چارگون چک‌لیست امنیت سایبری سازمان‌ها را منتشر کرد

در ماه‌های گذشته، بسیاری از سازمان‌ها با شرایطی کم‌سابقه در حوزه زیرساخت‌های دیجیتال مواجه بوده‌اند، اختلال‌ها و محدودیت‌های اینترنت گرفته تا افزایش نگرانی‌ها درباره امنیت سامانه‌های سازمانی در شرایط پرریسک. در چنین فضایی، توجه به امنیت سایبری بیش از هر زمان دیگری برای سازمان‌ها اهمیت پیدا کرده است.

در همین راستا، مهدی زرجویی، مدیر امنیت شرکت چارگون با مرور تجربیات فنی و عملیاتی سال‌های گذشته، مجموعه‌ای از توصیه‌ها و یک چک‌لیست کاربردی برای کارشناسان و مدیران فناوری اطلاعات و امنیت سازمان‌ها ارائه کرده است تا بتوانند آمادگی خود را در برابر تهدیدات سایبری افزایش دهند.

زرجویی معتقد است پایان هر سال فرصت مناسبی است تا سازمان‌ها با مرور تجربه‌های گذشته و ارزیابی وضعیت فعلی، برای ارتقای سطح امنیت فناوری اطلاعات خود برنامه‌ریزی بهتر و به‌روزتری مطابق با شرایط داشته باشند.

او در این‌باره می‌گوید: «ما در چارگون معتقدیم که می‌توان به سبک یک سنت سازمانی، در پایان هر سال مجموعه‌ای از تجربه‌ها، ملاحظات و توصیه‌های فنی را با سازمان‌ها به اشتراک گذاشت تا تیم‌های فناوری اطلاعات و امنیت بتوانند با آمادگی بیشتری وارد

سال جدید شوند.»

به گفته مدیر امنیت چارگون، بخش قابل توجهی از رخدادهای امنیتی در سازمان‌ها به دلیل غفلت از اقدامات پایه‌ای امنیتی اتفاق می‌افتد. «بسیاری از حملات سایبری پیچیده نیستند؛ در واقع مهاجمان اغلب از ساده‌ترین نقاط ضعف مانند سیستم‌های به‌روزرسانی‌نشده، دسترسی‌های بیش از حد کاربران یا نبود پایش مناسب لاگ‌ها استفاده می‌کنند.»

او تأکید می‌کند که تیم‌های فناوری اطلاعات باید امنیت را به عنوان یک فرآیند مستمر و دائمی در نظر بگیرند، نه یک اقدام مقطعی. «امنیت سایبری یک پروژه یک‌باره نیست؛ یک فرآیند دائمی است که شامل به‌روزرسانی مداوم، پایش مستمر، آموزش کارکنان و آمادگی برای مدیریت رخدادها می‌شود.»

به گفته زرجویی، تیم‌های فنی و امنیتی سازمان‌ها می‌توانند با اجرای مجموعه‌ای از اقدامات مشخص، ریسک‌های امنیتی را تا حد قابل توجهی کاهش دهند. «تیم‌های فنی و امنیتی می‌توانند مجموعه‌ای از اقدامات، تنظیمات و ملاحظات امنیتی را برای سامانه‌های سازمانی؛ از جمله نرم‌افزارهای سازمانی اتوماسیون اداری مانند دیدگاه به‌صورت دوره‌ای بررسی و اعمال کنند.»

او در ادامه مجموعه‌ای از مهم‌ترین اقدامات امنیتی را به‌عنوان چک‌لیست پیشنهادی برای سازمان‌ها مطرح می‌کند.

به گفته مدیر امنیت چارگون، سازمان‌ها بهتر است این موارد را به‌صورت دوره‌ای

بررسی کنند:

- به‌روزرسانی سرورها، سرویس‌ها و سیستم‌عامل‌ها به آخرین نسخه‌های امنیتی
- استفاده از رمزهای عبور پیچیده و فعال‌سازی احراز هویت دومرحله‌ای (2FA)
- بازبینی دسترسی کاربران و اعمال اصل حداقل دسترسی
- پایش بلادرنگ لاگ‌ها، هشدارهای امنیتی و ترافیک شبکه
- اجرای سیاست‌های پشتیبان‌گیری منظم و نگهداری نسخه‌های آفلاین خارج از دیتاسنتر
- استفاده از ارتباطات امن و رمزگذاری‌شده مانند HTTPS و VPN
- جلوگیری از ارسال اطلاعات حساس از طریق پیام‌رسان‌ها و ایمیل‌ها
- نظارت بر تغییرات غیرعادی در ساختار فایل‌ها، کاربران و تنظیمات سیستم
- آموزش و آگاهی‌بخشی مستمر به کارکنان درباره فیشینگ و مهندسی اجتماعی

- مستندسازی و طبقه‌بندی اطلاعات مطابق الزامات قانونی
- استفاده از کنترل دسترسی شبکه مانند Firewall و VLAN
- تدوین برنامه پاسخ به رخدادهای امنیتی (Incident Response Plan)
- پایش مستمر هشدارها و اطلاعیه‌های امنیت سایبری

زرجویی در ادامه پیشنهاد می‌کند مدیران فناوری اطلاعات و امنیت با طرح چند سؤال کلیدی، وضعیت امنیتی سازمان خود را ارزیابی کنند:

- آیا همه سیستم‌ها و سرورها به آخرین نسخه‌های امنیتی به‌روزرسانی شده‌اند؟
- آیا جهت پایداری سیستم‌ها و سامانه‌ها از قابلیت‌های HA و DR در معماری سرورها استفاده می‌شود؟
- آیا پیاده‌سازی شرایط امن و مناسب کاربران دورکاری برای استفاده از سامانه‌های سازمانی اتوماسیون مانند دیدگاه فراهم کرده‌اند؟
- آیا به‌صورت مداوم دستورالعمل‌های سخت‌سازی (Hardening) و ارتقاء امنیت برای سیستم‌ها و سامانه‌های سازمانی بررسی و اعمال می‌شوند؟
- آیا برای کاربران حساس احراز هویت دومرحله‌ای فعال است؟

- آیا دسترسی کاربران به‌صورت دوره‌ای بازبینی می‌شود؟
- آیا لاگ‌ها و هشدارهای امنیتی به‌صورت مداوم پایش می‌شوند؟
- آیا نسخه‌های پشتیبان مناسب آفلاین داخل و خارج از شبکه نگهداری می‌شود؟
- آیا برنامه مشخصی برای واکنش به رخدادهای امنیتی وجود دارد؟
- آیا کارکنان سازمان آموزش‌های لازم درباره تهدیدات سایبری را دیده‌اند؟

مدیر امنیت چارگون در پایان تأکید می‌کند: «اگر سازمانی از مشتریان چارگون در پاسخ به برخی از این سؤالات به نتیجه مشخصی نرسد و یا به‌دنبال راهکار مناسب برای پوشش این موارد بود، بهتر است هرچه سریع‌تر برای اصلاح وضعیت اقدام کند. در چنین شرایطی، تیم‌های فنی و امنیتی چارگون کاملاً می‌توانند در بررسی وضعیت امنیتی سامانه‌ها و اجرای اقدامات اصلاحی در کنار سازمان‌ها باشند.»