پیامدها غیرقابل تصور

امان از روزی که روبات‌ها هک شوند!

زمانی که درباره روبات‌ها صحبت می‌کنیم، گفته‌های ما عمدتا در ارتباط با مشاغلی است که از دست خواهند رفت. اما زمانی که درباره مخاطرات پیرامون روبات‌ها صحبت کنیم آن‌گاه چه می‌گوید؟ نرم‌افزارها و میان‌افزارهایی که امروزه در روبات‌ها نصب شده‌اند در برابر آسیب‌پذیری‌های بحرانی بی‌دفاع هستند و هکرها با کمی دانش اولیه این شانس را دارند تا کنترل از راه دور این ماشین‌های هوشمند را به راحتی به دست بگیرند.

اگر به اطراف خود نگاه کنید، انواع مختلفی از روبات‌ها را مشاهده می‌کنید که در مصارف خانگی، تجاری و صنعتی مورد استفاده قرار می‌گیرند. به طوری که هر روزه شاهد حضور هر چه پر رنگ‌تر این ماشین‌های هوشمند در حوزه‌های مختلف به ویژه پزشکی هستیم. IOActive گزارش کرده است تا سال 2020 هزینه‌ای که بابت طراحی، ساخت و سرویس‌های پشتیبانی روبات‌ها صرف خواهد شد به رقم 188 میلیارد دلار خواهد رسید. نزدیک به دو سال پیش بود که روبات‌ها چند حادثه جدی را برای کارگران کارخانه‌های ماشین‌سازی رقم زدند. اما به تازگی پژوهشگران IOActive درباره آسیب‌پذیری روزافزون روبات‌ها هشدار داده‌اند.

مطلب پیشنهادی

روبات‌هایی با توانایی انجام وظایف سنگین و پیچیده و حساس
۸ روبات معروفی که به استخدام پلیس درآمدند!

آن‌ها روبات‌های فعال در حوزه‌های خانگی، صنعتی و تجاری را که از سوی شش شرکت بزرگ طراحی شده‌اند مورد بررسی قرار دادند. این پژوهشگران نرم‌افزارها، برنامه‌ها، اسمارت‌فون‌ها و میان‌افزارهای مورد استفاده در این روبات‌ها را مورد تحلیل قرار دادند. این گروه گفته‌اند: «در این آزمایش موفق شدیم 50 آسیب‌پذیری مختلف را شناسایی کنیم، با این وجود بررسی ما عمیق نبود و به احتمال بسیار زیاد آسیب‌پذیری‌های به مراتب بیشتری وجود دارند. ما آسیب‌پذیری‌های فوق را به اطلاع شرکت‌های سازنده رسانده‌ایم اما تنها 4 شرکت به گزارش ما واکنش نشان داده‌اند.» از میان این شرکت‌ها SoftBank Robotics تنها شرکتی بود که اعلام کرده آسیب‌پذیری شناسایی شده را ترمیم کرده است اما هیچ‌گونه اطلاعی در ارتباط با جزییات این آسیب‌پذیری ارائه نکرد.

مطلب پیشنهادی

خدمتی دیگر در راستای تحویل مرسولات سفارشی
اگر یک روبات زنگ خانه را زد و گفت سفارش شما را آوردم؛ تعجب نکنید!

روبات‌ها و پیامدهای هک شدن آن‌ها

IOActive در گزارش خود آورده است: «روبات‌هایی که در این پژوهش مورد بررسی قرار گرفتند به طیف گسترده‌ای از آسیب‌پذیری‌ها و مشکلات آلوده بودند. از شایع‌ترین و جدی‌ترین این باگ‌ها به مشکلات مربوط به برقراری ارتباط، احرازهویت، رمزنگاری، حریم خصوصی، تنظیمات پیش‌فرض کارخانه و مولفه‌های متن‌باز می‌توان اشاره کرد. هر یک از این آسیب‌پذیری‌ها به هکرها اجازه می‌دهند مکانیزم‌های ارتباطی میان روبات و دستگاه کنترل کننده را استراق سمع کرده و بی آن‌که به گذرواژه و نام کاربری نیازی داشته باشند، به سرویس‌های حیاتی دست پیدا کرده، برنامه‌ها و میان‌افزارهای مخرب خود را نصب کرده و حتا اطلاعاتی که رمزنگاری نشده‌اند را برداشت کنند. در نهایت باید به این نکته اشاره کنیم که آسیب‌پذیری‌های فوق به راحتی بستری برای جاسوسی از روبات‌ها را فراهم می‌آورند. به شکلی که دوربین و میکروفون روبات هک شده و به هکرها اجازه می‌دهد داده‌های شخصی و تجاری را از روبات استخراج کنند. شرکت‌های سازنده بهتر است به جای آن‌که به فکر عرضه سریع روبات‌ها به بازار باشند مولفه امنیت را به دقت مورد بررسی قرار دهند.»

تاریخ انتشار:

25 اسفند 1395

نشانی منبع: https://www.shabakeh-mag.com/robot/7137