مرکز ماهر: دستگاه‌ها باید مسئولیت افشای اطلاعات کاربران را بپذیرند - دیجیاتو

آرش پارساپور | یکشنبه، ۰۷ اردیبهشت ۱۳۹۹

افزایش افشای اطلاعات کسب‌وکارهای خصوصی و حتی سازمان‌های دولتی در فضای مجازی در سال جدید بار دیگر این مساله را باز کرده که کسب‌وکارها در برابر اطلاعات کاربران چه مسئولیتی دارند؟ هرچند هنوز قانون دقیقی در این باره وجود ندارد و صحبت چنین موضوعی از مدت‌ها پیش در وزارت ارتباطات جریان دارد اما در حال حاضر مرکز ماهر طی بیانیه‌ای اعلام کرده که دستگاه‌ها باید مسئولیت افشای اطلاعات را بپذیرند.

در روزهای اخیر **اطلاعات لو رفته از کاربران ایرانی «تلگرام»** و همچنین **کاربران «سیب اپ»** و همچنین افشای اطلاعات سازمان ثبت احوال و چند کسب و کار کوچک دیگر نظیر فروشگاه اینترنتی شیکسون رخ داده بود و ادامه این دومینوی افشای اطلاعات می‌تواند ضرر جبران ناپذیری به اعتماد عمومی مردم وارد کند.

در همین راستا مرکز ماهر در بیانیه اخیر خود با استناد به بند 5-1 نظام ملی مقابله با حوادث فضای مجازی کشور تاکید کرده که «مسئولیت پیشگیری و مقابله با حوادث فضای مجازی هر دستگاه، بر عهده بالاترین مقام آن دستگاه خواهد بود.» مرکز ماهر باور دارد که مقابله با این دسته از حوادث فضای مجازی کشور که منجر به افشاء داده‌های شهروندان می‌شود، باید به صورت متمرکز و کاملا تخصصی، صرفا به یک مرکز مستقل دولتی واگذار شود و به نظر می‌رسد این مرکز از ایجاد یک شرکت خصوصی در این زمینه را منطقی نمی‌دند. مرکز ماهر دلیل این موضوع را امکان یک بررسی مستقل و بدون جانبداری همراه با واکنش سریع توسط یک نهاد دولتی اعلام کرده

است.

مرکز ماهر گفته که بر اساس وظایف ذاتی و قانونی خود موارد متعددی از این دست را همواره کشف می‌کند و تمام این موارد پس از بررسی‌های فنی جهت راستی‌آزمایی و استخراج شواهد و راهکار مقابله بر اساس چارچوب‌های قانونی به صورت محرمانه به صاحبان سرویس‌ها و داده‌ها اطلاع‌رسانی می‌شود. این ادعا در حالی مطرح می‌شود که برخی از افشای اطلاعات در ابتدای امر توسط کاربران در فضای مجازی اعلام می‌شود و پس از آن مرکز ماهر وارد عمل می‌شود. همانطور که خود این مرکز نیز در نامه اخیر خود از متخصصان امنیت سایبری خواسته تا در صورت مشاهده آسیب‌پذیری در هر مجموعه‌ای، آن را به مرکز ماهر اطلاع دهند و بدون اطلاع‌رسانی قبلی به خود مجموعه قربانی یا نهادهایی چون مرکز ماهر و افتا، مساله‌ای را در شبکه‌های اجتماعی منتشر نسازند چرا که به زعم مرکز ماهر، چنین کاری یک حرکتی سازنده حساب نمی‌شود.

«امیر ناظمی»، رییس سازمان فناوری و معاون وزیر ارتباطات می‌گوید سازمان فناوری مسئول پاسخگویی به این حوادث نیست و وظیفه امنیت بخش کسب‌وکار با نیروی انتظامی است.

مرکز ماهر در انتهای بیانیه خود تاکید کرده که «سکوت، پاسخ‌گویی مناسب نیست؛ بلکه تنها سرمایه اجتماعی را کاهش می‌دهد». در همین راستا مرکز ماهر دستورالعمل اقدامات پایه‌ای جهت پیشگیری از نشت اطلاعات سازمان‌ها و کسب و کارها را نیز منتشر ساخته است. متن این دستورالعمل به شرح زیر است:

- عدم اتصال مستقیم پایگاه‌های داده به صورت مستقیم به شبکه اینترنت. تا حد امکان لازم است دسترسی مستقیم به پایگاه‌های داده از طریق اینترنت برقرار نگردد. یکی از مواردی که باعث این اشتباه بزرگ می‌شود روال پشتیبانی شرکت‌های ارائه دهنده راهکارهای نرم‌افزاری کاربردی است که برای انجام پشتیبانی 24*7، مشتریان خود را الزام به برقراری دسترسی مستقیم راه دور از بستر اینترنت به بانک‌های اطلاعاتی می‌کنند. در صورت اجبار شرکت‌ها و سازمان‌ها به این مساله، این دسترسی حتما باید روی یک بستر امن و با استفاده از VPN ایجاد شود.

- دقت در راه‌اندازی پایگاه‌های داده به ویژه انواع پایگاه‌های داده‌ی NoSQL و اطمینان از عدم وجود دسترسی حفاظت نشده. لازم به توجه است بسیاری از موارد نشت اطلاعات مربوط به پایگاه‌های داده‌ای است که به طور موقت و جهت انجام فعالیت‌های موردی و کوتاه مدت راه‌اندازی شده است. لازم است اهمیت و حساسیت این نوع پایگاه‌های داده هم‌تراز پایگاه‌های اصلی درنظر گرفته شود.

- بررسی و غیرفعال‌سازی قابلیت Directory Listing غیر ضروری در سرویس دهنده‌های وب جهت جلوگیری از دسترسی به فایل‌ها.

- دقت در وضعیت دسترسی به دایرکتوری‌های محل بارگزاری داده‌ها و اسناد توسط کاربران وبسایت نظیر دایرکتوری‌های uploads و temp و ... .علاوه بر لزوم کنترل دسترسی‌ها و غیرفعالسازی قابلیت directory listing، لازم است تا حد امکان این اسناد به محل دیگری منتقل شده و از دسترس خارج گردند.

- سرویس دهنده‌ی رایج و پرکاربرد Microsoft Exchange و Microsoft Sharepoint و Zimbra با توجه به انتشار عمومی آسیب‌پذیری‌های حیاتی و اکسپلویت‌های مربوطه طی یکسال گذشته مورد سواستفاده جدی قرار گرفته‌اند. در صورت استفاده از این سرویس‌دهنده‌ها لازم است نسبت به بروز بودن آنها و نصب تمام وصله‌های امنیتی منتشر شده اطمینان حاصل گردد.

- از عدم دسترسی مستقیم از طریق اینترنت به هرگونه سرویس مدیریتی نظیر iLO، RDP، کنسول مدیریت vCenter و ESX، کنسول مدیریت فایروال و ... اطمینان حاصل نمایید. این دسترسی‌ها لازم است از طریق سرویس VPN اختصاصی و یا بر اساس آدرس IP مبدا مجاز محدود گردند.

- از نگهداری هرگونه نسخه پشتیبان از سیستم‌ها بر روی سرور وب خودداری نمایید.

- جهت اطمینان از عدم وجود دسترسی به سرویس‌ها و سامانه‌ها به صورت ناخواسته، نسبت به اسکن ساده‌ی سرویس‌های فعال بر روی بلوک‌های IP سازمان خود به صورت مداوم اقدام نموده و سرویس‌های مشاهده شده‌ی غیرضروری را از دسترسی خارج نمایید.

سیب اپ نیز در همین روزهای اخیر دچار افشای اطلاعات کاربران خود شده بود.

مرکز ماهر تاکید داشته که انجام موارد فوق به طور صد در صدی امنیت را تضمین نمی‌کند و این موارد برطرف کننده شماری از ضعف‌های جدی مشاهده شده توسط تیم آنها هستند.

گفتنیست پیش‌تر مرکز ماهر درباره دیتابیس‌های حفاظت نشده به مراجع قضایی نیز هشدار داده بود.

بیشتر بخوانید:

توضیح پلیس فتا درباره مسئولیت کسب‌وکارها در قبال افشای اطلاعات کاربران

رسپینا درباره میزبانی وب‌سایت شکار و افشای اطلاعات کاربران ایرانی تلگرام بیانیه داد

دیجیاتو