OUCH! | Juli 2013

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Hva er spear phishing
- Effektiviteten til spear phishing
- Hvordan beskytte deg selv

Spear Phishing

Hva er spear phishing

Du er kanskje kjent med phishing-angrep, dette er e-post sent av kriminelle til millioner av mulige ofre rundt hele verden. E-postene er lagd for å lure, villede eller angripe. Vanligvis ser disse beskjedene ut som de kommer fra en pålitelig kilde, som banken din, eller noen du kjenner. E-postene har ofte en beskjed som haster eller en avtale som er for god til å si nei til. Hvis du klikker på linken i en phishing e-post, blir du kanskje tatt til en ondsinnet side som prøver å angripe datamaskinen din eller samle inn brukernavn og passord. Eller så har kanskje phishing e-posten et infisert vedlegg, hvis du åpner vedlegget, prøver det å infisere og ta kontroll over maskinen din. Cyberkriminelle sender disse e-postene til så mange personer som mulig, vitende om at jo flere personer som mottar e-posten, desto flere vil falle for svindelen.

Gjesteredaktør

Lenny Zeltser er gjesteredaktør for denne utgaven av OUCH! Lenny fokuserer på å ivareta kunders IT-operasjoner hos HCR Corp og underviser hvordan bekjempe malware på SANS instituttet. Lenny er aktiv på Twitter som **@lennyzeltser** og skriver om sikkerhet på bloggen **blog.zeltser.com**.

Selv om phishing er effektivt, finnes det et relativt nytt angrep som kalles spear phishing. Konseptet er det samme, angripere sender e-post til offeret, utgir seg for å komme fra en organisasjon eller en person offeret stoler på. Men, i motsetning til vanlig phishing e-post, er spear phishing veldig målrettet. Istedenfor å sende en e-post til millioner av mulige ofre, sender de beskjeder til et begrenset utvalg av mennesker, kanskje fem til ti personer. Den andre forskjellen er at man, med spear phishing, gransker målene først. Dette kan gjøres ved å lese LinkedIn eller Facebook profil, eller andre beskjeder de legger ut på offentlige forum. Basert på denne granskingen, kan angriperne lage en veldig tilpasset e-post som virker relevant for det utvalgte målet. På denne måten er det mye mer sannsynlig at personer blir lurt av angrepet.

Effektiviteten til spear phishing

Spear phishing blir brukt når de vil angripere deg eller din organisasjon spesifikt. Mens de fleste kriminelle er ute etter å stjele penger, har angripere som bruker spear phishing veldig spesifikke mål, vanligvis tilgang til konfidensiell informasjon, som firmahemmeligheter, planer for sensitiv teknologi, eller konfidensiell statlig

Spear Phishing

kommunikasjon. Eller kanskje de prøver å bruke organisasjonen din som et springbrett til en annen organisasjon. Slike angripere har mye å vinne og er villig til å investere både tid og innsats i å granske målene sine.

Den beste måten å beskytte seg mot spear phishing er å være bevisst på at du kan være et mål, begrens informasjonen du legger ut om deg selv og rapporter mistenkelig e-post.

For eksempel, en utenlandsk regjering vil kanskje bestemme at din organisasjon utvikler produkter eller teknologi som er nøkkelen til det landets økonomiske suksess og vil derfor sette deg som et mål. De undersøker organisasjonens nettside og identifiserer tre nøkkelpersoner. De undersøker så LinkedIn-, Twitter- og Facebook-sidene til disse personene og lager en full mappe på dem. Etter å ha analysert disse tre personene vil angriperne lage en spear phishing e-post der de utgir seg for å være en leverandør av organisasjonen. E-posten har et vedlegg som tilsynelatende er en faktura, i virkeligheten er det en infisert fil. To av de tre personene som var målet, åpner vedlegget, samtidig gir de utenlandsk regjering tilgang til organisasjonens produkthemmeligheter, som de nå vil produsere selv.

Spear phishing er en mye større trussel en enkle phishing-angrep, siden angriperne utformer et angrep spesifikt til deg eller din organisasjon. Ikke bare øker det sannsynligheten for suksess, men angrepene er mye vanskeligere å oppdage.

Hvordan beskytte deg selv

Det første steget for å beskytte deg mot målrettede angrep er å forstå at du kan være et mål. Du og din organisasjon besitter sannsynligvis sensitiv informasjon som noen andre vil ha tak i, eller kan bli brukt til å aksessere en annen virksomhets informasjon, som er angriperens egentlige mål. Når du forstår at du kan bli angrepet, ta følgende forholdsregler for å beskytte deg og din organisasjon:

- Begrens informasjonen du legger ut om deg selv på forum, Facebook og LinkedIn. Jo flere personlige detaljer du deler, desto enklere er det for angripere å utforme en spear phishing e-post som virker relevant og ekte.

Spear Phishing

- Hvis en e-post ber deg om å åpne et vedlegg, klikke på lenke som virker mistenkelig eller ber deg om å oppgi sensitiv informasjon, verifiser meldingen. Hvis e-posten tilsynelatende kommer fra et selskap eller en person du kjenner, bruk kontaktinformasjonen du allerede har for å kontakte sender og verifiser at de sendte beskjeden.
- Støtt sikkerhetsinnsatsen i din organisasjon ved å følge aktuell sikkerhetspolicy og bruk sikkerhetsverktøy, som antivirus, kryptering og sikkerhetsoppdateringer når de er tilgjengelig.
- Husk at teknologi kan ikke filtrere og stoppe alle e-post-angrep, særlig spear phishing e-post. Hvis en e-post ser litt merkelig ut, les gjennom nøye. Hvis du er bekymret over at du kanskje har mottatt en spear phishing e-post eller blitt rammet av et spear phishing angrep, kontakt helpdesk eller informasjonssikkerhetsteamet umiddelbart.

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

Hvordan unngå å falle for spear phishing:	http://www.theatlanticwire.com/technology/2013/02/spear-phishing-security-advice/62304/
Unngå sosial manipulering og phishing angep:	http://www.us-cert.gov/ncas/tips/st04-014
Phishing:	http://www.securingthehuman.org/resources/newsletters/ouch/2013#february2013
Vanlige sikkerhetsbegrep:	http://www.securingthehuman.org/resources/security-terms
SANS daglige sikkerhetstips:	https://www.sans.org/tip_of_the_day.php

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