

**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 2020-21

**AΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

**«Ανάλυση και Διαχείριση Επικινδυνότητας**

**σε περιβάλλον Βιομηχανίας**»

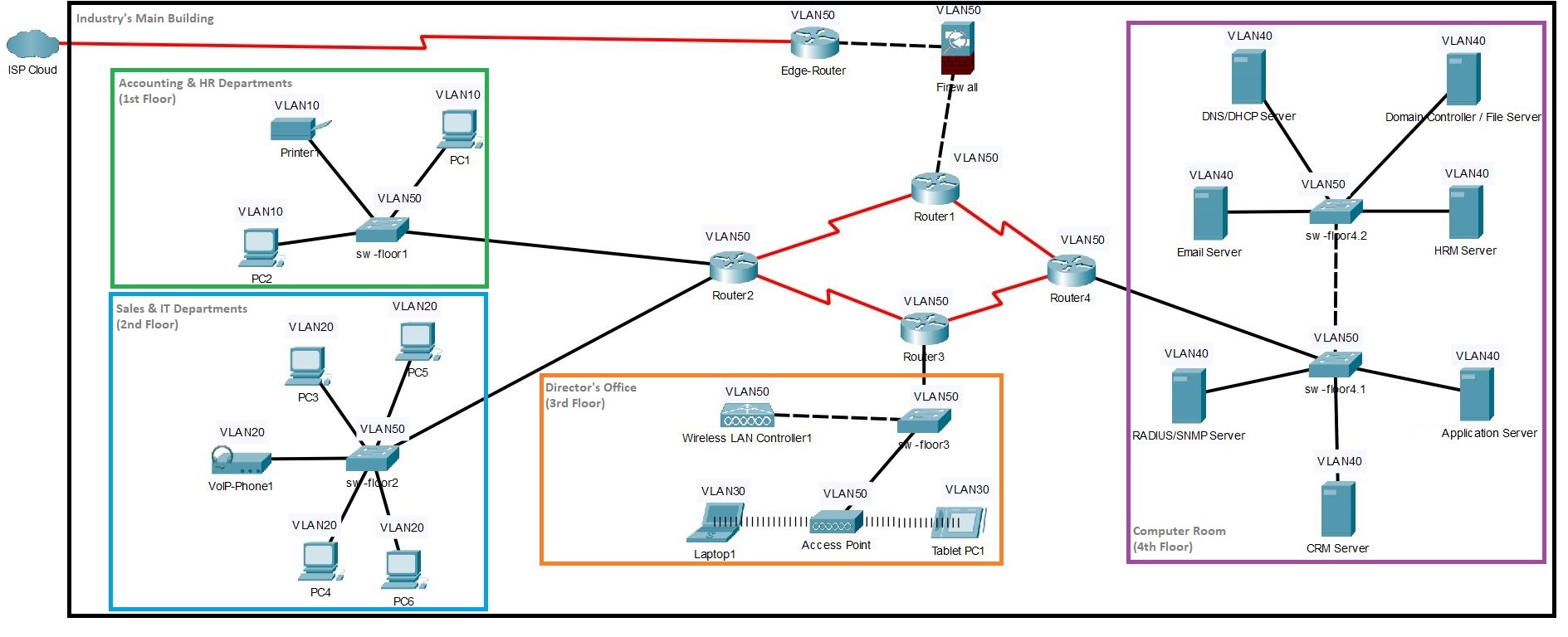
Γραπτή εργασία προόδου

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 βιομηχανία 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 για την απομακρυσμένη υλοποίηση βασικών λειτουργιών όπως πώληση προϊόντων, τιμολόγησης των πελατών της κτλ. Η εταιρεία μπορεί να πραγματοποιήσει πώληση τόσο στα γραφεία της εταιρίας (από κοντά) όσο και απομακρυσμένα από μέσω διαδικτύου.

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

Προσοχή, το scope του project (εύρος προστασίας συστημάτων) είναι τα εταιρικά μηχανήματα της εταιρείας (σημειώνεται με μαύρο κουτί). Κάθε αγαθό στο σχεδιάγραμμα έχει ένα όνομα (κάτω από το εικονίδιο) **και σε ποιο υποδίκτυο ανήκει** με την IP του (πάνω από το εικονίδιο). Συμβουλευτείτε τον σχετικό πίνακα διευθύνσεων καθώς και τον επεξηγηματικό πίνακα για τους servers.



|  |  |
| --- | --- |
| VLANS 172.10.X.0/24 | |
| VLAN 10 | Accounting / Human Resources |
| VLAN 20 | Sales / IT |
| VLAN 30 | Director’s Office |
| VLAN 40 | Computer Room |
| VLAN 50 | Native/Management |

|  |  |
| --- | --- |
| Server Name | Χρήση |
| CRM Server | Διαχείριση των αλληλεπιδράσεων της βιομηχανίας με τους πελάτες της αυτοματοποιώντας διεργασίες πωλήσεων που πραγματοποιούνται στο χώρο της βιομηχανίας (local sales). |
| DNS/DHCP Server | Ονοματοδοσία στα δίκτυα υπολογιστών που χρησιμοποιούν το πρωτόκολλο IP, καθώς και δέσμευση και αντιστοίχιση των διευθύνσεων δικτύου στους hosts. |
| Domain Controller/File Server | Παρέχει έλεγχο ταυτότητας στους χρήστες ενός τομέα (domain) καθώς και τα δικαιώματα που έχουν για πρόσβαση σε αρχεία, φακέλους, πόρους κλπ. Επιπλέον λειτουργεί ως μία κεντρική αποθήκη δεδομένων και αρχείων. |
| Email Server | Επιτρέπει την ανταλλαγή email με οποιονδήποτε χρήστη του διαδικτύου. |
| HRM Server | Προσφέρει ολοκληρωμένη παρακολούθηση όλου του εργασιακού κύκλου, όπως προσέλκυση υποψηφίων, επιτάχυνση της ένταξης του νέου εργαζομένου στην παραγωγική διαδικασία, παρακολούθηση της ανάπτυξης και εξέλιξης του εργαζομένου κ.ο.κ. |
| RADIUS/SNMP Server | Παρέχει συγκεντρωτικά έλεγχο ταυτότητας, εξουσιοδότηση και υπηρεσίες παρακολούθησης χρηστών (**A**uthentication, **A**uthorization και **A**ccounting - **AAA**) για όσους συνδέονται και χρησιμοποιούν δικτυακές υπηρεσίες. Επιπλέον αποτελεί το σύστημα διαχείρισης του δικτύου καθώς εκτελεί εφαρμογές οι οποίες παρακολουθούν και ελέγχουν τις διαχειριζόμενες συσκευές όπως server, workstations, printers, routers κλπ. |
| Application Server | Διαχείριση των αλληλεπιδράσεων της βιομηχανίας με τους πελάτες αυτοματοποιώντας διεργασίες απομακρυσμένων πωλήσεων (remote sales). Ειδικότερα, λαμβάνει τα HTTP requests κι αλληλοεπιδρά με τον CRM Server για την διεκπεραίωση μια πώλησης. |

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.

Οδηγίες:

* **Σας δίνεται η αρχική καταγραφή και προσδιορισμός των αγαθών** βάσει σχήματος στο συνοδευτικό αρχείο **IndustryAsset Inventory2020.xlsx.** Πέραν των αγαθών που αναγράφονται στο σχήμα και στο excel, παρουσιάζονται κάποιες διεργασίες (processes) που συνοψίζουν τις επιχειρησιακές διαδικασίες της βιομηχανίας. 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 IndustryAsset Inventory 2020. **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\_2020.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**.
* Πρέπει να καταθέσετε, πέραν του **Σχέδιου ασφάλειας βασισμένο στο template που δίνεται σε μορφή PDF, και το excel ISO27k FMEA - Risk Assessment spreadsheet\_2020 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](mailto:geostergiop@aueb.gr)), μέχρι τη **Κυριακή, 6 Δεκεμβρίου** **2020**, **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 2021.

Καλή επιτυχία!

**FAQ**

1. **Τι γράφουμε στο -1 -1.1 - 1.2 ?**

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 2 παρουσιάζεται η μεθοδολογία που ακολουθήσαμε, στην ενότητα 3 περιγράφονται τα κυριότερα στοιχεία από την μελέτη και την ανάλυση επικινδυνότητας που εκπονήθηκε... κτλ.).

1. **Πως να γράψουμε τα υλικά στο 2.1.1 (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.

1. **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.

1. **Στο 2.1.2 βάζουμε στα software και τα OS των επιμέρους συσκευών που δεν αναφέρονται ρητά στο excel?**

Ναι αν θέλετε μπορείτε να τα προσθέσετε.

1. **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.).

1. **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.

1. **Οι Διαδικασίες εμπίπτουν στα αγαθά?**

Αν εννοείτε επιχειρησιακές διαδικασίες (δημιουργία πελάτη, δημιουργία παραγγελίας κτλ) ναι είναι, αν εννοείτε διαδικασίες τύπου "διαδικασία backup από υπολογιστές" προφανώς και όχι.

1. **Πόσες απειλές να βάλουμε για κάθε asset?**

Θέλετε τουλάχιστον 1 απειλή ανά αγαθό στο excel, και συνολικά πρέπει να κάνετε 40-45 αλυσίδες το ελάχιστο, οπότε υπολόγισε. Επίσης, εστιάζετε σε ΙΤ απειλές.

1. **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 και 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 βιομηχανία και τα data όχι τόσο το switch ως αγαθό.

1. **Γίνεται ένας κίνδυνος να έχει 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.