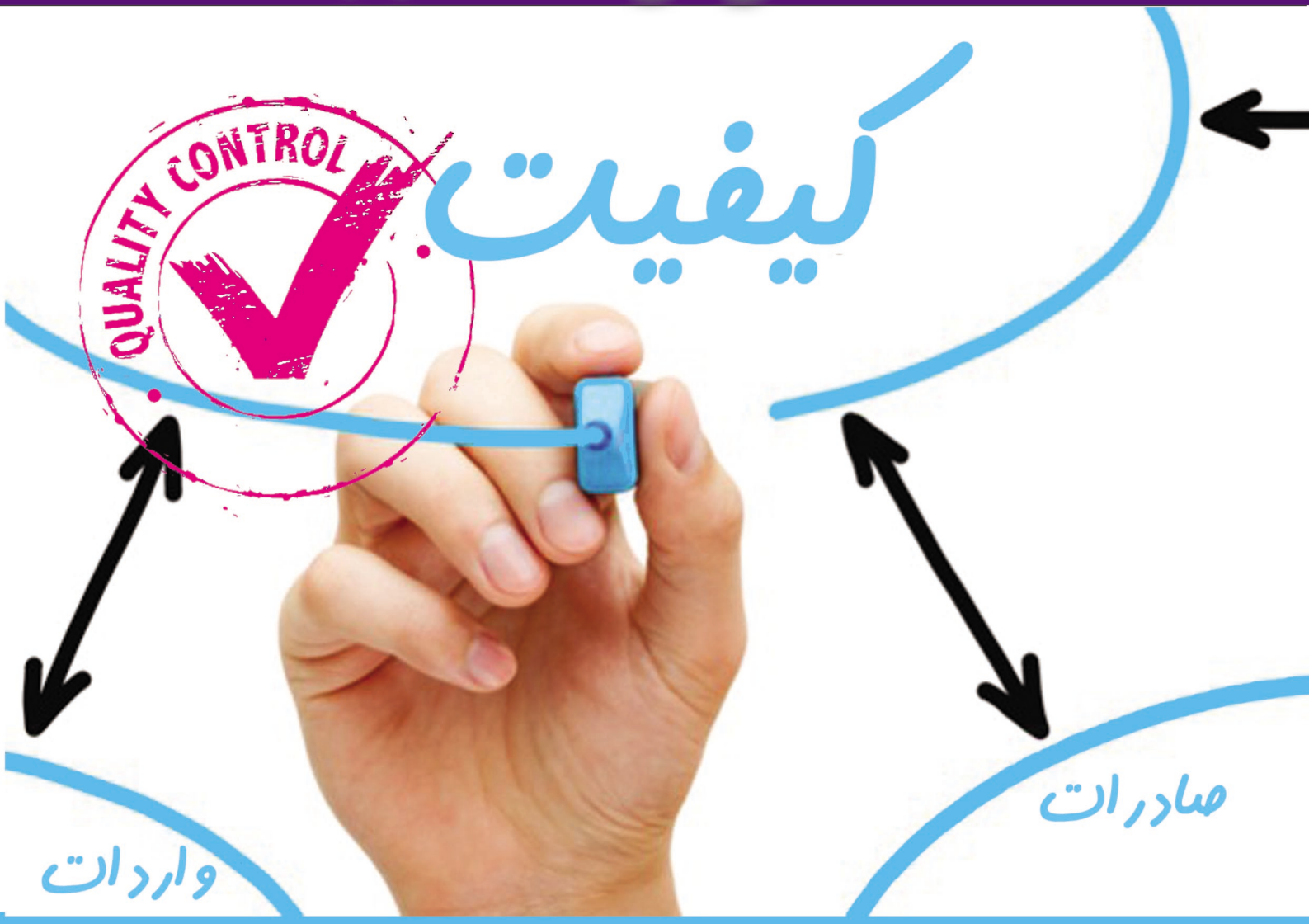
www.rcii.ir

فصلنامه مرکز تحقیقات صنایع انفورماتیک / دوره جدید / شماره ۲۰ / پاییز ۱۳۹۳

انفورماتیک

گزارش صنایع

RCII



تدبیری بیندیشیم که کیفیت‌فدای تسهیل در تجارت خارجی نشود

مقاله

امنیت در سیستم‌های کنترل صنعتی و SCADA

بازدید مشاور وزیر و مدیر کل دفتر محیط زیست وزارت صنعت، معدن و تجارت از مجتمع آزمایشگاهی مرکز تحقیقات صنایع انفورماتیک

در گفتگو با مدیر آزمایشگاه ارزیابی امنیت محصولات IT مطرح شد

پذیرفتن سند «افتا» به عنوان یک اصل باعث رفع نگرانی های امنیتی

به نام خداوند بخشنده مهربان

یادداشت نخست

به قلم مدیر مسئول

تدبیری بیندیشیم که کیفیت فدای تسهیل در تجارت خارجی نشود

تسهیل در تجارت خارجی یکی از بحث های روز است و آنچه در وهله اول از شنیدن این عبارت به ذهن متبادر می شود، ساده تر کردن تجارت است اما باید دقت کرد که مفهوم اصلی و بنیادین این عبارت ایجاد کارایی تجارت است. تسهیل تجارت خارجی شامل سیاستگذاری ها و اقداماتی جهت کاهش هزینه، زمان و عدم قطعیت مرتبط با تجارت بین الملل با حفظ کیفیت و مطلوبیت کلان حاصل از تجارت است. برای تسهیل تجارت خارجی طیف متنوعی از اقدامات از قبیل بهینه سازی مبادی ورود و خروج کالا، ساده سازی و هم نواسازی رویه ها و دستورالعمل های مرتبط با تشریفات گمرکی و سایر تشریفات قانونی در حوزه های تجارت، بانک، بیمه، حمل ونقل و غیره، توسعه زیرساخت های حمل و نقل و لجستیک، به کارگیری فناوری های جدید (مانند پنجره واحد تجاری) و اقدامات مشابه را می توان به کار گرفت.

اما باید دقت کرد که همه این اقدامات باید منجر به افزایش کیفیت واردات و صادرات نیز بشود. ورود آسان کالاهای بی کیفیت به داخل کشور که در بسیاری از موارد سلامت و امنیت جامعه را به خطر می اندازند را نمی توان تسهیل تجارت تعبیر کرد یا سهولت صدور کالاهای بی کیفیت به کشورهای هدف را که منجر به عودت کالا، ادعای خسارت و بدنامی تجار، کالاها و خدمات ایرانی می شود را نمی توان تسهیل در تجارت خارجی نامید. تضعیف نظارت های تطابق با استانداردهای ملی و بین المللی بر روی کالاهای وارداتی و صادراتی در میان مدت و بلند مدت و حتی در برخی موارد در کوتاه مدت، نتیجه مطلوبی را بر اقتصاد کشور درپی نخواهد داشت. نظارت های تطابق با استانداردهای ملی و بین المللی با هزینه هایی بسیار ناچیز و در زمانی کوتاه انجام می شود و آنالیز هزینه-منفعت آن حاکی از اثربخشی چنین نظارت هایی است.

از قانون گذاران، مجریان و تصمیم گیرندگان حوزه صنعت و تجارت کشور استدعا دارد در اصلاح قوانین و مقررات، رویه ها و دستورالعمل ها، تسهیل در تجارت همراه با حفظ کیفیت مدنظر قرار گیرد تا به این ترتیب علاوه بر ساده و روان سازی تجارت، کیفیت زندگی جامعه و اعتبار کشور نیز تامین شود.

گزارش صنایع انفورماتیک

فصلنامه مرکز تحقیقات صنایع انفورماتیک / دوره جدید / شماره ۲۰ / پاییز ۱۳۹۳

صاحب امتیاز: مرکز تحقیقات صنایع انفورماتیک

مدیر مسئول: ویدا سینا

مدیر اجرایی: افسانه عبادی

مدیرفنی: رامین رضایی

روابط عمومی: فریبا نبی زاده

همکاران این شماره: امین علی‌بلندی / ایرج ارقند

نشانی: تهران، خیابان کریم خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر،پلاک ۳

تلفن: ۸۸۹۲۵۹۵۰ (۱۰خط)

فکس: ۸۸۹۳۷۶۵۸

سایت : www.rcii.ir

مجری طرح فصلنامه:گروه رسانه‌ای مهرتابان/۰۹۱۲۳۰۸۹۳۰۳

[akbarkarimi40@gmail.com]

نشانی آزمایشگاه‌ها:

آزمایشگاه مرکزی:
تهران،خیابان کریم خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر،پلاک ۳
تلفن: ۸۸۹۲۵۹۵۰(۱۰خط)
فکس: ۸۸۹۳۷۶۵۸

آزمایشگاه پرند:
شهرک صنعتی پرند، بلوار فن آوری، خیابان گلزار، خیابان گلگشت، قطعه D 44
تلفکس:۵۶۴۱۸۸۹۲

آزمایشگاه بندر عباس:
مجتمع آزمایشگاهی اداره کل استاندارد و تحقیقات صنعتی هرمزگان مستقر در اسکله شهید رجایی
تلفن: ۰۷۶۱۴۵۱۴۲۵۹
فکس:۰۷۶۱۴۵۱۴۲۵۸

آزمایشگاه شیراز:
بلوار خلیج فارس، جاده نیروگاه، منطقه ویژه اقتصادی، فاز یک، مجتمع رها، واحد۱۸
تلفن:۷-۷۱۷۵۲۳۶-۰۷۱۱

آزمایشگاه سلفچگان:
منطقه ویژه اقتصادی سلفچگان، ساختمان تجاری، واحد۴
تلفن:۰۲۵۲۳۳۶۷۷۴۷۳

بازدید مشاور وزیر و مدیر کل دفتر محیط زیست وزارت صنعت، معدن و تجارت از مجتمع آزمایشگاهی مرکز تحقیقات صنایع انفورماتیک

سرکار خانم جلودارزاده مشاور محترم وزیرصنعت، معدن و تجارت به همراه جناب آقای دکتر یاراحمدی مدیر کل محترم دفتر محیط زیست وزارت صنعت، معدن و تجارت در تاریخ ۱۱ آذر ماه از بخش های مختلف مجتمع آزمایشگاهی پرند از جمله: آزمایشگاه ایمنی، آزمایشگاه EMC، آزمایشگاه IP، آزمایشگاه لوازم خانگی، آزمایشگاه کارآیی، آزمایشگاه SAR، چمبر الکترومغناطیسی ، آزمایشگاه لیزر و آزمایشگاه باتری بازدید به عمل آوردند.

بازدید حراست قوه مقننه از آزمایشگاه امنیت مرکز تحقیقات صنایع انفورماتیک

کارشناسان محترم حراست قوه مقننه در تاریخ ۱۲ آذر ماه از توانمندی ها و ظرفیت های ایجاد شده در آزمایشگاه امنیت مرکز تحقیقات صنایع انفورماتیک بازدید به عمل آوردند.

در گفتگو با مدیرآزمایشگاه ارزیابی امنیت محصولات IT مطرح شد

پذیرفتن سند «افتا» به عنوان یک اصل باعث رفع نگرانی های امنیتی

«امنیت» در محصولات IT موضوعی است که متاسفانه آنچنان که باید مورد توجه قرارنگرفته است.این بی توجهی گاه کار را به جایی رسانده که با به حاشیه کشیده شدن اصول اساسی در این زمینه، راه برای ورود تجهیزات مرتبط و استفاده از آنها تسهیل شده است.
امن سازی و پرداختن به مقوله امنیت موضوع هزینه بری است که شاید به همین دلیل باعث غفلت از این مساله و ایجاد مقاومت در برابر آن شده است. اینها نکاتی است که در گفتگو با مهندس مهری یحیایی مدیر آزمایشگاه ارزیابی امنیت مرکز تحقیقات صنایع انفورماتیک به آن پرداخته ایم.

انفورماتیک لطفا خودتان را معرفی کنید:

مهری یحیایی، فارغ التحصیل کارشناسی ارشد مهندسی فناوری اطلاعات، مدیر آزمایشگاه های ارزیابی امنیت محصولات IT و ارزیابی کیفیت نرم افزار مرکز تحقیقات صنایع انفورماتیک و از سال ۱۳۸۸ تا کنون مدرس دانشگاه جامع علمی کاربردی هستم.

از سال ۱۳۸۵ و از دوران تحصیل در مقطع کارشناسی، به عنوان کارشناس وب و شبکه مشغول به کار بوده ام. عضویت در هیئت رئیسه کمیته تخصصی JTC۱ و زیر شاخه SC۲۷، عضویت حقیقی انجمن آزمایشگاه های همکار و کالیبراسیون، تدوین بیش از پنجاه استاندارد تخصصی حوزه IT، مدیریت پروژه ارزیابی و ممیزی محصولات فاوا بر اساس استانداردهای بین المللی، مدیریت پروژه طراحی امن سامانه ها و تدریس استانداردهای تخصصی، جزء فعالیت هایی است که تا کنون داشته ام.

انفورماتیک به نظر شما نگاه امنیتی ساختارهای نظارتی به محصولات IT چگونه است؟

ایجاد ساختار نظارت برای حصول اطمینان از امنیت محصولاتی که به کار گرفته می شوند امر بسیار پیچیده ای است. در واقع پیچیده بودن شبکه های ارتباطی و اصطلاحاً «فتا» و همینطور حساسیت هایی که نسبت به مسأله تامین امنیت وجود دارد باعث شده تا هر بخش حاکمیتی با نگاه خود به این مقوله نگاه کند. مثلاً حوزه بانکداری، سازمان های دولتی، مراکز حساس و سایر مراکز مشابه هر کدام با دغدغه خاص خود امنیت را تعریف می کنند. البته گاه این تفاوت در

دیدگاه از ذات موضوع امنیت ناشی می شود ولی در برخی موارد نیز موجب شده تا مسأله اصلی که همان تامین امنیت است، مغفول بماند. در واقع همیشه اینطور به نظر می آید که امنیت و تامین آن به عبارتی موضوعی کلیشه‌ای و مانع توسعه و بستر سازی است. پس تلاش شده به حاشیه رانده شود تا مسیر ورود تجهیزات، استفاده و بهره برداری از زیرساخت های IT تسهیل شود. البته با توجه به اینکه امن سازی و امن بودن هزینه بر بوده و مستلزم صرف وقت کارشناسی زیادی است قطعاً مقاومت های بسیاری وجود دارد ولی تبعات ندیده گرفتن آن نیز غیر قابل انکار است و با اینکه دغدغه های سازمان های نظارتی و حاکمیتی در این رابطه زیاد است، اما متاسفانه بعضاً شاهد رخداد دور زدن موضوع امنیت هستیم.

انفورماتیک جایگاه اسنادی نظیر سند افتا و سند جامع فناوری اطلاعات را در این مقوله چه طور می بینید؟

همانطور که می دانیم سند جامع فناوری اطلاعات در سال ۱۳۸۶ و سپس یکسال بعد از آن در سال ۱۳۸۷ سند راهبردی افتا تصویب و ابلاغ شده است و همانطور که از نام سند اول مشخص است به صورت کلان حوزه فناوری اطلاعات و ارتباطات را مرزبندی کرده است و نه به طور خاص در حوزه امنیت. در ادامه سند افتا بسیار روشنگرانه و مبسوط به تبیین چارچوب امنیتی حاکم بر عرصه زیر ساخت IT پرداخته است. در همه حوزه هایی که امروز دغدغه بهره برداران این صنعت است، اعم از برنامه ریزان، تصمیم گیران، تولیدکنندگان، مصرف کنندگان، ممیزین و غیره این سند کاربرد دارد. از حوزه هایی که مربوط به سیاست گذاری می شود تا حوزه‌هایی که نقشه راه اجرا را تدوین می کنند. به نظر اینجانب، اگر این سند به عنوان یک اصل پذیرفته و اجرا شود، بسیاری از مشکلات موجود چه در ساختار، چه از باب رفع نگرانی های امنیتی و چه از منظر یکپارچه سازی نهادهای حاکمیتی حل شده و دیگر نیازی به تفکر در حوزه هدف گذاری کلان امنیت و اجرا وجود نخواهد داشت.

انفورماتیک سیاست گذاری در حوزه افتا در کشور و عملکرد سازمانهای وابسته چگونه است؟

اول باید ببینیم تعریف ما از سازمان های وابسته چیست؟ آیا سازمان هایی که مجری این مصوبه هستند؟ یا سازمان هایی که می خواهند از محصولات و خدمات IT به صورت امن استفاده کنند؟ در حال حاضر اتفاقی که افتاده است این است که تعداد متولیان در حال افزایش است. در صورتی که اگر ما به سند راهبردی افتا برگردیم، مجری و سازمان های همکار آن به خوبی مشخص شده است. در واقع سیاست گذاری و اجرا دچار موازی کاری شده است و همانطور که در قبل نیز اشاره کردم، این امر باعث شده است تا مساله اصلی مغفول بماند. در صورتیکه اگر تفکیک این امور صورت بگیرد و فقط کارگروهی جهت پیشبرد آنها تشکیل شود که به صورت ثابت در همه مقاطع و مراکز با رویکرد یکسان مدیریت تعارضات بین سازمان ها را به عهده بگیرد؛ بسیاری از این امور حل شده و هدف اصلی که همان تامین امنیت است محقق خواهد شد. البته تا حدودی این امر طبیعی است. مقوله امنیت IT در کشور ما موضوع جدیدی است و گاه تعابیر و تفاسیر مختلف نیز باعث ایجاد تداخل کاری در حوزه های گوناگون می شود ولی به هر حال انتظار این است که مصوبه سند راهبردی افتا به کار گرفته شود و تمامی ارگان های مربوطه بر سر اجرای آن با یکدیگر به توافق نظر برسند.

انفورماتیک وضعیت تولید تجهیزات امنیتی را چگونه ارزیابی می کنید؟

پتانسیل خوبی وجود دارد. در مقام یک آزمایشگاه که همواره نقطه تماس و دریافت محصولات هستم، ورود محصولات داخلی به آزمایشگاه و تلاش و همت تولیدکنندگان آنها بسیار جای تقدیر دارد. البته این واقعیت را باید بپذیریم که تکنولوژی های این زمینه بسیار پیچیده هستند و چون ما در ایران عموماً صاحب اصلی این فناوری ها نیستیم، در حوزه ایجاد، توسعه، فناوری و رقابت با چالش های متعددی روبرو می شویم. اما تلاش ها خوب است. اتفاقاً همان سند افتا رویکرد خیلی خوبی نسبت به کارگیری و لزوم استفاده از محصولات داخلی دارد. اما شاید اتفاقی که برای دیگر صنایع رخ نداده، باید برای این صنعت سیاستگذاری و اجرا شود. آن هم به کارگیری سیاست رقابتی و توسعه صادرات در جهت جلوگیری از واردات برای رفع نیاز داخلی است. یعنی اگر تولیدکنندگان داخلی با هدف صادراتی کردن محصول تلاش کنند، آنگاه رقابتی شدن و فضای کسب و کار آنها گسترش یافته و انگیزه رقابت با محصولات مشابه خارجی باعث ارتقاء ایشان خواهد شد. این امر نیز مستلزم به کارگیری استانداردها و تولید واقعی داخل است. بررسی تکنولوژی برتر و تلاش برای انتقال آن سنگ بنای خوبی است. با توانی که در شرکت های تولیدی داخلی می بینیم، دستیابی به نوآوری و خلق محصول جدید و قابل رقابت امری غیر ممکن نیست.

انفورماتیک برای افزایش امنیت تجهیزات امنیتی چه راهکارهایی را پیشنهاد می کنید؟

شاید اینجا بهتر است تمرکز فقط از روی محصولات امنیتی برداشته شود و موضوع صحبت به کل محصولات IT تغییر پیدا کند. تهدیدات و چالش های امنیتی که رخ می دهند، لزوماً به محصولات امنیتی محدود نمی شوند و آنچه مهم است امنیت کل محصولات است. فرآیند امن سازی محصول، فرآیند بسیار پیچیده ای است و لزوماً پرهزینه، اما امری است اجتناب ناپذیر.

خوب است که تولیدکنندگان با این دیدگاه نسبت به فرآیند تولید نگاه کنند که یک محصول باید از ایده تا پیاده سازی امن شود. از چرخه تجزیه و تحلیل، معماری، پیاده سازی، مستندات، نصب و پیکربندی و حتی نگهداری؛ البته این حوزه محدودیت های زیادی دارد ولی در برخی موارد ملاحظه می شود از یک پیکربندی ساده، یک تغییر رمز عبور اولیه، تنظیم یک قانون و کارهایی از این قبیل چه مشکلات و مسایلی رخ می دهد.

به نظر اینجانب ارتقاء سطح دانش و آگاهی عمومی و حتی تخصصی در حوزه امنیت بسیار راهگشا خواهد بود. امنیت یک زنجیر با حلقه های متصل به هم است. هر حلقه یک جزء است. یک حلقه محصول، یک حلقه تولید کننده، یک حلقه بهره بردار و غیره هر کدام از اینها با مسئله مواجه شود، زنجیر امنیت از هم خواهد

سند افتا بسیار روشنگرانه و مبسوط به تبیین چارچوب امنیتی حاکم بر عرصه زیر ساخت IT پرداخته است. در همه حوزه‌هایی که امروز دغدغه بهره‌برداران این صنعت است، اعم از برنامه‌ریزان، تصمیم‌گیران، تولیدکنندگان، مصرف‌کنندگان، ممیزین و غیره این سند کاربرد دارد. از حوزه‌هایی که مربوط به سیاست‌گذاری می‌شود تا حوزه‌هایی که نقشه راه اجرا را تدوین می‌کنند. به نظر اینجانب، اگر این سند به عنوان یک اصل پذیرفته و اجرا شود، بسیاری از مشکلات موجود چه در ساختار، چه از باب رفع نگرانی‌های امنیتی و چه از منظر یکپارچه‌سازی نهادهای حاکمیتی حل شده و دیگر نیازی به تفکر در حوزه هدف‌گذاری کلان امنیت و اجرا وجود نخواهد داشت.

گسیخت.
در مرحله بعدی نیز استانداردها و به کارگیری آنها در همه حوزه‌های مدیریتی، خدماتی و محصولی بسیار مهم است. خوب است که همواره چارچوب واحد و مشخص و دقیقی برای ارزیابی ها وجود داشته باشد که این امر محقق نمی شود مگر با به کارگیری استاندارد. در حوزه امنیت نیز استاندارد بسیار زیاد است. مراجع ارزیابی کاملاً مشخص هستند. اما متاسفانه به دلیل عدم آگاهی یا بعضاً نشر نظرات غیر کارشناسی و سطحی با این امر مواجه هستیم که عمده مشکلات در اثر عدم استفاده از این الزامات ناشی می شود.
در نهایت نیز مراکز ارزیابی براساس استاندارد با همین رویکرد فعالیت کنند. یعنی از هر گونه ارزیابی های سلیقه ای و مبتنی بر دایره محدود ابزار، دانش و معیار اندازه گیری پرهیز شود و مفهوم امنیت و ارزیابی امنیتی براساس استانداردهای جامع صورت پذیرد.

انفورماتیک نقش آزمایشگاه‌های امنیتی و کمکی که می توانند به افزایش سطح امنیت کنند؟

دقیقاً با همان رویکردی که در سئوال قبلی عرض کردم، آزمایشگاه های امنیت نقش به سزایی در رشد و توسعه محصولات امنیتی دارند، همواره شخص ثالث و ارزیاب، با بی طرفی و عدم تعصب می تواند نقاط ضعف، اشکالات یا حتی نقاط بهبود و قوت را بهتر ببیند و بشناسد. در دنیا نیز به آزمایشگاه های امنیت با همین نقش و جایگاه نگاه شده و امروز شاهد این امر هستیم که بسیاری از برندهای معتبر، با گواهی نامه های آزمایشگاه ذی صلاح به فروش مشغول اند و این گواهی را تداوم بخش فرآیندهای کسب وکار خود می دانند. شرایط خاص ایران، استفاده از پتانسیل آزمایشگاه ارزیابی امنیت را بیش از پیش ضروری می کند. از دو زاویه؛ یک ورود محصولات خارجی، که به تبع به کارگیری و حصول اعتماد و اطمینان از عملکرد امن آنها همواره محلی از تهدید و ابهام را دارد. دو، محصولات تولید داخل که به دلایلی که قبلاً گفته شد نیاز به ارتقاء و توسعه دارند. از هر دو منظر آزمایشگاه نقش عمده و کلیدی را در فرآیند امن سازی و پس از آن اعتماد، بازی می کند. کمک به رشد و توسعه و ارتقاء آزمایشگاه نیز موجب بالا بردن سطوح امنیت و اعتماد در قابلیت به کارگیری محصولات خواهد شد. یک آزمایشگاه که صحت و سلامت کاری و اصول محرمانگی را رعایت نموده و به عنوان امین هر دو سوی تولیدکننده و مصرف کننده باشد؛ همواره مورد نیاز بوده و لزوم آن غیر قابل انکار است.

انفورماتیک راهکارهای تعامل موفق با آزمایشگاه را چه می‌دانید؟

واقعیت این است که این تعامل خیلی ساده است ولی اراده تعامل بسیار سخت است. در واقع نگرش آزمایشگاه، رشد و توسعه و ارتقاء است و اساساً هدف این نیست که یک محصول یا یک زیرساخت آزمون شده و رد شود. همواره رفع اشکال و امن سازی باید سرلوحه کار آزمایشگاه‌باشد. وقتی موارد عدم انطباق با استاندارد و نقاط آسیب پذیر به متقاضی ارائه می شود، او باید یک برنامه و خط مشی برای برطرف کردن آن داشته باشد و در این فرآیند با برطرف کردن نقاط ضعف و آسیب پذیری محصول خود، قطعاً، محصولی امن، با کیفیت و با اطمینان خاطر به مشتریان خود عرضه می کند. اما قبول این واقعیت و انجام آن از طرف برخی صاحبان محصول امروزه کمی دشوار به نظر می رسد. اما اگر به عنوان یک تولیدکننده بپذیریم که چرخه تولید و ارتقاء یک سیکل نامتناهی است و بهبود و ارتقاء وظیفه اصلی و اولیه یک تولیدکننده است؛ استانداردها، حداقل های یک محصول هستند و ارائه یک محصول یا زیرساخت امن و قابل اعتماد وظیفه اصلی و ملی ماست، این تعامل بسیار سهل خواهد شد.

انفورماتیک لطفا به‌طور مختصر آزمایشگاه امنیت مرکز تحقیقات صنایع انفورماتیک و قابلیت‌های آن را توضیح دهید.

سابقه فعالیت این آزمایشگاه بسیار درخشان است و زیربنای آن با ملی کردن استاندارد بین المللی و مرجع ارزیابی محصولات ISO/IEC 15408 گذاشته شد. آزمایشگاه ارزیابی امنیت مرکز تحقیقات صنایع انفورماتیک، به عنوان اولین آزمایشگاه در کشور موفق به اخذ گواهینامه ISO 17025 از نظام تائید صلاحیت ایران شده و دقیقاً منطبق با رویکردها و راهبردهای مطروحه در سند افتا، به عنوان آزمایشگاه همکار مجموعه سازمان های حاکمیتی و نظارتی در کشور، نظیر سازمان فناوری اطلاعات ایران فعالیت می کند.
ماموریت این آزمایشگاه ارزیابی امنیتی محصولات و زیرساخت های فناوری اطلاعات و همچنین کمک به رشد، ارتقا و استانداردسازی این محصولات است. ارزیابی امنیتی و آزمون انطباق محصولات فاوا بر اساس استاندارد INSO/ISO/IEC 15408 در پنجاه گروه؛ نظیر:
-ارزیابی امنیتی انواع تجهیزات امنیت شبکه نظیر: IPS, IDS, UTM, Firewall و.... در دو گروه تجهیزات تولید داخل و محصولات خارجی
-ارزیابی امنیتی انواع تجهیزات شبکه نظیر: سوئیچ، روتر، Load Balancer، تجهیزات ثبت لاگ ممیزی آن ها، مونیتورینگ شبکه
- ارزیابی امنیتی کارت های هوشمند و ماژول های رمزنگاری
-ارزیابی امنیتی انواع نرم افزارها و سیستم های عامل در خانواده: اتوماسیون، ERP، احراز هویت و سایر نرم افزارهای کاربردی
-ارزیابی امنیتی نرم افزارهای کنترل صنعتی
-ارزیابی امنیتی تجهیزات و زیرساخت های بانکداری الکترونیک نظیر: POS, POS application, Anti Fraud و.... بر اساس استانداردهای ISO 8583, PCI DSS
- به روز رسانی و تدوین استانداردهای امنیتی بین المللی و بومی
- تدوین و به کارگیری متدولوژی های روز ارزیابی امنیتی
از جمله فعالیت های این آزمایشگاه است. با توجه به اینکه مرکز تحقیقات صنایع انفورماتیک با عمده فعالیت آزمایشگاهی در حوزه های مختلف IT و CT به ارائه سرویس می پردازد، از مزایای آزمایشگاه امنیت این مرکز بهره گیری از توان سایر آزمایشگاه های تخصصی موجود، نظیر آزمایشگاه ارزیابی نرم افزارهای با قابلیت پشتیبانی از زیرساخت کلید عمومی (PKI Enabled)، نرم افزارهای صدور گواهی دیجیتال، آزمایشگاه رمزنگاری آزمایشگاه های EMC و Safety است.
تاکنون محصولات و زیرساخت های متعددی در این آزمایشگاه مورد ارزیابی قرار گرفته است و امیدواریم با توسعه فرهنگ استانداردسازی و تبیین و تقویت جایگاه امنیت و نظام های ارزیابی شاهد رشد و ارتقاء آزمایشگاه و محصولات باشیم.

وقتی موارد عدم انطباق با استاندارد و نقاط آسیب پذیر به متقاضی ارائه می‌شود، او باید یک برنامه و خط‌مشی برای برطرف کردن آن داشته باشد و در این فرآیند با برطرف کردن نقاط ضعف و آسیب پذیری محصول خود، قطعاً، محصولی امن، با کیفیت و با اطمینان خاطر به مشتریان خود عرضه می‌کند. اما قبول این واقعیت و انجام آن از طرف برخی صاحبان محصول امروزه کمی دشوار به نظر می‌رسد.

امنیت در سیستم های کنترل صنعتی و SCADA

امین علی‌بلندی

سیستم کنترل صنعتی آمده است تا سرعت، دقت تولید و بهره‌وری را در صنعت بهبود ببخشد. حتی فرایندهای ناممکن و بسیار پیچیده را تسهیل کند و امکان کنترل و مانیتورینگ از راه دور را فراهم سازد. روند رو به رشد تکنولوژی‌های به‌کار رفته در سیستم‌های کنترل صنعتی، تغییرات مداوم، حرکت رو به جلو دانش فناوری‌اطلاعات و ظهور پدیده‌ها و امکانات جدید قابل استفاده در بخش‌های مختلف به خصوص بخش صنعت و نیز ارتباط تنگاتنگ صنعت و IT و از همه مهمتر مسایل سیاسی، پرداختن به مقوله امنیت را دوچندان می کند.

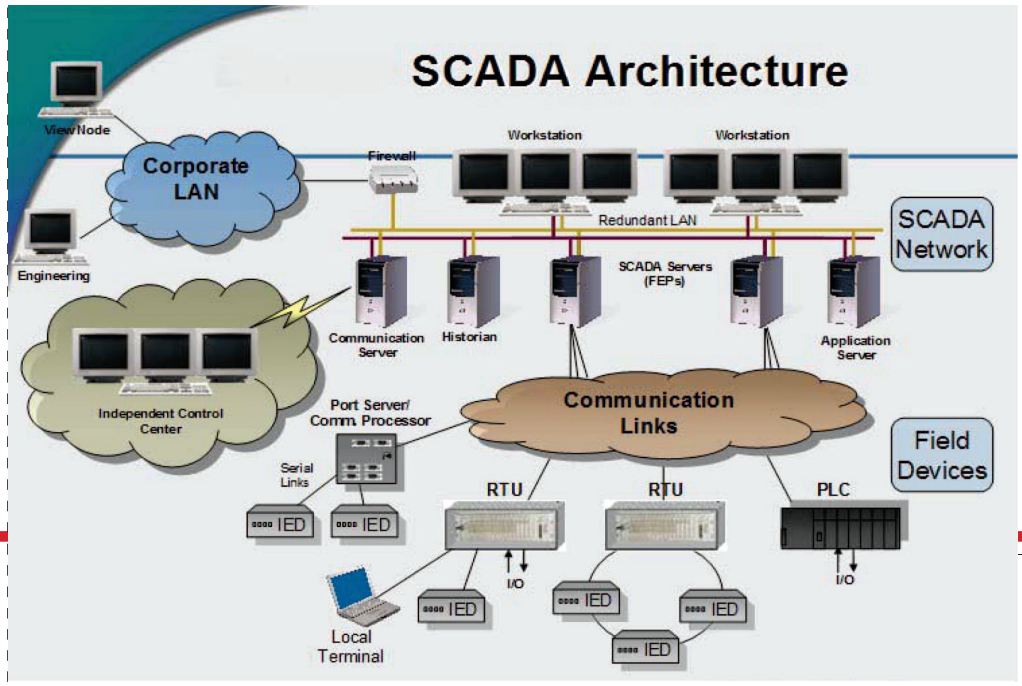
پیدایش SCADA

(Supervisory Control And Data Acquisition) SCADA به معنای کنترل نظارتی و دستیابی به اطلاعات است. با گسترش سامانه های رایانه ای، استفاده از SCADA جهت نظارت بر شبکه ی برق، توسعه ی چشمگیری یافت. سامانه های مدیریت شبکه ی برق از اواخر دهه ی ۱۹۷۰ جهت تحلیل رفتار شبکه ی برق، نظارت بر قابلیت اطمینان سامانه و برنامه ریزی تولید نیروگاه ها به کار گرفته شدند.

تا اواسط دهه ی ۱۹۹۰میلادی، عمدتاً شرکت های برق کشورهای مختلف مبادرت به خرید و راه اندازی سامانه ی جامع اتوماسیون و دیسپاچینگ برق به صورت یک سامانه ی یکپارچه شامل پایانه های راه‌دور (RTU)، سامانه ی مخابراتی، تجهیزات مرکز کنترل، نرم‌افزار اسکادا و نرم‌افزارهای کاربردی قدرت برای شبکه های تولید و انتقال می کردند.

در واقع این سامانه ها صرفاً کنترلی نیستند، بلکه بر سطح نظارتی نیز احاطه دارند و SCADA مجموعه ای نرم‌افزاری است که به همراه کنترل کننده های صنعتی نظیر PLCها و سایر ماژول های سخت‌افزاری عملیات کنترل نظارتی و داده‌برداری را در فرایندهای شیمیایی، حمل و نقل، نیروگاه های اتمی، سیستم های آبرسانی شهری، کنترل تولید و توزیع انرژی الکتریکی و در خطوط نفت و گاز و سایر فرایندهای گسترده و توزیع یافته استفاده می شود، حتی در شبکه‌های آبیاری و نیز به منظور جمع آوری اطلاعات، کنترل و نمایش وضعیت جایگاه های سوخت رسانی گاز طبیعی CNG کاربرد دارد و شامل فرایندهای زیر است :

- جمع آوری اطلاعات.
- انجام آنالیزها و کنترل های مورد نیاز.



- نشان دادن اطلاعات بر روی صفحات نمایش بهره برداران و گزارش گیری از آنها.
- ارسال اعمال کنترلی مورد نیاز به فرایند.

تهدیدات سامانه های کنترل صنعتی

استفاده بیش از پیش سیستم های کنترل صنعتی و همچنین ساده انگاری مقوله امنیت در اینگونه سامانه ها و نیز بهره گیری از این سیستم در فضاهای مهم در همه کشورها باعث شده تا مهاجمین سایبری توجه زیادی به این مجموعه ها داشته باشند. کنترل کننده های منطقی برنامه پذیر(PLC)، سامانه های کنترل توزیع شده (DSC) و پروتکل های ارتباط در شبکه های سامانه های کنترل صنعتی و اسکادا عمدتاً با تمرکز بر قابلیت اطمینان و سادگی رفع مشکلات شان طراحی شده اند و امنیت در آن ها کم تر مورد توجه بوده است و به راحتی در مقابل حملات سایبری آسیب پذیر هستند که نیاز به وصله شدن دارد. این محصولات عموماً دارای ۱۰۰۰ تا ۵۰۰۰ خط کد سفت افزاری[1] هستند.

انگیزه مهاجمین

واضح است که انگیزه ی مهاجمین تنها ایجاد اختلال و خسارت رساندن به زیرساخت های انرژی قربانیان نیست و آن ها به دنبال کسب اطلاعات و جزییات دقیق شبکه و تجهیزات قربانیان نیز هستند، تا در فرصت های بعدی با پیچیده تر کردن مولفه های بدافزار، کنترل کامل سامانه های کنترل صنعتی و اسکادای قربانی را به دست بگیرند.

دستاوردهای مهاجمین در برخی حملاتی که صورت داده اند

- نفوذ به اطلاعات
- تغییر سرعت خنک کننده سی پی یو
- دسترسی به رابط کاربری ماشین و انسان (HMI)[2]
- تغییرات در Modbus[3]
- تغییر فشار پمپ
- تغییر در دمای خروجی
- تغییر در سامانه ی پمپ

حملات شناخته شده علیه اسکادا

استاکس نت

در سال ۲۰۱۰(تیرماه ۱۳۸۹)، بدافزار استاکس نت که به عنوان اولین بدافزار در شروع حملات سایبری شناخته می شود با موفقیت توانست به شبکه های ایزوله یا gapped-air نفوذ کند و باعث اختلال در فرآیندهای صنعتی شود. این کرم مخرب، از روش های مختلفی برای انتشار استفاده می کرد که معروف ترین روش آن از طریق USB بوده است.

وزیر ارتباطات ایران در آبان ۱۳۸۹ در این خصوص اعلام نمود که منشاء ورود این ویروس به ایران نه از طریق شبکه اینترنت بلکه از طریق حافظه های جانبی بوده که افرادی از خارج از کشور به ایران آورده و بدون بررسی لازم به کامپیوترهای در داخل ایران متصل کرده اند.

هدف:

بنابر اظهارنظر کارشناسان سیمانتک، این بدافزار سیستم هایی را هدف قرار داده است که دارای یک مبدل فرکانس هستند که نوعی دستگاه برای کنترل سرعت موتور است. استاکس نت به دنبال این دستگاه ها بر روی سیستم قربانی می گردد و فرکانسی (بازه ای از ۸۰۰ تا ۱۲۰۰ هرتز) را که دستگاه های مذکور با آن کار می کنند شناسایی می کند. دستگاه های صنعتی که از این مبدل استفاده می کنند بسیار محدود هستند و غالباً در تاسیسات غنی سازی اورانیوم استفاده می شوند. این بدافزار فرکانس های مبدل را ابتدا تا بیشتر از ۱۴۰۰ هرتز بالا می برد و سپس آن را تا کمتر از ۲ هرتز پایین می آورد و سپس آن را فقط برای بالاتر از ۱۰۰۰ هرتز تنظیم می کند. در اصل، این بدافزار سرعتی را که موتور با آن کار می کند، به هم می ریزد. از این طریق کیفیت محصول پایین می آید و یا اینکه اصلا تولید نمی شود، مثلاً تاسیسات غنی سازی نمی توانند به درستی اورانیوم را غنی سازی کند و همچنین منجر به خرابی موتور به صورت فیزیکی می شود.

بدافزار هاوکس

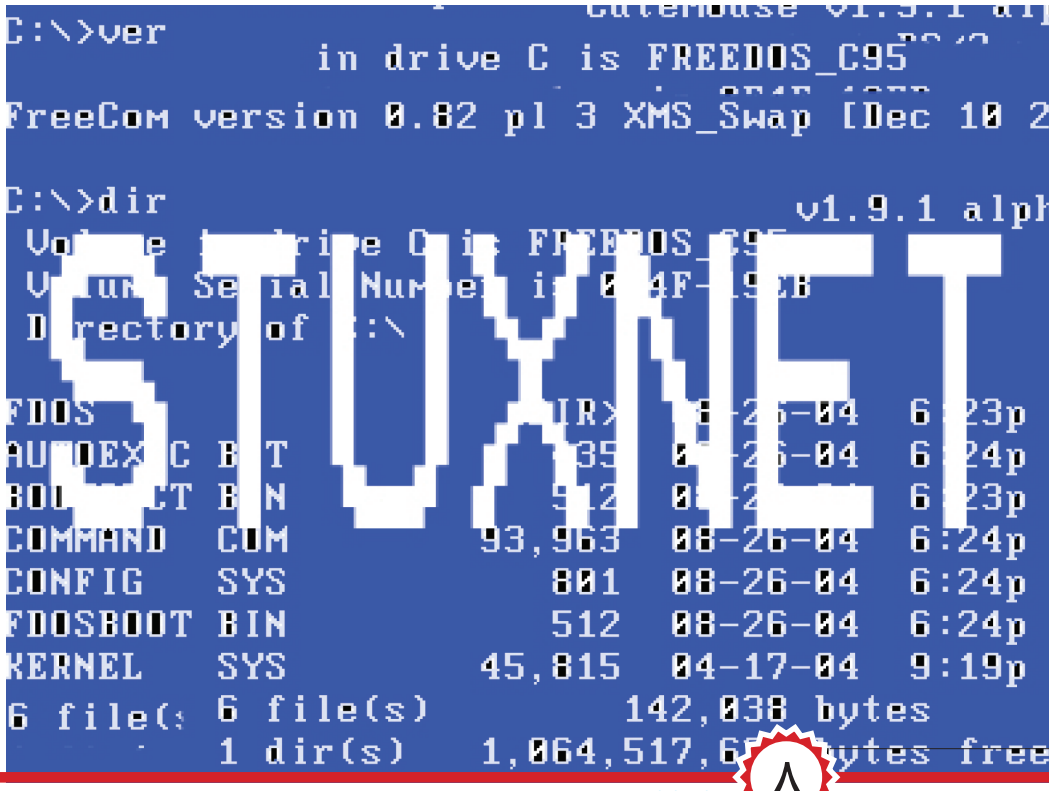
بدافزار هاوکس نیز درست مانند کرم واره ی استاکس نت، به نحوی طراحی شده است که نرم افزارهای اسکادا و سامانه های کنترل صنعتی را هدف قرار دهد و این بدافزار قابلیت حمله به سدهای برق آبی، سایت نیروگاه های هسته ای و حتی حمله به تاسیسات برق یک کشور تنها با یک کلید را داراست. از این بدافزار در برخی از حملات سایبری علیه زیرساخت های انرژی اروپا مورد استفاده قرار گرفته شد.

مهاجمین از سه شیوه ی مهم (که دو روش اول نسبتا مرسوم و روش سوم بسیار خلاقانه است) برای آلوده کردن قربانیان استفاده کرده اند:

- سوء استفاده از آسیب پذیری های موجود در ماشین آلات و نرم افزارهای قربانیان.
- ارسال هرزنامه های همراه با بدافزار.
- نفوذ به وب گاه های منتشر کننده ی نرم افزار و سفت افزارهای کنترل صنعتی و اسکادا، تا قربانیان نسخه های آلوده را از وب گاه دانلود کنند.

BlackEnergy

از سال ۲۰۱۱ میلادی، بسیاری از شرکت هایی که از



سامانه های کنترل صنعتی استفاده می کنند و به اینترنت متصل هستند، مورد حمله بدافزاری به نام Blackenergy قرار گرفته اند که با ایجاد یک درب مخفی (Backdoor) دسترسی غیرمجاز به سیستم ها و ماشین های صنعتی داشته اند. چندین شرکت صنعتی ، بدافزار Blackenergy را بر روی نرم افزار کاربردی HMI در سامانه های کنترل صنعتی متصل به اینترنت خود یافته و شناسایی کرده اند.

Regin

و حالا رجین «Regin» که چندی نیست کشف شده است، نه دقیقاً برای جاسوسی در سیستم های کنترل صنعتی بلکه با هدف پایش و جمع آوری اطلاعات در مراکز مخابراتی، ISPها،صنایع خطوط هوایی، بیمارستان هاو... به طور مخفیانه فعالیت کرده است. هر چند تاریخ شروع فعالیت این بدافزار و بازه های مختلف زمانی آن دقیق مشخص نیست ولی مهم آن است که بدون اینکه ما متوجه شویم، این ویروس با یک روش فوق العاده پیچیده ارتباط با مرکز فرماندهی خود برقرار کرده و حتی می تواند از صفحه کامپیوتر قربانیان اسکرین شات تهیه کند، صفحه کلید را کنترل و حتی اطلاعات حذف شده را بازسازی کند.

برخی کاستی‌های موجود در سیستم های کنترل صنعتی و SCADA که در نهایت منجر به آسیب پذیری می شود:

- بسیاری از پروتکل هایی که در سیستم های اسکادا و زیرمجموعه های آن استفاده می شود از رمزنگاری برای ارسال داده ها استفاده نمی کنند.
- آموزش ها و آگاهی های امنیتی در این زمینه محدود است.
- استفاده از ضد ویروس ها در این سیستم ها به دلیل الزام آنها بر بلادرنگ بودن بسیارسخت است.
- تست نفوذپذیری به صورت روتین انجام نمی شود و می بایست با دقت بسیار بالا صورت پذیرد.
- به روزکردن وصله های امنیتی روی این سیستم ها باید با دقت بالا و معمولاً با حضور تامین کننده سیستم ها و فروشندگان مربوطه انجام شود.
- اطلاعات از دست رفته بازیابی نمی شوند و این امر می تواند منجر به وقایع بسیار خطرناک شود.
- نیاز به پاسخ دهی بلادرنگ دارد و تاخیر در این سیستم ها قابل اصلاح نیست.
- سیستم ها همیشه باید پشتیبان داشته باشند زیرا باز ایستادن سیستم ها از فعالیت می تواند خطرات جبران ناپذیری به همراه داشته باشد.

توصیه های Wilhoit Kyle (پژوهشگر امنیتی شرکت ترندمیکرو) برای ایمن نگاه داشتن سامانه :

- قفل کردن درگاه های USB
- اعمال احراز هویت دومرحله ای در همه سامانه ها.
- غیرفعال کردن دسترسی به اینترنت در منابع.
- همواره آخرین وصله ها را به تجهیزات و سامانه های اعمال شود.
- استفاده از تقسیم بندی شبکه (مثلاً «WLAN» و «SCADA»).
- استفاده از TLs/SSL برای تمامی ارتباطات در سامانه های کنترل صنعتی مبتنی بر وب. (البته با در نظر گرفتن نکات مرتبط با آسیب‌پذیری جدید پروتکل SSLv[3] به نام POODLE)
- افزایش امکانات گزارش گیری در این محیط ها.
- یک مدل تهدید برای سازمان خود توسعه دهید تا دریابید چه کسی و چرا به آن حمله می کند. (مانند استفاده از Honeypot[4])
- استفاده از حفاظت بلادرنگ.
- طبقه بندی داده و دارایی.
- کنترل دسترسی پیمانکار: شبکه های کنترل صنعتی از پیمان کاران راه دور استفاده می کنند؛ کنترل دستیابی آن ها به منابع بسیار مهم و ضروری است.

نتیجه:

بنا بر روند قبل از این و پیش رو، تهدیدات بسیار پیشرفته تر در این حوزه انتظار می رود. هرچند که بیشتر مواقع هکرها و مهاجمین سایبری یک پله جلوتر از ما هستند ولی شاید بالا بردن دانش امنیت حوزه IT و همچنین دقت بیشتر در این مقوله و تبعیت از فرهنگ پیشگیری بهتر از درمان، راهی به سوی پایین آوردن آسیب باشد.

منابع :

1. http://news.asis.io
2. Kyle Wilhoit (Trend Micro Forward-Looking-Threat Research Team)
3. https://www.owasp.org/index.php/OWASP_Scada_Security_Project
4. http://www.f-secure.com
5. http://threatpost.com
6. https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B
7. http://www.kaspersky.com/about/news/virus/2014/Regin

1 - Firmware

۲ - HMI (Machine Interface-Human) : نوعی نرم افزار است که یک صفحه رابط گرافیکی برای مدیریت و کنترل ماشین های صنعتی در اختیار کاربر می گذارد.

۳ - MODBUS یک پروتکل ارتباطی سریال است که برای استفاده در کنترل کننده های منطقی قابل برنامه ریزی (PLC) به کار می رود.

۴ - Honeypot یک منبع سامانه ی اطلاعاتی با اطلاعات کاذب است که برای مقابله با رخنه گران و کشف و جمع آوری فعالیت های غیرمجاز در شبکه های رایانه ای بر روی شبکه قرار می گیرد.

تلفن‌های همراه و خطر ابتلا به سرطان

ایرج ارقند

از زمان پیدایش تلفن های همراه و به موازات آن رشد در علوم پزشکی نوین، چالش بررسی تاثیرات سیستم های بی سیم روی سلامتی انسان همواره مطرح بوده است. روزانه بیش از ۸۰درصد مردم جهان ساعت ها از تلفن همراه خود استفاده می نمایند. در سال ۲۰۱۱ بیش از ۵ میلیارد [۱]مشترک تلفن همراه در جهان ثبت شد که هر روز بر این تعداد افزوده می شود. حال این سوال مطرح است که آیا تلفن همراه و ابتلا به تومورهای سرطانی ارتباطی با یکدیگر دارند؟ یا این مطلب تبلیغ بوده و تنها یک بازی رسانه‌ای است؟ تا چه حد می توان به این تکنولوژی اعتماد نمود؟ آیا راهکاری جهت کاهش تاثیر منفی تلفن های همراه وجود دارد؟

در ارتباط بی سیم، موبایل ها، تبلت ها و تلفن های بی سیم خانگی و صنعتی جهت برقراری ارتباط از سطوح پایین فرکانس های مایکروویو استفاده می کنند که از این فرکانس ها به طور مشابه جهت گرم کردن و پختن غذا در اجاق های مایکروفر نیز استفاده می شود [۲].در راستای تحلیل خوب یا بد بودن تلفن های همراه به طور کلی دو نظریه وجود دارد:

۱- تلفن های همراه مضر هستند زیرا:

- آنها امواج الکترومغناطیس را منتشر می کنند.
- گرما تولید می کنند.
- کاربر استفاده کننده از تلفن همراه یک منبع تولید امواج الکترومغناطیس را در مجاورت سر یا بدن خود قرار می دهد.
- ادعا شده است که در سال های اخیر بیماران مبتلا به سرطان مغز با تومورهایی به اندازه هایی دقیقاً مشابه ابعاد تلفن های همراه و با مرکز تومور دقیقاً در جایی که آنتن های آنها قرار دارد مشاهده شده اند.

۲- تلفن ها همراه ایمن هستند زیرا:

- تلفن های همراه با توان بسیار پایین کار می کنند و این توان پایین موجب می شود که هیچ تاثیر منفی در سلامتی انسان نداشته باشند.
- به جهت غیریونیزه بودن انرژی شان، نمی توانند آثار بیولوژیکی منفی روی انسان ایجاد کنند.
- روزانه میلیاردها انسان از تلفن همراه استفاده می کنند و اگر قرار بر تاثیر منفی آنها باشد باید این امر در بسیاری از مردم مشاهده شود.

گزارش برخی مطالعات و گزارش های انجام شده در سال‌های اخیر با برداشت از مقالات معتبر به شرح زیر است:

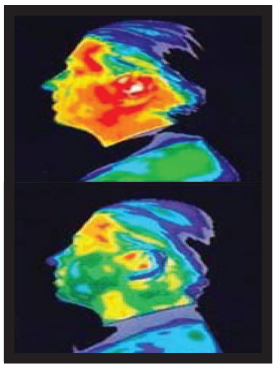
۱- در ۳۱ می ۲۰۱۱، سازمان بهداشت جهانی (WHO)[۱] اعلام نمود در هیچ تحقیق معتبری ثابت نشده است که تلفن های همراه می توانند به خودی خود موجب ابتلا به سرطان شده و در یک گزارش آماری نشان داد تاثیر آنها بر سلامتی انسان از مواردی مانند سرب ناشی از احتراق مواد سوختی خودروها و آلاینده های زیست محیطی به مراتب کمتر است. ولی درکنار آن راهکارهایی را برای کاهش خطرات ناشی از تلفن های همراه پیشنهاد نمود [۳].

۲- در ۲۱ اکتبر ۲۰۱۱ نتایج بزرگترین مطالعات انسانی برای بررسی تاثیر تلفن همراه و سرطان که روی ۳۵۸ هزار نفر به مدت ۱۳ سال در دانمارک انجام شد نشان داد که هیچ ارتباط مستقیمی ثابت شده‌ای در این دو مقوله وجود نداشته و با رعایت نکات ایمنی و بهره گیری از تلفن های همراه استاندارد می توان به این تکنولوژی اعتماد نمود [۴].

۳- در مقابل این تحقیقات در ۲۲ فوریه ۲۰۱۱ و پیش از آن در ۱۷ می ۲۰۱۰ فاکس نیوز و بخش تحقیقات سلامت WHO گزارشی ارائه نمودند که استفاده از تلفن همراه برای مدت های زمانی ۵۰ و حتی ۳۰ دقیقه به طور مداوم می تواند فعالیت مغز خصوصاً در نقاط نزدیک به آنتن تلفن همراه را کاملاً تغییر دهد. این تحقیقات با بهره گیری از اسکن های مغزی روی چندین گروه سنی انجام شد که بخشی از آن ارائه می شود.

تاثیر فرکانس‌های رادیویی در بدن انسان

انرژی یک فرکانس رادیویی به صورت تابش الکترومغناطیس است. تابش الکترومغناطیس را می توان به دو نوع: یونیزه[۲] (به عنوان مثال: اشعه x، رادون[۳] و پرتوهای کیهانی[۴]) و غیریونیزه (به عنوان مثال: فرکانس رادیویی، فرکانس های خیلی پایین یا فرکانس قدرت) تقسیم بندی کرد. قرار گرفتن در معرض پرتوهای یونیزه (جهت درمان برخی سرطان ها) مانند اشعه درمانی و پرتو درمانی و تاثیر آن در ایجاد تومورهای دیگر قابل پذیرش است. ولی در خصوص فرکانس های رادیویی تنها اثر بیولوژیکی شناخته شده گرم شدن بافت است. اینکه استفاده از تلفن همراه در مجاورت سر می تواند موجب گرم شدن، تغییر در متابولیزه شدن و استفاده از گلوکز بیشتر در مغز شود به طور قطع مورد پذیرش است[۵]اما اینکه تاثیر آن به طور مستقیم بتواند موجب ایجاد تومورهای سرطانی شود تاکنون ثابت نشده است. شکل ۱ تصویرپایین مقدار گرمای بافت سر انسان بدون حضور میدان الکترومغناطیس و در شکل بالا با وجود میدان الکترومغناطیس نشان داده است. بخش های گرم شده خصوصاً در نقاط حساس برای سطوح نازک پوست در شکل فوق کاملاً مشخص می باشد. احساس خستگی، کرخت شدن بافت و گاهی سردرد نتیجه گرم شدن ناشی از امواج فرکانس مایکروویو روی بافت سر است.



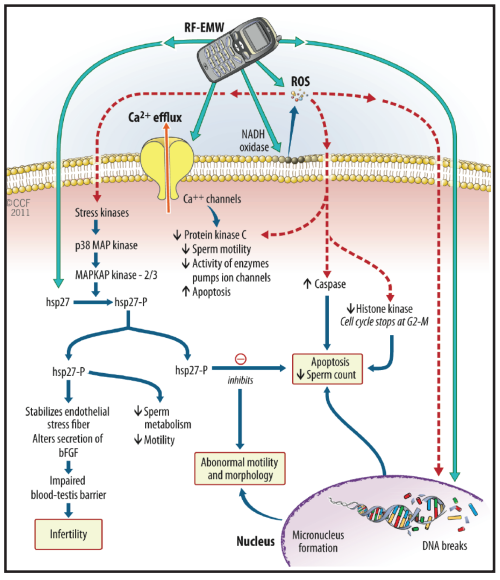
شکل۱: گرم شدن بافت سر بدون میدان الکترومغناطیس (تصویر پایین) و با حضور آن (تصویر بالا)

بدن انسان جهت انجام عملکرد روزانه خود همواره جریان های کوچک الکتریکی را تولید می کند که نتیجه واکنش های شیمیایی خصوصاً در مغز و ضربان قلب هستند. این جریان های کوچک حتی در غیاب میدان الکتریکی خارجی نیز وجود داشته به طوری که از این پارامتر جهت شناسایی عملکرد صحیح قلب و مغز انسان استفاده می شود. اگر بدن انسان در معرض میدان الکتریکی و خصوصاً مغناطیسی خارجی با فرکانس پایین (مانند خطوط انتقال) قرار گیرد، این میدان ها به طور مستقیم وارد جریان خون شده، توزیع بار الکتریکی سلول ها را برهم زده و در نهایت موجب مرگ سلولی می گردند. هرچقدر قدرت این میدان بیشتر باشد، تاثیر آن نیز بیشتر است. به همین جهت در تمام محیط های نزدیک خطوط انتقال قدرت به شدت توصیه می گردد که فاصله محل سکونت تا خطوط برق رعایت شود. برخی تحقیقات نشان داده اند که علاوه بر اثر گرمایی امواج تلفن همراه باید از نگاه تخصصی تر تاثیرات منفی سیگنال های موبایل بررسی شوند. برای مثال نتیجه تحقیقات در گروه بیوشیمی و زیست شناسی مولکولی پزشکی در فرانسه نشان داده است که سیگنالهای موبایل با فرکانس ۹۰۰مگاهرتز GSM می تواند در سیستم هورمون آدرنالین و هیپوفیز مردان تا مقدار ۲۸٪ تاثیر منفی بگذارند[۶]. همچنین تاثیر فرکانس های موبایل در ایمپلنت های استفاده شده در بدن انسان و خصوصاً پیسمیکرهای[۵] موقت قلبی نیز یک امر شناخته شده بوده که سیگنال های تلفن همراه با تحریک و ارسال پالس های ناخواسته موجب از دست رفتن ریتم منظم پیسمیکر شده و در بسیاری موارد به طور کامل اثربخشی خود را در موارد اضطراری افت ضربان قلب فرد بیمار

از دست می دهند. به همین جهت توصیه می شود که بیماران دارای پیسمیکر هرگز از تلفن همراه استفاده نکنند.

بدن انسان مشابه یک آنتن با عملکرد خوب در فرکانس های رادیویی عمل می کند. شاید تجربه کرده باشید که وقتی صفحه نمایش تلویزیون واضح نبوده یا رادیو در پخش صدا دچار مشکل است، با دست زدن به آنتن عملکرد آن درست شده و به محض رها کردن مجددا به وضعیت قبلی خود بازمی گردد. دلیل این امر بهبود آنتن دهی تلویزیون یا رادیو در تماس با بدن انسان می باشد. حال این سوال مطرح است که آیا تاثیر منفی علاوه بر گرم شدن بافت بدن نیز وجود دارد؟ جریان های متناوب القا شده در بدن انسان که بیشتر ناشی از تاثیر بخش مغناطیسی است یکی از نشانه های پنهان در بدن می باشد. نمونه ای از این تاثیرها در شکل ۳ نشان داده شده است. تغییر پتانسیل پلاسما و کاهش کلسیم که موجب افت فعالیت پروتئین Kinase C (PKC) در بدن شده که نتیجه آن کاهش آنزیم ها و یون ها را به همراه دارد. از هم گسیختگی سلولی، شکافت DNA، تغییر در فرم آن، تغییر در تعداد و شکل اسپرم های مردانه از دیگر عوارض غیرگرمایی تلفن های همراه است.

شکل ۲: عوارض منفی غیر گرمایی میدان های ناشی از تلفن همراه در بدن انسان

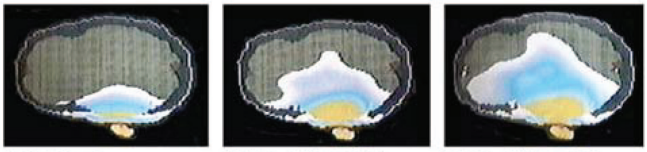


حال این سوال مطرح است که با توجه به تمام این خطرات باید این تکنولوژی را کاملاً فراموش نمود؟ آیا راهی برای کاهش این خطرات وجود دارد؟ چطور می توان بدن خود را کمتر در معرض این تشعشعات قرار داد؟

۱۰ روش جهت کاهش احتمال خطر ابتلا به سرطان ناشی از تلفن همراه

۱- کودکان، تنها و تنها در مواقع اضطراری از موبایل استفاده کنند. به جهت نازک بودن جمجمه کودکان نسبت به افراد بالغ و در حال رشد بودن مغزشان، تابش امواج با قدرت و تاثیر بیشتری روی سلول های مغزیشان تاثیر خواهد داشت. دور نگه داشتن تلفن همراه یا استفاده از بلندگو می تواند یک راهکار مناسب برای حل این مشکل باشد. در شکل ۴ میزان نفوذ میدان الکترومغناطیس ناشی از تلفن همراه در فرکانس ۱۹۰۰ مگاهرتز با استفاده از اسکن دمایی مغز برای یک کودک ۵ ساله در مقایسه با یک فرد ۱۰ ساله و یک انسان بالغ نشان داده شده است. با توجه به شکل مشخص است که تاثیرات منفی میدان ها و گرم شدن بافت مغز در یک کودک ۵ ساله بسیار بیشتر از یک انسان بالغ است.

شکل ۳: نفوذپذیری میدان الکترومغناطیس ناشی از موبایل در کودک در مقایسه با انسان بالغ



۲- تا حد ممکن سعی کنید در هنگام صحبت کردن گوشی موبایل را از بدن خود دور نگهدارید. دامنه میدان الکترومغناطیس در فاصله ۵ سانتیمتر به یک چهارم و در فاصله حدود ۹۱ سانتیمتر تا ۵۰ برابر کاهش خواهد یافت. استفاده از هدفون های غیربی سیم می تواند به این مهم کمک نماید. یک تلفن بی سیم غیر استاندارد در صورتی که در مجاورت بدن و روی گوش قرار گیرد می تواند تاثیرات منفی در بافت انسان به اندازه بیشتر از تلفن همراه ایجاد نماید.

۳- هنگامی که آنتن دهی موبایل در سطح پایین بوده یا در حال حرکت با سرعت بالا مانند حرکت با خودرو در اتوبان یا قطار هستید هرگز از تلفن همراه استفاده نکنید. در این حالات تلفن همراه به دلیل کاهش سطح سیگنال خود (خصوصاً در سیستم های نسل سوم[6]) سعی می کند با ارسال توان بیشتر این کاهش سیگنال را جبران نماید و متعاقباً تاثیر میدان های الکترومغناطیس بیشتر خواهد بود.

۴- سعی نکنید در تمام طول روز تلفن همراه خود را در مجاورت بدن خود قرار دهید. عادت به قراردادن تلفن همراه در هر زمان که در مکان ثابتی هستید برای مثال روی میز در محل کار، روی پیشخوان خودرو هنگام رانندگی یا مسافرت یا در منزل در مکانی دور از دسترس کودکان می تواند به این امر کمک کند. هرگز و هرگز در هنگام خواب تلفن همراه را زیر بالش یا در نزدیکی بدن قرار ندهید.

۵- یک نکته مهم: اگر مجبور هستید تلفن همراه را با خود حمل کنید، مطمئن شوید که به نحوی در جیب یا کیف موبایل قرار گرفته است که قسمت صفحه کلید به سمت بدن و پشت آن به سمت خارج قرار دارد. این امر به دلیل قرارگیری آنتن تلفن های همراه در پشت آنها بسیار موثر است. نحوه اشتباه قراردادن تلفن همراه در جیب در شکل ۴ نشان داده شده است.

شکل ۴: نحوه اشتباه قراردادن تلفن همراه در جیب

۶- تاثیر بیولوژیک میدان های الکترومغناطیس رابطه مستقیم با مدت زمان بهره گیری از بیشترین توان را دارد. سعی کنید تا حد امکان از تلفن همراه برای مکالمات کوتاه مدت استفاده کنید و در صورت نیاز به مکالمه طولانی از تلفن های ثابت آن هم از نوع سیمی (نه بی سیم[7]) استفاده کنید.

۷- هنگام ایجاد یک تماس جدید، پس از شماره گیری، صبر کنید تا طرف مقابل به تماس شما پاسخ داده و سپس تلفن همراه را در مجاورت گوش خود قرار دهید. در هنگام ارتباط اولیه بیشترین توان از گوشی ساطع می شود.

۸- اگر امکان دارد برای موارد کوتاه یا ارسال خبر و غیره از سرویس های پیام کوتاه به جای تماس مستقیم استفاده کنید.

۹- در مکان های عمومی مانند اتوبوس تا حد امکان از تلفن همراه خود استفاده نکنید تا دیگران نیز از ضررهای آن در امان باشند. تصور کنید در یک اتوبوس شهری تمام افراد از تلفن همراه خود به طور همزمان استفاده کنند، در این صورت پوش میدان الکترومغناطیس در یک فضای بسته بسیار زیاد شده و تاثیر آن چندین برابر خواهد شد.

۱۰- تاکید می شود که از تلفن همراه با نرخ جذب ویژه (SAR[8]) کم استفاده کنید.

[1]http://www.ehso.com/ehso2.php
[2] http://hyperphysics.phy-astr.gsu.edu/hbase/waves/mwoven.html.
[3] IARC classifies radiofrequency electromagnetic fields as possibly carcinogenic to humans, International Agency for Research of Cancer, 31 May 2011.
[4]http://www.ehso.com/ehso2
[5] Volkow ND, Tomasi D, Wang GJ, et al. Effects of cell phone radiofrequency signal exposure on brain glucose metabolism. JAMA 2011; 305(8):808–813.
[6] Djeridane Y, Touitou Y, de Seze R. Influence of electromagnetic fields emitted by GSM-900 cellular telephones on the circadian patterns of gonadal, adrenal and pituitary hormones in men. Radiat Res, 2008;169(3):337-43.

1.World Health Organization
2. Ionizing
3. Radon
4.cosmic rays
5. pacemakers
6. 3G
7. cordless phone
8. Specific Absorption Rate

بازرسی خدمات پس از فروش

بخش بازرسی خدمات پس از فروش مرکز تحقیقات صنایع انفورماتیک به عنوان بازوی اجرایی سازمان حمایت از مصرف کنندگان و تولید کنندگان با داشتن پروانه ISO 17020 بازرسی از سازمان ملی استاندارد ایران و گواهینامه از مرکز ملی تایید صلاحیت ایران نسبت به انجام موارد زیر اقدام می کند:

۱- ارزیابی شرکت های ارائه دهنده خدمات پس از فروش
۲- ارائه مشاوره جهت استقرار و طراحی سیستم برای مراکز خدمات پس از فروش
۳- برگزاری دوره های آموزشی در خصوص ارتقاء دانش فنی خدمات پس از فروش

شاخص های اصلی ارزیابی خدمات پس از فروش

۱- کیفیت خدمات
۲- سرعت خدمات
۳- هزینه خدمات
۴- نتیجه عملکرد

www.rcii.ir

RCII مرکز تحقیقات صنایع انفورماتیک
دفتر مرکزی و آزمایشگاه تهران: خیابان کریمخان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر، پلاک ۳، صندوق پستی: ۱۵۸۷۵/۳۴۸۵
تلفن: ۸۸۹۲۵۹۵(۱۰خط) فکس: ۸۸۹۳۷۶۵۸

مجتمع آزمایشگاهی اداره کل استاندارد و تحقیقات صنعتی استان هرمزگان مستقر در اسکله شهید رجایی
تلفن: ۴۵۱۴۲۵۹(۰۷۶۱) فاکس: ۴۵۱۴۲۵۸(۰۷۶۱)
آزمایشگاه شهرک صنعتی پرند:
شهرک صنعتی پرند،بلوار فناوری، خیابان گلزار، خیابان گلگشت
قطعه D44 تلفن: ۵-۵۶۴۱۸۸۶۴