Det månedlige nyhetsbrevet om sikkerhetsbevissthet for databrukere

OUCH!

I denne utgaven

- **Problemet**
- **Løsningen**
- **Eksempel**

To-faktor autentisering

GJESTEREDAKTØR

Fred Kerby er gjesteredaktør i denne utgaven. Han er tidligere Information Assurance Manager for Naval Surface Center Dahlgren avdelingen. Han er også senior instruktør i SANS og leder for Intro to Information Security kurset (SEC301). Fred underviser også Information Security Leadership (MGT512) og Security Essentials (SEC401).

PROBLEMET

For å bruke mange av tjenestene på Internett i dag, som e-post, nettbank eller netthandel, må du først bevise at du er den du sier du er. Prosessen med å bevise din identitet er kjent som autentisering. Autentisering blir gjort ved å bruke noe du vet (f.eks. passord), noe du har (f.eks. smarttelefon), eller noe som er unikt ved deg (f.eks. fingeravtrykk). Tradisjonelt sett er den vanligste måten å autentisere seg på; brukernavn og passord. Problemet med denne form for autentisering er enkel; alt en angriper trenger, er å gjette eller kompromittere passordet og de kan få tilgang til kontoen din og informasjonen din. Hvis du bruker samme brukernavn og passord på flere kontoer, kan skaden bli mye større. For å bedre beskytte kontoene dine, flytter flere nettsider over til sterkere autentisering, metoder som krever bruk av mer enn én faktor for autentisering. Vi vil forklare hva dette er, hvordan det fungerer og hvorfor du bør bruke det.

LØSNINGEN

Sterkere autentisering bruker mer enn én faktor; ikke bare må du vite noe hemmelig som ett passord, men du må også ha en eiendel (f.eks. smarttelefon) eller vise fram noe unikt ved deg (f.eks. fingeravtrykk). To-faktor autentisering er akkurat hva det høres ut som, du trenger to faktorer for å bevise hvem du er istedenfor én. Ett vanlig eksempel på to-faktor autentisering er bankkortet. For å bruke minibanken må du ha noe (bankkortet ditt) og du må vite noe (PIN koden). Hvis en angriper stjeler bankkortet, får de ikke brukt det, med mindre de også vet PIN koden (som er grunnen til at du aldri må skrive PIN koden på kortet). Ved å kreve to-

To-faktor autentisering

faktor autentisering er du bedre beskyttet, enn hvis det bare kreves én.

To-faktor autentisering på nett virker på samme måte som bankkortet og PIN kombinasjonen. Du bruker brukernavn og passord når du vil aksessere kontoen din. Men etter du har tastet inn korrekt passord, i stedet for å komme inn på kontoen, krever siden en ekstra faktor for å autentisere deg, f.eks. verifikasjonskode eller fingeravtrykk. Hvis du ikke har den andre faktoren, får du ikke tilgang. Det andre steget beskytter deg. Hvis en angriper har kompromittert passordet ditt, er du og kontoene dine er fortsatt trygge siden angriperen ikke kan fullføre det andre steget uten å ha den andre faktoren.

EKSEMPEL

La oss gå gjennom ett eksempel for hvordan to-faktor autentisering kan fungere. En av de mest brukte nettjenestene er Gmail. Mange autentiserer seg til Gmail kontoen og andre Google tjenester via brukernavn og passord. Google tilbyr nå ekstra sikkerhet med to-faktor autentisering, eller det Google kaller two-step verification (to-steg verifisering). Googles to-steg verifisering krever to ting for autentisering: passordet ditt (noe du vet) og smarttelefon (noe du har). For å bevise at du har smarttelefonen, så vil Google sende ut en SMS med en engangs verifiseringskode, som er unik for deg (merk deg at disse tjenestene kan koste penger; sjekk med din leverandør for mer informasjon). Du skriver deretter inn koden. Hvis du ikke vil at Google sender verifiseringskode via SMS, kan du installere en app som genererer den unike koden for deg. På denne måten trenger du ikke en gang tilgang til tjenesteleverandøren, bare din smarttelefon. Verdien i sterkere autentisering er; selv om en angriper har kompromittert Google passordet ditt, kan de ikke aksessere Google kontoene dine, med mindre de også har fysisk tilgang til din smarttelefon. Du og din verdifulle informasjon er beskyttet.

Bruk to-faktor autentisering hvis du kan, det er en av de beste måtene å beskytte tilgang til kontoene dine og informasjonen.

To-faktor autentisering

Vær oppmerksom på at verifikasjonskodene er unike; de er ulike hver gang du autentiserer deg. Derfor må du gå gjennom denne to-steg prosessen hver gang du trenger å autentisere deg for din Google konto. I tillegg er ikke denne funksjonen aktivert som standard, for å aktivere denne funksjonen, logg inn på din Google konto, gå til Account settings, velg Security og følg stegene for two-step verification.

Andre nettjenester tilbyr også to-faktor autentisering, som Dropbox, Paypal eller kanskje også banken din. Noen av disse tjenestene bruker kanskje smarttelefonen, mens andre som Paypal eller banken sender deg en spesiell brikke for å generere verifikasjonskoder. Andre tjenester igjen bruker kanskje en spesiell enhet som man plugger inn i USB-porten på datamaskinen, som Yubikey. Hvis noen av tjenestene du bruker, støtter to-faktor autentisering, vil vi sterkt anbefale at du benytter deg av det.

RESSURSER

Noen av linken har blitt nedkortet for bedre lesbarhet ved bruk av TinyURL tjenesten. For å beskytte mot sikkerhetstrusler bruker OUCH! alltid TinyURL sin funksjon for forhåndsvisning, som viser hvor linken fører hen og ber om bekreftelse før den tar deg dit.

Google To-Steg Verifisering:

http://preview.tinyurl.com/cncte9n

PayPal (og EBay) Security Key:

http://preview.tinyurl.com/838dpds

Vanlige sikkerhetsbegrep:

http://preview.tinyurl.com/6wkpae5

SANS daglige sikkerhetstips:

http://preview.tinyurl.com/6s2wrkp

LES MER

Abonner på månedlig OUCH! nyhetsbrev, få tilgang til OUCH! arkiver og lær mer om SANS sikkerhetsbevissthet løsninger ved å besøke oss 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 www.norsis.no.

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy

Oversatt av: Norsk senter for informasjonssikring(NorSIS)