OUCH! | April 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Ja, du er faktisk et mål

Oversikt

En vanlig oppfatning mange har, er at de ikke er et mål for cyberkriminalitet, de tror gjerne at de ikke har noe av verdi på datamaskinen deres; dette er helt feil. Hvis du har en datamaskin, mobil enhet, konto på nett, epostadresse, kredittkort eller hvilken som helst tilstedeværelse på nett, så er du verdt penger for cyberkriminelle. I dette nyhetsbrevet vil vi forklare hvorfor du er et mål, hvordan du blir angrepet og hva du kan gjøre for å beskytte deg selv.

Gjesteredaktør

Eric Conrad er president og CTO for Backshore Communication og hovedforfatter på bøkene: CISSP Study Guide andre utgave og Eleventh Hour CISSP andre utgave. Han er også medforfatter av seks-dagers kurset Continous Monitoring and Security Operations (SEC511) hos SANS.

Hvorfor du er et mål

Kriminelle handlinger som bedrageri, ID-tyveri eller utpressing har eksistert så lenge som det har vært sivilisasjoner, de er en del av vårt daglige liv. De kriminelles mål har alltid vært det samme: å tjene så mye penger som mulig, så lett som mulig og med minst mulig risiko. Før var dette vanskeligere, kriminelle var hemmet av deres lokasjon og måtte fysisk samhandle med det tiltenkte offeret. Dette begrenset ikke bare målgruppen til de kriminelle, men de ble også eksponert for større risiko. Med Internettet har kriminalitet forandret seg drastisk. Cyberkriminelle har nå hele verden som målgruppe, de kan angripe nesten uten kostnader og med veldig liten risiko. I tillegg har cyberkriminelle blitt godt organiserte og effektive, som betyr at de kan angripe flere enn noen gang før.

Cyberkriminelle vet at, desto flere kredittkort de kan stjele, desto flere bankkontoer kan de kompromittere, desto flere passord de kan kompromittere, desto mer penger kan de tjene. De vil bokstavelig talt prøve å kompromittere hvem som helst som er koblet til Internettet, inkludert deg. Å angripe millioner av mennesker rundt om i hele verden høres kanskje ut som mye arbeid, men det er overraskende lett siden de bruker automatiserte verktøy til å gjøre hele jobben. De vil, for eksempel, bygge opp en database med millioner av epostadresser og bruke automatiserte verktøy for å sende ut phishing epost til hver enkelt adresse. Sending av epost koster omtrent ingenting: de bruker bare kompromitterte datamaskiner, kanskje til og

© The SANS Institute 2014

Ja, du er faktisk et mål

med din datamaskin, til å gjøre jobben. Dette er et annet eksempel på hvorfor enheter har verdi, de kan alltid brukes til å angripe andre datamaskiner eller personer. De kriminelle vet ikke hvem som kommer til å bli offer for deres svindel, men de vet at, desto flere eposter de sender, desto flere vil falle for svindelen. En annen ting angriperne kan gjøre er å skanne alle datamaskinen på nettet (nok en gang via datamaskiner de allerede har kompromittert) for å lete etter datamaskiner de kan angripe. Du blir ikke valgt ut fordi du er spesiell, men kriminelle angriper alle de kan, som også inkluderer deg.

Du vet det kanskje ikke, men enhetene og informasjonen din har enorm verdi for cyberkriminelle rundt om i verden.

Beskytte deg selv

Når cyberkriminelle angriper personer rundt om i verden, så bruker de relativt enkle metoder. Du kan, heldigvis, beskytte deg ved å følge noen like enkle steg. Stegene under vil ta deg langt på vei for å beskytte deg mot angrep:

- **Deg selv**: Du er første forsvar for å beskytte deg mot angripere. Mange angrep starter med at kriminelle prøver å lure deg, som ved å få deg til å åpne et infisert vedlegg i en epost, eller lure deg til å gi fra deg passordet over telefonen. Sunn fornuft er ditt beste forsvar: hvis noe virker merkelig, mistenkelig eller for godt til å være sant, så er det mest sannsynlig et angrep.

- **Oppdatering**: Sørg for at alle datamaskiner eller mobile enheter du bruker er fullt oppdatert og har alle de siste sikkerhetsrettelsene. Dette gjelder både for operativsystemet og andre applikasjoner og utvidelser du har installert. Ved å alltid holde operativsystemet og applikasjoner oppdatert vil du sikre deg mot de fleste angrep.

- **Passord**: Bruk et sterkt, unikt passord til hver konto. Hvis en nettside du bruker blir kompromittert og alle passordene (inkludert ditt) blir kompromittert, så er de andre kontoene dine fortsatt trygge. Sørge også for at de forskjellige enhetene dine er beskyttet med et sterkt, unikt passord, PIN-kode eller annen låsemekanisme. For å sikkert holde oversikt over alle passordene dine, så kan du bruke en passordhåndterer.

© The SANS Institute 2014

Ja, du er faktisk et mål

- **Kredittkort**: Sjekk korttransaksjoner ofte, vi anbefaler ukentlig (månedlig er ikke nok). Med en gang du ser en uautorisert transaksjon, rapporter det til korttilbyderen. Hvis banken lar deg sette varsling på SMS eller epost ved store eller merkelige transaksjoner, bruk dette. Da får du raskere varsling ved mistenkelig aktivitet.

- **Nettverket ditt**: Sørg for at du sikrer det trådløse nettverket med et sterkt administratorpassord og sørg for at tilgang til nettverket krever et passord. I tillegg bør du ha en oversikt over hvilke enheter som er koblet til nettverket og sørge for at alle disse er oppdatert.

- **Sosiale medier**: Desto mere informasjon du legger ut å Internettet, desto mer sannsynlig er det at du utsetter deg selv for risiko. Ikke bare kan det bli enklere for angripere å lure deg, men informasjonen du legger ut, kan også identifisere deg som et verdifullt mål.

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

OUCH! Passordhåndterere:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Sikre hjemmenettverket:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Phishing angrep:	http://www.securingthehuman.org/ouch/2013#february2013
Plakat: Du er et mål:	http://www.securingthehuman.org/resources/posters

OUCH! utgis av SANS Securing The Human og er distribuert under Creative Commons BY-NC-ND 3.0 lisens.
Du kan fritt distribuere dette nyhetsbrevet eller bruke det i dine bevissthetsprogrammer, så lenge du ikke endrer nyhetsbrevet.
For å oversette eller mer informasjon, vennligst kontakt ouch@securingthehuman.org.

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