

2014/01/21

EPR0TBC/2014
www.enisa.europa.eu

Ο Ευρωπαϊκός οργανισμός για την ασφάλεια του κυβερνοχώρου ENISA, ζητάει ασφαλέστερη ηλεκτρονική τραπεζική και ηλεκτρονικές πληρωμές: τα διαπιστευτήρια μιας χρήσης που δεν αναπαράγονται είναι απαραίτητα για τις ηλεκτρονικές ταυτότητες στο χρηματοπιστωτικό τομέα

Διαφορετικά διακριτικά, συσκευές, κινητά τηλέφωνα, ηλεκτρονικές υπογραφές κλπ χρησιμοποιούνται για τον έλεγχο των ηλεκτρονικών μας ταυτοτήτων. Ωστόσο, ορισμένα χρηματοπιστωτικά ιδρύματα εξακολουθούν να μην λαμβάνουν υπόψη τον κίνδυνο που ενέχουν οι ανεπαρκείς μηχανισμοί ελέγχου ταυτότητας, σύμφωνα με μια νέα μελέτη του Οργανισμού ENISA της ΕΕ. Η έκθεση αναλύει τις τρέχουσες απάτες στην ηλεκτρονική τραπεζική και τις συσχετίζει με τους μηχανισμούς ελέγχου ταυτότητας των πελατών των χρηματοπιστωτικών ιδρυμάτων. Υπογραμμίζει επίσης την ανάγκη για ενημερωμένους μηχανισμούς ασφαλείας και παρέχει 10 προτεινόμενες προσεγγίσεις για περισσότερη ασφάλεια.

Ο Οργανισμός ανέλυσε περισσότερες από 100 απαντήσεις σε μια έρευνα που πραγματοποιήθηκε με την συμμετοχή εμπόρων και ειδικών ασφαλείας στην ηλεκτρονική τραπεζική σε σχέση με την μέθοδο ελέγχου της ηλεκτρονικής ταυτότητας (eIDA). Η μέθοδος αυτή χρησιμοποιείται καθημερινά από πολίτες, πελάτες και επιχειρήσεις σε συστήματα ηλεκτρονικής τραπεζικής και ηλεκτρονικών πληρωμών. Επιπρόσθετα, ο Οργανισμός εντόπισε τους κινδύνους και τους τρόπους επίθεσης σε σχέση με κάθε μέθοδο ελέγχου, συμπεριλαμβανομένων των επιθέσεων phishing (στοχευμένες επιθέσεις), την κλοπή της ταυτότητας, τον έλεγχο της συνόδου και της ταυτότητας, κλπ. των χρηματοπιστωτικών ιδρυμάτων, των εμπόρων και των παρόχων υπηρεσιών πληρωμών.

Σαν αποτέλεσμα, ο Οργανισμός δημοσίευσε οδηγίες, καλές πρακτικές και προτάσεις για την ηλεκτρονική τραπεζική και τις πληρωμές μέσω διαδικτύου. Στις κύριες προτάσεις περιλαμβάνονται:

- Βελτίωση της ασφάλειας του περιβάλλοντος της ηλεκτρονικής τραπεζικής**, που σημαίνει πως οι οικονομικοί παράγοντες θα πρέπει:
 - Να πραγματοποιούν μια ανάλυση κινδύνων με βάση το προφίλ των πελατών και το μέγεθος του ιδρύματος,
 - Να βελτιώσουν την ενημέρωση και τις ικανότητες των πελατών,
 - Να προσαρμόσουν τους ελέγχους ταυτότητας στα προφίλ συμπεριφοράς των πελατών και στις παραμέτρους των συναλλαγών (πχ τη χώρα προορισμού, το ποσό)
 - Να ελαχιστοποιήσουν το χρόνο εντοπισμού των συσκευών των πελατών που είναι σε κίνδυνο, με την καταχώρηση των συσκευών και με τον έλεγχο και την αξιολόγηση της ασφάλειας τους («[Ας υποθέσουμε ότι όλες οι συσκευές έχουν μολυνθεί](#)»).
- Βελτίωση της ασφάλειας των εφαρμογών της ηλεκτρονικής τραπεζικής και των καναλιών διανομής τους στους καταναλωτές**: ενθαρρύνοντας την παραδοσιακή «ασφάλεια από τον σχεδιασμό». Η νέα οδηγία για την προστασία των προσωπικών δεδομένων θα πρέπει επίσης να

ENISA is a Centre of Expertise in Network and Information Security in Europe

Securing Europe's Information Society

The European Union Agency for Network and Information Security

2014/01/21

EPR0TBC/2014
www.enisa.europa.eu

λαμβάνεται υπόψη, ενώ θα πρέπει να χρησιμοποιούνται και αξιόπιστα κανάλια για την εγκατάσταση των εφαρμογών στη συσκευή του πελάτη.

3. **Προώθηση της αναλογικότητας μεταξύ της ευρωστίας των επιλεγμένων μεθόδων και των διαπιστωμένων κινδύνων**, με έμφαση στη χρήση των " ελέγχου ταυτότητας 2-παράγοντων") ακόμη και για δραστηριότητες χαμηλού κινδύνου (π.χ. τα ATM έχουν μια κάρτα και ένα κωδικό PIN).
4. **Βελτίωση της γνώσης και της συμπεριφοράς των πελατών αλλά και των επαγγελματιών.**

Για να συνοψίσουμε, οι τρέχουσες πρακτικές ελέγχου ταυτότητας (eIDA) στον χρηματοπιστωτικό τομέα δεν καλύπτουν πολλούς κινδύνους. Η ΕΚΤ και η Ευρωπαϊκή Επιτροπή αναπτύσσουν συστάσεις και κανονισμούς που ευθυγραμμίζονται με την έκθεση του ENISA ώστε να εντοπίσουν και να δημιουργήσουν εργαλεία για να μειώσουν τις οικονομικές απώλειες που οφείλονται σε απάτη.

Ο εκτελεστικός Διευθυντής του ENISA, καθηγητής Udo Helmbrecht σχολίασε: "Ο χρηματοπιστωτικός τομέας διαχειρίζεται ηλεκτρονικές συναλλαγές εκατοντάδων δισεκατομμυρίων ευρώ κάθε χρόνο. Για το λόγο αυτό οι ασφαλείς ηλεκτρονικές ταυτοτήτες και ο έλεγχος των ταυτοτήτων είναι απλά απαραίτητα για την οικονομία της Ευρώπης. Τα χρηματοπιστωτικά ιδρύματα θα πρέπει να χρησιμοποιούν την ασφάλεια σαν ένα ανταγωνιστικό εργαλείο προώθησης. Με αυτή την έκθεση, οι παράγοντες του χρηματοπιστωτικού τομέα μπορούν να πραγματοποιήσουν μια ανάλυση κόστους/οφέλους για επιπλέον μηχανισμούς ελέγχου ταυτότητας"

[Για την πλήρη έκθεση](#)

Γενικές πληροφορίες:

[Η προτεινόμενη οδηγία για την προστασία των δεδομένων στην Ευρώπη](#), and [Δεύτερη οδηγία για τις υπηρεσίες πληρωμών](#), [ΕΚΤ "Προτάσεις για την ασφάλεια των διαδικτυακών πληρωμών"](#)

Για συνεντεύξεις: Ulf Bergström, Εκπρόσωπος, ulf.bergstrom@enisa.europa.eu, κινητό: + 30 6948 460 143, Manel Medina, Εμπειρογνώμονας του ENISA, sta@enisa.europa.eu

Μετάφραση. Η μόνη επίσημη έκδοση είναι η αγγλική.