

18/10/2012

EPR16/2012  
www.enisa.europa.eu

## Πληροφορική στο Χώρο Εργασίας : Ο ENISA προβλέπει ευκαιρίες και κινδύνους στην τάση: «Φέρε τη προσωπική σου συσκευή στο γραφείο»

Η διαρκώς εξελισσόμενη τάση των ανθρώπων να χρησιμοποιούν προσωπικούς υπολογιστές, κινητά τηλέφωνα, κοινωνικά δίκτυα ή έξυπνες συσκευές και εφαρμογές για την εργασία προσφέρει οφέλη, αλλά εγκυμονεί και κινδύνους. Αυτό είναι το μήνυμα του Ευρωπαϊκού Οργανισμού Ασφάλειας Δικτύων και Πληροφοριών (ENISA) στην τελευταία έκθεσή του [Consumerisation of IT: Top Risks and Opportunities](#) (Καταναλωτικοποίηση της Πληροφορικής: Κορυφαίοι Κίνδυνοι και Ευκαιρίες).

Στο σημερινό πιεστικό περιβάλλον εργασίας, η κινητικότητα και η δικτυωμένη γνώση είναι δύο βασικοί παράγοντες διαμόρφωσης του μέλλοντος της επαγγελματικής ζωής. Οι παράγοντες αυτοί, σε συνδυασμό με τις υπάρχουσες προσφορές ειδών πληροφορικής προς ιδιωτική κατανάλωση, καθιστούν επιτακτική την ανάγκη εξέτασης του ρόλου των προσωπικών gadgets και υπηρεσιών σε εταιρικές στρατηγικές πληροφορικής. Η επιλογή «Φέρε τη προσωπική σου συσκευή» ((Bring Your Own Device), όπου οι υπάλληλοι χρησιμοποιούν τους προσωπικούς τους υπολογιστές για την υλοποίηση καθηκόντων στο χώρο εργασίας ή αλλού, μπορεί να έχει ένα ευρύ φάσμα πιθανών οφελών. Μεταξύ των ευκαιριών που προκύπτουν από την παρούσα καταναλωτική τάση στην πληροφορική είναι:

- η ευελιξία του εργοδότη και του προσωπικού σχετικά με τις ώρες και τον τόπο εργασίας,
- η εξοικονόμηση μέσω της μείωσης του κόστους υποδομών,
- η αύξηση της παραγωγικότητας και της ικανοποίησης του προσωπικού, μέσω της ανάπτυξης των δικών τους δεξιοτήτων,
- η μείωση του κόστους της υποδομής μέσω της μετάβασης σε ευέλικτες λύσεις πληροφορικής, όπως το cloud computing.

Ωστόσο, με τα πιθανά οφέλη ενέχονται και κίνδυνοι, οι οποίοι πρέπει να προβλεφθούν αλλά και να αντιμετωπιστούν με κατάλληλες πολιτικές και στρατηγικές ασφάλειας. Μεταξύ των σημαντικότερων κινδύνων είναι οι εξής:

- απώλεια, κλοπή ή δημοσιοποίηση εμπιστευτικών πληροφοριών, είτε λόγω κακής πληροφοριακής ασφάλειας της προσωπικής συσκευής είτε λόγω κλοπής κινητών συσκευών ή υπολογιστών,
- πιθανά ζητήματα με κυριότητα δεδομένων, παράνομη διάδοση εταιρικών πληροφοριών, παράνομη χρήση συσκευών, προγραμμάτων και περιεχομένου,
- αυξημένες δυνατότητες για τους εγκληματίες του κυβερνοχώρου να στοχεύσουν σε εταιρικά δεδομένα.

Γενικά, ο ENISA εντοπίζει τρεις βασικούς τομείς κινδύνου, που σχετίζονται με το κόστος, τα ζητήματα νομοθεσίας και ρυθμιστικού πλαισίου, καθώς και την εμπιστευτικότητα / την ακεραιότητα/ τη διαθεσιμότητα των δεδομένων. Πιθανά οφέλη εμπίπτουν στους τομείς των οικονομικών, των ανθρωπίνων πόρων, των επιχειρησιακών ευκαιριών και της διαχείρισης δεδομένων.

Σχολιάζοντας την έκθεση, ο Εκτελεστικός Διευθυντής του ENISA, καθηγητής [Udo Helmbrecht](#), δήλωσε: «Στο σημερινό χώρο εργασίας, η κινητικότητα και η αύξηση της κατανάλωσης πληροφορικών συσκευών και υπηρεσιών αποτελούν συχνά ευκαιρία για εργαζομένους και εργοδότες να αποκομίσουν αμφίπλευρα οφέλη που προσφέρουν οι σύγχρονοι τομείς της πληροφορικής: αυξημένη ευελιξία και δυνατότητες



18/10/2012

EPR16/2012  
[www.enisa.europa.eu](http://www.enisa.europa.eu)

μείωσης του κόστους. Ορισμένοι από τους σχετικούς κινδύνους ασφαλείας είναι αρκετά κλασσικοί, όπως η αδυναμία να διασφαλιστεί η ασφάλεια των συσκευών και των εφαρμογών καθώς και η ανάρμοστη διάδοση πληροφοριών. Άλλοι κίνδυνοι, όπως ζητήματα νομιμότητας, είναι πιο περίπλοκοι όμως εάν αντιμετωπιστούν σωστά, θα επιτρέψουν τη δημιουργία πιο αποτελεσματικών εργαλείων και συνθηκών εργασίας.»

Η έκθεση είναι διαθέσιμη [εδώ](#).

Για συνεντεύξεις: Ulf Bergström, εκπρόσωπος, ENISA, Κινητό τηλέφωνο: +30 6948 460 143, ή Λούης Μαρίνος, [RiskManagement@enisa.europa.eu](mailto:RiskManagement@enisa.europa.eu).

*Μετάφραση. Η έκδοση στην αγγλική γλώσσα είναι η μόνη έγκυρη.*

<http://www.enisa.europa.eu/media/enisa-in-greek/>

[www.enisa.europa.eu](http://www.enisa.europa.eu)

