OUCH!

SANS SECURITY AWARENESS

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

Direktørsvindel

Hva er direktørsvindel?

Cyberkriminelle bruker en form for e-postangrep kalt direktørsvindel (CEO fraud eller business email compromise/BEC på engelsk), som de stadig videreutvikler. Dette er målrettede e-postangrep som lurer offeret til å gjøre en bestemt handling som de ikke burde gjøre. I de fleste tilfeller er skurkene ute etter penger. Det som gjør disse angrepene så farlige, er det at de kriminelle gjør grundige undersøkelser av ofrene sine før de angriper. Det er også veldig vanskelig for sikkerhetsteknologier å stoppe slike angrep, da det ikke er noen infiserte vedlegg eller skadelige lenker som kan oppdages. Slik virker angrepet:

Angriperen bruker nettet for å undersøke det tiltenkte offeret, samt folk som offeret omgås. For eksempel, dersom de velger seg ut deg som offer vil de forsøke å finne ut hvem som er sjefen din på jobben, eventuelt også andre medarbeidere. Angriperen utformer så en e-post hvor de utgir seg for å være en av disse, f.eks. sjefen din, og sender så e-posten til deg. E-posten fremstår som en hastesak og krever at du gjør noe umiddelbart, som å betale en faktura, endre en betalingsmottaker, eller svare med et sensitivt dokument vedlagt. E-posten fungerer slik at den legger press på deg for å få deg til å gjøre som angriperen vil. Her er to eksempler på hvordan slike angrep kan bli gjennomført:

Utbetaling: Cyberkriminelle er ute etter penger. De undersøker bedriften du jobber i, og finner ut hvem som jobber med regnskap og kontoer, og hvem som er ansvarlig for å utføre betalinger og pengeoverføringer. De kriminelle utformer så en e-post som de sender til disse ansatte, hvor de utgir seg for å være sjefen deres eller en annen med en prominent lederstilling. I e-posten står det at det er en nødsituasjon og at penger må flyttes til en ny bankkonto. E-posten legger press på dem til å forhaste seg å gjøre en feil, i realiteten sendes pengene til de kriminelle.

ID-tyveri: Cyberkriminelle er ute etter folks personlige detaljer for å bruke til ID-tyveri og ID-misbruk. En av de raskeste metodene for å få tak i dette er ved å stjele informasjonen om alle ansatte i en bedrift på en gang. De kriminelle undersøker og finner ut hvem som jobber i HR. De sender så en e-post til disse hvor de utgir seg for å være en leder i bedriften, eller kanskje noen fra en juridisk avdeling. E-posten skaper en følelse av hastverk, og ber om at personopplysninger for alle ansatte, inkludert personnummer, må sendes over med en gang. Medarbeiderne i HR tror de sender informasjonen til sjefen, når de egentlig sender det til de kriminelle.

Slik sikrer du deg selv

Så hva kan du gjøre for å sikre deg selv? Sunn fornuft er ditt beste forsvar. Her er de vanligste tegnene du kan se etter:

- **E-posten er kort og presentert som en hastesak. Ofte er den kun på noen få setninger, og i signaturen står det gjerne at den ble sent fra en mobiltelefon.**
- **Det skapes en sterk følelse av hastverk, hvor man blir forsøkt presset til å omgå sikkerhetsrutiner. Følg alltid arbeidsplassens rutiner og policy, selv om e-posten ser ut til å være fra sjefen eller til og med den øverste lederen.**
- **E-posten er jobbrelatert, men benytter en personlig e-postadresse, som @gmail.com eller @hotmail.com.**
- **E-posten ser ut til å komme fra en leder, kollega eller tjenesteyter du kjenner og jobber med, men er ikke skrevet slik de vanligvis skriver.**
- **Du blir gitt betalingsinformasjon som ikke samsvarer med det du er kjent med fra før av, som at penger skal utbetales til en annen konto enn vanlig.**

Dersom du mistenker at du har blitt forsøkt utsatt for direktørsvindel, stopp all kommunikasjon med angriperen og meld fra til din nærmeste leder. Dersom du har blitt utsatt for tilsvarende svindel på privaten og har sendt fra deg penger, må du øyeblikkelig melde fra til banken din. Anmeld også til politiet.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Don Cavender *er tidligere spesialagent i FBI, med over 22 års erfaring med digital etterforskning og cyberkriminalitet. Nylig jobbet han målrettet mot cyberkriminalitet som koordinator for Washington DC BEC. Han driver opplæring og trening, samt forskning innen digital etterforskning.* @don_cavender
https://www.linkedin.com/in/donald-cavender

Ressurser

Direktør-svindel (CEO-fraud):	https://nettvett.no/direktor-svindel/
Sosial manipulering:	https://nettvett.no/sosial-manipulering/
Phishing:	https://nettvett.no/phishing/
Sikker pålogging:	https://nettvett.no/sikker-palogging/