OUCH!

SANS SECURITY AWARENESS

Ditt månedlige nyhetsbrev om sikkerhetsbevissthet

Fire enkle sikkerhetstiltak

Grunnlag

Å få mest mulig ut av teknologi, samtidig som man ivaretar sikkerheten, kan virke overveldende og forvirrende. Men uansett hva slags teknologi du bruker, og hvordan, så kan du alltid gjøre disse fire enkle tiltakene.

1. Deg selv: Først og fremst, vit at teknologien i seg selv ikke kan beskytte deg fullt og helt, du er selv ditt eget beste forsvar. Angripere har lært at den enkleste måten å få det som de vil på, er ved å rette seg mot deg, ikke mot datamaskinen din eller andre enheter. Dersom de ønsker passordet ditt, detaljer om betalingskort, eller kontroll over datamaskinen din, vil de prøve å lure deg til å gi dem det, ofte ved å skape en følelse av frykt eller at det haster. For eksempel kan de ringe å hevde å være fra Microsoft, og si at datamaskinen din er infisert. Men i virkeligheten er de cyberkriminelle som vil at du skal gi dem tilgang til datamaskinen din. Eller kan hende sender de deg en e-post med varsel om at en pakke ikke kan leveres, og legger press på deg om å klikke på en lenke for å bekrefte postadressen din. Men i virkeligheten lurer de deg inn på et skadelig nettsted som kan kompromittere datamaskinen din. Til syvende og sist er det du selv som er det beste forsvaret mot slike angripere. Ved å bruke sunn fornuft kan du oppdage og stoppe mange angrep.

2. Passordsetninger: Moderne prosesseringshastighet har gjort gamle passord på 8 tegn utdaterte og sårbare. Når en side ber deg om å lage et passord, lag en sterk og unik passordsetning istedenfor. En passordsetning er en type passord som bruker en serie ord som er lett å huske, for eksempel «bie honning bourbon regn». Jo lenger passordsetningen er, jo sterkere er den. At de er unike, vil si at du har forskjellige for hver brukerkonto. På denne måten vil de andre brukerkontoene forbli trygge dersom en av passordsetningene skulle komme på avveie. Klarer du ikke huske alle passordsetningene? Bruk et program for passordhåndtering, en såkalt «password manager». Disse er spesiallaget for å lagre passord trygt og sikkert.

Til slutt bør du også aktivere totrinnsbekreftelse (også kjent som bl.a. 2-faktor autentisering, multifaktor-autentisering). I tillegg til passordet logger du da inn med en engangskode som sendes til telefonen din,

eller genereres av en app. Totrinnsbekreftelse er sannsynligvis det viktigste og beste tiltaket for å beskytte brukerkontoene dine, og er mye enklere enn du tror.

3. Oppdatering: Sørg for at alt du har av datamaskiner, mobile enheter, programmer og apper har siste versjon av programvaren sin. Cyberkriminelle ser konstant etter nye sårbarheter i programvaren du bruker. Når de oppdager dem, bruker de spesiallagde programmer for å utnytte dem, og hacke seg inn i enhetene dine. Imens jobber selskapene som har laget programvaren konstant med å finne og fikse sårbarhetene ved å utgi oppdateringer. Ved å sørge for at oppdateringene installeres uten forsinkelse på datamaskin og mobile enheter gjør du det mye vanskeligere å hacke deg. Du kan som regel gjøre dette ved å aktivere automatisk oppdatering der det lar seg gjøre. Denne regelen gjelder for så å si all teknologi som er tilkoblet et nettverk, inkludert smarte TV-er, babymonitorer, overvåkingskameraer, hjemmeroutere, spillkonsoller og nyere biler.

4. Sikkerhetskopiering og gjenoppretting: Av og til kan du bli hacket uansett hvor forsiktig du er. Dersom det skulle skje, har du ofte ikke noe annet valg enn å gjenopprette fra en sikkerhetskopi om du vil ha tilbake personlige filer. Sørg for å jevnlig ta sikkerhetskopi av alt som er viktig, og sjekk at du kan gjenopprette fra dem. De fleste operativsystemer for PC og mobil støtter automatisk sikkerhetskopiering, enten til eksterne harddisker, eller til skyen.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Steve Anson *er sertifisert SANS-instruktør, og gir veiledning til IT-sikkerhetsteam og stater verden over, slik at de kan forbedre sikkerheten sin. Steve er forfatteren av den kommende boken «Applied Incident Response», og har gratis ressurser tilgjengelig for de som jobber med IT-sikkerhet på nettsiden* AppliedIncidentResponse.com.

Ressurser

Sosial manipulering:	https://www.sans.org/u/W3G
Persontilpasset svindel:	https://www.sans.org/u/W3Q
Passord gjort enkelt:	https://www.sans.org/u/W3V
Har du sikkerhetskopi:	https://www.sans.org/u/W40

OUCH! utgis av SANS Security Awareness, og er distribuert under Creative Commons BY-NC-BD 4.0 lisensen. *Du står fritt til å distribuere dette nyhetsbrevet, eller bruke det i ditt eget bevissthetsprogram, så lenge du ikke gjør endringer på nyhetsbrevet. For oversettelser og mer informasjon, ta kontakt med oss på* www.sans.org/security-awareness/ouch-newsletter. *Redaksjon: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Oversatt av: NorSIS*

NorSIS Norsk senter for informasjonssikring