دوشنبه 18 مهر 1390 - 07:41

خطرناك تر از هكرها

جام جم آنلاين: وانگ كه به‌خاطر اخراج از محل كارش ناراحت بود، به شبكه شركت سابقش دسترسي پيدا كرد و اطلاعات آن را به‌طور كامل به‌هم ريخت.
كارمندان بخش فناوري اطلاعات در يك سازمان يا شركت، از قابل اعتمادترين كاركنان به‌شمار مي‌آيند. آنها نه تنها مسوول امور پشتيباني در حوزه رايانه هستند، بلكه در تصميمات مهم سازماني نيز موثرند و سلامت و امنيت زيرساخت سازماني را تضمين مي‌كنند.

بيشتر حرفه‌اي‌هاي اين حوزه با غرور خاصي از مهارت‌هاي خود حرف مي‌زنند كه كار را براي ديگر كارمندان راحت مي‌كنند.

البته گاهي اوقات نيز رضايت شخصي كه در ديپارتمان آي تي كار مي‌كند فراهم نمي‌شود، كه اين نارضايتي ناشي از جاي ديگري است: فناوري.

در يك سازمان، اين مسوولان فناوري اطلاعات هستند كه خوب مي‌دانند ضعف‌هاي امنيتي سيستم در كجاست. هر چند كه اين اتفاق چندان تكرار نمي‌شود، اما وقتي هم كه رخ مي‌دهد نتايج زيانباري در پي خواهد داشت. حملاتي همچون خرابي در پايگاه داده، هك‌شدن شبكه، پايين‌آمدن وب‌سايت‌ها يا سرورهاي مجازي كه مسوول عمليات مهم هستند.

رهايي از اين خرابي‌ها مي‌تواند براي يك شركت خسارات مالي زيادي تحميل كند و علاوه بر اين، پيگيري‌هاي قانوني و تلاش روابط عمومي براي حفظ اعتماد كاربران را به‌همراه داشته باشد.

از نمايش تصاوير نابهنجار در فايل پاورپوينت گروه بازاريابي تا فرستادن بدافزارها، مواردي است كه يك عضو فناوري اطلاعات ناراضي مي‌تواند به‌وسيله آن شركت را در شرايط بدي قرار دهد. مي‌گويند مرور تاريخ درس خوبي به آدم‌ها مي‌دهد، بنابراين شايد بهتر باشد شش مورد از بزرگ‌ترين خرابكاري‌هاي داخل سازماني را بررسي كنيم:

1ـ انتقام در مك دونالد
جيسون كرنيش كه در شعبه آمريكايي شركت ژاپني شيونوگي مشغول به‌كار بود، تنها به‌خاطر اين كه دوستش را ناعادلانه از محل كار اخراج كردند، با كمك اينترنت پرسرعتي كه در رستوران مك‌دونالد وجود داشت، 15 سيستم مجازي‌سازي شده را پاك كرد كه 88 سرور حياتي اين شركت روي آن مشغول فعاليت بودند.

ماموران FBI تلاش بسياري كردند تا اين كه توانستند از طريق خريدي كه همان زمان به وسيله كارت اعتباري از مك‌دونالد كرده بود، او را پيدا كنند. ضرري كه او به شركت زد، حدود 800 هزار دلار برآورد شد.

2ـ بيماري در شبكه بيمارستان
جيسون وانگ كه به‌خاطر اخراجش از بيمارستان نورت‌جنرال NYC ناراحت بود، به شبكه شركت سابقش دسترسي پيدا كرد و اطلاعات بيمارستان را به‌طور كامل به‌هم ريخت. او همچنين با نام دكترهاي مختلف به ارسال ايميل پرداخت و از بيمارستان چهره نادرستي نشان داد. او سرانجام به جرم اين خرابكاري‌ها دستگير شد.

3ـ خشم براي گزارش نادرست
جان پاول اسون، يك مهندس شبكه كه به‌دليل گزارش نادرست مافوقش، مشمول جريمه شد به رايانه او دسترسي پيدا كرد و تمام داده‌ها و نرم‌افزارهاي مهم در سرورهاي شركت را نابود كرد. اطلاعاتي از جمله اطلاعات مشتريان نيز حذف شد. او به 63 ماه زندان و پرداخت 409 هزار دلار محكوم شد.

4ـ شرمنده‌كردن مدير جلوي ديگران
والتر پاول بعد از اين كه از شركتش اخراج شد، با استفاده از نرم‌افزار Keylogger به رمز عبور كارفرماي خود دسترسي پيدا كرد و اعتبار تمام شركت را با يك حركت ساده از بين برد و عطش خود در انتقام را
فرو نشاند. او با قراردادن تصاوير مستهجن در فايل پاورپوينت مدير خود، باعث شد اين تصاوير ناخواسته براي مشتريانش به نمايش

گذاشته شود.وي پس از دستگيري به سه سال زندان و 100ساعت كار اجباري محكوم شد.

5 ـ حذف اطلاعات داوطلبان
تصور كنيد تمام اطلاعات موسسه‌اي كه بانك اعضاي پيوندي است از بين برود. دانيل دوان كه مسوول فناوري اطلاعات يك موسسه غيرانتفاعي اهداي اعضاي پيوندي بود، از اين كه او را اخراج كرده بودند كينه مسوولان موسسه را به دل گرفت و با دسترسي غيرمجاز به شبكه اين موسسه، اطلاعات تمام ارگان‌هاي اهدايي و فايل‌هاي پشتيبان آنها را پاك كرد. او به دو سال زندان، سه سال آزادي مشروط و پرداخت 94 هزار دلار محكوم شد.

6 ـ طمع در انتقام
راجر دورينيو كه براي شركت UBS تلاش‌هاي زيادي كرده بود، از مبلغ ناچيز پاداشش خيلي ناراضي بود و با طراحي يك حمله امنيتي بيش از دو هزار سرور اين شركت را از كار انداخت و بيش از سه ميليون دلار خسارت وارد كرد. وي البته پيش از اين حمله، تمام سهام خود را در شركت به فروش رساند تا در زمان خرابي پيش‌بيني‌شده سرورها و متعاقبا پايين‌آمدن سهام‌ها، سودهنگفتي به جيب بزند كه البته همين عامل هم باعث دستگيري‌اش شد و 97 ماه زندان برايش رقم خورد.