



به گفته کارشناسان امنیت، ایجاد سدهای دفاع سایبری عمیق بهترین راهکار برای مقاومت در برابر افزایش روزافزون تهدیدات در شبکه‌های تجاری است.

دالاس - گاهی اتفاق آرا نیروبخش است، ولی نه زمانیکه هیئتی پس از هیئت دیگر در کنفرانس Metro Ethernet Foundation GEN15 متفق القول اخبار دلسردکننده یکسانی را اعلام کنند. علیرغم اینکه تلاش‌های بسیاری در راستای بهبود امنیت شبکه و بنگاه‌های اقتصادی صورت پذیرفته است، ولی چشم‌انداز امروز بسیاری بدتر از مدت مشابه در گذشته است.

به گفته تیموتی والاچ نماینده ویژه نظارت نیروی ویژه مبارزه با جرایم سایبری دفتر سیاتل اداره تحقیقات فدرال، «سطح فعالیت مجرمانی که بنگاه‌های اقتصادی را در ایالات متحده مورد حمله قرار داده با بالاترین سطح خود تاکنون رسیده است.» به گفته وی، علیرغم نگرانی‌ها راجع به حملات داخلی، ولی آنها درصد اندکی از حملات مشاهده شده را تشکیل می‌دهند. از طرفی وی اذعان نمود اکثریت حملات علیه کسب و کارها عمدتاً با هدف سرقت اطلاعات از شرکت‌ها بوده که توسط رقبا قابل استفاده یا به بازار سیاه مجاری (Dark Web) قابل فروش بودند.

به گفته والاچ، علیرغم اینکه تبهکاران بزرگترین منبع این نوع تهدیدات به شمار می‌روند، ولی هنوز گروه اندکی مانند فعالان سیاسی وجود دارند که از این حملات با هدف ایجاد وقفه در کسب و کارها با نیت سیاسی بهره‌برداری می‌کنند. وی همچنین فهرستی از بازیگرانی ارائه کرد که با هدف دسترسی به شرکت‌های دیگر طرف تجارتشان ممکن یک بنگاه اقتصادی را هدف حمله قرار دهند. به گفته وی، «هیچ کس در برابر این حملات در امان نیست.»

آنچه که حملات جدید را متمایز می‌سازد، سازمان‌یافته‌تر بودن متخصصین و مهارت بیشترشان در مقایسه با گذشته است. البته همانطور که والاچ اشاره کرد، حتی هک‌هایی که از مهارت نسبتاً اندکی برخوردار بوده نیز می‌توانند به ابزارهای پیچیده‌ای برای شکستن سدهای دفاعی شبکه‌ها و انجام حملات‌شان دست یابند. به گفته وی، گاه مدیران فناوری اطلاعات متوجه می‌شوند که شبکه‌شان چندین سال است که آلوده شده و مورد نفوذ قرار گرفته است.

به گفته استوارت مک‌کلور موسس و مدیر ارشد Cylance در همین کنفرانس، «زمانیکه مدیران امنیتی شروع به جستجو تهدیداتی کنند که از قبل در شبکه‌شان وجود داشته‌اند؛ انگار Black Light را در اتاق هتل روشن کرده‌اند و آماده یافتن هر چیزی باشید.»

به گفته وی، کشف اینکه هک‌هایی مدت‌ها است به شبکه شرکت نفوذ کرده و سال‌هاست اطلاعات‌تان را سرقت می‌کنند چیز تازه‌ای نیست. در این زمان ممکن از اینکه اقدام به جستجو کردن نمودید واقعا پشیمان شوید.

در ابتدای بحث هیئت، مخترع اترنت رابرت متکالف اعلام کرد که قصد دارد حضار را به ارتقای سطح امنیت شبکه‌شان تشویق کند و اذعان نمود که در برخی نمونه‌ها، Internet of Things مهمترین نقطه ضعف [خطوط دفاعی در برابر تهدیدات] به شمار می‌رود. به گفته وی، رویه‌های احراز هویت بهتری باید طراحی و در دستگاه‌های الکترونیک تعبیه شوند. وی اظهار نمود که با

گسترش بیشتر Internet of Things بیش از پیش بر اهمیت چنین مسائل و مشکلات امنیتی افزوده خواهد شد.