جمهوری اسلامی ایران

وزارت کشور
استانداری اصفهان
فرمانداری مبارکه

شماره: ۸۹/۶۴۵۸

تاریخ: ۸۹/۵/۱۷

پیوست: .....

جلسه شناخت بدافزارها و راههای مقابله با آنها توسط گروه امنیت داده های کمیته فناوری اطلاعات و ارتباطات شهرستان مبارکه روز دوشنبه مورخ ۸۹/۵/۴ ساعت ۹.۳۰ صبح در محل فرمانداری مبارکه و با شرکت کارشناسان فناوری اطلاعات و مسئولین حراست دستگاههای اجرایی شهرستان برگزار گردید.

در ابتدای این جلسه جناب آقای محمدی معاون محترم فرماندار شهرستان مبارکه به اهمیت فناوری اطلاعات و ارتباطات اشاره و با بیان این که هر فناوری جدید معایب جدیدی را نیز با خود به همراه می آورد، وجود بدافزارها و تأثیرات آنها بر رایانه ها و شبکه های رایانه ای را از آن جمله خواند و شناخت دقیق راههای مقابله با آنها توسط کارشناسان ادارات را خواستار شد.

در ادامه جناب آقای همتیار کارشناس-مسئول محترم برنامه ریزی و امور عمرانی فرمانداری مبارکه ضمن تشریح فعالیتهای کمیته فناوری اطلاعات و ارتباطات شهرستان مبارکه طی یکسال گذشته، تشکیل جلسات و سمینارهای آموزشی مشابه این جلسه را از برنامه های کمیته خواند و بر ادامه برگزاری این جلسات در ماههای آتی تاکید نمود.

سپس آقای مهندس اولیایی کارشناس فنی شرکت مهندسی تحقیق و توسعه ارتباطات پانا به ارائه مبحث شناخت انواع بدافزارها و راههای مقابله با آنها پرداخت. وی توجه به امنیت شبکه های کامپیوتری را لازم و اولین گام به سوی تامین آن را تعیین منابع شبکه شامل شناسایی سرمایه های مرتبط با امنیت اطلاعات و ارتباطات سازمانی و شناسایی اهداف کوتاه مدت، میان مدت و بلند مدت امنیت شبکه دانست.

اهداف کوتاه مدت امنیت شبکه مواردی چون جلوگیری از حملات و دسترسیهای غیرمجاز، مهار خسارتهای ناشی از ناامنی موجود در شبکه و کاهش رخنه پذیری را شامل می شود که کاهش رخنه پذیری از طریق: مدیریت و به روزرسانی در سه سطح سیستم عامل- سرویسها و زیرساخت شبکه، تهیه ضدویروس و نرم افزار جلوگیری از نفوذ، سیستم پشتیبان گیری، سیستم ثبت رویداد، دیواره آتش و سخت افزارهای امنیتی صورت می پذیرد.

اهداف میان مدت را می توان تامین صحت عملکرد- قابلیت دسترسی و محافظت برای سخت افزارها و نرم افزارها، تامین محرمانگی- صحت و قابلیت دسترسی برای اطلاعات و ارتباطات متناسب با طبقه بندی آنها، تامین قابلیت تشخیص هویت- تعیین حدود اختیارات- پاسخگویی و آگاهی رسانی به کاربران شبکه متناسب با طبقه بندی و نوع کاربران دانست .

هدف درازمدت برای یک شبکه کامپیوتری اخذ گواهینامه استاندارد امنیت اطلاعات می باشد.

در ادامه جلسه مشابه سازی، رشد جمعیت و خاصیت انگلی عمده ترین مشخصه های مشترک بدافزارها عنوان و نقاط ورودی و منابع انتشار آنها اینترنت (ایمیل، مرورگرها، انتقال فایل، گروههای خبری)، منابع شبکه (دیسکهای اشتراکی، ایستگاههای کاری، سرورها، دیوارهای آتش، سرورهای پروکسی) و دیسکها ودرایوها (CDها، DVDها، دیسکتها، درایوهای اشتراکی، درایوهای قابل حمل و نقل) معرفی گردید.

در ادامه انواع کدهای مخرب شامل بمب منطقی، اسب تروجان، درب پشتی، ویروس، کرم، خرگوش، جاسوس، Adware و روت کیت معرفی و خصوصیات و مشخصات هرکدام از این بدافزارها بررسی شد و به عنوان نتیجه گیری روت کیتها به دلیل تغییر در عملکرد مولفه های سیستم عامل و دشواری تشخیص توسط آنتی ویروسها خطرناکترین نوع بدافزارها شناخته شدند.

سپس درخصوص راههای پیشگیری از آلوده شدن شبکه ها به بدافزارها مواردی متذکر گردید به ویژه بر استفاده از نرم افزارهای آنتی ویروس با قابلیتهای کلی: شناسایی و پاکسازی انواع کدهای مخرب، سازگاری و پشتیانی از انواع سیستم عاملها، به روزرسانی خودکار از طریق اینترنت، قابلیت شناسایی بدافزارها در فایلهای پیوست بازنشده پیامهای الکترونیکی و قرنطینه کردن فایلهای آسیب دیده تاکید شد و مرکز مدیریت برخی آنتی ویروسهای متداول جهت مشاهده موارد فوق برای حضار نمایش داده شد.

پس از پاسخگویی به سئوالات حاضران، جلسه شناخت بدافزارها و راههای مقابله با آنها در ساعت ۱۲ خاتمه یافت.