چهار شنبه 27 مهر 1390 - 08:13

2011 را سال هك ناميدند

سازمان فناوري اطلاعات ايران با اشاره به تعداد زياد گزارش‌هاي مربوط به نقض امنيت داده ها در سال جاري اعلام كرد كه اين موضوع موجب شد متخصصان امنيت سال 2011 را سال هك بنامند.

متخصصان امنيت
2011 را "سال هك" ناميدند
جام جم آنلاين: سازمان فناوري اطلاعات ايران با اشاره به تعداد زياد گزارش‌هاي مربوط به نقض امنيت داده ها در سال جاري اعلام كرد كه اين موضوع موجب شد متخصصان امنيت سال 2011 را " سال هك " بنامند.
در گزارش روز سه شنبه روابط عمومي سازمان فناوري اطلاعات ايران ، ضمن تاكيد بر انجام اقدامات امنيتي ،10 نكته براي تقويت امنيت شبكه و جلوگيري از نفوذ در داده ها تشريح شده است .

-1 خطرات مرتبط با حوزه فناوري اطلاعات (IT) را به خوبي بشناسيد: تمام شركت‌ها بايد حداقل سالي يك بار به ارزيابي خطرات آي‌تي اقدام كنند. ارزيابي كامل خطرات آي‌تي به شناسايي و تعيين اولويت‌هاي حوزه‌هاي مشكل‌آفرين كمك مي‌كند.

-2 از اين كه خطرات مرتبط با حوزه فناوري اطلاعات در كجا رخ مي‌دهند، مطلع باشيد: اين كه بدانيد مشكل 'چيست' كافي نيست؛ علاوه بر آن بايد بدانيد مشكل در 'كجاست'. ارزيابي دقيق خطرات پيشِ روي آي‌تي مي‌تواند در بلندمدت به صرفه‌جويي در هزينه‌ها منجر شود.

-3 سيستم‌هاي خود را با قوانين حفاظت از داده‌ها منطبق سازيد: نخست با تمام استانداردهاي مرتبط صنعتي و دولتي در زمينه حفاظت از داده‌ها انطباق يابيد.

اگر شركت نتواند مطابقت با استانداردها را به طور مداوم حفظ كند، اين مطابقت بي‌نتيجه خواهد بود. فرايندي براي مديريت تطابق با استانداردها ايجاد كنيد و اطلاعات سابقه تطابق را روزآمد نگه داريد.

-4 آزمون نفوذ را به اجرا در آوريد: بازرس مستقلي براي انجام آزمون‌هاي نفوذ استخدام كنيد تا نقاط آسيب‌پذير سستم را بيابيد. آزمون‌هاي مهندسي اجتماعي را نيز اجرا كنيد.

-5 با برنامه واكنش در برابر رخدادها آشنا شويد: تمام شركت‌ها بايد بدانند كه به برنامه واكنش در برابر رخدادها نياز دارند. اگر سازمان شما چنين برنامه‌اي ندارد خيلي زود يك برنامه براي خود تدوين كنيد. اين برنامه را به صورت تمريني اجرا كنيد تا وقتي داده‌هايتان مورد تهاجم هكرها قرار گرفت همه كاركنان بدانند كه بايد فوراً دست به چه اقدامي بزنند.

-6 همه كاركنان را آموزش دهيد: انسان بدون آن‌كه خود بخواهد اصلي‌ترين دليل نقض امنيت است. به تمام كاركنان، از رده بالا تا رده پايين، بياموزيد كه مراقب نحوه استفاده از ابزارهاي شخصي و داده‌هايي كه دانلود مي‌كنند ، باشند.
-7 داده‌هاي مهم را رمزگذاري كنيد: داده‌هاي مهم ذخيره‌شده در سرورها، لپ‌تاپ‌ها و وسايل قابل‌حمل را رمزگذاري كنيد. اگر داده‌ها در فلش‌هاي قابل‌حمل ذخيره شده‌اند، آن‌ها را نيز رمزگذاري كنيد. به اين ترتيب، اگر اين دستگاه‌ها گم شوند، هيچ كس نمي‌تواند به داده‌هاي رمزگذاري شده دست يابد.

-8 تعيين گذرواژه‌هاي مطمئن: تمام كاركنان، از رده بالا گرفته تا رده‌هاي پايين، را به تغيير گاه به گاه گذرواژه‌هايشان ملزم سازيد و اطمينان حاصل كنيد كه گذرواژه هاي آنان به اندازه كافي قدرتمند باشند. به كاربران بياموزيد كه از گذرواژه‌هاي تكراري براي حساب‌هاي كاربري شغلي و يا حتي شخصي خود استفاده نكنند.

-9 شبكه و كامپيوترها را از هم تفكيك كنيد: براي مبادلات مالي نظير امور بانكي و پرداخت حقوق از دستگاهي مستقل استفاده كنيد. به هيچ جاي ديگر، مانند حساب ايميل يا وب‌سايت‌ها، از آن دستگاه وارد نشويد تا امكان نفوذ بدافزارها و نقض امنيت فراهم نشود.

-10 امنيت را مايه دردسر تلقي نكنيد: امنيت چيزي فراتر از جلوگيري يا محدودسازي صرف كارهايي است كه افراد انجام مي‌دهند. امنيت كافي، با حفظ درآمدها و سودهايي كه ممكن است از طريق نقض امنيت داده‌ها از دست رود، صاحبان مشاغل را به اداره ايمن امور قادر مي‌سازد. امنيت را بخشي ضروري از مأموريت شركت بدانيد.