



Zelus Endpoint Security

**Προστασία τερματικών συσκευών,
υπολογιστών και συστημάτων**

Ιούλιος 2022

www.zelus.gr

Τατοΐου 92, 14452

Μεταμόρφωση, Αθήνα - GR

Σύντομη Περιγραφή

Στη σημερινή εποχή, το σύνολο των επιχειρήσεων του ιδιωτικού τομέα προχωρά στο σχεδιασμό και την υλοποίηση μακροπροθέσμων πλάνων για τον ψηφιακό τους μετασχηματισμό, βασιζόμενοι όλο και περισσότερο σε αντίστοιχες υπηρεσίες, εργαλεία και πληροφοριακά συστήματα. Έτσι, όλοι οι τομείς της οικονομίας στηρίζονται σε νέες, καινοτόμες τεχνολογίες για την αυτοματοποίηση και την εκτέλεση των εμπορικών και λοιπών δραστηριοτήτων τους. Παρά τις τεράστιες ευκαιρίες που προσφέρει η ψηφιοποίηση, το οικοσύστημα των επιχειρήσεων εκτίθεται όλο και περισσότερο σε κυβερνοαπειλές, ενώ, σύμφωνα με τα στοιχεία του Συμβουλίου της Ευρωπαϊκής Ένωσης, οι κυβερνοεπιθέσεις και τα κυβερνοεγκλήματα πολλαπλασιάζονται, οι δε μέθοδοι που χρησιμοποιούνται στις ενέργειες αυτές διαρκώς εξελίσσονται. Η τάση αυτή πρόκειται να ενισχυθεί περαιτέρω στο άμεσο μέλλον, καθώς αναμένεται ότι **22,3 εκατομμύρια συσκευές** παγκοσμίως θα είναι συνδεδεμένες στον Παγκόσμιο Ιστό έως το 2024. Αυτό έχει ως αποτέλεσμα να γεννάται η ανάγκη για εξειδικευμένα εργαλεία και **υπηρεσίες ψηφιακής ασφάλειας (cyber security)**, τα οποία μπορούν να αυξήσουν το επίπεδο ασφάλειας μίας επιχείρησης, ενισχύοντας την ικανότητα πρόληψης, εντοπισμού και διαχείρισης συμβάντων σχετικών με την κυβερνοασφάλεια, όπως αναφέρονται και στην Εθνική Στρατηγική Κυβερνοασφάλειας.

Προς την κατεύθυνση αυτή, η εταιρεία μας παρέχει το **Zelus Endpoint Security**, μία ολοκληρωμένη λύση προστασίας και ανίχνευσης απειλών ασφάλειας σε τερματικές συσκευές και κρίσιμα υπολογιστικά συστήματα και εφαρμογές. Σκοπός είναι η ολιστική προστασία της υποδομής και των υπαρχόντων πληροφοριακών συστημάτων, ιστοσελίδων και διαδικτυακών εφαρμογών με δημόσια πρόσβαση που διαθέτει μία επιχείρηση και η έγκαιρη ανίχνευση και αντιμετώπιση απειλών και επιθέσεων.

Προδιαγραφές

Η λύση Zelus Endpoint Security παρέχει ψηφιακά εργαλεία και υπηρεσίες για την αποτελεσματική προστασία και αντιμετώπιση κινδύνων ασφάλειας στον κυβερνοχώρο. Τα χαρακτηριστικά της λύσης συνοψίζονται στα ακόλουθα:

- Προστασία από πιθανές απειλές και κρίσιμα περιστατικά ασφάλειας στο διαδίκτυο (endpoint protection and security).
- Παρακολούθηση και προστασία της ψηφιακής δραστηριότητας μίας επιχείρησης, η οποία παράγεται από τις τερματικές συσκευές που χρησιμοποιούν οι χρήστες εντός μίας επιχείρησης.
- Παρακολούθηση και προστασία εισερχομένης και εξερχόμενης κίνησης στο διαδίκτυο και των ενεργειών που αφορούν την πρόσβαση σε υποσυστήματα και εφαρμογές που λειτουργεί ή χειρίζεται η επιχείρηση.
- Σύστημα ανίχνευσης περιστατικών ασφάλειας (intrusion detection).
- Ανάλυση, διαχείριση και οπτικοποίηση πιθανών απειλών και συμβάντων, μέσα από μία φιλική προς το χρήστη εφαρμογή διαδικτύου (online dashboard).

Πιο συγκεκριμένα, η λύση Zelus Endpoint Security μπορεί να παρακολουθεί ένα πλήθος υπολογιστών στο εσωτερικό δίκτυο μίας επιχείρησης και των τερματικών συσκευών (endpoint devices), όπως desktops, laptops, διακομιστές (servers), σταθμοί εργασίας (workstations), εκτυπωτές, εφαρμογές λογισμικού, routers, κλπ. Η λύση περιλαμβάνει τη συλλογή των αρχείων καταγραφής (logs) από αυτές τις συσκευές, συμπεριλαμβανομένων των αρχείων από το λειτουργικό σύστημα και τις βασικές

προεγκατεστημένες εφαρμογές τείχους προστασίας (firewall) και αντιϊικού προγράμματος (antivirus) και εν γένει από ψηφιακά στοιχεία με δημόσια πρόσβαση.

Επίσης, παρέχεται η δυνατότητα ενημέρωσης σχετικά με κρίσιμες απειλές και πιθανά συμβάντα και τους τρόπους αντιμετώπισης αυτών, καθώς και συστάσεις για την υιοθέτηση βέλτιστων πρακτικών ασφάλειας στο διαδίκτυο, με βάση τις απειλές και τους κινδύνους που αντιμετωπίζει η επιχείρηση. Στην περίπτωση εντοπισμού κρίσιμων απειλών, παρέχεται άμεση ενημέρωση με ηλεκτρονικά μέσα.

Η λύση Zelus Endpoint Security έχει αναπτυχθεί με κριτήρια την ανθρωποκεντρική προσέγγιση και την πρόσβαση στις παρεχόμενες υπηρεσίες σε όλους, υιοθετώντας διεθνή πρότυπα, κανόνες και βέλτιστες πρακτικές. Τα βασικά τεχνικά χαρακτηριστικά της λύσης περιλαμβάνουν:

- Υλοποίηση βασισμένη σε μία αρχιτεκτονική πολλαπλών επιπέδων και ανοιχτών προτύπων, με δυνατότητες συνεργασίας με διάφορες μορφές βάσεων δεδομένων, λειτουργικά συστήματα, εξυπηρετητές διαδικτύου & εφαρμογών.
- Παροχή και υποστήριξη συνεργατικών τεχνολογιών.
- Δυνατότητα διαχείρισης χρηστών και απόδοσης διαβαθμισμένης πρόσβασης σε συγκεκριμένες λειτουργίες και πληροφορίες συμβάντων.
- Εύκολη διασύνδεση και ενσωμάτωση με υπάρχοντα πληροφοριακά συστήματα ενός οργανισμού, βάσει διεθνών προτύπων και βέλτιστων πρακτικών, με χρήση ευρέως αποδεκτών τεχνολογιών και δομών μορφοποίησης και μετασχηματισμού δεδομένων και μεθόδων επικοινωνίας.
- Επεκτασιμότητα για την κάλυψη νέων και μελλοντικών υπηρεσιών σχετικά με τη διαχείριση περιπτώσεων ασφάλειας από πιθανές κυβερνοαπειλές.
- Τήρηση του Ελληνικού Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Προτύπων Διαλειτουργικότητας (e-GIF).
- Συμμόρφωση με διεθνή πρότυπα και οδηγίες για την ψηφιακή ασφάλεια δεδομένων, με τον Ευρωπαϊκό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), και τον κανονισμό διασφάλισης ιδιωτικότητας (e-Privacy).

Πρόσθετες Παροχές Λύσης

Παρέχεται η δυνατότητα εφαρμογής μέτρων πρόληψης και προστασίας από κυβερνοαπειλές, μέσα από την ασφαλή διαμόρφωση εξοπλισμού και κρίσιμων εφαρμογών προστασίας και τον έλεγχο για τη σωστή παραμετροποίηση της υπάρχουσας υποδομής ασφάλειας. Στην περίπτωση που η υποδομή της επιχείρησης δεν το υποστηρίζει, παρέχεται η δυνατότητα εγκατάστασης και παραμετροποίησης εφαρμογών τείχους προστασίας (firewall) και αντιϊικού προγράμματος (antivirus).