WORLD SUMMIT ON THE INFORMATION SOCIETY

Πρόσβαση και ασφάλεια για όλους, χρησιμοποιώντας

Τα θέματα υποδομών Τεχνολογιών Πληροφορικής και Επικοινωνιών, αλλά και το ζήτημα της ασφάλειας στη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) ήταν μερικά από τα βασικά ζητήματα που συζητήθηκαν στο πλαίσιο της Παγκόσμιας Συνόδου Κορυφής για την Κοινωνία της Πληροφορίας (World Summit on Information Society - WSIS) που διοργανώθηκε στη Γενεύη από τις 14 έως τις 25 Μαΐου. Περίπου 80 εκπρόσωποι Κυβερνήσεων, διεθνών οργανισμών, ο ιδιωτικός τομέας και η κοινωνία των πολιτών ήταν παρόντες στη συνεδρίαση, η οποία μεταδόθηκε επίσης από το διαδίκτυο, για να επιτρέψει ευρύτερη συμμετοχή.

Υποδομές Τεχνολογιών Πληροφορικής και Επικοινωνιών

Κατά τη διάρκεια των συζητήσεων, οι συμμετέχοντες δήλωσαν ότι είναι πρωταρχικό να υπάρχουν αξιόπιστες πηγές ηλεκτρικής ενέργειας προκειμένου να ενδυναμώσουν τις Τεχνολογίες Πληροφορικής και Επικοινωνιών. Η χρηματοδότηση είναι κρίσιμο ζήτημα για τα προγράμματα στις αναπτυσσόμενες χώρες και προτάθηκαν μελέτες για να συγκριθούν οι επιπτώσεις των ιδιωτικών επενδύσεων έναντι των δημόσιων. Η συνεδρίαση αναγνώρισε την προσφορά της ITU για την εναρμόνιση των πολιτικών και των νόμων και τονίστηκε ότι οι κυβερνήσεις πρέπει να υιοθετήσουν ρυθμίσεις που επιτρέπουν σε ιδιώτες επενδυτές να ανταγωνιστούν μέσα σε μια ελεύθερη αγορά.

Οι συμμετέχοντες υπογράμμισαν ότι η οικοδόμηση υποδομών ΤΠΕ πρέπει να είναι συντονισμένες, έτσι ώστε να αποφευχθούν οι επικαλυπτόμενες ενέργειες και τα περιττά προγράμματα. Τα ασύρματα δίκτυα θα μπορούσαν να αποτελέσουν την απάντηση στις αγροτικές περιοχές και οι τοπικές κοινωνίες θα πρέπει να ενισχυθούν προκειμένου να υλοποιήσουν σχέδια για αύξηση της πρόσβασης και μείωση του κόστους ευρυζωνικών υπηρεσιών. Είναι σημαντικό να δημιουργηθεί μια υποδομή, ανοικτή σε όλους, η οποία θα προάγει την οικονομική ανάπτυξη.

Ζητήθηκαν σχόλια για το προτεινόμενο Σχέδιο Δράσης σε έξι τομείς: προώθηση εθνικών στρατηγικών ΤΠΕ, εναρμόνιση των περιφερειακών πολιτικών ΤΠΕ, ανάπτυξη περιφερειακών και μεγάλης κλίμακας εθνικών πρωτοβουλιών, ανά-

Δράσεις, World Summit on the Information Society

- **C1.** Ο ρόλος της πολιτείας και των κοινωνικών εταίρων για την προώθηση των Τεχνολογιών Πληροφορικής και Επικοινωνιών με στόχο την ανάπτυξη
- **C2.** Υποδομές Τεχνολογιών Πληροφορικής και Επικοινωνιών
- **C3.** Πρόσβαση στις πληροφορίες και στη γνώση
- **C4.** Δημιουργία υποδομών και δικτύων
- **C5.** Οικοδομώντας Εμπιστοσύνη και Ασφάλεια στη χρήση των ΤΠΕ
- **C6.** Ευνοϊκό ρυθμιστικό περιβάλλον
- **C7.** Εφαρμογές ΤΠΕ (Ηλεκτρονική Διακυβέρνηση, Ηλεκτρονική Μάθηση και Ηλεκτρονική Υγεία)
- **C8.** Πολιτιστική ποικιλομορφία και ταυτότητα, γλωσσική ποικιλομορφία και περιεχόμενο
- **C9.** Μέσα Ενημέρωσης
- **C10.** Κοινωνία της Πληροφορίας -Ηθικές διαστάσεις
- **C11.** Διεθνής και Τοπική Συνεργασία

Τα ασύρματα δίκτυα θα μπορούσαν να αποτελέσουν την απάντηση στις αγροτικές περιοχές και οι τοπικές κοινωνίες θα πρέπει να ενισχυθούν προκειμένου να υλοποιήσουν σχέδια για αύξηση της πρόσβασης και μείωση του κόστους ευρυζωνικών υπηρεσιών

πτυξη πλατφόρμας χρηματοδότησης, δημιουργία on - line εργαλείου για την αποτίμηση της ανάπτυξης των ΤΠΕ και την έναρξη των παγκοσμίων θεματικών πρωτοβουλιών για τις ΤΠΕ. Αυτές οι πρωτοβουλίες θα καλύψουν: i. τη δημόσια πρόσβαση, ii. εφαρμογές ΤΠΕ για την ανάπτυξη, iii. την ευρυζωνική σύνδεση μέσω καλωδιακών και ασύρματων τεχνολογιών, και iv. τις υποδομές ΤΠΕ μεγάλης κλίμακας.

Οικοδομώντας Εμπιστοσύνη και Ασφάλεια στη χρήση των ΤΠΕ

Ξεχωριστή θέση στο WSIS, είχε το θέμα της ασφάλειας. Στην πρώτη συνεδρίαση της Δράσης για την εμπιστοσύνη και την ασφάλεια στη χρήση των ΤΠΕ, οι εργασίες εστιάστηκαν σε τέσσερις "περιοχές" της κυβερνο-ασφάλειας: εθνικές στρατηγικές, νομικό πλαίσιο, παρακολούθηση - προειδοποίηση και ανταπόκριση, spam και σχετικές απειλές. Περίπου 120 άτομα συμμετείχαν στη συνεδρίαση, την οποία άνοιξε ο Γενικός Γραμματέας της ITU, Hamadoun I. Touré. Ο ίδιος τόνισε ότι: "ενώ σημαντική πρόοδος έχει σημειωθεί στη χρήση των ΤΠΕ ως όχημα για την κοινωνική και οικονομική ανάπτυξη, προκειμένου να επιτευχθούν οι στόχοι μας και να συγκεντρωθούν όλα τα οφέλη της Κοινωνίας της Πληροφορίας, πρέπει να εξετάσουμε τις τρέχουσες και αναδυόμενες απειλές".

Ο καθηγητής Seymour Goodman του Georgia Institute of Technology - ΗΠΑ, σημείωσε ότι η εξουσιοδότηση που δόθηκε κατά τη διάρκεια του WSIS στην ITU για την κυβερνοασφάλεια, είναι ένα μοναδικό εργαλείο για εστίαση στις λύσεις και για πρακτικά παραδείγματα, προκειμένου να καταστήσει τον κυβερνοχώρο ασφαλέστερο.

Εθνικές στρατηγικές

Οι χώρες που αναπτύσσουν προγράμματα προστασίας (Critical Information Infrastructure Protection - CIIP), είναι δύσκολο να προσδιορίσουν βέλτιστες πρακτικές και παραδείγματα. Αυτό συμβαίνει επειδή τα πρότυπα CIIP είναι συχνά σύνθετα, δαπανηρά και διαμορφωμένα στις συνθήκες συγκεκριμένων χωρών. Ένα CIIP πρόγραμμα προστασίας, πρέπει να βασίζεται στην πρόληψη και στην έγκαιρη προειδοποίηση, στην ανίχνευση, αντίδραση, διαχείριση της κρίσης και στη συνεργασία με όλους τους ενδιαφερόμενους, σε εθνικό και διεθνές επίπεδο, ώστε να είναι επιτυχές. Μελέτες του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) για την Ασφάλεια και την Ιδιωτικότητα των δεδομένων, είχαν δείξει ότι "η κυβερνητική πολιτική, οι οργανώσεις και τα πρότυπα διαδραματίζουν βασικό ρόλο στη διαχείριση ασφάλειας κυβερνητικών συστημάτων, πληροφοριών και δικτύων".

Στη Λιθουανία, έρευνα για την κυβερνοασφάλεια που πραγματοποιήθηκε το 2004, διαπίστωσε ότι περίπου 52% των επιχειρήσεων είχαν υποστεί βλάβη από ιούς και spams. Μεταξύ των θεμάτων που συζητήθηκαν ήταν και το επίπεδο ανεξαρτησίας που πρέπει να δοθεί στις Ομάδες Ανταπόκρισης Εκτάκτων Αναγκών σε Υπολογιστές (Computer Emergency Response Teams, CERT), πώς να εμπλακεί ο ιδιωτικός τομέας στην αστυνόμευση του επιβλαβούς περιεχομένου και τα στοιχεία του παθητικού των χειριστών για τη διαβίβαση των ιών ή των spam.
Έκθεση ομάδας εμπειρογνωμόνων του Συμβουλίου της Ευρώπης (Council of Europe - CoE), τον Απρίλιο του 2007, κατέληξε σε νομοθετικά μέτρα για τη διεθνή συνεργασία, ενθαρρύνοντας τις χώρες να υπογράψουν τη Συνθήκη CoE για το Κυβερνοέγκλημα.

Spam και άλλες απειλές

Ο Mark Sunner, MessageLabs - Ηνωμένο Βασίλειο, τόνισε ότι κατά προσέγγιση τρία σε κάθε τέσσερα e-mail είναι spam, ενώ 1 σε κάθε 145 περιέχει ιό, και 1 σε κάθε 416 αποτελεί επίθεση phishing,

WORLD SUMMIT ON THE INFORMATION SOCIETY

Πρόσβαση και ασφάλεια για όλους, χρησιμοποιώντας Τεχνολογίες Πληροφορικής και Επικοινωνιών

ενώ οι προβλέψεις δείχνουν συνεχιζόμενη άνοδο στον όγκο των spam. Ο Gregoire Ribordy, ID Quantique - Ελβετία, σημείωσε ότι το παραδοσιακό σύστημα κρυπτογραφίας είναι βασισμένο σε κλειδιά που πρέπει να έχουν τη δυνατότητα επέκτασης. Ένα σύστημα κβαντικής κρυπτογράφησης θα μπορούσε να είναι κατάλληλο για κρίσιμες εφαρμογές μεγάλης αξίας. Σε αυτό τον τομέα εφαρμόζεται ένα πιλοτικό πρόγραμμα χρηματοδοτημένο από την Ε.Ε.

Η κυβερνητική πολιτική, οι οργανώσεις και τα πρότυπα διαδραματίζουν βασικό ρόλο στη διαχείριση ασφάλειας κυβερνητικών συστημάτων, πληροφοριών και δικτύων

Τα φίλτρα spam βελτιώνονται, αλλά λύνουν μόνο το πρόβλημα για τελικούς χρήστες, όχι για τους παρόχους υπηρεσιών και δικτύων. Τα φίλτρα είναι δαπανηρά και χρειάζονται συντήρηση. Το πρόβλημα είναι όλο και πιο σοβαρό. Υπάρχουν περιπτώσεις, που το μέσο μήνυμα spam περιλαμβάνει εγκληματικές δραστηριότητες σε τουλάχιστον τρεις χώρες και αρκούν μόνο 30 δευτερόλεπτα πριν σταλεί το spam από τη στιγμή που έχει μετατραπεί ένας υπολογιστής σε μέλος zombie ενός botnet. (Ένας υπολογιστής μπορεί να μολυνθεί από ιό που τον κάνει να παράγει spam e-mails ως τμήμα ενός δικτύου τέτοιων "zombies" ή υπολογιστών ρομπότ, που λέγονται "botnet").

Πριν από δέκα χρόνια, οι όγκοι spam ήταν συγκριτικά χαμηλοί, αλλά από το 2003, το πρόβλημα έχει γίνει πολύ χειρότερο. Εντούτοις, η επιβολή του νόμου ενάντια στο κυβερνοέγκλημα παγκόσμια είναι αργή. Σε διάστημα μερικών μηνών το πλήθος των νέων zombie botnets αυξήθηκε από 700.000 σε πάνω από ένα εκατομμύριο. Το πρόβλημα πρέπει να αντιμετωπιστεί στην πηγή του και τόσο η βιομηχανία ΤΠΕ, όσο και οι κυβερνήσεις πρέπει να εργαστούν από κοινού, ώστε να καταπολεμήσουν τις απειλές κατά της κυβερνοασφάλειας.

Σύμφωνα με στατιστικά στοιχεία, 15.000 περίπου νέα αντικείμενα "malware" έχουν ανιχνευτεί κατά τη χρονική περίοδο του Μαρτίου 2006, ενώ την αντίστοιχη περίοδο του Μαρτίου 2007 ανιχνεύθηκαν περίπου 90.000 νέα αντικείμενα. Για να μπορέσει το ευρύ κοινό, να αντιμετωπίσει τέτοιου είδους επιθέσεις, πρέπει να εκπαιδευθεί σε θέματα αντιμετώπισης απειλών.

Το πρόβλημα πρέπει να αντιμετωπιστεί στην πηγή του και τόσο η βιομηχανία ΤΠΕ, όσο και οι κυβερνήσεις πρέπει να εργαστούν από κοινού, ώστε να καταπολεμήσουν τις απειλές κατά της κυβερνοασφάλειας

Επόμενα βήματα

Η ITU έχει να διαδραματίσει σημαντικό ρόλο στο συντονισμό και στη διάδοση δράσεων για την κυβερνοασφάλεια. Η ITU προετοιμάζει ένα πλαίσιο για να βοηθήσει τις χώρες - μέλη της να αξιολογήσουν το επίπεδο κυβερνοασφάλειάς τους και να το προστατεύσουν. Στο πλαίσιο αυτό έχουν γίνει προτάσεις, ώστε όλοι οι εμπλεκόμενοι (πολίτες, βιομηχανία ΤΠΕ, πολιτεία) να συντονιστούν για να προσδιορίσουν τις βέλτιστες λύσεις για τις αναπτυσσόμενες χώρες.

Η τεχνολογία είναι ένα ισχυρό όπλο ενάντια στο spam και σε άλλες επιθέσεις. Η εγκληματικότητα στον κυβερνοχώρο ποτέ δεν θα μπορούσε να εκλείψει εντελώς, ακριβώς όπως δεν θα μπορούσε ποτέ να βρίσκεται στην αληθινή ζωή, ωστόσο, θα μπορούσε να φτάσει σε ανεκτό επίπεδο, έτσι ώστε η κοινωνία να μπορεί να συνεχίσει να λειτουργεί. Σ

Το παραπάνω άρθρο είναι αναδημοσίευση από το περιοδικό ITUnews, τεύχος 6/ 2007.