کد خبر: ۲۰۹۴۲۹
یکشنبه ۱۱ آبان ۱۳۹۹ ۱۶:۳۵

راه‌حل‌های امنیتی برای شرکت‌های دورکار

شیوع کرونا، دورکاری را در میان سازمان‌ها و شرکت‌ها در سراسر جهان افزایش داد و این در حالی است که همچنان بسیاری از شرکت‌ها روش‌های امنیتی درستی برای مقابله با باج‌افزارها و بدافزارها ندارند، هرچند نشانه‌هایی از پیشرفت وجود دارد، زیرا اکنون برخی سازمان‌ها به‌طور فزاینده‌ای از راه‌حل‌های مبتنی بر ابر مدرن نسبت به راه‌حل‌های قدیمی منسوخ پیروی می‌کنند.<;br&#۴۷;><br&#۴۷;>

به گزارش سایت خبری پرسون، همزمان با شیوع گسترده و بحران پاندمی ویروس کرونا که منجر به اعلام وضعیت اضطراری قرنطینه و دورکاری کارکنان در بخش‌های مختلف از سوی دولت کشورهای جهان شد، استفاده از سرویس‌های مبتنی بر فضای ابری و اینترنت نیز توسط کاربران افزایش قابل توجهی یافت که در کنار آن حملات سایبری به این سرویس‌ها نیز رکورد زده است.

در سال‌های گذشته باج‌افزار، بدافزار و ویروس‌های رایانه‌ای بسیاری در سراسر جهان، اطلاعات محرمانه، خصوصی و مالی میلیون‌ها نفر را به سرقت بردند و میلیاردها دلار به شرکت‌های مربوطه و دولت‌ها خسارت وارد کرده‌اند. خطر حملات سایبری در کمین تمامی افراد، کاربران و شرکت‌های کوچک و بزرگ در جهان است و دیگر نمی‌توان ادعا کرد که کسی از گزند و خطرات حملات سایبری در امان است.

از سوی دیگر کار از راه دور باعث شده است که بسیاری از سازمان‌ها به دلیل راه‌حل‌های دسترسی از راه دور، در بهره‌وری و درآمد عقب بمانند. در گزارش پلیس فتا، رهبران IT موردبررسی قرار گرفتند و ۱۹ درصد از آنها بیان کردند که هنگام استفاده از راه‌حل‌های دسترسی از راه دور قدیمی، اغلب یا همیشه مشکلات شبکه و تأخیر را تجربه می‌کنند و ۴۳ درصد دیگر نیز می‌گویند که بعضی‌اوقات این مشکلات را دارند.

ارزیابی ۸۱ مورد گزارش حاکی از آن است که این مسائل منجر به کاهش بهره‌وری برای ۶۸ درصد از پاسخ‌دهندگان و از دست دادن درآمد برای ۴۳ درصد شده است. بر اساس این گزارش، سازمان‌ها هنگام کار از راه دور به روش‌های مختلف به‌طور ایمن به شبکه‌های داخلی متصل می‌شوند. حدود ۶۶ درصد از آن‌ها از VPN استفاده کرده‌اند، ۵۸ درصد بیان کردند که از سرویس ابری از طریق مرورگر وب استفاده می‌کنند، ۴۸ درصد از راه‌حل دسترسی از راه دور و ۳۴ درصد از دیوار آتش استفاده می‌کنند. بسیاری از سازمان‌ها هنوز از راه‌حل‌های قدیمی مانند VPN و دیواره‌های آتش استفاده می‌کنند تا مقیاس‌بندی کنند و با تنگناهای پیش رو و دید کم شبکه مبارزه کنند.

راه‌حل‌های امنیتی و کار از راه دور

۳۳ درصد از پاسخ‌دهندگان گفتند که رمز عبور تنها راه تأیید اعتبار خود برای دسترسی به سیستم‌ها است؛ درحالی‌که ۶۲ درصد از مدیران فناوری اطلاعات گفتند از راه‌حل‌های امنیتی مبتنی بر ابر برای دسترسی امن از راه دور استفاده می‌کنند، ۴۹ درصد گفتند هنوز از دیوار آتش و ۴۱ درصد از VPN سخت‌افزاری استفاده می‌کنند.

اما نشانه‌هایی از پیشرفت وجود دارد، زیرا سازمان‌ها به‌طور فزاینده‌ای از راه‌حل‌های مبتنی بر ابر مدرن نسبت به راه‌حل‌های قدیمی منسوخ پیروی می‌کنند. به دنبال همه‌گیری بیماری و تغییر در شیوه کار، ۷۲ درصد از پاسخ‌دهندگان گفتند که به‌احتمال‌زیاد یا به‌طور کامل راه‌حل‌های امنیتی مبتنی بر ابر را افزایش می‌دهند، ۳۸ درصد بیشتر از قبل از همه‌گیری.

مدیرعامل شرکت Amit Bareket گفت: با نیروی کار توزیع‌شده و متحرک امروز، مدل شبکه سنتی و مبتنی بر محیط دیگر منطقی نیست. جای تعجب نیست که شرکت‌ها به‌طور فزاینده‌ای به سیستم‌عامل‌های سایبری و شبکه مبتنی بر ابر منتقل شوند. ازآنجایی‌که شرکت‌های تجاری در هراندازه برای مدیریت مشاغل خود به ابر تکیه می‌کنند، به روش‌های جدیدی برای برقراری امنیت نیاز دارند تا بدون در نظر گرفتن موقعیت مکانی یا شبکه از حملات سایبری به‌طور مؤثری جلوگیری کنند.

۷۴ درصد از پاسخ‌دهندگان به دلیل نگرانی‌های امنیتی، راه‌حل‌های امنیتی مبتنی بر ابر را از طریق سخت‌افزار استفاده می‌کنند، ۴۴ درصد با کمک روش مقیاس‌پذیری مقابله می‌کنند و ۴۳ درصد ملاحظات صرفه‌جویی در وقت را ذکر می‌کنند. ۶۱ درصد از سازمان‌ها معتقدند محافظت از دستگاه‌های جدید بیشترین نگرانی امنیتی با توجه به کار از راه دور است، درحالی‌که ۵۶ درصد اظهار کردند بیشترین نگرانی آن‌ها عدم دید کاربران از راه دور است. ۳۹ درصد از پاسخ‌دهندگان اظهار کردند مقیاس‌پذیری بزرگ‌ترین چالش آن‌ها در تأمین نیروی کار از راه دور است، درحالی‌که ۳۸ درصد گفتند تخصیص بودجه بزرگ‌ترین چالش آن‌ها است.

منبع: رکنا