فصلنامه مرکز تحقیقات صنایع انفورماتیک / دوره جدید / شماره ۱۴ / بهار ۱۳۹۲

www.rcii.ir

گزارش صنایع انفورماتیک

RCII

نقش نظارتی و سیاست گذاری دولت در اقتصاد

در گفتگو باحسین رفعتی مطرح شد:

سال حمایت از تولید ملی فرصتی که از دست رفت

آزمایشگاه ارزیابی کیفیت محصولات نرم افزاری تحت وب مرکز تحقیقات صنایع انفورماتیک راه‌اندازی شد

مقاله

هوش امنیتی

به نام خداوند بخشنده مهربان

یادداشت نخست

به قلم مدیر مسئول

نقش نظارتی و سیاست‌گذاری دولت در اقتصاد کشور

یکی از بزرگترین مشکلات در تصمیم گیری برخی مدیران دولتی، بحث افراط و تفریط است و یکی از بارزترین مصداق های آن را می توان در تصویب و ابلاغ آیین نامه ها و ارائه مجوزهای تاسیس و بهره برداری و تایید صلاحیت مشاهده کرد. همه مدیران محترم دولتی اذعان می کنند که برای نجات اقتصاد کشور از بحران کنونی، دولت باید نقش برنامه ریزی کلان و نظارت را برعهده گیرد و تصدی را به بخش خصوصی واگذار کند.

نظارت و برنامه ریزی یعنی چه؟ آیا غیر از این است که مزیت های رقابتی ملی خود را بشناسیم، برای حضور سرمایه گذاران در زمینه هایی که کشور در سطح منطقه ای یا ملی در آن فعالیت ها دارای شایستگی است، مشوق های لازم را طراحی کنیم، با هدایت صحیح سرمایه گذاران و متخصصان، از ائتلاف سرمایه ملی جلوگیری کنیم و شرایط را برای یک رقابت سالم و کامل مهیا سازیم؟

مروری بر تصمیمات اتخاذ شده در سه دهه اخیر نمایان گر آن است که در موارد بسیاری علاوه بر آنکه هدایت صحیح سرمایه گذاران و متخصصان، صورت نگرفته و این امر موجب اتلاف سرمایه ملی شده است، بعضاً آیین نامه ها و دستورالعمل هایی تصویب و ابلاغ شده که خود باعث سردرگمی مجریان و پاک کردن صورت مسئله شده است.

ارائه موافقت اصولی و پروانه بهره برداری به تعداد زیادی شرکت تولیدی در یک صنعت خاص، بدون درنظر گرفتن شرایط کشور در آن صنعت و وضعیت تقاضای بالفعل و بالقوه داخلی و خارجی، باعث شد تا بسیاری از شرکت های تولیدی ورشکسته شده و سرمایه بدون بازیافت آنها تلف شود، به عبارتی سرمایه ملی تلف شود.

برای رونق کسب و کار، بدون بررسی اصولی طرح های توجیهی و پایش فعالیت متقاضیان، مجوز صادر شده و تسهیلات در اختیار ایشان قرار گرفته و پس از مدتی با توجیه اینکه نتیجه مناسبی حاصل نشده به یکباره کل طرح منتفی شده است. همین مشکل برای شرکت های دانش بنیان در حال تکرار است و باز شاهد خواهیم بود که بدون برنامه ریزی صحیح و کلان سرمایه ی ملی به هدر خواهد رفت.

امروز مجددا شاهد آن هستیم که سازمان ها، با هدف حمایت از استاندارد و کیفیت، بدون بررسی توان مالی و تخصصی متقاضی و وضعیت تقاضای بالفعل و بالقوه داخلی، نسبت به صدور مجوز فعالیت برای آزمایشگاه ها اقدام می کنند یا بدون درنظر گرفتن توجیه فنی و اقتصادی، آزمایشگاه ها را برای ورود به فعالیت های جدید تشویق می نمایند.

امید است مدیران محترم دولتی با اتکاء به تجربیات قبلی، بررسی مشکلات فعلی بنگاه های اقتصادی، الگوبرداری از مدل های موفق برنامه ریزی و توسعه در کشورهای صنعتی، به گونه ای اثربخش تصمیم سازی و تصمیم گیری کنند و به دور از آمار کمی در دوره مدیریت خود، به کیفیت انجام کارها و ایجاد زیرساخت های لازم بیاندیشند تا شاهد رشد و شکوفایی هرچه بیشتر اقتصاد کشور باشیم.

گزارش صنایع انفورماتیک

فصلنامه مرکز تحقیقات صنایع انفورماتیک

دوره جدید / شماره۱۴ / بهار ۱۳۹۲

صاحب امتیاز: مرکز تحقیقات صنایع انفورماتیک

مدیر مسئول: ویدا سینا

مدیر اجرایی: افسانه عبادی

مدیرفنی: رامین رضایی

روابط عمومی: سمانه کیومرثی

همکاران این شماره: صفا رحیمیان / حمید شریفی / مهری یحیایی / ساناز خلیلی / محمد امین صابریان /

نشانی: تهران، خیابان کریم خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر،پلاک۳

تلفن: ۸۸۹۲۵۹۵۰ (۱۰خط)

فکس: ۸۸۹۳۷۶۵۸

سایت : www.rcii.ir

مجری طرح فصلنامه:گروه رسانه‌ای مهرتابان/۰۹۱۲۳۰۸۹۳۰۳

[akbarkarimi40@yahoo.com]

نشانی آزمایشگاه‌ها:

آزمایشگاه مرکزی: تهران، خیابان کریم خان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر،پلاک۳

تلفن: ۸۸۹۲۵۹۵۰ (۱۰خط) **فکس:** ۸۸۹۳۷۶۵۸

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

تلفن: ۰۷۶۱۴۵۱۴۲۵۹ فکس:۰۷۶۱۴۵۱۴۲۵۸

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

تلفکس:۵۶۴۱۸۸۹۲-۵۶۴۱۸۸۶۴-۵۶۴۱۸۸۶۵

صنعت انفورماتیک تفاوت عمده ای با صنایع دیگر دارد. آن هم سرعت تغییر تکنولوژی است. این سرعت تغییر، چابکی مقررات و آیین نامه ها را می طلبد که نیاز به ایجاد ساختار در بدنه اجرایی کشور دارد. صنعت انفورماتیک در عین حال می تواند صنعتی با ارزش افزوده بالا باشد. اما در این مسیر تولیدکنندگان نیازهایی دارند... توضیحات دبیر سندیکای تولید کنندگان تجهیزات فناوری اطلاعات ایران را در این باره می خوانید.

در گفتگو با حسین رفعتی مطرح شد:

سال حمایت از تولید ملی فرصتی که از دست رفت

انفورماتیک ضمن تشکر، لطفاً در ابتدا خودتان را معرفی فرمایید.

بنده هم از ایجاد این فرصت از شما تشکر می کنم. بنده حسین رفعتی دبیر سندیکای تولیدکنندگان تجهیزات فناوری اطلاعات ایران که از سال ۱۳۸۸ تا کنون افتخار خدمت به این صنف را داشته ام.

انفورماتیک دامنه فعالیت های سندیکا با توجه به اساسنامه آن چیست؟

همانطور که مستحضرید تشکل ها برای تقویت تک تک اعضای آن و حل مسائل گروهی و استفاده از فکر جمعی تشکیل می گردند. این سندیکا نیز مستثنی نبوده. در اساسنامه ماده ۶ با ۱۷ بند به شرح وظایف سندیکا می پردازد که می توانم به عنوان مثال به برآورد سطح نیاز ملی، تدوین طرح توسعه، بررسی طرحها و لوایح و مقررات، جمع آوری اطلاعات و آمار، همکاری با دولت و مجلس و اتاق بازرگانی، همکاری نزدیک با دفتر صنایع برق و الکترونیک وزارت صنعت و حتی مرکز تحقیقات صنایع انفورماتیک و بسیاری دیگر اشاره کنم. در هر صورت وظیفه اصلی سندیکا صیانت و حمایت از تولید و تولیدکنندگان این بخش می باشد.

انفورماتیک فعالیت های فعلی سندیکا با کدام سازمان ها است و اثربخشی آن را چگونه ارزیابی می کنید؟

همانطور که عرض کردم کلیه سازمانهای دولتی، بطور کلی سه قوه و اتاق بازرگانی سازمانهایی هستند که می بایست با آنها همکاری نماییم. در حال حاضر در بخش دولت سال گذشته به همت هیات رئیسه و مسئولین محترم وزارت صنعت، معدن و تجارت ارتباط بسیار نزدیکی با دفتر صنایع برق و الکترونیک برقرار شده است که در این راستا به عنوان بازوی مشاور و برخی امور اجرایی این دفتر در کنار ایشان فعالیت می نماییم. به نظر بنده این مهم که با تلاش دو طرف انجام گرفته است دستاورد بسیار مناسبی است. نماینده سندیکا در اتاق ایران در کلیه جلسات شرکت نموده و ارتباط بسیار قوی با اتاق برقرار است . البته سندیکا زیر مجموعه اتاق بوده و غیر از این نیز نباید باشد. نظرات سندیکا از طریق اتاق به مجلس، دولت و دیگر ارگانها نیز ارسال می گردد. به طور مثال در برنامه پنجم توسعه عیناً انشاء تهیه شده در سندیکا در بخش فناوری اطلاعات را می توانید مشاهده نمایید.

فکر می کنم دولت و مجلس به اهمیت وجودی تشکل ها پی برده‌اند در این صنعت تنها تشکل رسمی و موجود تولیدی‌سندیکای‌تولید کنندگان تجهیزات فناوری اطلاعات ایران است

در آن زمان جلسات متعددی در سندیکا با حضور اعضاء برگزار شد و پس از نظر خواهی و جمع بندی توسط نماینده محترم هیات مدیره در اتاق ایران که ایشان ریاست کمیسیون **ICT** اتاق ایران را نیز عهده دار می باشند در آنجا مطرح و سپس در کمیسیون مجلس مورد دفاع ایشان قرار گرفت و به تصویب رسید. فکر می کنم این کار خود به تنهایی بزرگترین خدمت به این صنعت بوده است و وجود آن در برنامه پنجم توسعه می تواند بسیار اثر بخش باشد. در سال گذشته و در این دوره از سندیکا ارتباط با کمیسیون ماده یک و حضور در جلسات مربوطه، ارتباط با مجمع عالی واردات و شرکت در جلسات ایشان ، ارتباط با کمیسیون سخت افزار نظام صنفی رایانه و نیز مرکز تحقیقات صنایع انفورماتیک ارتباط خوبی بوده و امید دارم که بیشتر نیز شود.

انفورماتیک وضعیت تولید، تولیدکنندگان و حمایت از تولید را در صنعت انفورماتیک چگونه ارزیابی می فرمایید؟

اکنون دوران بسیار سختی برای تولید کنندگان است. با توجه به سال حمایت از تولید ملی متاسفانه حمایت خاصی از تولید کنندگان که انصافاً سرمایه های واقعی ملی می باشند انجام نگرفته است. فرصت خوبی را از دست دادیم. با توجه به افزایش نرخ ارز تولید می توانست شکوفا شود ولی متاسفانه برخی سیاست های اشتباه مانع شد. این صنعت تفاوت عمده‌ای با صنایع دیگر دارد. آن هم سرعت تغییر تکنولوژی می باشد. این سرعت تغییر چابکی مقررات و آیین نامه ها را می طلبد که نیاز به ایجاد ساختار در بدنه اجرایی کشور دارد. صنعت انفورماتیک در عین حال می تواند صنعتی با ارزش افزوده بالا باشد. تولیدکنندگان در اولین مرحله نیاز به تسهیلات بانکی کم بهره برای سرمایه گذاری، سرمایه در گردش و توسعه دارند. نه اینکه هر ارگانی، هر قانونی، هر مقرراتی فقط برای تولیدکننده که مجبور به ادامه تولید می باشد وضع و اعمال گردد. هر جا مالیات، عوارض، تعزیرات، تغییر قانون است فقط برای تولید کننده اجباری است که ناگزیر به اجرا می باشد. ولی دیگران چه؟ در هر صورت حمایت از تولیدکننده ها با شعار و تنها وضع برخی قوانین میسر نمی شود و اجرای آن از همه مهمتر است. هیات رئیسه سندیکا در ارائه برنامه در سال جاری درخواست تصویب قانون حمایت از تولید را بدون تغییر در بندهای اصلی آن خواستار شده است ولی این گام اول آن است و اجرای آن از تصویب آن مهم تر است. امیدوارم که شرایط به سمت حمایت واقعی از تولید برود.

انفورماتیک جایگاه فعلی سندیکا را در کشور چگونه ارزیابی می فرمایید؟

از زمانی که بنده به عنوان دبیر سندیکا مسئولیت قبول کردم دغدغه اول من جایگاه سندیکا بوده است. عرض کردم، برخی جایگاه ها با تلاش فراوان به دست آمده است. ولی هنوز با مدینه فاضله فاصله بسیار است. جایگاه تشکل ها نمی بایست به صورت سلیقه ای یا احترام به اشخاص یا اخلاق تعیین گردد. جایگاه باید قانونی باشد. اینکه بنده یا اعضاء محترم هیات مدیره از ارتباط شخصی استفاده نمایم و نظر سندیکا را در یک جایگاه تصمیم گیر بگنجانم دائمی و مثمر ثمر نخواهد بود. تعریف جایگاه سندیکا را در بخش خصوصی و تولید کنندگان و از طرف دیگر در حاکمیت و دولت باید مورد بررسی قرار داد. این دو لازم و ملزوم هم هستند. اگر قانون و دولت به سندیکا بهاء دهد مطمئناً تولید کننده نیز با میل در سندیکا و تشکل خود همکاری و فعالیت می نماید. اکنون به نظر بنده جایگاه سندیکا در دفتر تخصصی برق و الکترونیک بسیار ارزنده و برای فعالان موثر بوده است. در حال حاضر با نظر مساعد ریاست محترم این دفتر و همکارانشان و همکاری و همفکری سندیکا خوشبختانه در کلیه مسائل مربوط به این بخش سندیکا مورد مشورت قرار می گیرد.

استعلام، برنامه ریزی، تصمیم گیری، شرکت در جلسات مختلف، ارائه نظر کارشناسی و بسیاری مطالب دیگر از جمله همکاری دفتر صنایع برق و الکترونیک با سندیکا است. البته همانطور که مستحضرید تمامی موارد مربوط به تولید در تجهیزات فناوری اطلاعات به این دفتر ارجاع شده و طرف دولتی سندیکا می باشند. در دستور جلسات کمیسیون ماده ۱ هر زمان که اقلام تولیدی فناوری اطلاعات مطرح می گردد سندیکا نیز حاضر شده و نظر مشورتی خود را ارائه می دهد. به نظرم جایگاه بسیار مهمی است و حضور سندیکا لازم و ضروری است. در کمیسیون ماده ۱ تصمیمات مهمی گرفته می شود که بر سرنوشت تولید یک محصول اثرگذار است.

انفورماتیک هیات مدیره جهت ارتقاء جایگاه سندیکا در مجامع دولتی و صنف تاکنون چه اقداماتی را انجام داده‌اند؟

هیات مدیره محترم در این خصوص تلاش فراوانی انجام داده است. در حال حاضر جایگاه سندیکا در اتاق، دفتر صنایع الکترونیک، مجمع عالی واردات بسیار خوب است. خوشبختانه اعضاء هیات مدیره به دنبال کسب جایگاه مناسب در صنف نیز هستند که در این خصوص از خودشان هزینه می نمایند. هیات مدیره بسیار قوی و خوبی داریم که هر یک شخصاً به کار تشکلی اعتقاد دارند و تلاش می نمایند.

انفورماتیک لطفاً برنامه‌های آتی سندیکا برای ایفای نقش بیشتر در تصمیم‌سازی‌های کلان ملی حوزه‌ی انفورماتیک را تشریح بفرمایید.

یکی از موارد، بررسی طرح ها و لوایح می باشد. با همکاری معاونت مجلس اتاق بازرگانی ایران طرح ها و لوایح مربوطه از قبل در سندیکا بررسی خواهد شد و نظرات از طریق کمیسیون **ICT** اتاق به مجلس ارائه می گردد. این روش در قبل نیز انجام گرفته و نتیجه بخش می باشد. در بخش مقررات کماکان به دنبال ارائه نظر مشورتی به دفتر صنایع برق و الکترونیک هستیم که تقریباً نظرات در این بخش اعمال می گردد، این نیز ادامه خواهد داشت. سال جاری به دنبال ایجاد یک جایگاه در سازمان فناوری اطلاعات هستیم تا بتوانیم از آن طریق نیز در تصمیم گیری های کلان در این حوزه مورد مشورت قرار بگیریم. ارائه نظر به کمیسیون ماده ۱ هم که نقش مهمی در تولید دارد کماکان در برنامه های سال جاری قرار خواهد داشت.

انفورماتیک چه پیشنهادی یا درخواستی از اعضای خود دارید؟

درخواست بنده از اعضاء محترم سندیکا مشارکت هر چه بیشتر آنهادر تشکل خودشان است. سندیکا نه برای بنده است نه متعلق به هیات رئیسه، بلکه برای همه تولیدکنندگان فناوری اطلاعات ایران است. علی الخصوص اعضاء. اعضاء می بایست نظرات، مشکلات و مسائلشان را در اینجا مطرح و پیگیری نمایند تا از طریق خرد جمعی بررسی و پیگیری شود که مطمئناً نتیجه بهتری خواهد داشت. اساساً فلسفه تشکیل سندیکا نیز همین است. درخواست دیگر از اعضاء پاسخ به نظرخواهی ها و ارائه نظر و شرکت در جلسات است. برنامه ما در سال جاری تمرکز بر همین مسئله خواهد داشت.

انفورماتیک اگر مطالب تکمیلی را در نظر دارید لطفا بیان فرمایید.

سوالات پیرامون جایگاه سندیکا زیاد بود که به نظرم از اهمیت خاصی برخوردار است. فکر می کنم دولت و مجلس به اهمیت وجودی تشکل ها پی بردند. در این صنعت تنها تشکل رسمی و موجود تولیدی سندیکا است. امیدوارم این جایگاه واقعی در تصمیم گیری و حتی در اجرای قوانین و مقررات در آینده نه چندان دور به وجود آمده و مطمئناً توسعه این صنعت را در بر داشته باشد. در نهایت از شما و مرکز تحقیقات بخاطر این همکاری تشکر می کنم.

خطرات ناشی از برق گرفتگی در اثر عبور جریان الکتریکی متناوب

ترجمه و تلخیص: حمید شریفی

شدت آسیب شوک الکتریکی به مقدار و مدت زمان عبور جریان الکتریکی از بدن انسان بستگی دارد. برای مثال، عبور جریانی معادل یک دهم آمپر از بدن، فقط برای ۲ ثانیه کافیست تا باعث مرگ انسان شود.

میزان جریان عبوری از درون بدن انسان که شخص می تواند در برابر آن مقاومت کند و قادر به کنترل عضلات بازو و دست خود است، کمتر از ۱۰ میلی آمپر است. جریان های بالای ۱۰ میلی آمپر می تواند باعث بی حسی و قفل عضلات شوند. وقتی که قفل عضلانی اتفاق می افتد، شخص قادر به رها کردن وسایل، سیم یا اجسام نیست. در واقع، ممکن است که جسم برق دار محکم تر در دست نگه داشته شده و باعث طولانی شدن زمان قرار گرفتن در معرض شوک جریان الکتریکی شود. به همین علت، شوک الکتریکی ناشی از وسایل دستی، می تواند بسیار خطرناک باشد. اگر شما نتوانید وسیله برق دار را رها کنید، جریان مداوم برای مدتی طولانی از بدن شما عبور کرده و می تواند باعث فلج تنفسی شود. (عدم حرکت عضلات کنترل تنفس) شما برای مدت زمانی دچار ایست تنفسی می شوید معمولاً عبور جریانی معادل ۳۰ میلی آمپر از بدن انسان باعث ایست تنفسی می شود.

عبور جریان های بیش از ۷۵ میلی آمپر از بدن انسان باعث ایجاد فیبریلاسیون بطنی قلب می شود. (ضربان بسیار سریع غیرموثر قلب، تقریبا ۳۰۰ بار در دقیقه) و در صورت عدم استفاده از دستگاهی خاص به نام دفیبریلاتور برای نجات جان مصدوم، فیبریلاسیون بطنی قلب در چند دقیقه باعث مرگ او خواهد شد. در اثر عبور جریانی برابر ۴ آمپر فلج قلبی رخ می دهد که به منزله عدم پمپاژ دائمی قلب خواهد بود. در اثر عبور جریان های بالای ۵ آمپر بافت های اندام بدن انسان دچار سوختگی خواهند شد.

افزایش مدت زمان قرار گرفتن بدن مصدوم در معرض عبور جریان شدت آسیب دیدگی ناشی از شوک الکتریکی را افزایش خواهد داد. برای مثال، عبور جریانی معادل ۱۰۰ میلی آمپر برای زمانی برابر با ۳ ثانیه به اندازه عبور جریانی برابر با ۹۰۰ میلی آمپر در کسری از ثانیه (۰/۰۳ ثانیه) خطرناک است.

شدت آسیب دیدگی ناشی از شوک الکتریکی با توجه به ساختار ماهیچه ای بدن افراد متفاوت خواهد بود. افراد دارای بافت ماهیچه ای کمتر، معمولاً در اثر عبور جریان های کمتر نیز دچار آسیب دیدگی می شوند. حتی ولتاژ های پایین نیز می توانند بسیار خطرناک باشند چرا که درجه آسیب دیدگی نه تنها به مقدار جریان عبوری از بدن، بلکه به مدت زمان تماس بدن انسان با برق نیز وابسته است.

جدول زیر اتفاقاتی که ناشی از عبور جریان های مختلف از بدن انسان (ظرف مدت حداکثر ۱ ثانیه) و در اثر تماس با ولتاژ برق خانگی، رخ خواهد داد را نشان می دهد.

جریان	واکنش بدن
۱ میلی آمپر	فقط احساس سوزش خیلی کم
۵ میلی آمپر	احساس شوک خفیف. نگران کننده اما بدون درد. اکثر افراد می‌توانند با واکنش طبیعی عکس العمل نشان داده و از برق جدا شوند. با این حال، حرکات غیر ارادی قوی می‌تواند باعث ایجاد صدمات شوند.
۶ تا ۲۵ میلی آمپر (خانم‌ها) ۹ تا ۳۰ میلی آمپر (آقایان)	شوک الکتریکی دردناک و از دست رفتن کنترل عضلات. این محدوده جریانی است که قفل عضلانی آغاز می‌شود. امکان جداکردن بدن از برق بصورت طبیعی وجود ندارد.
۵۰ تا ۱۳۰ میلی آمپر	شوک الکتریکی به شدت دردناک، ایست تنفسی، انقباض عضلانی شدید. جمع شدن عضلات ممکن است باعث نگه داشتن برق شود، انبساط عضلات ممکن است باعث پرتاب شدید فرد به اطراف شود. امکان وقوع مرگ وجود دارد.
۱۰۰۰ تا ۴۳۰۰ میلی آمپر (۱ تا ۴/۳ آمپر)	فیبریلاسیون بطنی رخ می‌دهد(عمل پمپاژ غیر یکنواخت قلب). انقباض عضلانی، ایجاد آسیب عصبی و احتمال وقوع مرگ وجود دارد.
۱۰۰۰۰ میلی آمپر (۱۰ آمپر)	ایست قلبی و سوختگی های شدید رخ می‌دهد. امکان مرگ وجود دارد.
۱۵۰۰۰ میلی آمپر (۱۵ آمپر)	حداقل اضافه جریانی که در آن فیوز معمولی یا قطع کننده مدار، مدار را قطع می‌کند.
این اثرات جریان الکتریکی برای ولتاژهای تقریبا کمتر از ۶۰۰ ولت است. ولتاژهای بالاتر نیز باعث سوختگی شدید می‌شود. تفاوت حجم عضلات و چربی بر شوک الکتریکی تأثیر می‌گذارد.	

در جریان ۱ میلی آمپر واکنش بدن فقط احساس سوزش خیلی کم است. در جریان ۵ میلی آمپر شوک خفیف رخ می دهد؛ این وضعیت نگران کننده اما بدون درد است. اکثر افراد می توانند با واکنش طبیعی عکس العمل نشان داده و از برق جدا شوند. با این حال، حرکات غیر ارادی قوی می تواند باعث ایجاد صدمات شوند. جریان ۶ تا ۲۵ میلی آمپر (خانم ها)، ۹ تا ۳۰ میلی آمپر (آقایان) شوک الکتریکی دردناک و از دست رفتن کنترل عضلات رخ می دهد. دراین محدوده جریانی است که قفل عضلانی آغاز می شود. امکان جداکردن بدن از برق بصورت طبیعی وجود ندارد. در جریان ۵۰ تا ۱۳۰ میلی آمپر شوک الکتریکی به شدت دردناک، ایست تنفسی، انقباض عضلانی شدید رخ می دهد. جمع شدن عضلات ممکن است باعث نگه داشتن برق شود، انبساط عضلات ممکن است باعث پرتاب شدید فرد به اطراف شود. امکان وقوع مرگ وجود دارد. در جریان ۱۰۰۰ تا ۴۳۰۰ میلی آمپر (۱ تا ۴/۳ آمپر) فیبریلاسیون بطنی رخ می دهد (عمل پمپاژ غیر یکنواخت قلب). انقباض عضلانی، ایجاد آسیب عصبی و احتمال وقوع مرگ وجود دارد. در جریان ۱۰۰۰۰ میلی آمپر (۱۰ آمپر) ایست قلبی و سوختگی های شدید رخ می دهد. امکان مرگ وجود دارد. در جریان ۱۵۰۰۰ میلی آمپر (۱۵ آمپر) حداقل اضافه جریانی که در آن فیوز معمولی یا قطع کننده مدار، مدار را قطع می کند. این اثرات جریان الکتریکی برای ولتاژ های تقریباً کمتر از ۶۰۰ ولت است. ولتاژ های بالاتر نیز باعث سوختگی شدید می شود. تفاوت حجم عضلات و چربی بر شوک الکتریکی تاثیر می گذارد.

ادامه ی این مقاله که حاوی اطلاعات بسیار سودمندی در رابطه با خطرات شوک الکتریکی برای بدن انسان است را در پورتال مرکز تحقیقات صنایع انفورماتیک به آدرس WWW.RCII.IR ملاحظه فرمایید.

مراجع:

1. 14 ELECTRICAL SAFETY by Walter H. Olson
2. ELECTRICAL SAFETY by Thaddeus W. Fowler, Ed.D. and Karen K. Miles, Ph.D

آشنایی با چارچوب COBIT در حاکمیت فناوری اطلاعات

محمد امین صابریان

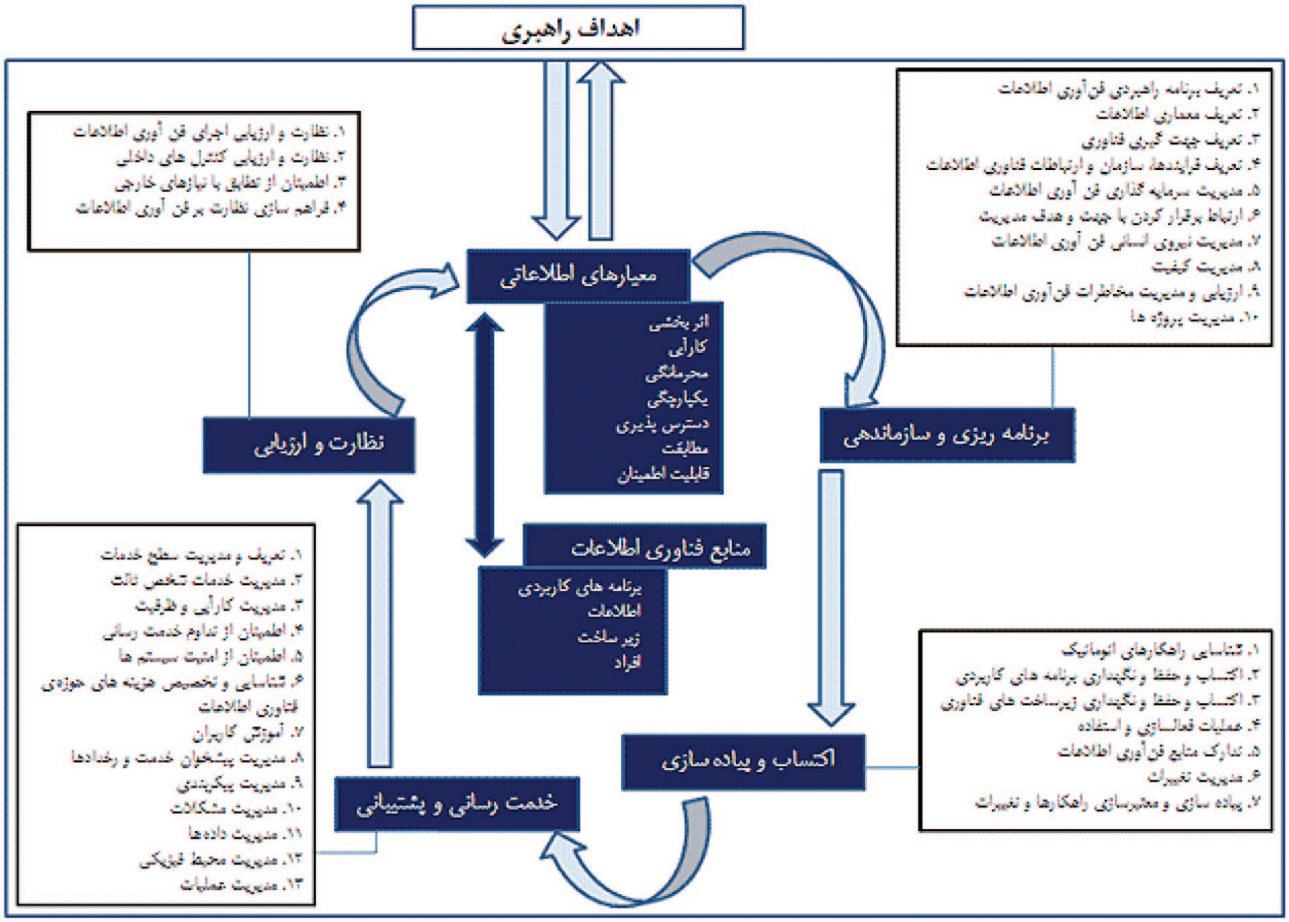
چارچوب COBIT[1] مجموعه‌ای از بهترین روش‌ها برای مدیریت فناوری اطلاعات است که توسط انجمن کنترل و ممیزی سیستم‌ها (ISACA) و سازمان راهبری فناوری اطلاعات (ITGI) در سال ۱۹۹۶ ایجاد شد. COBIT برای مدیران، ممیزان و کاربران فناوری اطلاعات مجموعه‌ای از سنجه‌ها، معیارها، فرایندها و بهترین روش‌های قابل قبول را ارائه می‌کند تا به آنان در افزایش سود حاصله از به کارگیری فناوری اطلاعات و توسعه کنترل و راهبری فناوری اطلاعات کمک نماید.

چارچوب COBIT دارای سه سطح است: در سطح پایین، فعالیت‌ها و وظایفی وجود دارند که برای دستیابی به نتایج قابل اندازه‌گیری مورد نیاز هستند. در یک لایه بالاتر فرایندها به عنوان مجموعه‌ای از فعالیت‌ها و وظایف تعریف شده‌اند و در بالاترین سطح که بیشتر مورد توجه COBIT است، فرایندها در چهار حوزه دسته‌بندی شده‌اند.

تاکنون پنج نسخه از چارچوب COBIT انتشار یافته است. نسخه اول COBIT در سال ۱۹۹۶ به عنوان یک چارچوب ممیزی منتشر شد. نسخه دوم در سال ۲۰۰۰ بر اساس منابع جدید بین‌المللی بازبینی شد و مفاهیمی شامل راهنمای مدیریت، پشتیبانی از افزایش کنترل مدیریت، معرفی مدیریت عملکرد و گسترش راهبری فناوری اطلاعات به آن اضافه شد. نسخه سوم در سال ۲۰۰۵ با یکپارچه‌سازی کتاب‌های مجزا به صورت یک جلد واحد منتشر شد.

نسخه چهارم با عنوان COBIT 4.1 در سال ۲۰۰۷ منتشر شد و شامل موارد تکمیلی زیر برای تسهیل بهره‌برداری از COBIT است:

- مراجعی شامل ورودی‌ها و خروجی‌های فرایندهای COBIT به یکدیگر
- فعالیت‌های مربوط به هر فرایند به همراه جدول RACI به ازای هر فعالیت (وظایف مربوط به مدیر خدمات فناوری اطلاعات، مدیر توسعه، مدیر اجرایی و ... را مشخص کرده است.)
- توضیحات ساده‌سازی شده از اهداف
- نمایش فرایندها و ارتباطات میان کسب و کار، اهداف فناوری اطلاعات و فرایندهای فناوری اطلاعات به شکل آبشاری.



نسخه پنجم COBIT 5 در اواسط ۲۰۱۲ انتشار یافته است. این نسخه از COBIT به یکپارچه سازی چارچوب مخاطرات فناوری اطلاعات، Val IT 2.1 و COBIT نسخه ۴.۱ پرداخته است.

چارچوب COBIT یک مرجع مدل فرایندی و یک زبان مشترک برای کلیه کسانی است که در یک سازمان مسئولیت مدیریت فعالیت های فناوری و اطلاعات را برعهده دارند.

۱-۱- دلایل نیاز سازمان به چارچوب COBIT

دلایلی که مدیران و تصمیم گیرندگان اصلی را به پذیرش COBIT تشویق می کند، عبارتند از:

- نیاز مدیران به نظارت بر منابع سازمان
- با کنترل منابع فناوری اطلاعات، هزینه کل ارائه خدمات آن کاهش می یابد.
- COBIT ترس و نگرانی و عدم اطمینان مدیران را نسبت به برآورده نشدن هدف های تجاری کاهش خواهد داد.
- ایجاد و برقراری ارتباطات بهبود یافته بین مدیران، کاربران و ممیزان با به کارگیری COBIT
- همسویی اهداف فناوری اطلاعات با اهداف کسب و کار و بالعکس
- تعریف نقش ها، وظایف و مسئولیت ها به صورت روشن و صریح و بر اساس روشی فرایند محور
- کیفیت خدمات فناوری اطلاعات را افزایش می دهد
- سنجش کارایی فناوری اطلاعات
- بهبود ارائه پروژه ها

۱-۲- حوزه‌ها و فرایندهای COBIT

در COBIT ۴.۱ مدل عمومی برای ارزیابی یک پروژه فناوری اطلاعات از ۳۴ فرایند IT استفاده می کند. این فرایندها به ۴ حوزه تقسیم شده اند که عبارتند از :

۱. برنامه ریزی و سازماندهی[2] شامل ده فرایند
۲. تهیه و پیاده سازی[3] شامل هفت فرایند
۳. تحویل و پشتیبانی[4] شامل سیزده فرایند
۴. نظارت و ارزیابی[5] شامل چهار فرایند

شکل ذیل بیانگر چارچوب COBIT بر اساس COBIT 4.1 است.

در حوزه برنامه ریزی و سازماندهی، استراتژی و تاکتیک ها و نگرانی های مربوط به شناسایی فناوری اطلاعات را می توان برای دستیابی به هدف های تجاری به بهترین شکل جمع آوری کرد. در حوزه تهیه و پیاده سازی برای شناخت و ایجاد استراتژی فناوری اطلاعات، امکانات باید شناسایی، توسعه یافته یا تهیه شوند. در حوزه تحویل و پشتیبانی، تحویل به موقع و ارائه خدمات مورد نیاز، مورد توجه قرار می گیرد و فرایندهای پشتیبانی مورد نیاز باید راه‌اندازی شوند. در حوزه نظارت و ارزیابی، تمامی فرایندهای فناوری اطلاعات به طور منظم از نظر کیفیت و مطابقت با الزامات کنترل، مورد ارزیابی قرار می گیرند.

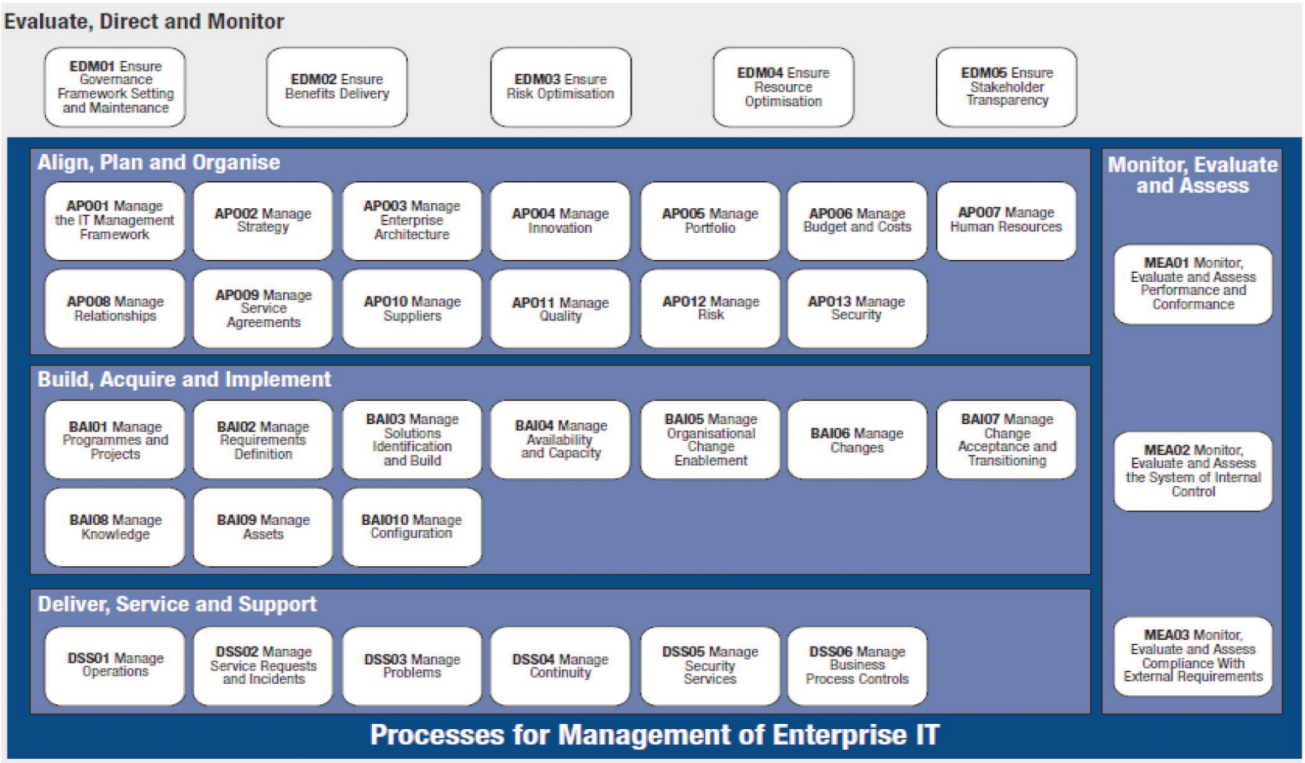
در COBIT 5 مدل عمومی برای ارزیابی یک پروژه فناوری اطلاعات از ۳۷ فرایند IT مطابق شکل زیر استفاده می کند.

چرخه پیاده سازی بر اساس COBIT 5 مطابق شکل شماره یک است.

شکل شماره یک

مراجع:

1. for information and related technology control objectives
2. Plan and Organize
3. Acquire and Implement
4. Deliver and Support
5. Monitor and Evaluate



آزمایشگاه ارزیابی کیفیت محصولات نرم افزاری تحت وب مرکز تحقیقات صنایع انفورماتیک راه‌اندازی شد

توسعه فناوری اطلاعات و لزوم افزایش بهره وری در سازمان های دولتی، حرکت به سوی دولت الکترونیکی را اجتناب ناپذیر کرده است، این امر فرصت تجاری مناسبی را برای بنگاه های اقتصادی کوچک و بزرگ فراهم کرده که از آن جمله می توان به تهیه محصولات نرم افزاری تحت وب و پورتال اشاره کرد.

با توجه به اینکه افزایش حجم تقاضا باعث شده تا بنگاه های اقتصادی متعددی در سال های اخیر تاسیس شده و محصولات متعدد و متنوعی روانه بازار شوند در حال حاضر دغدغه اصلی کاربران حصول اطمینان از صحت عملکرد و کیفیت محصولات تولیدی است. سازمان فناوری اطلاعات به عنوان متولی ساماندهی به محصولات حوزه فناوری اطلاعات اقدام به شناسایی و همکاری با آزمایشگاه های توانمند در امر ارزیابی این گونه محصولات کرده است. در این راستا مرکز تحقیقات صنایع انفورماتیک به منظور انجام خدمات ارزیابی و تایید نمونه محصولات نرم افزاری مبتنی بر وب و پورتال های سازمانی، به عنوان آزمایشگاه تخصصی معتبر در زمینه ارزیابی کیفیت محصولات نرم افزاری، توافق نامه ای با سازمان فناوری اطلاعات ایران امضا کرده که هدف از این توافق نامه، ارتقای کیفیت نرم افزار های مبتنی بر وب مورد استفاده در کشور است.

هوش امنیتی

مهری یحیائی، ساناز خلیلی

۱. مقدمه

با افزایش حجم رخدادهای گزارش شده توسط سیستم ها و ابزارهای امنیتی، کشف و شناسایی تهدیدات و حملات داخلی و خارجی بسیار دشوار و در مواردی غیرممکن شده است، از این رو نیاز به روش متمرکزی وجود دارد تا بتوان رخدادها و داده های گزارش شده را مانیتور کرده و بین آنها ارتباط برقرار نمود و از این طریق تهدیدها و حملات را شناسایی کرد. بسیاری از تحقیقات صورت گرفته بیانگر این است که از هر ده رخداد امنیتی، هفت رخداد هیچ وقت در سازمان ها گزارش نمی شوند و در ۳۰ درصد مواقع، حتی خود سازمان مور حمله نیز متوجه بروز حمله نمی شود. همچنین یک سوم نشت اطلاعات حیاتی در سازمان ها، تا یک ماه بعد هم تشخیص داده نمی شوند و سه پنجم از رخدادهای امنیتی توسط شرکت های بیرونی تشخیص داده می شوند و نه خود سازمان قربانی و ۴۳ درصد از حملات سایبری بر روی دارایی های لیست نشده سازمان ها، رخ می دهند.

با وجود این روند تصاعدی بروز تهدیدات جدید، محدودیت های فناوری در تحلیل سریع رخدادها، انبوه داده های غیریکپارچه در سیستم های مختلف یک سازمان، تغییرات سریع قوانین محلی و جهانی، منابع امنیتی محدود در سازمان از جمله نیروی متخصص، هزینه و فناوری و عدم توجه به مستندسازی اطلاعات، شرکت ها و سازمان ها را به اتخاذ تصمیمات جدی در خصوص امنیت وادار می کند.

۲. آشنایی با هوش امنیتی

استفاده از سخت افزار، نرم افزار، اسکنر یا سیستم های مانیتورینگ، هیچ یک به معنی احساس امن بودن نیست. راه کار پیشنهادی محققین امنیت اطلاعات، هوش امنیتی است که در واقع یک راه کار مدرن امنیتی برای مقابله با تهدیدات امروزی می باشد.

جمع آوری، هنجارسازی، همبسته سازی و تحلیل بزرگ داده های[1] امنیتی یک سازمان به منظور خودکار کردن فرآیندهای کاهش سطح مخاطرات در سازمان یا به عبارت دیگر تبدیل میلیون ها بسته اطلاعاتی به یک اقدام عملی آنی، تعاریفی از هوش امنیتی هستند.

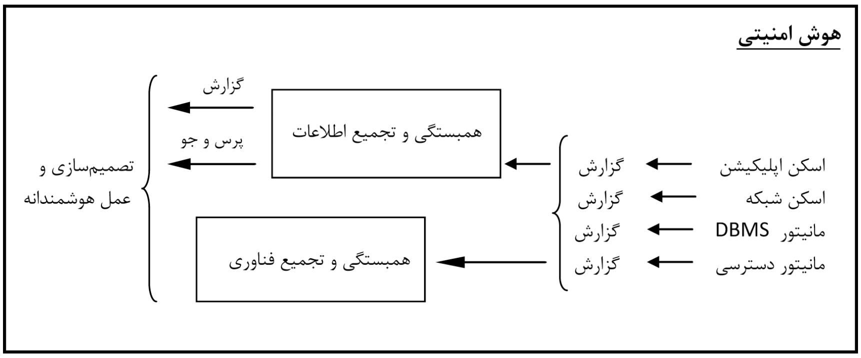
به دو دلیل مهم Big Data و APT[2]، سازمان ها ناگزیرند که به سمت هوش امنیتی حرکت کنند. بزرگ داده، به مجموعه هایی از داده با نرخ رشد بسیار بالا گفته می شود که در مدت زمان کوتاهی، باعث ایجاد چنان حجمی از اطلاعات می شوند که ذخیره سازی، جست وجو و تحلیل آنها با ابزارهای مدیریت داده موجود در یک زمان قابل تحمل و مورد انتظار، غیر ممکن است. چهار مشخصه مهم بزرگ داده ها، حجم بالای داده، سرعت بالای ایجاد داده، تنوع بالای داده و سرعت بالای تغییر داده است. APT، نوعی از حملات ترکیبی و پیچیده

سایبری است که هدفی خاص و دقیق دارد و از روش های مختلف برای پنهان ماندن از دید سامانه های پایش استفاده می کند.

همان‌طور که هوش تجاری[3] موجب کاهش ریسک در کسب و کار، تسهیل تصمیم گیری های تجاری و خودکار کردن فرآیندهای تجاری مانند خرید، پشتیبانی، ERP[4] و... می شود، هوش امنیتی نیز موجب کاهش تهدیدات، کاهش سطح عدم انطباق، تسهیل تصمیم گیری های امنیتی و خودکار کردن فرآیندهای امنیتی می شود.

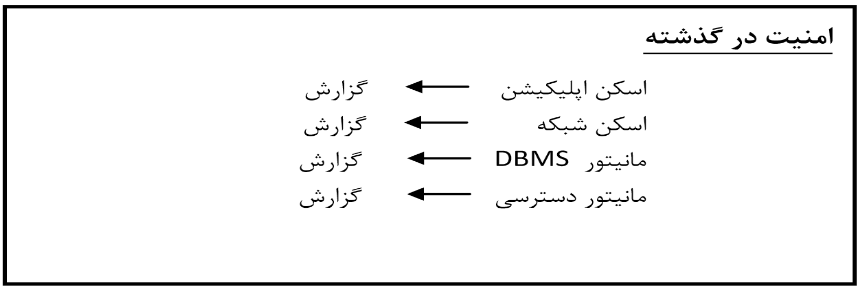
مدل امنیتی ده سال پیش سازمان ها، در شرایط کنونی ابدا موثر نیست و این مدل در بهترین حالت خود جزایر امنیتی را ایجاد می کند و هکرها از فاصله بین این اطلاعات استفاده می کنند.

جهت برقراری امنیت در روش های سنتی مطابق شکل زیر، از موارد مذکور گزارشی تهیه می شود، اما در روش هوش امنیتی پس از تهیه این گزارشات، با



استفاده از دو بخش مهم هوش امنیتی، بخش یکپارچگی اطلاعات و همبسته سازی و بخش برهم کنش تکنولوژی و همبسته سازی از گزارش حاصله، می توان تصمیم یا عمل هوشمندی را اتخاذ کرد.

مدیریت رویدادها و امنیت اطلاعات (SIEM)[5]، مدیریت مخاطرات (Risk Management) و پذیرش مقررات



(Regulatory Compliance)، سه جزء اصلی یک راه کار هوش امنیتی هستند.

SIEM، مهمترین جزء و متفاوت با Log Management است و ترکیبی از محصولات مدیریت رویدادهای امنیتی (SEM)[6] و مدیریت اطلاعات امنیتی (SIM)[7] می باشد. مدیریت رخداد نگاشت ها (log)، نرمال سازی، همبسته سازی رویدادها، عکس العمل آنی به تهدیدات، امنیت عناصر انتهایی، ذخیره سازی وقایع و ارائه گزارش به صورت based-Web و راه دور، نمونه های از سرویس های SIEM هستند. قسمت زیرساخت در یک راه کار هوش امنیتی توسط SIEM تامین می شود، وظایف نرمال سازی و همبسته سازی توسط SIEM انجام می شود، در بسیاری از محصولات تجاری SIEM، امکان مدیریت Compliance هم وجود دارد، محصولات تجاری SIEM عمدتاً توسعه پذیر[8] هستند و به دلایل مذکور SIEM، قلب یک راه کار هوش امنیتی است.

هدف مدیریت مخاطرات، کاهش زیان است که از طریق سه شاخص، شناسایی، ارزیابی و اولویت گذاری امکان پذیر است. بر مبنای ISO 27005، پنج قدم مهم در مدیریت مخاطرات وجود دارد که در ذیل آمده است.

قدم اول: تشخیص و شناسایی تهدیدات

قدم دوم: ارزیابی آسیب پذیری های هدف تهدیدات

قدم سوم: تشخیص زیان های ناشی از عملی شدن تهدیدات

قدم چهارم: تعیین راه کارهای کاهش مخاطرات

قدم پنجم: اولویت گذاری راه کارها

۲-۱ - خروجی‌های یک راه‌کار هوش امنیتی

Data silo consolidation: بدون تکنولوژی هوش تجاری، تحلیل بزرگ داده های تجاری برای تعیین مسیر حرکت یک کسب و کار عملاً ناممکن است. چنین تشبیهی در مورد هوش امنیتی نیز صادق است. بدون هوش امنیتی، دریافت log تجهیزات حتی در صورتی که به طور کامل نیز انجام گردد، باعث ایجاد یک سیلوی جدید می شود. در یک سازمان بزرگ این داده ها به اندازه های زتا بایت[9]، یوتا بایت[10] و هلا بایت[11] هم می رسد. هوش امنیتی به وسیله اضافه کردن Context باعث کاهش حجم اطلاعات امنیتی می شود.

Threat Management: از زمان ظهور اینترنت، مدل تهدیدات امنیتی از یک مدل متمرکز به یک مدل توزیع شده تغییر ماهیت داده است. امنیت دیگر تنها موضوع نصب فایروال نیست. امروزه تمرکز بر روی امنیت لایه های بالاتر مدل OSI بوده و محتوا اهمیت یافته است و حملات APT مطرح شده اند. فعالیتی که برای یک بخش از زیرساخت بی ضرر تشخیص داده می شود، پس از همبسته سازی با سایر منابع اطلاعاتی ممکن است برای بخش دیگری از زیرساخت مهلک تشخیص داده شود. وظیفه هوش امنیتی تشخیص این نوع حملات است.

Fraud Discovery: تشخیص تقلب بدون استفاده از هوش امنیتی عملاً غیرممکن است. تشخیص تقلب نیازمند جمع آوری Log کلیه المان های مسیر حرکت یک بسته اطلاعات یا تراکنش بانکی است که مجدداً با مشکل Big Data روبرو می شود.

Regulatory Compliance: مهمترین خروجی هوش امنیتی است که اهمیت certified بودن برای کسب و کار یک سازمان را دربردارد. در واقع یک بازرس[12] خودکار و time-real است. به جز حوزه های مربوط به منابع انسانی، سایر حوزه های یک استاندارد را پوشش می دهد و قابلیت تنظیم برای استانداردهای بومی، محلی و کشوری را دارد.

۲-۲ - چالش‌های پیاده‌سازی هوش امنیتی

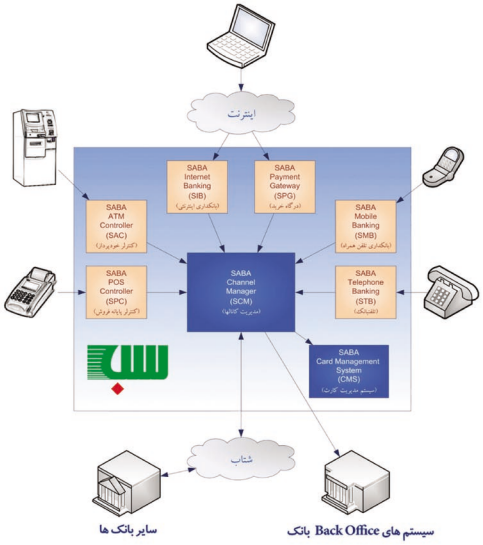
فناوری هوش امنیتی مانند سایر فناوری ها با چالش هایی روبروست که نمونه هایی از آنها در جهان و ایران در ادامه ذکر می شود. عدم پشتیبانی مدیریت ارشد، بودجه، کمبود نیروی انسانی متخصص، عدم درک درست از هوش امنیتی، پیچیدگی پیاده سازی و عدم توجه کافی به مدیریت ریسک نمونه هایی از چالش های پیاده سازی در جهان بوده و فرهنگ سازمانی نامناسب، عدم پشتیبانی مستقیم شرکت های فروشنده محصول در ایران و عدم هماهنگی بین سازمان های مختلف در مدیریت امنیتی نمونه هایی از چالش های پیاده سازی در ایران هستند.

1. big data
2. Advanced Persistent Threat
3. Business Intelligence
4. Enterprise resource planning
5. Information and Event Management Security
6. Security Event Management
7. Security Intelligence Management
8. Expandable
9. Zetta byte
10. Yotta byte
11. Hell byte
12. Auditor

شریک امین و قابل اتکا

محصولات

– نماینده انحصاری فروش و پشتیبانی محصولات شرکت GRG Banking در ایران شامل :
• انواع دستگاه های خودپرداز (ATM) و خودد ریافت (CRM/BNA) دیواری، سالنی، Teller Master، Drive up و Recycling.
• انواع دستگاه های فروش اتوماتیک بلیط مترو و قطار (TVM) شارژبلیط های اعتباری (AVM) و کنترل ورود و خروج مسافر توسط بلیت (TCM).
• دستگاه‌های اتوماتیک کنترل ورود و خروج مسافر توسط بلیت در مترو و قطار.
– تولید انواع دستگاه های خودپرداز ، کامپیوترهای شخصی و سرور.
– اولین تولید کننده داخلی انواع صندوق های فروشگاهی (RETAIL –POS) در کشور
– دستگاه‌های پایانه فروش (EFT-POS)
– ارائه دهنده سرورهای hp
– ماجول جلوگیری از کپی برداری کارت های مغناطیسی در خودپرداز
– پایانه های فروش شرکت ایران ارقام
– نرم افزار دوربین امنیتی خودپرداز ؛ نرم افزاری است که بر روی دستگاه خودپرداز نصب شده و مدیریت دوربین خودپرداز را به عهده می گیرد و با ورود کارت یا حین تراکنش های مختلف از زاویه دید دوربین از دارنده کارت عکس می گیرد. این نرم افزار دارای قابلیت های متعددی چون سازگاری با اکثر دوربین های USB، قابلیت تنظیم برای گرفتن عکس در زمان انجام تراکنش های مختلف، امکان ذخیره سازی، بازیابی و آرشیو عکس های تهیه شده و حذف عکس های خاص مربوط به گذشته و ... است.



– **سوئیچ تبادل اطلاعات بانکی « سبا » شامل :**
• Channel Manager
• ATM & POS Controller
• سیستم تولید کارت و Monitoring

خصیصه‌های پیشرفته Channel Manager ، یکپارچگی سیستم‌های بانکی مورد استفاده مشتریان را تضمین و بهره‌برداری از سایر خدمات بانکی از طریق اینترنت، تلفن، موبایل و... را در کوتاه‌ترین زمان جهت مشتریان بانک‌ها و مؤسسات مالی و اعتباری امکان‌پذیر می‌سازد.

سایر محصولات نرم افزاری نیز به شرح ذیل می باشند:
• سیستم مدیریت کارت (CMS) با قابلیت صدور انواع کارت های نقدی، خرید، هدیه، اعتباری و ...
• سیستم صدور کارت آنی در شعبه (BCMS)
• سیستم درگاه خرید (Payment Gateway)
• بانکداری اینترنتی (Internet Banking)
• بانکداری از طریق تلفن همراه (Mobile Banking)
• سیستم تلفنبانک مبتنی بر تکنولوژی VOIP

علاوه بر خدمات متعارف، سرویس هایی نظیر شارژ تلفن همراه، ارائه رمز دوم و CVV۲، انتقال وجه شتابی، پرداخت قبوض شتابی و پرداخت غیر حضوری شتابی از طریق درگاه های فوق ارائه می شوند.

دفتر مرکزی: تهران، خیابان استاد نجات اللهی، خیابان سپند غربی، شماره ۵۲
تلفن: ۸۸۹۰۷۱۶۳ – ۸۸۹۰۱۴۲۹ دورنگار: ۸۸۹۰۱۳۶۳ وب سایت : www.iranargham.com

نرم افزار هوش سازمانی

QlikView

Simplifying analysis for everyone

دارای تاییدیه از مرکز تحقیقات صنایع انفورماتیک ایران

RCII

RCII Certified

خدمتی دیگر از
شرکت مهندسین مشاور
نظم آران

www.nazmaranco.com شرکت مهندسین مشاور نظم آران

خیابان کریم خان- خیابان ویلا-کوچه حقیقت طلب پلاک ۹ -طبقه ۵ ، تلفن: ۳-۸۸۳۴۷۱۴۱

اولین آزمایشگاه تحقیقاتی و ارزیابی امنیت محصولات فناوری اطلاعات

Common Criteria

آزمایشگاه امنیت مرکز تحقیقات صنایع انفورماتیک، به عنوان اولین آزمایشگاه ارزیابی امنیت محصولات فناوری اطلاعات در سطح کشور موفق به اخذ گواهینامه استاندارد ISO17025 مربوط به تایید صلاحیت آزمایشگاه‌هایی که فعالیت‌های آزمون را انجام می‌دهند، شده است.

مبنای آزمون‌های ارزیابی امنیتی محصولات فناوری اطلاعات در این آزمایشگاه استاندارد ISO/IEC/ISIRI 15408 می‌باشد.

استاندارد ISO/IEC/ISIRI 15408 از سه بخش تشکیل شده است، بخش اول شامل مفاهیم، بخش دوم شامل الزامات امنیتی و بخش سوم شامل الزامات تضمین امنیت بوده و متدولوژی مورد استفاده در اجرای آزمون‌ها، متدولوژی CEM است.

الزامات امنیتی مورد نیاز هر یک از محصولات فناوری اطلاعات با توجه به اهداف امنیتی مورد نیاز هر محصول و نیز با توجه به تهدیدات و آسیب پذیری‌های هر هدف امنیتی، شناسایی شده و آزمون‌های امنیتی بر اساس آنها انجام می‌شود.

از استانداردهای جانبی که در فرآیند انجام ارزیابی امنیتی، نیز بکار گرفته می‌شوند می‌توان به استانداردهای CCWAPS, OWASP, CLASP, PTES,... اشاره نمود.

این آزمایشگاه در چهل گروه محصول در حوزه فاوا قابلیت انجام آزمون و ارزیابی را دارد، از جمله :

- ارزیابی محصولات امنیتی، انواعUTM و فایروال و...
- ارزیابی کارت هوشمند
- ارزیابی تجهیزات شبکه
- ارزیابی سیستم‌های تشخیص نفوذ
- ارزیابی انواع سیستم‌های پیشگیری از نفوذ
- ارزیابی انواع انتی ویروس
- ارزیابی سیستم‌های کنترل دسترسی
- ارزیابی سیستم‌های کنترل صنعتی
- ارزیابی سیستم‌های عامل
- ارزیابی انواع پایگاه داده
- ارزیابی الگوریتم‌های رمز نگاری بومی
- ارزیابی سیستم‌های بیومتریک
- ارزیابی سیستم‌های مبتنی بر وب
- ارزیابی سیستم‌های انتقال بی سیم
- ارزیابی انواع پرینترها، فکس و کپی

سایر فعالیتهای قابل انجام در آزمایشگاه ارزیابی امنیتی عبارتند از:

- طراحی معماری های امنیتی براساس مدل هایی چون Clark wilson , biba
- تدوین سند راهبردی امنیت برای سازمان ها
- ارزیابی نشت اطلاعاتی در یک سازمان علی الرغم استفاده از راهکارهایی همچون Anti virus / UMT / Firewall
- ارزیابی عملکرد تیم های امنیتی CSTRT / SOC
- ارزیابی امنیت و نفوذ پذیری به یک سازمان از طریق نیروی انسانی(Social Engineering)

مرکز تحقیقات صنایع انفورماتیک RCH

دفتر مرکزی و آزمایشگاه تهران: خیابان کریمخان زند، خیابان شهید عضدی(آبان جنوبی)، خیابان رودسر، پلاک۳، 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

ISO 9001:2008 NSCERT Corporate Solutions Provider

Iran Accreditation System IAS نظام تأیید صلاحیت ایران ISO 17025 ISO 17020