

- Αυτοματοποιημένες πολιτικές και μέτρα ασφαλείας για την πρόληψη και ανίχνευση των ελεγκτών δεδομένων και του επεξεργαστή δεδομένων για πιθανή κατάχρηση προσωπικών πληροφοριακών περιουσιακών στοιχείων.

- Καθιέρωση μετρήσεων απορρήτου και τακτική επανεξέταση και δοκιμή λύσεων προστασίας δεδομένων.

- Κατάλληλη εκπαίδευση του συνόλου του προσωπικού σε θέματα προστασίας της ιδιωτικής ζωής

Η ενσωμάτωση της ιδιωτικής ζωής στο σχεδιασμό δεν είναι απλό έργο και η βιομηχανία ακολουθεί ορισμένες προσεγγίσεις για την αποτελεσματική επίτευξή της. Μια κυρίαρχη πρακτική είναι η παρακολούθηση των μεθοδολογιών διαχείρισης κινδύνων, προκειμένου να ανιχνευθούν πιθανά ζητήματα προστασίας της ιδιωτικής ζωής και να αντιμετωπιστούν τα προβλήματα αυτά κατά τα πρώτα στάδια, με αποτέλεσμα να αποφευχθούν μεγαλύτερα έξοδα αργότερα. Μια έρευνα της PWC ανέφερε ότι λιγότερο από το 40% των ευρωπαϊκών οργανισμών διεξάγει "εκτιμήσεις κινδύνου (internal και external) για την προστασία της ιδιωτικής ζωής, την ασφάλεια, την εμπιστευτικότητα και την ακεραιότητα ηλεκτρονικών και εγγράφων που περιέχουν προσωπικές πληροφορίες".

Όταν πραγματοποιείται αξιολόγηση κινδύνου, το επόμενο βήμα είναι να ληφθούν υπόψη τα αποτελέσματά της για να διασφαλιστεί ότι όλοι οι κίνδυνοι για την ιδιωτική ζωή αντιμετωπίζονται ή μπορεί να αποδειχθεί ότι οι υπολειπόμενοι κίνδυνοι είναι αρκετά χαμηλοί.

Η αντιμετώπιση αυτών των προβλημάτων ιδιωτικού απορρήτου μπορεί να συνεπάγεται την ανάπτυξη τεχνικών και οργανωτικών μέτρων, τον ορισμό αρχιτεκτονικής προστασίας της ιδιωτικής ζωής (π.χ. αποφυγή συλλογής δεδομένων προσωπικού χαρακτήρα σε κεντρικό εξυπηρετητή), ενσωμάτωση με Privacy Enhancing Technology PETs και τροποποίηση του σχεδιασμού ή των χαρακτηριστικών ενός συστήματος. Όλα

αυτά τα μέτρα έχουν τους περιορισμούς τους και μερικές φορές θεωρούνται υπερβολικά δαπανηρά ή αποδιοργανωτικά.

Ορισμένα μέτρα (συμπεριλαμβανομένων των οργανωτικών μέτρων) δεν είναι μακριά από το να τις υιοθετήσουν οι περισσότερες βιομηχανίες. Οι εύλογοι λόγοι για τη χαμηλή υιοθέτησή τους είναι η έλλειψη ενημέρωσης, η έλλειψη εκπαιδευμένου προσωπικού ή η έλλειψη υποκειμένου των δεδομένων για το απόρρητο. Το αποτέλεσμα μιας έρευνας PWC μεταξύ παγκόσμιων οργανώσεων αποκάλυψε ότι μόνο το 55% των συμμετεχόντων στην έρευνα έχουν αναπτύξει ένα σύστημα πρόληψης εισβολής και πάνω από το 55% έχουν προνομιακούς λογαριασμούς πρόσβασης χρηστών, άλλα στατιστικά στοιχεία από την ίδια έρευνα υποδηλώνουν την έλλειψη προάσπισης της ιδιωτικής ζωής εντός των οργανισμών:

- Μόνο το 51% των οργανισμών παρακολουθεί τη συμμόρφωση των χρηστών με τις πολιτικές ασφάλειας.

- Μόνο το 51% των οργανώσεων διαθέτει πρόγραμμα κατάρτισης και ευαισθητοποίησης για την ασφάλεια των εργαζομένων.

- Λιγότερο από το 50% των ευρωπαϊκών οργανισμών διαθέτουν έναν "ακριβή κατάλογο όπου συλλέγονται, διαβιβάζονται και αποθηκεύονται προσωπικά δεδομένα για τους εργαζομένους και τους πελάτες"

- Σύμφωνα με έρευνα της Gartner, λιγότερο από το 40% των οργανισμών από τις Η.Π.Α., τον Καναδά, το Ηνωμένο Βασίλειο και τη Γερμανία διεξάγουν κάθε χρόνο έλεγχο προσωπικού απορρήτου.

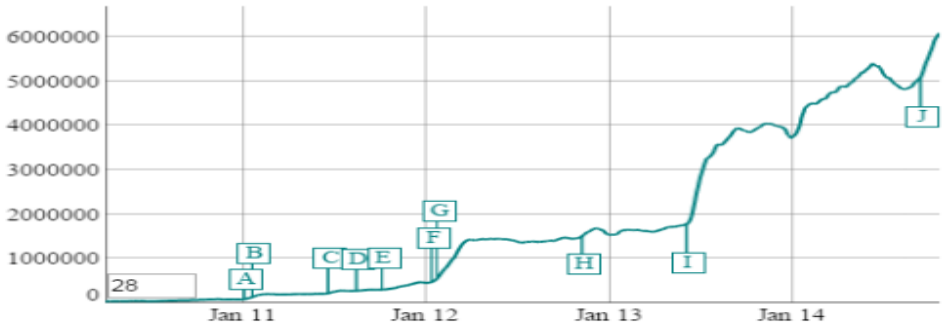
Ορισμένοι από τους ελέγχους απορρήτου που προτείνονται για να ακολουθήσουν αυτή την αρχή θεμελίωσης του PbD (π.χ. σύστημα ανίχνευσης και πρόληψης, έλεγχοι απορρήτου, διαχείριση κινδύνου, ελαχιστοποίηση δεδομένων) υποστηρίζονται από εμπορικά εργαλεία ή εργαλεία ανοικτού κώδικα, π.χ. υπάρχουν πολλά συστήματα SIEM στην αγορά και ακόμη και λύσεις opensource όπως το **OSSIM**[2]. Αυτές οι λύσεις (οι οποίες είναι συνήθως ειδικές για την ασφάλεια) είναι ευρέως διαθέσιμες και δεν επιβάλλουν πολύ περίπλοκες τεχνικές απαιτήσεις. Ωστόσο, οι λύσεις που σχετίζονται με την ιδιωτική ζωή δεν είναι τόσο διαδεδομένες, πολλές από τις οποίες είναι ακόμη πειραματικές (π.χ. βιβλιοθήκες κρυπτογράφησης homomorphy[3]) και άλλες επικεντρώνονται ως υπηρεσίες για τον τελικό χρήστη (π.χ. υπηρεσίες Passwordless[4] επιτρέποντας έτσι την ελαχιστοποίηση της συλλογής δεδομένων, η ανάγκη συλλογής κωδικών πρόσβασης, η οποία επιτρέπει στους χρήστες και τις υπηρεσίες να χρησιμοποιούν ανώνυμα συστήματα διαπιστευτηρίων, Silent Circle[5] ή DataLocker[6]) και όχι σε δομικά στοιχεία που θα ήταν εύκολο να ενσωματωθούν σε μια λύση.

2 https://www.alienvault.com/open-threat-exchange/projects
3 https://github.com/shaih/HElib
4 https://passwordless.net/
5 https://silentcircle.com/technology
6 http://datalocker.com/

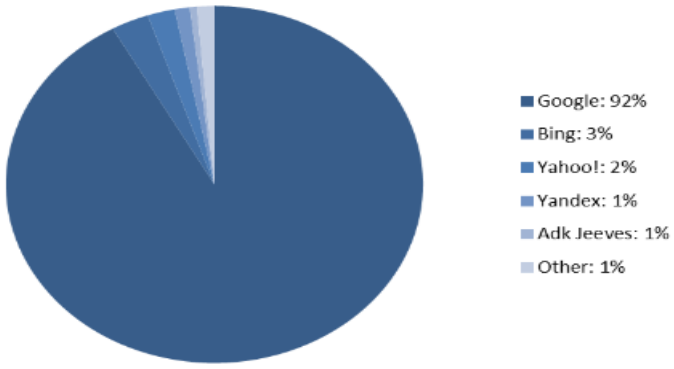
Ως αποτέλεσμα, δεν υπάρχουν πολλά ευρέως διαθέσιμα εργαλεία υποστήριξης για τους υπεύθυνους επεξεργασίας δεδομένων και επεξεργαστές, οι οποίοι είναι υπεύθυνοι για τη συλλογή, την αποθήκευση και την επεξεργασία τέτοιων δεδομένων. Οι περιοδικές αξιολογήσεις ή οι έλεγχοι είναι οργανωτικά μέσα που δεν έχουν τεχνικούς περιορισμούς και συνίστανται, για παράδειγμα, στην περιοδική επανεξέταση ή επαναξιολόγηση των ελέγχων απορρήτου, των διαδικασιών διαχείρισης κινδύνου ή των ίδιων των κινδύνων. Ενώ τα μέτρα αυτά είναι ιδιαίτερα αποτελεσματικά, τα έξοδα που απορρέουν από αυτές τις δραστηριότητες είναι περιορισμένα.

Δεδομένου ότι η βιομηχανία είναι ιδιαίτερα προσανατολισμένη στα οικονομικά οφέλη, φαίνεται ότι ο κύριος λόγος για την μη υιοθέτηση αυτών των ελέγχων απορρήτου είναι η εσφαλμένη αντίληψη ότι τα οφέλη από την υιοθέτηση αυτών των μέτρων δεν αντισταθμίζουν σαφώς το κόστος.

Το κόστος αυτών των μέτρων δεν φαίνεται υπερβολικά δαπανηρό, φαίνεται ότι υπάρχει το συμπέρασμα ότι το όφελος από την ενσωμάτωση τους δεν είναι υπερβολικά υψηλό, πιθανώς λόγω της έλλειψης κινήτρων από το νομικό πλαίσιο (π.χ. χαμηλά πρόστιμα) ή της πίεσης από την κοινωνία. Για παράδειγμα, ενώ ο αριθμός των άμεσων ερωτημάτων της πιο χρησιμοποιημένης μηχανής αναζήτησης για την προστασία της ιδιωτικής ζωής (DuckDuckGo) σχεδόν διπλασιάστηκε μετά τις αποκαλύψεις Snowden (βλέπε σημάδι 'I' στο παρακάτω σχήμα που αντιστοιχεί στην ημερομηνία αποκαλύψεων Snowden), το μερίδιο αγοράς τέτοιων εργαλείων παραμένει αμελητέα στην Ευρώπη. Η υψηλότερη προσέλκυση σε αυτού του είδους τις υπηρεσίες έχει τη δυνατότητα να ασκεί πίεση στους παρόχους υπηρεσιών για να αναπτύξουν περισσότερα χαρακτηριστικά φιλικά προς την ιδιωτικότητα.



DuckDuckGo απευθείας ερωτήματα ανά ημέρα



Κορυφαίες μηχανές αναζήτησης στην Ευρώπη από Απρίλιο έως Σεπτέμβριο του 2014((Source StatCounter GlobalStats)[7]

Η προστασία της ιδιωτικής ζωής από το σχεδιασμό προσεγγίζει με προληπτικό τρόπο τα ζητήματα που αφορούν τους κινδύνους ιδιωτικής ζωής. Τα ζητήματα πρέπει να αποτρέπονται πριν από την εμφάνισή τους και πρέπει να ληφθούν μέτρα για τον μετριασμό των δυνητικών κινδύνων, ακόμη και πριν καταστούν εμφανή. Οι κακές πρακτικές ασφάλειας και προστασίας της ιδιωτικής ζωής πρέπει επίσης να αναγνωρίζονται και να βελτιώνονται νωρίς, προτού να υποστούν οποιαδήποτε βλάβη.

Αυτό απαιτείται και ως δέσμευση ώστε να εφαρμόζει με συνέπεια τα πρότυπα προστασίας της ιδιωτικής ζωής από τον GDPR. Αυτό καλύπτεται από την απαίτηση να διεξάγονται αξιολογήσεις επιπτώσεων για την προστασία των δεδομένων πριν από την έναρξη των εργασιών επεξεργασίας. Οι αρμοδιότητες των υπεύθυνων επεξεργασίας δεδομένων (data controller) και ενός εξωτερικού τρίτου συνεργάτη (data processor) είναι επίσης σαφώς καταγεγραμμένες και πρέπει να τηρούνται. Αυτό απαιτεί μια σθεναρή δέσμευση για σωστή εφαρμογή.

3.2.2 Privacy as the default setting

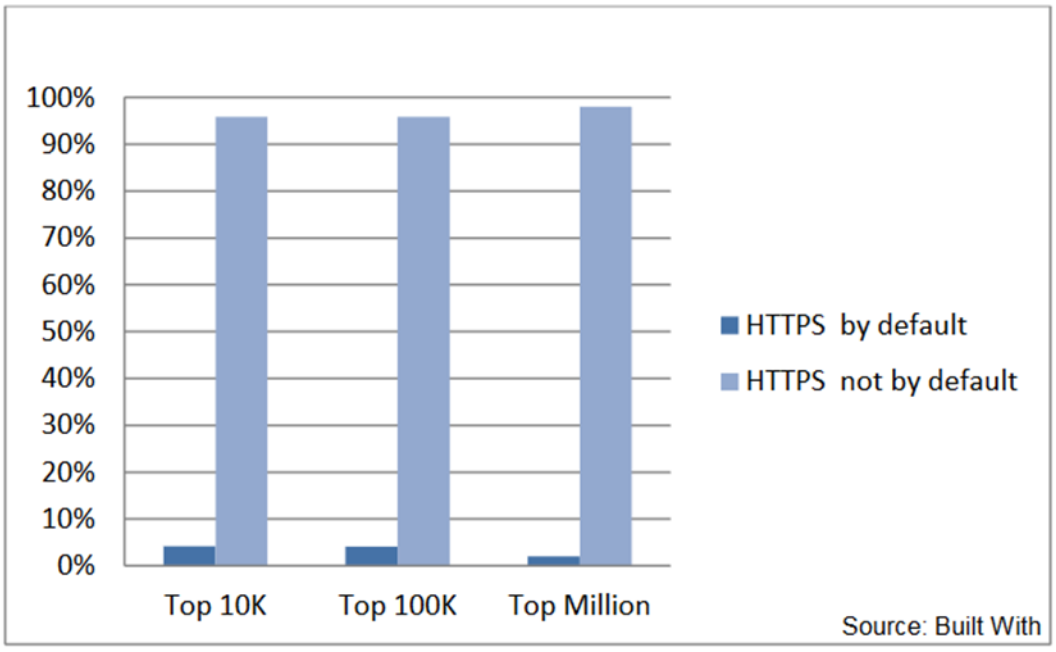
Επί του παρόντος, η βιομηχανία στον τομέα των τεχνολογιών πληροφόρησης και επικοινωνιών (ICT) αναμένει πολλά από τους πελάτες της όσον αφορά τις τεχνικές γνώσεις. Περιμένει δηλαδή να ξέρει τι είναι τα cookies και πώς να τα διαγράψουν, να διαχειριστούν τις ρυθμίσεις απορρήτου, να κατανοήσουν τις μακροχρόνιες πολιτικές απορρήτου στο διαδίκτυο, να γνωρίζουν τους κινδύνους ιδιωτικής ζωής όταν χρησιμοποιούν δημόσια δίκτυα Wi-Fi. Η πραγματικότητα όμως είναι εντελώς σε αντίθετη κατεύθυνση. Ένας μέσος χρήστης δεν γνωρίζει τίποτα για αυτά τα θέματα πόσο μάλλον να τροποποιούν τις ρυθμίσεις απορρήτου.

7 http://gs.statcounter.com/#search_engine-eu-monthly-201404-201409-bar

Οι οργανισμοί κατευθύνουν τις προεπιλεγμένες ρυθμίσεις των προϊόντων τους σύμφωνα με τα δικά τους επιχειρηματικά συμφέροντα, τα οποία και σαφώς δεν είναι απαραίτητα συμβατά με τις ανησυχίες των χρηστών όσον αφορά την ιδιωτική τους ζωή. Για παράδειγμα, εντός της Microsoft, η διαδικτυακή διαφήμιση ήταν σε θέση να αναγκάσει την ομάδα του Internet Explorer να θέσει την "InPrivate Filtering" ως απενεργοποιημένη από προεπιλογή, όταν αναμενόταν να οριστεί από προεπιλογή.

Θα ήταν αρκετά εύκολο για την Google ή τη Microsoft να τροποποιήσουν τα προγράμματα περιήγησης ιστού για να αποκλείσουν όλα τα διαφημιστικά δίκτυα, αλλά αυτό θα ήταν αντίθετο προς τα δικά τους συμφέροντα ως διαφημιστές στο διαδίκτυο. Το ίδιο θα μπορούσε να ειπωθεί για την διάρκεια διατήρησης δεδομένων στις μηχανές αναζήτησης. Από προεπιλογή, το Google αποθηκεύει όλες τις αναζητήσεις που συνδέονται με τους χρήστες της Google χωρίς χρονικό περιορισμό.

Όταν δεν υπάρχει σύγκρουση μεταξύ των ενδιαφερόντων της βιομηχανίας και των προεπιλεγμένων ρυθμίσεων, θα πρέπει να υπάρξει κάποια απορρόφηση από την προεπιλεγμένη ρύθμιση απορρήτου, π.χ. Το Google έχει τώρα το HTTPS από προεπιλογή σε όλες τις εφαρμογές του στο διαδίκτυο, ωστόσο, ένα τόσο εύκολο και οικονομικό μέτρο απέχει πολύ από το να είναι μια κοινή πρακτική. Το παρακάτω σχήμα δείχνει την υιοθέτηση του HTTPS / SSL ανά προεπιλογή (ο ιστότοπος ανακατευθύνει την κυκλοφορία σε μια έκδοση HTTPS / SSL από προεπιλογή) στους κορυφαίους 10.000 100.000 και 1.000.000 ιστότοπους.



Χρήση του HTTPS με βάση την προεπιλογή

Είναι σημαντικό να αναφέρουμε ότι η χρήση του HTTPS δεν διασφαλίζει την ασφάλεια, καθώς εξαρτάται σε μεγάλο βαθμό από το συγκεκριμένο πρωτόκολλο που διέπει την επικοινωνία. Όπως αποκαλύφθηκε από την πρόσφατη δημοσίευση τρωτών σημείων SSL 3.0 όπως POODLE και η Heartbleed, ορισμένες εκδόσεις πρωτοκόλλων ή συγκεκριμένες εφαρμογές των πρωτοκόλλων δεν μπορούν να θεωρηθούν ασφαλείς.

Όταν υπάρχει μια ρύθμιση που μπορεί εύκολα να ενεργοποιηθεί ή να απενεργοποιηθεί από τον χρήστη, ορισμένοι από τους λόγους για τους οποίους οι οργανισμοί αποφεύγουν να χρησιμοποιούν το ιδιωτικό απόρρητο στο έπακρο προστατεύοντας τον χρήστη έχοντας τις ρυθμίσεις ως προεπιλογή είναι:

- Σύγκρουση συμφερόντων (π.χ. επιχειρηματικά συμφέροντα έναντι συμφερόντων απορρήτου του χρήστη). Μεγάλες εταιρείες όπως το Google ή το Facebook έχουν επιχειρηματικό μοντέλο το οποίο βασίζεται στη χρήση των προσωπικών δεδομένων του χρήστη. Privacyfix, ένα εργαλείο AVG το οποίο μπορεί να χρησιμοποιηθεί για την εκτίμηση της αξίας των προσωπικών σας δεδομένων με βάση τον αριθμό των αναζητήσεων στο google, των tweets που κάνετε ή των cookies που έχει αποθηκεύσει ο πλοηγός σας.

- Ο περιορισμός της λειτουργικότητας (π.χ. μη κοινοποίηση της τοποθεσίας χρήστη εμποδίζει ένα σύστημα να του παρουσιάσει πληροφορίες διαφημιστικού είδους με βάση με την τοποθεσία του).

- Απόδοση (π.χ. το Android έχει μια επιλογή κρυπτογράφησης που καταναλώνει CPU και μπαταρία, εκπέμπεται από προεπιλογή).

- Η έλλειψη ευαισθητοποίησης, δηλαδή ενδέχεται οι οργανισμοί να μην γνωρίζουν τις προεπιλεγμένες επιλογές που θα ενισχύσουν την προστασία των προσωπικών δεδομένων του χρήστη ακόμη και τα δικά τους αποκλειστικά δεδομένα (η ελαχιστοποίηση των δεδομένων αποτελεί προστασία όχι μόνο για τα άτομα αλλά και για τους υπεύθυνους επεξεργασίας δεδομένων, διότι οδηγεί σε ελαχιστοποίηση κινδύνου)

Η αρχή της προστασίας της ιδιωτικής ζωής εξ ορισμού ορίζει ότι τα δεδομένα των χρηστών πρέπει να προστατεύονται χωρίς να απαιτείται η εισαγωγή τους. Τα άτομα δεν θα πρέπει να κάνουν τίποτα για να διασφαλίσουν ότι τα δεδομένα τους είναι ασφαλή αλλά θα πρέπει να είναι ασφαλή εξ ορισμού (PbD).

Αυτό καλύπτεται από τα άρθρα 25 και 32 του GDPR, ενώ οι υπεύθυνοι προστασίας δεδομένων (DPO) είναι επιφορτισμένοι με την τήρηση αυτών των κανόνων. Το GDPR περιλαμβάνει επίσης τα τρία βασικά στοιχεία της ιδιωτικής ζωής ως προεπιλογή, όπως:

i. **Purpose specification (Προδιαγραφή στόχου):** όπου τα άτομα θα πρέπει να ενημερώνονται για το ποια δεδομένα θα χρησιμοποιηθούν.

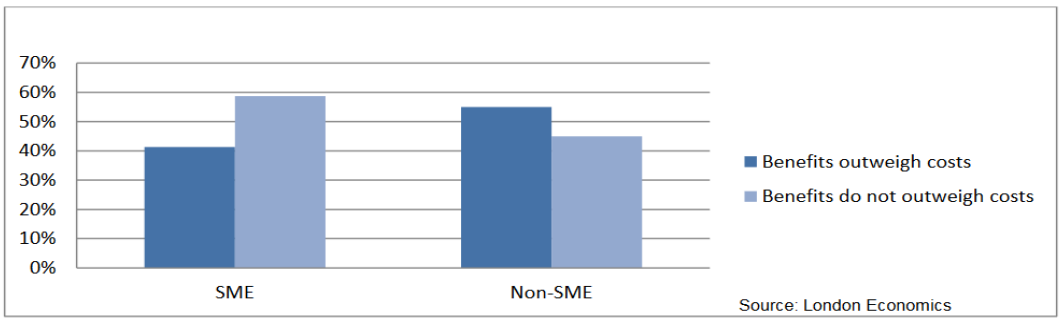
ii. **Collection limitation (Περιορισμός συλλογής):** όπου η συλλογή δεδομένων προσωπικού χαρακτήρα πρέπει να είναι νόμιμη και διαφανής.

iii. Data minimisation (Η ελαχιστοποίηση των δεδομένων): όσο το δυνατόν λιγότερα δεδομένα θα πρέπει να συλλέγονται και μόνο για σκοπούς άμεσης επεξεργασίας.

3.2.3 Privacy embedded into design

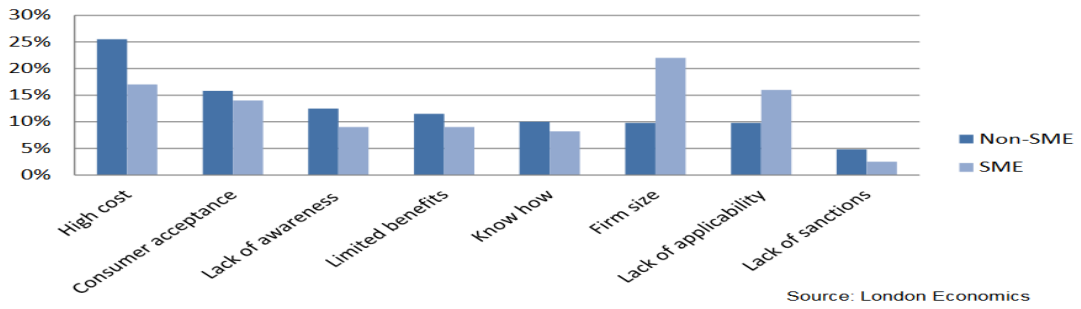
Η ουσία αυτής της αρχής είναι να εξετάσουμε τις πτυχές της ιδιωτικής ζωής του συστήματος από την έναρξή του και να μην τις βάλουμε ως πρόσθετο, την τελευταία στιγμή. Με αυτό τον τρόπο η ιδιωτικότητα αποτελεί ουσιαστικό μέρος του συστήματος. Σύμφωνα με μια έρευνα της Gartner, περισσότερο από το 33% των ερευνών εταιρειών από τις ΗΠΑ, τον Καναδά, το Ηνωμένο Βασίλειο και τη Γερμανία εξακολουθούν να "εξετάζουν τις πτυχές της προστασίας της ιδιωτικής ζωής κατά τρόπο ad hoc".

Οι παράγοντες που εμποδίζουν την ανάπτυξη τεχνικών Privacy Enhancing Technology PETs, οι οποίοι αποτελούν μέρος των μέσων που επιτρέπουν την ενσωμάτωση της ιδιωτικής ζωής στο σχεδιασμό ενός συστήματος, επηρεάζουν επίσης την ανάπτυξη σχεδίων που ενισχύουν την προστασία της ιδιωτικής ζωής. Σύμφωνα με τη μελέτη, η διαφορά της αντίληψης των οφελών και του κόστους των PET μπορεί να οφείλεται και στις δύο περιπτώσεις, στην εκτίμηση των επιδόσεων και των δαπανών των PET, η έλλειψη ευαισθητοποίησης και η σχέση των δεδομένων που συλλέγονται και επεξεργάζονται (οι Smes επεξεργάζονται λιγότερα δεδομένα, έτσι ώστε τα PET παρέχουν λιγότερα οφέλη).



Perception of benefits and costs of PETs

Στην ίδια μελέτη προέκυψαν άλλοι σημαντικοί λόγοι που εμποδίζουν την ανάπτυξη τεχνολογιών PET σε SME(small- medium enterprices) και non-SME οργανισμών:



Major reasons for not adopting implementing PETS

Επίσης, δεδομένου ότι τα οφέλη που συλλέγουν τα προσωπικά δεδομένα σε οργανισμούς (π.χ. στοχοθετημένη διαφήμιση, ανάλυση μεγάλων δεδομένων, ανταλλαγή δεδομένων με άλλες οντότητες κ.λπ.), τα κίνητρα για την εθελοντική εφαρμογή των PETs ενδέχεται να εμποδίσουν τη χρήση προσωπικών δεδομένων στα επιχειρηματικά τους μοντέλα είναι πολύ λίγα.

Έτσι λοιπόν κατά τη δημιουργία τεχνολογιών που θα χρησιμοποιηθούν από εταιρείες και υπηρεσίες σε απευθείας σύνδεση, πρέπει να ληφθεί μέριμνα ώστε να σχεδιαστούν με τέτοιο τρόπο ώστε η προστασία της ιδιωτικής ζωής να παραμείνει αναπόσπαστο μέρος του συστήματος.

Ακόμα και πριν τα συστήματα φθάσουν στους τελικούς χρήστες, πρέπει να έχουν ήδη τεθεί σε εφαρμογή όλα τα μέτρα προστασίας της ιδιωτικής ζωής. Η λειτουργία των χρηστών δεν θα πρέπει να επηρεάζεται από αυτά τα μέτρα προστασίας της ιδιωτικής ζωής και τα συστήματα θα πρέπει να γίνονται κατά τέτοιο τρόπο ώστε οι δυνητικές παραπλανήσεις ή λάθη να μην υποβαθμίζουν το απόρρητο. Και πάλι, η αρχή αυτή καλύπτεται κυρίως από τα άρθρα 25 και 32, μαζί με διάφορες αιτιολογικές σκέψεις.

3.2.4 Full functionality

Αυτή η αρχή υποστηρίζει ότι οι εντάσεις ή οι συγκρούσεις μεταξύ της προστασίας της ιδιωτικής ζωής και των άλλων απαιτήσεων είναι μερικές φορές υπερβολικές και χρησιμοποιούν ένα επιχείρημα για την αποφυγή των μέτρων προστασίας της ιδιωτικής ζωής. Ενώ το θετικό ποσό είναι πράγματι η ιδανική κατάσταση, πρέπει να παραδεχτούμε ότι η βιομηχανία βρίσκεται σήμερα αντιμέτωπη με πολλά εμπόδια. Είναι πολύ δύσκολο να πεισθεί κανείς ότι το ιδιωτικό απόρρητο της βιομηχανίας μπορεί να αντιμετωπιστεί σωστά χωρίς να χρειάζεται να αυξηθεί το κόστος, οι κίνδυνοι και η

πολυπλοκότητα του έργου ή να γίνουν κάποιες παραχωρήσεις από πλευράς χαρακτηριστικών, χρηστικότητας ή απόδοσης. Υπάρχουν πολλά παραδείγματα που αντικατοπτρίζουν την τρέχουσα κατάσταση.

- Blackphone: αυτό το τηλέφωνο Android ισχυρίζεται ότι τοποθετεί "το απόρρητο και τον έλεγχο απευθείας στα χέρια των χρηστών του", δεν υποστηρίζει το Play Store της Google όπου μπορούν να βρεθούν οι περισσότερες νόμιμες εφαρμογές για κινητά, επιτρέποντας στους χρήστες να χρησιμοποιούν λιγότερο ορθόδοξους (απαιτεί τεχνικές γνώσεις) μεθόδους για την εγκατάσταση νόμιμων εφαρμογών.

- Ανώνυμη πλοήγηση: Ο Tor είναι η πιο εκτεταμένη επιλογή για την παροχή ανώνυμης πλοήγησης στο διαδίκτυο. Ωστόσο, δεδομένης της δομής της, συνδέεται άμεσα με πολύ πιο αργές εμπειρίες πλοήγησης (εκτός από άλλα ζητήματα χρηστικότητας). Το πρωτόκολλο HTTPS είναι μια παρόμοια περίπτωση όπου η απόδοση μετρήθηκε σε περίπου 33% [Xub], σε σύγκριση με τη χρήση πρωτοκόλλου HTTP, παρόλο που αυτό προφανώς δεν αποκλείει (ή ακόμη και παρεμποδίζει σοβαρά) τη χρήση του HTTPS.

- Pretty Good Privacy: ενώ το πρωτόκολλο αυτό υφίσταται από το 1991, η υιοθέτησή του είναι αρκετά χαμηλή δεδομένου του περιορισμού της χρηστικότητας και της απαίτησής του για ορισμένες τεχνικές γνώσεις που πρέπει να ενσωματωθούν από τους προγραμματιστές.

Ορισμένα συμπεράσματα απορρέουν από τους τρέχοντες τεχνικούς περιορισμούς (π.χ. απόδοσης στην ομομορφική κρυπτογράφηση) ή από το πρόσθετο κόστος εφαρμογής των (Privacy Enhancing Technology) PETs στα συστήματα και αναπτύσσονται περαιτέρω στο τμήμα 4. Πρέπει να ειπωθεί ωστόσο ότι υπάρχουν μερικές πολλά υποσχόμενες εξελίξεις σε τέτοιες τεχνικές ως δεσμεύσεις ή αποδεικτικά μηδενικής γνώσης και ότι εφαρμογές όπως η έξυπνη μέτρηση ή η τιμολόγηση της ηλεκτρονικής κυκλοφορίας παρέχουν καλές εικονογραφήσεις ότι η θετική προσέγγιση είναι ρεαλιστική σε ορισμένους τομείς. Αυτές οι προσεγγίσεις θετικών αθροισμάτων, ενώ επιτρέπουν την υλοποίηση του κύριου επιχειρηματικού στόχου (π.χ. αποτελεσματική τροφοδότηση του ηλεκτρικού ρεύματος στην περίπτωση ενός έξυπνου δικτύου), εμποδίζουν μερικές φορές τη δευτερογενή χρήση των προσωπικών δεδομένων (π.χ. διαφήμιση), παρενέργεια αποθαρρύνουν την απορρόφηση από τη βιομηχανία, καθώς μερικές φορές αυτή η δευτερεύουσα χρήση είναι μια (κατά πάσα πιθανότητα παράνομη) ροή εισοδήματος

Ο στόχος της προστασίας της ιδιωτικής ζωής από την άποψη του σχεδιασμού είναι να δημιουργηθεί μια κατάσταση που θα είναι κερδοφόρα για όλους τους ενδιαφερόμενους. Η ιδέα είναι ότι αυτά τα μέτρα προστασίας της ιδιωτικής ζωής θα δημιουργήσουν οφέλη τόσο για τις εταιρείες όσο και για τους χρήστες. Αντί για μια

κατάσταση μηδενικού ποσού, όπου οι χρήστες μπορούν να επωφεληθούν μόνο από τα έξοδα των εταιρειών και αντιστρόφως, αυτά τα μέτρα προστασίας της ιδιωτικής ζωής από το σχεδιασμό στοχεύουν στη δημιουργία θετικών καθαρών αποτελεσμάτων χωρίς να προβούν σε τέτοιου είδους συμβιβασμούς.

Η προστασία της ιδιωτικής ζωής από το σχεδιασμό δεν πρέπει να ανταγωνίζεται τους στόχους σχεδιασμού και τις τεχνικές δυνατότητες του τελικού προϊόντος. Αντ 'αυτού, θα πρέπει να μετασχηματίσει τους στόχους που δεν συμμορφώνονται με την ιδιωτική ζωή με τέτοιο τρόπο ώστε η αξία τους να αυξάνεται λόγω της βελτίωσης της ιδιωτικότητας και της ασφάλειας.

3.2.5 End-to-end security

Η ασφάλεια και η ιδιωτικότητα πρέπει να αντιμετωπίζονται σε κάθε βήμα των διαδικασιών του συστήματος, από στάδια πριν από τη συλλογή προσωπικών δεδομένων, καθ 'όλη τη διάρκεια της επεξεργασίας του και έως ότου καταστραφεί. Το end-to-end έχει επίσης μια ερμηνεία "θέσης", που σημαίνει ότι η ασφάλεια πρέπει να υφίσταται και να είναι έγκυρη έως ότου τα δεδομένα φτάσουν στον προορισμό της.

Υπάρχουν διάφορες λύσεις στη βιομηχανία που αντιμετωπίζουν προβλήματα ασφάλειας από απόσταση σε διαφορετικούς τομείς με ποικίλους βαθμούς επιτυχίας:

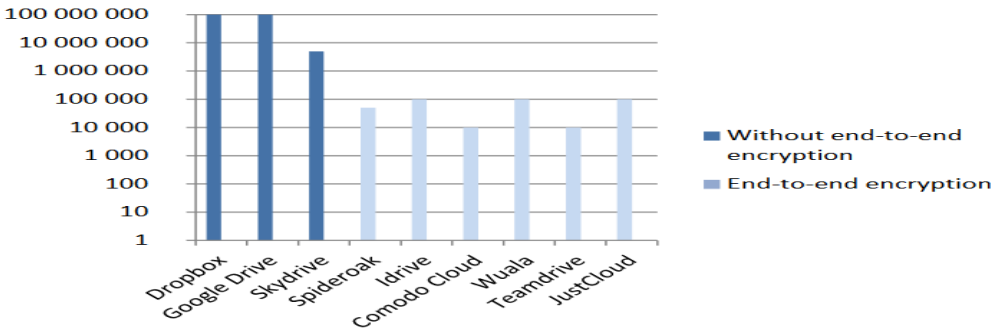
- Ο Telegram Messenger[8] είναι μια λύση ανταλλαγής μηνυμάτων, με περισσότερα από 35 εκατομμύρια χρήστες, πολλαπλών πλατφορμών με πελάτες ανοικτού κώδικα. Παρέχει διαφανή κρυπτογράφηση από άκρο σε άκρο και εγγυάται ότι μόνο οι δέκτες μπορούν να δουν τα απεσταλμένα μηνύματα.

- Πολλοί πάροχοι υπηρεσιών αποθήκευσης cloud προσφέρουν ασφάλεια από άκρο σε άκρο επιτρέποντας στους χρήστες να καθορίζουν τα δικά τους κλειδιά και να κρυπτογραφούν δεδομένα .

  Χρησιμοποιώντας στατιστικά στοιχεία για τον αριθμό των λήψεων εκδόσεων εφαρμογών κινητής τηλεφωνίας από παρόχους υπηρεσιών αποθήκευσης cloud, η χρήση αυτών των υπηρεσιών είναι κάτω από το 0,1% των αντικειμένων που δεν είναι φιλικά προς την ιδιωτικότητα. Η χρήση παροχέων αποθήκευσης ασφαλείας από άκρο σε άκρο φέρνει κάποιες λειτουργίες ανταλλαγής απόψεων, όπως αδυναμία παροχής υπηρεσιών διαδικτυακής προβολής και αναζήτησης αρχείων (web viewer) ή αναζήτησης.

8 https://telegram.org/

- Ο Silent Circle[9] παρέχει κρυπτογράφηση από άκρο σε άκρο για τηλεφωνικές κλήσεις και μηνύματα κειμένου μεταξύ των χρηστών τους. Η πρόσληψη εφαρμογών Silent Circle είναι μάλλον χαμηλή (λιγότερες από 100.000 λήψεις στο Android)



Google Play Store αριθμός downloads

Άλλες υπηρεσίες, όπως το ηλεκτρονικό ταχυδρομείο, είναι πιο δύσκολο να εφαρμοστούν όσον αφορά την ασφάλεια από απόσταση έως το τέλος λόγω της συμμετοχής πολλών παρόχων. Ένας πάροχος αλληλογραφίας μπορεί να παρέχει κρυπτογράφηση από άκρο σε άκρο των μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποστέλλονται μεταξύ των πελατών τους (π.χ. Hushmail[10]), αλλά μόλις μεταδοθούν σε άλλους παρόχους, ο έλεγχος χάνεται. Άλλος περιορισμός της κρυπτογράφησης από άκρο σε άκρο είναι ότι όλα τα μηνύματα θα πρέπει πρώτα να μεταφορτωθούν στη συσκευή του πελάτη πριν να μπορέσουν να εκτελέσουν οποιαδήποτε ενέργεια σε αυτά (π.χ. αναζήτηση).

Η Google και το Yahoo συνεργάζονται τώρα για να παρέχουν μια άπειρη εμπειρία ασφάλειας από το τέλος μέχρι το τέλος παρέχοντας συγκεκριμένα plug-ins του προγράμματος περιήγησης. Υπάρχουν άλλες προσεγγίσεις, όπως ανώνυμες υπηρεσίες αλληλογραφίας (π.χ. anonymous_email[11]), αλλά αυτές δεν μπορούν να παρέχουν ασφάλεια από άκρο σε άκρο. Απλώς λειτουργούν ως πληρεξούσιοι, κρύβοντας στον παραλήπτη τον χρήστη που στέλνει πραγματικά το μήνυμα ηλεκτρονικού ταχυδρομείου και επιβάλλει στον χρήστη να δημιουργήσει μια σχέση εμπιστοσύνης με αυτόν τον νέο πάροχο αλληλογραφίας, όπως θα συνέβαινε με τον παραδοσιακό.

Όσον αφορά την ασφαλή διαγραφή, διάφορα εργαλεία και δυνατότητες επιτρέπουν στους χρήστες να διαγράψουν με ασφάλεια τα αρχεία μεταξύ διαφορετικών λειτουργικών συστημάτων καθιστώντας σχεδόν αδύνατη την ανάκτηση των διαγραμμένων δεδομένων. Ωστόσο, πρέπει να αναγνωρίσουμε ότι υπάρχουν τεχνικοί

9 https://silentcircle.com/
10 https://www.hushmail.com
11 https://anonymousemail.us/

περιορισμοί που επιβάλλουν αντισταθμίσεις όταν χρησιμοποιούν την ασφάλεια από άκρο σε άκρο. Ενώ για ορισμένες εφαρμογές αυτοί οι περιορισμοί έχουν μικρό αντίκτυπο (π.χ. τηλεγράφημα), άλλοι είναι αρκετά ευάλωτοι σε αυτές και πιθανόν να υποστούν αρνητικές συνέπειες εάν εφαρμόζεται ασφάλεια από άκρο σε άκρο (π.χ. webmail χωρίς λειτουργία αναζήτησης).

Υπάρχει επίσης ένα άλλο σενάριο όπου η εφαρμογή της ασφάλειας από το ένα άκρο στο άλλο θα είχε πολύ μικρό αρνητικό αντίκτυπο και στην πραγματικότητα θα προστατεύσει αποτελεσματικά τα προσωπικά δεδομένα των χρηστών: πρόκειται για το Skype[12], το οποίο είναι τουλάχιστον ευάλωτο στην παρακολούθηση/υποκλοπή της NSA όπως αποδεικνύεται στη διαρροή της υπόθεσης Snowden.

Η ασφάλεια και το απόρρητο των δεδομένων πρέπει να εξασφαλίζονται από το σημείο συλλογής έως την ενδεχόμενη καταστροφή δεδομένων. Σε κάθε σημείο του κύκλου ζωής των δεδομένων, πρέπει να προστατεύεται συνεχώς. Οι πολλές διατάξεις σχετικά με τη συλλογή, την αποθήκευση και την καταστροφή δεδομένων καταγράφουν πλήρως το πνεύμα αυτού του κανόνα. Στόχος είναι να διασφαλιστεί ότι δεν υπάρχουν κενά στην ασφάλεια των δεδομένων, καθώς η ασφάλεια θεωρείται ουσιαστικό αντιστάθμισμα της ιδιωτικής ζωής. Έτσι, ο GDPR απαιτεί τη χρήση διαφόρων μεθόδων για την εξασφάλιση της λογοδοσίας (όπως η τήρηση αρχείων) και της ασφάλειας (ανωνυμοποίηση, έλεγχοι πρόσβασης κ.λπ.).

3.2.6 Visibility and transparency

Ο εφαρμοσμένος πλέον ευρωπαϊκός κανονισμός ,από την 21 Μάιου 2018, για τη γενική προστασία δεδομένων (GDPR), που έχει εγκριθεί από το κοινοτικό κοινοβούλιο, προσθέτει νέες αρχές όπως η «λογοδοσία», που απεικονίζεται ως ευθύνη του υπεύθυνου επεξεργασίας να "υιοθετεί πολιτικές και να εφαρμόζει τα κατάλληλα μέτρα για να διασφαλίσει και να καταδείξει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται σύμφωνα με τον παρόντα κανονισμό ". Εισάγει επίσης την αρχή της "διαφάνειας" η οποία υποχρεώνει τον υπεύθυνο επεξεργασίας να παρέχει:

- Διαφανείς και εύκολα προσβάσιμες και κατανοητές πληροφορίες.
- Μηχανισμοί διαδικασίας για την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων.

Πέραν της προβολής και της διαφάνειας, η προστασία της ιδιωτικής ζωής από το σχεδιασμό (PbD) θα πρέπει επίσης να διασφαλίζει την ικανότητα ελέγχου, δηλαδή με λίγα λόγια να έχει την ικανότητα να αποδείξει σε όλους τους ενδιαφερόμενους ότι οι οργανισμοί λειτουργούν σύμφωνα με τις υποσχέσεις και τους στόχους της προστασίας της ιδιωτικής ζωής.

12 http://www.skype.com/

Το πρώτο βήμα αυτής της αρχής είναι να παρέχει σε όλους τους ενδιαφερόμενους, με σαφή και κατανοητή γλώσσα (ή με μεταφορές, όπως τα εικονίδια προστασίας της ιδιωτικής ζωής) πληροφορίες σχετικά με τις πρακτικές απορρήτου που ακολουθούν το σύστημα και οι οργανισμοί (π.χ δημοσίευση πολιτικών απορρήτου, ειδοποιήσεις ή αναφορές Privacy Impact Assessment). Μια πρόσφατη έρευνα από το Global Surveillance Network Sweep , έχει διαπιστώσει ότι το 85% των 1.211 δημοφιλέστερων εφαρμογών για κινητά που ερωτήθηκαν δεν κατόρθωσε να εξηγήσει με σαφήνεια τον τρόπο συλλογής, χρήσης και αποκάλυψης προσωπικών πληροφοριών. Μια άλλη ανάλυση διεξήχθη σε 100 ιστότοπους που ανήκουν σε διαφορετικούς κλάδους της βιομηχανίας αποκάλυψε ότι, μεταξύ όλων των πολιτικών απορρήτου που αναλύθηκαν, η μέση βαθμολογία σύμφωνα με τη δοκιμή Flesch Reading Ease ήταν 37, γεγονός που σημαίνει ότι οι μέσες πολιτικές απορρήτου μπορούν να θεωρηθούν, τουλάχιστον, αρκετά δυσνόητες.

Διαθέτοντας πολλά δωρεάν εργαλεία, όπως το GeneratePrivacyPolicy.com[13] ή το PrivacyChoice[14], μπορεί να βοηθήσει οργανισμούς να παρέχουν κατανοητές πολιτικές απορρήτου, κάτι τέτοιο δεικνύει την έλλειψη ενημέρωσης αυτών των εργαλείων εκ μέρους αυτών των οργανισμών ή το χαμηλό ενδιαφέρον για την προβολή των πρακτικών απορρήτου τους. Για παράδειγμα, η Google ενημέρωσε την πολιτική απορρήτου το 2012 κάτι για το οποίο κατακρίθηκε έντονα από τις ευρωπαϊκές αρχές προστασίας δεδομένων, διότι δεν παρείχαν σαφείς και πλήρεις πληροφορίες σχετικά με τα δεδομένα και τους σκοπούς συλλογής των εργασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Επίσης, η Google δεν πρόσφερε πουθενά τον έλεγχο στους χρηστές για τον συνδυασμό δεδομένων στις υπηρεσίες της.

Η δημοσίευση αναφορών του Privacy impact Assessment-PIA (εκτίμηση αντικτύπου στην ιδιωτική ζωή), όπου οι οργανισμοί αναφέρουν τα μέτρα που λαμβάνουν για την προστασία των προσωπικών δεδομένων του πελάτη, είναι ένας τρόπος που η βιομηχανία μπορεί να χρησιμοποιήσει για να αποδείξει τον συμβιβασμό της με την προστασία των προσωπικών δεδομένων του πελάτη.

Ωστόσο, το PIAWatch[15], το παρατηρητήριο της PIA μπόρεσε (έως τον Σεπτέμβριο του 2014) να συλλέξει 41 δημόσιες εκθέσεις PIA, εκ των οποίων μόνο 13 προέρχονται από την ΕΕ. Εάν αυτές οι πληροφορίες σχετικά με τον αριθμό των δημόσιων εκθέσεων PIA συγκριθούν με τον αριθμό των οργανισμών που διεξάγουν PIA (όχι μόνο στην βιομηχανία), μόνο το 64% των ερωτηθέντων μιας έρευνας ανέφεραν ότι διενεργούν PIAs, άρα συμπεραίνουμε ότι υπάρχει ένα σαφές κενό που μπορεί να μεταφραστεί σε έλλειψη κινήτρων για τη δημοσίευση των εκθέσεων της PIA, για να είναι διαφανής.

Το κλειδί της λογοδοσίας και συμμόρφωσης με το GDPR είναι η διαφάνεια. Όλοι οι ενδιαφερόμενοι, οι εταίροι και οι συνεργαζόμενοι πρέπει να ελεγχθούν και να είναι

13 http://www.generateprivacypolicy.com/
14 http://privacychoice.org/policymaker
15 www.piawatch.eu

ανοικτές σε εξωτερική επαλήθευση. Χωρίς διαφάνεια και ξεκάθαρα κατανοητά, δεν υπάρχει κανένας πραγματικός τρόπος να εξακριβωθεί κατά πόσον οι αρχές της προστασίας της ιδιωτικής ζωής από το σχεδιασμό (PbD) έχουν εφαρμοστεί σωστά.

Μπορούν να χρησιμοποιηθούν τυποποιημένα συμβόλαια για να εξασφαλιστεί η λογοδοσία μεταξύ των εταίρων κοινής χρήσης δεδομένων και όλες οι πληροφορίες σχετικά με πιθανές παραβιάσεις πολιτικής θα πρέπει να κοινοποιούνται ανοιχτά και χωρίς κανένα πρόβλημα.

Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων GDPR εισάγει πολλούς μηχανισμούς για τη διασφάλιση της διαφάνειας. Στα άρθρα 51 έως 59, θεσπίζει την έννοια των εποπτικών αρχών που εποπτεύουν όλους τους φορείς επεξεργασίας δεδομένων σε ολόκληρη την ΕΕ. Επιπλέον, καθιερώνει το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και εισάγει αυστηρά πρόστιμα για όλους τους παραβάτες.

3.2.7 Respect for user privacy

Αυτή η αρχή[16] ενθαρρύνει τους σχεδιαστές συστημάτων να θέσουν τα συμφέροντα του ατόμου πάνω από οποιοδήποτε άλλο. Αυτή η θεμελιώδης αρχή μπορεί να προκαλέσει συγκρούσεις στον κλάδο, καθώς τα συμφέροντα του οργανισμού συνήθως τοποθετούνται πάνω από τα συμφέροντα του πελάτη. Ένα σαφές παράδειγμα αυτής της σύγκρουσης είναι η παρακολούθηση των χρηστών για την παροχή πιο στοχοθετημένων διαφημίσεων. Η έρευνα από που πραγματώθηκε από την μη κερδοσκοπική οργάνωση Pew (Pew Research Center) που εδρεύει στην Ουάσιγκτον αποκάλυψε ότι πάνω από το 65% των χρηστών απέρριπταν τις μηχανές αναζήτησης και τις τοποθεσίες Web που παρακολουθούσαν τη συμπεριφορά τους στο διαδίκτυο.

Εν τω μεταξύ, περισσότερο από το 40%[17] των εφαρμογών για κινητά smartphone περιλαμβάνει στοχευμένες διαφημίσεις ή, σύμφωνα με τα στατιστικά στοιχεία είναι "χτισμένο με", πάνω από το 40%[18] από τις κορυφαίες τοποθεσίες Web χρησιμοποιούν διαφημιστικές υπηρεσίες DoubleClick[19]. Ένα άλλο ενδιαφέρον στατιστικό στοιχείο που αποκαλύπτει ένα χάσμα στις πρακτικές προστασίας της ιδιωτικής ζωής στον κλάδο, «σχεδόν 1 στις 3 εφαρμογές φάνηκε να ζητεί υπερβολικό αριθμό δικαιωμάτων

16 Όπως έχει παρουσιαστεί με την έρευνα στον τομέα της οικονομίας, των γνωστικών επιστημών ή της αλληλεπίδρασης ανθρώπου-υπολογιστή, η πολυπλοκότητα είναι τέτοια που οι κρίσεις μας σε αυτόν τον τομέα είναι επιρρεπείς σε σφάλματα που οφείλονται στην έλλειψη πληροφορίας ή υπολογιστικής ικανότητας, ή από προβλήματα αυτοελέγχου και μεροληπτικής διαδικασίας λήψης αποφάσεων. Είναι αδύνατο να ελέγχεται κάθε πληροφορία για τον εαυτό του που κυκλοφορεί στα δίκτυα μέσω πολλών καναλιών και βάσεων δεδομένων. Επιπλέον, ενώ μοιράζονται τα δεδομένα τους με τα μέλη των κοινωνικών δικτύων ή με διάφορους παρόχους, έχουμε την "ψευδαίσθηση ελέγχου".

17 http://www.appbrain.com/stats/libraries/details/admob/admob

18 http://trends.builtwith.com/ads/DoubleClick.Net

19 http://www.google.com/doubleclick

πρόσβασης σε πρόσθετες προσωπικές πληροφορίες». Η βιομηχανία φαίνεται να αγνοεί συστηματικά τις επιθυμίες των χρηστών όσον αφορά την προστασία της ιδιωτικής ζωής, πιθανώς επειδή οι ίδιοι πελάτες είναι αδύναμοι και έχουν λίγη εναλλακτική λύση από το να συνεχίσουν να αποδέχονται το καθεστώς(η αλλιώς status quo) και να χρησιμοποιούν υπηρεσίες διεισδυτικής προστασίας.

Ακόμη και όταν προσπαθεί, η βιομηχανία συνεχίζει να μην προστατεύει τα προσωπικά δεδομένα των χρηστών. Η έκθεση Gartner ανέφερε ότι οι οργανισμοί συνεχίζουν να επενδύουν περισσότερο στην προστασία της ιδιωτικής τους ζωής εξαιτίας της συνεχιζόμενης προσοχής του κοινού και ορισμένων νέων ή αναμενόμενων νομικών απαιτήσεων · ωστόσο ο αριθμός των παραβιάσεων, η έκταση και το κόστος τους αυξάνεται, παρουσιάζοντας ένα χάσμα στην αποτελεσματικότητα των πρακτικών απορρήτου της βιομηχανίας, γεγονός που μπορεί να επιδεινωθεί από το ταυτόχρονο γεγονός ότι η αύξηση του συνολικού όγκου δεδομένων που είναι δυνατόν να συγκεντρωθούν, να μεταδοθούν και να επεξεργαστούν αυξάνεται με πρωτοφανή ρυθμό.

Επίσης, σημαντικό μέρος της βιομηχανίας παρουσιάζει γενικευμένη απάθεια κατά την προστασία των προσωπικών δεδομένων των πελατών, σύμφωνα με έρευνα της Gartner ότι το 7% των οργανισμών παραδέχεται ότι "κάνει το ελάχιστο" όσον αφορά τους νόμους περί απορρήτου.

Ο καλύτερος τρόπος για να επιτύχετε εξαιρετικό αποτέλεσμα στην εφαρμογή της προστασίας της ιδιωτικής ζωής από τα σχεδιαστικά χαρακτηριστικά θα πρέπει να είναι η δημιουργία προϊόντων με γνώμονα τους τελικούς χρήστες. Θα πρέπει να σχεδιάζονται έτσι ώστε να ανταποκρίνονται στις ανάγκες των χρηστών και να περιλαμβάνουν απλές δυνατότητες για τον έλεγχο και την επίβλεψη της επεξεργασίας των δεδομένων τους. Με την θέσπιση του «Γενικού Κανονισμού για την Προστασία Δεδομένων» GDPR απαιτείται να γίνονται σεβαστά τα δικαιώματα των πολιτών, απαιτώντας τη συγκατάθεσή τους πριν χρησιμοποιηθούν τα δεδομένα τους, δίνοντάς τους ανά πάσα στιγμή πρόσβαση στα δεδομένα τους αλλά και επιτρέποντας την εύκολη απόσυρση της συναίνεσης όποτε εκείνος το θελήσει.

Είναι εύκολο να διαπιστώσουμε ότι η ορθή εφαρμογή της αρχής της προστασίας της ιδιωτικής ζωής από το σχεδιασμό θέτει τις εταιρείες στη σωστή κατεύθυνση προς τη συμμόρφωση. Στην πραγματικότητα, το μεγαλύτερο μέρος του GDPR, στην ουσία, αφορά την εισαγωγή της ιδιωτικής ζωής από το σχεδιασμό σε όλες τις εταιρείες και οργανισμούς που επεξεργάζονται στοιχεία της ΕΕ.

3.3 Γιατί οι τεχνολογίες χρειάζονται privacy και security by design;

Η αγορά Παγκόσμιου Ίντερνετ των πραγμάτων (IoT) αυξάνεται με εκπληκτικό ρυθμό. Η αγορά προβλέπεται να καταγράψει σύνθετο ετήσιο ρυθμό ανάπτυξης (CAGR) 13,2% κατά την περίοδο πρόβλεψης 2016-2023 παγκοσμίως. Ενώ αυτή η ανάπτυξη είναι συναρπαστική, η ασφάλεια και η ιδιωτικότητα παραμένουν οι κύριοι προβληματισμοί.

Με την ανάπτυξη του Διαδικτύου, η εμπιστοσύνη γίνεται όλο και πιο σημαντικός παράγοντας στο ψηφιακό οικοσύστημα. Η εκτεταμένη συλλογή, επεξεργασία και ανάλυση προσωπικών πληροφοριών προκάλεσε σοβαρές ανησυχίες όσον αφορά την προστασία της ιδιωτικής ζωής, ιδίως όσον αφορά την ευρεία ηλεκτρονική εποπτεία, τη δημιουργία προφίλ και τη γνωστοποίηση ιδιωτικών δεδομένων. Η προστασία της ιδιωτικής ζωής έχει γίνει ένας κρίσιμος παράγοντας εμπιστοσύνης και ελευθερίας στην σημερινή κοινωνία της πληροφορίας. Είναι πλέον ευρέως αναγνωρισμένο ότι, αν δεν αναπτυχθεί ένα σύστημα από το "έδαφος" με προστασία στον πυρήνα του, η αποτυχία θα προκύψει από απροσδόκητες αδυναμίες. Έτσι, η ενσωμάτωση της ιδιωτικής ζωής σε συνεργασία με την ασφάλεια απευθείας στο σχεδιασμό είναι ένα κρίσιμο βήμα για την προστασία της ιδιωτικής ζωής.

Σύμφωνα με μια μελέτη που πραγματοποιήθηκε από τη Forrester, "2017 Προβλέψεις: Δυναμική που θα διαμορφώσει το μέλλον είναι η εμπιστοσύνη (Trust) η οποία θα είναι το κύριο νόμισμα της επιχείρησης. Οι πελάτες την σήμερον ημέρα έχουν πολύ μεγαλύτερη και καλύτερη επίγνωση, επιφυλακτικότητα και απογοήτευση από τον κίνδυνο ασφάλειας και προστασίας προσωπικών δεδομένων. Έτσι λοιπόν μια επιχείρηση θα κερδίζει ή θα χάνει όλο και περισσότερο ανάλογα με το πόσο το κοινο εμπιστεύεται μια εταιρεία.

Επομένως, οι επιχειρήσεις θα πρέπει να πραγματοποιούν τους κατάλληλους ελέγχους προστασίας της ιδιωτικής ζωής και των δεδομένων καθώς αρχίζει ένα έργο. Η ιδιωτικότητα και η ασφάλεια δεν πρέπει να θεωρούνται μόνο ως άσκηση στο πλαίσιο ελέγχου. Το απόρρητο δεν μπορεί να εξασφαλιστεί μόνο με τη συμμόρφωση με τα κανονιστικά πλαίσια αλλά θα πρέπει να γίνει ιδανικά ο τρόπος λειτουργίας ενός οργανισμού.

3.4 Πώς να εφαρμόσουμε το Privacy by Design (How To Implement Privacy by Design)

Στα νέα συστήματα, η προστασία της ιδιωτικής ζωής από το σχεδιασμό ξεκινά με την έμφαση στην ιδιωτικότητα και την ασφάλεια σε όλη τη διαδικασία σχεδιασμού του συστήματος. Το απόρρητο θα ενσωματωθεί ομαλά στο σύστημά μας - επιτρέποντάς του να λειτουργεί ομαλά και με ασφάλεια από την πρώτη μέρα.

Η εφαρμογή της ιδιωτικής ζωής από το σχεδιασμό σε ένα υπάρχον σύστημα είναι πιο δύσκολη και χρονοβόρα, επειδή πρέπει να αποικοδομήσετε και να αναλύσετε πλήρως το σύστημα που διαθέτουμε. Πρέπει πρώτα να κάνουμε έναν έλεγχο ιδιωτικού απορρήτου στο σύστημά μας, από την αρχή μέχρι το τέλος. Ελέγχουμε πώς ενσωματώθηκε το ιδιωτικό απόρρητο στο υπάρχον σύστημα μας, εντοπίζουμε αδύναμα σημεία και δημιουργούμε νέες φιλικές προς το χρήστη λύσεις.

3.5 Κενά στα νομικά πλαίσια και έλλειψη ενημέρωσης (Gaps in the legal frameworks and lack of awareness)

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, η έλλειψη κινήτρων είναι ένας από τους παράγοντες που εξηγούν τη βραδεία υιοθέτηση της ιδιωτικής ζωής από τη σχεδίαση στη βιομηχανία. Αυτά τα κίνητρα θα μπορούσαν να προκύψουν είτε από την κοινωνική ζήτηση είτε από κανονισμούς υψηλού επιπέδου με πιθανές κυρώσεις για τους υπεύθυνους επεξεργασίας δεδομένων που δεν συμμορφώνονται ή από μια σαφή απαίτηση από την κοινωνία. Εάν η νομική πίεση δεν αρκεί, η αγορά για προϊόντα διατήρησης της ιδιωτικής ζωής θα πρέπει να βασίζεται μόνο στην ύπαρξη ρητής ανάγκης για τους καταναλωτές. Μόνο εάν οι εταιρείες είναι πεπεισμένες ότι η κοινωνία ζητά υπηρεσίες και προϊόντα με αυξημένη προστασία της ιδιωτικής ζωής, η ιδιωτικότητα μπορεί να λειτουργήσει ως παράγοντας διαφοροποίησης για τα προϊόντα επικοινωνιών (ICT Information Communications Technology).

Ενώ οι τρέχουσες κοινωνικές συμπεριφορές (αυτο-έκθεση, ανταλλαγή δεδομένων, επιλογή δωρεάν υπηρεσιών διαδικτύου έναντι εξατομικευμένων διαφημίσεων κ.λπ.) δεν φαίνονται να ευνοούν την ανάπτυξη τεχνολογιών προστασίας από το σχεδιασμό (secure by design), έτσι λοιπόν ο κύριος λόγος εντοπίζεται στην έλλειψη ενημέρωσης των χρηστών σχετικά με τις συνέπειες της χρήσης των νέων τεχνολογιών στην ιδιωτική τους ζωή. Εστιάζουμε οπότε την προσοχή μας στους ισχύοντες κανονισμούς και στα κίνητρα που ενδέχεται να παράσχουν ή αποτυγχάνουν να εξασφαλίσουν την ευρύτερη υιοθέτηση τεχνολογιών προστασίας από την ιδιωτική ζωή (PbD). Αναγνωρίζουμε τρία βασικά εμπόδια: τις αβεβαιότητες που συνδέονται με τη συζήτηση για την προστασία της ιδιωτικής ζωής από το σχεδιασμό έναντι της προστασίας δεδομένων (PbdD vs DPbD), τα περιορισμένα νομικά κίνητρα συμμόρφωσης και τις αντικρουόμενες νομικές υποχρεώσεις διατήρησης ή ανταλλαγής προσωπικών δεδομένων.

3.5.1 Έλλειψη ευαισθητοποίησης (Lack of Awareness amongst the general public)

Οι κοινωνικές συμπεριφορές συχνά έρχονται σε αντίθεση με την ανάπτυξη και την αφομοίωση των λύσεων προστασίας από την ιδιωτικότητα. Η εμφάνιση των νέων

τεχνολογιών σε διάφορες πτυχές της καθημερινής ζωής συνοδεύεται από το κοινωνικό φαινόμενο που οι άνθρωποι αισθάνονται όλο και πιο άνετα με την έκθεση τους στο διαδίκτυο. Στο μυαλό τους, η αποκάλυψη προσωπικών δεδομένων θεωρείται ως ένα αυξανόμενο μέρος της σύγχρονης ζωής, ενώ οι ανησυχίες για την προστασία της ιδιωτικής ζωής φαίνεται να ξεθωριάζουν όταν έρχεται η επιθυμία συμμετοχής στα κοινωνικά μέσα και τα ηλεκτρονικά ψώνια. Οι Ευρωπαίοι έχουν την τάση να μοιράζονται το όνομα τους, φωτογραφία και εθνικότητα για σκοπούς κοινωνικής δικτύωσης. και τα ονόματά τους, τις διευθύνσεις στο σπίτι και τον αριθμό τηλεφώνου για ηλεκτρονικές αγορές. Τέτοιες κοινωνικές συμπεριφορές συχνά δίνουν την εντύπωση ότι οι άνθρωποι δεν ενδιαφέρονται πραγματικά για την προστασία της ιδιωτικής ζωής, γεγονός που έχει ως αποτέλεσμα την περιορισμένη κοινωνική ζήτηση για το Privacy by Design. Ωστόσο, όταν κοιτάζουμε πιο προσεκτικά το φαινόμενο, αξίζει να επισημανθούν δύο πτυχές:

- Η αντίληψη των ανθρώπων σχετικά με την ιδιωτική ζωή αλλάζει ανάλογα με το πλαίσιο της ηλεκτρονικής συμπεριφοράς.

- Η γενική αντίληψη ότι η ιδιωτικότητα είναι σημαντική δεν σημαίνει ότι οι άνθρωποι καταλαβαίνουν λεπτομερώς για το τι είναι.

Η προθυμία των πολιτών να ανταλλάσσουν το απόρρητό τους για μια ηλεκτρονική υπηρεσία διαφέρει σημαντικά από περίπτωση σε περίπτωση. Οι πληροφορίες που οι χρήστες θα είναι έτοιμες να αποκαλύψουν σε περιβάλλοντα κοινωνικής δικτύωσης ή ηλεκτρονικού εμπορίου δεν θα είναι αναγκαστικά οι ίδιες με εκείνες που αφορούν την ηλεκτρονική τραπεζική, την ηλεκτρονική υγεία, το ηλεκτρονικό δημόσιο περιβάλλον.

Ο λόγος είναι ότι η ιδιωτικότητα δεν είναι απόλυτη αξία. μπορεί να γίνει κατανοητό μόνο σε σχέση με το πλαίσιο στο οποίο τα άτομα αποκαλύπτουν τα προσωπικά τους δεδομένα. Αυτό σημαίνει ότι, παρόλο που οι άνθρωποι ασχολούνται με πολυάριθμες δραστηριότητες στο διαδίκτυο, υπάρχουν διαφορετικές υποθέσεις σχετικά με το πόσο σημαντική είναι η προστασία της ιδιωτικής ζωής και ποιες πτυχές της θέλουν να διατηρήσουν ανάλογα με το πλαίσιο. Επομένως, η ανάληψη γενικής προθυμίας για κοινή χρήση πληροφοριών χωρίς να γίνεται διάκριση δεν θα ήταν ακριβής, καθώς ο τρόπος με τον οποίο οι άνθρωποι αντιλαμβάνονται τις διαφορετικές τους δραστηριότητες στο διαδίκτυο διαφέρει από περίπτωση σε περίπτωση.

Η πολυπλοκότητα του διαδικτύου αυξάνεται συνεχώς μαζί με τον καθημερινό αριθμό αποφάσεων που οι άνθρωποι πρέπει να κάνουν σχετικά με τις δραστηριότητές τους στο διαδίκτυο. Παρ 'όλα αυτά, φαίνεται ότι οι άνθρωποι αντιλαμβάνονται την ιδιωτικότητα ως κάτι σημαντικό. Ωστόσο, πρέπει να σημειωθεί ότι η σημασία της ιδιωτικής ζωής

είναι περισσότερο ένα συναίσθημα παρά μια καλά κατανοητή έννοια. Οι άνθρωποι δυσκολεύονται να εκτιμήσουν τον τρόπο με τον οποίο οι συγκεκριμένες δραστηριότητές τους στο διαδίκτυο μπορούν να επηρεάσουν την ιδιωτικότητα τους.. Αυτό που μπορεί να φανεί ως έλλειψη ενδιαφέροντος για τις λύσεις προστασίας από την ιδιωτικοποίηση, εξηγείται στην πραγματικότητα από την έλλειψη κατανόησης και συνειδητοποίησης που συνδέεται με το γεγονός ότι οι περισσότεροι χρήστες αισθάνονται αβοήθητοι πιστεύοντας ότι δεν έχουν άλλη επιλογή παρά να εγκαταλείψουν την ιδιωτική τους ζωή ώστε να μην αποκλειστούν από την ψηφιακή κοινότητα.

Για να υποστηρίξουμε αυτό το επιχείρημα, μπορούν να αναφερθούν αρκετά πρόσφατα παραδείγματα τεχνολογιών που απελευθερώθηκαν με τον εκφρασμένο στόχο να αυξηθεί το ιδιωτικό απόρρητο των ατόμων. Αρχικά, ας πάρουμε το παράδειγμα του "Blackphone". Σε αντίθεση με τις αυξανόμενες παραβιάσεις των δεδομένων και τις αποκαλύψεις του Snowden, δύο εταιρείες, το Geeksphone και το SilentCircle, ξεκίνησαν ένα smartphone με μια τροποποιημένη έκδοση του Android που ονομάζεται PrivatOS και φορτώνονται με χαρακτηριστικά ασφαλείας όπως κρυπτογραφημένα μηνύματα κειμένου, κρυπτογράφηση φωνής και κλήσεις βίντεο, ιδιωτική περιήγηση, ανώνυμη αναζήτηση. Στο ίδιο πνεύμα, οι αποφάσεις της Apple και της Google να ενσωματώσουν στα αντίστοιχα λειτουργικά τους συστήματα ισχυρότερο λογισμικό κρυπτογράφησης που δεν μπορούν να ξεκλειδώσουν οι ίδιοι, έστω και αν υποβάλλονται με ένταλμα, αποτελούν άμεση απάντηση στις ανησυχίες που προκαλεί η υποτιθέμενη συνεργασία τους με μυστικές υπηρεσίες στο σκάνδαλο PRISM.

3.5.2 Προστασία της ιδιωτικής ζωής ως νομική αρχή (Privacy by Design as a legal principle)

Η διαφοροποίηση μεταξύ προστασίας της ιδιωτικής ζωής και των δεδομένων έχει προκαλέσει πολλές συζητήσεις και συζητήσεις, οι οποίες αφορούν ιδίως δικηγόρους, πολιτικούς επιστήμονες και επιστήμονες υπολογιστών. Αυτή η συζήτηση έφθασε ακόμη στο επίπεδο των κύκλων χάραξης πολιτικής της Ευρωπαϊκής Ένωσης με τις συνεχιζόμενες συζητήσεις σχετικά με το σχέδιο γενικού κανονισμού για την προστασία των δεδομένων (GDPR): η αρχική έκδοση του κειμένου αναφέρεται στην "προστασία της ιδιωτικής ζωής από το σχεδιασμό" (Privacy by Design) ενώ η τρέχουσα έκδοση αναφέρεται "Προστασία δεδομένων από το σχεδιασμό" (data protection by design), η οποία ερμηνεύθηκε από ορισμένους δικηγόρους ως το γεγονός ότι στοχεύει μόνο στην προστασία της ιδιωτικής ζωής, στο βαθμό που συνεπάγεται η προστασία των δεδομένων.

Μια παρόμοια διαφοροποίηση εμφανίζεται στις ΗΠΑ μεταξύ της "ιδιωτικότητας" και της "προστασίας της ιδιωτικής ζωής των πληροφοριών", την οποία θεωρούν ορισμένοι ακαδημαϊκοί ως "κατασκεύασμα της τεχνολογικής εποχής", το οποίο παρέχει μικρή προστασία από τον κίνδυνο επιτήρησης και παρέμβασης από οποιαδήποτε κυβέρνηση, από ρητές εξαιρέσεις ή από οργανισμούς του ιδιωτικού τομέα, οι οποίοι θεωρούνται εμπιστευτικά μέρη. Σύμφωνα με αυτή τη σκέψη, η προστασία της ιδιωτικής ζωής θεωρεί τον υπεύθυνο επεξεργασίας δεδομένων ως αξιόπιστο τρίτο μέρος, γεγονός που καθιστά περιττή τη χρήση των τεχνολογιών διατήρησης της ιδιωτικής ζωής, ιδίως των τεχνικών ελαχιστοποίησης των δεδομένων.

Όπως αναφέρεται στην εισαγωγή, το Privacy by Design θεωρείται γενικά ως μια προσέγγιση που μπορεί να συμβάλει στην προώθηση ισχυρών αρχών προστασίας της ιδιωτικής ζωής που υιοθετήθηκαν από τα αρχικά στάδια του σχεδιασμού και της ανάπτυξης ενός συστήματος και καθ 'όλη τη διάρκεια του κύκλου ζωής του. Για να επιτευχθεί αυτός ο στόχος, κατέστη σαφές κατά τη διάρκεια των προπαρασκευαστικών σταδίων της μεταρρύθμισης της προστασίας των δεδομένων στην Ευρώπη ότι η προστασία της ιδιωτικής ζωής από το σχεδιασμό πρέπει να αναγνωρίζεται ως γενική αρχή.

Παρόλο που η έννοια αναφερόταν ως σχετική με την ιδιωτική ζωή ως σχέδιο προστασίας σε προγενέστερα έγγραφα πολιτικής, η ίδια η διατύπωση του σχεδίου γενικού κανονισμού για την προστασία των δεδομένων αναφέρεται στην "προστασία δεδομένων από το σχεδιασμό" ως αρχή που απαιτεί την ενσωμάτωση της προστασίας δεδομένων σε ολόκληρο τον κύκλο ζωής της τεχνολογίας από το πολύ πρώιμο στάδιο του σχεδιασμού έως την τελική διάθεσή της, τη χρήση και την τελική διάθεσή της. Σύμφωνα με την αρχή αυτή, οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να υιοθετούν εσωτερικές πολιτικές καθώς και κατάλληλα τεχνικά και οργανωτικά μέτρα, τόσο κατά τον σχεδιασμό της επεξεργασίας όσο και κατά τη στιγμή της ίδιας της επεξεργασίας, κατά τρόπον ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντα κανονισμού και την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα.

3.5.2.1 Ιδιωτικότητα - Προστασία δεδομένων (Privacy by design VS Data Protection by design)

Η προστασία της ιδιωτικής ζωής (Privacy by Design) από το σχεδιασμό αναφέρεται σε τεχνικά και οργανωτικά μέτρα που υιοθετήθηκαν από τα πρώτα στάδια του σχεδιασμού και της ανάπτυξης ενός συστήματος και καθ 'όλη τη διάρκεια του κύκλου ζωής του, ώστε να διατηρηθούν οι επιπτώσεις στην ιδιωτική ζωή που υπερβαίνουν την απλή επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Η προστασία των δεδομένων από το σχεδιασμό (Data Protection by Design), αφετέρου, αναφέρεται στα μέτρα που αποσκοπούν ειδικά στην αποφυγή παρεμβολών που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η ανακοίνωση

της Επιτροπής η οποία δρομολόγησε τη συζήτηση για τη μεταρρύθμιση της προστασίας των δεδομένων αναφερόταν αρχικά στο «Privacy by Design», καθώς η συζήτηση στην αρχή της μεταρρύθμισης επέτρεψε μια γενική και ευρεία θεώρηση. Αργότερα, η επιλογή που έγινε στο πρώτο σχέδιο του Κανονισμού περί Γενικής Προστασίας Δεδομένων (GDPR) ήταν να εισαχθεί αρχικά η αρχή της προστασίας δεδομένων, σύμφωνα με το πεδίο εφαρμογής του κανονισμού. Έχει υπονοηθεί ότι οι δύο έννοιες χρησιμοποιούνται εναλλακτικά στο σχέδιο, αλλά έχει επίσης σημειωθεί ότι η «νομική προστασία από το σχεδιασμό» που εισάγεται στο άρθρο 23 αναφέρεται σαφώς στην προστασία των δεδομένων και στοχεύει μόνο στην ιδιωτική ζωή, στο μέτρο που συνεπάγεται η προστασία των δεδομένων.

Η εισαγωγή του Privacy by Design θα γίνει κατανοητή σε σχέση με το σχεδιασμό της ιδιωτικής ζωής των τεχνολογιών χωρίς απαραίτητα να αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Αυτό θα ήταν περίπλοκο καθήκον, δεδομένου ότι η προστασία της ιδιωτικής ζωής είναι μια ανοικτή και ουσιαστικά αμφισβητούμενη έννοια και, επομένως, θα ήταν πολύ δύσκολο να προσδιοριστεί ποιος σχεδιάζει πραγματικά την προστασία της ιδιωτικής ζωής. Από την άλλη πλευρά, η προστασία δεδομένων από το σχεδιασμό θα μπορούσε να κάνει χρήση της νομοθεσίας για την προστασία των δεδομένων.

Οι αρχές προστασίας δεδομένων που απορρέουν από τον ήδη ελεγχόμενο τομέα προστασίας δεδομένων θα μπορούσαν να χρησιμοποιηθούν ως βάση για την οικοδόμηση τεχνικών απαιτήσεων οι οποίες θα συνάδουν με την έννοια της νομικής προστασίας από το σχεδιασμό(data protection law). Επομένως, η επιλογή της εισαγωγής της προστασίας δεδομένων από το σχεδιασμό συνδέεται με το πεδίο εφαρμογής αυτού του μέσου το οποίο αποσκοπεί στην προστασία των θεμελιωδών δικαιωμάτων και της ελευθερίας των ατόμων, και ιδίως του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα σε σχέση με την επεξεργασία τέτοιων δεδομένων.

Επομένως, εισάγεται η αρχή της "προεπιλεγμένης προστασίας δεδομένων" (data protection by default) και όχι της "απορρήτου από προεπιλογή" (privacy by default). Η αρχή της προστασίας δεδομένων από προεπιλογή απαιτεί ρυθμίσεις προστασίας της ιδιωτικής ζωής στις υπηρεσίες και τα προϊόντα, οι οποίες οφείλουν να συμμορφώνονται με τις γενικές αρχές προστασίας δεδομένων, όπως η ελαχιστοποίηση των δεδομένων και ο περιορισμός των σκοπών. Υπό την προϋπόθεση ότι η προστασία δεδομένων από την άποψη του σχεδιασμού αναφέρεται στην εφαρμογή των αρχών προστασίας δεδομένων εν γένει, η προστασία δεδομένων από προεπιλογή, ως ξεχωριστή αρχή, έχει μικρότερο πεδίο εφαρμογής και συνιστά υποσύνολο προστασίας δεδομένων από την άποψη του σχεδιασμού.

3.5.3 Περιορισμένα κίνητρα συμμόρφωσης που περιέχονται στο πλαίσιο προστασίας δεδομένων

Η εισαγωγή της αρχής της προστασίας δεδομένων από το σχεδιασμό (και από προεπιλογή) στο σχέδιο κανονισμού προέκυψε από διάφορα κίνητρα και είχε υποστηριχθεί από πολλούς ενδιαφερόμενους. Για παράδειγμα, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων(European Data Protection Supervisor)τόνισε την ανάγκη να αντιμετωπιστούν από την αρχή οι κίνδυνοι για την ιδιωτική ζωή και ζήτησε την εφαρμογή της προστασίας της ιδιωτικής ζωής από το σχεδιασμό ως πρόσθετη υποχρέωση για τους υπευθύνους επεξεργασίας δεδομένων.

Ο στόχος είναι διπλός, πρώτων να επιβληθεί η εφαρμογή των αρχών προστασίας δεδομένων και δεύτερων να προωθηθεί η υιοθέτηση τεχνολογιών ενίσχυσης της προστασίας της ιδιωτικής ζωής. Η προστασία της ιδιωτικής ζωής από το σχεδιασμό θεωρείται ως εργαλείο για την οικοδόμηση εμπιστοσύνης στην τεχνολογία της πληροφορίας(ICT), ιδίως μέσω της εξουσιοδότησης του χρήστη και της ανάπτυξης τεχνολογιών για την προστασία της ιδιωτικής ζωής.

Η εισαγωγή του Privacy by Design στο σχέδιο κανονισμού ακολουθεί μια διεθνή τάση για την αναγνώριση μιας τέτοιας έννοιας ως κατευθυντήριας αρχής για την εφαρμογή του πλαισίου προστασίας δεδομένων. Το 2010 οι Επιτρόποι Πληροφόρησης και Προστασίας Προσωπικών Δεδομένων που συγκεντρώθηκαν στην Ιερουσαλήμ, επικύρωσαν τις 7 θεμελιώδεις αρχές περί της Προστασίας Προσωπικών Δεδομένων από το σχεδιασμό (PbD) που σχεδιάστηκαν από την Information and Privacy Commissioner Ann Cavoukian οι οποίες έχουν αναλυθεί στο κεφάλαιο 3 παράγραφος 3.2.

Σε αυτό το κεφάλαιο αναλύουμε τις διάφορες παγίδες στη διατύπωση της υποχρέωσης στον προτεινόμενο κανονισμό, οι οποίες θα μπορούσαν να εμποδίσουν την ευρεία υιοθέτηση της αρχής της προστασίας των δεδομένων από το σχεδιασμό. Αρχικά θα αναλύσουμε πώς η ασαφής διατύπωση της αρχής μπορεί να δημιουργήσει νομική αβεβαιότητα ως προς την έκταση του περιεχομένου της υποχρέωσης. Στη συνέχεια, θα δούμε πώς το σύστημα επιβολής του νόμου μπορεί να μην είναι σαφές και ως εκ τούτου είναι δύσκολο να εφαρμοστεί αποτελεσματικά στην πράξη.

3.5.3.1 Δυσκολίες στον ορισμό του ακριβούς περιεχομένου της υποχρέωσης (Difficulties in defining the exact content of the obligation)

- Η διατύπωση της αρχής

Ο γενικός κανονισμός για την προστασία των δεδομένων(GDPR) περιλαμβάνει, βάσει μιας νέας αρχής της προστασίας των δεδομένων από το σχεδιασμό, την υποχρέωση των υπευθύνων επεξεργασίας δεδομένων να λαμβάνουν τεχνικά και οργανωτικά μέτρα κατάλληλα για τη δραστηριότητα επεξεργασίας και τους στόχους τους, κατά τρόπον ώστε η επεξεργασία να πληροί τις απαιτήσεις κανονισμού και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων. Το Privacy by Design απορρέει από τις αρχές προστασίας δεδομένων που είχαν ήδη περιληφθεί στην οδηγία για την προστασία των δεδομένων και ειδικότερα από την αρχή της ελαχιστοποίησης των δεδομένων και της αρχής της ασφάλειας των δεδομένων. Στόχος του είναι η εφαρμογή όλων των αρχών προστασίας δεδομένων γενικά στο σχεδιασμό συστημάτων πληροφορικής καθώς και η συνολική προσαρμογή των εσωτερικών πολιτικών ενός οργανισμού.

Η προσέγγιση που υιοθέτησε η Επιτροπή στο πρώτο της σχέδιο το 2012 ήταν ότι η αρχή θα καθοριστεί γενικά στη νομοθετική πράξη και το περιεχόμενό της θα περιγραφή περαιτέρω από την Επιτροπή μέσω πράξεων κατ 'εξουσιοδότηση και εκτέλεσης. Ωστόσο, το Κοινοβούλιο προτίμησε μια άλλη προσέγγιση που θα παρείχε επαρκή εξειδίκευση της αρχής στο κείμενο του κανονισμού και θα ενίσχυε έτσι την ασφάλεια δικαίου. Το κείμενο που εγκρίθηκε τον Μάρτιο του 2014 συμπλήρωσε τον ορισμό της αρχής με διατάξεις που περιλαμβάνονται σε πολλά άρθρα που θα διευκρινίσουν τις υποχρεώσεις που συνεπάγεται η αρχή αυτή για τους ελεγκτές δεδομένων. Οι τρέχουσες τεχνικές γνώσεις, οι βέλτιστες διεθνείς πρακτικές και οι κίνδυνοι προστασίας δεδομένων που παρουσιάζονται από τη δραστηριότητα επεξεργασίας δεδομένων αναφέρονται ρητά ως στοιχεία που λαμβάνονται υπόψη για τον καθορισμό των ελέγχων που έχουν τεθεί σε εφαρμογή.

Το Συμβούλιο έκανε ένα ακόμη βήμα στο κείμενο που εγκρίθηκε τον Δεκέμβριο του 2014 . Απέρριψε τους προηγούμενους ορισμούς της έννοιας της "προστασίας δεδομένων από το σχεδιασμό" και, αντίθετα, πρότεινε έναν μη εξαντλητικό κατάλογο παραδειγμάτων μέτρων προστασίας δεδομένων μέσω σχεδιασμού, όπως ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ψευδώνυμο προσωπικών δεδομένων, βελτιώνοντας τη διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία των προσωπικών δεδομένων, επιτρέποντας στο υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία δεδομένων, επιτρέποντας στον ελεγκτή να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφαλείας. Εισάγονται επίσης διάφοροι παράγοντες που σχετίζονται με την επεξεργασία δεδομένων, οι οποίοι πρέπει να λαμβάνονται υπόψη κατά τη λήψη αποφάσεων σχετικά με την εφαρμογή της προστασίας δεδομένων μέσω σχεδιαστικών μέτρων. Εκτός από τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, αυτές περιλαμβάνουν επίσης τη φύση, το πεδίο,

το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και την πιθανότητα και τη σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες των ατόμων που προκαλεί η επεξεργασία (άρθρο 23).

- Πεδίο εφαρμογής της υποχρέωσης σε σχέση με τα προϊόντα και τις υπηρεσίες με τις οποίες λειτουργεί ο υπεύθυνος επεξεργασίας δεδομένων.

Σύμφωνα με την οδηγία 46/1995 / ΕΚ για την προστασία των δεδομένων, ο υπεύθυνος επεξεργασίας δεδομένων, αυτός που καθορίζει τις δραστηριότητες επεξεργασίας δεδομένων, ήταν ο υπεύθυνος για τη λήψη των σχετικών μέτρων για την προστασία των δεδομένων. Παρ 'όλα αυτά, η επεξεργασία δεδομένων πραγματοποιείται με προϊόντα και υπηρεσίες που έχουν σχεδιαστεί από φορείς των οποίων η δραστηριότητα μέχρι σήμερα δεν υπόκειται άμεσα στη νομοθεσία περί προστασίας δεδομένων. Στην οδηγία για την προστασία των δεδομένων δεν δόθηκαν περαιτέρω προδιαγραφές στους κατασκευαστές, παραγωγούς των τεχνολογιών επεξεργασίας δεδομένων.

Κατά τη διάρκεια της μεταρρύθμισης της προστασίας δεδομένων, το ζήτημα τέθηκε σε εξέλιξη από πολλούς ενδιαφερόμενους, ιδίως στο πλαίσιο της συζήτησης της αρχής της προστασίας δεδομένων προσωπικού χαρακτήρα και προστασίας δεδομένων από το σχεδιασμό. Το άρθρο 29 του WP έχει δηλώσει ότι οι προγραμματιστές εφαρμογών για κινητά καθώς και οι κατασκευαστές λειτουργικών συστημάτων και συσκευών πρέπει να λαμβάνουν υπόψη το απόρρητο. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (EDPS) έχει επίσης υποστηρίξει την εφαρμογή της προστασίας της ιδιωτικής ζωής μέσω σχεδιασμού όχι μόνο από τους ελεγκτές δεδομένων αλλά και από τους κατασκευαστές συστημάτων αεροναυτιλίας.

- Έμμεση υποχρέωση συμμόρφωσης όσον αφορά την προστασία των δεδομένων: Η Επιτροπή και το Κοινοβούλιο (επιτροπή LIBE και Ολομέλεια του Ευρωπαϊκού Κοινοβουλίου) υποστήριξαν ότι οι κατασκευαστές, σχεδιαστές θα πρέπει να έχουν την έμμεση υποχρέωση να εφαρμόζουν την προστασία δεδομένων από το σχεδιασμό. Μία εξήγηση για αυτό μπορεί να είναι ότι οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να φέρουν την άμεση ευθύνη, καθώς αυτοί θα επωφεληθούν από τη χρήση της επεξεργασίας δεδομένων. Η υπόθεση για αυτή την προσέγγιση είναι ότι ο υπεύθυνος επεξεργασίας πρέπει να επενδύσει σε προϊόντα-υπηρεσίες συμβατές με την προστασία δεδομένων. Ως φαινόμενο ντόμινο, οι κατασκευαστές, οι σχεδιαστές και οι προγραμματιστές θα έχουν τελικά το κίνητρο να συμμορφωθούν με την προστασία δεδομένων από το σχεδιασμό τους.

- Άμεση υποχρέωση συμμόρφωσης με την προστασία δεδομένων: Η έκθεση Albrecht, ακολουθώντας τις απόψεις του άρθρου 29 του ΠΕΠ και του ΕΕΠΔ όπως εξηγήθηκε παραπάνω, υποστήριξε ότι εκτός από τους υπεύθυνους επεξεργασίας δεδομένων, οι παραγωγοί τεχνολογίας εφαρμόζουν τα κατάλληλα μέτρα και διαδικασίες για την εξασφάλιση της προστασίας δεδομένων κατά το σχεδιασμό

- Υβριδική προσέγγιση: Το Συμβούλιο έχει τοποθετηθεί πρόσφατα κάπου ενδιάμεσα. Η έκθεσή της απευθύνεται άμεσα στην ανάγκη για τους παραγωγούς τεχνολογίας να λαμβάνουν μέτρα προστασίας από τα σχεδιαστικά μέτρα, αλλά δεν την διατυπώνει ως άμεση υποχρέωση. Αντ 'αυτού, προβλέπει ότι οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη το δικαίωμα προστασίας των δεδομένων.

3.5.3.2 Κυρώσεις (Sanctions)

Η πολύ πιο αυστηρή προσέγγιση των κυρώσεων για μη συμμόρφωση με τον προτεινόμενο κανονισμό για την προστασία των δεδομένων αναμένεται, κατ 'αρχήν, να αποτελέσει σημαντικό κίνητρο για την εφαρμογή της προστασίας δεδομένων από το σχεδιασμό. Για την ορθή εφαρμογή δύο τύπων κυρώσεων μπορεί να συμβεί:

- Οι αρχές προστασίας δεδομένων θα έχουν το δικαίωμα να επιβάλλουν ειδικές διοικητικές κυρώσεις, το ύψος των οποίων εκτιμάται ότι είναι πολύ υψηλότερο από ότι στην περίπτωση της οδηγίας 46/1995 /EC για την προστασία των δεδομένων. Λαμβάνοντας ως αναφορά το κείμενο που ενέκρινε το Κοινοβούλιο τον Μάρτιο του 2014. Στο κείμενο αυτό, το άρθρο 79 παράγραφος 2α προβλέπει ότι τα πρόστιμα ενδέχεται να φθάνουν έως και τα 100.000.000 ευρώ ή μέχρι και το 5% του ετήσιου παγκόσμιου τζίρου σε επιχείρησης. Αυτό είναι πολύ αυστηρότερο σε σχέση με το πρώτο σχέδιο της Επιτροπής, το οποίο πρότεινε 2% του ετήσιου παγκόσμιου τζίρου και 10.000.000 ευρώ στο άρθρο 79 παράγραφος 6. Το γεγονός ότι το ποσό των προστίμων αυξάνεται σημαντικά , θα ενθαρρύνει σίγουρα τη συμμόρφωση με το άρθρο 23.

- Η τελευταία έκθεση του Συμβουλίου παρέχει επίσης τη δυνατότητα στα κράτη μέλη να θεσπίσουν κανόνες που επιβάλλουν ποινικές κυρώσεις για παραβάσεις του κανονισμού, εφόσον τηρείται η αρχή «κανείς δεν διώκεται, ούτε τιμωρείται ποινικά δις για το ίδιο αδίκημα»

Περαιτέρω, ένα άλλο κίνητρο για την εφαρμογή της Προστασίας Προσωπικών Δεδομένων Σχεδιασμένο μπορεί να αφορά τη διαδικασία διαμόρφωσης διοικητικών προστίμων για παραβάσεις προστασίας δεδομένων (άρθρο 79 παράγραφος 2ε). Η σαφής πρόθεση του νομοθέτη να επιβραβεύσει τους υπευθύνους επεξεργασίας δεδομένων για μέτρα προστασίας δεδομένων που έχουν εφαρμοστεί αναμένεται να προκαλέσει σε κάποιο βαθμό την εφαρμογή της προστασίας δεδομένων κατά το σχεδιασμό (άρθρο 79 2ε).

Προκειμένου να διασφαλιστεί η συμμόρφωση και, ενδεχομένως, να αποφευχθούν κυρώσεις, το σχέδιο κανονισμού προβλέπει περαιτέρω υποχρεώσεις. Η συμμόρφωση με τον κανονισμό για την προστασία των δεδομένων, συμπεριλαμβανομένης της πρόβλεψης για την προστασία των δεδομένων κατά το σχεδιασμό, αναμένεται να παρακολουθείται εσωτερικά με τον διορισμό ενός υπεύθυνου προστασίας δεδομένων, όπως ορίζεται στα άρθρα 35, 36, 37.Οι υπεύθυνοι προστασίας δεδομένων(Dpo) θα πρέπει να παρακολουθούν τη συμμόρφωση με τη νομοθεσία περί προστασίας δεδομένων και να αναλαμβάνουν διάφορες δραστηριότητες για την προώθηση της προστασίας των δεδομένων στην οργάνωσή τους. Η ευαισθησία του ρόλου τους αναγνωρίστηκε από το Συμβούλιο, το οποίο έλαβε μέτρα για την προώθηση της ανεξαρτησίας τους.

Έτσι δηλώνει στην έκθεσή της ότι οι υπεύθυνοι προστασίας δεδομένων θα πρέπει να προστατεύονται από την τιμωρία τους να απολύονται για λόγους άλλους πλην της καλής εκτέλεσης των καθηκόντων συμμόρφωσης στον τομέα της προστασίας δεδομένων (άρθρο 36 παράγραφος 3, άρθρο 35 παράγραφος 7). Παρόλα αυτά, μολονότι ο κανονισμός προφανώς προσπαθεί να αποφύγει καταστάσεις σύγκρουσης συμφερόντων (άρθρο 36 παράγραφος 4), θα πρέπει να σημειωθεί ότι τέτοιες φιλοδοξίες φαίνονται αρκετά φιλόδοξες και αμφισβητείται σε ποιο βαθμό θα υλοποιηθεί η ιδέα των εντελώς ανεξάρτητων υπευθύνων προστασίας δεδομένων.

3.5.4 Περιορισμοί της αρχής σε σχέση με τις νομικές υποχρεώσεις διατήρησης ή αποκάλυψης προσωπικών δεδομένων.

Η εφαρμογή των αρχών προστασίας δεδομένων από το σχεδιασμό και από προεπιλογή αναμένεται να βοηθήσει τους υπεύθυνους επεξεργασίας δεδομένων να συμμορφωθούν με τις αρχές προστασίας δεδομένων, όπως η ελαχιστοποίηση των δεδομένων

Όπως προαναφέρθηκε, η προστασία των δεδομένων σχεδιάστηκε αρχικά από την ελαχιστοποίηση των δεδομένων, η οποία απαιτεί το επίπεδο των προσωπικών δεδομένων που πρέπει να υποβάλλονται σε επεξεργασία θα πρέπει να είναι το ελάχιστο δυνατό (άρθρο 6 παράγραφος 1γ Οδηγία για την προστασία των δεδομένων) και από την ασφάλεια των δεδομένων, η οποία απαιτεί από τον υπεύθυνο επεξεργασίας δεδομένων να λάβει τεχνικά και οργανωτικά μέτρα για να εξασφαλίσει ένα επίπεδο ασφάλειας κατάλληλο για τους κινδύνους που αντιπροσωπεύεται από την επεξεργασία και τη φύση των δεδομένων που πρέπει να προστατευθούν (άρθρο 17 παράγραφος 1 της οδηγίας για την προστασία των δεδομένων). Καθώς αναπτύχθηκε η έννοια, κρίθηκε σκόπιμο να συμβάλει στην εφαρμογή των αρχών που συνδέονται στενότερα με το δικαίωμα των χρηστών, όπως είναι η διαφάνεια, η πρόσβαση και η υπευθυνότητα.

Ωστόσο, οι τεχνολογίες PbD που προσπαθούν να επιβάλουν αυτές τις αρχές αντιμετωπίζουν συχνά αντικρουόμενες απαιτήσεις που απορρέουν από τις νομικές υποχρεώσεις που επιβάλλουν τη διατήρηση δεδομένων ή τη δευτερογενή χρήση προσωπικών δεδομένων. Η κατάσταση αυτή αναφέρεται στις εγγενείς δυσκολίες που απορρέουν από το γεγονός ότι το δικαίωμα στην ιδιωτική ζωή και το δικαίωμα στην προστασία των δεδομένων δεν είναι απόλυτα δικαιώματα και, ως εκ τούτου, η προστασία που παρέχεται ενδέχεται να πρέπει να εξισορροπηθεί με άλλα ανταγωνιστικά συμφέροντα, όπως η ανάγκη διασφάλισης της δημόσιας ασφάλειας ή τα νόμιμα συμφέροντα και τα δικαιώματα των άλλων.

Οι παρεμβάσεις στα δύο δικαιώματα μπορούν να δικαιολογηθούν βάσει του Ευρωπαϊκού Χάρτη των Θεμελιωδών Δικαιωμάτων και της οδηγίας για την προστασία των δεδομένων, αλλά υπό αυστηρές προϋποθέσεις. Πρέπει να αξιολογούνται πάντοτε ανάλογα με την αναγκαιότητα και την αναλογικότητα. Ένα παράδειγμα νομοθεσίας που μπορεί να δημιουργήσει παρεμβάσεις στα δικαιώματα της ιδιωτικής ζωής και της προστασίας δεδομένων μπορεί να βρεθεί στους νόμους που επιβάλλουν στους παρόχους υπηρεσιών Διαδικτύου (ISP) να διατηρούν δεδομένα κίνησης και θέσης για περαιτέρω πρόσβαση από αρχές επιβολής του νόμου, υποχρέωση που αρχικά προέκυψε από την οδηγία περί διατήρησης δεδομένων33. Για λόγους εθνικής ασφάλειας, η οδηγία απαιτούσε από τους φορείς εκμετάλλευσης να διατηρούν ορισμένες κατηγορίες δεδομένων για περίοδο μεταξύ έξι μηνών και δύο ετών. Αυτά τα δεδομένα ήταν δεδομένα κίνησης και τοποθεσίας και δεν περιλάμβαναν περιεχόμενο επικοινωνίας. Τα δεδομένα θα μπορούσαν να διατεθούν, κατόπιν αιτήματος, στις αρχές επιβολής του νόμου για τους σκοπούς της διερεύνησης, της ανίχνευσης και της δίωξης σοβαρών εγκλημάτων και τρομοκρατίας.

Τα δεδομένα που πρέπει να τίθενται στη διάθεση των αρχών επιβολής του νόμου επιτρέπουν την ταυτοποίηση προσώπου με το οποίο ο συνδρομητής ή ο εγγεγραμμένος χρήστης έχει κοινοποιήσει και με ποιο τρόπο προσδιορίζει την ώρα της επικοινωνίας καθώς και τον τόπο από τον οποίο πραγματοποιήθηκε η επικοινωνία αυτή και πληροφορίες σχετικά με τη συχνότητα των επικοινωνιών του συνδρομητή ή του εγγεγραμμένου χρήστη με συγκεκριμένα πρόσωπα κατά τη διάρκεια μιας δεδομένης περιόδου. Η υποχρέωση διατήρησης δεδομένων που επιβάλλεται στους προμηθευτές υπηρεσιών διαδικτύου(Internet service provider - ISP)αποτελεί ένα παράδειγμα των πιθανών εμποδίων για την αυστηρή εφαρμογή της αρχής της ποιότητας των δεδομένων (τα δεδομένα που παράγονται από μια ανακοίνωση δεν μπορούν να διαγραφούν τη στιγμή που δεν είναι πλέον απαραίτητα) και την αρχή των προδιαγραφών του σκοπού (τα δεδομένα που παράγονται στο πλαίσιο μιας εμπορικής συναλλαγής μοιράζονται περαιτέρω με τις αρχές επιβολής του νόμου).

Ένα άλλο παράδειγμα που μπορεί να βρεθεί στον Κώδικα Συνόρων του Σένγκεν απαιτεί τον έλεγχο των διαβατηρίων και των προσώπων. «Όλα τα πρόσωπα υποβάλλονται σε έναν ελάχιστο έλεγχο προκειμένου να διαπιστώνουν την ταυτότητά τους με βάση την προσκόμιση των ταξιδιωτικών τους εγγράφων» (άρθρο 7 παράγραφος 2). Στον παραδοσιακό έλεγχο των συνόρων, η διάταξη αυτή θα απαιτούσε την ταυτοποίηση όλων των επιβατών από τις συνοριακές αρχές με βάση την παρουσία τους στο σημείο διέλευσης των συνόρων και το ταξιδιωτικό τους έγγραφο. Η καθιέρωση ταυτότητας σε EU/EEA/CH θα περιλαμβάνει ελάχιστες πληροφορίες σχετικά με το αν επιτρέπεται στον ταξιδιώτη να εισέλθει στα σύνορα του Σένγκεν και συγκεκριμένα εάν ο ταξιδιώτης έχει την ιθαγένεια της ΕΕ, εάν διαθέτει έγκυρο και αυθεντικό ταξιδιωτικό έγγραφο, το οποίο δεν έχει χαθεί, κλαπεί ή υπεξαιρεθεί. Επιπλέον, όπου είναι απαραίτητο, οι αρχές των συνόρων μπορούν να διενεργούν περισσότερους ελέγχους στους επιβάτες με μη συστηματικό τρόπο. Αυτοί οι έλεγχοι μπορούν να περιλαμβάνουν περισσότερα δεδομένα προσωπικού χαρακτήρα καθώς και διαβουλεύσεις με εθνικές και ευρωπαϊκές βάσεις δεδομένων, προκειμένου να διασφαλιστεί ότι οι επιβάτες δεν αποτελούν απειλή για το κράτος μέλος.

Οι απαιτήσεις του κώδικα συνόρων του Σένγκεν για τους ανωτέρω ελέγχους καθώς και η ορθολογική εξάντληση όλων των δυνατών τρόπων ανακαλύψεως πληροφοριών για ύποπτους επιβάτες είναι προφανώς αντίθετες προς την έννοια της προστασίας των δεδομένων κατά το σχεδιασμό (DPbD). Για λόγους ασφάλειας των συνόρων, η οδηγία για την προστασία των δεδομένων επιτρέπει την άρση ορισμένων διατάξεων, όπως η διαφάνεια. Αυτό, ωστόσο, δεν σημαίνει ότι ο υπεύθυνος επεξεργασίας δεδομένων (data controller) λαμβάνει γενική εξουσιοδότηση για την επεξεργασία προσωπικών δεδομένων. οι επιβάτες δεν μπορούν να τεθούν υπό γενικό καθεστώς υποψίας, αλλά όλες οι περιπτώσεις πρέπει να αντιμετωπίζονται βάσει της αναλογικότητας.

3.6 Περιορισμοί της τρέχουσας τεχνολογίας (Gaps in technologies and development methods)

Στο κεφάλαιο αυτό εξετάζουμε και συζητούμε τους περιορισμούς της τρέχουσας τεχνολογίας όσον αφορά τις τεχνολογίες και τις μεθόδους ανάπτυξης. Διακρίνουμε δύο κατηγορίες τεχνικών: τις τεχνικές διαχείρισης δεδομένων προσωπικού χαρακτήρα (personal data management) και τις τεχνικές ελαχιστοποίησης των δεδομένων(data minimization). Τα χάσματα στις τεχνικές περιλαμβάνουν όχι μόνο περιορισμούς όσον αφορά τις λειτουργικότητες αλλά και πιθανές κυρώσεις όσον αφορά τις επιδόσεις, τη χρηστικότητα ή γενικότερα δυνατότητα ανάπτυξης. Τα κενά στις αναπτυξιακές μεθόδους είναι οριζόντια και ενδέχεται να εμποδίσουν την υιοθέτηση των τεχνικών ανεξαρτήτως των αποτελεσματικών οφελών τους.

3.6.1 Κενά στις τεχνολογίες διαχείρισης προσωπικών δεδομένων (Gaps in technologies for personal data management)

Οι τεχνικές διαχείρισης προσωπικών δεδομένων είναι χρήσιμες όταν τα άτομα πρέπει ή αποφασίσουν να αποκαλύψουν προσωπικά τους δεδομένα. Σε τέτοιες καταστάσεις, θα πρέπει να είναι ακόμη σε θέση να διατηρούν τον έλεγχο (ή μια μορφή ελέγχου) πάνω στα προσωπικά τους δεδομένα. Οι τεχνολογίες μπορούν να τους βοηθήσουν να επιβάλουν τα δικαιώματά τους με τρεις τρόπους:

- Πριν λάβουν την απόφασή τους, παρέχοντας επαρκείς πληροφορίες για να διασφαλιστεί ότι η απόφαση αυτή είναι καλά ενημερωμένη.

- Όταν λαμβάνουν την απόφασή τους, παρέχοντάς τους έναν τρόπο να εκφράσουν αυτή την απόφαση χωρίς αμφιβολία (και να διασφαλίσουν ότι τα προσωπικά δεδομένα αποκαλύπτονται για συγκεκριμένο σκοπό).

- Μετά τη γνωστοποίηση, ώστε να είναι δυνατή η επαλήθευση ότι τα προσωπικά τους δεδομένα έχουν χρησιμοποιηθεί με τον κατάλληλο τρόπο από τον υπεύθυνο επεξεργασίας δεδομένων.

Εν συνέχεια, αναλύουμε τα κενά σε καθεμία από αυτές τις κατηγορίες τεχνικών πριν συζητήσουμε τους γενικούς περιορισμούς της προσέγγισης "διαχείριση προσωπικών δεδομένων".

3.6.1.1 Περιορισμοί των εργαλείων πληροφόρησης (Limitations of information tools)

Σε γενικές γραμμές, τα εργαλεία πληροφόρησης θα πρέπει να θέτουν τα υποκείμενα σε μια θέση στην οποία θα μπορούν να παρέχουν μια νόμιμα έγκυρη και ενημερωμένη συγκατάθεση. Η συγκατάθεση ορίζεται στο GDPR ως "κάθε ελεύθερη, συγκεκριμένη, ενημερωμένη και ρητή ένδειξη της επιθυμίας του, με την οποία το υποκείμενο των δεδομένων, είτε με δήλωση είτε με σαφή καταφατική ενέργεια, συμφωνεί με την επεξεργασία των προσωπικών δεδομένων που σχετίζονται με αυτά."[20]. Η πρώτη οικογένεια εργαλείων αυτής της κατηγορίας είναι οι "τεχνολογίες ενίσχυσης της διαφάνειας", οι οποίες περιλαμβάνουν, για παράδειγμα, εικονίδια ιδιωτικού απορρήτου, πίνακες ελέγχου ή ειδικές διασυνδέσεις για κοινωνικά δίκτυα. Συνήθως, οι πίνακες ελέγχου ενημερώνουν τους χρήστες σχετικά με τα αποθηκευμένα προσωπικά δεδομένα και ποια τρίτα μέρη μπορούν να έχουν πρόσβαση σε αυτά. Αλλά αυτό το είδος του ιστότοπου πρέπει να έχει πολύ προσεκτικά σχεδιασμένες διεπαφές για να εξασφαλίσει ότι δεν παραπλανούν τους χρήστες[21]. Για παράδειγμα, οι Lederer εντοπίζει πέντε παγίδες για τους σχεδιαστές:

- Δυσνόητη πιθανή ροή πληροφοριών
- Δυσνόητη πραγματική ροής πληροφοριών
- Έμφαση στη ρύθμιση παραμέτρων κατά τη δράση
- Έλλειψη ελέγχου άσεμνου λεξιλογίου
- Περιορισμός της υπάρχουσας πρακτικής

Δείχνουν επίσης ότι τα υπάρχοντα συστήματα πέφτουν σε αυτές τις παγίδες ή απλά της αποφεύγει. Οι πίνακες ελέγχου παρουσιάζουν επίσης σημαντικές αδυναμίες ως εργαλεία πληροφόρησης:

- Είναι συνήθως αφιερωμένες σε συγκεκριμένες υπηρεσίες και ως εκ τούτου δεν μπορούν να παρέχουν στους χρήστες την παγκόσμια και πιστή αναπαράσταση όλων των προσωπικών δεδομένων που έχουν αποκαλύψει.

- Απαιτούν μια μορφή ελέγχου ταυτότητας που να εμποδίζει τους χρήστες να τα χρησιμοποιούν ανώνυμα.

20 Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (κανονισμός για την προστασία των γενικών δεδομένων), ο οποίος ψηφίστηκε από το Ευρωπαϊκό Κοινοβούλιο στις 12 Μαρτίου 2014.

21 Ο Πίνακας ελέγχου Google παρέχει αυτή τη δυνατότητα, αλλά εμφανίζει μόνο ένα υποσύνολο των δεδομένων που συλλέγονται, τα οποία ενδέχεται να είναι παραπλανητικά για τον χρήστη.

- Είναι υπό τον έλεγχο του χειριστή (ή του υπεύθυνου επεξεργασίας) ο οποίος μπορεί να αποφασίσει να παράσχει μόνο μερικές πληροφορίες σχετικά με τα δεδομένα(ο πίνακας εργαλείων Google αποτελεί μια απεικόνιση αυτού του περιορισμού).

Ένα αντίθετο παράδειγμα είναι το εργαλείο βελτίωσης της διαφάνειας DataTrack που αναπτύχθηκε στο πρόγραμμα PrimeLife το οποίο μπορεί να χρησιμοποιηθεί από τα άτομα στα οποία αναφέρονται τα δεδομένα για να δει όλα τα δεδομένα που έχουν αποκαλύψει σε διαφορετικές υπηρεσίες ή σε τρίτους.

Σε γενικές γραμμές, χρειάζεται περισσότερη δουλειά για την αλληλεπίδραση ανθρώπου με υπολογιστές (Human Computer Interaction - HCI) και αυτή η προσπάθεια να διεξαχθεί με διεπιστημονικό τρόπο διότι πρέπει να λαμβάνει υπόψη ένα ευρύ φάσμα παραγόντων (κοινωνικό, ψυχολογικό, τεχνικό, νομικό κ.λπ.). Για παράδειγμα, έχει δείξει ότι οι χρήστες δυσκολεύονται να διαφοροποιήσουν την πλευρά του χρήστη και τις υπηρεσίες, γεγονός που δυσκολεύει να κατανοήσουν τις συνέπειες των πληροφοριών του πίνακα ελέγχου.

Υπάρχουν και άλλοι τύποι εργαλείων που μπορούν να χρησιμοποιηθούν για την ευαισθητοποίηση του κοινού σχετικά με την προστασία της ιδιωτικής ζωής, είτε με το να δείξει στους χρήστες του Διαδικτύου τους τρόπους με τους οποίους έχουν ή μπορούν να εντοπιστούν είτε βοηθώντας τους να αναλύσουν τις πολιτικές προστασίας προσωπικών δεδομένων των ιστότοπων και να προειδοποιήσουν τα ζευγάρια τους για τους απαράδεκτους όρους που υπάρχουν τέτοιους είδους εργαλεία είναι το Lightbeam[22], το TaintDroid[23] ή το Mobilitics[24].

Αυτά τα εργαλεία είναι σίγουρα χρήσιμα και ελπίζουμε ότι θα συμβάλουν στην αύξηση της αντίληψης των χρηστών σχετικά με τους κινδύνους για την προστασία της ιδιωτικής ζωής και στην αύξηση των απαιτήσεών τους, αλλά είναι σαφώς μια μακροπρόθεσμη προσπάθεια. Μια πιο απαισιόδοξη άποψη θα μπορούσε επίσης να είναι ότι αυτό το είδος εργαλείου μπορεί να πείσει μόνο τους πεπεισμένους, διότι η εγκατάστασή τους και η ανάλυση των αποτελεσμάτων τους απαιτεί ήδη κάποια

22 Το Lightbeam είναι ένα πρόσθετο του Firefox που καταγράφει τα συμβάντα που σχετίζονται με τους ιστότοπους που επισκέπτονται και επιτρέπει στους χρήστες να εμφανίζουν ένα γράφημα που εμφανίζει τους ιστότοπους παρακολούθησης και τις αλληλεπιδράσεις τουςhttp: //www.mozilla.org/en-US/lightbeam

23 Το TaintDroid είναι μια επέκταση του λειτουργικού συστήματος Android που παρακολουθεί τη ροή των προσωπικών πληροφοριών μέσω εφαρμογών τρίτων, οι οποίες μπορούν να χρησιμοποιηθούν για τον εντοπισμό εσφαλμένων εφαρμογών

24 Η Mobilitics παρακολουθεί τα προσωπικά δεδομένα που αποστέλλονται σε τρίτους και παρέχει ένα εργαλείο απεικόνισης που εμφανίζει όλα τα προσωπικά δεδομένα που έχουν αποθηκευτεί ή αποστέλλονται από τις εφαρμογές, λαμβανομένων επίσης υπόψη των δυνητικών συγκεντρώσεων

κίνητρα και προκαταρκτικές γνώσεις ή συνειδητοποίηση σχετικά με θέματα ιδιωτικότητας.

Ένας άλλος περιορισμός των υφιστάμενων εργαλείων διαφάνειας είναι το γεγονός ότι δεν παρέχουν καμία γνώση σχετικά με τη λογική της επεξεργασίας των δεδομένων ή των αλγορίθμων που χρησιμοποιούνται για την παρακολούθηση ή τη διαφοροποίησή τους. Αυτή η "αλγοριθμική διαφάνεια" θα αποτελέσει βασικό ζήτημα με την ανάπτυξη μεγάλων δεδομένων και τη χρήση αναλυτικών στοιχείων για την υποστήριξη της εξατομίκευσης ενός αυξανόμενου αριθμού υπηρεσιών.

3.6.1.2 Περιορισμοί εργαλείων για επιλογή απορρήτου(Limitations of tools for expressing privacy choices)

Το πρώτο καλά γνωστό πλαίσιο για την έκφραση των προτιμήσεων για την προστασία της ιδιωτικής ζωής, το P3P, προτάθηκε το 2000. Από τότε η P3P έχει υποβληθεί σε ορισμένες επικρίσεις. Πρώτον, οι κατηγορίες δεδομένων που μπορούν να χρησιμοποιηθούν στο P3P είναι πολύ άκομψες σε πολλές περιπτώσεις και υποχρεώνουν τους χρήστες να αποκαλύπτουν περισσότερα δεδομένα ή να χορηγούν σε τρίτους ευρύτερα δικαιώματα από ό, τι θα ήθελαν πραγματικά. Μια άλλη κριτική που ασκήθηκε εναντίον του P3P είναι η έλλειψη σαφήνειας (ή ακόμη και παραπλανητικών) αναπαραστάσεων των πολιτικών απορρήτου[25]. Αυτό οφείλεται εν μέρει στη χρήση ασαφών όρων, στους προεπιλεγμένους κανόνες και στην πολυπλοκότητα που προκαλεί ο συνδυασμός κανόνων. Η έλλειψη σαφήνειας μπορεί να καταστρέψει ολόκληρη την προσέγγιση, διότι, όπως αναφέρεται στο GDPR, η συγκατάθεση πρέπει να είναι ελεύθερη, ειδική, ενημερωμένη και ρητή.

Τα κοινωνικά δίκτυα είναι ένα άλλο πλαίσιο στο οποίο τα θέματα διαδραματίζουν βασικό ρόλο στην προστασία της ιδιωτικής τους ζωής. Στην πράξη, ο ορισμός των ρυθμίσεων για την προστασία της ιδιωτικής ζωής σε ένα κοινωνικό δίκτυο αποτελεί από μόνο του ένα δύσκολο έργο λόγω της ποικιλίας των εμπλεκόμενων φορέων, της ποικιλίας των λειτουργιών αυτών των συστημάτων και του εγγενούς σκοπού τους, επιτρέποντας στους χρήστες να ανταλλάσσουν πληροφορίες με άλλους.

Ως παράδειγμα, ένας χρήστης του Facebook μπορεί να ορίσει μεταξύ πολλών άλλων παραμέτρων όπως "ποιος μπορεί να δει το προφίλ μου στις αναζητήσεις στο διαδίκτυο", "ποιος μπορεί να δει τις μελλοντικές αναρτήσεις μου", "ποιος μπορεί να δημοσιεύει στο προφίλ μου", "ποιος μπορεί να στείλει αιτήματα φιλίας ", κλπ .; Για να ορίσετε αυτές τις παραμέτρους, οι χρήστες μπορούν να χρησιμοποιήσουν τέσσερις

25 Μπορούν να χρησιμοποιηθούν για να καθορίσουν κανόνες, με μια γενικότερη έννοια, για παράδειγμα το CI εφαρμόστηκε στην HIPPA (Νόμος περί φορητότητας και λογοδοσίας ασφάλισης υγείας), COPPA (νόμος για την προστασία της ιδιωτικής ζωής των παιδιών στο διαδίκτυο) και GLBA (Gramm-Leach-Bliley Act).

προκαθορισμένες ομάδες: όλες (δημόσιες), φίλους, φίλους φίλων και κανείς (μόνο εμένα) ή να ορίσουν συγκεκριμένες (προσαρμοσμένες) ομάδες φίλων[26]. Η παραπάνω λίστα είναι ένα μικρό δείγμα των δυνατοτήτων που προσφέρει το Facebook. Στην πραγματικότητα, η πολυπλοκότητα του ορισμού των πολιτικών απορρήτου του Facebook είναι τέτοια που έχει δημιουργήσει αφιερωμένες υπηρεσίες που βοηθούν τους χρήστες να κατανοήσουν και να διορθώσουν τις ρυθμίσεις απορρήτου τους.

Επειδή η έννοια μιας παραμέτρου απορρήτου δεν είναι πάντοτε προφανής και η επίδραση του συνδυασμού τους είναι δύσκολο να κατανοηθεί, διεξήχθη ερευνητική εργασία για την παροχή επίσημων μοντέλων πολιτικών απορρήτου κοινωνικής δικτύωσης. Αυτός ο τύπος μοντέλων, ο οποίος γενικεύει το πρότυπο ελέγχου πρόσβασης, μπορεί να χρησιμοποιηθεί όχι μόνο για την καλύτερη κατανόηση του αποτελέσματος μιας πολιτικής αλλά και για τη διερεύνηση εναλλακτικών επιλογών που δεν υποστηρίζονται απαραίτητα από υπάρχοντα κοινωνικά δίκτυα, αλλά μπορεί να αποδειχθούν χρήσιμες.

Τέλος, πρέπει να τονιστεί ότι για τα κοινωνικά δίκτυα όπως το Facebook, ο αντίκτυπος της επιλογής των ρυθμίσεων απορρήτου περιορίζεται στην προστασία των χρηστών σε σχέση με άλλους χρήστες και όχι σε σχέση με την ίδια την εταιρεία Facebook. Για παράδειγμα, σύμφωνα με την πολιτική απορρήτου, το Facebook διατηρεί το δικαίωμα να χρησιμοποιεί τα προσωπικά δεδομένα των χρηστών του για να προβάλει διαφημίσεις και να μετρήσει την αποτελεσματικότητά τους, να παρέχει υπηρεσίες βάσει τοποθεσίας, να κάνει προτάσεις και να προσφέρει καινοτόμα χαρακτηριστικά και υπηρεσίες που θα αναπτύξει μελλοντικά. Επιπλέον, το Facebook μπορεί να αλλάξει τους όρους του και η συνεχής χρήση της υπηρεσίας μετά από αλλαγές στους όρους αποτελεί αποδοχή των τροποποιημένων όρων.

Άλλα παραδείγματα συγκεκριμένων εργαλείων ή υπηρεσιών που επιτρέπουν στους χρήστες να διαχειρίζονται από μόνοι τους την προστασία της ιδιωτικής τους ζωής περιλαμβάνουν αποκλεισμό διαφημίσεων και αποκλεισμό αναδυόμενων παραθύρων από προγράμματα περιήγησης. Για παράδειγμα, το Adblock Plus[27], μια ευρέως χρησιμοποιούμενη επέκταση του προγράμματος περιήγησης, αποκλείει ορισμένα αιτήματα και αποκρύπτει αυτόματα ορισμένα κείμενα όπως οι διαφημίσεις στη σελίδα που εμφανίζεται στον χρήστη. Ο χρήστης μπορεί να ορίσει φίλτρα για να αποφασίσει ποιες πληροφορίες θα πρέπει να αποκρύπτονται.

26 Ωστόσο, οι χρήστες πρέπει να είναι προσεκτικοί σχετικά με τη χρήση αυτών των ομάδων, δεδομένου ότι είναι δυναμικοί από τη φύση τους: τα δικαιώματα που παρέχονται σε μια ομάδα όπως οι φίλοι φίλων σε μια δεδομένη στιγμή ενδέχεται να μην είναι πλέον κατάλληλα ένα χρόνο μετά (επειδή το μέγεθος της ομάδας μπορεί έχουν αυξηθεί δραματικά).

27 https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/

Τα εργαλεία θωράκισης, όπως το TrackMeNot, έχουν επίσης αρκετές αδυναμίες: καταρχήν, παράγουν πολλή πρόσθετη κίνηση που οδηγεί σε σπατάλη εύρους ζώνης δικτύου. Η αποτελεσματικότητά τους έχει επίσης τεθεί υπό αμφισβήτηση, καθώς βασίζεται εξ ολοκλήρου στη τυχαιοποίηση των παραγόμενων ερωτημάτων (και του χρόνου τους) και κάθε αδυναμία αυτής της διαδικασίας θα μπορούσε να καταστήσει τους χρήστες εύκολα αναγνωρίσιμους.

3.6.1.3 Γενικοί περιορισμοί της προσέγγισης διαχείρισης προσωπικών δεδομένων (General limitations of the personal data management approach)

Αφού αποκαλύψουν τα προσωπικά δεδομένα σε τρίτους, τα άτομα δεν μπορούν να έχουν καμία απόλυτη εγγύηση ότι τα δεδομένα τους θα χρησιμοποιηθούν όπως αναμένεται (σύμφωνα με το νόμο και τους συγκεκριμένους όρους που ενδεχομένως εκφράζονται μέσω μιας πολιτικής απορρήτου). Εξετάζοντας αυτόν τον περιορισμό, θα πρέπει να έχουν τη δυνατότητα να ελέγχουν με τον ένα ή τον άλλο τρόπο τη συμπεριφορά των ελεγκτών δεδομένων

Η λογοδοσία αυξάνεται με τα τελευταία χρόνια ως λύση για την άμβλυνση αυτής της απώλειας ελέγχου. Σε γενικές γραμμές, η λογοδοσία μπορεί να λάβει χώρα σε διάφορα στάδια, οδηγώντας σε διαφορετικά είδη αποδεικτικών στοιχείων (λογοδοσία της πολιτικής, λογοδοσία των διαδικασιών και λογοδοσία της πρακτικής). Ωστόσο, η λογοδοσία δεν είναι αρχή που λαμβάνει ομόφωνη υποστήριξη. Από την τεχνική πλευρά, η ίδια η εφαρμογή των μέτρων λογοδοσίας ενδέχεται να εισάγει περαιτέρω κινδύνους παραβίασης των προσωπικών δεδομένων, διότι ενδέχεται να οδηγήσει στην αποθήκευση πρόσθετων προσωπικών δεδομένων σε ημερολόγια ελέγχου.

Ωστόσο, έχει αποδειχθεί ότι ο προσεκτικός σχεδιασμός μπορεί να ελαχιστοποιήσει αυτόν τον κίνδυνο. Από τη νομική πλευρά, ο πολλαπλός χαρακτήρας της λογοδοσίας, σε συνδυασμό με τους ασαφείς ορισμούς σε νομικά μέσα, μπορεί να οδηγήσει ορισμένους υπεύθυνους επεξεργασίας δεδομένων να προωθήσουν την υπευθυνότητα, με την ελπίδα να αποφευχθούν πιο περιοριστικοί και περιεκτικοί κανονισμοί. Για το λόγο αυτό, η λογοδοσία έχει επικριθεί επειδή προσφέρει στις εταιρείες μια φτηνή φήμη "προστασίας δεδομένων", ακόμη και αν οι πρακτικές τους και οι κανόνες περί ευθύνης τους προσφέρουν πραγματικά περιορισμένες εγγυήσεις ιδιωτικότητας.

Γενικότερα, η λογοδοσία συχνά συνδέεται με την αυτορρύθμιση, η οποία είναι μια αμφιλεγόμενη προσέγγιση. Τα κυριότερα οφέλη της αυτορρύθμισης είναι η ευελιξία και η ευρύτερη αποδοχή της στη βιομηχανία: επειδή οι κανόνες μπορούν να προσαρμοστούν σε δεδομένο επιχειρηματικό τομέα και να ελέγχονται από τους ενδιαφερόμενους φορείς, οι παράγοντες αυτοί είναι πιθανότερο να τους ακολουθήσουν. Γενικότερα, λαμβάνοντας υπόψη τη δυσκολία ρύθμισης του Διαδικτύου στο διεθνές πλαίσιο, η αυτορρύθμιση συχνά παρουσιάζεται ως μια

κατάλληλη λύση για την αντιμετώπιση της «αποσύνθεσης των παραδοσιακών μοντέλων κυριαρχίας». Ωστόσο, το κύρος της αυτορρύθμισης ως κανόνα πρέπει να αξιολογείται με βάση παραδοσιακά κριτήρια όπως η νομιμότητα των δημιουργών της, η συμμόρφωση του περιεχομένου της σε σχέση με άλλους νομικούς κανόνες και η αποτελεσματικότητά της, συμπεριλαμβανομένης της δυνατότητας κυρώσεων. Στο πλαίσιο της λογοδοσίας, θα μπορούσε κανείς να υποστηρίξει ότι το δεύτερο κριτήριο πρέπει γενικά να ικανοποιηθεί, αλλά ο πρώτος δεν ικανοποιείται, εκτός εάν τα δεδομένα η αρχή προστασίας προστατεύει επίσημα τους κανόνες, ούτε γενικά η τελευταία. Θα πρέπει να είναι σαφές ότι η έλλειψη πραγματικών συνεπειών για τον υπεύθυνο επεξεργασίας δεδομένων που παραβιάζει τον κώδικα ή η έλλειψη αποτελεσματικού ελέγχου θα εξασθένιζε σοβαρά τη διαβεβαίωση που παρέχεται από αυτορρυθμιζόμενα συστήματα λογοδοσίας

3.6.2 Τεχνικά κενά που υπάρχουν στις τεχνολογίες διατήρησης της ιδιωτικής ζωής (GAPS in privacy - preserving technologies for data minimization)

Σε αυτή την ενότητα θα αναλύσουμε τα τεχνικά κενά που υπάρχουν στις τεχνολογίες διατήρησης της ιδιωτικής ζωής που εμποδίζουν ή τουλάχιστον ελαχιστοποιούν την αποκάλυψη προσωπικών πληροφοριών σε μη αξιόπιστους τρίτους που εμπλέκονται σε συστήματα ICT.

3.6.2.1 Κρυπτογράφηση από άκρο σε άκρο (End-to-end encryption)

Η κρυπτογράφηση από άκρο σε άκρο προστατεύει την εμπιστευτικότητα των δεδομένων από τον εντολέα στον προορισμό, δηλαδή το περιεχόμενο των μηνυμάτων δεν είναι διαθέσιμο στο χειριστή δικτύου ή στους ενδιάμεσους διακομιστές (π.χ., ηλεκτρονικό ταχυδρομείο ή παροχέας υπηρεσιών άμεσων μηνυμάτων).

Επιθυμητή κατάσταση:

Στην ιδανική περίπτωση, η κρυπτογράφηση από άκρο σε άκρο πρέπει να είναι διαφανής για τους χρήστες. Δεν πρέπει να απαιτεί πρόσθετες αλληλεπιδράσεις, ούτε να επηρεάζει τη λειτουργικότητα ή την απόδοση του συστήματος.

Τρέχουσα κατάσταση:

Κρυπτογράφηση από άκρο σε άκρο είναι διαθέσιμη προς το παρόν στις ακόλουθες περιπτώσεις:

- **Email**: για παράδειγμα Enigma[28], ένα plugin αρκετά καλό κρυπτογράφησης (PGP) διαθέσιμο για email δημοφιλή προγράμματα ηλεκτρονικού ταχυδρομείου όπως το Thunderbird[29] ή το SeaMonkey[30]. Το PGP χρησιμοποιείται επίσης στο "End-to-End[31]" μια επέκταση του Chrome που κυκλοφορεί από την Google για την παροχή κρυπτογραφημένης περιγραφής των περιεχομένων των μηνυμάτων στο Gmail, την υπηρεσία ηλεκτρονικού ταχυδρομείου της Google.

- **Instant Messaging:** αρκετοί πελάτες IM προσφέρουν plugins για κρυπτογράφηση από το τέλος έως το τέλος και ακόμη και το Off-The-Record (το οποίο επιπλέον παρέχει μυστικότητα και εμπιστευτικότητα) υποστηρίζεται εγγενώς από μερικούς πελάτες IM ή ως plugin ή addon.

- **Η αποθήκευση Cloud**: για παράδειγμα η Wuala[32] ή η Tresorit[33] προσφέρουν κρυπτογράφηση από την πλευρά του πελάτη, όπου τα αρχεία κρυπτογραφούνται πριν αποθηκευτούν στο cloud με τέτοιο τρόπο ώστε το περιεχόμενο να μην είναι διαθέσιμο για τον παροχέα cloud.

- **Φωνητική επικοινωνία:** Τα πρωτόκολλα όπως το ZRTP επιτρέπουν στους χρήστες να μοιράζονται ένα κλειδί και να δημιουργούν μια ασφαλή φωνητική επικοινωνία στην οποία το περιεχόμενο δεν μπορεί να παρακολουθείται από άλλα μέρη παρά από αυτόν που πραγματοποιεί την κλήση και τον παραλήπτη.

Gaps:

Απόδοση:

Στις περισσότερες περιπτώσεις, ο χρόνος κρυπτογράφησης/ αποκρυπτογράφησης και η κατανάλωση είναι αμελητέος. Οι μοναδικές περιπτώσεις όπου η κρυπτογράφηση από άκρο σε άκρο επηρεάζει την εμπειρία των χρηστών είναι όταν υπάρχει μεγάλη

28 https://www.enigmail.net/
29 https://www.mozilla.org/thunderbird/
30 http://www.seamonkey-project.org/
31 https://code.google.com/p/end-to-end/
32 https://www.wuala.com/
33 https://tresorit.com

ποσότητα δεδομένων για κρυπτογράφηση (π.χ. μεγάλα συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου, ή μεγάλα αρχεία που έχουν μεταφορτωθεί στο Cloud).

Λειτουργικότητα:

Η χρήση κρυπτογράφησης από άκρο σε άκρο επιτρέπει την κανονική αποστολή και λήψη δεδομένων. Ωστόσο, μειώνουν τη λειτουργικότητα του συστήματος ή επιβάλλουν απαιτήσεις που δεν απαιτούνται όταν δεν εφαρμόζεται κρυπτογράφηση:

- Τα κρυπτογραφικά πρωτότυπα που χρησιμοποιούνται επί του παρόντος σε κρυπτογράφηση από άκρο σε άκρο εμποδίζουν την αναζήτηση λειτουργιών σε απομακρυσμένα δεδομένα στο Cloud, στον παροχέα υπηρεσιών email.
- Η κρυπτογράφηση από άκρο σε άκρο θέτει σε κίνδυνο τις εφαρμογές πολλαπλών χρηστών, πολύ συνηθισμένες στη φωνητική επικοινωνία, ακόμα και σε περιβάλλοντα Cloud (έκδοση πολλαπλών χρηστών σε αρχεία).
- Για να είναι δυνατή η εξακρίβωση της ταυτότητας των οντοτήτων με τις οποίες είναι εγκατεστημένη η επικοινωνία, οι χρήστες πρέπει να αλληλοεπιδρούν με ένα κανάλι εκτός ζώνης (δηλαδή ξεχωριστά από την εφαρμογή).

Ανάπτυξη δυνατότητας:

Ενώ οι βιβλιοθήκες κρυπτογράφησης είναι ευρέως διαθέσιμες, ειδικά εργαλεία για την παροχή κρυπτογράφησης από άκρο σε άκρο δεν είναι διαθέσιμα για όλους τους τύπους πλατφορμών, αν και η τρέχουσα τάση δείχνει ότι σύντομα αυτό δεν θα είναι περιορισμός.

3.6.2.2 Ανώνυμο σύστημα επικοινωνίας (Anonymous communication systems)

Ένα ανώνυμο σύστημα επικοινωνίας είναι ένα σύστημα που προστατεύει τη διεύθυνση IP / MAC του χρήστη ή οποιαδήποτε άλλη μορφή αναγνωριστικού επιπέδου δικτύου από τον πάροχο δικτύου, από τους εταίρους επικοινωνίας, ακόμη και από τον ίδιο τον παροχέα υπηρεσιών ανωνυμίας.

Επιθυμητή κατάσταση:

Στην ιδανική περίπτωση, οι ανώνυμες επικοινωνίες πρέπει να είναι διαφανείς για τους χρήστες και τους παρόχους υπηρεσιών. Δεν πρέπει να απαιτεί πρόσθετες

αλληλεπιδράσεις, ούτε να επηρεάζει τη λειτουργικότητα ή την απόδοση του συστήματος.

Τρέχουσα κατάσταση:

Στην ακαδημαϊκή σφαίρα υπάρχουν πολλά ανώνυμα συστήματα επικοινωνίας, από τα οποία λίγα έχουν φτάσει σε μια ώριμη κατάσταση στην εφαρμογή τους. Οι Tor[34], I2P[35], Freenet[36] και JonDonym[37] (επίσης γνωστοί ως JAP ή AN.ON), είναι τα πιο σημαντικά παραδείγματα ανεπτυγμένων ανώνυμων δικτύων επικοινωνίας.

Gaps:

- **Απόδοση**: οι ανώνυμες επικοινωνίες έχουν μεγάλη επίδραση στην απόδοση των δραστηριοτήτων στο διαδίκτυο. Δεδομένου ότι όλα τα συστήματα βασίζονται στη μετάδοση μηνυμάτων μέσω διαφόρων αναπηδήσεων (hops), προκειμένου να κρύψουν μηνύματα ή ροές προέλευσης, κρυπτογράφησης και αποκρυπτογράφησης σε κάθε ένα από τα hop, καθώς και παράγοντες αναμονής που σχετίζονται με πρωτόκολλα μεταφοράς (transport layer), αντικατοπτρίζονται σε σημαντική καθυστέρηση στις επικοινωνίες.

- **Λειτουργικότητα:** Για να διατηρούνται οι χρήστες ανώνυμοι, πολλές υπηρεσίες πρέπει να απενεργοποιούνται (π.χ. Javascript, Flash), επειδή μπορούν να χρησιμοποιηθούν ως δευτερεύοντα κανάλια για την ανάκτηση της ταυτότητας του δημιουργού επικοινωνίας. Αυτό με τη σειρά του περιορίζει τον αριθμό των εφαρμογών που μπορούν να χρησιμοποιηθούν σε ένα ανώνυμο κανάλι επικοινωνίας.

- **Ανάπτυξη**: πολλά από τα ανώνυμα συστήματα επικοινωνίας που προτάθηκαν στη βιβλιογραφία δεν εφαρμόστηκαν ποτέ [Corr10, Nam06, Rei98] ή οι εφαρμογές τους προσαρμόστηκαν στις ανάγκες της δημοσίευσης στην οποία παρουσιάστηκαν και δεν είναι κατάλληλες για χρήση σε ρεαλιστικές εφαρμογές. Από την άλλη πλευρά, άλλα συστήματα παρέχουν εργαλεία για την

34 https://www.torproject.org/
35 https://geti2p.net
36 https://freenetproject.org/
37 http://anonymous-proxy-servers.net/

ενσωμάτωση ανώνυμων επικοινωνιών στις αναπτύξεις, όπως οι βιβλιοθήκες και τα plugins που προσφέρονται από το Tor ή το I2P

3.6.2.3 Κρυπτογραφικά πρωτόκολλα για τη διατήρηση της ιδιωτικής ζωής (Privacy-preserving cryptographic protocols)

Τα κρυπτογραφικά πρωτόκολλα που προστατεύουν την ιδιωτική ζωή είναι κρυπτογραφικές λειτουργίες που έχουν σχεδιαστεί για να παρέχουν μια δεδομένη λειτουργικότητα διατηρώντας παράλληλα την ιδιωτική ζωή ακόμη και με την παρουσία αντιφατικών συμμετεχόντων που προσπαθούν να συλλέξουν πληροφορίες σχετικά με τις εισόδους ομότιμων (peers).

Επιθυμητή κατάσταση:

Στην ιδανική περίπτωση, τα κρυπτογραφικά πρωτόκολλα για την προστασία της ιδιωτικής ζωής θα πρέπει να είναι διαφανή για τους χρήστες και να έχουν ελάχιστη επίδραση στην πλευρά του διακομιστή. Επιπλέον, δεν θα πρέπει να απαιτούνται επιπλέον αλληλεπιδράσεις, ούτε να επηρεάζουν τη λειτουργικότητα ή την απόδοση του συστήματος.

Τρέχουσα κατάσταση:

Ανώνυμος έλεγχος ταυτότητας (ανώνυμα διαπιστευτήρια): Ένα ανώνυμο πρωτόκολλο ελέγχου ταυτότητας επιτρέπει στον κάτοχο ανώνυμης πιστοποίησης να αποδείξει επιλεκτικά ένα υποσύνολο τιμών χαρακτηριστικών σε έναν επαληθευτή, π.χ. ένας χρήστης μπορεί να αποδείξει ότι κατέχει άδεια οδήγησης ή ότι η ηλικία είναι μεγαλύτερη από 18 ετών. Ο ακαδημαϊκός κόσμος παράγει συνεχώς νέα σχήματα για ανώνυμα διαπιστευτήρια και ανώνυμα πρωτόκολλα ελέγχου ταυτότητας που προσφέρουν ευέλικτες λειτουργίες ενώ καταναλώνουν όλο και λιγότερους πόρους. Ωστόσο, προς το παρόν υπάρχουν μόνο δύο διαθέσιμες υλοποιήσεις διαπιστευτηρίων: Microsoft UProve[38] και IBM Idemix[39]. Και οι δύο έχουν κυκλοφορήσει ως open source, Idemix ως μέρος του έργου PrimeLife EU[40], και UProve με άδεια Apache[41].

Anonymous eCash: Τα ανώνυμα προγράμματα ηλεκτρονικού χρήματος επιτρέπουν την ασφαλή πληρωμή offline χωρίς να αποκαλύπτουν την ταυτότητα του πληρωτή,

38 http://research.microsoft.com/en-us/projects/u-prove/
39 http://www.zurich.ibm.com/idemix/details.html
40 https://prime.inf.tu-dresden.de/idemix/
41 https://uprovecsharp.codeplex.com/

μιμούμενοι τις ιδιότητες των παραδοσιακών μετρητών. Πολλά σχέδια για eCash έχουν προταθεί στη βιβλιογραφία και έχει αποδειχθεί ότι μπορούν να υλοποιηθούν αποτελεσματικά, π.χ., για συστήματα μεταφοράς. Επίσης, από την εμφάνιση του Bitcoin[42] το 2009, στην αγορά εμφανίστηκαν πολλά λεγόμενα κρυπτογραφικά νομίσματα (περισσότερα από 500 έως τον Νοέμβριο του 2014[43]).

Ανάκτηση ιδιωτικών πληροφοριών: αυτά τα πρωτόκολλα επιτρέπουν στους πελάτες να ανακτούν ιδιωτικά αρχεία από δημόσιες βάσεις δεδομένων χωρίς να αποκαλύπτουν το ανακτώμενο στοιχείο, ούτε καν στον κάτοχο της βάσης δεδομένων. Αυτά τα πρωτόκολλα έχουν αποδειχθεί αποτελεσματικά για πολλές εφαρμογές, για παράδειγμα, ψάχνοντας ιδιωτικά κοντινά σημεία ενδιαφέροντος και ακόμη και κατάλληλα για μεγάλες εργασίες δεδομένων.

Οι κρυπτογραφικές δεσμεύσεις: επιτρέπουν στους χρήστες να δεσμεύονται σε μια δεδομένη αξία διατηρώντας ταυτόχρονα κρυμμένο σε τρίτους, με τη δυνατότητα να αποκαλύψουν αργότερα την δεσμευμένη αξία. Οι κρυπτογραφικές δεσμεύσεις έχουν αποδειχθεί χρήσιμες για την οικοδόμηση συστημάτων διατήρησης της ιδιωτικής ζωής ή συστημάτων έξυπνης μέτρησης που προστατεύουν την ιδιωτική ζωή, επιτρέποντας στους χρήστες να δεσμεύονται ιδιωτικά για τις τιμές χρήσης με τέτοιο τρόπο ώστε να μπορεί να επαληθευτεί η καλή συμπεριφορά με βάση αυτές τις δεσμεύσεις.

Η κρυπτογράφηση με δυνατότητα αναζήτησης: επιτρέπει σε ένα συμβαλλόμενο μέρος να αναθέτει την αποθήκευση των δεδομένων του σε ένα άλλο μέρος (έναν κεντρικό υπολογιστή) με ιδιωτικό τρόπο, διατηρώντας παράλληλα τη δυνατότητα επιλεκτικής αναζήτησης σε αυτόν.

Gaps:

Απόδοση: Τα πρωτόκολλα συντήρησης της ιδιωτικής ζωής βασίζονται σε ακριβούς υπολογισμούς που έχουν ισχυρό αντίκτυπο στην απόδοση. Η επίπτωση μπορεί να έρθει υπό μορφή χρόνου υπολογισμού, απαιτήσεων αποθήκευσης ή απαιτήσεων σχετικά με το εύρος ζώνης. Για ορισμένες εφαρμογές, τα γενικά έξοδα είναι αμελητέα ή ακόμα κατάλληλα για ανάπτυξη, ενώ για άλλα γίνεται απαγορευτικό.

Λειτουργικότητα: Τα πρωτόκολλα διατήρησης της ιδιωτικής ζωής υπόσχονται ένα ευρύ φάσμα λειτουργιών. Ωστόσο, αυτή η προσφορά δεν είναι άνευ όρων και απαιτεί αλλαγές στον τρόπο σχεδιασμού των συστημάτων ICT. Οι ιδιότητες απορρήτου αυτών των πρωτοκόλλων διατηρούνται μόνο κάτω από ορισμένες υποθέσεις, ιδιαίτερα σε κάθε μία από αυτές. Τέτοιες υποθέσεις μπορεί να μην ικανοποιούνται από τα σενάρια

42 https://bitcoin.org/es/
43 https://coinmarketcap.com/

στα οποία πρέπει να ενσωματωθούν. απαιτώντας επανασχεδιασμό του συστήματος από το μηδέν προκειμένου να πληρούνται οι όροι.

Ανάπτυξη: παρόλο που υπάρχει μεγάλη βιβλιογραφία και ορισμένες βιβλιοθήκες είναι διαθέσιμες στο κοινό, η ανάπτυξη συστημάτων που ενσωματώνουν αυτά τα πρωτόκολλα διατήρησης της ιδιωτικής ζωής εξακολουθεί να είναι ένα δύσκολο έργο. Δηλαδή οι λειτουργίες που προσφέρονται από αυτά τα πρωτόκολλα διατήρησης της ιδιωτικής ζωής (privacy-preserving protocols) είναι δύσκολο να κατανοηθούν, να διαμορφωθούν και να αξιοποιηθούν σωστά από τους χρήστες, οι οποίοι, γενικά, ενδέχεται να μην έχουν προηγμένη γνώση συστημάτων ICT ή κρυπτογράφησης. Επιπλέον ακόμη και όταν είναι σε θέση να ενσωματώσουν πρωτόκολλα διατήρησης της ιδιωτικής ζωής στο σχεδιασμό, δεν μπορούν να βρουν τις κατάλληλες υλοποιήσεις ή ακόμα και η έλλειψη γνώσης για να εφαρμόσουν σωστά αυτές τις λειτουργίες.

3.6.2.4 Τεχνικές θωράκισης (Obfuscation approaches)

Οι τεχνικές θωράκισης εφαρμόζουν μετασχηματισμούς όπως η προσθήκη τυχαίου θορύβου, η μερική καταστολή των δεδομένων, η εναλλαγή δεδομένων ή οι γραμμικοί μετασχηματισμοί. Αυτές οι προσεγγίσεις στρεβλώνουν τα δεδομένα με τέτοιο τρόπο ώστε ορισμένες από τις πληροφορίες που περιέχει να κρύβονται.

Επιθυμητή κατάσταση:

θα πρέπει να είναι διαφανείς για τους χρήστες και να έχουν ελάχιστες επιπτώσεις στην πλευρά του διακομιστή. Επιπλέον, δεν πρέπει να απαιτεί επιπλέον αλληλεπιδράσεις ούτε να έχει επιπτώσεις στη λειτουργικότητα ή την απόδοση του συστήματος.

Τρέχουσα κατάσταση:

Ένας μη εξαντλητικός κατάλογος των προσεγγίσεων περί παρεμβολής είναι οι εξής:

- Η προστασία του ιδιωτικού απορρήτου στην αναζήτηση ιστού, στην οποία προστίθεται θόρυβος στις αναζητήσεις στο διαδίκτυο, προκειμένου να αποκρύπτονται οι προτιμήσεις των χρηστών και να εμποδίζεται η μηχανή

αναζήτησης να πραγματοποιεί προφίλ χρηστών. Μόνο τα TrackMeNot[44] και GooPIR[45] είναι προς το παρόν διαθέσιμα για δημόσια χρήση.

- Βάσεις δεδομένων για τη διατήρηση της ιδιωτικής ζωής: οι τεχνικές αυτές επιτρέπουν την εξωτερική ανάθεση ή τη διαβούλευση με βάσεις δεδομένων για στατιστικές μελέτες. Οι τεχνικές βασίζονται είτε στην προσθήκη θορύβου στη βάση δεδομένων είτε στην συγκάλυψη ή γενίκευση δεδομένων έτσι ώστε να μην είναι δυνατή η ταυτοποίηση των ατόμων.

- Υπηρεσίες που βασίζονται στη διατήρηση της ιδιωτικής ζωής: αυτές οι τεχνικές επιτρέπουν στους χρήστες να αναζητούν υπηρεσίες βασισμένες σε τοποθεσίες χωρίς να αποκαλύπτουν την ακριβή τους θέση. Οι προσεγγίσεις μπορούν να συνίστανται στην απόκρυψη της θέσης, την παροχή ανακριβούς ή ασαφούς θέσης ή την προσφυγή σε ανωνυμία

Gaps:

Απόδοση: Οι προσεγγίσεις αυτές είναι αποτελεσματικές στον τομέα των υπηρεσιών που βασίζονται σε τοποθεσίες ή όταν πρόκειται για την προσθήκη θορύβου σε μια βάση δεδομένων. Ωστόσο, για άλλες περιπτώσεις, όπως η ιδιωτική αναζήτηση ιστού, στην οποία η επιλογή θορύβου ακολουθεί πολύπλοκους αλγορίθμους, η παραμόρφωση μπορεί να έχει μεγάλο αντίκτυπο στην απόδοση.

Λειτουργικότητα: Η εμπλοκή προκαλεί εγγενή απώλεια ακρίβειας στην απόκριση του διακομιστή, καθώς δεν παρέχεται ποτέ το πραγματικό ακριβές ερώτημα του χρήστη. Αυτή η απώλεια μπορεί να διαγραφεί για αύξηση του εύρους ζώνης (π.χ., εάν ο θόρυβος αντικαθίσταται από ψευδείς ερωτήσεις που υπονομεύουν την πραγματική πρόθεση του χρήστη).

Ανάπτυξη: παρόλο που υπάρχει μεγάλη βιβλιογραφία που προτείνει τέτοιου είδους τεχνολογίες διατήρησης της ιδιωτικής ζωής, η ανάπτυξή τους εμποδίζεται από πολλά πρακτικά προβλήματα:

- Δεν είναι σαφές το ποσοστό της ιδιωτικής ζωής το οποίο παρέχεται από αυτά τα μέτρα προστασίας.

44 http://cs.nyu.edu/trackmenot/
45 http://unescoprivacychair.urv.cat/goopir.php

- Η χρήση της αποκρυπτογράφησης μπορεί να συνεπάγεται αλλαγές στην πλευρά του διακομιστή ώστε να είναι σε θέση να παρέχει την υπηρεσία παρουσία ανακριβών ή ασαφών πληροφοριών.

3.6.3 Κενά στις μεθόδους ανάπτυξης (Gaps in development methods)

Οι προηγούμενες ενότητες υπογράμμισαν τα κενά στις υφιστάμενες τεχνολογίες βελτίωσης της ιδιωτικής ζωής. Ωστόσο, πρέπει να αναφερθεί ότι υπάρχει ήδη ένα ευρύ φάσμα τεχνολογιών που δεν χρησιμοποιούνται τόσο πολύ όσο θα μπορούσαν. Ένας από τους λόγους αυτής της έλλειψης υιοθεσίας είναι ένας άλλος τύπος κενών: κενά στις ίδιες τις μεθόδους ανάπτυξης. Αυτό το κενό περιλαμβάνει δύο τύπους ελλείψεων:

- Πρώτον, χρειάζεται περισσότερη δουλειά για να κατανοήσουμε πώς οι υφιστάμενες αναπτυξιακές μεθοδολογίες μπορούν να προσαρμοστούν στην προστασία της ιδιωτικής ζωής από το σχεδιασμό(privacy by design).

- Επιπλέον, το Privacy by Design δημιουργεί νέες προκλήσεις και δημιουργεί ειδικές ανάγκες. Πράγματι, αρκετοί συγγραφείς έχουν ήδη επισημάνει την πολυπλοκότητα της "μηχανικής προστασίας απορρήτου" καθώς και τον "πλούτο του χώρου δεδομένων" που απαιτεί την ανάπτυξη πιο γενικών και συστηματικών μεθοδολογιών για την προστασία της ιδιωτικής ζωής από το σχεδιασμό. Όσον αφορά τους μηχανισμούς προστασίας της ιδιωτικής ζωής, δεν υπάρχει γενική μεθοδολογία που να βοηθά τους σχεδιαστές να επιλέγουν μεταξύ των υφιστάμενων τεχνικών και να τις ενσωματώνουν κατά τρόπο συνεπή ώστε να πληρούν ένα σύνολο απαιτήσεων προστασίας της ιδιωτικής ζωής. Μία πρόκληση στον τομέα αυτό είναι επομένως να υπερβούμε τις ατομικές περιπτώσεις και να δημιουργήσουμε υγιή θεμέλια και μεθοδολογίες για την προστασία της ιδιωτικής ζωής από το σχεδιασμό(PbD).

4. Security by Default

4.1 Θεμελιώδης Αρχές ώστε να δημιουργήσουμε πιο ασφαλείς εφαρμογές (Five Principles for Building More Secure Apps)

Πέρυσι, η Accenture άφησε τέσσερις αποθηκευτικούς χώρους της Amazon (AWS S3) χωρίς κωδικούς πρόσβασης, εκθέτοντας ευαίσθητα δεδομένα σχετικά με την πλατφόρμα του cloud Accenture και τους πελάτες της. Ομοίως, η MongoDB, μια δημοφιλής πλατφόρμα βάσης δεδομένων, ανακαλύφθηκε ότι είναι μη ασφαλής,

ανοίγοντας ένα διάνυσμα επίθεσης σε όλες τις εφαρμογές που την χρησιμοποιούν. Οι δύο αυτές περιπτώσεις αναφέρουν γεγονότα με προβλήματα στην ασφάλεια από αξιόπιστες εταιρείες, με αμέτρητους πελάτες και συνδέσεις, κάτι που αφήνει στους κακόβουλους ανοιχτά πεδία για να επιτεθούν.

Οι σημερινές εφαρμογές είναι αλληλένδετες και εξωτερικά προσβάσιμες. Σε παλαιότερες λύσεις λογισμικού, οι εφαρμογές απομονώνονταν στο ενδοδίκτυο της εταιρείας και υπήρχαν πίσω από ένα τείχος προστασίας (firewall). Σήμερα όμως υπάρχουν εφαρμογές στο cloud με ενσωματώσεις σε αμέτρητες άλλες υπηρεσίες βασιζόμενες σε cloud και ροές δεδομένων από μια υπηρεσία σε άλλη και από έναν χρήστη σε άλλο, δημιουργώντας ένα πλήθος επιφανειών επίθεσης.

Ακόμα και οι μεγαλύτερες εταιρίες έχουν σφάλματα και προβλήματα σε θέματα ν ασφάλειας, κάτι που δεν επηρεάζει μόνο τον εαυτό τους αλλά και του πελάτες/χρήστες τους, γι 'αυτό το λόγο η δημιουργία ασφαλών εφαρμογών πρέπει να γίνει μια βέλτιστη πρακτική. Εδώ είναι πέντε αρχές που οι προγραμματιστές πρέπει να έχουν κατά νου για να δημιουργήσουν πιο ασφαλείς εφαρμογές:

- **Principle One: Security Trumps Usability**

Τα τελευταία χρόνια, οι βέλτιστες πρακτικές σχεδιασμού λογισμικού υποστηρίζουν την απρόσκοπτη εμπειρία και τις διεπαφές των χρηστών, θυσιάζοντας την ασφάλεια στο βωμό της ευχρηστίας. Με απλά λόγια, το λογισμικό χωρίς κατάλληλες προφυλάξεις ασφαλείας είναι ευάλωτο. Για παράδειγμα είναι σαν να φτιάχνουμε ένα όμορφο σπίτι χωρίς όμως να βάλουμε κλειδαριές στην μπροστινή πόρτα, έτσι είναι και για το λογισμικό εάν δεν έχουμε ενσωματωμένη ασφάλεια.

Η ασφάλεια πρέπει να επανακτήσει τον θρόνο ως βέλτιστη πρακτική. Ανεξάρτητα από το κόστος, η χρηστικότητα πρέπει να έρχεται μετά από ασφάλεια, όχι πρώτα. Ακόμη και αν δημιουργείτε μια εφαρμογή χωρίς διακυμάνσεις του πραγματικού κόσμου, μια ανασφαλής εφαρμογή μπορεί να λειτουργήσει ως φορέας επίθεσης για έναν κακόβουλο για να αποκτήσει πρόσβαση στο σύστημα μας και να προκαλέσει ζημιές.

- **Principle Two: Secure Configurations by Default**

Το να βασιστούμε στο ότι ο τελικός χρήστης θα κάνει τις κατάλληλες ενέργειες έτσι ώστε να ρυθμίσει μια εφαρμογή κατάλληλα για να είναι ασφαλής είναι ο λόγος που έχουμε πολλά κενά ασφαλείας.

Μετά την ολοκλήρωση του λογισμικού για όλα τα είδη τελικών χρηστών, καταναλωτών, εταιρικών διαχειριστών πληροφορικής ακόμη και προγραμματιστών, λίγοι είναι αυτοί που αλλάζουν τις προεπιλογές. Μια μελέτη, σύμφωνα με την οποία μόνο το 5% των χρηστών άλλαξε τις ρυθμίσεις από προεπιλογή. Είναι μια παρόμοια ανησυχητική μάχη με το να κάνεις τους χρήστες να αλλάζουν κωδικούς πρόσβασης συχνά.

Κατά την εγκατάσταση ενός νέου λογισμικού, οι χρήστες συνήθως ακολουθούν τη διαδρομή με τη μικρότερη αντίσταση. Κάνουν το ελάχιστο για να πάρει την εφαρμογή και να τρέξει και να σταματήσει εκεί. Πολλοί προγραμματιστές υποθέτουν, λανθασμένα βέβαια , ότι μπορούν να μεταφέρουν λογισμικό με ευρύτατες ρυθμίσεις ώστε οι χρήστες να μπορούν να ρυθμίσουν αργότερα την ασφάλεια, αλλά αυτό δεν συμβαίνει ποτέ για τη συντριπτική πλειοψηφία των χρηστών είτε λόγω του ότι δεν γνωρίζουν πώς να το κάνουν ή απλά δεν το δίνουν σημασία. Έτσι λοιπόν μόλις η εφαρμογή τεθεί σε λειτουργία, η ασφάλεια δεν λαμβάνεται υπόψη.

Αυτό σημαίνει ότι η προεπιλεγμένη διαμόρφωση με την οποία το λογισμικό μεταφέρει είναι κρίσιμη και πρέπει να είναι όσο το δυνατόν πιο καλά προστατευμένη. Επιπλέον, ενδέχεται να απαιτήσετε από τους χρήστες να εκτελούν ορισμένες ρυθμίσεις πριν από την έναρξη λειτουργίας του λογισμικού. Κάθε ασφάλεια που αφήνεται στην αυτοδιάθεση του τελικού χρήστη είναι πιθανό να είναι ένα κενό ασφαλείας.

- **Principle Three: Ensure Perimeter Security**

Το σύγχρονο λογισμικό είναι περίπλοκο. Συνήθως είναι Cloud-based με αμέτρητες συνδέσεις και χρήστες. Ως εκ τούτου, τα δεδομένα προέρχονται από κάθε κατεύθυνση, τα οποία διακινούνται από διαφορετικά επίπεδα λογισμικού.Εάν η ασφάλεια χειρίζεται σε κάθε επίπεδο, τότε τα ζητήματα ασφαλείας θα εμφανιστούν. Υπό σχεδόν όλες τις συνθήκες, η περιμετρική ασφάλεια του λογισμικού θα πρέπει να επαληθεύει και να επικυρώνει όλες τις εισροές. Μόνο αν πληρούνται όλες οι συνθήκες ασφαλείας, πρέπει να αφήσει το επόμενο εσωτερικό επίπεδο να χειριστεί την είσοδο.

Σκεφτείτε αυτό το εξώτατο στρώμα ως έναν ελεγκτή ο οποίος ελέγχει την ταυτότητα (IDs) αυτού που θέλει να εισέλθει σε μια χώρα. Αν ο ελεγκτή αυτός επιτρέπει σε κάποιον να περάσει στο εσωτερικό, αφού ελέγξει την ταυτότητά του, δεν χρειάζονται περαιτέρω έλεγχοι. Ομοίως, σε ένα αεροδρόμιο, όλοι οι έλεγχοι γίνονται στην πύλη. Για να δημιουργηθεί καλύτερη περιμετρική ασφάλεια, το τέχνασμα είναι να διασφαλίζεται συνεχώς ότι ο ελεγκτής κάνει σωστά τη δουλειά του και προσαρμόζεται για οποιεσδήποτε εξελίξεις σε πλαστά IDs τα οποία θέλουν να εισέλθουν.

- **Principle Four: Always Assume Lowest Security for Any Action + Condition**

Ακριβώς επειδή ελέγχετε διαπιστευτήρια στην πόρτα δεν σημαίνει ότι μόλις ο χρήστης λάβει πρόσβαση ότι θα πρέπει να έχουν πρόσβαση σε όλα. Απαιτούνται περαιτέρω έλεγχοι για να αποκτήσετε βαθύτερα επίπεδα λειτουργικότητας και πρόσβασης στις πληροφορίες. Για παράδειγμα, απλώς και μόνο επειδή περάσατε από την πύλη του αεροδρομίου, δεν σημαίνει ότι μπορείτε να βαδίζετε στην αίθουσα ελέγχου του αεροδρομίου. Εξακολουθείτε να χρειάζεστε υψηλότερα προνόμια για να μπείτε σε αυτό.

Το ίδιο ισχύει για το λογισμικό. Το προεπιλεγμένο επίπεδο πρόσβασης πρέπει να έχει το λιγότερο προνόμιο. Το πιο σημαντικό, εάν οι έλεγχοι δεν περάσουν, η προεπιλογή είναι το χαμηλότερο δυνατό πλαίσιο ασφαλείας και η ενέργεια δεν επιτρέπεται. Αυτή η αρχή του λιγότερου προνομίου δημιουργεί λογισμικό που είναι από προεπιλογή ασφαλές και ανθεκτικό.

- **Principle Five: Always Create a Security Context**

Η επιτυχής ασφάλεια εξαρτάται από τη δημιουργία ενός σταθερού πλαισίου λογισμικού στο εσωτερικό της εφαρμογής από την πρώτη μέρα. Η ασφάλεια που έχει προστεθεί εκ των υστέρων είναι πάντα δύσκολη να επιδιορθωθεί ή να προσαρμοστεί όταν εντοπιστούν νέοι φορείς επίθεσης.

Θα πρέπει να είναι εύκολο να χρησιμοποιήσετε μια εφαρμογή και να ρυθμίσετε κατάλληλα την ασφάλεια ή θα πρέπει να έχει γίνει από προεπιλογή. Ένα πρόβλημα που διαπιστώθηκε μετά την αποδέσμευση του λογισμικού όπου κάτι δεν είναι διαθέσιμο λόγω της ασφάλειας είναι καλύτερο από το αντίθετο. Η κατασκευή σύνθετων δομών ασφαλείας θα σήμαινε ότι είναι λιγότερο κατανοητή από τους προγραμματιστές και είναι ευκολότερο να χρησιμοποιηθεί εσφαλμένα.

Για να είναι ασφαλές λογισμικό δεν είναι αδύνατο, απλά απαιτεί συνεχή προσπάθεια και πρακτική, αλλά οι ανταμοιβές αξίζουν τον κόπο. Με την προτεραιότητα στην ασφάλεια από την αρχή, την έρευνα και την αξιολόγηση των τεχνολογιών που χρησιμοποιούνται για τη δημιουργία μιας εφαρμογής, τη δημιουργία ισχυρών βημάτων

ελέγχου ταυτότητας και εξουσιοδότησης, διπλού ελέγχου ασφαλών επικοινωνιών και εργασίας για την προστασία δεδομένων με κρυπτογράφηση, οι προγραμματιστές θα μπορούν να ελαχιστοποιήσουν τυχόν τρωτά σημεία.

Παρόλο που η νέα, αλληλένδετη πραγματικότητα του cloud παρέχει αμέτρητα οφέλη, παρουσιάζει επίσης και νέους τύπους κινδύνων που πρέπει να ληφθούν υπόψη κατά την ανάπτυξη εφαρμογών. Οι εφαρμογές πρέπει να είναι κατασκευασμένες με μέτρα εγγύτητας που είναι εγγενή για την αντιμετώπιση ποικίλων επιθέσεων και δυνητικών φορέων επίθεσης.

4.2 Ευαίσθητα δεδομένα (Sensitive data on consumer platforms)

Καθώς η απειλή από τον κυβερνοχώρο αυξάνεται, η ανάγκη να υιοθετηθεί η στρατηγική «ασφαλής από προεπιλογή» γίνεται πιο επείγουσα. Συχνά, προκειμένου να είναι ασφαλή τα σημερινά προϊόντα και υπηρεσίες, η χρηστικότητα τους πρέπει να μειωθεί σημαντικά. Εάν μια επιχείρηση πρόκειται να λειτουργήσει με ασφάλεια σε έναν συνδεδεμένο κόσμο, κάθε προϊόν, σύστημα ή υπηρεσία που προμηθεύεται ή αναπτύσσεται πρέπει να είναι ασφαλής από προεπιλογή. Θα πρέπει να είναι δύσκολο να τα κάνετε ανασφαλείς.

Οι επιχειρήσεις που έχουν συνείδηση της ασφάλειας (συμπεριλαμβανομένων των κυβερνητικών υπηρεσιών) μπορούν να συμβάλουν στη διαμόρφωση της αγοράς για την υποστήριξη αυτής της στρατηγικής. Αρχικά θα επικεντρωθούμε στις πλατφόρμες υπολογιστικής / καταναλωτικής πληροφορικής, συμπεριλαμβανομένων των φορητών υπολογιστών, των smartphones και των συσκευών tablet.

Η διαχείριση των κινδύνων για τις σύγχρονες πλατφόρμες προϋποθέτει συνήθως την προσθήκη επιπλέον ελέγχων. απαιτώντας την πρόσβαση των χρηστών σε ευαίσθητα δεδομένα ή την παρακολούθηση / περιορισμό της χρήσης ορισμένων λειτουργιών. Μειώνουμε την πιθανότητα ή την επίδραση ενός συμβιβασμού, αλλά με αυτόν τον τρόπο μειώνουμε επίσης τη χρηστικότητα. Οι πρόσθετοι έλεγχοι μπορούν επίσης να επηρεάσουν αρνητικά την ταχύτητα εφαρμογής ή τη διάρκεια ζωής της μπαταρίας της συσκευής.

Οι πλατφόρμες Secure από προεπιλογή περιγράφουν τα επιθυμητά τεχνικά χαρακτηριστικά των ασφαλών πλατφόρμων και σημειώνει ότι πολλά από αυτά τα χαρακτηριστικά θα μπορούσαν να ενεργοποιηθούν τουλάχιστον σε κάποιο βαθμό σε υπάρχουσες συσκευές. Η ευρεία υιοθέτηση δεν συμβαίνει επειδή η ζήτηση της αγοράς θεωρείται ότι είναι χαμηλή.

4.2.1 How can we create demand for 'Secure by Default' technology?

Απλά η «βελτίωση της ασφάλειας» δεν επαρκεί για τη δημιουργία εμπορικής ζήτησης. Πρέπει να ενεργοποιήσουμε τις δυνατότητες που είναι επιτακτικές στους χρήστες και στους διαχειριστές συστημάτων.

- Showcase examples

Όπου υπάρχουν παραδείγματα εργασίας, θα πρέπει να εκπονούνται δημόσιες διαδηλώσεις για να καταδειχθεί πώς μπορούν να επιλυθούν πραγματικά επιχειρηματικά προβλήματα με την τεχνολογία ασφάλειας. Καθώς το υποστηρικτικό λογισμικό ωριμάζει, μπορούν να διεξαχθούν δοκιμές για να εξασφαλιστούν οι στόχοι χρηστικότητας.

- Publish requirements

Καθώς οι δοκιμές βελτιώνουν την ευαισθητοποίηση, οι επιχειρήσεις πρέπει να ενθαρρύνονται να δηλώνουν δημοσίως τις απαιτήσεις τους και να χρησιμοποιούν περιπτώσεις για την τεχνολογία ασφάλειας πλατφόρμας.

- Differentiate — use assurance to show the difference

Προκειμένου να αναπτυχθεί η τεχνολογία ασφαλείας με εμπιστοσύνη, είναι απαραίτητη η ανεξάρτητη διαβεβαίωση για την ευρωστία των κρίσιμων λειτουργιών. Οι προμηθευτές και οι πελάτες πρέπει να συνεργαστούν για να διασφαλίσουν ότι τα εξαρτήματα μπορούν να πιστοποιηθούν σε κατάλληλο επίπεδο χωρίς να αυξηθεί σημαντικά το κόστος παραγωγής ή τα χρονοδιαγράμματα.

5. Ιδιωτικότητα από προεπιλογή (Privacy by default)

Το απόρρητο ως προεπιλεγμένη ρύθμιση είναι μία από τις "επτά θεμελιώδεις αρχές" της προστασίας της ιδιωτικής ζωής από την άποψη του σχεδιασμού, μια έννοια που αναπτύχθηκε από τη δεκαετία του '90. Η PbD έχει αναγνωριστεί ευρέως στο επιχειρηματικό περιβάλλον και στη συνέχεια έγινε μέρος διαφόρων νομικών πλαισίων. Για παράδειγμα, περιλαμβάνεται ρητά στις Αυστραλιανές Αρχές Προστασίας Προσωπικών Δεδομένων.

Πιο πρόσφατα, η προστασία δεδομένων από το σχεδιασμό και από προεπιλογή εισήχθη από τους νομοθέτες της ΕΕ ως ένα σημαντικό μέρος των διατάξεων του GDPR. Σε αυτό το πλαίσιο (βλέπε άρθρο 25 του GDPR) αναφέρονται τεχνικά και οργανωτικά μέτρα, τα οποία θα πρέπει να αποσκοπούν στο να διασφαλίζεται ότι τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας υποβάλλονται σε επεξεργασία.

Το άρθρο 25 παράγραφος 2 του GDPR απαιτεί από τους υπεύθυνους επεξεργασίας δεδομένων να εφαρμόζουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίζουν ότι, εκ των προτέρων, μόνο δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας υποβάλλονται σε επεξεργασία. Η υποχρέωση αυτή ισχύει για το ποσό των συλλεγόμενων προσωπικών δεδομένων, την έκταση της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Συγκεκριμένα, τα μέτρα αυτά διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσιτά χωρίς την παρέμβαση του ατόμου σε απεριόριστο αριθμό ατόμων.

Η αρχή της απορρόφησης της ιδιωτικής ζωής έχει πρωταρχική σημασία για υπηρεσίες και προϊόντα, όπου το υποκείμενο των δεδομένων έχει την επιλογή να μοιράζεται τα προσωπικά του δεδομένα. Η προστασία απορρήτου υποχρεώνει τους οργανισμούς να προστατεύουν την ιδιωτικότητα του υποκειμένου των δεδομένων εφαρμόζοντας τις πιο φιλικές προς το περιβάλλον ρυθμίσεις. Ειδικότερα, η αρχή αυτή διαδραματίζει σημαντικό ρόλο στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που σχετίζεται

με τις πλατφόρμες επιγραμμικών και κοινωνικών μέσων. Κατ 'αρχήν, τα πλαίσια και οι εφαρμογές που έχουν προηγουμένως επισημανθεί και παρακολουθούν αυτόματα την τοποθεσία του υποκειμένου δεδομένων δεν πληρούν τις απαιτήσεις απορρήτου από προεπιλογή.

6. Οδηγός Ανάπτυξης λογισμικού κατά των σχεδιασμό ώστε να συμμορφωθούμε με τον γενικό κανονισμό GDPR

Με τον νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 που εφαρμόστηκε στις 25 Μαΐου 2018, καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ.

Η προστασία των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα απαιτεί τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε να διασφαλίζεται ότι τηρούνται οι απαιτήσεις του παρόντος κανονισμού. Προκειμένου να μπορεί να αποδείξει συμμόρφωση προς τον παρόντα κανονισμό, ο υπεύθυνος επεξεργασίας θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τα οποία ανταποκρίνονται ειδικότερα στις αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Τέτοια μέτρα θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, την ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα το συντομότερο δυνατόν, τη διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία δεδομένων και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφάλειας. Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των τελευταίων εξελίξεων, να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων. Οι αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού θα πρέπει επίσης να λαμβάνονται υπόψη στο πλαίσιο των δημόσιων διαγωνισμών.

Η Αρχή Προστασίας Δεδομένων της Νορβηγίας έχει αναπτύξει κάποιες κατευθυντήριες γραμμές για να βοηθήσει τους οργανισμούς έτσι ώστε να κατανοήσουν και να συμμορφωθούν με την απαίτηση για την προστασία δεδομένων από το σχεδιασμό και εξ ορισμού σύμφωνα με το άρθρο 25 του Κανονισμού Γενικής Προστασίας Δεδομένων(GDPR).

Παρακάτω υπάρχει η ανάπτυξη και ανάλυση αυτού του οδηγού ώστε να καταλάβουμε τα στάδια και της απαιτήσεις για την συμμόρφωση με τον γενικό κανονισμό GDPR

6.1 Τι είναι η Προστασία Προσωπικών Δεδομένων (What is data protection)

Προτού αναλύσουμε τα στάδια που απαιτούνται για την συμμόρφωση με τον γενικό κανονισμό θα μιλήσουμε για το τί σημαίνει η προστασία των προσωπικών δεδομένων. Η δημιουργία προφίλ, η αυτοματοποιημένη λήψη αποφάσεων και οι εξατομικευμένες υπηρεσίες έχουν γίνει μέρος της καθημερινής μας ζωής. Αυτές οι τάσεις συχνά περιλαμβάνουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε μεγάλη κλίμακα. Οι χρήστες αναμένουν ότι οι υπηρεσίες θα είναι ασφαλείς και θα προστατεύουν το απόρρητό τους με αποτελεσματικό τρόπο. Οι επιχειρήσεις που αντιμετωπίζουν σοβαρά τα ζητήματα προστασίας δεδομένων δημιουργούν εμπιστοσύνη. Έτσι, τα ισχυρά μέτρα προστασίας δεδομένων μπορούν να αποτελέσουν ανταγωνιστικό πλεονέκτημα.

Η νομοθεσία για την προστασία των δεδομένων περιέχει βασικές αρχές για τη διασφάλιση της ιδιωτικής ζωής των υποκειμένων των δεδομένων. Η προστασία δεδομένων από το σχεδιασμό και από προεπιλογή συμβάλλει στη διασφάλιση ότι τα πληροφοριακά συστήματα που χρησιμοποιούμε πληρούν αυτές τις αρχές προστασίας δεδομένων και ότι τα συστήματα διασφαλίζουν τα δικαιώματα των υποκειμένων των δεδομένων.

Η προστασία δεδομένων από το σχεδιασμό και η προεπιλεγμένη προστασία δεδομένων (data protection by design, and data protection by default) αποτελούν κεντρικές απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) που ισχύει από τον Μάιο του 2018. Αυτός ο οδηγός περιγράφει τον τρόπο συμμόρφωσης με αυτές τις απαιτήσεις. Ο υπεύθυνος επεξεργασίας δεδομένων (data controller) πρέπει να συμμορφώνεται με τις απαιτήσεις που διέπουν την προστασία δεδομένων κατά το σχεδιασμό κατά την ανάπτυξη λογισμικού και κατά την παραγγελία συστημάτων, λύσεων και υπηρεσιών. Οι απαιτήσεις πρέπει επίσης να συμπεριληφθούν κατά την σύναψη συμφωνιών με τους προμηθευτές και κατά τη χρήση συμβούλων.

Η διαφάνεια είναι μια αρχή του νέου κανονισμού και είναι ζωτικής σημασίας για την οικοδόμηση της προστασίας δεδομένων στο λογισμικό. Η διαφάνεια σχετικά με τη χρήση των προσωπικών δεδομένων συνεπάγεται την παροχή πληροφοριών σχετικά με το τι υποβάλλονται σε επεξεργασία, από ποιον, γιατί, πώς και για πόσο καιρό διατηρείται. Προκειμένου τα πρόσωπα στα οποία αναφέρονται τα δεδομένα να ασκούν τα δικαιώματά τους, οι οργανώσεις πρέπει να είναι ανοιχτές όσον αφορά την επεξεργασία των προσωπικών δεδομένων τους. Με αυτόν τον τρόπο, τα υποκείμενα των δεδομένων μπορούν να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με το εάν θα χρησιμοποιήσουν ή όχι λογισμικό και αυτό εξασφαλίζει τη νομιμότητα και την αποτελεσματικότητα του υπεύθυνου επεξεργασίας δεδομένων.

Η δέσμευση της διοίκησης είναι ζωτικής σημασίας για τη λήψη αποφάσεων για την εφαρμογή των αρχών της προστασίας δεδομένων χρήσης από το σχεδιασμό στις προμήθειες του οργανισμού και την ανάπτυξη λογισμικού. Η διοίκηση πρέπει επίσης να διασφαλίσει ότι θα διαθέτει επαρκείς πόρους για το έργο αυτό. Η συνεκτίμηση της προστασίας δεδομένων σε όλη τη διαδικασία ανάπτυξης είναι τόσο αποδοτική όσο και αποδοτικότερη από την πραγματοποίηση αλλαγών σε υπάρχον κομμάτι λογισμικού. Οι επιχειρήσεις που δεν συμμορφώνονται με το GDPR κινδυνεύουν με σημαντικό κόστος, τόσο με πρόστιμα για παραβίαση του νόμου, όσο και με απώλεια εσόδων λόγω ζημιών στη φήμη τους.

6.2 Βασικές υποχρεώσεις για τους υπευθύνους επεξεργασίας Data

Οδηγός Συμμόρφωσης:

Παρακάτω θα δούμε κάποιες βασικές υποχρεώσεις του υπεύθυνου ασφαλείας ώστε να εναρμονιστεί με τον κανονισμό:

- **Ευθύνη**: Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη να αποδεικνύει ότι λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων και ότι συμμορφώνεται με τον Κανονισμό.

- **Προστασία δεδομένων κατά τον σχεδιασμό («Data protection by design»)**: Ο Κανονισμός επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων σας. Για παράδειγμα, στις υπηρεσίες ηλεκτρονικής κοινωνικής δικτύωσης πρέπει να σας δίνεται η δυνατότητα να επιλέγετε ρυθμίσεις που θα προστατεύουν περισσότερο τα προσωπικά σας δεδομένα.

- **Προστασία δεδομένων εξ ορισμού («Data protection by default»)**: Ο Κανονισμός επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας.

- **Ασφάλεια επεξεργασίας**: Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας.

- **Γνωστοποίηση παραβιάσεων δεδομένων**: Έχει υποχρέωση, μόλις αντιληφθεί παραβίαση, να ενημερώσει τις αρμόδιες εποπτικές Αρχές και εσάς, εφ' όσον η παραβίαση μάς θέτει σε σοβαρό κίνδυνο.

- **Εκτίμηση επιπτώσεων και προηγούμενη διαβούλευση**: Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων (Data protection impact assessment). Όταν βάσει της διενεργηθείσας εκτίμησης επιπτώσεων και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την εποπτική Αρχή.

- **Υπεύθυνος προστασίας δεδομένων**: Προβλέπεται, υπό προϋποθέσεις, ο ορισμός «υπευθύνου προστασίας δεδομένων» ο οποίος έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εποπτική Αρχή.

- **Κώδικες δεοντολογίας**: Ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας από τους υπεύθυνους επεξεργασίας, οι οποίοι υποβάλλονται προς έγκριση στην εποπτική Αρχή. Σε περίπτωση διευρωπαϊκής δραστηριότητας ζητείται και η γνώμη του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.

- **Πιστοποίηση**: Ενθαρρύνεται η θέσπιση μηχανισμών πιστοποίησης, σφραγίδων και σημάτων προστασίας δεδομένων για την απόδειξη της συμμόρφωσης προς τον Κανονισμό ή για την απόδειξη παροχής κατάλληλων εγγυήσεων κατά την επεξεργασία.

6.3 Προετοιμαστείτε σε 10 βήματα

Οδηγός Συμμόρφωσης:

Παρακάτω θα δούμε κάποια βασικά βήματα έτσι ώστε να προετοιμαστούμε για την εναρμόνιση του οργανισμού μας με τον γενικό κανονισμό GDPR.

- **ΕΝΗΜΕΡΩΣΗ - ΕΤΟΙΜΟΤΗΤΑ**: Ενημερώστε το ανθρώπινο δυναμικό του οργανισμού σας για τις επερχόμενες μεταβολές, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων. Αξιολογήστε τους πιθανούς κινδύνους για τα προσωπικά δεδομένα που συλλέγετε και επεξεργάζεστε. Διαμορφώστε στρατηγική αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα.

- **ΚΑΤΑΓΡΑΦΗ**: Αν Οφείλουμε να τηρούμε ειδικά αρχεία επεξεργασιών θα πρέπει να καταγράψουμε τα δεδομένα που τηρούμε και μεταβιβάζουμε, τις επεξεργασίες στις οποίες προβαίνουμε, τον σκοπό τους και τη νομική βάση.
- **ΕΛΕΓΧΟΣ ΤΗΡΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ**: Εξετάζετε συνεχώς αν κατά την επεξεργασία των δεδομένων τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των υποκειμένων.
- **ΕΛΕΓΧΟΣ ΣΥΓΚΑΤΑΘΕΣΗΣ**: Εξετάστε τις μεθόδους για εξασφάλιση συγκατάθεσης για κάθε επιδιωκόμενο σκοπό επεξεργασίας.
- **ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ**: Οι διαδικασίες για τον χειρισμό των αιτημάτων των πολιτών, ιδίως ως προς τη διαγραφή δεδομένων (δικαίωμα στη λήθη) ή φορητότητα δεδομένων.
- **ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ**: Θα πρέπει να είστε σε θέση να εκτιμήσετε τις πιθανότητες κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.
- **ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ**: Ανάλογα με τη δραστηριότητα που ασκείτε, εξετάστε αν χρειάζεται να ορίσετε «υπεύθυνο προστασίας δεδομένων».
- **ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ**: Υιοθετήστε μεθόδους για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων.
- **ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΣΕ ΠΕΡΙΣΣΟΤΕΡΑ ΚΡΑΤΗ ΜΕΛΗ**: Στην περίπτωση αυτή πρέπει να προτείνετε το κράτος της κύριας εγκατάστασής σας.
- **ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΕΕ**: Αν διαβιβάζετε δεδομένα και σε τρίτες χώρες, επιλέξτε κάποιο μηχανισμό διαβίβασης, όπως δεσμευτικούς εταιρικούς κανόνες (BCRs), τυποποιημένες συμβατικές ρήτρες (SCCs), πιστοποιήσεις στο Privacy Shield (για τις ΗΠΑ).

6.4 Προστασία Προσωπικών Δεδομένων και Προστασία Δεδομένων από το σχεδιασμό (Data protection by Design & by Default)

Οδηγός συμμόρφωσης - How to prepare your team for the GDPR

Η Προστασία Προσωπικών Δεδομένων και Προστασία Δεδομένων από το σχεδιασμό δίνεται ως σημείο εκκίνησης στο να διερευνήσουμε το πώς θα ενσωματώσουμε τις αρχές προστασίας δεδομένων, τα υποκείμενα δικαιώματα και τις απαιτήσεις του GDPR σε κάθε βήμα της διαδικασίας ανάπτυξής ενός λογισμικού η μιας υπηρεσίας.

Αυτές οι οδηγίες απευθύνονται κυρίως σε προγραμματιστές, αρχιτέκτονες λογισμικού (software architects), διαχειριστές (project managers), αξιωματούχους προστασίας δεδομένων (data protection officers) και συμβούλους ασφαλείας(security advisors). Όλοι όσοι αναπτύσσουν και συμβάλλουν στην ανάπτυξη λογισμικού που περιέχει ή επεξεργάζεται δεδομένα προσωπικού χαρακτήρα.

Η ανάπτυξη λογισμικού αρχίζει με μια ιδέα δημιουργίας ενός προϊόντος που θα συμβάλει στην απλούστευση ή τη βελτίωση της ποιότητας μιας διαδικασίας ή μιας εργασίας. Υπάρχουν λειτουργικές απαιτήσεις για το πώς το λογισμικό θα πρέπει να επιλύσει την εργασία.

Η ανάπτυξη λογισμικού πρέπει να ακολουθεί μια μεθοδολογία με βασικές δραστηριότητες για να διασφαλιστεί ότι το τελικό προϊόν είναι ισχυρό. Υπάρχει κάποια τεχνική βιβλιογραφία που επικεντρώνεται στην ασφάλεια από το σχεδιασμό ως μέρος της ανάπτυξης λογισμικού. Ωστόσο, υπάρχει λιγότερη προστασία δεδομένων από το σχεδιασμό και από προεπιλογή ως μέρος της ανάπτυξης λογισμικού. Για τον οδηγό αυτόν, χρησιμοποιήθηκε το Microsoft Life Cycle Development Lifecycle (SDL), το Secure Software Development LifeCycle (S-SDLC) και τον ENISA.

6.4.1 Εκπαίδευση (Training):

Οι επτά δραστηριότητες αυτού του οδηγού ξεκινούν με την εκπαίδευση. Στο τμήμα για την κατάρτιση, καλύπτουμε τα πιο σημαντικά θέματα για την παροχή εκπαίδευσης, γιατί, πώς να το κάνουμε αυτό και ποια εργαλεία να χρησιμοποιήσετε.

Κατά τη διάρκεια αυτής της δραστηριότητας, προσδιορίζονται οι ειδικοί τύποι κατάρτισης που πρέπει να δοθούν. Για να διασφαλιστεί ότι όλοι οι οργανισμοί κατανοούν τόσο την ανάγκη όσο και τους κινδύνους που σχετίζονται με την προστασία και την ασφάλεια των δεδομένων, πρέπει να δομηθεί η κατάρτιση. Η ομάδα-στόχος αυτής της δραστηριότητας είναι η διοίκηση και οι υπάλληλοι του οργανισμού.

6.4.1.1 Τι είναι σημαντικό να μάθουμε;

Η κατανόηση της προστασίας των δεδομένων και της ασφάλειας των πληροφοριών αποτελεί προϋπόθεση για την ανάπτυξη λογισμικού με προστασία δεδομένων από το σχεδιασμό και από προεπιλογή. Οι εργαζόμενοι θα πρέπει να γνωρίζουν ποιες απαιτήσεις ισχύουν, τι πρέπει να προσέχουν και ποια εργαλεία τους επιτρέπουν να μετατρέπουν τις γνώσεις σχετικά με την προστασία των δεδομένων και την ασφάλεια των πληροφοριών σε λογισμικό που το προστατεύει.

Οι εργαζόμενοι πρέπει επίσης να γνωρίζουν ποια μεθοδολογία και ρουτίνα πρέπει να ακολουθούνται. Ο ίδιος ο οργανισμός πρέπει να αποφασίσει τι είναι συναφές και τι

είδους κατάρτιση απαιτείται για τους μεμονωμένους υπαλλήλους. Πρέπει να καταρτιστεί σχέδιο κατάρτισης.

6.4.1.2 Ποιες απαιτήσεις ισχύουν για τον οργανισμό;

Οι εργαζόμενοι θα πρέπει να εκπαιδεύονται στις σχετικές εσωτερικές και εξωτερικές απαιτήσεις. Οι εσωτερικές απαιτήσεις μπορούν να αφορούν την προστασία δεδομένων, την ασφάλεια των πληροφοριών, τον εσωτερικό έλεγχο και τη διαχείριση των πόρων. Αυτό περιλαμβάνει ρουτίνες για την εκτίμηση κινδύνου και απαιτήσεις για την τεκμηρίωση. Οι εξωτερικές απαιτήσεις περιλαμβάνουν γενικά τη νομοθεσία για την προστασία των δεδομένων, τη σημασία των αρχών προστασίας δεδομένων ειδικότερα και τα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα.

Άλλες εξωτερικές απαιτήσεις ενδέχεται να περιλαμβάνουν κανονιστικές και υποχρεωτικές απαιτήσεις σχετικά με τον τομέα ή τη βιομηχανία για την οποία πρόκειται να αναπτυχθεί το λογισμικό. Μπορεί επίσης να υπάρχει η απαίτηση να ακολουθείτε τις βέλτιστες πρακτικές, τα πρότυπα, τον κώδικα συμπεριφοράς για την επιλεγμένη τεχνολογία. Παραδείγματα αυτών είναι ο νόμος για την ελευθερία της πληροφόρησης, ο νόμος περί ασθενών, ο κανονισμός για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, οι κανονισμοί για τη χρήση της τεχνολογίας πληροφοριών και επικοινωνιών (ICT), το πλαίσιο για την ασφάλεια των πληροφοριών (για παράδειγμα το ISO27001 και το πρότυπο καλής ασφάλειας ISF Πρακτική για την Ασφάλεια Πληροφοριών (SoGP).

6.4.1.3 Πώς να το κάνετε αυτό στην πράξη;

Οι προγραμματιστές λογισμικού θα πρέπει να έχουν μια καθιερωμένη αναπτυξιακή μεθοδολογία, που θα εγκρίνεται από τη διοίκηση, την οποία ακολουθούν κατά την ανάπτυξη λογισμικού. Κατά την ανάπτυξη λογισμικού που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, η μεθοδολογία πρέπει να περιλαμβάνει την προστασία δεδομένων από το σχεδιασμό και από προεπιλογή (data protection by design and by default) και την ασφάλεια από το σχεδιασμό (SbD). Παραδείγματα πλαισίων ανάπτυξης με ενσωματωμένη ασφάλεια είναι τα έργα κορυφαίας ανάπτυξης της Microsoft Security Development Lifecycle (SDL) και OWASP.

6.4.1.4 Ποια εργαλεία μπορούν να χρησιμοποιηθούν;

Ο οργανισμός θα πρέπει να προετοιμάσει μια επισκόπηση των εργαλείων, των προτύπων και των βέλτιστων πρακτικών που θα πρέπει να χρησιμοποιούνται κατά την ανάπτυξη του λογισμικού. Οι εργαζόμενοι θα πρέπει να εκπαιδεύονται σε ποια εργαλεία μπορούν να χρησιμοποιήσουν, πώς να τα χρησιμοποιήσουν και για ποιους σκοπούς

6.4.2 Απαιτήσεις (Requirements)

Το τμήμα σχετικά με τις απαιτήσεις περιγράφει τα μέτρα που είναι αναγκαία για την προστασία και την ασφάλεια των δεδομένων, τα επίπεδα ανοχής που ο οργανισμός πρέπει να ορίσει για την προστασία και την ασφάλεια των δεδομένων και την ανάγκη εκτίμησης τόσο των κινδύνων ασφάλειας όσο και των επιπτώσεων στην προστασία των δεδομένων.

Αυτή η δραστηριότητα περιστρέφεται γύρω από τις απαιτήσεις ρύθμισης για την προστασία δεδομένων και την ασφάλεια των πληροφοριών για το τελικό προϊόν. Αυτές οι απαιτήσεις πρέπει να αντανακλούν την ανάγκη προστασίας δεδομένων και ασφάλειας των πληροφοριών και πρέπει να συμπεριλαμβάνονται ως μέρος του σχεδίου του έργου.

Η ομάδα-στόχος περιλαμβάνει όλους όσους εμπλέκονται στην ανάπτυξη ή στην ιδιοκτησία του λογισμικού, συμπεριλαμβανομένων εκείνων που είναι υπεύθυνοι για τον καθορισμό των απαιτήσεων, των ιδιοκτητών προϊόντων, των πελατών / αγοραστών, των ηγετών των έργων, των προγραμματιστών, των αρχιτεκτόνων και των δοκιμαστών. Ο υπεύθυνος προστασίας δεδομένων και ο σύμβουλος ασφάλειας πρέπει επίσης να συμμετέχουν στη δραστηριότητα αυτή.

Όταν εντοπίζονται νωρίς οι απαιτήσεις για προστασία και ασφάλεια των δεδομένων, τα επίπεδα ανοχής, οι επιπτώσεις στην προστασία δεδομένων και οι κίνδυνοι ασφαλείας, η ομάδα ανάπτυξης θα γνωρίζει ήδη ποιες απαιτήσεις πρέπει να καλύψουν και, ως εκ τούτου, μπορεί να μετριάσει τους κινδύνους που συνδέονται με την προστασία των δεδομένων και την ασφάλεια των πληροφοριών. διαδικασία ανάπτυξης.

6.4.2.1 Τι πρέπει να γίνει πριν τεθούν οι απαιτήσεις;

1. Καθορίστε την επεξεργασία που πρέπει να γίνει και δημιουργήστε μια επισκόπηση των προσωπικών δεδομένων:

   ✓ Θα επεξεργαστούν τα προσωπικά δεδομένα από το λογισμικό;

- ✓ Προσδιορισμός του ελεγκτή και όλους τους επεξεργαστές και τους υπεργολάβους. Οι συμβάσεις επεξεργασίας πρέπει να υπογράφονται και οι υπεργολάβοι πρέπει να εγκρίνονται από τον υπεύθυνο επεξεργασίας.

- ✓ Ποια είναι η νομική βάση για τη μεταποίηση;

- ✓ Ποιος είναι ο σκοπός της επεξεργασίας;

- ✓ Για πόσο καιρό η νομική βάση ή / και ο σκοπός επιτρέπουν την αποθήκευση δεδομένων προσωπικού χαρακτήρα; Είναι απαραίτητο να σχεδιάσετε την αυτόματη διαγραφή;

- ✓ Ορίστε τις κατηγορίες προσωπικών δεδομένων που είναι απαραίτητες προς επεξεργασία για την επίτευξη του σκοπού. Η επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και των δεδομένων προσωπικού χαρακτήρα που αφορούν τις ποινικές καταδίκες και τα αδικήματα (ευαίσθητα προσωπικά δεδομένα) απαγορεύεται γενικά, με ορισμένες εξαιρέσεις, ώστε να καθοριστεί εάν ισχύει μία από αυτές τις εξαιρέσεις. Καταγράψτε το πλήρες εύρος των δεδομένων που είναι αποθηκευμένα στο λογισμικό.

- ✓ Πώς επιτυγχάνεται η διαφάνεια; Αυτόματες ειδοποιήσεις από το σύστημα, τον πίνακα ελέγχου απορρήτου.

- ✓ Τα προσωπικά δεδομένα μεταφέρονται σε τρίτη χώρα ή σε διεθνή οργανισμό; Οι όροι ισχύουν για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς, συμπεριλαμβανομένων περιορισμών σχετικά με την πρόσβαση, τη λειτουργία και την αποθήκευση. Σε περίπτωση μεταφοράς προσωπικών δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό, είναι σημαντικό να διασφαλιστεί ότι όλες αυτές οι μεταφορές είναι νόμιμες.

2. Σε ποιο πλαίσιο θα πραγματοποιηθεί η επεξεργασία; Είναι πιθανό ότι το λογισμικό θα μπορούσε να χρησιμοποιηθεί σε άλλο πλαίσιο;

3. Προσδιορίστε όλες τις απαιτήσεις που ισχύουν για την επιχείρησή σας: Υπάρχουν κωδικοί συμπεριφοράς συγκεκριμένων για τον κλάδο ή τον τομέα; Υπάρχουν κάποιες πολιτικές και απαιτήσεις που μπορούν να σας βοηθήσουν να προσδιορίσετε τις απαιτήσεις για το λογισμικό;

4. Υπάρχουν προγράμματα πιστοποίησης που μπορείτε και πρέπει να ακολουθήσετε; Ποιες απαιτήσεις ισχύουν σε τέτοιες περιπτώσεις;

6.4.2.2 Ποιες οι απαιτήσεις για την προστασία των δεδομένων και την ασφάλεια των πληροφοριών;

Προκειμένου να οριστούν οι σωστές απαιτήσεις, είναι σημαντικό να γνωρίζουμε ποιες κατηγορίες προσωπικών δεδομένων θα υποβάλλονται σε επεξεργασία στο λογισμικό, ποια συμπεράσματα μπορούν να εξαχθούν σχετικά με τα άτομα με βάση τα δεδομένα που επεξεργάζονται, ποιος είναι ο χρήστης και ιδιοκτήτης των δεδομένων, ο οποίος ορίζεται ως ελεγκτής και, κατά περίπτωση, ποιος είναι ο επεξεργαστής δεδομένων ή ο αποδέκτης των προσωπικών δεδομένων. Αυτό είναι απαραίτητο για τον καθορισμό των νόμων, των κανόνων, των οδηγιών και των κωδίκων δεοντολογίας που ισχύουν για το λογισμικό που αναπτύσσεται. Αυτές παρέχουν οδηγίες για τον καθορισμό των απαιτήσεων που θα πρέπει να καθοριστούν για το λογισμικό.

Οι σχετικές απαιτήσεις για την προστασία και την προστασία των δεδομένων περιέχονται στον κανονισμό για την προστασία των δεδομένων, τις επιχειρηματικές πρακτικές και τις πολιτικές για την προστασία των δεδομένων και την ασφάλεια των πληροφοριών, διάφορα πρότυπα ασφάλειας και κώδικες δεοντολογίας ή άλλους σχετικούς νόμους και κανονισμούς που αφορούν τον τομέα. Η εταιρεία πρέπει να αποφασίσει για τον εαυτό της ποιες απαιτήσεις σχετίζονται με την επιχείρησή, το λογισμικό που αναπτύσσεται και το πλαίσιο εντός του οποίου θα χρησιμοποιηθεί το τελικό προϊόν. Οι απαιτήσεις για την προστασία των δεδομένων και την ασφάλεια των πληροφοριών πρέπει να διατυπώνονται σε έναν κατάλογο ελέγχου ο οποίος θα πρέπει να ενσωματωθεί στο σχέδιο του έργου και να παρακολουθείται καθ 'όλη τη διαδικασία ανάπτυξης.

Αρχές προστασίας δεδομένων (Data protection principles)

Η σημαντικότερη απαίτηση που ισχύει για το λογισμικό με προστασία δεδομένων κατά το σχεδιασμό είναι ότι τηρούνται οι αρχές προστασίας δεδομένων. Η επεξεργασία είναι νόμιμη, δίκαιη και διαφανής. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται για καθορισμένους, σαφείς και νόμιμους σκοπούς και συλλέγονται μόνο τα δεδομένα που είναι απαραίτητα για τη λειτουργία του λογισμικού.

Συνοπτικές πληροφορίες και ασφαλή δεδομένα (Concise information and secure the data)

Σαφείς και συνοπτικές πληροφορίες σχετικά με τον τρόπο με τον οποίο θα χρησιμοποιηθούν τα προσωπικά δεδομένα είναι θεμελιώδους σημασίας για την εξασφάλιση της προστασίας των δικαιωμάτων των προσώπων στα οποία αναφέρονται τα δεδομένα. Το λογισμικό πρέπει να διευκολύνει τα πρόσωπα στα οποία αναφέρονται τα δεδομένα να ασκούν τα δικαιώματά τους, όπως πρόσβαση, ενημέρωση, διόρθωση, περιορισμός και φορητότητα δεδομένων.

Καθορισμός επιπέδων ανοχής κινδύνου (Defining risk tolerance levels)

Η εκτίμηση κινδύνου αφορά τον εντοπισμό των πιθανών συνεπειών των διαφορετικών περιστατικών ή σεναρίων και την εκτίμηση του πόσο πιθανό ή εύκολο είναι να συμβεί ένα ανεπιθύμητο περιστατικό. Είναι η διοίκηση της εταιρείας που καθορίζει τον βαθμό κινδύνου που η εταιρεία είναι διατεθειμένη να αναλάβει σε διάφορα σενάρια. Αυτό ονομάζεται ανοχή κινδύνου. Αυτό το επίπεδο ανοχής παρέχει καθοδήγηση σχετικά με τα μέτρα και τους πόρους που πρέπει να τεθούν σε εφαρμογή για να διασφαλιστεί ότι το λογισμικό δεν υπερβαίνει το καθορισμένο επίπεδο αποδεκτού κινδύνου.

Αξιολόγηση κινδύνου ασφάλειας (Security Risk Assessment)

Η εκτίμηση κινδύνου ξεκινά με τις τιμές χαρτογράφησης που πρέπει να εξασφαλιστούν. Ο κανονισμός για την προστασία των δεδομένων ορίζει τα προσωπικά δεδομένα ως αξία. Πρέπει να διεξαχθεί αξιολόγηση των απειλών για τον προσδιορισμό των παραγόντων που θα μπορούσαν να ενδιαφέρονται για τις αξίες. Στη συνέχεια πραγματοποιείται αξιολόγηση για να προσδιοριστούν οι τιμές που είναι ευάλωτες σε οποιαδήποτε δεδομένη απειλή. Τα πρότυπα ασφάλειας πληροφοριών μπορούν να βοηθήσουν στην ανίχνευση τρωτών σημείων, προσδιορίζοντας έτσι τις απαιτήσεις που πρέπει να καθοριστούν για την προστασία και την ασφάλεια των δεδομένων.

Εκτίμηση αντικτύπου προστασίας δεδομένων (Data protection impact assessment)

Σκοπός της αξιολόγησης αντικτύπου για την προστασία των δεδομένων είναι να εκτιμηθεί ο αντίκτυπος που ενδέχεται να έχει ένα σχεδιαζόμενο λογισμικό ή μια διαδικασία επεξεργασίας στην προστασία των προσωπικών δεδομένων. Πρέπει να διασφαλίσει ότι το λογισμικό δεν παραβιάζει τα θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων.

6.4.3 Σχεδίαση (Design)

Το επόμενο τμήμα λαμβάνει περαιτέρω αυτές τις απαιτήσεις, για να σχεδιάσει, χωρίζοντάς τις σε προσανατολισμένες σε δεδομένα και σχεδιασμένες απαιτήσεις σχεδίασης. Κατά τη διάρκεια αυτής της δραστηριότητας, είναι σημαντικό ο οργανισμός να εκτελεί τόσο μοντελοποίηση απειλών όσο και ανάλυση των επιφανειών επίθεσης.

Κατά τη διάρκεια αυτής της δραστηριότητας, πρέπει να διασφαλίσετε ότι οι απαιτήσεις για την προστασία των δεδομένων και την ασφάλεια των πληροφοριών εκφράζονται στο σχεδιασμό. Οι απαιτήσεις που προσδιορίζονται κατά τη διάρκεια της δραστηριότητας απαιτήσεων πρέπει να πληρούνται και πρέπει να καθορίζονται οι απαιτήσεις για το σχεδιασμό.

Είναι σημαντικό να λαμβάνεται υπόψη η ύπαρξη φορέων απειλής που ενδέχεται να επιχειρήσουν να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα και να αποκτήσουν πρόσβαση σε αυτά. Για να μειωθεί η επιφάνεια επίθεσης, πρέπει να αναλυθεί, και το λογισμικό να διαμορφωθεί και να σχεδιαστεί έτσι ώστε να εξασφαλίζει ένα ισχυρό τελικό προϊόν.

Η ομάδα-στόχος αυτής της δραστηριότητας είναι κυρίως αρχιτέκτονες, δευτερευόντως αξιωματικοί προστασίας δεδομένων, σύμβουλοι ασφάλειας και προγραμματιστές.

Οι απαιτήσεις σχεδίασης περιγράφουν με ακρίβεια και συνολική περιγραφή του τρόπου ανάπτυξης των χαρακτηριστικών κάθε λογισμικού. Οι απαιτήσεις πρέπει να περιγράφουν τον τρόπο με τον οποίο η λειτουργικότητα μπορεί να εφαρμοστεί και να διανεμηθεί σε ασφαλές περιβάλλον και με ασφαλή τρόπο. Ένα παράδειγμα μπορεί να είναι ένα σύστημα διαχείρισης ταυτότητας και πρόσβασης, όπου ο χρήστης μπορεί να δει τι έχει συναινέσει, τις ρυθμίσεις ασφαλείας και τις ρυθμίσεις του, τη διαχείριση του κωδικού πρόσβασης και πώς λειτουργεί η διαδικασία σύνδεσης.

6.4.3.1 Κατηγορίες Απαιτήσεων

Όπως συνιστά και ο Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) της Ευρωπαϊκής Ένωσης, υπάρχουν δύο κατηγορίες απαιτήσεων σχεδιασμού οι οποίες είναι απαιτήσεις δεδομένων και απαιτήσεις βάσει διαδικασιών.

Απαιτήσεις δεδομένων (Data oriented design requirements)

1. **Ελαχιστοποίηση και περιορισμός**

Ο όγκος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται και μεταποιούνται πρέπει να περιορίζεται σε ό, τι είναι νόμιμο και αυστηρά απαραίτητο. Τα δεδομένα θα πρέπει να διαγράφονται όταν η αποθήκευση δεν απαιτείται πλέον.

2. **Απόκρυψη και προστασία**

Τα προσωπικά δεδομένα και οι αλληλεπιδράσεις τους δεν πρέπει να κοινοποιούνται, να υποβάλλονται σε επεξεργασία ή να αποθηκεύονται με απλή προβολή. Με την απόκρυψη άμεσα αναγνωρίσιμων προσωπικών δεδομένων από απλή άποψη, τον κίνδυνο κατάχρησης και πεδίο των δυνατοτήτων συμβάντων μειώνεται σημαντικά.

3. **Ξεχωριστό**

Με τον διαχωρισμό της επεξεργασίας ή της αποθήκευσης διαφόρων πηγών δεδομένων προσωπικού χαρακτήρα που ανήκουν στο ίδιο πρόσωπο, μειώνεται η δυνατότητα δημιουργίας ολοκληρωμένων προφίλ ενός ατόμου.

4. **Συνολικά**

Προκειμένου να διασφαλιστεί η προστασία των δικαιωμάτων των δεδομένων του υποκειμένου, δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται και να υποβάλλονται σε επεξεργασία με όσο το δυνατόν μεγαλύτερη συγκέντρωση.

5. **Προστασία δεδομένων από προεπιλογή**

Όλες οι ρυθμίσεις πρέπει, από προεπιλογή, να ρυθμιστούν σύμφωνα με τις πιο φιλικές προς το περιβάλλον ρυθμίσεις. Ο χρήστης θα πρέπει να επιλέξει συνειδητά να αλλάξει οποιαδήποτε ρύθμιση που θα είχε ως αποτέλεσμα λιγότερη διαμόρφωση απορρήτου.

Απαιτήσεις βάσει διαδικασιών (Process oriented design requirements)

1. **Ενημέρωση**

Το λογισμικό πρέπει να σχεδιάζεται και να διαμορφώνεται έτσι ώστε το υποκείμενο των δεδομένων να είναι επαρκώς ενημερωμένο για το πώς λειτουργεί το λογισμικό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων. Κατά τη διεξαγωγή του προφίλ ή της αυτοματοποιημένης λήψης αποφάσεων των δεδομένων προσωπικού χαρακτήρα, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για τον τρόπο με τον οποίο γίνεται αυτό.

2. **Έλεγχος**

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ελέγχει τα προσωπικά του δεδομένα. Αυτό περιλαμβάνει δικαίωμα πρόσβασης, ενημέρωσης και / ή διαγραφής των δικών τους δεδομένων. Όταν λαμβάνει χώρα αυτοματοποιημένη διαδικασία λήψης αποφάσεων ή αποφασίζονται χωρίς ανθρώπινη παρέμβαση, το υποκείμενο των δεδομένων μπορεί να ζητήσει χειροκίνητη επεξεργασία.

3. **Εφαρμογή**

Το λογισμικό θα πρέπει να σχεδιάζεται έτσι ώστε να διευκολύνει την τεκμηρίωση του τρόπου με τον οποίο διασφαλίζει τα δικαιώματα του υποκειμένου των δεδομένων. Η τεκμηρίωση θα πρέπει να καλύπτει την υποχρέωση λογοδοσίας και τον τρόπο με τον οποίο εφαρμόζεται ο κανονισμός για την προστασία των δεδομένων.

4. **Επίδειξη**

Ο υπεύθυνος επεξεργασίας πρέπει να μπορεί να τεκμηριώνει τη συμμόρφωση με τον κανονισμό για την προστασία των δεδομένων και την ασφάλεια της επεξεργασίας. Το λογισμικό πρέπει να σχεδιάζεται και να αναπτύσσεται έτσι ώστε ο ελεγκτής να μπορεί να τεκμηριώνει και να καταδεικνύει τον τρόπο με τον οποίο έχουν εφαρμοστεί οι απαιτήσεις του κανονισμού για την προστασία των δεδομένων.

6.4.3.2 Μειώστε τις ευκαιρίες εκμετάλλευσης των τρωτών σημείων

Θα πρέπει να αναλύσουμε την επιφάνεια επίθεσης του σχεδιαζόμενου λογισμικού για τη μείωση των φορέων επίθεσης και των ευκαιριών εκμετάλλευσης των αδύναμων σημείων και των τρωτών σημείων. Σε μια ανασκόπηση του σχεδιασμού, τόσο η επικοινωνία όσο και η ροή δεδομένων, η είσοδος και η έξοδος πρέπει να αναλύονται μέσω των οφθαλμών ενός εισβολέα. Θα πρέπει επίσης να διερευνηθεί εάν συλλέγεται ή αποθηκεύεται ο ίδιος τύπος πληροφοριών (διπλή λειτουργικότητα) και να δούμε εάν η λειτουργία αυτή μπορεί να απλοποιηθεί. Με την απλή διατήρηση του σχεδιασμού και την εξάλειψη περιττών χαρακτηριστικών και πολυπλοκότητας, η πιθανότητα σφαλμάτων θα μειωθεί.

Σε αυτό το είδος ανάλυσης, θα πρέπει να χρησιμοποιήσουμε τις αξιολογήσεις τόσο των κινδύνων ασφαλείας όσο και των επιπτώσεων προστασίας δεδομένων που ολοκληρώθηκαν κατά τη διάρκεια της δραστηριότητας απαίτησης. Εάν διαπιστωθεί μια ευπάθεια, θα πρέπει να εφαρμοστούν μέτρα μετριασμού ώστε να επιτευχθεί το αποδεκτό επίπεδο κινδύνου για την προστασία και την ασφάλεια των δεδομένων. Το επίπεδο ανοχής / κινδύνου πρέπει να καθοριστεί στη δραστηριότητα απαίτησης.

Η μοντελοποίηση των απειλών περιλαμβάνει την ανάλυση των εξαρτημάτων, των σημείων πρόσβασης, της ροής δεδομένων και της ροής διαδικασιών μέσα στο λογισμικό. Οι συμμετέχοντες θα πρέπει να αναλύσουν πώς κάποιος θα μπορούσε να καταχραστεί το λογισμικό σε διάφορα σενάρια. Θα πρέπει να επανεξετάσετε κάθε σενάριο για να δείτε πώς μπορεί να βελτιωθεί ο σχεδιασμός, ώστε να αποφευχθούν τυχόν απειλές που εντοπίζονται. Αυτό γίνεται με την εφαρμογή μέτρων μείωσης της ευπάθειας, με αποτέλεσμα ένα πιο ισχυρό τελικό προϊόν.

Εν συνέχεια, πρέπει να προβούμε σε μια εκτίμηση κινδύνου για τυχόν τρωτά σημεία τα οποία παραμένουν και θα πρέπει να μετριαστούν λαμβάνοντας περαιτέρω μέτρα. Εφόσον γίνει η διαδικασία αυτή τα τρωτά σημεία που βρήκαμε θα πρέπει να καταχωρούνται σε ένα αρχείο καταγραφής κινδύνων.

6.4.4 Κωδικοποίηση (Coding)

Η διαδικασία της κωδικοποίησης θα επιτρέψει στους προγραμματιστές να γράψουν ασφαλή κώδικα εφαρμόζοντας τις απαιτήσεις για προστασία δεδομένων και ασφάλεια.

Είναι σημαντικό η εταιρεία να επιλέξει μια ασφαλή και κοινή μεθοδολογία, τόσο για την κωδικοποίηση όσο και για να επιτρέψει στους προγραμματιστές να ανιχνεύσουν και να καταργήσουν τις ευπάθειες από τον κώδικα. Θα πρέπει να εισαχθούν αυτοματοποιημένα εργαλεία ανάλυσης κώδικα και η εταιρεία πρέπει να έχει θεσπίσει διαδικασίες για την ανάλυση στατικού κώδικα και την αναθεώρηση κώδικα.

6.4.4.1 Χρησιμοποιήστε εγκεκριμένα εργαλεία και πλαίσια

Για να εξασφαλιστεί συνεπής πρακτική, πρέπει να καθοριστεί και να τεκμηριωθεί κατάλογος εγκεκριμένων και επιτρεπόμενων εργαλείων, διαδικασιών και πλαισίων για την ανάπτυξη και την ανάπτυξη λογισμικού. Επιπλέον, πρέπει να είναι σαφές για ποιο λόγο μπορούν να χρησιμοποιηθούν τα διάφορα εργαλεία. Για να εξασφαλιστεί συνεπής πρακτική, πρέπει να καθοριστεί και να τεκμηριωθεί κατάλογος εγκεκριμένων και επιτρεπόμενων εργαλείων, διαδικασιών και πλαισίων για την ανάπτυξη και την ανάπτυξη λογισμικού. Επιπλέον, πρέπει να είναι σαφές για ποιο λόγο μπορούν να χρησιμοποιηθούν τα διάφορα εργαλεία.

Αυτό συνεπάγεται την περιγραφή εγκεκριμένων εργαλείων και συναφών χαρακτηριστικών ασφάλειας που μπορούν να βοηθήσουν στην αυτοματοποίηση και την επιβολή διαδικασιών ασφαλείας στην κωδικοποίηση. Ο κατάλογος θα πρέπει επίσης να περιλαμβάνει τα συστατικά που υποστηρίζουν και τα εξαρτήματα και τα εργαλεία ανάπτυξης άλλων κατασκευαστών επιτρέπεται να χρησιμοποιηθούν κατά την ανάπτυξη. Τα εργαλεία και τα υποστηρικτικά εξαρτήματα πρέπει να αξιολογούνται με βάση τον κίνδυνο και να αναλύονται για ευπάθειες

Το λογισμικό σήμερα αποτελείται συχνά από πολλές συνεργαζόμενες υπηρεσίες. Αυτό σημαίνει ότι ένας πολύ μεγαλύτερος αριθμός γλωσσών προγραμματισμού, βιβλιοθηκών και πλαισίων χρησιμοποιείται τώρα στην ανάπτυξη λογισμικού από ό, τι στο παρελθόν.. Παραδείγματα τέτοιων εργαλείων μπορούν να βρεθούν στο GitHub και στο Docker Security Scanning.

6.4.4.2 Απενεργοποιήστε τις ανασφαλείς λειτουργίες και τις λειτουργικές μονάδες

Πολλές λειτουργίες, API, βιβλιοθήκες και τρίτα μέρη οι ενότητες ενδέχεται να είναι ανασφαλείς για χρήση βάσει των σημερινών επιπέδων απειλών. Πρέπει να γίνει ανάλυση για όλες τις λειτουργίες, τα API, τις βιβλιοθήκες τρίτων και τις ενότητες που χρησιμοποιούνται κατά την ανάπτυξη του λογισμικού. Αυτά που δεν είναι ασφαλή θα πρέπει να απαγορευτούν, ενώ αυτά που είναι ξεπερασμένα ή περιέχουν γνωστά τρωτά σημεία θα πρέπει να ενημερώνονται.

Όταν είναι διαθέσιμη μια μαύρη λίστα, ο κώδικας πρέπει να ελεγχθεί (συμπεριλαμβανομένου κληρονομούμενου κώδικα) για να αντικαταστήσει τις μαύρες λίστες με ασφαλέστερες εναλλακτικές λύσεις. Αυτό μπορεί να γίνει χρησιμοποιώντας εργαλεία σάρωσης κώδικα. Επιπλέον, πρέπει να ελέγχεται ο κώδικας για να απενεργοποιηθεί η περιττή παρακολούθηση, η καταγραφή και η συλλογή προσωπικών δεδομένων. Για παράδειγμα, οι επικίνδυνες λειτουργίες και οι μονάδες μπορούν σε ορισμένες περιπτώσεις να αντιμετωπιστούν με εργαλεία όπως ο Έλεγχος Εξάρτησης OWASP.

6.4.4.3 Στατική ανάλυση κώδικα και επανεξέταση κώδικα

Η στατική ανάλυση κώδικα και η αναθεώρηση του κώδικα πρέπει να εκτελούνται σε τακτική βάση. Η στατική ανάλυση κώδικα διασφαλίζει ότι ακολουθούνται κατευθυντήριες γραμμές για ασφαλή κωδικοποίηση και μπορούν να μετρηθούν για να διασφαλιστεί ότι οι έλεγχοι λειτουργούν. Θα πρέπει να χρησιμοποιήσετε όσο το δυνατόν περισσότερο τα αυτοματοποιημένα εργαλεία ανάλυσης κώδικα και ανασκόπησης κώδικα.

Επιπλέον, ο κώδικας θα πρέπει να επανεξετάζεται με το χέρι, ώστε να εξασφαλίζεται ότι τυχόν αδυναμίες που θα μπορούσαν να οδηγήσουν σε ακατάλληλη χρήση ή διαρροή προσωπικών δεδομένων. Για παράδειγμα, μπορεί να είναι δύσκολο να εντοπιστούν τα πρότυπα, διότι τα δεδομένα δεν αποτελούν απαραίτητα προσωπικά δεδομένα, αλλά οι συνδέσεις μεταξύ διαφορετικών τύπων δεδομένων μπορούν να παρέχουν προσωπικές πληροφορίες. Προκειμένου να διασφαλιστεί η προστασία των δεδομένων, είναι σημαντικό να χαρτογραφηθεί όπου στο λογισμικό αποθηκεύονται τα προσωπικά δεδομένα. Μια ανασκόπηση του κώδικα θα πρέπει να εξετάζει ειδικότερα την καταγραφή των προσωπικών δεδομένων. Μια κοινή αδυναμία είναι να γράψετε προσωπικά δεδομένα σε αρχεία καταγραφής εφαρμογών με ανεπαρκή ασφάλεια.

6.4.5 Έλεγχος (Testing)

Το τμήμα που αφορά τις δοκιμές περιλαμβάνει μια σύσταση για να ελεγχθεί εάν οι απαιτήσεις προστασίας και ασφάλειας των δεδομένων εφαρμόζονται σωστά, μια περιγραφή του είδους των δοκιμών ασφαλείας και μια εξήγηση της σημασίας της μοντελοποίησης απειλών και της ανάλυσης της επιφάνειας επίθεσης.

Κατά τη διάρκεια αυτής της δραστηριότητας, οι ελεγκτές ελέγχουν ότι οι απαιτήσεις για την προστασία δεδομένων και την ασφάλεια των πληροφοριών που ορίζονται κατά τις δραστηριότητες Απαιτήσεων και σχεδιασμού υλοποιήθηκαν όπως είχε προγραμματιστεί, καθώς και να επαληθεύσουν ότι οι απαιτήσεις πληρούνται σωστά.

Το λογισμικό πρέπει επίσης να δοκιμάζεται για ευπάθειες. Αυτό γίνεται με τη χρήση dynamic testing, fuzz testing, και penetration testing. Είναι σημαντικό να αναθεωρήσουμε την επιφάνεια προσβολής για να επαληθεύσουμε ότι οι φορείς επίθεσης που αποκαλύφθηκαν κατά τη διάρκεια της δραστηριότητας σχεδίασης, και πιθανοί νέοι φορείς προσβολής που εισάγονται κατά τη διάρκεια της κωδικοποίησης, αντιμετωπίζονται.

6.4.5.1 Δοκιμές για να διασφαλίζεται ότι πληρούνται οι απαιτήσεις για την προστασία και την ασφάλεια των δεδομένων (Test that requirements for data protection and security have been implemented)

Στο σημείο αυτό πρέπει να διεξάγονται δοκιμές για να διασφαλίζεται ότι πληρούνται οι απαιτήσεις για την προστασία και την ασφάλεια των δεδομένων μέσω του σχεδιασμού και της κωδικοποίησης και ότι οι απαιτήσεις έχουν εφαρμοστεί σωστά στο λογισμικό.

Ο κατάλογος ελέγχου που εκπονήθηκε κατά τη διάρκεια των απαιτήσεων πρέπει να χρησιμοποιηθεί για να βεβαιωθεί ότι όλα τα στοιχεία που απαιτούνται για την ικανοποίηση των απαιτήσεων περιλαμβάνονται στο λογισμικό.

Η επαλήθευση θα πρέπει να περιλαμβάνει νέα στοιχεία που θα εισαχθούν αργότερα στη διαδικασία ανάπτυξης, κατά τη διάρκεια του σχεδιασμού και της κωδικοποίησης. Για τη δοκιμή αυτή θα πρέπει να χρησιμοποιήσουμε προσωπικά δεδομένα.

6.4.5.2 Τεστ ασφαλείας (Security testing)

Οι έλεγχοι ασφαλείας περιλαμβάνουν ολοκληρωμένη δοκιμή του λογισμικού για να εντοπιστούν τα τρωτά σημεία και να διασφαλιστεί ότι ο κώδικας διασφαλίζει επαρκώς την ασφάλεια και την προστασία των δεδομένων. Συνιστάται η καθιέρωση διαδικασιών για την αυτόματη εκτέλεση δοκιμαστικών συνόλων, τα οποία θα πρέπει να εκτελούνται κάθε φορά που δημιουργείται το λογισμικό.

6.4.5.3 Δυναμικός έλεγχος (Dynamic testing)

Με τον δυναμικό έλεγχο ελέγχουμε τη λειτουργία του κώδικα που εκτελείται χρησιμοποιώντας εργαλεία ή εγχειρίδια για να αναλύσουμε τον τρόπο με τον οποίο συμπεριφέρεται το λογισμικό σε σχέση με διαφορετικά δικαιώματα χρήστη και σε περιπτώσεις κρίσιμων βλαβών ασφαλείας. Οι δοκιμές θα διασφαλίσουν ότι οι χρήστες έχουν πρόσβαση μόνο στις πληροφορίες και τη λειτουργικότητα για τις οποίες έχουν εξουσιοδοτηθεί. Είναι σημαντικό να επαληθεύσετε ότι οι προσπάθειες απόκτησης μη εξουσιοδοτημένων πληροφοριών καταγράφονται ως παραβιάσεις ασφαλείας.

6.4.5.4 Σκόπιμη ενεργοποίηση σφαλμάτων (Fuzz testing)

Αυτός ο τύπος δοκιμών διεξάγεται με σκόπιμη ενεργοποίηση σφαλμάτων στο λογισμικό. Αυτό μπορεί να γίνει χρησιμοποιώντας εργαλεία που στέλνουν τυχαία και εσφαλμένα δεδομένα (λανθασμένες τιμές εισόδου) σε όλα τα πιθανά πεδία εισόδου στο λογισμικό, είτε με το χέρι είτε χρησιμοποιώντας έξυπνα εργαλεία που αναλύουν τις ευπάθειες σε εφαρμογές ιστού.

6.4.5.5 Ανάλυση ευπαθειών (Penetration testing/vulnerability analysis)

Προκειμένου να ανιχνευθούν τα τρωτά σημεία, πρέπει να διενεργηθούν δοκιμές διείσδυσης ή ανάλυση ευπάθειας πριν από την απελευθέρωση και σε τακτά χρονικά διαστήματα. Μια τέτοια δοκιμή ασφάλειας πρέπει να είναι μια νόμιμη και εξουσιοδοτημένη προσπάθεια να βρεθούν, να εκμεταλλευτούν και να εντοπίσουν τρωτά σημεία.

6.4.5.6 Μοντέλο απειλής και επιφάνεια επίθεσης (Threat model and attack surface review)

Καθώς το λογισμικό μπορεί να διαφέρει από τις λειτουργικές και τεχνικές προδιαγραφές που ορίζονται κατά τις δραστηριότητες Απαιτήσεων και Σχεδιασμού, τόσο το μοντέλο απειλής όσο και η επιφάνεια επίθεσης θα πρέπει να αναθεωρηθούν μόλις το λογισμικό ολοκληρωθεί για απελευθέρωση. Αυτή η ανασκόπηση θα πρέπει να επαληθεύει ότι έχουν εντοπιστεί και διαχειριστεί νέοι φορείς επίθεσης που ενδέχεται

να έχουν εισαχθεί κατά τη διάρκεια της κωδικοποίησης και ότι το μοντέλο απειλής εξετάζεται σε σχέση με το πρόσφατα αναπτυχθέν λογισμικό.

6.4.6 Ημερομηνία κυκλοφορίας (Release date)

Κατά τη διάρκεια αυτής της δραστηριότητας, το λογισμικό είναι έτοιμο για να κυκλοφορήσει στην αγορά. Αυτό περιλαμβάνει τον προγραμματισμό για τον τρόπο με τον οποίο ο οργανισμός μπορεί να χειριστεί αποτελεσματικά περιστατικά που μπορεί να προκύψουν μετά την κυκλοφορία, καθώς και διαδικασίες ενημέρωσης του λογισμικού. Μια ολοκληρωμένη και τελική επισκόπηση ασφαλείας θα πρέπει να γίνει πριν από την κυκλοφορία του λογισμικού.

Σε οργανισμούς όπου οι εκδόσεις του λογισμικού είναι συχνές, πρέπει να εκπονηθεί ένα σχέδιο αντιμετώπισης περιστατικών πριν από την αρχική κυκλοφορία, ενώ οι αξιολογήσεις ασφάλειας θα πρέπει να διεξάγονται κατά την εκάστοτε κυκλοφορία. Είναι σημαντικό στο σημείο αυτό να αρχειοθετήσουμε όλα τα δεδομένα από την αναπτυξιακή διαδικασία.

6.4.6.1 Διαχείριση περιστατικών (Incident response plan)

Ο οργανισμός θα πρέπει να καταρτίσει ένα σχέδιο για τη διαχείριση περιστατικών που σχετίζονται με το λογισμικό. Το σχέδιο πρέπει να περιλαμβάνει καθορισμένους πόρους και ένα σημείο επαφής ή κέντρο ανταπόκρισης που να μπορεί να διαχειρίζεται περιστατικά. Το σχέδιο πρέπει να περιέχει σχετικές πληροφορίες επικοινωνίας για υποστήριξη και κλιμάκωση, συμπεριλαμβανομένων πληροφοριών επικοινωνίας για τον υπεύθυνο προστασίας δεδομένων του οργανισμού. Το σχέδιο θα πρέπει επίσης να περιλαμβάνει μια επισκόπηση του τρόπου διαχείρισης των κρουσμάτων κληρονομούμενων από τρίτους.

Ο υπεύθυνος προστασίας δεδομένων (data protection officer) και ο σύμβουλος ασφαλείας (security advisor) πρέπει να επαληθεύουν ότι όλες οι απαιτήσεις προστασίας και προστασίας δεδομένων έχουν εφαρμοστεί και λειτουργούν όπως προβλέπεται. Ο οργανισμός πρέπει να καθορίσει ποιος είναι εξουσιοδοτημένος να κάνει την τελική έγκριση για την απελευθέρωση του λογισμικού.

6.4.6.2 Αναθεώρηση (Full security review of the software)

Η αναθεώρηση πρέπει να βασίζεται σε προηγούμενες αναθεωρήσεις κατά τη διάρκεια της διαδικασίας ανάπτυξης και να περιλαμβάνεται στις πύλες ελέγχου που πρέπει να

πραγματοποιηθούν πριν από την απελευθέρωση. Όλες οι απαιτήσεις, οι αναλύσεις και οι αξιολογήσεις που διενεργούνται κατά τη διάρκεια της διαδικασίας ανάπτυξης πρέπει να επανεξεταστούν και να αποκαλυφθούν τυχόν αποκλίσεις. Θα πρέπει να συμμετέχουν διάφορες ομάδες εμπειρογνωμόνων σε κάθε επισκόπηση ασφαλείας, ώστε να εξασφαλίζεται η καλύτερη δυνατή αναθεώρηση των διαφόρων σεναρίων και συνεπειών, καθώς και η βέλτιστη δυνατή ποιότητα των μέτρων που εφαρμόζονται ως αποτέλεσμα.

6.4.7 Συντήρηση (Maintenance)

Πλέον έχουμε φτάσει στην τελική φάση του οδηγού μας όπου είναι το πιο σημαντικό στοιχείο αυτής της δραστηριότητας. Στο σημείο αυτό ο οργανισμός έχει εφαρμόσει ένα σχέδιο αντιμετώπισης περιστατικών (που προετοιμάστηκε κατά τη διάρκεια της δραστηριότητας απελευθέρωσης) και το ακολουθεί.

Ο οργανισμός πρέπει να είναι προετοιμασμένος να χειρίζεται περιστατικά, παραβιάσεις ασφαλείας και επιθέσεις που μπορεί να οδηγήσουν σε παραβιάσεις της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας (confidentiality, integrity, availability CIA) δεδομένων προσωπικού χαρακτήρα. Θα πρέπει να έχει ένα κέντρο απόκρισης που να μπορεί να χειρίζεται συμβάντα και να παρέχει ενημερώσεις, οδηγίες και πληροφορίες στους χρήστες και τα πρόσωπα στα οποία αναφέρονται τα δεδομένα.

6.4.7.1 Αντιμετώπιση περιστατικών (Handling incidents and data breaches)

Ο οργανισμός θα πρέπει να εφαρμόζει σχέδιο αντιμετώπισης περιστατικών. Όταν συμβαίνουν κρίσιμα συμβάντα, είναι σημαντικό να παραμείνετε ήρεμοι και να αναλύσετε το περιστατικό με ολοκληρωμένο τρόπο.

Η φύση του περιστατικού μπορεί να οδηγήσει σε αλλαγές στον τρόπο εκτέλεσης του σχεδίου. Η ομάδα συμβάντων πρέπει να γνωρίζει με ποιους να επικοινωνήσει, όταν είναι απαραίτητο, και ποιος είναι υπεύθυνος για την κατασκευή, τον έλεγχο και την εγκατάσταση ενημερώσεων. Η ομάδα περιστατικών αντιμετώπισης πρέπει επίσης να γνωρίζει ποιες προτεραιότητες ισχύουν, καθώς και ακριβώς τι μπορούν και πρέπει να κάνουν σε περίπτωση κρίσης. Προκειμένου να επιτευχθεί αυτό, το προσωπικό απαιτεί περιοδική εκπαίδευση για την αντιμετώπιση περιστατικών

Πώς να χειριστείτε περιστατικά και παραβιάσεις δεδομένων;

1. Εφαρμογή ενός σχεδίου για απόκριση περιστατικών διαχείρισης

2. Τα περιστατικά ασφάλειας πρέπει να έχουν υψηλή προτεραιότητα.

3. Αντιμετώπιση περιστατικών και παραβιάσεων δεδομένων:

- ✓ Εντοπίστε μη φυσιολογική δραστηριότητα, κίνηση, συμβάντα ασφαλείας και παραβιάσεις δεδομένων.

- ✓ Αναλύστε / επαληθεύστε αν η μη φυσιολογική δραστηριότητα, η κυκλοφορία, τα περιστατικά ασφάλειας και οι παραβιάσεις δεδομένων είναι πραγματικές παραβιάσεις ασφαλείας ή λάθος συναγερμός.

- ✓ Αναφέρετε παραβιάσεις ασφαλείας και παραβιάσεις δεδομένων σύμφωνα με τις εσωτερικές οδηγίες για τον χειρισμό της απόκρισης σε περιστατικά.

- ✓ Αντιμετώπιση συμβάντων ασφαλείας και παραβιάσεων δεδομένων σύμφωνα με το σχέδιο συνέχειας του οργανισμού για την αποκατάσταση της κανονικής κατάστασης συντήρησης, συντήρησης και λειτουργίας.

4. Η εκπαίδευση για την ανταπόκριση σε περιστατικά που καλύπτει απρόβλεπτα σενάρια πρέπει να γίνεται περιοδικά.

6.4.7.2 Διαδικασίες οργάνωσης για τη συντήρηση, την υπηρεσία και τη λειτουργία του λογισμικού (Maintenance, service and operation of the software)

Στο σημείο αυτό θα πρέπει να ακολουθήσουμε τις διαδικασίες της οργάνωσης για τη συντήρηση, την υπηρεσία και τη λειτουργία του λογισμικού. Αυτό περιλαμβάνει διαδικασίες για τη συνεχή διασφάλιση της προστασίας και της ασφάλειας των δεδομένων. Παραδείγματα τέτοιων διαδικασιών είναι οι τακτικοί έλεγχοι ασφαλείας, η ανάλυση ευπάθειας και οι δοκιμές διείσδυσης του λογισμικού, της υποδομής και του δικτύου. Οι διαδικασίες θα πρέπει να περιλαμβάνουν error debugging, performance improvements, updates, and patching. Είναι σημαντικό να ορίσετε τι μπορεί και τι πρέπει να καταγραφεί. Η εταιρεία πρέπει επίσης να έχει την ικανότητα να εξασφαλίζει τακτικά, να παρακολουθεί και να χειρίζεται περιστατικά στα αρχεία καταγραφής.

Η εταιρεία θα πρέπει να έχει ένα σύστημα διαχείρισης για την προστασία δεδομένων και την ασφάλεια των πληροφοριών που περιλαμβάνει προμήθεια, συντήρηση, εξυπηρέτηση και λειτουργία. Το σύστημα διαχείρισης θα πρέπει να καθιερωθεί σύμφωνα με αναγνωρισμένα πλαίσια, όπως:

- ✓ ISO 27001

- ✓ Το πρότυπο ISF για ορθή πρακτική της ασφάλειας πληροφοριών (SoGP)

6.4.7.3 Γιατί να επιβάλλετε απαιτήσεις για συντήρηση, συντήρηση και λειτουργία;

1. Ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να έχει πλήρη καταγραφή των δραστηριοτήτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα και επεξεργαστών δεδομένων

2. Πρέπει να τηρούν παρόμοιο αρχείο των ενεργειών τους για λογαριασμό διαφορετικών ελεγκτών δεδομένων, βλ. Άρθρο 30.

3. Υπάρχουν απαιτήσεις ασφάλειας για την επεξεργασία προσωπικών δεδομένων, βλ. Άρθρο 32.

4. Υπάρχουν απαιτήσεις για την προστασία δεδομένων από το σχεδιασμό και από προεπιλογή σε λύσεις, προγράμματα, εφαρμογές και συστήματα που διαχειρίζονται προσωπικά δεδομένα, βλ. Άρθρο 25.

5. Υπάρχουν απαιτήσεις για την αξιολόγηση των επιπτώσεων στην προστασία δεδομένων εκκίνηση ή για σημαντικές αλλαγές σχετικά με την επεξεργασία προσωπικών δεδομένων, βλ. Άρθρο 35.

6. Υπάρχουν απαιτήσεις για την εξασφάλιση των δικαιωμάτων του υποκειμένου των δεδομένων, βλ. άρθρα 12-23.

7. Υπάρχουν απαιτήσεις για τη διασφάλιση της συμμόρφωσης με τις αρχές προστασίας της ιδιωτικής ζωής, βλ. Άρθρο 5.

8. Ο υπεύθυνος επεξεργασίας υποχρεούται να χρησιμοποιεί επεξεργαστές δεδομένων οι οποίοι δεσμεύονται από αυτόν τους Γενικούς Κανονισμούς Προστασίας Δεδομένων, βλ. Άρθρο 28

7. ΣΥΜΠΕΡΑΣΜΑΤΑ

Παρατηρήσαμε ότι τα χαρακτηριστικά προστασίας προσωπικών δεδομένων και δεδομένων γενικά, αγνοούνται από τις παραδοσιακές προσεγγίσεις στην υλοποίηση της επιθυμητής λειτουργικότητας. Αυτή η άγνοια προκαλείται και υποστηρίζεται από τους περιορισμούς στην ευαισθητοποίηση και την κατανόηση των προγραμματιστών και των υπευθύνων επεξεργασίας δεδομένων, καθώς και τα ελλιπή εργαλεία για την υλοποίηση της ιδιωτικής ζωής από το σχεδιασμό. Ενώ η ερευνητική κοινότητα είναι πολύ δραστήρια και αναπτυσσόμενη και συνεχώς βελτιώνει τα υφιστάμενα και συνεισφέροντας περαιτέρω δομικά στοιχεία, είναι μόνο χαλαρά συνδεδεμένη με την πρακτική. Αυτό το κενό πρέπει να γεφυρωθεί για να επιτευχθεί επιτυχής σχεδιασμός συστημάτων και υπηρεσιών φιλικό προς την ιδιωτικότητα και να εξελιχθεί η σημερινή κατάσταση της τέχνης. Περαιτέρω, η επιβολή της συμμόρφωσης με το ρυθμιστικό πλαίσιο για την προστασία της ιδιωτικής ζωής και των δεδομένων πρέπει να καταστεί αποτελεσματικότερη, δηλ. Χρειάζονται καλύτερα κίνητρα συμμόρφωσης καθώς και σοβαρές κυρώσεις για μη συμμόρφωση. Επίσης, η διαφύλαξη της ιδιωτικής ζωής μπορεί να προωθηθεί σε μεγάλο βαθμό από τα κατάλληλα πρότυπα, τα οποία θα πρέπει να ενσωματώνουν τα χαρακτηριστικά προστασίας της ιδιωτικής ζωής και των δεδομένων ως γενικό κανόνα.

8. ΒΙΒΛΙΟΦΡΑΦΙΑ

https://ec.europa.eu/info/index_en

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

https://www.owasp.org/index.php/OWASP_Secure_Application_Design_Project

https://www.ncsc.gov.uk/articles/secure-default-platforms

https://gdpr-info.eu/

National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html2

International Organization for Standardization - https://www.iso.org3

Privacy Management Reference Model and Methodology (PMRM) Version 1.0. 26 March 2012. OASIS Committee Specification Draft 01.http://docs.oasisopen.org/pmrm/PMRM/v1.0/csd01/PMRM-v1.0-csd01.html.

Open Web Application Security Project - https://www.owasp.org/index.php/Main_Page5

Cloud Security Alliance - https://cloudsecurityalliance.org/6

Center for Internet Security - https://www.cisecurity.org/7 DoD Information Security Agency - http://iase.disa.mil/stigs/Pages/index.aspx8

The American Institute of CPAs - http://www.aicpa.org9

Federal Trade Commission - https://www.ftc.gov10

Open Threat Taxonomy - http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a

https://www.imperva.com/data-security/regulation-glossary/gdpr/gdpr-article-25/

https://gdprinformer.com/gdpr-articles/7-key-principles-privacy-design

https://www.cio.com/article/2685279/internet/once-your-cars-connected-to-the-internet-who-guards-your-privacy.html#tk.drr_mlt

https://dentons.boekel.com/en/insights/alerts/2017/april/18/monthly-newsletter-gdpr-accountability-privacy-by-design-and-privacy-by-default

https://www.itgovernance.co.uk/blog/what-is-privacy-by-design

https://www.imperva.com/data-security/regulation-glossary/gdpr/gdpr-article-25/

https://www.i-scoop.eu/gdprarticle/gdpr-article-25-data-protection-design-default/

https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/gbl_thought_leadership_esa_gdpr_uea_v1_1

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

https://www.cio.com/article/2685279/internet/once-your-cars-connected-to-the-internet-who-guards-your-privacy.html#tk.drr_mlt

https://www.complianceforge.com/blog/security-privacy-by-design-principles/

https://en.wikipedia.org/wiki/Secure_by_default

https://ec.europa.eu/info/index_en

https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Privacy Payoff: How Successful Businesses Build Customer Trust Hardcover – 2002 by Ph.D. Ann Cavoukian (Author)

Privacy by Design: Take the Challenge Paperback – 2009 by Ann Cavoukian (Author)

https://m.isaca.org/chapters4/Sweden/OmOss/Documents/Stipendie2017_ElShekeil-Laoyookhong.pdf

Privacy by Design: A Hands-On Tutorial Paperback – October 14, 2017 by Gerard Blokdyk (Author)

European Commission RFID Applications Privacy and Data Protection Impact Assessment Framework

ACLU. American Civil Liberties Union The ACLU's view on Body Scanners.15 March 2002. https://www.aclu.org/technology-and-liberty/body-scanners (geopend October 30, 2014).

Antignac, T., Le Métayer, D.: Privacy architectures: Reasoning about data minimization and integrity. In: Mauw, S., Jensen, C.D. (eds.) Security and Trust Management,Lecture Notes in Computer Science, vol. 8743, pp. 17–32. Springer (2014)

Antignac, T., Le Métayer, D.: Privacy by design: From technologies to architectures.In: Preneel,B., Ikonomou, D. (eds.) Privacy Technologies and Policy, LectureNotes in Computer Science, vol. 8450, pp. 1–17. Springer (2014)

Article 29 Data Protection Working Party, ‘Opinion 02/2013 on apps on smart devices’ .Opinion, WP202, 00461/13/EN , 2013.

Article 29 Data Protection WP letter to the Commission.” 11 February 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2009_05_11_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf (geopend October 25, 2014).

Article29 WP. ‘The future of Privacy’ Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data .WP168, 2009.

AhnLab, AhnLab Reports the Analysis of the Best Apps in the Android Market, Seoul, April 2012

Brandimarte, L., Acquisti, A., Loewenstein, G., and Babcock, L., (2009) Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis, https://www.ideals.illinois.edu/handle/2142/15344.

Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, and Christophe Geuens. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, pages 63{78. USENIX Association, 2010.

Baldimtsi, Foteini, and Anna Lysyanskaya. "Anonymous credentials light." Proceedings of the ACM SIGSAC conference on Computer & communications security. ACM, 2013.

Boneh, D., Di Crescenzo, G., Ostrovsky, R., & Persiano, G. Public key encryption with keyword search. In Advances in Cryptology-Eurocrypt. pp. 506-522, Springer Berlin Heidelberg. 2004

S. Brands, Rethinking public key infrastructures and digital certificates: building in privacy. MIT Press, 2000.

Cavoukian, Ann. „Resolution of Privacy by Design, 32 International Conference of Data Protection and Privacy Commissioners.” Jerusalem, 2010.

J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Advances in Cryptology—EUROCRYPT 2001 (pp. 93-118). Springer Berlin Heidelberg. 2001.

J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In CRYPTO, volume 3152 of LNCS, pages 56–72. Springer, 2004.

J. Camenisch, S.Hohenberger and A. Lysyanskaya. Compact e-cash. In Advances in Cryptology–EUROCRYPT 2005 (pp. 302-321). Springer Berlin Heidelberg, 2005.

J. Camenisch, S. Hohenberger. M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. How to win the clonewars: efficient periodic n-times anonymous authentication. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 201-210). ACM, 2006.

Camenisch, Jan, and Thomas Groß. "Efficient attributes for anonymous credentials." ACM Transactions on Information and System Security (TISSEC) 15.1 (2012): 4.

Cavoukian, Ann. Privacy by Design, The 7 Foundational Principles. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In Proceedings on Advances in Cryptology. S. Goldwasser, Ed. Springer-Verlag New York, New York, NY, 319-327.1990.

Commission Nationale de l'Informatique et des libertés (CNIL), Google's new privacy policy : incomplete information and uncontrolled combination of data across services, 16 October 2012. http://www.cnil.fr/linstitution/actualite/article/article/googles-new-privacy-policy-incomplete-information-and-uncontrolled-combination-of-data-across-ser/

Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'15395/14 2012/0011 (COD) Brussels, 19 December 2014.

Court of Justice of the EU. „Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.” Press Release No 54/14, Luxembourg, 2014.

ConsumerReports.org. Facebook & your privacy, Who sees the data you share on the biggest social network?, Consumer Reports magazine, June 2012.

H. Corrigan-Gibbs and B. Ford. Dissent: accountable anonymous group messaging. In ACM conference on Computer and communications security(CCS '10). p. 340-350, 2010.

Curtmola, R., Garay, J., Kamara, S., and Ostrovsky, R. Searchable symmetric encryption: Improved definitions and efficient constructions. Journal of Computer Security, 19(5), 895-934. 2011.

Court of Justice of the EU. „C-427/12 European Commission v European Parliament, Council of the EU.” Biocides case, 2012.

Erin Ayers, Report sees 2014 overtaking 2013 in number of breaches, Cyber Risk Network, August 26, 2014

G. Danezis, R. Dingledine, N. Mathewson. Mixminion: Design of a type III anonymous remailer protocol. IEEE Symposium on Security and Privacy, 2003. Proceedings. IEEE. p. 2-15. 2003.

G. Danezis, S. Gürses. A critical review of 10 years of Privacy Technology, 2010.

Denis Butin, Daniel Le Métayer, Log Analysis for Data Protection Accountability, 19thInternational Symposium on Formal Methods (FM 2014), Springer Verlag LNCS Volume 8442, 2014, pp 163-178.

D. Dingledine, N. Mathewson, and P. Syverson. Tor: The second generation onion router. In Proceedings of the 13th USENIX Security Symposium, pages 303–319, 2004.

J. Domingo-Ferrer, A. Solanas, and J. Castellà-Roca. h(k)-private information retrieval from privacy uncooperative queryable databases. Online Information Review, 33(4):720–744, 2009.

Claudia Diaz, Omer Tene, Seda Gürses, Hero or Villain: The Data Controller in Privacy Law and Technologies, Ohio State Law Journal, Vol 74:6, pp. 923-964, 2013.

De Hert P., Gutwirth S. „Privacy, Data protection and Law enforcement. Opacity of the individual and transparency of the power, op.cit." In Privacy and the Criminal Law, door Anthony Duff and Serge Gutwirth Erik Claes. 2006.

C. Dwork. Differential Privacy. In 33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006), 2006.

EDPS. "EDPS comments on the draft proposals for a Commission Regulation amending Regulation (EC) No 272/20091 and for a Commission implementing Regulation amending Regulation (EC) No 185/20102 on common basic strandards on civil avaition security." EDPS.2011. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2011/11-10-17_Comments_security_scanners_EN.pdf (geopend October 25, 2014).

EDPS, "Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy." OJ C 280/01, 2010.

EDPS, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation -Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner", 26 November 2014.

European Commission. „Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union 4.11.2010 COM(2010) 609 final." COM, Brussels, 2010.

European Commission. Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).first draft, Brussels: COM(2012) 11 final, 2012.

European Parliament . Body Scanners at Airports: MEPs say that Fundamental Rights are Under Threat: Press Release 20081022IPR40394 .http://www.statewatch.org/news/2008/oct/ep-body-scanners-resolution.pdf (geopend October 20, 2014).

European Parliament „European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data." (General Data Protection Regulation).COM(2012)0011 -07 0025/2012, 12 March 2014.

European Parliament, Albrecht Report. „Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (GDPR)." Albrecht Report, 2012, 2012.

European Parliament, LIBE Committee. „Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR), unofficial consolidated version after LIBE vote provided by the Rapporte."consolidated version after LIBE vote, 2013.

European Union. European Union Legal Acts.2010. http://europa.eu/legislation_summaries/institutional_affairs/treaties/lisbon_treaty/ai0032_en.htm.

European Commission, 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' 2011.

Michael McConnell,IE 8 privacy filter neutered in favour of Microsoft's ad division. Examiner, August 4, 2010. http://www.examiner.com/article/ie-8-privacy-filter-neutered-favor-of-microsoft-s-ad-division