شرکت آب منطقه‌ای گلستان

نشریه داخلی شرکت آب منطقه‌ای گلستان/ شماره پنجم/ مرداد ماه ۱۴۰۴

وقتی نرم‌افزار سالم و قانونی

جاسوس می‌شود!

LEGAL SPY

STEPHANE NAPPO

پنج مدافع سایبری کارآمد عبارتند از:
پیش بینی، آموزش، تشخیص، واکنش
و انعطاف پذیری. به یاد داشته باشید:
اهمیت امنیت سایبری بسیار بیشتر از
موضوع فناوری اطلاعات است.

نشریه داخلی شرکت آب منطقه‌ای گلستان

شماره پنجم ـــ مرداد ماه ۱۴۰۴

فهرست

دکتر امیرحسین رحیمیان

وقتی نرم‌افزار سالم و قانونی جاسوس می‌شود!

به نام آن‌که امنیت را در کنار آگاهی به ما هدیه کرد.

هر روز که صفحه گوشی یا لپ‌تاپ خود را روشن می‌کنیم، بی‌آنکه متوجه باشیم، وارد دنیایی می‌شویم کـه مرز میان «امن» و «ناامن» در آن به باریکی یک تار مو رسـیده اسـت. سـال‌ها پیـش، وقتی صحبت از امنیت دیجیتال می‌شـد، ذهن بیشتر ما به سمت «هکرها»، «ویروس‌های کامپیوتری» یا «ایمیل‌های مشکوک» می‌رفت؛ تصاویری که رسانه‌ها از مهاجمان سایبری به نمایش می‌گذاشتند: افرادی با هودی مشکی، نشسته در اتاقـی تاریـک، در حال تایپ بی‌وقفـه روی صفحه‌کلید. اما امـروز، تهدیدات سـایبری الزاماً با چنین چهره‌هایی وارد زندگی ما نمی‌شـوند. بسـیاری از خطرها، در سکوت، با لبخندی آرام و حتی در قالب یک نرم‌افزار کاملاً قانونی، به خانه و محل کار ما راه پیدا می‌کنند.

امروزه بازار اپلیکیشـن‌ها به طرز چشـمگیری گسترده شده اسـت. از نرم‌افزارهای کاربردی و حرفه‌ای گرفته تا بازی‌های سـاده و ابزارهای روزمره مثل چراغ‌قوه، دیکشنری، یا ویجت آب‌وهوا؛ همه‌وهمه تنها با چند لمس ساده روی صفحه نمایش در دسترس ما قرار می‌گیرند. بسیاری از این برنامه‌ها رایگان‌اند و حتی از طریق مارکت‌های رسمی مانند Google Play یا App Store عرضه می‌شوند. این شرایط باعث شده که اعتماد به این برنامه‌ها، برای بیشـتر کاربران، امری بدیهی به نظر برسـد. اما پرسش اساسی اینجاست: آیا صرفاً به دلیل حضور یک اپلیکیشن در یک فروشگاه رسمی، می‌توانیم آن را ایمن و بی‌خطر بدانیم؟

پاسـخ، متأسفانه، منفی است. تجربه‌های چند سـال اخیر نشان داده که حتی در مارکت‌های رسمی نیز، برنامه‌هایی وجود دارند که با سوءاستفاده از اعتماد کاربر و مجوزهایی که هنگام نصب دریافت می‌کنند، به جمع‌آوری، تحلیل و انتقال داده‌های شـخصی یا سازمانی مشغول‌اند. این جمع‌آوری داده‌ها گاهی با اهداف تبلیغاتی و تجاری صورت می‌گیرد، اما در مواردی هم می‌تواند بخشـی از یک عملیات جاسوسـی هدفمند باشد.

موضوع این شماره ماهنامه، به یکی از همین تهدیدات کمتر دیده‌شده می‌پردازد: «وقتی نرم‌افزار سالم و قانونی، جاسوس می‌شود». هدف ما این است که برای شما، کارکنان سازمان، روشن کنیم که امنیت دیجیتال، تنها با شـناخت ویروس‌ها و بدافزارهای شناخته‌شـده تضمین نمی‌شود؛ بلکه باید دید خود را نسبت به هر

ابزار دیجیتال گسترش دهیم.

در نگاه اول، ممکن است باور این‌که یک اپلیکیشن چراغ‌قوه یا یک دیکشنری رایگان بتواند به اطلاعات محرمانه سازمانی شما دسترسی پیدا کند، دشوار باشد. اما واقعیت این است که همین برنامه‌های کوچک و بی‌آزارنما، با گرفتن دسترسی به موقعیت جغرافیایی، دوربین، میکروفون، یا حتی لیست تماس‌ها، می‌توانند به تدریج پروفایلی کامل از فعالیت‌های شما و حتی جزئیات کاری سازمانتان بسازند. این داده‌ها، هرچند ممکن است به‌طور مستقیم محرمانه نباشند، اما در ترکیب با سایر اطلاعات جمع‌آوری‌شده، می‌توانند تصویری دقیق از ساختار، روند کاری و حتی نقاط ضعف سازمان ارائه دهند.

به عنوان نمونه، چند سال پیش گزارش‌هایی منتشر شد که نشان می‌داد برخی اپلیکیشن‌های به ظاهر بی‌ضرر، از جمله بازی‌های ساده موبایلی، داده‌های مکانی و الگوهای رفت‌وآمد کاربران را به سرورهایی در خارج از کشور ارسال می‌کردند. این داده‌ها در نگاه اول ممکن است تنها یک مجموعه بی‌اهمیت از مختصات جغرافیایی باشند، اما با تحلیل آن‌ها می‌توان محل زندگی، مسیرهای رفت‌وآمد روزانه، و حتی الگوی حضور فرد در محل کار را شناسایی کرد. حال تصور کنید این الگوها برای یکی از کارکنان بخش حساس سازمان استخراج شود؛ نتیجه، چیزی جز یک تهدید امنیتی جدی نخواهد بود.

این ماهنامه می‌خواهد به شما نشان دهد که تهدیدات دیجیتال همیشه با چهره «آشکار» وارد نمی‌شوند. بسیاری از نرم‌افزارها، حتی آن‌هایی که روی کاغذ قانونی و تأییدشده‌اند، می‌توانند به ابزاری برای نفوذ و جاسوسی تبدیل شوند. این اتفاق نه به دلیل شکستن دیوارهای امنیتی سازمان، بلکه با ساده‌ترین و پیش‌پاافتاده‌ترین مسیر ممکن رخ می‌دهد: با کلیک روی دکمه نصب.

به همین دلیل، آگاهی در این حوزه، یک نیاز حیاتی برای هر کارمند سازمان است. شما به عنوان بخشی از یک مجموعه، نه‌تنها مسئول حفاظت از اطلاعات شخصی خود هستید، بلکه باید بدانید که هر اقدامی در فضای دیجیتال، می‌تواند بر امنیت کل سازمان اثر بگذارد. نصب یک نرم‌افزار بدون بررسی دقیق، به همان اندازه خطرناک است که بازکردن یک ایمیل مشکوک یا کلیک روی یک لینک ناشناس.

در ادامه این شماره، ما به چند محور اصلی می‌پردازیم:

- شناسایی اپلیکیشن‌های مشکوک با ظاهر ساده
- آشنایی با دسترسی‌های پرخطر و نحوه بررسی آن‌ها
- معرفی پرونده‌های واقعی جاسوسی اپلیکیشن‌ها
- راهنمای گام‌به‌گام ارزیابی یک اپلیکیشن پیش از نصب
- چک‌لیست کاربردی برای مدیریت و پاک‌سازی نرم‌افزارها
- ابزارهایی که می‌توانند دسترسی‌های غیرضروری را محدود کنند

هر کدام از این بخش‌ها، با هدف افزایش قدرت تشخیص و تصمیم‌گیری شما نوشته شده‌اند. ما نمی‌خواهیم باعث هراس یا بی‌اعتمادی بی‌پایه شویم؛ بلکه قصد داریم شما را به دیدگاهی واقع‌گرایانه و دقیق‌تر مجهز کنیم. باید به یاد داشته باشیم که در دنیای امروز، مرز میان «بدافزار» و «نرم‌افزار سالم» گاهی بسیار باریک است. ممکن است یک برنامه واقعاً بدافزار نباشد، اما داده‌هایی را جمع‌آوری کند که با ترکیب‌شدن با سایر اطلاعات، بتوانند به ابزاری برای جاسوسی یا سوءاستفاده تبدیل شوند. این همان جایی است که نقش شما به عنوان کاربر آگاه و مسئولیت‌پذیر پررنگ می‌شود.

پیامی که در این شماره تلاش می‌کنیم منتقل کنیم، این است: امنیت، یک فرآیند جمعی و پیوسته است. همان‌طور که تیم امنیت سازمان وظیفه دارد زیرساخت‌ها و شبکه‌ها را ایمن کند، شما هم به عنوان کارمند، باید از دروازه‌های ورودی که در اختیار دارید (گوشی، لپ‌تاپ، و حتی اپلیکیشن‌های کوچک) به خوبی محافظت کنید.

امید ما این است که پس از مطالعه این شماره، پیش از نصب هر برنامه‌ای، حتی ساده‌ترین و کوچک‌ترین آن‌ها، لحظه‌ای مکث کنید و از خود بپرسید: «این برنامه واقعاً به چه چیزهایی دسترسی پیدا می‌کند و چرا؟» شاید همین پرسش کوتاه، مانع از یک رخنه امنیتی بزرگ شود.

در پایان، یادآور می‌شوم که امنیت دیجیتال دیگر یک مهارت لوکس یا اختیاری نیست؛ بلکه بخشی از سواد حرفه‌ای هر فرد در دنیای امروز است. همان‌طور که یاد می‌گیریم چطور ایمیل سازمانی را مدیریت کنیم یا یک سند اداری را درست تنظیم کنیم، باید بیاموزیم که چگونه با نرم‌افزارها تعامل ایمن داشته باشیم.

در این مسیر، ماهنامه آگاهی‌رسانی سازمان، همراه و پشتیبان شما خواهد بود. با ما همراه باشید تا در کنار هم، محیطی امن‌تر و هوشمندتر برای کار و زندگی بسازیم.

MAIN ARTICLE

مقاله اصلی ...

اعتمـــاد به اپلیکیشن‌ها بی‌گناه تا اثبات خلافش؟

در دنیای دیجیتال امروز، ما به شکلی بی‌سابقه به اپلیکیشن‌ها و نرم‌افزارها وابسته شده‌ایم. تقریباً هر فعالیت روزمره، از چک‌کردن وضعیت آب‌وهوا تا پرداخت قبض یا ارتباط با همکاران، از طریق یک برنامه انجام می‌شود. این وابستگی، همراه با تصور رایج «هرچه از مارکت رسمی بیاید، امن است»، باعث شده بسیاری از کاربران بدون بررسی دقیق، هر برنامه‌ای را نصب و استفاده کنند.

اما واقعیت این اســت که مرز میان یک اپلیکیشــن مفید و یک ابزار جاسوسی بسیار باریک است. تفاوت آن‌ها گاهی فقط در نیت پنهان توسعه‌دهنده یا قراردادن چند خط کد اضافی در برنامه است. امروزه، حتی برنامه‌هایی که میلیون‌ها کاربر دارند و ظاهراً معتبرند، می‌توانند داده‌های شــخصی و حساس کاربران را جمع‌آوری کنند؛ داده‌هایی که ارزش تجاری یا حتی امنیتی بالایی دارند.

یکی از عوامل اصلی این پدیده، اقتصاد داده است. در این مدل اقتصادی، داده‌ها همان «ســوخت» و «ســرمایه» شرکت‌ها هستند. اپلیکیشــن‌های رایگان یا ارزان، هزینــه خود را نه از طریق فروش مستقیم، بلکه با فروش داده‌های کاربران جبران می‌کنند.

مســئله وقتی نگران‌کننده‌تر می‌شــود که کاربر، به‌صورت کاملاً آگاهانه یا ناآگاهانه، اجازه این دسترســی را داده باشــد. اینجاست که مفهوم «جاسوسی قانونی» مطرح می‌شود؛ یعنی برنامه‌ها در چارچوب قوانیــن، اما برخلاف انتظار و آگاهی کاربر، داده‌های او را جمع‌آوری و استفاده می‌کنند.

اپلیکیشن‌هایی با ظاهر ساده ولی نیت‌های پنهان

یکی از شگردهای همیشگی مهاجمان و حتی شرکت‌های بزرگ، عرضه برنامه‌هایی با کاربردهای روزمره و بی‌خطر به‌ظاهر اســت. این برنامه‌ها، به دلیل سادگی کارکرد، اعتماد کاربر را جلب می‌کنند، اما در پشت پرده، عملکردی کاملاً متفاوت دارند.

چراغ‌قوه‌هایی که روشنایی‌شان پرهزینه است

اپلیکیشــن چراغ‌قوه، شاید ساده‌ترین نرم‌افزاری باشد که روی گوشی نصب می‌کنیم. اما بررسی‌های امنیتی نشان داده‌اند که برخی از این اپ‌ها، علاوه بر دسترسی به فلش، مجوزهایی برای موقعیت مکانی، لیست تماس‌ها، حافظه و حتی میکروفون دریافت کرده‌اند. داده‌های جمع‌آوری‌شده گاهی به سرورهایی در کشورهای مختلف ارسال می‌شود که مقصد و هدف آن‌ها برای کاربر ناشناخته است.

ویجت‌های آب‌وهوا با ردپای دیجیتال شما

یک برنامه هواشناســی به‌طور منطقی بــه موقعیت مکانی نیاز دارد، اما وقتی همین اپ اطلاعات ســخت‌افزاری گوشــی، لیست برنامه‌های نصب‌شــده و حتی الگوی اتصال شــما بــه اینترنت را ذخیــره می‌کند، موضوع از نیاز عملیاتــی فراتر می‌رود. این داده‌ها می‌توانند برای ســاخت یک پروفایل دقیق از شما استفاده شوند که ارزش بالایی در بازار تبلیغات و حتی در ســناریوهای جاسوســی دارد.

مترجم‌های ساده با چشم و گوش باز

اپلیکیشن‌های ترجمه آنلاین، برای بسیاری از کاربران ابزاری سریع و مفید هســتند. اما وقتی این اپ‌ها هر متنی که شــما وارد می‌کنید را ذخیره و ارسال می‌کنند، حتی اسناد کاری و شخصی شما می‌توانند به پایگاه‌های داده‌ای منتقل شوند که بعداً مورد سوءاستفاده قرار می‌گیرد.

بازی‌های رایگان؛ سرگرمی یا تله؟

بازی‌هــای موبایلــی رایگان، به‌ویــژه آن‌هایی که نیــاز به اتصال دائــم به اینترنت دارند، یکی از منابع بزرگ جمع‌آوری داده هســتند. درخواست مجوز برای دسترسی به موقعیت، لیست مخاطبین یا حتی تاریخچه مرورگر، هیچ ارتباط مستقیمی با اجرای بازی ندارد، اما برای شرکت‌های تبلیغاتی بسیار ارزشمند است.

دسترسی‌هایی که باید نگران‌کننده باشند

هر اپلیکیشــن برای عملکرد خود به مجموعه‌ای از مجوزها نیاز دارد. مشکل زمانی آغاز می‌شود که این مجوزها بیش از حد لازم باشند یا ارتباطی با عملکرد برنامه نداشته باشند.

برخی مثال‌ها:

- یک اپ ویرایش عکس که دسترسی به تماس‌ها را می‌خواهد.
- یک ماشین‌حساب که به GPS شما متصل می‌شود.
- یک اپ پخش موسیقی که به میکروفون و دوربین نیاز دارد.

این دسترســی‌های غیرمنطقی، می‌تواننــد کانال‌های پنهانی برای جمــع‌آوری داده ایجاد کنند. مشــکل اینجاســت که بیشــتر کاربران به‌محض دیدن درخواســت دسترســی، بدون بررســی، روی گزینه «Allow» کلیک می‌کنند.

جاسوسی قانونی؛ وقتی کاربر خودش اجازه می‌دهد

یکــی از پیچیده‌ترین جنبه‌هــای امنیت دیجیتال، این اســت که بســیاری از اقدامات جمع‌آوری داده، به‌صــورت کاملاً قانونی انجام می‌شود. علت ساده اســت: کاربر، خود، با پذیرش شرایط استفاده یا صدور مجوز دسترسی، اجازه این کار را داده است.

اغلب کاربران، هنگام نصب برنامه، متن شــرایط و سیاست‌های حریــم خصوصی را نمی‌خوانند. این متن‌ها معمــولاً طولانی و پر از اصطلاحات حقوقی‌اند و در میان جمــلات، بندهایی وجود دارد که اجازه جمع‌آوری و اشتراک‌گذاری داده‌های شخصی را صادر می‌کند.

چرا نصب از مارکت رسمی هم همیشه ایمن نیست؟

وجود یک اپلیکیشــن در Google Play یــا App Store، به معنای امنیت مطلق نیست. هرچند این فروشگاه‌ها سیستم‌های بررسی دارند، اما تجربه نشان داده که بسیاری از برنامه‌های مخرب و جاسوسی توانسته‌اند از این فیلترها عبور کنند.

نمونه‌های واقعی

- Joker Malware: ده‌ها اپلیکیشن به ظاهر بی‌ضرر که توانایی سرقت پیامک، لیست تماس‌ها و حتی ثبت‌نام در سرویس‌های پولی بدون اطلاع کاربر را داشتند.
- برنامه‌های ویرایش تصویر محبوب: ارســال مخفیانه تصاویر و ویدئوهای کاربر به سرورهای ناشناس.
- ابزارهای هواشناسی: جمع‌آوری داده‌های مکان، شناسه دستگاه و تاریخچه مرور اینترنتی کاربران.

سناریو داستانی: «همه‌چیز از یک اپ چراغ‌قوه شروع شد...»

علی، کارمند یک شــرکت بازرگانی، برای مواقع قطعی برق در خانه به دنبال یک اپ چراغ‌قوه می‌گشت. برنامه‌ای با هزاران نصب و امتیاز بالا را از گوگل‌پلی دانلود کرد. چند روز بعد، متوجه شــد که تماس‌های مشــکوکی از تلفن او انجام شده و حساب ایمیلش مورد نفوذ قرار گرفته اســت. بررســی‌های فنی نشــان داد که اپ چراغ‌قوه، به لیست تماس‌ها، پیامک‌ها و حتی اینترنت او دسترسی داشته و داده‌ها را به سرور ناشناسی منتقل می‌کرده است.

راهکارهای پیشگیری

- پیش از نصب، نام توسعه‌دهنده را جستجو کنید.
- نقدها و نظرات کاربران را بخوانید، به‌ویژه نظرات منفی
- به دسترسی‌های درخواستی حساس باشید.
- اپ‌های بلااستفاده را حذف کنید.
- مصرف اینترنت و باتری را مانیتور کنید
- از اپ‌های مدیریت مجوز استفاده کنید.

A PRACTICAL GUIDE

••• راهنمای عملی

چطور اپلیکیشن‌ها را قبل از نصب ارزیابی کنیم؟

در دنیای امروز که بخش قابل توجهی از ارتباطات، سرگرمی و حتی امور مالی ما از طریق تلفن همراه یا تبلت انجام می‌شود، نصب اپلیکیشن‌های جدید به یک عادت روزمره تبدیل شده است. اما پشت این عادت ساده، ریسک‌های امنیتی بزرگی پنهان است. بسیاری از تهدیدات سایبری از همین مسیر وارد می‌شوند؛ یعنی کاربر با نصب یک اپ به ظاهر بی‌ضرر، در واقع به مهاجم دروازه‌ای باز می‌کند.

بررسی و ارزیابی دقیق قبل از نصب، اولین و مهم‌ترین گام در جلوگیری از این تهدیدات است. این فرآیند نه‌تنها باید برای اپلیکیشن‌های ناشناخته، بلکه حتی برای برنامه‌های موجود در فروشگاه‌های رسمی نیز انجام شود. چرا که بارها ثابت شده است که اپ‌های مخرب توانسته‌اند از فیلترهای امنیتی مارکت‌های معتبر عبور کنند.

گام اول: منبع دانلود

همیشه از مارکت‌های رسمی و شناخته‌شده مانند **Google Play** و **Apple App Store** استفاده کنید. با این حال، این به معنای امنیت مطلق نیست. حتی در مارکت‌های معتبر نیز اپ‌های مخرب مشاهده شده‌اند. نکته مهم این است که از نصب اپلیکیشن‌های موجود در سایت‌های ناشناس یا لینک‌های ارسال‌شده در شبکه‌های اجتماعی خودداری کنید. فایل‌های **APK** یا **IPA** که خارج از فروشگاه رسمی دریافت می‌شوند، بیشترین احتمال آلودگی را دارند.

گام دوم: بررسی توسعه‌دهنده

نام و سابقه توسعه‌دهنده، شاخص مهمی برای سنجش اعتبار اپلیکیشن است. توسعه‌دهندگان معتبر معمولا:

- چندین اپلیکیشن دیگر در مارکت دارند.
- وب‌سایت رسمی و فعال دارند.
- اطلاعات تماس معتبر و شفاف ارائه می‌دهند. اگر توسعه‌دهنده فقط یک اپ منتشر کرده و هیچ اطلاعات قابل‌اعتمادی از او پیدا نمی‌شود، باید با احتیاط بیشتری عمل کرد.

گام سوم: بررسی حجم و جزئیات برنامه

حجم غیرمعمول برنامه می‌تواند نشانه‌ای از مشکل باشد. برای مثال، یک اپ چراغ‌قوه با حجم ۵۰ مگابایت جای سؤال دارد. همچنین توضیحات برنامه در صفحه دانلود را بخوانید و به نکات زیر دقت کنید:

- آیا توضیحات با کارکرد اپ سازگار است؟
- آیا متن توضیح پر از غلط املایی یا ترجمه ماشینی است؟
- آیا ویژگی‌های برنامه بیش از حد گسترده و نامربوط است؟

گام چهارم: بررسی مجوزهای درخواستی

یکی از مهم‌ترین مراحل ارزیابی اپلیکیشن، توجه به دسترسی‌هایی است که برنامه در زمان نصب یا اجرای اولیه درخواست می‌کند. به این موارد دقت کنید:

- اپلیکیشن باید فقط دسترسی‌هایی را بگیرد که برای عملکردش ضروری است.
- اگر یک اپ ساده درخواست دسترسی به دوربین، میکروفون، موقعیت مکانی یا لیست تماس‌ها می‌کند، باید شک کنید.
- در سیستم‌عامل اندروید، پیش از تأیید مجوزها، آن‌ها را بررسی کنید. در iOS نیز می‌توانید بعد از نصب، دسترسی‌ها را از مسیر تنظیمات کنترل کنید.

گام پنجم: بررسی امتیاز کاربران

امتیاز بالای کاربران معمولاً نشانه خوبی است، اما همیشه کافی نیست. بعضی از توسعه‌دهندگان، امتیازهای جعلی خریداری می‌کنند. به همین دلیل باید:

- به تعداد امتیازها نگاه کنید؛ اپ با ۵ ستاره و فقط ۵ نظر، قابل اعتماد نیست.
- امتیاز متوسط (مثلاً ۳ تا ۴) همراه با نظرات واقعی، معمولاً نشانه اعتبار بیشتر است.

گام ششم: مطالعه نظرات کاربران

بخش نظرات را به دقت بخوانید، به‌خصوص نظرات منفی. گاهی کاربران گزارش می‌دهند که اپلیکیشن پس از نصب باعث کندی دستگاه، تبلیغات ناخواسته یا مصرف بیش از حد باتری شده است. این نشانه‌ها می‌تواند هشداردهنده باشد.

گام هفتم: تاریخ آخرین به‌روزرسانی

برنامه‌هایی که مدت طولانی به‌روزرسانی نشده‌اند، ممکن است دارای آسیب‌پذیری‌های امنیتی برطرف‌نشده باشند. اپلیکیشن‌های معتبر معمولاً به‌روزرسانی‌های منظم دارند تا اشکالات و باگ‌ها را اصلاح کنند.

گام هشتم: بررسی نشانه‌های ظاهری

گاهی با نگاه به آیکون برنامه یا اسکرین‌شات‌های ارائه‌شده، می‌توان متوجه غیرحرفه‌ای بودن اپ شد. آیکون‌های بی‌کیفیت، تصاویر نامرتبط یا دزدی از برنامه‌های مشهور، نشانه‌هایی از تقلبی بودن اپلیکیشن هستند.

مثال واقعی

در سال‌های اخیر، چندین اپ چراغ‌قوه در Google Play کشف شدند که علاوه بر عملکرد اصلی، اطلاعات موقعیت مکانی، لیست تماس‌ها و پیامک‌ها را به سرورهای خارجی ارسال می‌کردند. این اپ‌ها میلیون‌ها بار دانلود شده بودند، اما بررسی مجوزها و خواندن نظرات منفی می‌توانست قبل از نصب، کاربران را آگاه کند.

معیارهای انتخاب اپ سالم و نمونه‌تحلیل

پس از شناخت مراحل ارزیابی، باید معیارهای اصلی انتخاب یک اپ سالم را مشخص کنیم. این معیارها به کاربران کمک می‌کنند تا حتی بدون دانش فنی بالا، تصمیمی آگاهانه بگیرند.

معیار اول: شفافیت توسعه‌دهنده

یک اپلیکیشن سالم معمولاً:

- دارای وب‌سایت رسمی و فعال است.
- آدرس ایمیل پشتیبانی معتبر دارد.
- سیاست حریم خصوصی واضح و قابل‌دسترسی ارائه می‌کند.

معیار دوم: تناسب مجوزها با عملکرد

هیچ اپلیکیشنی نباید فراتر از نیاز واقعی خود، دسترسی دریافت کند. برای مثال:

- اپ ویرایش تصویر نباید به پیامک‌ها یا لیست تماس‌ها دسترسی داشته باشد.
- اپ پخش موسیقی نباید به موقعیت مکانی دقیق دسترسی بگیرد.

معیار سوم: سابقه و بازخورد کاربران

- اپ‌هایی که مدت زیادی در مارکت حضور دارند و امتیاز بالایی از هزاران کاربر گرفته‌اند، معمولاً امن‌تر هستند.
- بررسی چند نظر منفی، می‌تواند نشانه‌های مهمی از مشکلات امنیتی یا عملکردی را آشکار کند.

معیار چهارم: فعالیت در پس‌زمینه

اپ‌هایی که به‌طور مداوم در پس‌زمینه فعال‌اند و مصرف اینترنت یا باتری غیرعادی دارند، باید با دقت بیشتری بررسی شوند. برخی از این برنامه‌ها، حتی زمانی که کاربر از آن‌ها استفاده نمی‌کند، داده ارسال می‌کنند.

مثال تحلیلی – اپ مشکوک در مقابل اپ سالم

فرض کنید دو اپلیکیشن مدیریت فایل را بررسی می‌کنیم:

اپ مشکوک:

- حجم: ۷۰ مگابایت (غیرعادی برای یک فایل‌منیجر ساده)
- مجوزها: دسترسی کامل به اینترنت، موقعیت مکانی، دوربین، میکروفون و لیست تماس‌ها
- توسعه‌دهنده: ناشناخته، بدون وب‌سایت رسمی
- آخرین به‌روزرسانی: ۱۸ ماه قبل
- نظرات: گزارش کاربران از تبلیغات ناخواسته و کند شدن دستگاه

اپ سالم:

- حجم: ۱۵ مگابایت
- مجوزها: فقط دسترسی به حافظه داخلی (متناسب با کارکرد)
- توسعه‌دهنده: شرکت معتبر با چندین اپ دیگر در مارکت
- آخرین به‌روزرسانی: ۲ ماه قبل
- نظرات: بیشتر مثبت، گزارش عملکرد روان و بدون تبلیغات مخرب

گام پایانی: تصمیم آگاهانه

بعد از بررسی تمام موارد فوق، اگر کوچک‌ترین شکی نسبت به اپلیکیشن دارید، آن را نصب نکنید. همواره به یاد داشته باشید که پیشگیری، ساده‌تر و کم‌هزینه‌تر از مقابله با پیامدهای یک نفوذ یا سرقت داده است.

CASE STUDY

... مطالعه موردی

همه‌چی از یه اپ چراغ‌قوه شروع شد...

بخش اول – شروع ماجرا
یک روز عادی کاری در سازمان بود. علی، کارشناس واحد پشتیبانی، پشت میزش نشسته بود و مشغول بررسی ایمیل‌های صبحگاهی بود. همه چیز طبق روال پیش می‌رفت تا اینکه برق‌ها برای چند دقیقه قطع شد. وقتی برق برگشت و سیستم‌ها روشن شدند، علی متوجه شد چراغ‌قوه تلفن همراهش درست کار نمی‌کند. با خودش فکر کرد: این هم از شانس منه! همین امروز که قراره انبار رو بررسی کنم، چراغ‌قوه گوشیم خراب شد.

مثـل خیلی از ما، اولین کاری که کرد این بود که به Google Play سر زد و عبارت «Flashlight» را جست‌وجو کرد. نتیجه‌ها پر بود از انواع اپلیکیشن‌های چراغ‌قوه با لوگوهای براق و وعده‌ی نـور قوی‌تر، حالت‌های مختلف روشـنایی و حتـی ویژگی‌های هوشـمند. یکی از اپ‌ها با نام «Super Bright Pro» نظرش را جلـب کرد. آیکون زیبا و امتیاز ٤.٦ سـتاره، همراه با بیش از ۵۰۰ هزار دانلود. علی نگاه سـریعی به توضیحات انداخت، اما راستش را بخواهید خیلی دقیق نخواند. چیزی که دید فقط این بود: ساده، سـریع، بدون تبلیغات آزاردهنده. روی دکمـه «Install» زد. چند ثانیه بعد، اپ روی گوشـی نصب شد و اولین پیام ظاهر شد: برای عملکرد بهتر، لطفاً مجوزهای زیر را تأیید کنید.

لیست مجوزها طولانی بود:

- دسترسی به دوربین (برای چراغ‌قوه)
- دسترسی به موقعیت مکانی
- دسترسی به حافظه داخلی
- دسترسی به لیست تماس‌ها
- دسترسی به میکروفون

علی کمی مکث کرد. دوربین منطقی بود، چون چراغ‌قوه معمولاً با فلاش دوربین کار می‌کند. اما موقعیت مکانی؟ میکروفون؟ خودش را قانع کرد که «شاید این‌ها برای تبلیغات یا امکانات جانبی باشه، مهم نیست.» و همه مجوزها را با یک کلیک تأیید کرد. اپ به ظاهر همان‌طور که قول داده بود، ساده و سریع بود. چراغ‌قوه‌اش روشن شـد و علی خوشـحال رفت که انبار را بررسی کند. اما چیزی که نمی‌دانست این بود که همان لحظه، یک فرآیند مخفی در پس‌زمینه گوشی فعال شده بود.

چند سـاعت بعد، وقتی علی در جلسه آنلاین واحد پشتیبانی حضور داشت، اپ چراغ‌قوه با استفاده از مجوز میکروفون، صدای جلسه را ضبط می‌کرد. هم‌زمان، دسترسی به حافظه داخلی باعث شده بود که فایل‌های ذخیره‌شده در پوشه Downloads و حتی تصاویر پوشـه کاری سازمان، به یک سـرور ناشناس در خارج از کشور ارسال شود.

دو روز گذشـت و علی هیچ مشکلی متوجه نشد. حتی زمانی که متوجه شـد باتری گوشی زودتر از همیشه خالی می‌شود، فکر کرد شـاید به خاطر استفاده زیاد از چراغ‌قوه یا جلسه‌های طولانی آنلاین باشد. اما واقعیت این بود که اپلیکیشن هر روز در پس‌زمینه کار می‌کـرد، داده‌ها را جمـع‌آوری و مخفیانه ارسـال می‌کرد. نه آنتی‌ویروس سـازمان روی موبایل شخصی علی نصب بود، نه او آموزش کافی در مورد بررسی مجوزهای اپلیکیشن دیده بود.

حادثه زمانی آشکار شـد که چند سند داخلی سازمان (شامل گزارش وضعیت موجودی انبار) در یک وب‌سایت ناشناس منتشر شد. تیم امنیت سازمان شروع به بررسی کرد و متوجه شد که نقطه آغاز نشت اطلاعات، دستگاه شخصی علی بوده است.

وقتی تیم امنیتی گوشـی او را بررسی کرد، ردپای واضحی از فعالیت اپ چراغ‌قوه پیدا شد:

- اتصال‌های مکرر به یک سرور ناشناس در شرق آسیا
- ارسال فایل‌های PDF و تصاویر
- ضبـط صداهـای محیـط و ارسـال آن‌هـا در بسـته‌های رمزگذاری‌شده

علی شوکه شـده بود. او هرگز فکر نمی‌کرد یک اپ به ظاهر بی‌ضرر بتواند این همه کار مخرب انجام دهد. اما اتفاق افتاده بود.

بخش دوم – پیامدها و درس‌آموخته‌ها

بعد از کشف ماجرا، سازمان مجبور شد سریع وارد حالت بحران شود. تیم امنیتی دستور داد تمام حساب‌های کاربری علی در سامانه‌های داخلی موقتاً غیرفعال شود. همه سیستم‌ها برای بررسی آلودگی احتمالی اسکن شدند. گزارش نهایی تیم امنیتی نشان داد که خوشبختانه، داده‌های لو رفته محدود به چند سند داخلی بوده و به اطلاعات حیاتی یا داده‌های مشتریان دسترسی پیدا نکرده‌اند. اما همین میزان هم می‌توانست برای وجهه سازمان و روابطش با شرکا مشکل‌ساز باشد.

جلسه‌ای فوری با حضور مدیران واحدها برگزار شد. مدیر امنیت اطلاعات توضیح داد که این حادثه نه به دلیل هک پیشرفته یا نفوذ مستقیم، بلکه به دلیل نصب یک اپ مشکوک توسط یک کارمند اتفاق افتاده است. علی در جلسه گفت: من فقط دنبال یه چراغ‌قوه ساده بودم. اصلاً فکر نمی‌کردم همچین چیزی ممکن باشه. مدیر امنیت جواب داد: دقیقاً مشکل همین‌جاست. تهدیدهای امروز خودشون رو پشت ظاهر ساده و قانونی پنهان می‌کنن. نصب یک اپ بدون بررسی، می‌تونه به اندازه باز کردن یک ایمیل فیشینگ خطرناک باشه.

این حادثه بهانه‌ای شد تا سازمان یک برنامه جدید برای آموزش کارکنان راه‌اندازی کند. در این آموزش‌ها، به کارمندان یاد داده شد که:

۱. قبل از نصب هر اپ، حتماً مجوزهای درخواست‌شده را بررسی کنند.

۲. به حجم و ویژگی‌های غیرعادی اپ دقت کنند.

۳. حتی اپ‌های موجود در مارکت رسمی را با احتیاط نصب کنند.

۴. دستگاه شخصی که برای کار استفاده می‌شود، باید آنتی‌ویروس و سیستم مانیتورینگ فعال داشته باشد.

علی بعد از این ماجرا، گوشی‌اش را به طور کامل ریست کرد و تنها اپ‌های ضروری و رسمی را نصب نمود. تجربه تلخی بود که به او یاد داد اعتماد بی‌جا به ظاهر یک اپلیکیشن می‌تواند عواقب سنگینی داشته باشد.

درس‌آموخته‌های کلیدی از این ماجرا:

- ظاهر فریبنده است: یک آیکون زیبا یا امتیاز بالا در مارکت، تضمین امنیت نیست.
- مجوزها را جدی بگیرید: هر دسترسی اضافه باید علامت هشدار باشد.
- آموزش کارکنان حیاتی است: حتی بهترین سیستم‌های امنیتی هم نمی‌توانند جلوی خطاهای انسانی بدون آموزش را بگیرند.
- تلفن شخصی هم دروازه ورود است: اگر دستگاه شخصی برای کار استفاده می‌شود، باید همان‌قدر که به سیستم سازمانی حساس هستیم، به امنیت آن نیز توجه کنیم.

پیام پایانی:

حادثه علی نمونه‌ای کوچک از هزاران سناریوی واقعی در سراسر دنیاست. هکرها و توسعه‌دهندگان مخرب همیشه به دنبال ساده‌ترین راه برای نفوذ هستند. و چه چیزی ساده‌تر از این که قربانی خودش با دست خودش، ابزار نفوذ را نصب کند؟ امنیت سایبری فقط داشتن رمز قوی یا فایروال نیست. امنیت یعنی در هر تصمیم کوچک، از نصب یک اپ تا کلیک روی یک لینک، با آگاهی و دقت عمل کنیم.

موضوع ویژه

پرونده‌های واقعی جاسوسی اپ‌ها

در عصر اپلیکیشن‌های رایگان و پرطرفدار، ظاهر ساده یک برنامه موبایل همیشه به معنای بی‌خطر بودن آن نیست. پرونده‌های واقعی نشان می‌دهد حتی اپ‌های به ظاهر بی‌آزار – از چراغ‌قوه و هواشناسی تا پیام‌رسان – می‌توانند در پس‌زمینه داده‌های حساس کاربران را جمع‌آوری کنند. در این گزارش، پنج نمونه واقعی بررسی شده که میلیون‌ها بار نصب شدند اما به جاسوسی از موقعیت مکانی، مکالمات یا حتی فهرست اپ‌های کاربر پرداختند. از Brightest Flashlight Free که مختصات GPS را می‌فروخت، تا ToTok که ابزاری برای رصد ارتباطات بود، همه این‌ها هشداری روشن‌اند: امنیت دیجیتال فقط با بررسی دقیق مجوزها و منبع توسعه‌دهنده به دست می‌آید، نه با اعتماد به ظاهر یا تعداد دانلود.

بخش اول – سه پرونده واقعی جاسوسی اپ‌ها

پرونده ۱
نرم‌افزار Brightest Flashlight Free - اندروید، ۲۰۱۳

در نگاه اول، این اپ فقط یک چراغ‌قوه ساده برای گوشی‌های اندرویدی بود. میلیون‌ها کاربر در سراسر جهان آن را نصب کردند، چون سبک، رایگان و با رابط کاربری ساده عرضه شده بود. اما تحقیقات کمیسیون فدرال تجارت آمریکا نشان داد که این اپ در پس‌زمینه، موقعیت مکانی دقیق کاربران را جمع‌آوری و به شرکت‌های تبلیغاتی شخص ثالث ارسال می‌کند – آن هم بدون رضایت واقعی کاربر.

شیوه کشف

یک محقق امنیتی هنگام بررسی مصرف داده اینترنتی غیرعادی متوجه شد که اپ در زمان‌هایی که اصلاً استفاده نمی‌شود، همچنان اطلاعات به سرورهای ناشناس ارسال می‌کند. پس از بررسی بسته‌های داده، مشخص شد که مختصات GPS کاربران و شناسه دستگاه به آدرس‌های متعلق به یک شرکت تبلیغاتی ارسال می‌شود.

پیامدها

FTC سازنده اپ را ملزم کرد که سیاست حفظ حریم خصوصی خود را اصلاح کند و قبل از جمع‌آوری اطلاعات، رضایت صریح کاربران را بگیرد. اپ از گوگل پلی حذف شد، اما تا قبل از آن بیش از ۵۰ میلیون نصب داشت.

درس‌آموخته‌ها

- اپ‌های بسیار ساده که دسترسی‌های غیرضروری می‌خواهند، باید زنگ خطر باشند.
- بررسی مصرف داده‌های پس‌زمینه می‌تواند رفتار مخرب را آشکار کند.
- حتی اپ‌های پرنصب و محبوب هم می‌توانند جاسوسی کنند.

پرونده ۲
نرم‌افزار ToTok - اندروید و iOS، ۲۰۱۹

ToTok یک پیام‌رسان رایگان بود که در کشورهای مختلف، به‌خصوص در امارات متحده عربی، محبوبیت زیادی پیدا کرد. رسانه‌ها اعلام کردند این اپ در واقع ابزاری برای جاسوسی دولتی بوده که تماس‌ها، پیام‌ها، موقعیت مکانی و حتی ارتباطات تصویری کاربران را رصد می‌کرده است.

شیوه کشف

تحقیقات نیویورک تایمز و کارشناسان امنیتی نشان داد که ToTok داده‌ها را به یک شرکت مرتبط با دولت امارات ارسال می‌کند. بررسی‌های ترافیک شبکه ثابت کرد که اپ تقریباً به همه داده‌های کاربر دسترسی دارد و آن‌ها را به‌طور رمزگذاری‌شده به سرورهایی در امارات می‌فرستد.

پیامدها

اپلیکیشن ابتدا از هر دو مارکت گوگل پلی و اپ استور حذف شد. کاربران زیادی شوکه شدند چون این اپ در تبلیغاتش خود را جایگزین «ایمن و سریع» برای واتساپ و اسکایپ معرفی می‌کرد.

درس‌آموخته‌ها

- اپ‌های ارتباطی ناشناخته، حتی اگر سریع و راحت باشند، می‌توانند کانال جاسوسی گسترده باشند.
- منبع و مالکیت توسعه‌دهنده اپ باید پیش از نصب بررسی شود.
- تبلیغات «امنیت بالا» بدون شفافیت فنی، کافی نیستند.

پرونده ۳
نرم‌افزارهای Weather Forecast و Weather-10Days - اندروید، ۲۰۱۸

این دو اپ هواشناسی ظاهراً بی‌خطر، توسط میلیون‌ها کاربر نصب شده بودند. اما مشخص شد که آن‌ها داده‌های مکانی و شناسه‌های دستگاه را جمع‌آوری و به یک شبکه تبلیغاتی در

چین ارسال می‌کنند.

شیوه کشف

محققـان امنیتی شـرکت Upstream هنـگام مانیتورینگ ترافیک موبایل در برخی کشورها متوجه شدند که این اپ‌ها در پس‌زمینه درخواست‌های HTTP به دامنه‌های مشکوک ارسال می‌کنند. بررسی بیشتر نشان داد که اپ‌ها حتی زمانی که کاربر از آن‌ها استفاده نمی‌کند، همچنان داده جمع‌آوری و ارسال می‌کنند.

پیامدها

گـوگل این اپ‌هـا را به دلیـل نقض سیاسـت‌های حریم خصوصی از پلی اسـتور حذف کرد. اما تـا آن زمان، داده‌های میلیون‌ها کاربر جمع‌آوری شده بود.

درس‌آموخته‌ها

- اپ‌های هواشناسـی و مشابه آن که به موقعیت مکانی نیاز دارند، باید فقط در زمان استفاده فعال باشند.
- ارسـال مداوم داده به سـرورهای ناشـناس نشانه فعالیت مشکوک است.
- مجوز «Location» همیشه باید با احتیاط داده شود.

این سـه پرونده نشـان می‌دهند که حتی اپ‌های ساده مثل چراغ‌قوه یا هواشناسـی می‌توانند ابزار جاسوسی باشند. کشف این فعالیت‌ها معمولاً با تحلیل مصرف داده یا بررسـی رفتار اپ در پس‌زمینه انجام می‌شود. مهم‌ترین پیام این است که اعتماد به ظاهر اپلیکیشن و تعداد دانلودها، تضمین امنیت نیست.

بخش دوم – دو پرونده دیگر و نکات پیشگیرانه

پرونده ۴
نرم‌افزار CamScanner - اندروید، ۲۰۱۹

CamScanner یک اپ بسـیار معروف اسـکن سند بود که میلیون‌ها کاربر داشـت. نسـخه رایگان آن در گوگل پلی به مدت سـال‌ها بدون مشـکل فعالیت می‌کرد. اما در سال ۲۰۱۹، محققان شرکت Kaspersky کشف کردند که نسخه‌های اخیر اپ حاوی ماژول تبلیغاتی مخربـی به نـام Trojan-Dropper بودند که می‌توانست بدافزارهای دیگر را روی دستگاه نصب کند.

شیوه کشف

کاربران در انجمن‌های آنلاین گزارش کردند که اپ رفتاری غیرعـادی دارد و تبلیغات پاپ‌آپ ناخواسـته نمایش می‌دهد. بررسی فنی نشان داد که کد مخرب در قالب یک SDK شخص ثالث به اپ اضافه شده است.

پیامدها

گـوگل اپ را موقتـاً از پلی اسـتور حذف کرد تا نسـخه پاک‌سازی‌شده منتشر شود. بسیاری از کاربران بی‌اعتماد شدند و به دنبال جایگزین‌های دیگر رفتند.

درس‌آموخته‌ها

- حتی اپ‌های مشهور هم ممکن است با آپدیت‌های جدید ناامن شوند.
- نصب آپدیت‌ها بدون بررسـی تغییـرات می‌تواند خطرناک باشد.
- توسـعه‌دهندگان بایـد از امنیـت کدهای شـخص ثالث اطمینان حاصل کنند.

پرونده ۵
اپ‌های بازی کودکان با جاسوسی تبلیغاتی - اندروید، ۲۰۲۰

در اوایل ۲۰۲۰، شرکت امنیتی Check Point کشف کرد که بیش از ۵۶ اپ بازی کودکانه در پلی اسـتور حاوی کدهای تبلیغاتـی مخربی هسـتند که علاوه بر نمایـش آگهی، داده‌های حسـاس کاربر (از جمله لیسـت اپ‌ها و موقعیـت مکانی) را جمع‌آوری می‌کردند.

شیوه کشف

ایـن شـرکت با اسـتفاده از ابزارهـای تحلیل اسـتاتیک و داینامیـک، ترافیک شـبکه این اپ‌ها را بررسـی کرد و متوجه شـد که آن‌ها اطلاعات را به دامنه‌های متعلق به شبکه تبلیغاتی غیرقانونی ارسال می‌کنند.

پیامدها

گوگل تمام این اپ‌ها را حذف کرد و توسعه‌دهندگان آن‌ها را برای همیشه از انتشار اپ در پلی استور محروم نمود.

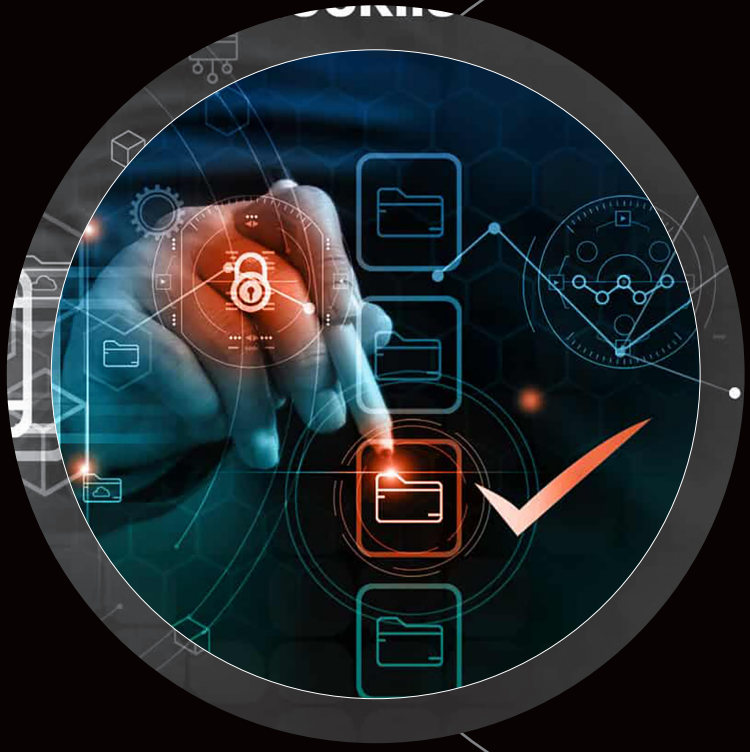
درس‌آموخته‌ها

- بازی‌هـای رایگان مخصـوص کـودکان می‌توانند هدف مناسبی برای جاسوسی باشند.
- والدیـن باید قبل از نصب هر اپ، آن را به دقت بررسـی کنند.
- نظـارت بر رفتار شـبکه اپ‌هـا حتی پـس از نصب نیز ضروری است.

نکات پیشگیرانه برگرفته از همه پرونده‌ها

۱. بررسـی مجوزها قبل از نصب: هر دسترسی غیرمرتبط با عملکرد اصلی اپ باید علامت هشدار باشد.
۲. شناخت توسـعه‌دهنده: جست‌وجو درباره تیم یا شرکت سازنده اپ قبل از نصب، ضروری است.
۳. مانیتورینـگ مصـرف دیتا و باتـری: افزایـش ناگهانی مصرف، نشانه فعالیت پنهان است.
۴. به‌روزرسـانی آگاهانه: همیشه قبل از نصب نسخه جدید، تغییرات را مطالعه کنید.
۵. اسـتفاده از ابزارهای امنیتی: اپلیکیشـن‌های امنیتی معتبر می‌توانند رفتار مشکوک اپ‌ها را شناسایی کنند.

CHECKLIST



چک‌لیست ...

مدیریت و پاک‌سازی اپلیکیشن‌ها

در دنیای امروز، گوشی هوشمند و لپ‌تاپ ما پر از اپلیکیشن‌هایی است که شاید فقط یک‌بار نصبشان کرده‌ایم و دیگر هرگز استفاده نکرده‌ایم. این اپ‌ها نه‌تنها فضای ذخیره‌سازی را اشغال می‌کنند، بلکه ممکن است در پس‌زمینه فعال باشند، منابع سیستم را مصرف کنند و حتی اطلاعات ما را بدون اطلاعمان ارسال کنند.

مدیریت و پاک‌سازی منظم اپلیکیشن‌ها یکی از مهم‌ترین اقدامات برای حفظ امنیت و حریم خصوصی است. این چک‌لیست، راهنمای گام‌به‌گام شما برای انجام این کار به شکل ایمن و مؤثر است.

۱. شناسایی و حذف اپ‌های بلااستفاده

- مرور فهرست اپ‌ها: ماهی یک‌بار به فهرست برنامه‌های نصب‌شده مراجعه کنید. هر اپی که در ۳۰ روز گذشته استفاده نکرده‌اید، در اولویت حذف است.
- سؤال کلیدی: آیا واقعاً به این اپ نیاز دارم؟ اگر جواب منفی است، آن را حذف کنید.
- چرا مهم است؟ اپ‌های بلااستفاده می‌توانند به‌روزرسانی‌های ناخواسته بگیرند و مجوزهایی را حفظ کنند که همچنان فعال باقی می‌مانند.

۲. بررسی و مدیریت مجوزها

- ورود به بخش تنظیمات مجوز در گوشی یا کامپیوتر و مرور مجوزهای هر اپ.
- دسترسی‌های پرخطر که باید محدود شوند:
  - موقعیت مکانی
  - دوربین
  - میکروفون
  - دسترسی به مخاطبین
  - دسترسی به پیام‌ها و تماس‌ها
- اصل حداقل دسترسی: فقط مجوزهایی را بدهید که برای عملکرد اصلی اپ لازم است.

۳. کنترل مصرف اینترنت (داده)

- مانیتورینگ مصرف داده: از بخش **Data Usage** یا ابزارهای مانیتورینگ استفاده کنید تا ببینید هر اپ چه میزان اینترنت مصرف می‌کند.
- علامت هشدار: مصرف بالای داده برای اپی که به اینترنت نیازی ندارد، نشانه فعالیت مشکوک است.
- اقدام اصلاحی: محدودکردن دسترسی به اینترنت در پس‌زمینه برای اپ‌های غیرضروری.

۴. کنترل مصرف باتری

- مشاهده آمار مصرف باتری در بخش **Battery Usage**.
- نشانه‌های خطر: اپی که در حالت بیکار، باتری زیادی مصرف می‌کند، ممکن است در حال انجام فعالیت پنهان باشد.
- راهکار: محدودکردن فعالیت در پس‌زمینه یا حذف اپ.

۵. استفاده از ابزارهای مدیریت مجوز

- اپلیکیشن‌های کمکی: استفاده از اپ‌های معتبر مانند «**Bouncer**» یا قابلیت‌های داخلی اندروید و **iOS** برای دادن مجوز موقت به اپ‌ها.
- مزیت: مجوزها پس از مدتی به‌صورت خودکار لغو می‌شوند و خطر سوءاستفاده کاهش می‌یابد.

۶. به‌روزرسانی آگاهانه

- اصل طلایی: همیشه قبل از نصب به‌روزرسانی، توضیحات تغییرات (**Change Log**) را بخوانید.
- خطر: برخی بدافزارها پس از به‌روزرسانی وارد اپ می‌شوند، حتی اگر نسخه اولیه سالم بوده باشد.

۷. حذف اپ‌های تبلیغ‌محور

- نشانه‌ها: نمایش پاپ‌آپ‌های ناخواسته، بازشدن خودکار مرورگر یا کاهش ناگهانی سرعت دستگاه.
- چرا حذف کنیم؟ این اپ‌ها ممکن است داده‌های شما را برای اهداف تبلیغاتی یا بدتر، به سرورهای ناشناس ارسال کنند.

۸. مانیتورینگ پس از نصب

- دوره آزمایشی: پس از نصب هر اپ جدید، مصرف باتری و داده آن را طی یک هفته زیر نظر بگیرید.
- واکنش سریع: اگر فعالیت غیرعادی مشاهده کردید، فوراً اپ را حذف کنید.

۹. پاک‌سازی کامل

- پس از حذف اپ: حافظه کش و فایل‌های باقیمانده آن را هم پاک کنید. برخی اپ‌ها حتی بعد از حذف، فایل‌هایی روی دستگاه باقی می‌گذارند.
- ابزارهای پاک‌سازی: استفاده از ابزارهای داخلی سیستم یا اپ‌های معتبر مدیریت فایل.

۱۰. بازبینی دوره‌ای

- زمان‌بندی پیشنهادی: هر سه ماه یک‌بار بازبینی کامل اپ‌ها و مجوزها.
- مزیت: کاهش احتمال سوءاستفاده طولانی‌مدت از مجوزهای داده‌شده.

پیام پایانی

مدیریت اپلیکیشن‌ها یک کار یک‌باره نیست، بلکه باید به یک عادت امنیتی تبدیل شود. اپ‌های بلااستفاده را حذف کنید، مجوزها را محدود کنید و همیشه حواستان به رفتار برنامه‌ها باشد. در نهایت، به یاد داشته باشید که هر کلیک و هر مجوزی که می‌دهید، می‌تواند دروازه‌ای به اطلاعات شخصی و سازمانی شما باز کند.

Manage and clean up applications

TOOLS

معرفی ابزار

اپلیکیشن‌ها و قابلیت‌هایی برای محدودکردن دسترسی‌ها

یکی از مهم‌ترین گام‌ها در حفظ امنیت دیجیتال و حریم خصوصی، مدیریت مجوزهایی است که به اپلیکیشن‌ها می‌دهیم. بسیاری از کاربران، هنگام نصب یک اپ، بدون مطالعه، همه دسترسی‌های درخواستی را تأیید می‌کنند. نتیجه این رفتار، باز گذاشتن درهای اطلاعاتی به روی برنامه‌هایی است که شاید به ظاهر سالم باشند، اما می‌توانند از داده‌های شخصی و حتی سازمانی ما سوءاستفاده کنند. خوشبختانه، ابزارها و قابلیت‌هایی وجود دارند که به ما کمک می‌کنند این دسترسی‌ها را کنترل، محدود یا حتی به‌صورت موقت فعال کنیم. در این بخش، ۴ تا ۵ ابزار و قابلیت کاربردی را معرفی می‌کنیم.

۱. Bouncer – مدیریت موقت مجوزها (اندروید)

عملکرد: Bouncer یک اپلیکیشن اندرویدی است که امکان می‌دهد مجوزهایی مانند دسترسی به موقعیت مکانی یا دوربین را فقط برای مدت کوتاهی فعال کنید. به عنوان مثال، اگر می‌خواهید در یک اپ تاکسی اینترنتی آدرس خود را وارد کنید، می‌توانید دسترسی به لوکیشن را تنها برای همان لحظه فعال کنید. Bouncer بعد از چند دقیقه یا بلافاصله پس از خروج از اپ، مجوز را به‌طور خودکار لغو می‌کند.

مزایا:

- جلوگیری از سوءاستفاده طولانی‌مدت اپ‌ها از مجوزها
- حذف نیاز به یادآوری برای لغو دستی مجوزها
- کارکرد ساده و قابل فهم برای کاربران عادی

محدودیت‌ها:

- فقط برای اندروید در دسترس است
- برخی اپ‌ها ممکن است بدون دسترسی دائمی عملکرد ناقصی داشته باشند

۲. Access Dots – هشدار تصویری فعال بودن دوربین یا میکروفون (اندروید)

عملکرد: این اپلیکیشن با الهام از قابلیت iOS، هر زمان که دوربین یا میکروفون گوشی فعال شود، یک نقطه کوچک رنگی روی صفحه‌نمایش نشان می‌دهد (نقطه سبز برای دوربین، نقطه نارنجی برای میکروفون). این علامت‌ها به شما اطلاع می‌دهند که کدام اپ در حال استفاده از این سخت‌افزارهاست.

مزایا:

- شناسایی فوری اپ‌های مشکوکی که بدون اطلاع کاربر از دوربین یا میکروفون استفاده می‌کنند
- کارکرد ساده و بدون نیاز به تنظیمات پیچیده
- قابل شخصی‌سازی رنگ و مکان نمایش نقطه

محدودیت‌ها:

- فقط هشدار می‌دهد و مانع استفاده نمی‌شود
- ممکن است با برخی رابط‌های کاربری اندروید تداخل ظاهری ایجاد کند

۳. Privacy Dashboard داشبورد حریم خصوصی (اندروید ۱۲ به بعد)

عملکرد: این قابلیت که به‌صورت پیش‌فرض در نسخه‌های جدید اندروید وجود دارد، گزارش کاملی از اینکه چه اپلیکیشن‌هایی در ۲۴ ساعت گذشته به دوربین، میکروفون یا لوکیشن شما دسترسی داشته‌اند، ارائه می‌دهد. علاوه بر آن، می‌توانید از همین بخش، مجوزها را لغو یا محدود کنید.

مزایا:

- بدون نیاز به نصب اپ جداگانه
- ارائه تاریخچه استفاده از مجوزها
- رابط کاربری ساده و رسمی

محدودیت‌ها:

- فقط در اندروید ۱۲ و بالاتر موجود است
- فاقد امکان مجوز موقت خودکار

۴. App Privacy Report گزارش حریم خصوصی (iOS)

عملکرد: مشابه Privacy Dashboard در اندروید، این قابلیت در iOS گزارش می‌دهد که چه اپ‌هایی در بازه زمانی اخیر از دسترسی‌ها استفاده کرده‌اند و حتی به چه وب‌سایت‌هایی داده ارسال کرده‌اند.

مزایا:

- شفافیت کامل در مورد رفتار اپ‌ها
- مشاهده ارتباطات شبکه‌ای اپلیکیشن‌ها
- بدون نیاز به نصب اپ اضافی

محدودیت‌ها:

- فقط برای کاربران iOS در نسخه‌های جدید در دسترس است
- صرفاً گزارش‌دهنده است و جلوی دسترسی را به‌طور مستقیم نمی‌گیرد

۵. Permission Manager مدیریت مجوزها (اندروید و iOS)

عملکرد: این قابلیت داخلی در بیشتر گوشی‌ها وجود دارد و از طریق آن می‌توان به‌صورت دستی، مجوز هر اپلیکیشن را مشاهده، تغییر یا لغو کرد. برای مثال، می‌توانید دوربین را فقط برای اپ تماس تصویری فعال نگه دارید و برای بقیه اپ‌ها غیرفعال کنید.

مزایا:

- بدون نیاز به نصب نرم‌افزار اضافی
- کنترل کامل روی هر اپ و هر نوع مجوز
- امکان مسدودسازی کامل یک دسترسی برای یک اپ خاص

محدودیت‌ها:

- نیاز به بررسی و تغییرات دستی دارد (فرآیند زمان‌بر)
- برخی کاربران ممکن است به دلیل آشنا نبودن با اصطلاحات فنی، تنظیمات اشتباه انجام دهند

جمع‌بندی

با استفاده از این ابزارها و قابلیت‌ها، می‌توان کنترل بیشتری روی دسترسی‌های اپلیکیشن‌ها داشت و خطرات احتمالی را کاهش داد. توصیه می‌شود کاربران سازمانی:

- از قابلیت‌های داخلی سیستم‌عامل به‌عنوان خط اول دفاع استفاده کنند
- برای افزایش امنیت، ابزارهایی مثل Bouncer و Access Dots را نصب کنند
- به‌صورت دوره‌ای گزارش‌های حریم خصوصی را بررسی و مجوزهای غیرضروری را لغو کنند

SCENARIO

سناریو ...

دستیار دیجیتال من، چشم و گوش دیگران

شروع آرام یک روز شلوغ

شاهین، کارشناس منابع انسانی یک سازمان بزرگ، صبح یکشنبه پشت میز کارش نشست. لیست جلسات هفتگی روی صفحه مانیتورش باز بود و کارهای روز، از مصاحبه با داوطلبان گرفته تا بررسی پرونده‌های پرسنلی، منتظر او بودند. چند هفته قبل، او یک نرم‌افزار سازمانی جدید روی لپ‌تاپش نصب کرده بود؛ یک «دستیار دیجیتال» رسمی که از طرف مدیریت معرفی شده بود تا کارها را راحت‌تر کند:

- هماهنگ‌کردن جلسات
- ثبت خودکار صورتجلسه‌ها
- جستجوی سریع در اسناد
- ارسال یادآوری‌ها

نرم‌افزار توسط یک شرکت معتبر داخلی طراحی شده بود، لوگوی رسمی سازمان در صفحه ورودش دیده می‌شد و حتی واحد فناوری اطلاعات، لینک دانلود آن را در پرتال داخلی قرار داده بود. همه‌چیز به ظاهر امن و بی‌دغدغه بود.

ویژگی «هوشمند» که همه دوست داشتند

مریم و همکارانش بیشتر از همه از قابلیت جدید «تشخیص گفتار» این برنامه خوششان می‌آمد. کافی بود جلسه را شروع کنند، نرم‌افزار به‌طور خودکار صدای حاضران را ضبط و به متن تبدیل می‌کرد. این متن بعداً در قالب فایل صورتجلسه برای همه ارسال می‌شد. هیچ‌کس حتی یک لحظه هم به این فکر نکرد که این حجم از داده صوتی، می‌تواند فراتر از سازمان برود. چون برنامه، از دید همه، بخشی از زیرساخت داخلی سازمان بود و شرکتی که آن را ساخته بود، سابقه خوبی داشت.

اتفاقی که همه‌چیز را تغییر داد

یک روز، جلسه محرمانه‌ای با موضوع «تغییرات ساختاری و تعدیل نیرو» برگزار شد. مدیرعامل، مدیران بخش‌ها و مریم، به‌عنوان مسئول ثبت صورتجلسه، حضور داشتند. طبق عادت، مریم نرم‌افزار دستیار دیجیتال را فعال کرد تا صحبت‌ها را ضبط کند.

جلسه پر از بحث‌های حساس بود:

- فهرست نام کارکنانی که در معرض تعدیل هستند
- برنامه تغییرات حقوق
- مذاکرات با یک شرکت رقیب برای ادغام

بعد از جلسه، همه‌چیز طبق روال پیش رفت... تا دو هفته بعد.

نشانه‌های اولین نشت

یکی از کارکنان که نامش در فهرست تعدیل بود، قبل از اعلام رسمی، از موضوع باخبر شد. او به همکارانش گفت که «یک منبع موثق» این اطلاعات را به او داده است. کمی بعد، خبر ادغام احتمالی با رقیب، به گوش همان رقیب رسید! مدیریت شوکه شد. این اطلاعات تنها در یک جلسه خصوصی مطرح شده بود. فرضیه‌ی «جاسوسی داخلی» مطرح شد، ولی شواهدی نبود که کسی عمداً اطلاعات را لو داده باشد.

سرنخ پنهان

واحد امنیت سازمان تصمیم گرفت لاگ‌های سرور و سیستم‌ها را بررسی کند. در این بررسی، متوجه شدند نرم‌افزار دستیار دیجیتال، علاوه بر ذخیره‌سازی فایل صوتی روی سرور داخلی، نسخه‌ای رمزگذاری‌شده را هم به یک دامنه خارجی ارسال کرده است. دامنه متعلق به زیرپیمانکاری بود که در قراردادش، وظیفه «پشتیبانی فنی و بهبود عملکرد نرم‌افزار» ذکر شده بود. ظاهراً این انتقال داده، برای «آموزش مدل تشخیص گفتار» استفاده می‌شد. از نظر فنی، این کار خلاف قوانین مالکیت داده‌ها نبود، چون در متن مجوز نصب نرم‌افزار، بندی وجود داشت که کاربر با ارسال داده‌های صوتی برای بهبود خدمات موافقت کرده بود!

جاسوسی قانونی

اینجا بود که همه فهمیدند «جاسوسی» لزوماً با هک و نفوذ و بدافزار انجام نمی‌شود. این یک نرم‌افزار قانونی، با مجوز رسمی و نصب‌شده از منبع داخلی بود، اما داده‌ها را برای استفاده خود به خارج از سازمان ارسال می‌کرد. بدتر از همه این بود که هیچ‌کس متن کامل شرایط استفاده را نخوانده بود. از نظر حقوقی، شرکت توسعه‌دهنده تخلفی مرتکب نشده بود؛ اما از نظر امنیت سازمانی، فاجعه رخ داده بود.

بحران اعتماد

مدیرعامل جلسه‌ای فوری با واحد فناوری اطلاعات، حقوقی و امنیت برگزار کرد. پرسش اصلی این بود: چطور یک نرم‌افزار به ظاهر بی‌ضرر توانست اطلاعات حساس‌ترین جلسه سازمان را به بیرون ببرد؟ پاسخ ساده و در عین حال تلخ بود: چون ما بدون بررسی دقیق مجوزها و رفتار نرم‌افزار، آن را به بخشی از کار روزمره‌مان تبدیل کرده بودیم.

اقدامات فوری

سازمان بلافاصله:

- استفاده از نرم‌افزار را متوقف کرد
- کلیه داده‌های صوتی و متنی ذخیره‌شده روی سرورهای آن را حذف کرد
- در قراردادهای بعدی، بندهای دقیق‌تری درباره مالکیت داده‌ها و ممنوعیت ارسال به خارج اضافه کرد
- آموزش اجباری «ارزیابی امنیت نرم‌افزار» را برای همه کارکنان اجرا کرد

پیام داستان

این اتفاق به همه نشان داد که «نرم‌افزار سالم و قانونی» هم می‌تواند ناخواسته به ابزار جاسوسی تبدیل شود، اگر:

- دسترسی گسترده‌ای داشته باشد (میکروفون، دوربین، فایل‌ها)
- داده‌ها را خارج از کنترل سازمان ارسال کند
- کاربران بدون خواندن مجوزها، آن را نصب و استفاده کنند

KNOWLEDGE TEST

••• آزمون دانشی

نرم‌افزارهای سالم با نیت‌های پنهان

راهنما: برای هر سؤال یکی از گزینه‌ها را انتخاب کنید.
پاسخ‌ها و تفسیر در پایین صفحه آمده است.

» کدام مورد می‌تواند نشانه‌ای از رفتار مشکوک یک اپلیکیشن به ظاهر سالم باشد؟

A. حجم کم و سرعت اجرای بالا
B. درخواست دسترسی به میکروفون بدون دلیل واضح
C. طراحی ساده و کاربرپسند
D. دریافت امتیاز بالا در مارکت رسمی

» اگر یک اپ چراغ‌قوه درخواست دسترسی به موقعیت مکانی شما را دارد، بهترین اقدام چیست؟

A. نادیده گرفتن چون همه اپ‌ها این دسترسی را می‌خواهند
B. دادن دسترسی چون به عملکرد اپ آسیب نمی‌زند
C. بررسی دلیل درخواست و در صورت بی‌ارتباط بودن، حذف یا جایگزینی اپ
D. فعال کردن همه مجوزها برای راحتی استفاده

» وجود یک اپ در Google Play یا App Store یعنی:

A. صد درصد امن است
B. احتمالاً امن‌تر از منابع ناشناس است، اما باز هم باید بررسی شود
C. توسط گوگل یا اپل به‌طور کامل از نظر امنیتی تحلیل شده
D. هیچ خطری ندارد

» کدام رفتار می‌تواند «جاسوسی قانونی» محسوب شود؟

A. ارسال داده‌های صوتی به سرور توسعه‌دهنده با رضایت کاربر در شرایط استفاده
B. نصب بدافزار توسط هکر ناشناس
C. نفوذ غیرمجاز به ایمیل سازمانی
D. حمله فیشینگ از طریق ایمیل جعلی

» اولین اقدام پیش از نصب یک اپ جدید باید چیست؟

A. دیدن اسکرین‌شات‌های برنامه
B. خواندن نظرات کاربران و بررسی مجوزها
C. امتحان کردن سریع برای فهمیدن عملکرد
D. نصب و سپس حذف در صورت مشکل

» اگر بعد از نصب یک اپ، مصرف باتری یا اینترنت دستگاه به‌طور غیرعادی بالا رفت، چه باید کرد؟

A. بی‌توجهی چون طبیعی است
B. بررسی تنظیمات و مجوزها و در صورت نیاز حذف اپ
C. خاموش کردن دستگاه برای چند ساعت
D. نصب اپ‌های بیشتر برای مدیریت مصرف

» کدام گزینه بهترین تعریف از «اپ جعلی» است؟

A. اپی که نسخه قانونی دارد اما ظاهر آن تغییر کرده
B. اپی که عمداً برای تقلید از یک اپ معتبر ساخته شده تا کاربران را فریب دهد
C. اپی که در دو مارکت مختلف وجود دارد
D. اپی که به‌روزرسانی نشده

» کدام یک از این اقدامات می‌تواند به کاهش خطر جاسوسی اپ‌ها کمک کند؟

A. حذف اپ‌های بلااستفاده
B. بررسی دوره‌ای مجوزها
C. نصب اپ‌ها فقط از منابع معتبر
D. همه موارد بالا

» پاسخ‌ها و تفسیر:

سوال ۱: B) درخواست دسترسی بی‌ارتباط می‌تواند نشانه سوءاستفاده باشد.
سوال ۲: C) فقط دسترسی‌های مرتبط را بدهید و اپ‌های مشکوک را جایگزین کنید
سوال ۳: B) وجود در مارکت رسمی، امنیت را تضمین نمی‌کند؛ همچنان باید ارزیابی شود.
سوال ٤: A) برخی نرم‌افزارها با موافقت شما داده‌ها را منتقل می‌کنند؛ این «قانونی» است ولی خطرناک.
سوال ٥: B) بررسی نظرات، امتیاز و مجوزها پیش از نصب ضروری است.
سوال ٦: B) مصرف غیرعادی می‌تواند نشانه فعالیت مخفی اپ باشد.
سوال ۷: B) اپ جعلی نسخه‌ای فریبنده از یک اپ معتبر است که معمولاً برای سرقت داده ساخته می‌شود.
سوال ۸: D) ترکیب این اقدامات بیشترین تأثیر را دارد.

جمع‌بندی و پیام پایانی

در این شماره از ماهنامه آگاهی‌رسانی امنیتی، تلاش کردیم به یکی از مهم‌ترین و در عین حال کمتر مورد توجه قرار گرفته‌ترین تهدیدات دنیای دیجیتال بپردازیم: نرم‌افزارهایی که در ظاهر سالم، قانونی و حتی محبوب هستند، اما می‌توانند در نقش یک ابزار جاسوسی، اطلاعات ارزشمند ما و سازمان را به خطر بیندازند.

آنچه از پرونده‌ها و مثال‌های مطرح‌شده آموختیم، این است که تهدیدات همیشه در قالب بدافزارهای شناخته‌شده یا حملات سایبری آشکار ظاهر نمی‌شوند. گاهی تنها با نصب یک اپ ساده، در اطلاعات شخصی و کاری خود را به روی مهاجمان باز می‌کنیم، آن هم بدون اینکه حتی متوجه شویم.

در این مسیر، سه اصل کلیدی را باید همیشه به خاطر داشت:

- ارزیابی قبل از اعتماد: هر اپلیکیشنی، صرف‌نظر از منبع دانلود، باید پیش از نصب بررسی شود؛ از مجوزهای درخواستی گرفته تا هویت توسعه‌دهنده.
- مدیریت مداوم دسترسی‌ها: اپ‌ها را پس از نصب رها نکنید. به‌طور دوره‌ای مجوزها را بررسی و محدود کنید، و هر برنامه بلااستفاده را حذف کنید.
- مسئولیت‌پذیری فردی: هر کاربر، بخشی از زنجیره امنیت سازمان است. بی‌توجهی یک نفر می‌تواند آسیب‌های جبران‌ناپذیری ایجاد کند.

در نهایت، امنیت دیجیتال سازمان یک وظیفه جمعی است، اما نقطه آغاز آن از هر فرد شروع می‌شود. انتخاب آگاهانه، دقت در نصب و استفاده از نرم‌افزارها، و به‌روز ماندن در برابر روش‌های جدید نفوذ، نه‌تنها شما را در برابر تهدیدات محافظت می‌کند، بلکه سد محکمی برای دفاع از کل سازمان خواهد بود.

یادمان باشد: در دنیای امروز، هر کلیک می‌تواند تفاوت بین امنیت و آسیب باشد. با دقت و آگاهی، این تفاوت را به نفع خود و سازمان رقم بزنیم.