OUCH!
SANS SECURITY AWARENESS
Det månedlige nyhedsbrev om IT-sikkerhed

CEO svindel / BEC

Hvad er CEO svindel / BEC?

IT-angriberne har udviklet et e-mailangreb kaldet CEO svindel eller "Business Email Compromise" (BEC). Disse er målrettede e-mailangreb, der snyder deres offer til at udføre en handling, de ikke bør udføre. I de fleste tilfælde er de kriminelle ude efter penge. Det, der gør disse angreb så farlige, er at de IT-kriminelle undersøger deres ofre, inden de starter deres angreb. Det er også meget svært for sikkerhedsteknologier at stoppe disse angreb, fordi der ikke er inficerede e-mail, vedhæftede filer eller ondsindede links som teknologierne kan registrere. Sådan fungerer angrebet.

En IT-kriminel bruger internettet til at undersøge deres påtænkte offer og personer, som deres offer interagerer med. Hvis de f.eks. retter deres angreb mod dig, vil de undersøge, hvem din chef er eller måske din ejendomsmægler. Den IT-kriminelle sender derefter en e-mail, hvor han foregiver at være en af disse personer, til dig. E-mailen er presserende, og kræver, at du straks handler, f.eks. straks betaler en faktura, ændrer hvem du betaler til eller overbeviser dig om at sende følsomme dokumenter. E-mailen fungerer ved at presse dig til at gøre, hvad de vil have. Her er to eksempler på, hvordan bare et sådant angreb kunne fungere. "

Bankoverførsel: En gruppe IT-kriminelle er efter penge. De undersøger det firma, du arbejder for, f.eks. identificere, hvem der arbejder med udbetalinger eller hvem der er ansvarlig for overførsel af midler. De kriminelle sender en e-mail til disse personer og foregiver at være deres chef eller en højtstående leder. E-mailen fortæller dem, at der er en nødsituation, og penge straks skal overføres til en ny bankkonto. E-mailen presser dem til at begå en fejl, og i virkeligheden sender de penge til de kriminelle.

Skattesvindel: IT-kriminelle er efter folks personlige oplysninger til brug for skattesvig. En af de hurtigste måder at få dette på er at stjæle informationen for alle medarbejderne hos en virksomhed. De IT-kriminelle forsker og identificerer, hvem der arbejder i HR. De sender så falske e-mails til disse personer, udgiver sig for at være en højtstående leder eller måske nogen fra myndighederne. E-mailsene fortæller en presserende historie, om at skatteoplysningerne på alle medarbejdere skal indsendes med det samme. Folk i HR tror, at de sender de følsomme dokumenter til den øverste leder, men i virkeligheden sender de dem til en IT-kriminel.

Beskyt dig selv

Så hvad kan du gøre for at beskytte dig selv? Sund fornuft er dit bedste forsvar. Her er de mest almindelige spor du kan lede efter.

E-mailen er meget kort og presserende (ofte kun et par sætninger) og signaturen siger, at e-mailen blev sendt fra en mobilenhed.

E-mailen giver udtryk for at det haster, og presser dig til at ignorere eller omgå din arbejdsgivers politikker eller arbejdsgange. Følg altid arbejdsrelaterede politikker og procedurer, selvom e-mailen synes at komme fra din chef eller endda administrerende direktør.

E-mailen er arbejdsrelateret, men der brugers en personlig e-mailadresse, f.eks. @gmail.com eller @hotmail.com.

E-mailen ser ud til at komme fra en leder, kollega eller sælger, du kender eller arbejder med, men tonen i meddelelsen lyder ikke som dem.

Betalingsinstruktioner er angivet, og disse instruktioner adskiller sig fra dem, du allerede har modtaget, som f.eks. anmodning om øjeblikkelig betaling til en anden bankkonto.

Hvis du har mistanke om, at du har været udsat for et målrettet angreb på arbejde, skal du stoppe al interaktion med afsenderen og rapportere det til din leder. Hvis du har været udsat for det hjemme eller hvis du er blevet offer og har foretaget en overførsel, skal du straks rapportere det til din bank og derefter til politiet.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

Don Cavender *er tidligere FBI "Special Agent", med over 22 år erfaring i "digital forensics" og IT-kriminalitet. Hans seneste indsats mod IT-kriminalitet er som Washington DC BEC-koordinator. Han giver træning og gennemfører forskning inden for "digital forensics" og IT-efterforskning.*

@don_cavender https://www.linkedin.com/in/donald-cavender

Hvis du vil vide mere

Social Engineering:	https://www.sans.org/u/HE3
Stop That Phish:	https://www.sans.org/u/HE8
Stop That Malware:	https://www.sans.org/u/HEd
Lock Down Your Login:	https://www.sans.org/u/HEi