کد خبر: ۱۰۰۶۳۵۴
دوشنبه ۶ خرداد ۱۳۹۸ ۱۲:۴۴

فناوری های مراقبتی منازل، حریم خصوصی را نقض می کنند

دوربین های مداربسته ، جاسوس یا محافظ؟

دوربین های مراقبتی منازل و دستیارهای هوشمند از جمله تحولات جدید عرصه تکنولوژی هستند که می توانند به راحتی اطلاعات کاربران را در اختیار شرکت های ارائه دهنده خدمات قرار داده و یا هکرها با نفوذ به این سیستم ها از این داده ها استفاده کنند که این امر تهدیدی بزرگ در زمینه نقض حریم خصوصی به شمار می رود.

به گزارش گروه علم و فناوری ایسکانیوز، روزنامه انگلیسی تلگراف با انتشار گزارشی اعلام کرد تکنولوژی های هوشمند مبتنی بر دوربین های متصل به اینترنت در منازل که توسط شرکت های آمازون، گوگل و فیس بوک راه اندازی شده است حریم خصوصی کاربران را تهدید می کند.

در گزارش این روزنامه می خوانیم: کاربران در مورد بلندگوهای هوشمند و امکان اعتماد به آنها به دلیل احتمال شنود مکالمات توسط این تجهیزات توسط دیگران احساس نگرانی می کنند اما باید گفت خطر دیگری در کمین حریم خصوصی وجود دارد. در واقع شرکت های بزرگ فناوری تنها به ثبت اصوات تولید شده در منازل مردم رضایت نمی دهند بلکه می خواهند تمام اقدامات انجام شده در خانه ها را نیز مشاهده کنند.

فیس بوک دوربین هوشمند پورتال را روانه بازار کرده و شرکت آمازون نیز بلندگوهای هوشمند اکو شو که دارای صفحه نمایش لمسی و دوربین است را به مشتریان ارائه کرده است. شرکت گوگل اعلام کرده است صفحه نمایش هوشمند جدید خود به نام نست هاب مکس را با قیمت ۲۱۹ دلار به بازار عرضه می کند که دارای دوربین مکالمه ویدئویی و دوربین عکاسی است. چنانچه می توانید با استفاده از این دستگاه و از طریق اجرای نرم افزار نست به دوربین اختصاصی خودتان متصل شده و آنچه در منزل می گذرد را مشاهده کنید.

شرکت های گوگل، فیس بوک و آمازون تمایل دارند بر منازل دارای تجهیزات هوشمند تسلط یافته و مصرف کنندگان را به خدمات خود جذب کنند اما ظهور چنین دوربین هایی نگرانی هایی را میان مدافعان حریم خصوصی و امنیت به وجود آورده است و نسبت به عادت کردن مصرف کنندگان به نصب دوربین های ویدئویی متصل به اینترنت در تمام اتاق های منازل خود ابزار نارضایتی کرده اند.

صفحه نمایش هوشمند نست هاب مکس هوشمند شرکت گوگل علاوه بر دستیار صوتی پورتال فیسبوک و اکو شو آمازون مجهز به صفحه نمایش لمسی و دوربین و میکروفن است، هنگامی که می خواهید یک مکالمه ویدئویی داشته باشید فقط کافی است در برابر صفحه نمایش دستگاه خود ایستاده و فردی را که می خواهید با وی مکالمه داشته باشید انتخاب کنید تا این دستگاه ارتباط را برای شما برقرار کند.

دستیار منزل پورتال فیس بوک عبارت است از یک دوربین هوشمند که ظاهراً برای گفتگوهای تصویری با دوستان از طریق فیس بوک مسنجر ویژه این شرکت طراحی شده است. دستگاه اکو شو ویژه آمازون نیز دارای حسگرهای حرکتی است که با ورود شخصی به داخل

اتاق فعال می شود.

در این وضعیت نگرانی هایی مربوط به حریم خصوصی در مورد میکروفن هایی که دائماً به اینترنت متصل است وجود دارد چرا که معمولاً نرم افزارهای دستیار صوتی مانند آلکسا و دستیار گوگل گفتگوهای کاربر را ضبط می کنند. در سال گذشته شرکت آمازون اعتراف کرد دستگاه اکو شو تصادفاً مکالمه خصوصی یک زوج را ضبط کرده و آن را برای یکی از کارمندان شوهر ارسال نموده است.

تاکید مقامات مسئول در این باره که می توان به فایل های ضبط شده پس از ارسال به سرورهای شرکت دسترسی پیدا کرد از مسائل بسیار قابل توجه است، بنابراین کلیپ های ویدئویی و صوتی ضبط شده توسط اکو شو در خود این دستگاه ها ضبط نمی شود بلکه به سرورهای شرکت آمازون ارسال می گردد.

شرکت رینگ متخصص در امنیت منزل وابسته به شرکت آمازون نوعی دوربین هوشمند متصل به اینترنت برای منازل تولید کرده است که به عنوان زنگ درب منزل و دوربین نظارتی داخل منزل عمل کرده و به سرورهای آمازون متصل است. این شرکت با انتقادات زیادی به دلیل اجازه به مقامات نظارتی اوکراین برای دسترسی به ویدئوهای ضبط شده توسط این دوربین ها مواجه گردید.

شرکت رینگ به در اختیار داشتن الگوریتم های پیچیده خود افتخار می کند که با استفاده از آن می توان فایل ضبط شده را تحلیل کرد. این مساله تنها به زنگ های هوشمند درب منازل محدود نمی شود بلکه شرکت آمازون فایل های صوتی ضبط شده از طریق اکو شو را با عوامل این شرکت به اشتراک گذاشته و آنها می توانند به آن گوش داده و در صورت لزوم آنها را کپی کنند.

کارشناسان از مصرف کنندگان این گونه تجهیزات هوشمند منازل می خواهند شروط استفاده از آنها را مورد تحقیق قرار دهند. مات والمسلی مدیر منطقه اروپا، شرق خاورمیانه و آفریقا در شرکت امنیتی سایبری فکترا در این باره گفت: این شروط را پیش از مطالعه کامل آن نپذیرید و در مورد گزینه های مدیریت اطلاعات ثبت شده توسط این دستگاه ها تحقیق کنید که مربوط به ایجاد محدودیت برای استفاده و اشتراک گذاری و حذف اطلاعات ثبت شده توسط شرکت ارائه دهنده خدمات است.

ژوزف کارسون یکی از کارشناسان برجسته امنیت اطلاعات می گوید: کاربران باید در مورد نصب دوربین های متصل به اینترنت در منازل خود بسیار هوشیار باشند، به ویژه در اتاق هایی که نمی خواهند دیگران از آنچه در آن می گذرد آگاه شوند. هنگامی که یک دوربین متصل به اینترنت در منزل خود نصب می کنید باید بدانید که شرکت مربوطه را به منزل خود دعوت کرده اید و در واقع اطلاعات خود را با آن شرکت به اشتراک گذاشته اید.

شرکت گوگل نیز نمی تواند از خانواده هایی که اطلاعات آنان در اینترنت منتشر شده است حمایت کند زیرا هکرها از شناسه های ایمیل و کلمات عبور مختلف در عملیات های نفوذ خود استفاده می کنند تا به دوربین های منازل نفوذ کنند که در برخی مواقع موفق به انجام این

کار می شوند.

سال گذشته گزارشاتی در خصوص نفوذ به دوربین های نست هاب مکس گوگل و سرقت اطلاعات آنها منتشر شد. یکی از خانواده ها در آمریکا اعلام کرد یکی از هکرها توانسته با نفوذ به دوربین مراقبتی اختصاصی نست آنها و با استفاده از بلندگوی این دستگاه با کودک آنان گفتگو کرده و پس از مداخله والدین در این مکالمه هکر واکنش های نژاد پرستانه انجام داده است.

بیشتر این تجهیزات دارای سیستم های حفاظتی داخلی است که از لحاظ تئوری می توانید پس از متصل کردن دستگاه به برق برای حفاظت از حریم خصوصی خود آنها را فعال کنید. آلکسا، آمازون و نست گوگل به شما اجازه می دهد ارسال فایل های ضبط شده به شرکت را متوقف کنید یا می توانید میکروفن را به صورت دستی غیر فعال کرده و اجازه ندهید مکالمات شما را ضبط کند.

بهترین راه حل برای حفاظت از حریم خصوصی شما آن است که از یک پوشش بر روی دوربین ها استفاده کرده یا هنگامی که به این گونه دستگاه ها احتیاج ندارید آنها را از برق جدا کنید.

انتهای پیام/ح.ع/