

**Dr. Γιώργος Χ. Στεργιόπουλος**, B.Sc., M.Sc., Ph.D.

Lecturer, IT Security Researcher and Consultant Ταχυδρομική διεύθυνση:

**Τμήμα Πληροφορικής**

τηλ. 210-82.03.158 Πατησίων 76

e-mail: [geostergiopHYPERLINK "mailto:dgrit@aueb.gr"@HYPERLINK "mailto:dgrit@aueb.gr"auebHYPERLINK "mailto:dgrit@aueb.gr".HYPERLINK "mailto:dgrit@aueb.gr"gr](file:///C:\Users\giakovakis\Desktop\ISSEC-17-project\geostergiop@aueb.gr), website: [www.infosec.aueb.gr](http://www.cis.aueb.gr/) Αθήνα 10434

**Τμήμα Πληροφορικής**

Χειμερινό εξάμηνο 2019-20

**AΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

**«Ανάλυση και Διαχείριση Επικινδυνότητας**

**σε περιβάλλον Τραπέζης**»

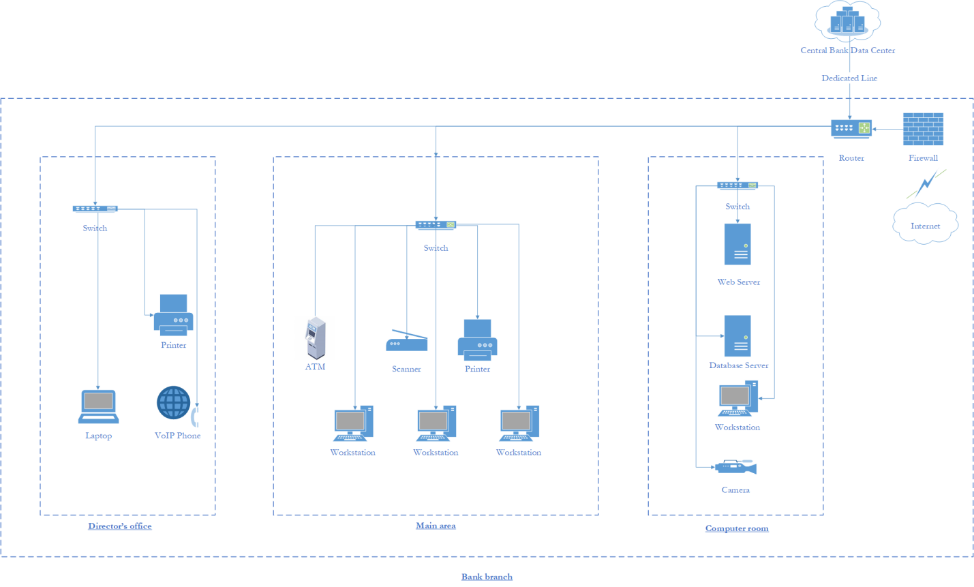
Γραπτή εργασία προόδου

Η ανάλυση επικινδυνότητας των Πληροφοριακών Συστημάτων αποτελεί έναν πρότυπο έλεγχο των υποδομών, διαδικασιών και λογισμικού κάθε εταιρείας και οργανισμού προκειμένου να εντοπιστούν πιθανές απειλές, υπάρχουσες ευπάθειες στην ασφάλειά του και να υπολογιστούν οι συνέπειες από την πραγματοποίηση μιας υπάρχουσας απειλής.

Μία τράπεζα χρειάζεται την υλοποίηση ενός Πληροφοριακού Συστήματος για την αποτελεσματική της λειτουργία, την καταγραφή και εξυπηρέτηση των πελατών της. Βασίζεται στις διαδικτυακές τεχνολογίες επικοινωνιών και νέας γενιάς συσκευών επεξεργασίας και αποθήκευσης πληροφοριών.

Στην παρούσα εργασία καλείστε να εκπονήσετε **μία ολοκληρωμένη πρόταση ενός σχεδίου ασφαλείας** μιας εταιρείας που ειδικεύεται σε θέματα τραπεζών που επεξεργάζονται προσωπικά δεδομένα, χωρίς όμως να γνωρίζουν αυτά από θέματα ασφάλειας δικτύων και πληροφοριακών συστημάτων. Στηριχτείτε στην τοπολογία που σας δίνεται στην ακόλουθη σελίδα.

Το σχέδιο ασφάλειας που θα παραδώσετε πρέπει **να παρουσιάσει όλα τα βήματα ανάλυσης επικινδυνότητας** (προφανώς σε θεωρητικό επίπεδο καθώς δεν μπορείτε να χρησιμοποιήσετε το εργαλείο), δηλαδή να εντοπίζονται και να περιγράφονται τα οργανωτικά και τεχνικά μέτρα που πρέπει να ληφθούν για την διαχείριση της επικινδυνότητας, αφού πρώτα έχετε εντοπίσει πιθανές απειλές και ευπάθειες του συστήματος \*.



**\* Σας δίνεται η αρχική καταγραφή και προσδιορισμός των αγαθών** βάσει σχήματος στο συνοδευτικό αρχείο **BankAsset Inventory2019.xlsx.** Πέραν των αγαθών που αναγράφονται στο σχήμα και στο excel, παρουσιάζονται κάποιες διεργασίες (processes) που συνοψίζουν τις επιχειρησιακές διαδικασίες της τράπεζας. Καλείστε να τις αξιολογήσετε αναλόγως, **αλλά να μην επεκταθείτε σε περαιτέρω πιθανές διαδικασίες.**

**\*** Κατά την συγγραφή και πρόταση των μέτρων ασφάλειας στο κείμενο του Σχεδίου, κάθε μέτρο που προτείνετε πρέπει να συνοδεύεται μετά από τα ID των αγαθών που προστατεύουν. Το Inventory ID υπάρχει στην λίστα του excel φύλλου BankAsset Inventory 2019. **Πιθανή καταγραφή μέτρων χωρίς σύνδεσή τους με 1 ή περισσότερα αγαθά ή υπηρεσίες/διαδικασίες, συνεπάγεται μη βαθμολόγηση του συγκεκριμένου μέτρου.**

**\* Σας δίνεται excel φύλλο (ISO27k FMEA - Risk Assessment spreadsheet\_2019.xlsx)** που παρέχει μέσα όλες τις αναγκαίες δομές για την διεξαγωγή της προσομοίωσης ανάλυσης επικινδυνότητας **(**κλίμακες **Impact, Likelihood, Vulnerability** καθώς και **Risk Assessment** φύλλο με formula**).**

**\* Σας δίνεται ενδεικτικό template για το κείμενό σας** (Σχέδιο Ασφάλειας - Template), με περιεχόμενα και βασικά κεφάλαια που πρέπει να έχετε μέσα. **Μη τήρηση του template θα οδηγήσει σε απώλεια 15% του συνολικού βαθμού της εργασίας.**

Διευκρινίσεις:

* Το κείμενο που θα παραδώσετε πρέπει να ακολουθεί την κατάλληλη δομή, προσεκτική μορφοποίηση και αυτοματοποιημένα περιεχόμενα, όπως σας δίνονται στο συνοδευτικό **template** του σχεδίου ασφάλειας **Σχέδιο Ασφάλειας - Template.docx**.
* Μπορείτε να κάνετε οποιαδήποτε παραδοχή χρειαστείτε. **Πρέπει να προσθέσετε τουλάχιστον άλλα 3 αγαθά** τα οποία θα εντάξετε ρητά μετά από έρευνα, εύλογη σκέψη και τεκμηρίωση και εφόσον δεν παραβλάπτεται η γενικότητα των μελετών περιπτώσεων.
* Πρέπει να καταθέσετε, πέραν του **Σχέδιου ασφάλειας βασισμένο στο template που δίνεται σε μορφή PDF, και το excel ISO27k FMEA - Risk Assessment spreadsheet\_2019 συμπληρωμένο** με την αποτίμηση που θα πραγματοποιήσετε.

Διαδικαστικές διευκρινίσεις:

Παραδοτέο: Κείμενο τεκμηρίωσης σε μορφή pdf, έκτασης τουλάχιστον 2.000 λέξεων, μη προσμετρούμενων του υπάρχοντος κειμένου στο template και πιθανών βιβλιογραφικών πηγών που θα προστεθούν.

Υποβολή: Ηλεκτρονική διαβίβαση στο διδάσκοντα ([geostergiopHYPERLINK "mailto:dgrit@aueb.gr"@HYPERLINK "mailto:dgrit@aueb.gr"auebHYPERLINK "mailto:dgrit@aueb.gr".HYPERLINK "mailto:dgrit@aueb.gr"gr](file:///C:\Users\giakovakis\Desktop\ISSEC-17-project\geostergiop@aueb.gr)), μέχρι τη **Κυριακή, 1 Δεκεμβρίου** 2019, **ώρα 18:00** (δεν θα δοθεί παράταση).

Εκπόνηση: Ανά ομάδες, αποτελούμενες από **2-3 φοιτητές**.(δεν θα γίνουν δεκτές εργασίες που εκπονήθηκαν από έναν μόνο φοιτητή).

Βαρύτητα: Ποσοστό 30% του συνολικού βαθμού. Επιτυχόντες στο μάθημα είναι όσοι α­ξι­ο­­λογηθούν με ≥5.0 και στην εργασία και στο εργαστήριο και στην τελική γρα­πτή εξέταση.

Κατοχύρωση: Ο βαθμός της εργασίας κατοχυρώνεται, αποκλειστικά και μόνον, για τις (κα­νο­νι­κές) εξε­τα­στι­κές περιόδους Φλεβάρη και Σεπτέμβρη 2020.

Καλή επιτυχία!

**FAQ**

**-1)Τι γράφουμε στο -Α1 -Α1.1 - Α1.2 ?**

Στο 1.1 πρέπει να γράψετε μια εισαγωγή που περιγράφει σε μια παράγραφο τι είναι το έγγραφο αυτό (στην περίπτωσή σας, ένα σχέδιο ασφάλειας, στα πλαίσια της εργασίας κτλ.). Στο 1.2 γράφετε μια παράγραφο με την δομή του παραδοτέου, πχ. στην "...στην ενότητα Α2 παρουσιάζεται η μεθοδολογία που ακολουθήσαμε, στην ενότητα 3 περιγράφονται τα κυριότερα στοιχεία από την μελέτη και την ανάλυση επικινδυνότητας που εκπονήθηκε... κτλ.).

**-2) Πως να γράψουμε τα υλικά στο Α2.1.1 (Τι attributes να γράψουμε δηλαδή από το dataset και με τι μορφή(π.χ κείμενο ή στήλες)?**

Βάζετε έναν πίνακα και επιλέγετε τα κατάλληλα αγαθά από το excel που σας δόθηκε

**-3) Πως και πού γράφουμε την τεκμηρίωση σχετικά με τα τρία δικά μας assets?**

Δεν χρειάζεται να υπάρχει συγκεκριμένος τρόπος. Μια καλή ιδέα είναι να τα παρουσιάσετε μαζί με τα υπόλοιπα, σαν να ήταν κομμάτι τις αρχικής εκφώνησης. Απλά σημειώστε με μία πρόταση στο αντίστοιχο υποκεφάλαιο που εμφανίζονται ότι αυτό είναι δικό σας αγαθό. Αν θέλετε βάζετέ τα με κείμενο εκεί που καταγράφονται τα αγαθά.

**-4) Μπορούμε να προσθέσουμε ένα δωμάτιο ή μια πόρτα ή ένα κουμπί ως αγαθό στην εργασία?**

Όχι, τυπικά το κτήριο είναι το αγαθό όχι τα δωμάτια. Παρόμοια, το κουμπί είναι μέρος ενός ολόκληρου συστήματος (πχ. Υπολογιστής) και αυτό είναι το αγαθό, όχι το «γρανάζι». Επίσης, εστιάζετε σε ΙΤ και θέματα πληροφορικής όταν εισάγετε τα δικά σας αγαθά.

**-5)Στο Α2.2.2 βάζουμε στα software και τα OS των επιμέρους συσκευών που δεν αναφέρονται ρητά στο excel?**

Ναι αν θέλετε. Μπορείτε να τα προσθέσετε και ως ένα δικό σας αγαθό από τα τρία που πρέπει να βάλετε.

**-6) Πως να γράψουμε την δομή του δικτύου (σχεδιάγραμμα ή απλό κείμενο)?**

Βάζετε το σχεδιάγραμμα, όπως σας δίνεται στην εκφώνηση. Επίσης μπορείτε να πείτε 1-2 περιγραφικά λόγια (πχ. ότι είναι ένα δίκτυο μόνο κτλ.).

**-7) Το firewall, antivirus, IDS, security camera etc. ανήκει στα assets?**

Στα πλαίσια του μαθήματος ***ΔΕΝ*** βάζετε αυτά τα συστήματα ως αγαθά, γιατί τυπικά είναι μέτρα ασφάλειας και το θεωρούμε αγαθό μόνο σε ιδιαίτερες περιπτώσεις στα απλά σχέδια ασφάλειας.

**-8) Οι Διαδικασίες εμπίπτουν στα αγαθά?**

Αν εννοείτε επιχειρησιακές διαδικασίες (πληρωμή φόρου, κατάθεση χρημάτων κτλ) ναι είναι, αν εννοείς διαδικασίες τύπου "διαδικασία backup από υπολογιστές" προφανώς και όχι.

**-9) Πόσες απειλές να βάλουμε για κάθε asset?**

Θέλετε τουλάχιστον 1 απειλή ανά αγαθό στο excel, και συνολικά πρέπει να κάνετε 25-30 αλυσίδες το ελάχιστο, οπότε υπολόγισε. Επίσης, εστιάζετε σε ΙΤ απειλές.

**-10) Γίνεται να υπάρξει επίπτωση χωρίς ζημία στο αγαθό (Παράδειγμα: Είχαμε πει πως ο κίνδυνος πλήττει κάποιο αγαθό κι προκύπτει η επίπτωση. Από την άλλη όμως, σε περίπτωση switch sniffing αν κι η απειλή σχετίζεται με το switch,το αγαθό που πλήττεται κι έχει επιπτώσεις είναι τα datagrams.)?**

Μπορεί να υπάρχει impact σε πάνω από ένα αγαθό με την ίδια επίθεση. Επίσης το sniffing έχει impact λόγω data που κυκλοφορούν στο δίκτυο όχι λόγω switch, το switch είναι ο φορέας του vulnerability στην παρούσα περιγραφή. Impact στο switch δεν ορίζεται στην παρούσα φάση, impact έχει η τράπεζα και τα data όχι τόσο το switch ως αγαθό.

**-11) Γίνεται ένας κίνδυνος να ‘χει ως επίπτωση κάποιον άλλο κίνδυνο κι αν ναι πως διαμορφώνεται η αλυσίδα όταν υπάρχουν επιπτώσεις και στα δυο αγαθά?(π.χ. Αλυσίδα ριζικού κινδύνου ----> Αλυσίδα κινδύνου β)**

Ναι, μπορεί μια επίθεση να δώσει πρόσβαση για να γίνει δεύτερη αλλά μην το παρουσιάσετε έτσι. Εσείς θεωρείστε μια αλυσίδα με τον τελικό χειρότερο κίνδυνο στο impact και βάλτε τα vulnerabilities μαζί.