مدیر پشتیبانی فنی چارگون تشریح کرد: شیوه‌های مقابله با بدافزارها و اختلالات شبکه‌ها

مدیر پشتیبانی فنی چارگون توضیحاتی درباره زمینه‌ها و خطاهای غیرعمدی بروز مشکلات در شبکه و سرور سازمان‌ها و شیوه‌های پیشگیری از آلودگی به بدافزارها ارائه کرد.

روزبه بهرامی در گفت‌گو با روابط عمومی **چارگون** گفت: طی اعلام یکی از مشتریان شرکت **چارگون** مبنی بر عدم دسترسی و امکان استفاده از مجموعه نرم افزاری دیدگاه با بررسی همکاران پشتیبانی فنی متوجه شدیم که متاسفانه سرور با وجود داشتن آنتی‌ویروس و بروز بودن آنها آلوده به بدافزاری است که کلیه فایل‌های داخل سرور را رمزنگاری کرده است.

وی ادامه داد: این اختلال به حدی بود که کلیه بانک‌های اطلاعاتی مشتری رمزنگاری، فایل‌های مهم سیستم عامل نیز به تغییرات و اختلالات زیادی دچار شد و بیشتر سرویس‌ها از کار افتادند؛ ضمن اینکه هارد اکسترنالی که کلیه بکاپ‌های مشتری در آن نگهداری شده است نیز به دلیل متصل بودن به سرور آلوده شد و تمامی فایل‌های بکاپ از دست رفتند.

مدیر پشتیبانی فنی چارگون با بیان اینکه کل سیستم‌های داخل شبکه این مشتری آلوده شده بود گفت: این اختلالات و مشکلات ممکن است برای هر سازمان و شرکتی اتفاق بیفتد که باید تلاش کرد تا از زمینه‌های بروز چنین مشکلاتی جلوگیری کرد.

بهرامی خاطرنشان کرد : زمانی که شما غیر عمد خطاهایی را انجام دهید، امکان درگیر شدن سیستم، سرور و شبکه به باج افزار و بدافزارها بیشتر می‌شود.

وی ادامه داد: باز کردن یک ایمیل دارای پیوست یا ضمیمه مشکوک و مخرب و یا کلیک روی لینک‌های مخرب که در ایمیل، شبکه‌های اجتماعی یا سایت‌ها قرار دارند از جمله این خطاهاست.

مدیر پشتیبانی فنی چارگون همچنین بازدید از سایت‌های مخرب و ناشناس را از دیگر خطاها در آلوده شدن شبکه‌های سازمانی دانست و گفت: دانلود فایل‌های مشکوک کرک‌ها، نرم‌افزارهای اجرایی و آلوده از وب سایت‌ها، باز کردن ماکروهای فاسد در اسناد برنامه مثل واژه پردازها word و صفحه گسترها Excel واتصال به دستگاه‌های جانبی USB مثل memory ،هارد اکسترنال، MP3 player و ... که محتویات آنها مطمئن نیستند یا به سیستم‌های عمومی متصل شده‌اند نیز از جمله بسترهایی است که سیستم‌ها، شبکه‌ها و سرورها را تهدید می‌کنند.