Μελέτη περίπτωσης

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑ 4.0

***Λέξεις κλειδιά*:** *κυβερνοασφάλεια, τεχνολογία, κυβερνοεπιθέσεις, ασφάλεια.*

Υπόβαθρο μελέτης περίπτωσης

Ο μεγάλος όγκος νέων τεχνολογιών, δημιουργεί ευκαιρίες και χώρους για κυβερνοεπιθέσεις, γι 'αυτό η διασφάλιση της ασφάλειας στον κυβερνοχώρο είναι ζωτικής σημασίας για την επιτυχία της Βιομηχανίας 4.0. Είναι πραγματικά σημαντικό για τους οργανισμούς να επικαιροποιούν τις γνώσεις και τα εργαλεία τους προκειμένου να ανταποκριθούν στις μελλοντικές προκλήσεις. Τα περισσότερα βιομηχανικά περιβάλλοντα δεν σχεδιάστηκαν με γνώμονα την υψηλή ασφάλεια στον κυβερνοχώρο. Τα συστήματα παραγωγής κινούνται τώρα προς τα κυβερνο-φυσικά συστήματα, όπου τυχόν αδυναμίες θα μπορούσαν να εντοπιστούν και να αξιοποιηθούν από κακόβουλα άτομα.

Εισαγωγή στην παρούσα μελέτη περίπτωσης και στην ανάπτυξή της μέσα στην Βιομηχανία 4.0

Η ασφάλεια στον κυβερνοχώρο εξακολουθεί να συνδέεται με την προστασία από ιούς ή κακόβουλο λογισμικό, αλλά σήμερα η κλίμακα και η απειλή είναι σίγουρα περισσότερο παγκόσμια. Υπάρχουν όλο και περισσότερα οικονομικά εγκλήματα ή πράξεις κατασκοπείας, αλλά και επιθέσεις σε υποδομές ζωτικής σημασίας, η σε κυβερνήσεις. Για να ελαχιστοποιηθεί η απειλή και να αξιοποιηθεί η ευκαιρία που προσφέρει η Βιομηχανία 4.0, είναι απαραίτητο να διαδοθούν ευρέως και να εφαρμοστούν ορθές πρακτικές για την προστασία από απειλές στον κυβερνοχώρο.

Η ψηφιακή ασφάλεια πρέπει να είναι το αποτέλεσμα μιας ολοκληρωμένης πολιτικής διαχείρισης περιεχομένων πληροφορικής και της ενίσχυσης της ικανότητας των χρηστών. Ο ανθρώπινος παράγοντας είναι πιο δύσκολος από τον παράγοντα υλικής υποδομής, επειδή ο πιο συνηθισμένος λόγος για τη λήψη δεδομένων από τον χώρο εργασίας είναι η εμπλοκή των χρηστών, π.χ. με τη χρήση ιδιωτικού ταχυδρομείου ή τη σύνδεση μη εξουσιοδοτημένων φορέων δεδομένων. Οι εταιρείες υφίστανται πραγματικές οικονομικές ζημίες σε περίπτωση διαρροής εμπορικών και βιομηχανικών πληροφοριών.

Ως εκ τούτου, η προστασία των δεδομένων ξεκινά με την εφαρμογή και την επιβολή των κανόνων ασφαλείας από τους εργαζομένους.

Project No. 2019-1-PL01-KA202-064936

Μελέτη περίπτωσης

Μελέτη περίπτωσης και στοιχεία Βιομηχανίας 4.0 Περιληπτική Απεικόνιση.

Η Παγκόσμια Δικτύωση και η Βιομηχανία 4.0 ανοίγουν νέες ευκαιρίες για επικοινωνία και ανταλλαγή πληροφοριών, αλλά η ανεπαρκής ασφάλεια μπορεί να επιφέρει ορισμένους σοβαρούς κινδύνους και οικονομικές απώλειες. Η ασφάλεια, είναι μια διαδικασία κατά την οποία ένα σύνολο δραστηριοτήτων πρέπει να εκτελείται συνεχώς. Ένα από τα μοντέλα που περιγράφουν την ασφάλεια είναι το μοντέλο της Ε.Α.Δ. το οποίο κάθε εταιρεία πρέπει να καθορίσει, να παρακολουθεί και να συντηρεί.

Το μοντέλο ασφαλείας της Ε.Α.Δ. βασίζεται σε τρία βασικά στοιχεία:
*- **Εμπιστευτικότητα** - τα δεδομένα και οι υπηρεσίες θα πρέπει να είναι προσβάσιμα μόνο σε εκείνους που έχουν δικαίωμα σε αυτά (Confidentiality)*
*- **Ακεραιότητα** - κάθε προσπάθεια αλλοίωσης δεδομένων και υπηρεσιών θα πρέπει να εντοπίζεται και να καταγράφεται (Integrity)*
*- **Διαθεσιμότητα** – μόνο όποιος δικαιούται θα πρέπει να μπορεί να χρησιμοποιήσει τους πόρους (Availability).*

Project No. 2019-1-PL01-KA202-064936

Μελέτη περίπτωσης

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑ 4.0

Το στοιχείο που εξετάζεται για την εφαρμογή της Βιομηχανίας 4.0	*Η Polski Tytoń Dystrybucja είναι ένας από τους μεγαλύτερους διανομείς προϊόντων καπνού στην Πολωνία. Προσφέρει υπηρεσίες εφοδιαστικής αλυσίδας και εμπορικές υπηρεσίες. Η πώληση πραγματοποιείται από το Τμήμα Πωλήσεων και μέσω αντιπροσώπων πωλήσεων, οι οποίοι προσεγγίζουν απευθείας τους πελάτες. Η εταιρεία εργάζεται συνεχώς για τη βελτίωση της ποιότητας των υπηρεσιών της, ώστε να ταιριάζει καλύτερα στον απαιτητικό πελάτη. Για την παροχή υπηρεσιών στο υψηλότερο επίπεδο επενδύει στην κατάρτιση του προσωπικού και στον εκσυγχρονισμό του συστήματος.* *Η Polski Tytoń έχει εφαρμόσει το σύστημα διαχείρισης Axence nVision, το οποίο επιτρέπει τη διαχείριση και τη συνεχή υποβολή εκθέσεων σχετικά με την κατάσταση κάθε συσκευής που είναι συνδεδεμένη στο δίκτυο, αυξάνοντας έτσι το επίπεδο ασφάλειας των εφαρμογών πληροφορικής της εταιρείας.* *Η κύρια πρόκληση της εταιρείας, ήταν να βρει ένα εργαλείο που θα επέτρεπε τον έλεγχο των διαδικασιών που λαμβάνουν χώρα στο δίκτυο σε μεμονωμένα υποκαταστήματα. Ένας άλλος τομέας που έπρεπε να βελτιωθεί, ήταν η παρακολούθηση του εξοπλισμού πληροφορικής στην αίθουσα διακομιστών και στους μεμονωμένους σταθμούς εργασίας, καθώς και η χρήση υπολογιστών και συσκευών δικτύου από τους υπαλλήλους.* *Με την εφαρμογή αυτής της λύσης, η εταιρεία έχει τη δυνατότητα να συνεργαστεί με μια απομακρυσμένη κονσόλα, η οποία επιτρέπει σε καθορισμένους διαχειριστές να έχουν πρόσβαση στο πρόγραμμα από οποιονδήποτε υπολογιστή, αυτό διευκολύνει τη συνεχή παρακολούθηση των παραμέτρων της εφαρμογής, την προβολή του αρχείου καταγραφής συμβάντων ή τις υπηρεσίες του συστήματος. Η χρήση μονάδων δικτύου περιορίζει τη σύνδεση εξωτερικών ιδιωτικών συσκευών και επιτρέπει επίσης την παρακολούθηση των περιβαλλοντικών συνθηκών στην αίθουσα διακομιστών, η οποία παρέχει προστασία από αστοχίες.* *Ο διαχειριστής ενημερώνεται σε περίπτωση επικίνδυνης αύξησης της θερμοκρασίας του διακομιστή ή έλλειψης χώρου στο δίσκο. Η εταιρεία, επίσης έχει περιορίσει την λειτουργία προφίλ σε κοινωνικά δίκτυα και υπηρεσιών Youtube, κάτι που είχε θετικό αντίκτυπο στην απόδοση των εργαζομένων.*

Project No. 2019-1-PL01-KA202-064936

	Η εφαρμογή αυτής της λύσης έχει αποφέρει στην εταιρεία πολλά αποτελέσματα: *- Βελτίωση της διαφάνειας και της εταιρικής ευχρηστίας,* *-Πρόσβαση στο τμήμα πληροφορικής για την παρακολούθηση όλων των διαδικασιών που λαμβάνουν χώρα στο δίκτυο,* *- Πληροφορίες σχετικά με τα δεδομένα που συλλέγονται και αναλύονται από το σύστημα,* *- Εύκολη ανίχνευση δυσλειτουργιών όλων των συσκευών,* *-Μείωση του κόστους χρήσης και συντήρησης του εξοπλισμού πληροφορικής,* *- Αύξηση της αποτελεσματικότητας του τμήματος τεχνικής βοήθειας,* *- Έλεγχος της λειτουργίας και της χρήσης του δικτύου,* *-Αυξημένη αποτελεσματικότητα των επιχειρηματικών διαδικασιών,* *-Εξοικονόμηση χρόνου με το να είναι σε θέση να αντιδρά γρήγορα σε σφάλματα συστήματος και να παρέχει απομακρυσμένη βοήθεια στους υπαλλήλους.*
Ομάδα στόχος εφαρμογής	*Τα αποτελέσματα της παρούσας μελέτης περίπτωσης προορίζονται για χρήση από ΜΜΕ, επιχειρήσεις και επιχειρηματίες.*
Πηγές :	*https://axence.net/files/pdf/media/case_study_polski_tyton.pdf* *http://ptdystrybucja.pl/o-firmie/*
Περαιτέρω Βιβλιογραφία:	*https://ik.org.pl/wp-content/uploads/wyzwania-w-cyberprzestrzeni.-przyklady-rozwiazan-zagrozenia-regulacje.pdf* *https://axence.net/pl/o-nas* *http://websecurity.pl/pojecie-bezpieczenstwa-cia/*

Project No. 2019-1-PL01-KA202-064936