OUCH! | October 2016

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Fire viktige sikkerhetstiltak

Oversikt

Ettersom teknologi fortsetter å utgjøre en større rolle i livene våre, blir den også mer komplisert. Det kan være forvirrende å holde seg oppdatert på sikkerhetstips på grunn av hvor fort teknologien forandrer seg. Det ser ut til at det alltid er en ny guide på hva du burde, eller ikke burde gjøre. Selv om detaljene om hvordan man holder seg sikker endrer seg over tid, finnes det alltid grunnleggende måter å sikre seg selv på. Samme hva slags teknologi du bruker, eller hvor du bruker det, så anbefaler vi å bruke disse fire følgende huskereglene. For å lære mer om dem, se ressursseksjonen i slutten av nyhetsbrevet.

Gjesteredaktør

Ryan Johnson fokuserer på å sørge for at organisasjoner er forberedt på å takle et uunngåelig sikkerhetsbrudd. Han er også lærer ved SANS instituttet, der han lærer bort avansert nettverksetterforskning. Ryan er aktiv på Twitter som **@ForensicRJ**.

1. **Deg**: Først og fremst, husk at teknologien i seg selv aldri vil kunne beskytte deg helt. Angripere har lært at den enkleste måten å trenge igjennom de mest avanserte sikkerhetstiltakene er ved å angripe deg. Hvis de er ute etter passordet ditt, bankkortet, eller personlig data, lurer de deg for å få deg til å gi fra deg denne informasjon. For eksempel kan de ringe deg og utgi seg for å være Microsoft support og påstå at PC-en din er infisert, mens i realiteten er de bare kriminelle som vil at du skal gi dem tilgang på maskinen din. Eller kanskje de sender deg en e-post hvor de forklarer at pakken din ikke kunne bli levert, og ber deg om å trykke på en link for å bekrefte adressen din, men i realiteten lurer de deg til å besøke en ondsinnet nettside som vil hacke seg inn på maskinen din. Dette er hvordan angrep som løsepengevirus eller direktørsvindel starter. Det beste forsvar mot angripere er deg. Vær mistenksom. Ved å bruke sunn fornuft kan du oppdage og stoppe de fleste angrep.

2. **Passord**: Det neste steget for å holde deg sikker, er å bruke et sterkt, unikt passord for hver digitale enhet og nettbaserte brukerkonto. Nøkkelordene her er sterkt og unikt. At et passord er sterkt, vil si at det er vanskelig å gjette for hackere, og for de automatiserte programmene deres. Men er du lei av komplekse passord som er vanskelige å huske og skrive? Da bør du prøve å bruke en passord-setning istedenfor. Istedenfor et enkelt ord, kan du bruke en serie med ord som du husker godt, for eksempel “Hvor er kaffen min?”. Jo lenger passordsetningen din er, jo sterkere

Fire viktige sikkerhetstiltak

er den. At passordet ditt er unikt, vil si at du bruker forskjellige passord for hver enhet og brukerkonto. På denne måten vil alle andre kontoer og enheter forbli sikre, selv om et passord skulle bli kompromittert og kjent. Sliter du med å huske alle disse sterke, unike passordene? Det gjør vi også. Derfor anbefaler vi at du bruker et passordhåndteringsprogram, også kjent som et passordhvelv (eller password manager på engelsk). Et slikt program kan brukes på mobilen eller PC-en for å lagre alle passordene dine kryptert og sikkert, slik at du slipper å huske alle sammen.

Ved å gjøre disse 4 nøkkeltiltakene kommer du langt med å sikre deg selv, mens du kan utnytte den nyeste teknologien til fulle.

Men kanskje det aller viktigste grepet du kan ta for å sikre en brukerkonto, er å aktivere 2-trinns bekreftelse. Passord alene er ikke lenger nok til å beskytte brukerkontoene våre, vi har behov for noe bedre. 2-trinns bekreftelse er mye sterkere. Da brukes passordet ditt, men det legges til et steg nummer to, enten noe du er (biometri), eller noe du har (som en engangskode sendt til mobilen din eller en app på mobilen som genererer en kode for deg). Aktiver denne funksjonen på hver eneste brukerkonto hvor det er mulig. 2-trinns bekreftelse er sannsynligvis det aller viktigste grepet du kan ta for å beskytte deg selv og er mye enklere å sette opp å bruke enn du tror.

3. **Oppdatering**: Sørg for at programvaren på datamaskinene dine, de mobile enhetene dine, apper og alt annet som er tilkoblet internett, er oppdatert til nyeste versjon. Cyberkriminelle er på konstant utkikk etter nye sårbarheter i programvaren som kjører på enhetene dine. Når de oppdager sårbarheter, bruker de spesiallagde programmer til å utnytte dem for å hacke seg inn på enhetene du bruker. Samtidig jobber selskapene som lager programvaren hardt for å sørge for at de er sikre, ved å gi ut oppdateringer som fikser sikkerhetsfeil. Ved å sørge for at disse oppdateringene blir installert på dine datamaskiner og mobile enheter, gjør du det mye vanskeligere for noen å hacke deg. For å holde deg oppdatert kan du ganske enkelt aktivere automatisk oppdatering der dette er mulig. Denne regelen gjelder for så å si all teknologi tilkoblet et nettverk, inkludert internett-tilkoblede TV-er, babymonitorer, hjemmeroutere, spillkonsoller og kanskje til og med bilen din. Om operativsystemet eller enheten er for gammel til å få nye sikkerhetsoppdateringer, anbefaler vi at du bytter dem ut med nye der sikkerhetsoppdateringer er mulig.

Fire viktige sikkerhetstiltak

4. **Sikkerhetskopiering**: Noen ganger, uansett hvor forsiktig du er, kan du bli hacket. I slike tilfeller er det å slette alt og gjenoppbygge systemet fra bunnen av ofte den eneste måten å forsikre seg om at alt av skadevare er borte. Angriperen kan til og med forhindre deg fra å få tilgang til personlige filer, fotografier og annen informasjon lagret på det hackede systemet. Ofte er den eneste måten du kan få tilbake de personlige filene på, å gjenopprette dem fra sikkerhetskopier. Sørg for at du jevnlig tar sikkerhetskopi av viktig informasjon, og bekreft at du kan gjenopprette fra sikkerhetskopiene. De fleste operativsystemer og mobile enheter støtter automatisk sikkerhetskopiering. I tillegg anbefaler vi at du lagrer sikkerhetskopiene i skyen eller på et separat lagringsmedium ikke tilknyttet noe nettverk, for å sikre dem mot cyberkriminelle.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

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.

Ressurser

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Passordhåndterere:	https://securingthehuman.sans.org/ouch/2015#october2015
Totrinns pålogging:	https://securingthehuman.sans.org/ouch/2015#september2015
Passordsetninger:	https://securingthehuman.sans.org/ouch/2015#april2015
Sikkerhetskopiering & gjenoppretning:	https://securingthehuman.sans.org/ouch/2015#august2015

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversatt av: NorSIS