Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

Sikker brug af apps

Overblik

Mobile enheder, så som tablets, smartphones og smartwatches, er blevet en af de teknologier, vi bruger mest både på arbejdet og i fritiden. Det, der gør de mobile enheder så alsidige, er at der er millioner af apps, man kan vælge mellem. Disse apps giver os mulighed for at være mere produktive, kommunikere med andre, træne og uddanne os eller bare have det sjovt. Med alle disse muligheder kommer der også nogle risici. I det følgende beskrives nogle forholdsregler, du kan tage for at bruge dine apps på en sikker måde.

Gæsteredaktør

Joshua Wright er "technical director" ved "Counter Hack" og er senior instruktør ved SANS Institute. Han er forfatter af "SEC575: Mobile Device Security and Ethical Hacking" og "Hacking Exposed: Wireless". Du kan følge Josh på Twitter **@joswr1ght**.

Sådan får du fat i apps

Det første du skal gøre, er at sikre dig, at du altid downloader apps fra et sted, du har tillid til. IT-kriminelle er dygtige til at lave og distribuere ondsindede apps, der ser ud til at være legitime. Hvis du installerer en af disse ondsindede apps, kan de IT-kriminelle tage fuldstændig kontrol over din mobile enhed. Hvis du kun downloader apps fra steder, som du har tillid til, reducerer du risikoen for at downloade en ondsindet app. Hvilke muligheder, du har for at downloade apps, afhænger af mærket af din mobile enhed

Hvis du har en Apple enhed såsom en iPad eller en iPhone, skal du downloade apps fra "Apple App Store". Fordelen ved dette er at Apple laver et sikkerhedstjek af alle apps, før det er muligt at downloade dem. Selvom Apple kan ikke fange alle de ondsindede apps, vil dette kraftigt mindske risikoen for at downloade en ondsindet app. Oveni dette vil Apple hurtigt fjerne en app, hvis de mener, den er ondsindet. Windows Phone håndterer deres apps på en tilsvarende måde.

Androids mobile enheder er anderledes. Android giver dig mere fleksibilitet ved at give dig mulighed for at downloade apps alle steder på internettet. Man skal være opmærksom på, at med denne fleksibilitet følger der et ansvar. Du skal

Sikker brug af apps

være mere forsigtig med, hvilke apps du downloader og installerer, da de ikke alle er tjekket. Google har en app store, Google Play, der minder om Apple App Store. De apps du downloader fra Google Play, har været gennem nogle grundlæggende sikkerhedstjek. Vi vil derfor anbefale, at du til din Android enhed kun downloader fra Google Play. Du skal undgå at downloade apps fra andre steder, da alle inklusive IT-kriminelle let kan lave og distribuere ondsindede apps, og snyde dig til at inficere din mobile enhed. Som yderligere beskyttelse kan du installere anti-virus på din enhed.

Nøglen til at benytte sig af apps uden at gå på kompromis med sikkerheden, er at installere fra steder du har tillid til, opdatere når det er muligt samt kun give appen de tilladelser det er nødvendigt.

Uanset hvilken enhed du bruger, er der flere nogle forholdsregler du kan tage. Undgå at installere helt nye apps, apps der ikke er downloadet af ret mange eller apps der har få positive anmeldelser. Jo længere tid en app har været tilgængelig, jo flere folk, der har brugt den og jo flere positive anmeldelse, den har fået, des større er chancen for, at man kan have tillid til appen. Oveni dette bør du kun installere apps du har brug for. Spørg altid dig selv om du virkelig har brug for denne app. Med hver app du installerer øger du ikke kun risikoen for at installere en ondsindet app, der er også nye privatindstillinger du skal tage stilling til. Hvis der er en app, du ikke længere bruger, skal du fjerne den fra din enhed (du kan altid installere den igen hvis du får brug for den). Sidst men ikke mindst skal du aldrig ”jailbreake” eller ”root” din enhed. Dette er processer, hvor du hacker din enhed og installerer ikke-godkendte apps eller ændrer funktioner, der er indbygget i enheden. Hvis du gør dette, bypasser eller fjerner du ikke blot mange af de sikkehedskontroller din enhed kommer med, du risikerer desuden, at din garanti ikke længere gælder samt at der ikke længere ydes support.

Tilladelser

Når først du har installeret en app fra et sted du har tillid til, skal du sikre dig at den er konfigureret korrekt og beskytter dit privatliv. Du skal altid tænke dig om før du giver en app tilladelse: vil du give appen den tilladelse, den beder om, har appen virkelig brug for det? Eksempelvis vil nogle apps bruge geolokation. Hvis du giver en app tilladelse til altid at kende din lokation, giver du måske den der har lavet appen tilladelse til at følge dine bevægelser og måske endda sælge

Sikker brug af apps

den information til tredjepart. Hvis du ikke ønsker at give appen den tilladelse, den beder om, kan du kigge efter en anden app der lever op til dine forventninger. Husk der er mange muligheder.

Opdaterer apps

Ligesom computere og mobile enheders operativsystem skal apps opdateres. IT-kriminelle leder efter svagheder i apps og udvikler angreb for at udnytte disse svagheder. Udviklerne der laver apps udgiver opdateringer, der har løst svaghederne og beskytter dine enheder. Jo oftere du søger efter og installerer opdateringer des bedre sikret er du. Du kan konfigurere de fleste enheder til automatisk at opdatere apps. Hvis du har den mulighed, anbefaler vi, at du benytter dig af den. Hvis du ikke har den mulighed, anbefaler vi at du tjekker for opdateringer hver fjortende dag. Når du opdaterer dine apps, skal du sikrer dig, at du kan acceptere eventuelle tilladelser, som de kræver.

Hvis du vil vide mere

På securingthehuman.sans.org/ouch/archives kan du tilmelde dig det månedlige nyhedsbrev om IT-sikkerhed fra OUCH! Her kan du ligeledes få adgang til ældre udgaver af OUCH! og læse mere om SANS IT-sikkerhedsløsninger

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Tidligere udgivelser

Social Engineering (oversat til dansk):	https://securingthehuman.sans.org/ouch/2017#january2017
Disposing Your Mobile Device (oversat til dansk):	https://securingthehuman.sans.org/ouch/2016#december2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH Archives & Translations:	https://securingthehuman.sans.org/ouch/archives
Mobile Device Security Course:	https://sans.org/sec575

Licensinformation

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity