OUCH! | November 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Sosial manipulering
- Oppdage / stopp sosiale manipuleringsangrep
- Stopp fremtidige angrep

Sosial manipulering

Oversikt

En vanlig oppfatning mange har av digitale angrep er at de bruker avanserte hacker-verktøy og teknologi for å bryte inn i personers datamaskiner, kontoer og mobile enheter, dette er feil. Angripere har lært at den enkleste måten å stjele informasjon på eller hacke deg på er ved å snakke med deg å mislede deg til å gi fra deg informasjonen. I dette nyhetsbrevet vil vi lære deg hvordan disse sosiale angrepene, kalt sosial manipulering fungerer og hva du kan gjøre for å beskytte deg selv.

Gjesteredaktør

Alissa Torres er sertifisert SANS instruktør, som spesialiserer seg i avansert digital etterforskning og hendelseshåndtering. Hun har erfaring i industrien med å håndtere hendelser og jobber på et internt sikkerhetsteam som digital etterforsker, Alissa er også på Twitter: **@sibertor**.

Sosial manipulering

Sosial manipulering er et psykologisk angrep hvor en angriper misleder deg til å gjøre noe de vil at du skal gjøre. Disse angrepene har eksistert i tusenvis av år, ideen om å lure noen eller svindle noen er ikke ny. Bruk av disse teknikkene på Internett har likevel vist seg å være veldig effektivt og man kan angripe millioner av personer. Den enkleste måten å forstå hvordan disse angrepene fungerer på er ved å se på et ekte eksempel.

Du mottar en telefon fra noen som sier de er fra at data support selskap, kanskje din Internettleverandør, eller kanskje Microsoft tech support. De forklarer at datamaskinen din oppfører seg merkelig, som at den skanner Internettet eller sender ut spam og de tror at den har blitt infisert. De har fått i oppgave å undersøke saken og hjelpe deg med å sikre din datamaskin. De bruker deretter en rekke med tekniske begrep og ber deg følge forvirrende steg for så å forsikre deg om at datamaskinen din er infisert.

De kan for eksempel be deg om å sjekke om du har spesifikke filer på datamaskinen og fortelle deg steg for steg hvordan du finner dem. Når du finner disse filene, så vil de forsikre deg om at dette er et tegn på at datamaskinen din er infisert, i realiteten er disse filene vanlige systemfiler som finnes på alle datamaskiner. Etter at de har lurt deg til å tro at datamaskinen er infisert, så vil de presse deg til å gå til deres nettside for å kjøpe deres sikkerhetsprogramvare eller gi dem fjerntilgang til din datamaskin så de kan fikse problemet. I realiteten er programmet ondsinnet. Hvis du kjøper og installerer programmet, så

Sosial manipulering

har de ikke bare lurt deg til å infisere din egen datamaskin, men du har også betalt dem for å gjøre det. Hvis du gir dem fjerntilgang til datamaskinen, så vil de ta over datamaskinen og infisere den.

Sosiale angrep som beskrevet over er ikke begrenset til telefonsamtaler; de kan skje med hvilken som helst teknologi, inkludert e-post, SMS, Facebook-meldinger, Twitter eller andre samtaler på nett. Det som er viktig er at man vet hva man burde se etter.

Å lære hvordan du kan forhindre, detektere og stoppe sosiale angrep er en av de mest effektive stegene du kan ta for å beskytte deg selv.

Oppdage / stoppe sosiale manipuleringsangrep

Den enkleste måten å beskytte mot sosiale angrep på er å bruke sunn fornuft. Hvis noe virker mistenkelig eller ikke føles riktig, så kan det være et angrep. Noen vanlige indikatorer på angrep er:

- De skaper en form for hastverk, hvis du føler at du er under press for å ta en hurtig beslutning, så bør du være forsiktig.
- De ber om informasjon de ikke burde ha tilgang til eller informasjon de allerede bør ha tilgang til.
- Noe som er for godt til å være sant. Et vanlig eksempel er at du får beskjed om at du har vunnet i et lotteri du ikke en gang har deltatt i.

Hvis du mistenker at noen prøver å lure deg, stopp kommunikasjonen med personen. Hvis de ringer deg på telefonen, legg på. Hvis de snakker med deg på nett, avslutt tilkoblingen. Hvis det er en e-post du ikke stoler på, slett den. Hvis angrepet er arbeidsrelatert, rapporter det til support eller sikkerhetstjenesten umiddelbart.

Hindre fremtidige angrep

Heldigvis er det noen steg du kan ta for å minimisere muligheten for fremtidige angrep.

- **Aldri del passordet ditt**: Ingen seriøs organisasjon vil kontakte deg og spørre om passordet ditt. Hvis noen spør om passordet ditt er det et angrep.

Sosial manipulering

- **Ikke del for mye informasjon**: Desto mer en angriper vet om deg, desto lettere er det for dem å finne og lure deg. Selv deling av små detaljer om deg selv over tid kan bli satt sammen til å bli et komplett bilde av deg. Det er mindre sjanse for at du blir angrepet hvis du offentliggjør mindre informasjon om deg selv på nett, dette inkluderer sosiale medier, produktanmeldelser, forum og e-postlister.

- **Verifiser kontaktperson**: Noen ganger blir du kanskje oppringt av banken, kredittkortselskapet, tjenesteleverandøren for mobilen eller andre organisasjoner for legitime årsaker. Hvis du tviler på at en forespørsel er legitim, spør personen om navn og telefonnummer. Deretter finner du organisasjonens telefonnummer fra en kilde du stoler på, som på bankkortet, tidligere brev, eller på organisasjonens nettside (sørg for at du taster inn adressen riktig). Nå kan du ringe organisasjonen og være sikker på at du snakker med den riktige organisasjonen. Dette virker kanskje tungvint, men sikring av din personinformasjon og identitet er verdt det ekstra steget.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos
http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på www.norsis.no.

Ressurser

E-post phishing angrep:	http://www.securingthehuman.org/ouch/2013#february2013
Sikkerhet I sosiale medier:	http://www.securingthehuman.org/ouch/2013#march2013
Veiledning om nettsvindel:	http://www.onguardonline.gov/topics/avoid-scams

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis