بسمه تعالی

«حراست دانشگاه»
آموزش

بولتن علمی و آموزشی پیام

شماره سوم دی ماه ۱۳۸۷ « ویژهٔ امنیت شبکه های رایانه ای »" قسمت دوم"

دانشگاه علوم پزشکی و خدمات بهداشتی درمانی گلستان

بلوتوث (Bluetooth):

یک فناوری بی سیم با برد کوتاه است، که به تلفنهای همراه، مینی کامپیوتر(PDA)، کامپیوترها، دستگاههای ضبط و پخش استریو، لوازم خانگی، اتومبیل ها و همه وسایل دیگری که می توانید ارتباط آنها را با یکدیگر برقرار نمائید، امکان ارتباط می دهد.

بلوتوث که بعضی ها در فارسی آن را به **دندان آبی** ترجمه کرده اند، با دارابودن قابلیت عملکرد به عنوان یک روش شبکه سازی بی سیم دربرگیرنده طیفی از دستگاه ها می باشد. وسایل مجهز به تراشه های بلوتوث حدود ۱۰ الی ۱۰۰۰ متر برد داشته و می توانند قادر به انتقال داده ها با سرعت ۷۲۰ کیلوبایت در ثانیه از پشت دیوار ها، کیف و پوشاک می باشد.

کاربرد ها و مصارف bluetooth

۱. ایجاد یک شبکه بیسیم برای کامپیوتر های رومیزی با یک پهنای باند کوچک
۲. استفاده در تجهیزاتی مثل پرینتر، میکروفون، کیبرد، موس
۳. انتقال فایلها (مثل عکس و موسیقی و غیره) بین گوشی های موبایل و کامپیوترها
۴. استفاده در دستگاههای اندازه گیری و ابزارهای پزشکی مثل وسایل کمک شنوایی
۵. استفاده در گیرنده های مکان یاب " GPS "
۶. استفاده بعنوان handsfree در اتومبیل
۷. کنترل از راه دور تلویزیون بجای اینفرارد

محبوبیت بلوتوث باعث افزایش پاره ای تهدیدات امنیتی به شرح ذیل شده است :

۱. روش bluejacking : فردی به صورت ناشناس اتصال را برقرار می نماید و کارت ویزیت الکترونیکی بر روی یک دستگاه مجهز به بلوتوث را ارسال می کند.
۲. روش bluebugging : خطر جدی تری دارد. به صورتی که یک کاربر دیگر بلوتوث امکان می یابد با متصل شدن به یک تلفن همراه یا یک مینی کامپیوتر(PDA)، به اجرای دستورات ، برقراری مکالمه، ارسال پیام های متنی و حتی استراق سمع یک مکالمه اقدام کند.
۳. روش bluesnarfing: به یک کاربر بلوتوث امکان می دهد با اتصال به دستگاه های دیگری که در بردکاری و موثر قرار دارند، به مشخصات تماس ها، تقویم، و سایر اطلاعات دیگر دسترسی پیدا کند.

ابزارهایی با قابلیت بلوتوث،

هدف مناسبی برای تهدیدات امنیتی مختلف هستند.

تنها با تائید و ok نمودن یک سوال نامفهوم انگلیسی اجازه انتقال تمامی اطلاعات ذخیره شده داخل تلفن همراه خود را (شامل اسامی، شماره تلفن،sms ، عکس و فیلم ها) در اختیار فرد بیگانه قرار داده اید.

حمایت و محافظت از دستگاه های مجهز به بلوتوث، این ارزش را دارد که با بی مبالاتی و ساده انگاری، هدف اولین موج حملات امنیتی قرار نگیریم. با رشد بیشتر استفاده از بلوتوث ، این امکان وجود دارد که این پروتکل ارتباطی، به هدف محبوبی برای کلیه تهدیدات امنیتی ، شامل ویروس ها ، تهدیدات هکرها و عمدتا حملاتی با سبک تروجان ها تبدیل گردد.

فناوری بلوتوث اکنون از تجهیزات پزشکی تا کنسول های بازی را در بر می گیرد. حتی سرویس پک۲ ویندوز XP هم از بلوتوث پشتیبانی می نماید. ابزارهایی با قابلیت بلوتوث، هدف تهدیدات امنیتی گوناگونی هستند.

هوشیار باشید:

تلفن همراه خود را به جلسات و همایشهای مهم نبرید.

توصیه حراستی: بلوتوث کامپیوتر و تلفن همراه بصورت پیش فرض روشن است، آن را خاموش و دسترسی آن را با رمز محدود نمائید

ایمن سازی ادوات بلوتوث

- با توجه به این که ایمن سازی ادوات بلوتوث کار چندان دشواری نیست، راه کار های ذیل برای ایمن سازی ادوات با قابلیت بلوتوث توصیه می گردد:
- همیشه عمل اتصال به تجهیزات را در مکان های خصوصی و امن انجام دهید تا ریسک لو رفتن PIN Code شما به حداقل برسد.
- برای از بین بردن خطر دسترسی افراد ناشناس به دستگاه موبایل شما، تنظیمات آن را روی حالت غیر قابل شناسایی (nondiscoverable) قرار دهید.
- به طور مرتب و در فواصل زمانی کوتاه ، وب سایت کارخانه سازنده دستگاه خود را جهت دریافت برزورسانی ها و وصله های امنیتی جدید بازدید نمایید.
- هیچ گاه پیغام ها و درخواست های اتصال از طریق بلوتوث را از جانب کاربران ناشناس نپذیرید. ویروس Cabir تنها از طریق قبول دریافت پیغام و اجرای فایل پیوست آن ، دستگاه را آلوده می نماید.
- اگر با یک پیوست مشکوک مواجه شدید که به همراه یک ایمیل از طریق بلوتوث به دستتان رسید، احتیاط و پیشگیری مشابه را بنمایید.
- باید Pair کردن یا ارتباط ابزارهای خود را با رعایت جنبه های ایمنی انجام دهید. از کد PIN(شماره شناسایی شخصی) با داشتن حداقل هشت رقم، استفاده نمایید.

این فناوری (بلوتوث) به دلیل استفاده آسان و رایگان بودن آن مورد توجه بسیاری از جوانان و نوجوانان قرارگرفته است، اما دستاورد استفاده ازاین فناوری نوین تنها و تنها یک روی سکه است چراکه هر فناوری درکنار مزایائی که برای کاربران خود دارد خالی ازمعایب هم نیست.

یکی ازمعایب بسیار مهم این فن آوری استفاده های غیر اخلاقی آن می باشد.

در شماره بعدی بولتن

علمی آموزشی پیام ویژه امنیت شبکه های رایانه ای با گواهینامه امنیت SSL : Socket Secure Layer آشنا خواهید شد.

منتظر توصیه های امنیتی ما باشید.

GOUMS ISMS

پروژه استاندارد سازی

مدیریت امنیت در فن آوری اطلاعات دانشگاه

مفهوم امنیت در زمینه فن آوری اطلاعات ، مواردی چون حفاظت داده ها در مقابل حوادث, خرابکاری ها ,تغییرات و یا افشاء اطلاعات را شامل می شود .تعبیر عامه از فعالیت در این مقوله , حرفهٔ متخصصینی از قبیل کارشناسان سیستم های اطلاعاتی , خبرگان در زمینه امنیت سیستم ها و کسانی که در امور حقوقی و قانونی فعا لیت دارند، بحساب می آید .با استفاده روز افزون از رایانه های شخصی و توزیع توانایی پردازش اطلاعات بین سطوح مختلف کارکنان , مسئولیت امنیت نیز بین کارمندان ,مسئولین ومدیران توزیع شده است . لذا هیچ مدیری نمی تواند با خیالی آسوده تصور نماید که فرد دیگری این مسئولیت را دارا می باشد .متخصصین این امر با توجه به سطح دانش و آگاهی بالایی که در این زمینه دارند بایستی برنامه ریزی مطلوبی را جهت حفاظت داده ها و اطلاعات، متناسب با ماهیت داده های سازمان خود ارائه دهند . بطور خلاصه مسائلی که مدیریت امنیت بر آنها تأکید دارد عبارتند از:

"دقت اطلاعات" "طبقه بندی اطلاعات " " استمرار فعالیت"

بررسی نیازهای امنیتی:

برای بررسی نیازها ابتدا باید به این سؤال پاسخ داد : شما در دنیای فن آوری اطلاعات , امنیت را چگونه مدیریت می کنید؟ از دیدگاه سیاست مدیریت مخاطره ، «مدیریت امنیت»، وظیفه صاحب و مالک سیستم است «نه لزوماً کاربر آن» باید توجه نمود که حتی پیچیده ترین معیارهای امنیتی می تواند، توسط یک کاربر بی‌دقت، بی استفاده و بی مصرف گردد . این مدیران هستند که با مدیریت خود میتوانند همه افراد یک سازمان را در مسئولیت حفاظت و امنیت اطلاعات موجود در آن سازمان شریک سازند و با آموزش وتشویق کارکنان زیر نظر خود، از خطاهای آنها بکاهند.