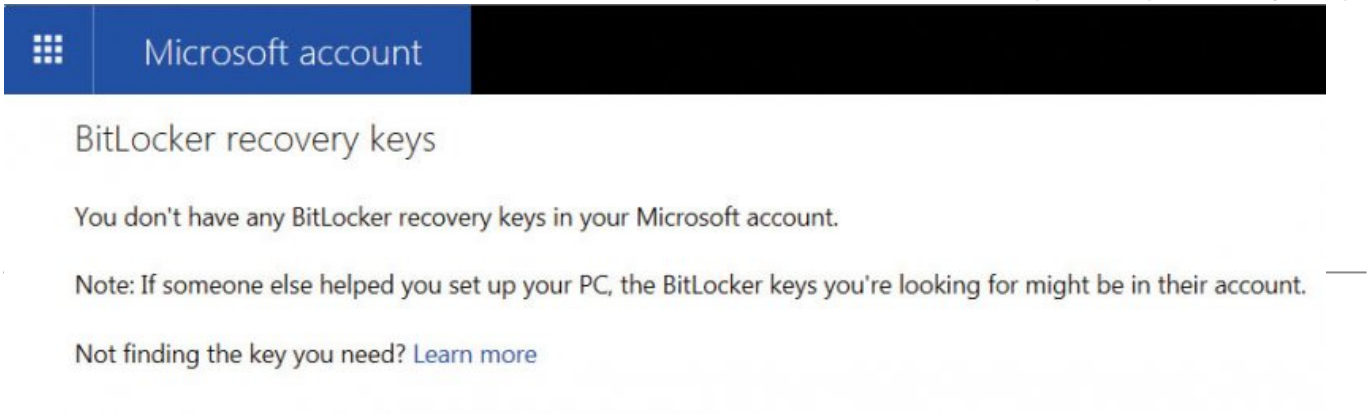
مستر کارت برای مبارزه با هکرها، از فناوری Safety Net استفاده می‌کند

زنگ پایان برای کارت‌های بانکی جعلی



مستر کارت در نظر دارد فناوری Safety Net را برای محافظت از تراکنش‌های پرداختی در بانک‌های اروپایی به خدمت بگیرد. مستر کارت سال گذشته میلادی برای افزایش سطح ایمنی تراکنش‌های بانکی از فناوری Safety Net در ایالات‌متحده استفاده کرد.

به‌کارگیری فناوری Safety Net از سوی مستر کارت زنگ پایان را برای کارت‌های جعلی به صدا درآورده است. این فناوری به‌عنوان یک‌لایه خارجی امنیتی روی سیستم پرداخت بانکی قرارگرفته تا به‌سرعت توانایی شناسایی کارت‌های تقلبی را در زمان انجام تراکنش‌ها داشته باشد. با استفاده از این فناوری شناسایی کارت‌های تقلبی به‌صورت بلادرنگ انجام می‌شود. مستر کارت به‌طور خودکار، نام صادرکنندگان کارت‌ها را ثبت کرده تا به‌راحتی بتواند معیارهای سنجش تقلب و هک کارت‌ها را کنترل کند. این کار برای آن انجام می‌شود تا در صورت نیاز، به‌سرعت توانایی مسدود کردن تراکنش‌های مشکوک را داشته باشد.

مطلب پیشنهادی

تراشه‌های اعتباری
کارت‌های تراشه‌دار چیستند و چگونه کار می‌کنند؟

مستر کارت در توصیف این فناوری اعلام کرده است، با استفاده از این الگوریتم پیچیده، نظارت بر کانال‌های متفاوت و موقعیت‌های جغرافیایی و پشتیبانی از بازارهای هدف و شرکای این شرکت با دقت بیشتری انجام می‌شود، همچنین امکان افزودن لایه محافظتی جدید و کامل به سامانه‌های پرداختی بدون آن‌که اختلالی درروند کاری شبکه رخ دهد، وجود دارد.

آجای بیهالا، مسئول امنیت جهانی شرکت مستر کارت دراین‌باره گفته است: «Safety Net این قابلیت را در اختیار ما قرار می‌دهد تا در بیست‌وچهار ساعت شبانه‌روز و هفت روز هفته میلیاردها تراکنش را در سراسر جهان مورد نظارت و ارزیابی قرار دهیم. همچنین از صادرکنندگان کارت‌ها در برابر اتفاقاتی نظیر سوءاستفاده از حساب‌های پرداختی مشتریان و برداشت‌های غیرمجاز از حساب مشتریان محافظت به عمل‌آوریم.» در کنار به‌کارگیری این فناوری، مستر کارت از آمادگی خود در ارائه سرویس‌های نشانه‌گذاری شده (Token) برای صادرکنندگان کارت‌های اعتباری تجاری خبر داده است تا شرکت‌ها و کسب‌وکارها بتوانند از کارت‌هایی که با مشارکت سرویس‌های کیف پولی موبایل کار می‌کنند، استفاده کرده و هزینه‌های خود را با استفاده از اسمارت‌فون خود پرداخت کنند. ساشین مهرا، مدیر اجرایی محصولات تجاری جهانی مستر کارت دراین‌ارتباط گفته است: «دیجیتالی کردن پرداخت‌های تجاری به کسب‌وکارهای مسافرتی این توانایی را می‌دهد تا بدون نیاز به حذف کنترل‌های متمرکز و از دست دادن کنترل مبادلات ارزی، فعالیت‌های خود را به‌آسانی انجام دهند». درحالی‌که مستر کارت تمام توان خود را بر فناوری Safety Net متمرکز داده است، در طرف مقابل شرکت ویزا، سعی کرده است به امنیت سایبری توجه بیشتری داشته باشد.

برای این منظور شرکت ویزا از سرویس هوشمند سایبری جدید خود که تعامل خوبی با FireEye دارد، رونمایی کرده است. FireEye شرکتی است که در حوزه امنیت شبکه فعالیت می‌کند. این شرکت به‌طور خودکار راه‌حل‌هایی برای تهدیدهای امنیتی و محافظت در برابر تهدیدهای پویای بدافزارها و فیشینگ ارائه می‌کند. پلتفرم پیش‌گیری از تهدیدها

شامل شبکه، ایمیل، نقاط پایانی، موبایل، محتوا، تحلیل‌ها و راه‌کارهای قانونی است. این شرکت بیش از چهار هزار مشتری در 67 کشور جهان دارد. FireEye ازجمله شرکت‌های امنیتی است که به‌سرعت توانایی تحلیل حملات هکری را دارد. درنتیجه طبیعی است ویزا به فکر همکاری مؤثر با این شرکت باشد. سرویس ابداعی ویزا به شرکت‌ها و صادرکنندگان کارت‌ها اجازه می‌دهد به پورتال اینترنتی، هشدارها و اعلان‌های موردنظر در طول یک زمان‌بندی مشخص با توجه به الگوها و تحلیل روش‌هایی که در یک حمله هکری مورداستفاده قرارگرفته‌اند، دسترسی داشته باشند.

همچنین امکان ارسال این تحلیل‌ها برای صادرکنندگان کارت‌ها و شرکت‌های تجاری وجود دارد. درنتیجه می‌توان این‌گونه بیان کرد که راهکار مورداستفاده از سوی هر دو شرکت باعث می‌شود تا هکرها چون گذشته قادر به سوءاستفاده از رخنه‌ها و جعل کارت‌های اعتباری نباشند. در کنار این الگوهای ایمن‌سازی، ایالات‌متحده از اول اکتبر سال گذشته میلادی طرح جایگزینی کارت‌های تراشه دار بانکی را با کارت‌های مغناطیسی رایج به مرحله اجرا گذاشت. طرحی که در آن امکان سوءاستفاده هکرها به حداقل می‌رسد.

تاریخ انتشار:

08 اسفند 1394

نشانی منبع: https://www.shabakeh-mag.com/security/2945