OUCH! | December 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Phishing

Oversikt

E-post er en av de vanligste kommunikasjonsformene vi har. Ikke bare bruker vi det på jobben hver eneste dag, men vi bruker det også for å holde kontakten med venner og familie. I tillegg benytter de fleste virksomheter nå e-post for å tilby sine tjenester, som bekreftelser for netthandel. Nettopp fordi så mange mennesker verden over er avhengige av e-post, har det blitt en av de primære angrepsvektorene brukt av cyberkriminelle. I dette nyhetsbrevet forklarer vi phishing, som er et av de vanligste angrepsmetodene for e-post, og hva du kan gjøre for å være trygg når du bruker e-post.

Gjesteredaktør

Dr. Lance Hayden er administrerende direktør for Berkeley Research Group. Han er ekspert på sikkerhetskultur og handlemønster, og har skrevet boken People-Centric Security: Transforming Your Enterprise Security Culture fra McGraw-Hill. Han kan nåes her: **https://www.linkedin.com/in/drhayden**.

Phishing

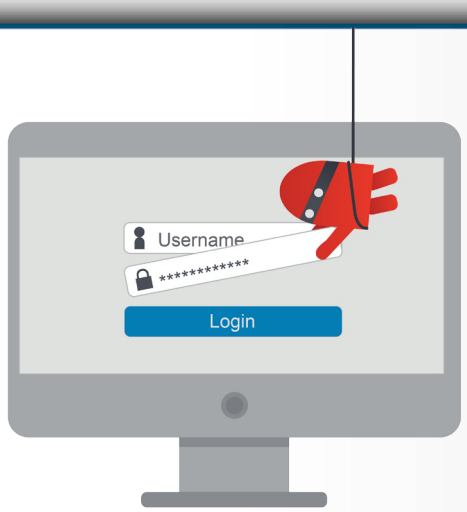
Phishing refererer til et angrep som benytter e-post eller meldingstjenesten til et sosialt nettverk for å lure deg til å gjøre en bestemt handling, som å klikke på en lenke, eller åpne et vedlegg. Dersom man blir rammet av et slikt angrep er risikoen stor for at svært sensitiv informasjon kommer på avveie, og/eller at datamaskinen din blir infisert av skadelig programvare. Angriperne jobber hardt for å gjøre phishing-e-postene troverdige. For eksempel vil de prøve å få det til å se ut som om e-posten kommer fra noen eller noe du kjenner, som en venn, eller en virksomhet du bruker ofte. De kan til og med legge inn logoen til banken din, eller forfalske avsenderadressen slik at e-posten virker mer ekte. Deretter sender angriperne phishing-e-postene til millioner av mennesker. De vet aldri hvem som vil bli rammet, det eneste de vet er at jo flere e-poster de sender ut, jo større er sjansen for suksess. Phishing fungerer litt på samme måte som å fiske med et garn. Du vet aldri hva du vil fange, men jo større garnet er, jo mer fisk får du tak i. Angripere bruker phishing på flere ulike måter for å oppnå det de vil:

- **Samle inn informasjon**: Angripernes mål er å samle inn personlig informasjon som passord, kredittkort-/bankkortnumre, eller bankdetaljer. For å oppnå dette sender de deg en e-post med en lenke til en nettside som fremstår som ekte. På denne nettsiden blir du bedt om å oppgi kontoinformasjon eller persondata. Nettsiden er derimot falsk, og all informasjon du taster inn, går direkte til de kriminelle.
- **Skadelige lenker**: Angripernes mål er å ta kontroll over maskinen eller enheten din. For å oppnå dette sender de deg en e-post med en lenke. Dersom du klikker på lenken, tas du til et nettsted som kjører et angrep mot

Phishing

maskinen din. Hvis angrepet er suksessfullt, blir skadelig programvare installert på maskinen eller enheten din.

- **Skadelig vedlegg**: Angripernes mål er også her å infisere og ta kontroll over maskinen din. Men istedenfor å sende deg en lenke, sender angriperne deg en infisert fil, som et Word-dokument. Hvis du åpner vedlegget trigges angrepet, noe som potensielt kan gi angriperne full kontroll over systemet ditt.
- **Lureri**: Noen phishing-e-poster er ikke annet enn vanlig svindel over digitale kanaler. De prøver å lure deg ved å fortelle at du har vunnet i et lotteri, eller ved å utgi seg for å være en veldedig organisasjon som trenger donasjoner, eller ved å be om din hjelp til å flytte millioner av kroner. Hvis du svarer vil de forsøke å lure til seg pengene dine ved å for eksempel si at de trenger betaling for sine tjenester, eller at de trenger tilgang til bankkontoen din.



Ditt beste forsvar er sunn fornuft. Hvis en e-post eller en melding virker merkelig, mistenksom, eller for god til å være sann, kan det være et forsøk på phishing.

Slik beskytter du deg

I nesten alle tilfeller er det å åpne og lese en e-post helt greit. For at et phishingangrep skal fungere, må de kriminelle lure deg til å gjøre noe aktivt. Det finnes heldigvis flere tegn som kan indikere at en henvendelse egentlig er et angrep, her er de mest vanlige:

- E-posten forsøker å skape en følelse av hastverk, der det kreves at du «handler umiddelbart» før noe negativt skjer, som for eksempel at kontoen din stenges. Angriperen ønsker å stresse deg opp til å gjøre en feil før du rekker å tenke gjennom hva som skjer.
- Du mottar en e-post med et vedlegg du ikke forventer å få, eller e-postmeldingen forsøker å lokke deg til å åpne vedlegget. For eksempel kan det stå at vedlegget inneholder detaljer om uanmeldte permitteringer, lønningslister, eller varsel om restskatt.
- E-posten bruker en generisk hilsen som «Kjære kunde» eller lignende, istedenfor å bruke navnet ditt. De fleste venner eller virksomheter du har kontakt med vet navnet ditt, og bruker det i ekte henvendelser.
- Svært sensitiv informasjon som kredittkort-/bankkortnummer og passord blir etterspurt i e-posten.
- Det står i e-posten at henvendelsen kommer fra en offisiell organisasjon, men staving og grammatikk er dårlig, eller e-postadressen som er brukt er av personlig karakter, som @gmail.com, @yahoo.com, eller @hotmail.com.

Phishing

- Lenken i e-posten ser merkelig eller uoffisiell ut. Et tips er å holde musepekeren over lenken til en liten infoboks eller et vindu dukker opp, der du kan se hvor lenken egentlig vil føre deg. Hvis lenken i e-posten ikke stemmer overens med det egentlige målet, bør du ikke klikke på den. På mobile enheter kan du få opp en tilsvarende boks ved å trykke og holde inne på lenken. En enda tryggere metode er å kopiere lenken og lime den inn i nettleseren din, eller å manuelt taste inn den korrekte lenken.
- Du mottar en melding fra noen du kjenner, men den er ordlagt på en annen måte en slik vedkommende vanligvis ordlegger seg. Hvis du mistenker mulig phishing kan du ringe vedkommende for å få verifisert at han/hun faktisk har sendt e-postmeldingen. Det er enkelt for cyberkriminelle å lage en e-post som virker som om den kommer fra en venn eller kollega.

Dersom du mistenker at en e-post eller en melding er et forsøk på phishing, kan du ganske enkelt slette den. Til syvende og sist er sunn fornuft det 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 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 https://norsis.no.

Ressurser

Sosial manipulering:	https://www.securingthehuman.org/ouch/2014#november2014
Fem steg for å holde seg sikker:	https://www.securingthehuman.org/ouch/2014#october2014
Jeg er blitt hacket, hva nå?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS Dagens sikkerhetstips:	https://www.sans.org/tip_of_the_day.php

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Oversatt av: Mats Authen