OUCH! | Oktober 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Fem steg for å holde seg sikker

Oversikt

Etter som teknologi får en viktigere rolle i livet vårt, blir det også mer komplekst. Teknologi forandrer seg så ofte at det kan være vanskelig å holde følge med sikkerheten. Det kan virke som det hele tiden er nye retningslinjer du må følge. Detaljene forandrer seg kanskje over tid, men det er fundamentale tips du alltid bør følge for å sikre deg selv. Uansett hvilken teknologi du bruker eller hvor du bruker det, så burde du følge disse fem stegene.

Gjesteredaktør

Lenny Zeltser fokuserer på å sikre kundenes IT-operasjoner hos NCR Corp og underviser i hvordan man bekjemper skadevare (virus) hos SANS. Lenny er aktiv på Twitter som **@lennyzeltser** og skriver en sikkerhetsblogg på **blog.zeltser.com**.

Fem steg

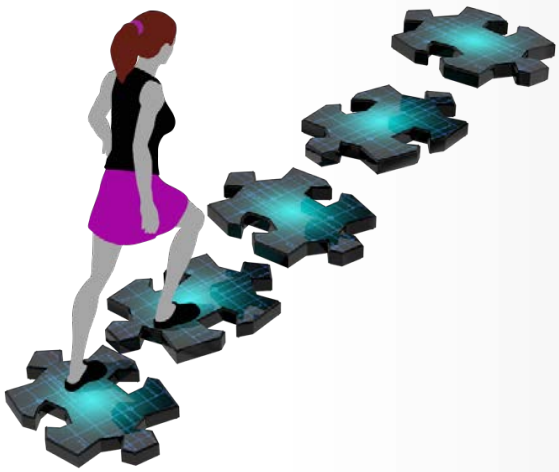
De fem stegne under er en enkel oversikt, for å lære mer om hvert steg, se på linkene under ressurser til slutt.

1. **Deg**: Du bør alltid huske at teknologi alene kan ikke beskytte deg. Angripere har lært at den enkleste måten å angripe de fleste systemer på er ved å angripe brukeren. Den enkleste måten å få passordet eller kredittkortet ditt på, er ved å lure deg til å gi det til dem. De kan for eksempel ringe og utgi seg for å være fra Microsoft tech support og si at datamaskinen din er infisert, i realiteten er de kriminelle som vil at du skal gi de tilgang til maskinen. En annen mulighet er at de sender deg en e-post og sier at pakken din ikke kunne bli levert og du må klikke på en link for å bekrefte adressen din, i realiteten vil de bare at du besøker en side slik at de kan prøve å ta over datamaskinen din. Det beste forsvaret du har imot en angriper er deg selv. Vær mistenksom, bruk sunn fornuft så kan du oppdage og stoppe de fleste angrep.

2. **Oppdatere**: Sørg for at datamaskiner, mobile enheter, applikasjoner og alt annet du kobler til nettverket er oppdatert til siste versjon. Kriminelle leter konstant etter svakheter i teknologien du bruker. Når de oppdager disse svakhetene, bruker de spesielle programmer for å utnytte svakheten (ofte kalt exploit på engelsk) og få tilgang til

Fem steg for å holde seg sikker

utstyret du bruker, inkludert nettverket, datamaskinen og mobile enheter. Samtidig jobber selskapene som lagde teknologien hele tiden med å redusere antall svakheter, noe som reduserer muligheten for at noen kan angripe deg. For å holde deg oppdatert, skru på automatisk oppdatering der det er mulig. Denne regelen gjelder for alt som er koblet til et nettverk, inkludert TV-er, baby monitor, rutere, spillkonsoller som er koblet til Internettet. Hvis datamaskinen operativsystem, mobile enhet eller hvilken som helst annen teknologi du benytter ikke lenger er støttet og ikke vil motta sikkerhetsoppdateringer, så anbefaler vi å bruke en versjon som er støttet.



Ved å følge disse fem stegene, så vil du være langt på vei til å beskytte deg selv mens du bruker den nyeste teknologien.

3. **Passord**: Det neste steget for å beskytte deg selv er å bruke et sterkt, unikt passord til hver av dine enheter, nettkontoer og applikasjoner. Nøkkelordene her er sterkt og unikt. Et sterkt passord betyr at en angriper ikke enkelt kan gjette det, enten manuell gjetting eller automatisk via verktøy. I stedet for å bruke ett ord, bruk en frase som består av flere ord og noen andre tegn og spesialsymboler for å være på den sikre siden. Unik vil si at du bruker forskjellige passord til forskjellige enheter og tjenester. Hvis ett passord blir kompromittert, så er fortsatt alle dine andre kontoer og enheter trygge. Du greier nok ikke å huske alle disse passordene, da er det anbefalt å bruke en passordhåndterer. Dette er et spesielt program til datamaskinen eller smarttelefonen som kan lagre passordene dine sikkert i et kryptert format. Til slutt, hvis tjenesten støtter to-faktor autentisering, aktiver det; dette er en av de sterkeste måtene du kan beskytte kontoen på.

4. **Kryptering**: Et tredje steg vi anbefaler er å bruke kryptering. Kryptering sørger for at bare du og personer du stoler på kan aksessere informasjonen. Data kan bli kryptert på to steder: stillestående eller i transitt. Kryptering av stillestående informasjon er beskyttelse av data lagret på harddisken eller USB minnepenn. De fleste operativsystemer har en mulighet til å automatisk kryptere alle dine data, oftest via full disk kryptering. Vi anbefaler at du aktiverer dette når det er mulig. Kryptering av data i transitt betyr kryptering av data mens det overføres fra din datamaskin eller enhet til en annen enhet, som når du bruker nettbanken. En enkel måte å sjekke om du krypterer informasjonen på er ved å sjekke at adressen starter med “https” og adressefeltet viser en hengelås.

Fem steg for å holde seg sikker

5. **Sikkerhetskopi**: Noen ganger, uansett hvor forsiktig du er, så kan en av enhetene eller kontoen dine bli kompromittert. Hvis det skjer er det, så må du ofte rense og slette alt på enheten for å sørge for at den er fri for virus. Angriperen kan også nekte deg tilgang til dine personlige filer, bilder og annen informasjon lagret på systemet. Den eneste muligheten er kanskje å gjenopprette filene fra en sikkerhetskopi. Sørg for at du tar regelmessig sikkerhetskopi av all viktig informasjon og sjekk at du kan gjenopprette filene hvis det skulle være nødvendig. De fleste operativsystem og mobile enheter støtter automatisk sikkerhetskopiering.

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

E-post phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Holde nettbrettet sikkert:	http://www.securingthehuman.org/ouch/2013#december2013
Sterke passord:	http://www.securingthehuman.org/ouch/2013#may2013
Passordhåndterere:	http://www.securingthehuman.org/ouch/2013#october2013
To-steg verifisering:	http://www.securingthehuman.org/ouch/2013#august2013
Kryptering:	http://www.securingthehuman.org/ouch/2014#august2014
Sikkerhetskopi:	http://www.securingthehuman.org/ouch/2013#september2013

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