Experţii CyBourn avertizeaza cu privire la ameninţarile de securitate cibernetica care pot afecta serviciile fintech

Pe masura ce soluţiile fintech devin din ce în ce mai integrate cu viaţa de zi cu zi, probleme şi incidentele de securitate cibernetica şi vulnerabilitaţi devin tot mai frecvente - de la furtul de date, pâna la furtul de bani şi atacuri de tip phishing mai complexe, care pot ajunge sa afecteze utilizatorul final, avertizeaza specialiştii în securitate cibernetica de la CyBourn.

Atracţia produselor fintech consta în faptul ca reprezinta o alternativa mai simpla şi mai rapida la serviciile financiare convenţionale, dar dezvoltarea foarte rapida a acestor aplicaţii de transfer de bani sau schimb valutar face ca aceasta industrie sa fie vulnerabila în mod special în faţa problemelor de securitate.

„Pe masura ce mai multe servicii financiare pot fi folosite online, sau direct de pe telefonul mobil, ubicuitatea datelor şi, în consecinţa, securitatea datelor, se dovedesc a fi o provocare majora pentru industrie. Gestionarea şi protejarea identitaţilor digitale ale persoanelor fizice şi ale întreprinderilor poate deveni o provocare majora pentru companiile fintech. Pe masura ce penetrarea serviciilor bancare online creşte, aceste companii sunt în masura sa adune cantitaţi imense de date despre clienţi, care sunt analizate în scopuri de marketing sau dezvoltare de afaceri. Aceste date pot fi foarte valoroase pentru hackeri ”, explica **Tiberiu Anghel**, *Director of Cybersecurity Operations în cadrul CyBourn*.

Pentru a asigura dezvoltarea unor astfel de platforme sigure, experţii în securitate cibernetica de la CyBourn recomanda revizuirea modelelor convenţionale de securitate, prin încorporarea securitaţii ca parte a fazelor iniţiale de dezvoltare a produselor.

Companiile fintech cresc în popularitate foarte rapid, ceea ce duce la o dezvoltare rapida a reţelelor lor IT. Totuşi, acest lucru face ca securitatea cibernetica sa fie una dintre sarcinile cu prioritate scazuta pentru fondatorii fintech, deoarece operaţiunile de dezvoltare ocupa cea mai mare parte a resurselor.

Astfel, doar 32% din companii au confirmat ca planuiesc sa achiziţioneze tehnologii de securitate cibernetica în 2018. Mai mult, dezvoltarea rapida a companiilor pune presiune asupra dezvoltatorilor de software şi solicita echipele, lasând produsele şi infrastructura vulnerabile chiar şi în faţa unor atacuri comune sau malware. Achiziţia rapida a unor volume mari de utilizatori face din companiile fintech ţinta perfecta pentru atacurile de phishing, care au potenţialul de a afecta dezvoltarea rapida şi credibilitatea companiilor, având impact financiar semnificativ.

Astfel, verificarile de securitate în mod regulat şi monitorizarea securitaţii infrastructurii devin diferenţiatori puternici. „Pe partea de monitorizare, verificarile de cod şi arhitectura IT, scanarile pentru identificarea vulnerabilitaţilor şi testele de penetrare ajuta la reducerea riscurilor. Pe plan operaţional, folosirea unui antivirus centralizat, soluţiile IDS / IPS şi SIEM ajuta la prevenirea şi detectarea malware şi a anomaliilor din sistem.”, recomanda Catalin Moisei, Chief Technology Officer în cadrul CyBourn. “Monitorizarea constanta şi alertele asigura detectarea rapida şi capacitatea de reacţie la incidente, atenuând efectul atacurilor cibernetice care ar putea perturba operaţiunile. Între timp, instruirea angajaţilor ramâne cel mai eficient mod de a atenua tentativele de phishing.”, explica Moisei.

CyBourn este o companie de securitate cibernetica românească, cu sediul central şi Centrul de Operaţiuni în Bucureşti, susţinuta de o echipa de cercetare în Napoli, Italia şi de o echipa de dezvoltare software la Washington D.C., SUA. CyBourn ofera o gama completa de servicii de securitate cibernetica pentru clienţi la nivel european, precum monitorizarea continua a infrastructurii IT, raspuns la incidente de securitate cibernetica, teste de

penetrare, cât și audit și consultanța privind sistemele de guvernanța a securitații informației.