OUCH! | September 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Totrinns pålogging

Overblikk

Det å bevise hvem du er (såkalt autentisering) er nøkkelen til å sikre informasjonen din. Sterk autentisering skal sørge for at du er den eneste som har tilgang til din informasjon og tjenester som email, bilder og bankkontoer. Det er tre forskjellige måter å bekrefte hvem du er; hva du vet – for eksempel passordet ditt, hva du har – som blant annet førerkort eller kodebrikke og hvem du er – som fingeravtrykk.

Gjesteredaktør

Keith Palmgren har over 30 år erfaring med informasjonssikkerhet. Han er sertifisert instruktør for SANS Institute og er forfatter av SANS SEC301 – en femdagers introduksjon til informasjonssikkerhetskurset. Når han ikke underviser, fokuserer Keith på konsultasjon og skriveprosjekter. Du kan følge Keith på **@kpalmgren**.

Hver av disse metodene har sine fordeler og ulemper. Passord er, som du kanskje vet, den vanligste autentiseringsmetoden. I dette nyhetsbrevet skal vi lære deg å sikre informasjonen din med totrinns pålogging, som gir langt bedre beskyttelse enn passord alene og samtidig er veldig enkelt å bruke. For å forstå hvordan totrinns pålogging fungerer starter vi med passord.

Passord

Passord brukes for å bevise hvem du er basert på noe du vet. Faren med passord er at alle eggene kan bli liggende i én kurv. Om noen gjetter seg til eller får tak i passordet ditt kan de utgi seg for å være deg og enkelt få tilgang all informasjonen som passordet skal beskytte. Det er derfor man lærer å lage gode passord, for eksempel å bruke sterke passord som er vanskelig for andre å gjette, ha forskjellige passord til alle brukerkontoer og tjenester, samt aldri del passordet ditt med noen. Selv om disse rådene fortsatt er gyldige, ser vi at passord ikke lenger er effektive i dagens samfunn. Den siste teknologien gjør det alt for lett for angripere å finne ut hva passordet er. Det vi trenger er en autentiseringsmetode som er enkel å bruke og samtidig gir høy sikkerhet. Et slik alternativ er totrinns pålogging, som nå tilgjengelig hos en rekke tjenester.

Totrinns pålogging

Totrinns pålogging (også kalt to-faktor autentisering eller 2FA) er en sikrere bekreftelsesløsning enn passord alene. Disse løsningene krever at du bruker to ulike metoder for å bekrefte hvem du er. Et eksempel er bankkortet ditt. Når du tar ut

Totrinns pålogging

penger i en minibank, bruker du faktisk totrinns pålogging. For å logge inn trenger du både bankkortet ditt (noe du har) og PIN-koden din (noe du vet). Om du skulle miste bankkortet ditt er pengene dine fortsatt trygge. Dersom noen finner kortet ditt, kan de ikke bruke det i og med at de ikke vet PIN-koden din (med mindre du har den skrevet ned på kortet ditt, som er en veldig dårlig idé). Det samme gjelder om noen har fått tak i PIN-koden din, men ikke har kortet. En angriper må derfor ha både kort og kode for å få tilgang til bankkontoen din. Dette gjør totrinns pålogging mye sikrere, siden du har to lag med sikkerhet.

Bruk totrinns pålogging der du kan, det er en av de beste tiltakene du kan gjøre for å sikre informasjonen din.

Å bruke totrinns pålogging

Totrinns pålogging er noe du aktiverer individuelt for hver av kontoene dine. I dag tilbyr heldigvis mange tjenester dette på nett. Google er en av de ledende aktørene for totrinns pålogging. Google-kontoer er et kjent mål for cyber-angripere, i og med at Google tilbyr en rekke gratistjenester på nett til millioner av brukere verden over. Google så seg derfor nødt til å tilby en sikrere autentisering, og ble dermed en av de første til å tilby totrinns pålogging for de fleste internett-tjenestene sine. Om du forstår hvordan Googles totrinns pålogging fungerer, vil du også forstå konseptet for de fleste andre sider, som Twitter, Facebook, Apple, Instagram og banker.

Først aktiverer du totrinns pålogging på Google-kontoen din, og registerer et telefonnummer. Når du har gjort dette, vil totrinns pålogging fungere på følgene måte: Du logger inn som vanlig med brukernavn og passord. Dette er den første bekreftelesen – noe du vet. Deretter sender Google en SMS til mobilen din som innholder en unik kode på seks siffer. Denne koden skriver du inn på nettsiden, og det er dermed den andre faktoren. For å logge inn på kontoen må du altså ha både passordet ditt og telefonen din for å motta den unike koden. Dersom en angriper skulle få tak i passordet ditt, må de også ha telefonen din for å få tilgang. For å sikre at kontoen din er godt beskyttet sender Google en ny, unik kode hver gang du logger inn.

Totrinns pålogging

Det er også et annet alternativ for totrinns pålogging med Google og en rekke andre sider. Istedenfor å motta en unik kode på SMS, kan du installere en autentiseringsapp på smarttelefonen din. Appen genererer en unik kode for deg hver gang du vil logge inn. Fordelen med å bruke en app er at du ikke trenger å være tilkoblet et teleselskap for å motta koden – telefonen gjør det for deg. I tillegg kan ikke koden bli snappet opp, siden den blir generert lokalt på din telefon.

Husk at totrinns pålogging ikke er aktivert som standardoppsett, du må aktivere det selv. Selv om totrinns pålogging kan virke som mye jobb i starten, anbefaler vi på det sterkeste at du bruker det der det er mulig, spesielt for kritiske tjenester som e-post, nettbank og lagringstjenester på nett. Totrinns pålogging sikrer informasjonen din i mye større grad enn kun et passord.

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

Passordsetninger:	http://www.securingthehuman.org/ouch/2015#april2015
Sider som støtter totrinns pålogging:	https://twofactorauth.org
Stopp. Tenk. Klikk:	http://stopthinkconnect.org/2stepsahead
Google totrinns pålogging:	http://www.google.com/landing/2step/
SANS Dagens sikkerhetstips:	http://www.sans.org/tip_of_the_day.php

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