Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

Escrocheria CEO sau Fraudarea email-ului de afaceri

Ce este escrocheria CEO sau fraudarea email-ului de afaceri?

Infractorii cibernetici continuă să-și rafineze atacurile mijlocite de email, cunoscute ca escrocheria CEO sau fraudarea email-ului de afaceri (Business Email Compromise, sau BEC). Acestea sunt atacuri bine orientate care păcălesc victimele determinându-le să facă lucruri pe care în mod normal n-ar trebuie să le facă. În majoritatea cazurilor acești răufăcători vor bani. Ce face acest tip de atacuri așa periculos este că atacatorii își analizează atent victimele înaintea lansării atacului. Este de asemenea foarte dificil pentru soluțiile tehnice de protecție să oprească aceste atacuri, pentru că nu sunt mesaje email cu conținut infectat sau adrese suspicioase care să fie detectate. Iată cum funcționează aceste atacuri.

Infractorii cibernetici folosesc Internet-ul pentru a-și studia victima vizată și oamenii cu care aceasta interacționează. De exemplu, dacă vă iau în vizor vor căuta să afle cine vă este șef la serviciu sau un agent imobiliar cu care colaborați. Infractorul va concepe apoi un email pretinzând că este una dintre aceste persoane, apoi vă trimite mesajul. Acesta are un ton de urgență, cerându-vă să faceți ceva neîntârziat, cum ar fi să plătiți o factură, schimbând destinatarul plății sau convingându-vă să răspundeți cu documente confidențiale. Email-ul funcționează forțându-vă să faceți ce-și doresc. Iată două exemple în care astfel de atacuri ar putea reuși.

Transferul bancar: Un infractor urmărește să obțină bani. El cercetează compania la care lucrați, identificând persoanele care lucrează în departamentul de plăți sau pe oricine e responsabil pentru transferurile de bani. Escrocii concep și trimit apoi un email către aceste persoane pretinzând că sunt șeful lor sau vreun director executiv. Mesajul spune că o urgență impune transferul imediat de bani într-un cont bancar nou. Mesajul pune presiune pe aceștia, făcându-i să greșească, în realitate ei trimițând bani infractorilor.

Frauda fiscală: Răufăcătorii caută informații personale pentru a le folosi la fraudarea taxelor. Una dintre cele mai rapide căi de a le obține este furtul informațiilor despre toți angajații unei companii. Infractorii caută și identifică persoanele din departamentul de resurse umane. Apoi trimit mesaje frauduloase către aceștia, pretinzând că sunt din conducerea companiei sau cineva din departamentul juridic. Mesajul are un caracter urgent, cum că taxele pentru toți angajații trebuie plătite imediat. Cei din departamentul de resurse umane cred, astfel, că trimit documente confidențiale către conducere, când de fapt ei le trimit infractorilor.

Protejați-vă

Așadar, ce puteți face ca să vă protejați? Simțul realității este cea mai bună defensivă. Iată cele mai frecvente indicii pe care să le căutați:

- **Mesajul este foarte scurt și are un ton imperativ (deseori numai câteva propoziții) iar semnătura indică trimiterea lui de pe un dispozitiv mobil.**
- **Există un pronunțat caracter de urgență, ce vă forțează să ignorați sau să ocoliți politicile angajatorului dumneavoastră. Întotdeauna urmați politicile și procedurile de lucru, chiar și dacă mesajul pare să vină de la șef sau de la directorul general al companiei.**
- **Email-ul ține de activitatea profesională dar este expediat de la o adresă personală, cum ar fi @gmail.com sau @hotmail.com.**
- **Mesajul pare să fie trimis de un superior ierarhic, coleg sau furnizor pe care-l cunoașteți, sau cu care lucrați, dar stilul mesajului nu se potrivește cu aceștia.**
- **Instrucțiunile de plată primite sunt diferite de cele cunoscute, cum ar fi solicitarea unui transfer imediat către un cont bancar diferit.**

Dacă suspectați că sunteți ținta unui astfel de atac la serviciu, opriți orice interacțiune cu atacatorul și anunțați-vă superiorul ierarhic. Dacă ați fost victima unui astfel de atac acasă și ați făcut deja un transfer bancar, anunțați-vă imediat banca, apoi autoritățile.

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Editor invitat

Don Cavender *este un fost agent special FBI, cu o experiență de peste 22 de ani în analiza criminalistică digitală și criminalitatea informatică. Recent s-a concentrat pe grupurile de crimă organizată, din postura de coordonator BEC la Washington DC. Oferă training și desfășoară activități de cercetare în analiza criminalistică digitală și investigații cibernetice. Poate fi urmărit pe Twitter la* @don_cavender *și pe LinkedIn:* https://www.linkedin.com/in/donald-cavender

Resurse online

Ingineria socială:	https://www.sans.org/u/HE3
Opriți atacurile de phishing:	https://www.sans.org/u/HE8
Opriți programele malware:	https://www.sans.org/u/HEd
Securizați-vă conturile de acces:	https://www.sans.org/u/HEi