OUCH! | Januar 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Sikker bruk av mobilapplikasjoner

Oversikt

Mobile enheter som nettbrett og smarttelefoner har blitt en av de viktigste teknologiene vi bruker i privat og i jobbsammenheng. Det som gjør mobile enheter så allsidig er alle applikasjonene du kan installere på enheten. Disse applikasjonene gjør at man kan bli mer produktiv, øyeblikkelig kommunisere og dele med andre, trene og utdanne, eller bare leke. Disse enhetene bringer også med seg en viss risiko; her er noen steg du kan ta for å bruke mobile applikasjoner sikkert.

Gjesteredaktør

Chris Crowley er uavhengig konsulent, sertifisert SANS instruktør og kursforfatter. Han er aktiv på Twitter (**@CCrowMontance**) og på Google plus (**+ChrisCrowley**).

Installere applikasjoner

Det første steget er å alltid sørge for at du laster de ned fra en leverandør du stoler på. Husk at hvem som helst kan lage en mobilapplikasjon, derfor må du være forsiktig med hvor du laster de ned fra. Cyberkriminelle har blitt flinke til å lage og distribuere infiserte mobilapplikasjoner som tilsynelatende er legitime. Hvis du installerer en av disse infiserte applikasjonene, så kan kriminelle ta kontroll over enheten; nå kan angriperen lese e-posten din, lytte på kommunikasjonen din og samle inn kontaktlisten din. Ved å kun laste ned applikasjoner fra kjente kilder som er til å stole på, så reduserer du muligheten for å installere en infisert applikasjon. Hvilken merke enheten har er det som bestemmer hva som er mulighetene dine.

For Apple enheter som iPad, eller iPhone, så kan du kun laste ned og installere applikasjoner fra et kontrollert miljø, Apple app store. Fordelen med dette er at Apple gjør en sikkerhetssjekk av applikasjonen og utviklerne av applikasjonen. Det er umulig for Apple å fange alle ondsinnete applikasjoner, men de reduserer risikoen for at du installerer en ondsinnet applikasjon dramatisk. Apple er også rask med å fjerne applikasjoner hvis de tror at den er ondsinnet. Windows Phone bruker lignende metoder og et lignende miljø for å håndtere applikasjoner.

Android enheter er annerledes. Android gir deg mer fleksibilitet ved at du kan laste ned en applikasjon fra hvilken som helst nettside. Denne fleksibiliteten legger mer ansvar over på brukeren, brukeren må være mer forsiktig med hvilke applikasjoner han installerer, da det ikke nødvendigvis er noen som sikkerhetssjekker de. Google vedlikeholder også et kontrollert applikasjonsbutikk som ligner på Apple sin, Google sin butikk heter Google Play.

Sikker bruk av mobilapplikasjoner

Applikasjonene du laster ned fra Google Play har blitt sjekket opp mot noen sikkerhetsrisikoer; det er derfor anbefalt at du kun laster ned mobilapplikasjoner til Android fra Google Play. Det er enkelt for angriper å lage falske applikasjoner og sette opp falske nettsider til å distribuere applikasjonene, det er derfor lurt å ikke installere applikasjoner fra andre steder. Som en ekstra beskyttelse kan du også vurdere å installere antivirus på enheten.

Nøkkelen til å bruke mobilapplikasjoner sikkert er å kun installere fra kilder du stoler på, verifisere tillatelser og holde applikasjonene oppdatert.

For å redusere risikoen enda mer, unngå applikasjoner som er helt nye og som få personer har installert, eller som har få positive kommentarer. Hvis en applikasjon har vært på markedet en stund og har mange positive kommentarer, er det mer sannsynlig at du kan stole på applikasjonen. Det er også viktig å kun installere applikasjoner man trenger. Før du installerer en applikasjon bør du spørre deg selv: trenger jeg virkelig denne applikasjonen? Hver applikasjon du har installer kan introdusere sårbarheter og personvernproblemer. Hvis du slutter å bruke en applikasjon, fjern den fra enheten (du kan alltid installere den på nytt hvis du finner ut at du trenger den likevel).

Det kan være fristende å jailbreake eller roote enheten. Dette er en prosess der man bryter seg inn i enheten og installerer uautoriserte applikasjoner eller forandrer eksisterende innebygd funksjonalitet. Vi anbefaler sterkt at du ikke gjør dette, dette eliminerer flere av sikkerhetsmekanismene innebygd i enheten, det kan også ugyldiggjøre garantien og support avtaler.

Tillatelser

Etter at du har installert en applikasjon fra en kilde du stoler på er det viktig at sørger for at den er konfigurert riktig og beskytter personvernet ditt. Installering eller konfigurering av mobilapplikasjoner krever ofte at du gir applikasjonen visse tillatelser. Tenk deg om før du gir ut slike tillatelser, trenger applikasjonen virkelig de tillatelsene for å gjøre den jobben den lover? Noen applikasjoner bruker for eksempel geo-lokasjonstjenester. Hvis du tillater applikasjonen å aksessere denne informasjonen, så kan applikasjonen muligens følge alle dine bevegelser og kanskje til og med selge denne informasjonen videre. Hvis du ikke ønsker å gi applikasjonen disse tillatelsene, se etter en annen applikasjon som tilfredsstiller kravene dine, det finnes mange muligheter. Apple-enheter gjør det mulig å forandre noen tillatelser etter applikasjonen er installert, som tilgang til geo-lokasjon. Windows og Android

Sikker bruk av mobilapplikasjoner

enheter er annerledes, her må du godta alle tillatelsene eller ingen; hvis du ikke godtar alle tillatelsene kan du ikke installere applikasjonen.

Oppdatere applikasjoner

Mobilapplikasjoner, på samme måte som datamaskinen din og operativsystemet på smarttelefonen, må oppdateres regelmessig. Kriminelle leter hele tiden etter svakheter i applikasjoner; hvis de finner en kan de utvikle angrep for å utnytte svakheten. Utviklerne av applikasjonen utvikler og slipper rettelser for å rette disse svakhetene og dermed beskytte enheten din. Det er viktig at du sjekker for oppdateringer regelmessig slik at du hele tiden er oppdatert. De fleste systemer kan konfigureres slik at applikasjoner oppdateres automatisk, dette er anbefalt. Hvis dette ikke er mulig, bør du sjekke etter oppdatering omtrent hver andre uke. Når du oppdaterer må du også verifisere eventuelle nye tillatelser de krever.

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

Sosial manipulering:	http://www.securingthehuman.org/ouch/2014#november2014
Avhende mobile enheter:	http://www.securingthehuman.org/ouch/2014#june2014
Sikre ditt nye nettbrett:	http://www.securingthehuman.org/ouch/2013#december2013
Sikring av nettbrett og smarttelefoner:	https://norsis.no/2013/01/sikring-av-nettbrett-og-smarttelefoner/
SEC575: Mobile Device Security Course:	http://www.sans.org/sec575

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