

حمله های اینترنتی؛ هشدار برای جهان

حمله های اینترنتی (سایبری) به شبکه ها و سایت ها روز به روز بیشتر می شود. گوگل روز ۱۲ ژانویه، در اقدامی غیرمنتظره اعلام کرد که در اواسط ماه دسامبر ۲۰۰۹، چندین بار مورد حمله های پیچیده اینترنتی قرار گرفته است.

به گفته گوگل، مهاجمان به حساب های جی میل فعالان حقوق بشر چین حمله کرده اند. تحقیقات بعدی نشان داد که دست کم ۲۰ شرکت بزرگ دیگر هم مورد حمله های اینترنتی قرار گرفته اند.

روز ۲۷ آذر امسال توئیتر مورد حمله گروهی به نام "ارتش سایبری ایرانی" قرار گرفت. در روزهای گذشته نیز اخباری مبنی بر حمله این گروه به چند سایت اینترنتی در داخل و خارج ایران هم منتشر شد. سایت رادیو زمانه و خبر نامه امیر کبیر، پایگاه خبری تحلیلی دانشجویان دانشگاه امیرکبیر (پلی تکنیک تهران) از جمله این سایت ها بودند.



بر اساس یک تحقیق جهانی که توسط مرکز مطالعات استراتژیک و بین المللی در واشنگتن در ماه گذشته صورت گرفته، در ۱۴ کشور جهان، بیش از ۶۰۰ مدیر آتی که با اطلاعات زیربنایی و حساس سروکار دارند گزارش داده اند که شبکه های تحت مدیریت آنها اخیرا مورد حمله های شدید اینترنتی قرار گرفته اند.

۵۹ درصد آنها گفته اند شبکه های کامپیوتری و سیستم های کنترلی مورد حمله های اینترنتی بسیار سطح بالا قرار گرفته است. به نظر آنها بسیاری از این حمله ها چنان پیچیدگی و ظرافتی داشته که قطعا بدون حمایت برخی دولت های خارجی امکان تحقق نداشته است.

امریکا؛ یکی از هدف های اصلی

دنيس بلر، مدير آژانس اطلاعاتی ملی امریکا روز سه شنبه، پانزده بهمن، حمله های اینترنتی علیه گوگل را "زنگ خطر" دانست.

"این جور حمله های اینترنتی ساده و سرودستی انجام نمی گیرد؛ اینها کار یکشنبه نیست."

راب لی، متخصص امنیت شبکه

آقای بلر گفت "اطلاعات کامپیوتری زیربنایی و مهم در امریکا را حمله های اینترنتی بی سابقه و فوق العاده پیچیده ای تهدید می کند. شبکه های کامپیوتری در مراکز مهم دولتی و غیردولتی مورد حمله های مداوم و مکرر قرار گرفته و می گیرند".

بخشی از نتایج تحقیقات آقای بلر که به کمیته امنیت مجلس سنای امریکا ارائه شده، از این قرار است:

- اطلاعات حساس هر روز از شبکه های دولتی و خصوصی به سرقت می رود.
- تحقیقات نشان دهنده حضور غیرمجاز و دائمی مهاجمان در شبکه هاست.
- امریکا به هیچ وجه نباید مطمئن باشد که در بحران های مهم، به اطلاعات زیربنایی خود دسترسی خواهد داشت.

حرف های بلر ممکن است برای عده ای تازگی داشته باشد اما متخصصان امنیت شبکه هر روز با این تهدید ها دست و پنجه نرم می کنند .

راب لی، مدیر ماندیانت، یکی از شرکت های متخصص امنیت سایبر، می گوید: "این جور حمله ها ساده و سرودستی انجام نمی گیرد؛ اینها کار یک شبه نیست. هدف مهاجمان اشغال کامل شبکه است. آنها حرفه ای هستند. این قبیل کارها، کار تمام وقت چندین آدم است و مراحل مختلفی دارد: از نفوذ اولیه به شبکه بگیریید تا استخراج کامل اطلاعات. افراد در این حمله ها مسوولیت ها را تقسیم می کنند".

آیا باید چین را سرزنش کرد؟

از میان ۴۰ تا ۴۵ حمله بسیار پیچیده در سال قبل در امریکا، حدود دو سوم آن بی ارتباط با چین نبوده است. این نتیجه ای است که متخصصان امنیت شبکه پس از تحقیق، به آن رسیده اند .

چین چند روز پس از اعلام خبر گوگل مبنی بر حمله به حساب های جی میل فعالان چینی، از کنترل دولتی بر اینترنت دفاع کرد.

یکی از مقام های بلندپایه رسمی چین گفت پورنوگرافی، کلاهبرداری و شایعه پراکنی خطرناک است و رسانه های اینترنتی در چین باید به "هدایت افکار عمومی" کمک کنند.

گوگل، در جست و جوی راه حل

خطر حمله های شدیدتر و خطرناک تر، غول اینترنتی گوگل را وادار کرده تا با آژانس امنیت ملی امریکا قراردادی ببندد و به این آژانس اجازه بدهد حمله های جاسوسی گروهی را که احتمال می رود از چین هدایت شده باشد تحقیق و بررسی کند .

واشنگتن پست، به نقل از منابع آگاه نوشته است هدف این تحقیق، کمک به بهبود امنیت برای دفاع از گوگل و کاربرانش از حمله های آتی اینترنتی است.

این منابع گفته اند گوگل به این آژانس اطلاعاتی که قدرتمندترین سازمان تحقیقاتی الکترونیکی جهان به شمار می رود، اجازه استفاده از اطلاعات حساس و پراهمیت را می دهد، اما به شرط زیر پا نگذاشتن قوانین و سیاست های گوگل که مبتنی است بر حفظ اسرار کاربران و ارتباطات آنلاین.

بر اساس شرط گوگل، این آژانس اجازه مشاهده جست و جوی کاربران یا حساب های پست الکترونیکی آنها را نخواهد داشت.

احتمال می رود این آژانس از "اف بی آی" و دپارتمان امنیت داخلی هم برای شرکت در این پروژه دعوت کند.

هدف اصلی این پروژه یافتن فرد یا افرادی که پشت این حمله ها بوده اند، نیست؛ چون این کار تقریباً غیر ممکن است؛ هدف اصلی یافتن راه حل هایی است برای بهبود سیستم دفاعی گوگل یا آنچه متخصصان "اطمینان اطلاعاتی" نام گذاشته اند.

این روزها با رشد روزافزون تجمع صدا، تصویر، فیلم، و سایر شکل های اطلاعاتی در یک شبکه واحد (یعنی اینترنت) همه کشورهای جهان در قبال دستبرد اطلاعاتی آسیب پذیرتر شده اند.



حمله به سایت ها و شبکه ها و استخراج اطلاعات شخصی افراد، شرکت ها و موسسات خصوصی و دولتی منجر به خسارت های حقوقی، امنیتی، اقتصادی و سیاسی خواهد شد، و غفلت از بهبود سیستم امنیتی شبکه ها مایه پشیمانی است.

http://www.bbc.co.uk/persian/world/2010/02/100205_l41_cyber_attack_google.shtml

© BBC 2010