OUCH! | Mars, 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Sikker bruk av mobile apper

Oversikt

Mobile enheter som nettbrett, smarttelefoner og klokker har blitt en av de viktigste teknologiene vi bruker, både privat og i arbeidslivet. Det som gjør mobile enheter så allsidige, er at det er millioner av apper å velge mellom. Med disse appene blir vi mer produktive, kan ha rask kommunikasjon med andre, trene og lære opp andre, eller bare ha det moro. Imidlertid, med mulighetene alle disse appene gir kommer det også mer risiko. Her er noen grep du kan ta for å sørge for at du bruker appene sikkert, og får mest mulig ut av bruken.

Gjesteredaktør

Joshua Wright er teknisk direktør for Counter Hack og seniorinstruktør ved SANS instituttet. Han er forfatter av SEC575: Mobile Device Security and Ethical Hacking, og Hacking Exposed: Wireless. Du kan nå Josh på Twitter **@ joswr1ght**.

Få tak i mobile apper

For det første burde du sørge for at du alltid laster ned apper fra en kilde som er trygg og pålitelig. Cyberkriminelle har blitt mestere i å lage og distribuere infiserte apper som fremstår som legitime. Dersom du installerer en slik infisert app, kan de kriminelle ta full kontroll over din mobile enhet. Du reduserer risikoen for å installere infiserte apper ved å kun laste ned apper fra godt kjente, pålitelige kilder. Det du kanskje ikke er klar over, er at hva slags mobil enhet du har avgjør alternativene dine for nedlastning av apper.

For Apple-enheter som iPad eller iPhone, burde du kun laste ned apper fra Apple App Store. Fordelen med dette er at Apple gjennomfører sikkerhetssjekker av alle apper før de blir tilgjengelige for nedlastning. Selv om Apple ikke kan fange opp absolutt alle infiserte apper, bidrar dette til å drastisk redusere risikoen for å installere infiserte apper. I tillegg fjerner Apple raskt apper som de finner i App Stor dersom de mistenker at den er infisert. Windows Phone har en tilsvarende tilnærming for å bestyre appene sine.

Android-enheter er annerledes. Android gir deg mer fleksibilitet ved å gi deg muligheten til å laste ned apper fra hvor som helst på nettet. Men denne fleksibiliteten kommer med mer ansvar. Du må være mer forsiktig med hvilke apper du laster ned

Sikker bruk av mobile apper

og installerer ettersom ikke alle er sjekket. Google har en app-butikk lik Apple sin, kalt Google Play. Appene man kan laste ned fra Google Play har bestått noen sikkerhetstester, derfor anbefaler vi at du kun laster ned apper til Android fra Google Play. Unngå å laste ned Android-apper fra andre nettsider, siden hvem som helst, inkludert cyberkriminelle, enkelt kan lage og distribuere skadelige apper og lure deg til å infisere de mobile enhetene dine med dem.

Nøkkelen til sikker bruk av mobile apper er å installere appene fra trygge kilder, installere oppdateringer når de er tilgjengelige, og kun gi de tillatelsene som er nødvendige.

Uavhengig av hva slags enhet du har kan du ta et ekstra sikkerhetsgrep ved å unngå apper som er helt nye og er lite lastet ned, eller som har få positive kommentarer. Jo lenger en app har vært tilgjengelig, jo flere folk som har brukt den, og jo flere positive kommentarer den har, jo mer sannsynlig er det at den er pålitelig. I tillegg burde du kun installere apper du faktisk trenger og bruker. Spør deg selv: Trenger jeg virkelig denne appen? Ikke bare fører hver app med seg potensielle sårbarheter, men også potensielle personvernproblemer. Dersom du slutter å bruke en app bør du fjerne den fra enheten, du kan alltids legge den til igjen senere dersom du skulle få bruk for den igjen. Til slutt, aldri jailbreak eller root din mobile enhet. Dette innebærer å hacke inn i den og installere ikke-godkjente apper, og endre på eksisterende, innebygd funksjonalitet. Dette omgår og eliminerer mange sikkerhetskontroller, og fører også ofte til at du mister garantier og mulighet for kundeservice.

Tilganger

Når du har installert en app fra en sikker kilde, burde du forsikre deg om at den er riktig konfigurert og beskytter personvernet ditt. Før du tillater at en app får visse tilganger, bør du tenke etter om du faktisk vil gi appen tilgangene den ber om, har den faktisk behov for dem? For eksempel bruker noen apper geolokasjonstjenester. Dersom du tillater at en app alltid vet hvor du er, tillater du kanskje at de som lagde appen kan spore bevegelsene dine, kanskje til og med selge den informasjonen til andre. Om du ikke vil gi de tilgangene kan du avvise dem, eller lete videre etter en annen app som møter dine standarder. Husk at du har massevis av alternativer å velge mellom.

Sikker bruk av mobile apper

Oppdatering av apper

Akkurat som datamaskiner og mobile operativsystemer, må mobile apper oppdateres for å fungere riktig. Kriminelle leter etter og oppdager konstant nye svakheter i apper. De utvikler så angrep for å kunne utnytte disse svakhetene. Utviklerne som lager appene du bruker lager og gir ut regelmessige oppdateringer for fikse disse svakhetene og dermed beskytte enheten din. Jo oftere du ser etter og installerer oppdateringer, jo bedre. De fleste enheter lar deg konfigurere systemet slik at appene dine blir oppdatert automatisk. Vi anbefaler disse innstillingene. Dersom dette ikke er mulig, anbefaler vi at du ser etter oppdateringer til appene dine minst hver andre uke. Til slutt, når appene er oppdatert, undersøk om de ber om noen nye tilganger.

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

Sosial manipulering:	https://securingthehuman.sans.org/ouch/2017#january2017
Sikker avhending av mobile enheter:	https://securingthehuman.sans.org/ouch/2016#december2016
Slik sikrer du ditt nye nettbrett:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH arkivet & oversettelser:	https://securingthehuman.sans.org/ouch/archives
Sikkerhetskurs for mobile enheter:	https://sans.org/sec575

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

