# DTS NETWORK COMPROMISE ASSESSMENT

*Το Network Compromise Assessment είναι μια ιδιαίτερη προσφορά, αποκλειστικά για νέους πελάτες της DTS. Βάσει του μοντέλου αξιολόγησης Assume Breach, στοχεύουμε στην ανάδειξη κενών ασφαλείας του εσωτερικού δικτύου μιας επιχείρησης, που είναι ικανά να θέσουν σε κίνδυνο τις υποδομές της. Διερευνούμε με ποιον τρόπο θα μπορούσε ένας εισβολέας να αποκτήσει πρόσβαση στους πόρους μιας επιχείρησης παραβιάζοντας το δικτυακό της εξοπλισμό. Τελικός μας στόχος είναι η αξιολόγηση της ανθεκτικότητας του δικτύου απέναντι σε σύγχρονες μεθόδους επίθεσης και ο εντοπισμός πιθανών ευάλωτων σημείων.*

## ΤΙ ΕΞΕΤΑΖΟΥΜΕ

- Πόσο εύκολα μπορεί ένας εισβολέας να αποκτήσει πρόσβαση στο εσωτερικό δίκτυο της επιχείρησης;
- Ποια κενά ασφαλείας θα μπορούσαν να οδηγήσουν σε παραβίαση του δικτυακού εξοπλισμού;
- Σε ποιο βαθμό μπορεί ένας εισβολέας να κινηθεί στο εσωτερικό δίκτυο μιας επιχείρησης μετά την απόκτηση πρόσβασης σε αυτό;

## ΤΙ ΠΕΡΙΛΑΜΒΑΝΕΙ (ΜΕΘΟΔΟΛΟΓΙΑ)

1. Ανάλυση Ευπαθειών: Αρχικά, οι ειδικοί κυβερνοασφαλείας της DTS συλλέγουν και αναλύουν πληροφορίες σχετικά με τη δικτυακή υποδομή και τις παρεχόμενες υπηρεσίες της επιχείρησης. Με την ανάλυση αυτή αποκτούμε μια λεπτομερή εικόνα του δικτύου και μπορούμε να εντοπίσουμε πιθανά ευαίσθητα σημεία που μπορούν να δεχθούν επίθεση.
2. Προσομοίωση Ρεαλιστικών Επιθέσεων: Πραγματοποιούνται εικονικές επιθέσεις, ακολουθώντας μεθοδολογίες και τεχνικές που συνήθως χρησιμοποιούν οι εισβολείς, και μπορεί να είναι βάσει:
   - Πρωτοκόλλου (π.χ. SMB, RDP, DNS)
   - Εσφαλμένων ρυθμίσεων στα firewalls και στην τμηματοποίηση του δικτύου (network segmentation)
   - Γνωστών ευπαθειών σε δικτυακές συσκευές.
3. Αποτίμηση: Εξετάζουμε και αξιολογούμε τη δυνατότητα του εισβολέα να εισχωρήσει περαιτέρω στο εσωτερικό δίκτυο της επιχείρησης, έχοντας αρχικά παραβιάσει μια δικτυακή συσκευή και μέσω αυτής να αποκτήσει πρόσβαση και στο υπόλοιπο δίκτυο. Ακολουθούμε τεχνικές όπως:
   - Lateral Movement: Απόπειρα διείσδυσης σε όλο το υπόλοιπο του δικτύου μεταπηδώντας σε άλλες δικτυακές συσκευές
   - Privilege Escalation: Απόπειρα διείσδυσης και απόκτησης δικαιωμάτων διαχειριστή (admin rights)
   - Persistence: Απόπειρα απόκτησης μόνιμου ελέγχου του εσωτερικού δικτύου

## ΑΝΑΛΥΤΙΚΑ Η ΔΙΑΔΙΚΑΣΙΑ

- Προετοιμασία: Παροχή των απαραίτητων συσκευών & διαπιστευτηρίων και εγγραφή στη σχετική πλατφόρμα της DTS
- Εναρκτήρια Συνάντηση: Καθορισμός στόχων & τεχνικών λεπτομερειών
- Εκτέλεση: Διεξαγωγή της άσκησης με έμφαση σε επιθέσεις κατά εταιρικών δικτυακών συσκευών & τεκμηρίωση των αποτελεσμάτων
- Τελική Παρουσίαση: Παρουσίαση των ευρημάτων & προτάσεις για την ενίσχυση της ασφάλειας του δικτύου
- Προαιρετικά: Ανάλυση των αποτελεσμάτων μέσω της πλατφόρμας της DTS και δυνατότητα επαναξιολόγησης

## ΤΑ ΟΦΕΛΗ ΣΑΣ

- Ανίχνευση ευπαθειών και ευάλωτων σημείων σε επίπεδο εσωτερικού δικτύου:
  - Εντοπισμός κενών ασφαλείας που θα μπορούσαν να οδηγήσουν σε παραβίαση πόρων
  - Προτάσεις για την ενίσχυση της ασφάλειας του δικτύου (απαραίτητες άμεσες ενέργειες, αλλά και μακροπρόθεσμες βελτιώσεις)
  - Προσομοίωση σεναρίων επίθεσης, για την αξιολόγηση της ανθεκτικότητας του δικτύου έναντι σύγχρονων απειλών
- Δυνατότητα προσαρμογής στις επιχειρησιακές απαιτήσεις & το δίκτυο της εταιρείας
- Άμεσα εφαρμόσιμες πρακτικές για ένα ασφαλέστερο δίκτυο

**DTS Cloud Security MonEPE - Athens**
+30 211 1040-710

**dts.de/el**
info@dts-cloudsecurity.gr