OUCH! | Juli 2016

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- **Hvad er CEO svindel?**
- **Sådan beskytter du dig selv.**

CEO svindel

Hvad er CEO svindel?

IT-kriminelle er snedige, de finder hele tiden på nye metoder til at opnå det, de vil. En af deres mest effektive metoder er at angribe folk som dig. IT-kriminelle har fundet ud af, at utrænede personer er det svageste led i alle organisationer. De kriminelle har glemt, at der er folk, der har viden om IT-sikkerhed, måske fordi de læser OUCH!. Disse folk kan være organisationens bedste forsvar.

Gæsteredaktør

Angela Pappas er chef for informationssikkerhed og træning ved Thomson Reuters. I denne rolle er Angela ansvarlig for ambassadørprogrammet, eLearning og for træning af ansatte om phishing.

IT-kriminelle har udviklet en ny type angreb som kaldes CEO svindel (”CEO Fraud”) eller ”Business Email Compromise” (BEC). I disse angreb lader en IT-kriminel som om, han er CEO’en eller en anden leder fra din organisation. De sender en e-mail til ansatte som dig, og prøver at snyde dig til at gøre noget, du ikke burde gøre. Disse angreb er meget effektive, fordi de kriminelle har gjort deres forarbejde godt. De har undersøgt din organisations hjemmeside for informationer og ved derfor, hvor organisationen er placeret, hvem lederne er, samt hvilke organisationer der samarbejdes med. Herefter undersøger de IT-kriminelle sider som LinkedIn, Facebook og Twitter og finder ud af så meget som muligt om andre medarbejderne. Når først der er styr på organisationens struktur, koncentrerer de deres angreb om specifikke medarbejdere. De udvælger medarbejderne ud fra deres mål. Hvis de er ude efter penge, vil de ofte gå efter en medarbejdere i økonomiafdelingen. Hvis de er ude efter skatteinformationer, vil de måske gå efter ansatte i HR. Hvis de ønsker adgang til database serverne vil målet være medarbejdere i IT.

Når først de har fundet ud af hvad de vil have og hvem de vil angribe, begynder de at planlægge det egentlige angreb. Ofte bruger de målrettet phishing (”spear phishing”). Phishing er når en IT-kriminel sender en e-mail til millioner med det formål at få dem til at gøre et eller andet, det kan være at åbne en vedhæftet ondsindet fil eller besøge en ondsindet hjemmeside. Målrettet phishing er anderledes end phishing ved, at man i stedet for at sende en standard mail til millioner af mennesker målretter mailen til en lille udvalgt skare. Disse målrettede e-mails er meget svære at genkende, da de er skrevet meget virkelighedstro. Ofte kommer disse e-mails fra en du kender eller arbejder sammen med, måske en kollega eller din leder. De er virkelighedstro, da der ofte bruger den samme jargon

CEO svindel

som du og dine kollegaer bruger, måske indeholder de organisationens logo eller den officielle signatur fra en leder. Mailen giver dig ofte en fornemmelse af, at det det haster og kræver, at du gør noget øjeblikkeligt uden at fortælle det til noget. De IT-kriminelle ønsker at skynde på dig så du begår en fejl. Her er de tre oftest brugte metoder:

CEO svindel er et kraftfuldt angreb, der kan slippe i gennem de fleste af dine sikkerhedssystemer. Ultimativt er du det bedste forsvar.

- **Bankoverførsel**: En IT-kriminel er ude efter penge. Det betyder, at de finder ud af hvem der arbejder i økonomiafdelingen eller hvilket team der håndterer din organisations økonomi. De IT-kriminelle sender en e-mail, hvor de udgiver sig for at være en leder og i e-mailen står der at der er opstået en kritisk situation og der skal straks overføres penge til en bestemt konto.

- **Skattesvindel**: IT-kriminelle ønsker at stjæle information om dine kollegaer, så de kriminelle kan udgive sig for kollegaer over for skattemyndighederne og begå skattesvig. De IT-kriminelle undersøger de organisation for at fastslå hvilke medarbejder der håndterer medarbejderoplysningerne, for eksempel HR. Herefter sender the IT-kriminelle falske e-mails, hvor i de udgiver sig som en leder eller en medarbejder fra den juridiske afdeling og kræver adgang til bestemte dokument øjeblikkelig.

- **Udgive sig for at være advokat**: Ikke al CEO svindel er baseret udelukkende på e-mail. Andre metoder så som telefonen kan bruges. I dette scenario starter de IT-kriminelle med at sende dig en e-mail hvor de udgiver sig for at være leder og gør dig opmærksom på, at en advokat vil ringe angående et spørgsmål, der haster. Den kriminelle ringer så til dig og udgiver sig for at være advokaten. De kriminelle skaber en fornemmelse af, at det haster ved at sige, at det drejer sig om oplysninger af tidsfølsomme og fortrolige karakter.

Sådan beskytter du dig selv.

Hvad kan du så gøre for at beskytte dig og din organisation? Almindelig sund fornuft er det det bedste forsvar. Hvis du modtager en besked fra din leder eller kollega og den ikke lyder rigtig eller føles rigtig, så er det måske et angreb. Hints kan være, at mailen giver udtryk for at det haster enormt meget, en signatur der ikke ser helt rigtig ud, eller at

CEO svindel

beskeden er skrevet i en anden tone end den plejer, måske bliver der brugt et andet navn end hvad personen normalt kalder dig. Et andet hint kan være at angriberen bruger en e-mailadresse eller telefonnummer, du aldrig har set før, eller måske bruger de en e-mailadresse der minder om, men som ikke er helt magen til en kollegas eller en leders. Hvis du er i tvivl, skal du ringe til personen på et telefonnummer, du har tillid til eller mødes med dem, og få dem til at bekræfte at de har sendt mailen. Du skal naturligvis ikke svare på den sendte e-mail og bede dom bekræfte at de har afsendt mailen. Du skal aldrig gå uden om sikkerhedspolitikken eller sikkerhedsprocedurer. Din organisation har måske politikker, der beskriver de korrekte procedurer for at autorisere overførsel af penge eller fortrolig information. Hvis du får en forespørgsel, der beder dig gå uden om disse politikker, skal du være mistænksom og få en bekræftelse før du handler -uafhængig af, hvem der sender forespørgslen. Hvis du modtager en sådan forespørgsel, skal du straks kontakte din nærmeste leder, informationen eller teamet der står for information om sikkerhed.

Hvis du vil vide mere

På securingthehuman.sans.org/ouch/archives kan du tilmelde dig det månedlige nyhedsbrev om IT-sikkerhed fra OUCH! Her kan du ligeledes få adgang til ældre udgaver af OUCH! og læse mere om SANS IT-sikkerhedsløsninger

WelcomeSecurity samarbejder med netop din virksomhed og med at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på http://www.welcomesecurity.net.

Tidligere udgivelser (ikke oversat til dansk)

Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Two-step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Tip of the Day:	https://www.sans.org/tip-of-the-day

Licensinformation

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity