OUCH! | January 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- **Hva er sosial manipulering?**
- **Oppdage og stoppe forsøk på sosial manipulering**

Sosial manipulering

Oversikt

En vanlig misforståelse om cyberangrep som er vanlig hos veldig mange, er at kun avanserte angrepsverktøy og teknikker brukes for å hacke folks datamaskiner og brukerkontoer. Dette stemmer ganske enkelt ikke. Cyberkriminelle har lært at den enkleste måten å stjele informasjon, hacke en konto eller infisere et datasystem er å lure deg til å gjøre en feil. I dette nyhetsbrevet ser vi nærmere på hvordan angrepene kalt sosial manipulering fungerer, og hva du kan gjøre for å beskytte deg mot dem.

Gjesteredaktør

James Lyne (**@jameslyne**) er sertifisert SANS-instruktør og global leder for forskning ved Sophos. Han dekonstruerer og undersøker de siste og viktigste av de cyberkriminelles kreasjoner. Han er også forfatter for SANS-kursene for Metasploit (SEC850) og Social Engineering (SEC567).

Hva er sosial manipulering?

Sosial manipulering (Social Engineering på engelsk) er et psykologisk angrep hvor en angriper lurer deg til å gjøre noe du ikke burde gjøre. Selve konseptet sosial manipulering er ikke nytt, det har eksistert i tusenvis av år. I bunn og grunn er det de samme teknikkene som svindlere og bedragere bruker. Det som gjør sosial manipulering så mye mer effektivt for de kriminelle med dagens teknologi, er at du ikke er i stand til å fysisk se dem. På den måten kan de svært enkelt utgi seg for å være hva eller hvem som helst, og de kan nå ut til millioner av folk over hele verden, inkludert deg. I tillegg kan forsøk på sosial manipulering lett omgå mange teknologiske sikkerhetstiltak. For enklest mulig å forstå hvordan slike angrep virker, og hvordan du unngår dem, kan vi se på to eksempler fra virkeligheten.

Du får en telefon fra noen som hevder de jobber i et datasupportfirma, gjerne for nettleverandøren din eller for Microsoft Tech Support. Vedkommende forteller deg at datamaskinen din aktivt skanner internett, de tror den er infisert, og har fått i oppgave å hjelpe deg med å sikre den. De bruker så flere forskjellige tekniske ord og uttrykk, og tar deg gjennom flere forvirrende steg for å overbevise deg om at datamaskinen din faktisk er infisert. For eksempel kan det være de ber deg om å sjekke om du har visse filer på datamaskinen din, og hjelper deg med å finne frem til dem. Når du finner dem forsikrer de deg om at disse filene er bevis på at datamaskinen er infisert. I virkeligheten er dette vanlige systemfiler som finnes på nesten alle datamaskiner. Når de har lurt deg til å tro at du er infisert, presser de deg til å kjøpe sikkerhetsprogramvare eller til å gi dem fjernstyringstilgang til datamaskinen din, slik at de kan fikse den. Men programvaren de selger er egentlig

Sosial manipulering

skadelig programvare. Om du kjøper og installerer den har du ikke bare blitt lurt til å infisere datamaskinen din, du har også betalt dem for det. Om du gir dem fjernstyringstilgang til maskinen tar de den over, og stjeler data og informasjon som de bruker til sine egne formål.

Sunn fornuft er ditt sterkeste forsvar når du må oppdage og stoppe forsøk på sosial manipulering.

Et annet eksempel er et e-postangrep kjent som direktørsvindel, som for det meste skjer på jobb. De cyberkriminelle undersøker organisasjonen din på nettet, og finner navnet på sjefen din eller kollegaen din. Deretter utformer de en e-post hvor de utgir seg for å være den personen, og sender den så til deg. E-posten gir inntrykk av dårlig tid, den ber deg skynde deg med å gjøre noe, som å overføre penger eller sende e-post tilbake med sensitiv ansattinformasjon. Ganske ofte prøver disse e-postene å få deg til å tro at det er snakk om en alvorlig hastesak, som krever at du omgår standard prosedyre. For eksempel kan de be om at svært sensitiv informasjon sendes til en privat @gmail.com-adresse. Det som gjør slike angrep så alvorlige, er at de cyberkriminelle gjør grundige undersøkelser på forhånd. Slike angrepsforsøk kan heller ikke bli oppdaget eller stoppet av tekniske sikkerhetsmekanismer som antivirus eller brannmurer, fordi det ikke er noen skadevare eller skadelige linker involvert.

Husk at angrep som benytter sosial manipulering, som disse, ikke er begrenset til telefonoppringninger og e-post. De kan forekomme i enhver form, inkludert tekstmeldinger, henvendelser over sosiale medier, eller ansikt til ansikt. Nøkkelen er å vite hva du skal være på utkikk etter, du er selv ditt eget beste forsvar.

Oppdage og stoppe forsøk på sosial manipulering

Heldigvis er det enklere enn du tror å stoppe slike angrep – sunn fornuft er ditt beste forsvar. Om noe virker mistenkelig eller ikke føles riktig, kan det være et angrepsforsøk. De vanligste tegnene på forsøk på sosial manipulering inkluderer:

- Noen skaper en stor følelse av hastverk, de forsøker å lure deg til å gjøre en feil før du rekker å tenke deg om.
- Noen ber om informasjon de ikke burde ha tilgang til, eller allerede burde vite, som for eksempel kontonummer.
- Noen ber om passordet ditt, ingen legitim organisasjon vil noensinne gjøre det.
- Noen legger press på deg for å omgå sikkerhetsrutiner du normalt må følge på jobben.

Sosial manipulering

- Noe som er for godt til å være sant. For eksempel får du beskjed om at du har vunnet et lotteri, eller vunnet en iPad, selv om du aldri har deltatt i lotteriet eller konkurransen.
- Du mottar en merkelig e-post fra en venn eller kollega, som inneholder ordformuleringer som ikke virker likt dem. En cyberkriminell kan ha hacket seg inn på e-postkontoen deres og forsøker kanskje å lure deg. For å beskytte seg i slike tilfeller kan du ta kontakt med vennen din på en annen måte, for eksempel ansikt til ansikt eller på telefon, og bekrefte at e-posten er legitim.

Dersom du mistenker at noen prøver å lure deg, avbryt all kommunikasjon med personen det gjelder. Dersom angrepsforsøket er jobbrelatert må du sørge for å rapportere det til arbeidsplassens helpdesk eller informasjonssikkerhetsgruppe med en gang. Husk, sunn fornuft er ofte ditt beste forsvar.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

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.

Ressurser

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Direktørsvindel:	https://securingthehuman.sans.org/ouch/2016#july2016
Løsepengevirus:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH-arkivet:	https://securingthehuman.sans.org/ouch/archives

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversatt av: NorSIS

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus