وای! | مارس 2017

SafeNet Network & Security Services
شبکه امن اندیشه فردا

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

استفاده امن از برنامه های موبایل

مقدمه

سردبیر مهمان

جاشوا رایت مدیر فنی شرکت Counter Hack و مدرس ارشد موسسه SANS است. وی مولف SEC575 : Mobile Device and Ethical Hacking و همچنین کتاب Hacking Exposed : Wireless میباشد. برای ارتباط با Josh به حساب توییتری وی به آدرس **@joswr1ght** سر بزنید.

دستگاههای همراه نظیر تبلت، گوشی و ساعت هوشمند به یکی از تکنولوژی های اصلی که در زندگی شخصی و حرفه ای ما به وفور استفاده میشوند تبدیل شده اند. علت همه گیر شدن آنها وجود میلیونها برنامه کاربردی است که میتوان از آنها بهره برد. استفاده از این برنامه ها موجب میشود تا بهره وری بالاتری داشته باشیم، بدون وقفه با یکدیگر ارتباط و اشتراک داشته باشیم، در آموزش و پرورش از آنها استفاده کنیم و یا فقط از کار با آنها لذت ببریم. در کنار همه این مزایا استفاده از این ابزار خطراق نیز دارد.در این مقاله به قدمهایی اشاره میشود که برای استفاده امن از این ابزار ها باید برداشته شود تا بهترین استفاده را از آنها داشت.

تهیه برنامه های همراه

بعنوان اولین قدم حتما این ابزار ها را از منبع امن و قابل اطمینان دانلود کنید. مجرمان سایبری مهارتهای خود را در نوشتن و توزیع برنامه های آلوده افزایش داده اند و به نحوی که این برنامه ها قانونی به نظر میرسند. با نصب یکی از این برنامه های آلوده، مجرمان کنترل کامل دستگاه همراه را در دست خواهند داشت. با دانلود و نصب برنامه های کاربردی از منابع شناخته شده و مطمئن، احتمال نصب برنامه های آلوده کاهش خواهد یافت. نکته قابل توجه این است که نوع وسیله همراه تعیین میکند که چه گزینه هایی برای دانلود برنامه ها دارید.

برای دستگاههای شرکت اپل نظیر iPad و iPhone برنامه های همراه فقط از اپ استور شرکت اپل دانلود میشوند. مزیت این کار این است که شرکت اپل قبل از اینکه ابزارها را در دسترس عموم قرار دهد آنها را از نظر امنیت بررسی میکند. با توجه به اینکه شرکت اپل قادر به تشخیص همه برنامه های آلوده نیست، وجود این محیط مدیریت شده تا حد زیادی خطر نصب برنامه های آلوده را کاهش میدهد.علاوه بر این در صورتیکه شرکت اپل متوجه آلودگی یک برنامه در اپ استور شود به سرعت آن را حذف خواهد کرد. موبایل ویندوز نیز با همین روش برنامه ها را کنترل میکند.

استفاده امن از برنامه های موبایل

دستگاههای موبایل اندرویدی متفاوت هستند. اندروید انعطاف پذیرتر است چون قادرید از هر جایی از اینترنت دانلود کنید. اما این انعطاف پذیری مسئولیت پذیری بیشتری می طلبد. با توجه به اینکه همه برنامه ها بررسی نمیشوند میبایست با مراقبت بیشتری برنامه ها را دانلود و نصب کرد. شرکت گوگل هم مشابه شرکت اپل محیط مدیریت شده ای برای برنامه های موبایل ایجاد کرده است که به آن Google Play میگویند. برنامه های همراه که از گوگل پلی دانلود میشوند از برخی از بررسی های امنیتی اولیه عبور میکنند. از دانلود کردن برنامه های اندروید از سایتهایی غیر از گوگل پلی خودداری کنید چون هر شخصی از جمله مجرمان سایبری میتوانند برنامه های مخرب را بنویسند و توزیع کنند و در نهایت موجب آلوده شدن وسیله همراه شما شوند. برای حفاظت مضاعف در صورت امکان بر روی تجهیزات خود آنتی ویروس نصب کنید.

کلید استفاده امن از برنامه های موبایل نصب آنها تنها ار منابع مطمین، نصب بروز رسانی ها و تنها تایید اجازه دسترسی های لازم می باشد.

صرف نظر از اینکه از چه وسیله ای استفاده میکنید قدم دیگری که میتوانید بردارید خودداری از نصب برنامه هایی است که جدید هستند و تعداد کمی از افراد آن را دانلود کردند و یا برای آنها تعداد کمی نظرات مثبت ثبت شده است. قدیمی بودن یک برنامه به این مفهوم است که تعداد بیشتری از افراد از آن استفاده کرده اند و تعداد نظرات مثبت آنها نیز بیشتر است. همچنین برنامه هایی را نصب کنید که به آنها نیاز دارید. از خودتان بپرسید که آیا واقعا به این برنامه احتیاج دارید؟ هر برنامه ای بطور بالقوه آسیب پذیری های جدیدی را به همراه می اورد و همچنین برای حریم خصوصی افراد مشکل ایجاد خواهد کرد. در صورتیکه از یک برنامه استفاده نمیکنید، آنرا از وسیله همراه خود حذف کنید (شما میتوانید در هر زمانی که نیاز داشتید آن را مجددا نصب کنید). در آخر به هیچ عنوان وسیله همراه خود را جیلبریک و یا روت نکنید. جیلبریک و یا روت کردن نوعی هک کردن دستگاه است که با این روش امکان نصب برنامه های تایید نشده و یا تغییر عملکرد اصلی برنامه امکان پذیر میشود. این کار نه تنها باعث محدود کردن و یا دور زدن بسیاری از کنترل های امنیتی موجود دردستگاه شما میشود بلکه موجب از بین رفتن قراردادهای پشتیبانی و گارانتی نیز خواهد شد.

مجوز ها

زمانیکه یک برنامه را از یک منبع مطمئن بر روی دستگاه خود نصب کردید مطمئن شوید که آن برنامه بطور امن پیکربندی شده و از حریم خصوصی شما نیز محافظت میکند. قبل از اینکه به یک برنامه اجازه دسترسی دهید به دقت فکر کنید. آیا میخواهید مجوز درخواستی برنامه را به آن بدهید یا خیر؟ آیا آن برنامه واقعا به آن سطح دسترسی نیاز دارد؟ بعنوان مثال، بعضی از برنامه ها از (geo-location services) استفاده میکنند. در صورتیکه شما برای همیشه به یک برنامه اجازه بدهید که موقعیت شما را بداند، در واقع به نویسنده آن برنامه اجازه دادید که مسیر حرکتی شما را رد یابی

استفاده امن از برنامه های موبایل

کنند و آن اطلاعات را به دیگران بفروشند. اگر نمیخواهید به یک برنامه اجازه دسترسی بدهید، درخواست دسترسی را رد کنید و یا برنامه دیگری که با نیازمندی های شما مطابقت کند تهیه کنید. همیشه به خاطر داشته باشید که حق انتخاب زیادی دراپ استور و یا گوگل پلی دارید.

بروزرسانی برنامه ها

برنامه های همراه نیز مانند سیستم عامل های موجود در رایانه و موبایل، باید به نسخه جدید بروز شوند. مجرمان دایما در حال بررسی و پیدا کردن ضعف در برنامه ها هستند. قدم بعدی برای مجرمان بهره برداری از این ضعف هاست. نویسندگان آن برنامه نیز برای ترمیم نقاط ضعف و حفاظت از دستگاه شما نسخه های بروز رسانی را ارائه میدهند. هر چقدر بیشتر امکان نصب نسخه های بروز رسانی را چک کنید بهتر است. اغلب دستگاه ها به شما اجازه میدهند تا برنامه های خود را بصورت خودکار بروز رسانی کنید و توصیه ما استفاده از این تنظیمها است. اگر این کار شدنی نیست توصیه میشود هر ۲ هفته آخرین نسخه بروز رسانی را بررسی کنید و در آخر، بعد از انجام بروز رسانی همیشه بررسی کنید که آیا برنامه نیاز به مجوز دسترسی جدید دارد یا خیر.

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

مهندسی اجتماعی:	https://securingthehuman.sans.org/ouch/2017#january2017
نابودی دستگاه موبایل:	https://securingthehuman.sans.org/ouch/2016#december2016
امن کردن تبلت:	https://securingthehuman.sans.org/ouch/2016#january2016
آرشیو ها و ترجمه های SANS:	https://securingthehuman.sans.org/ouch/2016#june2016
درس امنیت دستگاه موبایل:	https://sans.org/sec575

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی