



***The IT Security
Expert Profile***

Dimitris Gritzalis

February 2013

Ελληνική Αστυνομία
2^ο Συνέδριο Υποδ/σης Δίωξης Ηλεκ/κού Εγκλήματος
«Η ασφαλής πλοήγηση είναι υπόθεση όλων μας»
Αθήνα, Φεβράρης 2013

*Ο μορφότυπος του
Ειδικού Ψηφιακής Ασφάλειας
στο πλαίσιο της κρίσης*

Δημήτρης Α. Γκρίτζαλης

(dgrit@aub.gr, www.cis.aub.gr)

Καθηγητής Ασφάλειας Πληροφορικής & Επικοινωνιών
Διευθυντής Προγράμματος Μεταπτυχιακών Σπουδών
Τμήμα Πληροφορικής
Οικονομικό Πανεπιστήμιο Αθηνών

Το *puzzle* και η “διανομή των ρόλων”

Ε.Ε., Δ.Ν.Τ., Π.Δ.Ε., Επιχειρήσεις (Χρηματοδότες)

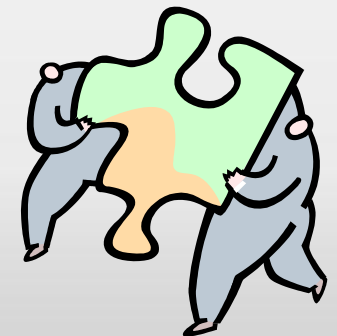
Κυβέρνηση, Οργανισμοί (Διαχειριστές)

Εταιρείες ΤΠΕ κ.ά. (Προμηθευτές)

Χρήστες (Δημόσια Διοίκηση, Οργανισμοί κ.ά.)

Πολίτες (Πελάτες, Χρήστες)

Ειδικοί Ψηφιακής Ασφάλειας (εσ/μείς)



Η κυρίαρχη (;) αντίληψη κάθε ρόλου

Εταιρείες ΤΠΕ κ.ά. (Προμηθευτές)

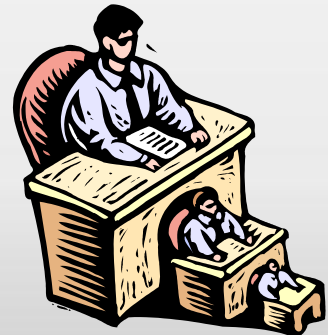
- ⇒ “Είναι ευέλικτο το εργασιακό καθεστώς;”
- ⇒ “Είναι ρεαλιστικό το πλαίσιο προμηθειών;”
- ⇒ “Τα περιθώρια, στο έργο αυτό, είναι πολύ μικρά”
- ⇒ “Ε, όχι! Θα ζητήσω ασφαλιστικά μέτρα!”
- ⇒ Ειδικός Ψηφιακής Ασφάλειας;
“Είναι απαραίτητος; Τι λέει η σύμβαση;”



Η κυρίαρχη (;) αντίληψη κάθε ρόλου

Χρήστες (Δημόσια Διοίκηση, Οργανισμοί κ.ά.)

- ⇒ “Ποια κίνητρα προβλέπονται;”
- ⇒ “Αυτά μας τα ‘παν κι άλλοι!”
- ⇒ “Δεν μπορώ να τα κάνω όλα μόνος μου!”
- ⇒ “Βγαίνω στη σύνταξη/εφεδρεία”
- ⇒ “Χρειάζομαι - επιπλέον αυτών - και...”
- ⇒ “Υπάρχουν άλλες προτεραιότητες”
- ⇒ Ειδικός Ψηφιακής Ασφάλειας;
“Για ασφάλεια θα φροντίσει ο προμηθευτής!”



Εμείς, οι Πληροφορικοί

Αυτοκριτικά

Ως χρήστες (ή ως πελάτες):

- ⇒ Γενικά, “έχουμε άποψη”!
- ⇒ Συνήθως, δεν αμοιβόμαστε “αρκετά”...
- ⇒ “Ο manager μου ευνοήθηκε, αλλιώς εγώ...”
- ⇒ “Εγώ απλώς εισηγούμαι”
- ⇒ “Δεν παραλαμβάνω!”



Εμείς, οι Πληροφορικοί

Όποιοι κι αν είμαστε:

- ⇒ Δεν συμμεριζόμαστε το ίδιο όραμα (*γιατί άλλωστε;*)
- ⇒ Λειτουργούμε αποσπασματικά ή μοναχικά (*ξέρουμε πού οφείλεται;*)
- ⇒ Μπορούμε - και πρέπει - να κρίνουμε (*όπως και να κρινόμαστε!*)
- ⇒ Κανένας μας δεν περισσεύει (*αλλά και όλοι μαζί ίσως δεν αρκούμε...*)



Ερωτήματα του Πολίτη - Ειδικού Ασφάλειας

Το όραμά μας δεν (μπορεί να) είναι ανάπτυξη χωρίς κοινωνικά αντίβαρα. **Ποιά είναι αυτά;**

Το ΕΣΠΑ είναι ένας ακόμη (μείζον) κρίκος σε μια αναπτυξιακή αλυσίδα. **Ποιός τη διαμορφώνει;**

(Συν)Ευθυνόμαστε για τη μορφή που έχει πάρει η Κοινωνία της Πληροφορίας. **Ποιά μορφή θέλουμε;**

Έχουμε “άποψη”, αλλά δεν έχουμε “φωνή”. **Γιατί;**

Ψηφιακή ανάπτυξη χωρίς ασφάλεια και ιδιωτικότητα είναι “ρότα δίχως πυξίδα”. **Πώς να παρέμβουμε;**

Ειδικοί Ψηφιακής Ασφάλειας

- ⇒ Η ψηφιακή ασφάλεια είναι **ολιστικό ζήτημα** - δεν είναι, ούτε πρωτίστως, ούτε αμιγώς, τεχνικό ζήτημα.
- ⇒ Η ψηφιακή ασφάλεια είναι επιτεύξιμη με **μεθοδικές προσεγγίσεις** - όχι με αποσπασματικές παρεμβάσεις.
- ⇒ Η ψηφιακή ασφάλεια απαιτεί **Ειδικούς Ψηφιακής Ασφάλειας** - όχι (τυχάρπαστους) εμπειροτέχνες.
- ⇒ Η ψηφιακή ασφάλεια απαιτεί **ειδικές επιστημονικές γνώσεις/δεξιότητες** - δεν αρκούν (μόνον) πιστοποιήσεις.
- ⇒ Ο ρόλος του **ανθρώπινου παράγοντα** - των αξιών, του ήθους, της προσωπικότητας - παραμένει θεμελιώδης.
- ⇒ **“Too much security is bad security!”**



Ψηφιακή Ασφάλεια: Με ποια πυξίδα; (1/2)

1. Σε κάθε πολίτη πρέπει να παρέχονται επαρκώς ασφαλείς ψηφιακές υπηρεσίες.
2. Η ψηφιακή ασφάλεια προϋποθέτει γνώση, ευαισθητοποίηση και υπευθυνότητα.
3. Η ψηφιακή ασφάλεια είναι ολιστικό ζήτημα, με κύρια συνιστώσα τον ανθρώπινο παράγοντα.



Ψηφιακή Ασφάλεια: Με ποια πυξίδα; (2/2)

4. Η ψηφιακή ασφάλεια προϋποθέτει **επιστημονική και κοινωνική υπευθυνότητα** και διευκολύνεται από τη **συλλογική δράση**.

5. Η ψηφιακή ασφάλεια είναι, πρωτίστως, έργο **ειδικών επιστημόνων**.

6. Η ψηφιακή ασφάλεια διασφαλίζεται πληρέστερα όταν σχεδιάζεται με **διεπιστημονική συνεργασία**.

7. Η ψηφιακή ασφάλεια πρέπει να αποβλέπει, πρωτίστως, στην **προστασία ευαίσθητων κοινωνικών ομάδων**.



References

1. Gritzalis D., Kandias M., Stavrou V., Mitrou L., "History of Information: The case of Privacy and Security in Social Media", in *Proc. of the History of Information Conference*, Law Library Publications, 2014.
2. Kandias M., Galbogini K., Mitrou L., Gritzalis D., "Insiders trapped in the mirror reveal themselves in social media", in *Proc. of the 7th International Conference on Network and System Security*, pp. 220-235, Springer, 2013.
3. Kandias M., Mitrou L., Stavrou V., Gritzalis D., "Which side are you on? A new Panopticon vs. privacy", in *Proc. of the 10th International Conference on Security and Cryptography*, pp. 98-110, ScitecPress, 2013.
4. Kandias M., Stavrou V., Bozovic N., Mitrou L., Gritzalis D., "Can we trust this user? Predicting insider's attitude via YouTube usage profiling", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, pp. 347-354, IEEE Press, 2013.
5. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Conference on Critical Infrastructure Security*, pp. 93-103, Springer, 2011.
6. Mylonas A., Tsoumas B., Dritsas S., Gritzalis D., "A secure smartphone applications roll-out scheme", in *Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business*, pp. 49-61, Springer, 2011.
7. Mylonas A., Kastania A., Gritzalis D., "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers & Security*, Vol. 34, pp. 47-66, Elsevier, 2013.
8. Mylonas A., Meletiadiis V., Mitrou L., Gritzalis D., "Smartphone sensor data as digital evidence", *Computers & Security* (Special Issue: Cybercrime in the Digital Economy), Vol. 38, pp. 51-75, October 2013.
9. Theoharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in *Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability*, pp. 171-178, Springer, 2012.
10. Mylonas A., Gritzalis D., Tsoumas B., Apostolopoulos T., "A qualitative metrics vector for the awareness of smartphone security users", in *Proc. of the 10th International Conference on Trust, Privacy & Security in Digital Business*, pp. 173-184, Springer, 2013.
11. Soupionis Y., Dritsas S., Gritzalis D., "An adaptive policy-based approach to SPIT management", in *Proc. of the 13th European Symposium on Research in Computer Security*, pp. 446-460, Springer, 2008.
12. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in *Proc. of the 8th International Conference on Availability, Reliability and Security*, pp. 248-254, IEEE Press, 2013.