Intensificarea numarului și a metodelor de fraude cibernetice în perioade de incertitudine. Care sunt pașii de urmat în cazul în care ați fost victima noilor atacuri de tip smishing

Departamentul de White Collar Crime al casei de avocatura Mușat & Asociații, cu o vasta expertiza în domeniul cybersecurity, respectiv în oferirea de asistență și reprezentare juridica în cauze complexe privind fraudele cibernetice, informeaza clienții sai și publicul interesat despre o noua modalitate de smishing (phishing prin intermediul mesageriei telefoanelor mobile) aparuta recent în spațiul virtual, prin care faptuitorii vizeaza compromiterea unor conturi pe platforme de mesagerie și telefonie (de ex. Whatsapp) pentru a clona aceste conturi și a savârși prin intermediul lor diferite infracțiuni.

Prin urmare, aducem în atenția publicului anumite aspecte privind noile metode de atacuri cibernetice aparute recent.

În prezent, se deruleaza o noua campanie de smishing (o forma de phishing care utilizeaza drept platforma de atac telefoanele mobile), care presupune transmiterea catre utilizatori a unui mesaj pe Whatsapp prin care se solicita votarea unei anumite persoane în scopul de a câștiga un anumit premiu. Un exemplu de mesaj este: „Te rog sa o susţii pe Ana, verişoara mea, la concursul şcolii ei! Poate câştiga un an de şcolarizare gratuita, iar un vot din partea ta ar conta enorm. Mulţumesc mult! (link)”.

În realitate, ca urmare a accesarii link-ului respectiv și a finalizarii „votului”, utilizatorul ofera acces la contul sau de Whatsapp faptuitorilor, care îl folosesc ulterior pentru a compromite alte conturi sau pentru a solicita sume de bani.

Acesta este doar un exemplu recent al campaniilor de smishing folosite în practica, existând și alte metode care sunt în continuare actuale, precum metoda accidentului, frauda de tip 1800 și schema plata pentru click (sau plata pentru like-uri pe anumite platforme).

Aceste metode de frauda, indiferent de tipul lor, se intensifica, de regula, în perioade de incertitudine economica, politica și sociala, în prezent aceste atacuri fiind îndreptate atât împotriva marilor corporații, cât și împotriva persoanelor vulnerabile, respectiv persoane în vârsta, din medii defavorizate sau care nu dețin cunoștințe tehnice.

Casa de avocatura *Mușat & Asociații* are o vasta experiența în asistarea clienților, societați și persoane fizice în diverse tipuri de fraude, spre exemplu: (i) cea mai mare frauda de tip „CEO Fraud” din România; (ii) atacuri cibernetice privind perturbarea unor platforme online de streaming video; (iii) fraude împotriva persoanelor fizice prin furt de cryptomonede din portofelele electronice; (iv) compromiterea datelor conturilor și a cardurilor bancare; (v) plata unor taxe inexistente în vederea ridicarii unor premii substanțiale, precum și altele asemenea.

În cazul unor astfel de atacuri cibernetice, ar trebui urmați o serie de pași în vederea înlaturarii sau diminuarii efectelor negative generate de atacatori.

Daca fraudatorii reușesc sa intre în posesia datelor conturilor bancare sau a datelor de card, primul pas ar fi contactarea unității bancare pentru blocarea conturilor și a cardurilor compromise, precum și luarea tuturor masurilor de conservare a sumelor de bani aflate în conturi și anularea potențialelor tranzacții efectuate ca urmare a fraudei informatice.

În cazul fraudei de tip smishing menționate mai sus, daca utilizatorul mai are acces la contul de Whatsapp, recomandarea este sa acceseze secțiunea Settings (Setari/Configurari), sa selecteze 'Linked devices' (Dispozitive asociate) și sa elimine din lista dispozitivele necunoscute, apoi sa activeze autentificarea în doi pași (2FA), daca nu a facut-o deja.

În cazul în care utilizatorul nu mai are acces la cont, va fi necesara contactarea Centrului de Ajutor al Whatsapp pentru a parcurge pașii necesari recuperarii contului.

Imediat ce accesul la cont a fost recuperat/securizat, este recomandata trimiterea unui mesaj persoanelor care au primit mesaje nesolicitate din partea atacatorilor din contul utilizatorului, pentru a evita ca aceștia sa ajunga și ei victime ale respectivei fraude.

În cazul în care sunt înregistrate pagube financiare, este indicata raportarea cât mai rapida a incidentului atât catre organele de urmarire penala, respectiv parchet sau poliție, cât și catre DNSC (Directoratul Național de Securitate Cibernetica).

Totodata, consideram oportuna consultarea unor avocați specializați în acest domeniu pentru asistența și îndrumare în vederea înlaturarii sau diminuarii consecințelor atacurilor cibernetice descrise anterior.

Astfel, Casa de avocatura Mușat & Asociații, prin **Ștefan Diaconescu** – *Partner* și **Florian Negurici** – Associate, avocați din cadrul *Departamentului de White Collar-Crime*, specializați în domeniul infracțiunilor informatice, va sta la dispoziție pentru orice solicitare privind aceste tipuri de atacuri cibernetice.