بنام خدا

نگاه رو به جلو: مهم‌ترین مسائل امنیت سایبری در سال ۲۰۱٦

کم‌تر از دو ماه به پایان سال ۲۰۱۵ میلادی باقی مانده است. دنیای امنیت سایبری در سال ۲۰۱۵ میلادی با تغییرات جدی مواجه شد که انتظار می‌رود این تغییرات در سال ۲۰۱۶ هم ادامه داشته باشد. به نظر می‌رسد برای همگام شدن با تغییرات سال ۲۰۱۶ بهتر است درک بهتری از برخی مسائل وجود داشته باشد. در ادامه فهرست ۱۰ موضوع از مهم‌ترین مسائل دنیای امنیت سایبری که انتظار می‌رود سال آینده موضوعات محوری باشند آورده شده است.

۱- اینترنت اشیاء

اینترنت اشیاء یا IoT مفهمومی است که در مورد ارتباط اشیاء از راه اینترنت یا سایر راه‌های ارتباطی بحث می‌کند، در این مفهوم اشیاء فیزیکی همگی جزیی از یک شبکه‌ی اطلاعاتی محسوب می‌شوند. در واقع ایده‌ی اصلی ارتباط بین لوازم خانگی با اینترنت است، مثلاً این‌که یخچال خانگی با دریافت یک منو بتواند لوازم مورد نیاز آن را بررسی نماید. به این ترتیب ره‌گیری جزیی‌ترین فعالیت‌های کاربر هم ممکن می‌شود. اما آیا دنیای امنیت آماده‌ی پذیرش چنین شبکه‌ای است؟ آیا می‌توان مطمئن بود جزییات فعالیت این اشیاء ره‌گیری نمی‌شود؟ چه سوءاستفاده‌های احتمالی ممکن است از اطلاعات هر یک از این محصولات شود؟

۲- اینترنت و وسایل نقلیه

داشتن شبکه‌ی WiFi در خودروی شخصی بسیار هیجان‌انگیز است، اما اتصال به اینترنت همیشه تهدیداتی را به همراه می‌آورد. اگر خودروی شما به اینترنت متصل باشد و به صورت اتفاقی یک نفوذگر راهی را پیدا کند که به کمک آن بتواند وسیله‌ی نقلیه‌ی شما را کنترل کند، چه اتفاقی می‌افتد؟ کنفرانس بلک‌هت که یکی از مهم‌ترین کنفرانس‌های بررسی تهدیدات امنیتی است، در سال ۲۰۱۵ تمرکز ویژه‌ای روی مسئله‌ی نفوذ به خودروهای شخصی داشته است. این نشان می‌دهد نفوذگران به اندازه‌ی کافی جذب این موضوع شده‌اند و ممکن

است حتی راهکارهایی برای نفوذ به سامانه‌های فعلی در نظر داشته باشند. آسیب‌پذیری‌های این حوزه بسیار جدی است و ممکن است خطرات زیادی به همراه داشته باشد.

۳- تبلیغات و ره‌گیری کاربران

همه‌ی ما تبلیغاتی که به صورت خاص برای ما و در مرورگر ما به نمایش درمی‌آیند را مشاهده کرده‌ایم. به محض این‌که در مورد اطلاعات یک پرواز جست‌وجو کنید، تبلیغات مرتبط با آژانس‌های مسافرتی برای شما به نمایش درمی‌آید. بسیاری از وب‌گاه‌ها فعالیت‌های کاربر را ره‌گیری می‌کنند و برای کاربر یک نمایه‌ی کامل می‌سازند که در عمل تجاوز به حریم شخصی کاربر محسوب می‌شود. بسیاری از مرورگرها در تلاش هستند با ارائه‌ی راهکارهایی در مقابل این ره‌گیری عکس‌العمل نشان دهند و در مقابل وب‌گاه‌ها هر روز از ترفندهای جدیدتری استفاده می‌کنند. تبلیغات روی مثبت ماجرا است. اگر وب‌گاه‌ها از هر آن‌چه که ما در اینترنت می‌خوانیم، مقالات، کتاب‌ها و اخبار، یک رونوشت تهیه کنند، به راحتی از همه‌ی مسائل خصوصی و علمی یک فرد مطلع می‌شوند و ممکن اس این اطلاعات را به آژانس‌های جاسوسی از جمله از NSA بفروشند.

٤- انتشار بدافزار از راه تبلیغ

زمانی‌که یک نفوذگر تلاش می‌کند از شبکه‌های تبلیغاتی سوءاستفاده نماید و بدافزار و ویروس‌های اینترنتی را منتشر کند، گرفتاری‌های جدی برای کاربران و شبکه‌های تبلیغاتی ایجاد می‌شود. یعنی مسئله از این‌که فقط یک کاربر از یک وب‌گاه آلوده بازدید کند، به این‌که تبلیغات آلوده بدون بازدید از وب‌گاه خاص به سمت کاربر بیاید تغییر کرده است. تصور کنید شما یک وب‌گاه سالم را باز می‌کنید و یک تبلیغ نمایش داده می‌شود که آلوده است. شما هیچ کار اشتباهی نکرده‌اید، اما بدافزاری مهمان ناخوانده‌ی شما شده است.

٥- بدافزارهای تلفن همراه

تلفن‌های همراه، جایی است که شما خصوصی‌ترین تصاویر، پیامک‌ها و اطلاعات خود را نگه می‌دارید. از آن‌ها برای دسترسی به حساب‌های بانکی استفاده می‌کنید. تلفن‌های همراه و تبلت‌ها به قدری اطلاعات حساس دارند که به تنهایی ترسناک هستند. حال تصور کنید که توجه نفوذگران هم به سمت این دستگاه‌ها جلب شود. به کمک آسیب‌پذیری‌های سامانه‌عامل‌های تلفن همراه که بسیار زیاد هستند، مدت زمان کمی طول می‌کشد که نفوذگر مقیم دستگاه شما شود و به همه‌ی اطلاعات شما خصوصاً اطلاعات بانکی دسترسی پیدا کند. برای مقابله با این تهدیدها چه باید کرد؟ نرم‌افزارهای تلفن همراه چقدر امن هستند؟

٦- باج‌افزار

نام دیگر باج‌افزار، دردسر است. قطعه بدافزارهایی که پس از آلوده کردن سامانه‌ی شما، پرونده‌های مهم شما رمز می‌کنند و از شما می‌خواهند برای دسترسی دوباره به پرونده‌های خود مبلغی پول، احتمالاً پول رمزشده و ناشناس بیت‌کوین به حساب مهاجمین پرداخت کنید. برخی از انواع باج‌افزارها حتی پس از پرداخت پول هم پرونده‌های شما را بازگردانی نمی‌کنند. تهدید جدی که تاکنون در سامانه‌عامل‌های ویندوز، لینوکس و اندروید مشاهده شده است. باج‌افزارها تا کجا پیچیده می‌شوند و برای مقابله با آن‌ها چه راه‌کارهایی پیشنهاد خواهد شد؟

۷- بازگردانی داده

در دنیای امروز، خصوصاً در حوزه‌های کسب‌وکار، داده و محافظت از آن مهم‌ترین نقش را بازی می‌کند. اگر نفوذگران به سامانه‌های شما دسترسی پیدا کنند و با موفقیت بخشی از داده‌های شما را حذف کنند، برای بازیابی چه خواهید کرد؟ با گسترش باج‌افزارها این مسئله به صورت جدی‌تری در سال ۲۰۱۶ پی‌گیری خواهد شد.

۸- ارائه‌دهندگان خدمات شخص ثالث

همیشه لازم نیست نفوذگران برای دسترسی به حساب‌های بانکی، حمله‌ی سایبری علیه یک بانک راه‌اندازی نمایند. کافی‌ست یک ارائه‌دهنده‌ی سرویس شخص ثالث را شناسایی کنند که کاربران برای خریدهای ساده از کارت اعتباری استفاده می‌کنند و با نفوذ به پایگاه‌داده‌ی این ارائه‌دهنده همه‌ی اطلاعات حساس مشتریان را به سرقت ببرند. نوعی حمله که از سال ۲۰۱۴ به شدت افزایش پیدا کرده است. آیا بالاخره راهی برای مقابله با این تهدید کشف می‌شود؟

۹- رمزنگاری داده و مخالفت دولت‌ها

رمزنگاری یکی از مهم‌ترین بخش‌های محافظت از داده است. اما همین رمزنگاری مهم‌ترین چالش دولت‌ها برای شنود و جاسوسی علیه کاربران می‌باشد. دولت‌ها معتقد هستند برای مبارزه با تروریسم به شنود احتیاج دارند و به همین دلیل نباید رمزنگاری به صورت عمومی انجام شود. اما کاربران می‌خواهند برای حفظ حریم خصوصی از رمزنگاری استفاده کنند. بالاخره کدام طرف برنده خواهد شد؟

۱۰- آسیب‌پذیری در زیرساخت‌های حساس

۱۶ سازمان یا موسسه در هر کشوری جزء زیرساخت‌های حساس آن کشور محسوب می‌شوند که شامل بخش دفاعی، کشاورزی و فناوری اطلاعات هم می‌شوند. حمله‌ی سایبری به هر یک از این زیرساخت‌ها خسارت جبران‌ناپذیری را به کشور تحمیل می‌کند، در حالی‌که همه‌ی این زیرساخت‌ها دارای آسیب‌پذیری‌های جدی در بخش فناوری هستند که اگر توجه نفوذگران به آن‌ها جلب شود، امنیت ملی کشور به خطر می‌افتد. آیا در سال ۲۰۱۶ شاهد چنین حوادث سایبری خطرناکی خواهیم بود؟ یا حتی آیا پژوهش‌گران برنامه‌های بلندمدت و کوتاه‌مدتی برای مقابله با این آسیب‌پذیری‌ها ارائه می‌دهند؟

پیروز و موفق باشید.

منبع :

http://gadellnet.com/2015/10/cyber-security-trends-for-2016/