

کارمندان ناراضی، خطرناک تر از هکرها

کارمندان بخش فناوری اطلاعات در یک سازمان یا شرکت، از قابل اعتمادترین کارکنان به شمار می آیند. آنها نه تنها مسوول امور پشتیبانی در حوزه رایانه هستند، بلکه در تصمیمات مهم سازمانی نیز موثرند و سلامت و امنیت زیرساخت سازمانی را تضمین می کنند. بیشتر حرفه ای های این حوزه با غرور خاصی از مهارت های خود حرف می زنند که کار را برای دیگر کارمندان راحت می کند.

البته گاهی اوقات نیز رضایت شخصی که در دپارتمان آتی کار می کند فراهم نمی شود، که این ناراضی ناشی از جای دیگری است؛ فناوری. در یک سازمان، این مسوولان فناوری اطلاعات هستند که خوب می دانند ضعف های امنیتی سیستم در کجاست. هر چند که این اتفاق چندان تکرار نمی شود، اما وقتی هم که رخ می دهد نتایج زیانباری در پی خواهد داشت. حملاتی همچون خرابی در پایگاه داده، هک شدن شبکه، پایین آمدن وبسایت ها یا سرورهای مجازی که مسوول عملیات مهم هستند. رهایی از این خرابی ها می تواند برای یک شرکت خسارات مالی زیادی تحمیل کند و علاوه بر این، پیگیری های قانونی و تلاش روابط عمومی برای حفظ اعتماد کاربران را به همراه داشته باشد. از نمایش تصاویر نابهنجار در فایل پاورپوینت گروه بازاریابی تا فرستادن بدافزارها، مواردی است که یک عضو فناوری اطلاعات ناراضی می تواند به وسیله آن شرکت را در شرایط بدی قرار دهد. می گویند مرور تاریخ درس خوبی به آدمها می دهد، بنابراین شاید بهتر باشد ۶ مورد از بزرگترین خرابکاری های داخل سازمانی را بررسی کنیم:

۱- انتقام در مک دونالد

جیسون کرنیش که در شعبه آمریکایی شرکت ژاپنی شیونوگی مشغول به کار بود، تنها به خاطر این که دوستش را ناعادلانه از محل کار اخراج کردند، با کمک اینترنت پرسرعتی که در رستوران مک دونالد وجود داشت، ۱۵ سیستم مجازی سازی شده را پاک کرد که ۸۸ سرور حیاتی این شرکت روی آن مشغول فعالیت بودند. ماموران FBI تلاش بسیاری کردند تا این که توانستند از طریق خریدی که همان زمان به وسیله کارت اعتباری از مک دونالد کرده بود، او را پیدا کنند. ضرری که او به شرکت زد، حدود ۸۰۰ هزار دلار برآورد شد.

۲- بیماری در شبکه بیمارستان

جیسون وانگ که به خاطر اخراجش از بیمارستان نورت جنرال NYC ناراحت بود، به شبکه شرکت سابقش دسترسی پیدا کرد و اطلاعات بیمارستان را به طور کامل به هم ریخت. او همچنین با نام دکترهای مختلف به ارسال ایمیل پرداخت و از بیمارستان چهره نادرستی نشان داد. او سرانجام به جرم این خرابکاری ها دستگیر شد.

۳- خشم برای گزارش نادرست

جان پاول اسون، یک مهندس شبکه که به دلیل گزارش نادرست مافوقش، مشمول جریمه شد به رایانه او دسترسی پیدا کرد و تمام داده ها و نرم افزارهای مهم در سرورهای شرکت را نابود کرد. اطلاعاتی از جمله اطلاعات مشتریان نیز حذف شد. او به ۶۳ ماه زندان و پرداخت ۴۰۹ هزار دلار محکوم شد.

۴- شرمند کردن مدیر جلوی دیگران

والتر پاول بعد از این که از شرکتش اخراج شد، با استفاده از نرم افزار Keylogger به رمز عبور کارفرمای خود دسترسی پیدا کرد و اعتبار تمام شرکت را با یک حرکت ساده از بین برد و عطش خود در انتقام را فرو نشانید. او با قراردادن تصاویر مستهجن در فایل پاورپوینت مدیر خود، باعث شد این تصاویر ناخواسته برای مشتریان به نمایش گذاشته شود. وی پس از دستگیری به ۳ سال زندان و ۱۰۰ ساعت کار اجباری محکوم شد.

۵- حذف اطلاعات داوطلبان

تصور کنید تمام اطلاعات موسسه ای که بانک اعضای پیوندی است از بین برود. دانیل دوان که مسوول فناوری اطلاعات یک موسسه غیرانتفاعی اهدای اعضای پیوندی بود، از این که او را اخراج کرده بودند کینه مسوولان موسسه را به دل گرفت و با دسترسی غیرمجاز به شبکه این موسسه، اطلاعات تمام ارگان های اهدایی و فایل های پشتیبان آنها را پاک کرد. او به ۲ سال زندان، ۳ سال آزادی مشروط و پرداخت ۹۴ هزار دلار محکوم شد.

۶ - طمع در انتقام

راجر دورینو که برای شرکت UBS تلاش‌های زیادی کرده بود، از مبلغ ناچیز پاداشش خیلی ناراضی بود و با طراحی یک حمله امنیتی بیش از ۲ هزار سرور این شرکت را از کار انداخت و بیش از ۳ میلیون دلار خسارت وارد کرد. وی البته پیش از این حمله، تمام سهام خود را در شرکت به فروش رساند تا در زمان خرابی پیش‌بینی‌شده سرورها و متعاقباً پایین‌آمدن سهام‌ها، سودهنگفتی به جیب بزند که البته همین عامل هم باعث دستگیری‌اش شد و ۹۷ ماه زندان برایش رقم خورد.

منبع <http://www.jamejamonline.ir/>