سیستم هوشمند مدیریت امنیت اطلاعات: مسائل مربوط به معماری و طراحی

چکیده

محدودیت های هر تکنولوژی امنیتی همراه با رشد حملات سایبری بر کارایی مدیریت امنیت اطلاعات تاثیر می گذارد و فعالیت های انجام شده توسط مدیران شبکه و کارمندان امنیتی را افزایش می دهد. بنابراین، نیاز به افزایش حسابرسی(رسیدگی) خودکار و مکانیسم گزارش دهی هوشمند برای اعتماد و اطمینان سایبری وجود دارد. سیستم های هوشمند، سیستم های محاسباتی در حال ظهور مبتنی بر تکنیک های هوشمند هستند که از نظارت مستمر و کنترل فعالیت های کارخانه ای پشتیبانی می کنند. هوش، توانایی فرد برای تصمیم گیری بهتر را بهبود می بخشد. این مقاله یک معماری مطرح شده از یک سیستم هوشمند را برای مدیریت امنیت اطلاعات (ISISM) ارائه می دهد. هدف این سیستم بهبود فرآیندهای مدیریت امنیت مانند نظارت، کنترل و تصمیم‌گیری با اندازه تاثیر آنها است که نسبت به یک متخصص امنیت، با ارائه مکانیسم‌های افزایش ساختار فعال دانش در مورد تهدیدها، سیاست‌ها، رویه‌ها، و خطرات، بالاتر است. ما بر نیازها و مسائل طراحی برای اجزای اساسی سیستم هوشمند تمرکز می کنیم.

کلمات کلیدی: مدیریت امنیت اطلاعات، امنیت سایبری، سیستم هوشمند، معماری، کنترل مبتنی بر عامل.

مروری برامنیت سایبری

رشد چشمگیر اینترنت، همگرایی اینترنت و برنامه های چندرسانه ای بی سیم و خدمات، چالش های امنیتی جدیدی را وضع می کند (Miller، 2001). امنیت یک سیستم پیچیده است (Volonino، 2004) و باید از هر جهتی و برای هر کاربر مورد توجه قرار گیرد. سازمانها به یک

رویکرد سیستماتیک برای مدیریت امنیت اطلاعات نیاز دارند که به طور مداوم در هر سطح به امنیت کمک می کند. آنها به سیستم هایی نیاز دارند که به طور مطلوب تخصیص منابع امنیتی محدودشده را بر اساس ریسک پیش بینی شده به جای آسیب پذیری های درک شده پشتیبانی کنند. با این حال، زیرساخت های امنیتی بسیاری از سازمانها به جای برنامه ریزی، یک رویکرد مبتنی بر واکنش مانند شناسایی آسیب پذیری ها و به روز رسانی نرم افزار (Cardoso & Freire، 2005) به جای یک برنامه پیشگیرانه مطرح می کنند(Gordon، Loeb & Lucyshyn، 2003). از سوی دیگر، برنامه های امنیتی سایبر، الزامات خاصی را برای امنیت رایانه و شبکه و همچنین تاکید بر دسترسی مکانیسم های گزارش دهی و رسیدگی خودکار تجاری و ارتقاء محصولات برای ارزیابی های امنیتی و مدیریت فرا می خوانند (Hwang, Tzeng & Tsai, 2003; ;۲۰۰۳ Chan & Perrig Leighton, 2004).

علاوه بر کنترل های امنیتی فنی (فایروال ها، رمزهای عبور، تشخیص نفوذ، برنامه های بازیابی فاجعه و غیره)، امنیت سازمان شامل مسائلی دیگر است که به طور معمول روند و مسائل افراد مانند سیاست ها، آموزش، عادات، آگاهی، روش ها و انواع دیگر مسائل فنی و غیر فنی (Heimerl & Voight، 2005). آموزش و آگاهی امنیتی از استفاده سریع و گسترده زیربنای جدید دیجیتال عقب مانده است (Tassabehji، 2005). تمام این عوامل امنیت را فرآیندی متمرکز بر تکنیک های بین رشته ای می سازد(Maiwald، 2004؛ Mena، 2004). چالش های موجود در مدیریت امنیت اطلاعات همراه با فقدان درک علمی رفتار سازمانی که برای بهبود سیستم های محاسباتی فراخوانی می شوند ،از اثربخشی استفاده از فناوری های اطلاعاتی خاص و رویکردهای جدید مبتنی بر تکنیک های هوشمند و اطلاعات امنیت به عنوان ابزار هماهنگی و به اشتراک گذاری اطلاعات پشتیبانی می کنند. سیستم های هوشمند به عنوان سیستم های نرم افزاری جدید برای پشتیبانی برنامه های پیچیده، بوجود آمدند. در این مقاله، معماری سیستم هوشمند مدیریت امنیت اطلاعات (ISISM) را پیشنهاد می کنیم که از فرایندها و زیرساخت های امنیتی در یک سازمان پشتیبانی می کند. در میان این مولفه ها، سیستم های هوشمند عبارتند از عوامل هوشمند که سطح بالایی از خودمختاری را نشان می دهند و در شرایطی با عدم اطمینان بالایی عمل می کنند. این سیستم از دانش اکتسابی

، که احتمالا به کاربر انسانی کمک می کند، به ویژه در سطح عمیق تر درک و حل مسئله برای حوزه اطمینان امنیت اطلاعات،پشتیبانی می کند.

بخش بعدی این مقاله خلاصه ای از موضوعات و روند مدیریت امنیت اطلاعات را ارائه می دهد، یک مرور کلی از تهدیدات امنیت اطلاعات، و در ادامه بررسی تکنیک های AI برای برنامه های امنیت سایبری. سپس معماری و اجزای اصلی سیستم هوشمند را نشان می دهیم و شامل الزامات خاص طراحی برای عوامل هوشمند می شود. ما با استفاده از رویکرد مهندسی سیستم، مسائل کلیدی مرتبط با طراحی و فن آوری را مورد بحث قرار می دهیم. در ارتباط با سیستم های مبتنی بر کنترل عامل هوشمند که یک راه برای تحلیل، طراحی و اجرای سیستم های نرم افزاری پیچیده ارائه می دهند ف بحث می کنیم. ما با استفاده از رویکرد چند پارادایمی با نگاهی به آینده در مورد کارایی و اثربخشی مدیریت امنیت اطلاعات نتیجه گیری می کنیم.

مدیریت امنیت اطلاعات

مسائل و روندها

مدیریت امنیت اطلاعات یک چارچوب برای اطمینان از اثربخشی کنترل امنیت اطلاعات بر منابع اطلاعاتی است. این، نظارت و کنترل مسائل امنیتی مربوط به رعایت سیاست های امنیتی، فن آوری ها و اقدامات مبتنی بر تصمیمات یک انسان را مورد بررسی قرار می دهد. هدف مدیریت امنیت اطلاعات، اطمینان از عدم انکار، اعتبار، محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات درون یک سازمان است. اگرچه فن آوری های امنیتی مختلف از توابع امنیتی ویژه پشتیبانی می کنند، مسائل بسیاری وجود دارد که بر مدیریت موثر امنیت اطلاعات تأثیر می گذارد. این تکنولوژی ها کارآمد و مقیاس پذیر نیستند، زیرا آنها به تخصص انسانی متکی هستند تا به طور دوره ای داده ها را تجزیه و تحلیل کنند. بسیاری از دستگاه ها و سیستم ها، صدها رویداد را ایجاد می کنند و مشکلات یا نشانه های مختلف را گزارش می دهند. همچنین این دستگاه ها ممکن است همه در زمان های مختلف و از فروشندگان مختلف با قابلیت گزارش و مدیریت متفاوت و شاید بدت از همه

برنامه های بروز رسانی متفاوت ، بدست آیند. فن آوری های امنیتی یکپارچه نیستند و هر فن آوری، اطلاعات را در فرمت و معنی خود فراهم می کند. این سیستم های عملیاتی در سراسر نسخه ها، خطوط تولید و فروشندگان ممکن است ویژگی های سازگاری کم یا ناسلزگار با شرایط خاص خود را نشان دهند که نشان دهنده یک علامت مشابه هستند. این فن آوری ها فاقد ویژگی های جمع آوری و آنالیز داده های جمع آوری شده هستند. در مدیریت امنیتی، تحلیل گران باید نحوه انتخاب مشاهدات، جنبه‌های ایزوله کردن سود را انتخاب کنند. یک تصویر لحظه ای استاتیک ارائه‌شده توسط یک فن‌آوری امنیتی (حفاظت)، نوع درک مورد نیاز برای تحلیل پیش‌بینی را فراهم نمی‌کند. سازمانها بر روی انسانها مانند مدیر شبکه یا کارکنان امنیتی متکی هستند تا به طور منظم پایگاههای اطلاعاتی مختلفی را برای آسیب پذیری های جدید مورد استفاده قرار دهند و از سیستم های خود برای جلوگیری از حملات استفاده می کنند.

اغلب، کارمندان امنیتی مختلف مسئول نظارت و آنالیز اطلاعات ارائه شده توسط یک سیستم واحد هستند. گزارش ها نشان می دهد که کارمندان امنیتی به صورت دوره ای داده ها را تجزیه و تحلیل نمی کنند و به موقع جمع نمی شوند و نتایج گزارش های تجزیه و تحلیل را به تمام طرف های درگیر در مدیریت امنیت انتقال نمی دهند. همچنین ابزارهای کاربردی تاثیر بسیار کمی در پیشگیری از امنیت دارند، زیرا این سیستم ها به طور کلی قادر به تعمیم، یادگیری و سازگاری در زمان نیستند. فن‌آوری‌های امنیت کنونی فاقد یکپارچه‌سازی، پیش‌بینی و بازخورد بلادرنگ به انسان‌ها برای اتخاذ تدابیری برای جلوگیری یا توقف حمله هستند. همچنین، فناوری ها برای حملات در مقیاس بزرگ کارآمد نیستند. علاوه بر این، محدودیت‌های هر تکنولوژی امنیتی همراه با رشد حملات، اثربخشی مدیریت امنیت اطلاعات را تحت‌تاثیر قرار داده و فعالیت‌های انجام‌شده توسط مدیران شبکه را افزایش می‌دهد. مسائل خاص شامل جمع آوری داده ها، کاهش داده ها، نرمال بودن داده ها، همبستگی رویداد، طبقه بندی رفتار، گزارش گیری و پاسخ است. برای ارائه یک تصویر کامل، دقیق و جامع از وقایع شبکه ای که مورد نظر مدیران شبکه است، مقدار زیادی پردازش رویداد تقریبا بلادرنگ، رویدادها تثبیت و همبستگی مورد نیاز است.

بنابراین، راه حل های جامعی شامل شناسایی و فیلتر کردن حمله ، شناسایی و ردیابی منبع حمله و پیشگیری از حمله، مورد نیازاست (Chang، 2002). افزایش مکانیسم های حسابرسی خودکار و گزارش دهی هوشمند که ارزیابی امنیتی و مدیریت تهدید را پشتیبانی می کنند، ضروری است. Savely در مقدمه کتاب Giarratano and Riley خود گفت: "کلید اتوماسیون و آینده ما در استفاده موثر از حوزه علوم کامپیوتر به نام هوش مصنوعی است" (Giarratano & Riley, 1989). راه حل هایی که آنالیز بلادرنگ داده های تهدید را پشتیبانی می کنند، بسیار مهم هستند زیرا تشخیص زمان واقعی اجازه می دهد تا کارکنان امنیتی از نفوذ اولیه در چرخه حمله جلوگیری کنند. این امر موجب کاهش آسیب ناشی از حملات موفقیت آمیز و همچنین کاهش خطرات از دست دادن داده ها و نیاز به انجام بازیابی و تحلیل های قانونی گسترده پس از حادثه می شود.

بیانیه IBM (Kephart & Chess، 2003) مشکلات مدیریت سیستم های محاسباتی را نشان می دهد، چرا که پیچیدگی آن‌ها در حال نزدیک شدن به محدودیت‌های توانایی انسانی است در حالی که نیاز به افزایش اتصالات و ادغام وجود دارد. سیستم ها حتی برای عامل های(ایجادکننده ها) ماهر برای نصب، پیکربندی، بهینه سازی و نگهداری سیستم پیچیده تر می شوند. یکی از راه حل های پیشنهادی، سیستم های محاسباتی مستقل است که می توانند خود را با اهداف سطح بالای مدیران مدیریت کنند. این سیستم ها به قابلیت های خود پیکربندی،خود بهینه سازی ، خود شفا و خود محافظ نیاز دارند. متاسفانه، محاسبات خودمختار موفق هنوزهم در آینده است، سال های دور.

بر خلاف سیستم های مستقل، روند دیگری بر روی سیستم هایی است که متمرکز بر تعامل مؤثر عامل انسان هستند. برای مثال، سیاست های امنیتی می توانند اجرای عامل را کنترل و با یک انسان ارتباط برقرار کنند تا اطمینان حاصل شود رفتار عامل با محدودیت های مورد نظر و اهداف سیاست های امنیتی مطابقت دارد (Bhatti, Bertino, Ghafoor & Joshi, 2004; Bradshaw, Cabri & Montanari, 2003). راه حل های مدیریت رویداد امنیتی برای ادغام داده های تهدید از محصولات مختلف امنیتی و شبکه برای حذف هشدارهای اشتباه، وقایع مربوط به منابع مختلف و رویدادهای قابل توجه برای کاهش خطرات ناامن و بهبود کارایی امنیت عملیاتی مورد نیاز هستند. نیاز به افزایش استفاده از ابزارهای خودکار برای پیش بینی وقوع حملات امنیتی وجود دارد. مکانیزم

های رسیدگی و گزارش دهی هوشمند باید ارزیابی امنیتی و مدیریت تهدید را در مقیاس وسیعتر و در ارتباط با رویدادهای گذشته، جاری و آینده پشتیبانی کنند. ابزارهای خودکار باعث کاهش بار بر روی انسان می شود تا داده های قابل توجهی که توسط منابع مختلف جمع آوری شده پردازش شوند. همچنین، آن‌ها به طور قابل‌توجهی زمان را برای استخراج اطلاعات از سیستم‌های متعدد کاهش می‌دهند و ریسک از دست دادن حملات احتمالی را کاهش می‌دهند.

مدیریت امنیت اطلاعات کارآمد به یک رویکرد مدیریت رویداد امنیتی با افزایش قابلیت های بلادرنگ ، تطبیق و تعمیم پیش بینی حملات احتمالی و حمایت از اقدامات انسانی نیاز دارد.Dowd و McHenry (1998) اشاره می کنند که "امنیت شبکه باید بهتر درک و پذیرفته شود" و استراتژی هایی مانند شناخت پتانسیل حمله کننده، ارزش دارایی های محافظت شده و درک منابع خطر مانند سیستم مدیریت ضعیف، مهندسی اجتماعی ، نفوذ خارجی یا داخلی،را پیشنهاد می کنند . برای ارائه حفاظت در برابر آخرین نسل از تهدیدات سایبری، قوانین محافظت پیشگیرانه باید معیارهای اثربخشی، عملکرد و حفاظت را برآورده کنند. اثربخشی سیستم مدیریت امنیت توسط هوش سیستم تعیین می‌شود، که به عنوان توانایی تشخیص دقیق حملات ناشناخته ، به همراه زمان کافی برای اقدام استراتژیک علیه مهاجمان،تعریف می‌شود (Wang, 2005).

تهدیدات امنیت اطلاعات

تهدیدات امنیتی اطلاعات به دو دسته تقسیم می شوند (Tassabehji، 2005):

- منابع فنی مانند حملات نفوذ، کاوش کردن و یا اسکن، استراق سمع خودکار، حملات رمز عبور خودکار، spoofing(گمراه کردن)، انکار سرویسها و بدافزارها
- غیر فنی مانند بلایای طبیعی، حملات زیرساختی فیزیکی، خطاهای انسانی و مهندسی اجتماعی.

اگر سازمان ها از یک ابزار خودکار برای تجزیه و تحلیل رفتار شبکه استفاده می کردند، خسارات ناشی از کرم Slammer در ژانویه سال ۲۰۰۳ می توانست بسیار کاهش یابد یا از آن اجتناب شود.

این کرم حداقل ۷۵،۰۰۰ میزبان را آلوده کرده است و موجب وقفه فعالیت های تجاری و روزمره شده است (لغو پروازهای هواپیما، دخالت در انتخابات و خرابی ماشین خودکار بانک) (Moore et al, 2003). این کرم به سرعت از یک شبکه به یک دیگر پخش شد. این کرم به علت فرسودگی منابع (CPU و حافظه) و حملات داخلی DoS از جمله افزایش ترافیک چند ریخته گری، باعث ترافیک سنگین در شبکه، مصرف پهنای باند، تجهیزات شبکه و سرورهای سرور شد. اگر تمام این روندهای اندازه گیری مورد تجزیه و تحلیل قرار می گرفتند و همبستگی با یک ابزار هوشمند انجام می شد، آسیب های ناشی از این کرم می توانست به میزان قابل توجهی کاهش یا نادیده گرفته شود. تفسیر ترافیک شبکه نیاز به بررسی بسیاری از چیزها دارد و به منطق تجزیه و تحلیل بسیاری از داده ها برای ترسیم تفسیر یا نتیجه گیری در یک زمان کوتاه نیاز دارد.

مدیریت کارآمد امنیت اطلاعات مستلزم درک فرآیندهای اکتشاف و بهره‌برداری برای حمله است. به طور معمول یک حمله یک مجموعه از مراحل است. مرحله اول کشف یا شناسایی شبکه است. مهاجم اطلاعات مربوط به هدف را با استفاده از پایگاه‌های داده عمومی و اسناد و همچنین اسکنرهای تهاجمی و گیرنده ها جمع‌آوری می‌کند. سپس، مهاجم تلاش می کند آسیب پذیری های سرویس های شناسایی شده را ، یا از طریق تحقیق بیشتر یا با استفاده از یک ابزار طراحی شده برای تعیین اینکه آیا سرویس حساس است یا نه،کشف کند. از نقطه‌نظر خسارت، اسکن کردن معمولا بی‌خطر است. سیستم های تشخیص نفوذ، اسکن ها را به عنوان حملات سطح پایین دسته بندی می کنند، زیرا آنها به سرور یا سرویس آسیب نمی رساند و مدیران شبکه این اطلاعات را نادیده می گیرند.

با این حال، اسکن ها پیشگامان حملات هستند. اگر یک پورت کشف شود، هیچ تضمینی وجود ندارد که مهاجم به آن بازگردد، اما احتمال دارد که او بیاید و فاز حمله آغاز شود. چندین سرویس و برنامه کاربردی هدف حمله قرار می گیرند. علیرغم استفاده از فن آوری های امنیتی، مدیران شبکه باید تصمیم بگیرند که چگونه سیستم ها را از حملات مخرب و ناکامی های متوالی ناخواسته محافظت کند. یک روش بنام شناسایی، توسط هکرها برای انتخاب شبکه‌ها و دامنه‌ها برای جستجوی اهداف استفاده می‌شود. شناسایی به یک هکر اجازه می‌دهد تا اهداف مورد حمله قرار گرفته شده و یا مورد استفاده برای انجام حملات را شناسایی کند. اهداف، سیستم یا شبکه های آسیب پذیر

هستند. برای محافظت در برابر مهاجمان بالقوه، لازم است که روش ها و دلایل شناسایی آنها را درک کنید. برای مثال، با دانستن اهداف شناسایی هکرها، مدیران شبکه و پرسنل امنیتی می‌توانند اهداف را تایید کرده و امنیت اهداف یا شبکه را بهبود بخشند. بنابراین، نظارت و تجزیه و تحلیل الگوهای شناسایی هکرها باید به درستی و به طور مداوم انجام شود تا تاثیری که آنها ممکن است در مدیریت امنیت داشته باشند تعیین شوند. در حمایت از این فعالیت ها، مدیران شبکه و کارمندان امنیتی نیازمند روش های خودکار و موثر برای شناخت و تحلیل الگوهای شناسایی هستند.

بخش زیر در مورد برنامه های مختلف بر اساس تکنیک های مختلف هوش مصنوعی برای برنامه های نظارت، کنترل و امنیت صحبت می کند.

تکنیک های هوش مصنوعی

تکنیک‌های هوش مصنوعی مثل داده کاوی، شبکه‌های عصبی مصنوعی، منطق فازی و سیستم‌های خبره می‌توانند با روش‌های سنتی رویه‌ای و آماری، برای تجزیه و تحلیل داده‌های جمع‌آوری‌شده از طریق حسگرها، شناسایی الگوهای تشخیص، فیلتر و رویدادهای مرتبط برای پشتیبانی مدیریت رویداد امنیتی و جلوگیری از نفوذهای دامنه، ادغام شوند. این تکنیک ها توانایی سیستم های مدیریت امنیت را برای مرتبط کردن رویدادهای ایجاد شده توسط مجموعه متنوعی از ابزارهای مدرن که برای مدیریت شبکه و نظارت امنیتی مورد استفاده قرار می گیرند، بهبود دهند (Hentea، 2005a). روش های آماری برای ساختن مدل های تشخیص نفوذ و خرابی(Manikopoulos & Papavassiliou، 2002) استفاده شده است، اما این مدل ها قادر به یادگیری و سازگاری در زمان نیستند.

سیستم‌های خبره رایج‌ترین شکل از هوش مصنوعی هستند که امروزه در تولید، مخابرات، تجارت و حوزه‌های دیگر بکار گرفته می‌شوند. برای مثال، ریزسیستم خورشیدی یک سیستم تشخیص نفوذ مبتنی بر میزبان را با استفاده از تکنیک‌های سیستم خبره برای پلت فرم Solaris خورشیدی توسعه داد (Lindqvist & Porras، ۲۰۰۱). سیستم هایی که مبتنی بر سیستم خبره و تکنیک های

استنتاج هستند، کارآمد و مقیاس پذیر نیستند زیرا عمدتا به تخصص انسانی، حقایق و آمار های شناخته شده در قوانین پیاده سازی شده برای یک میزبان یا شبکه خاص و قابلیت آنها ،محدود است. با این حال، سیستم های خبره به یک روند جدید ادغام با پردازش اطلاعات سنتی تکامل یافتند، به طوری که در اوایل دهه نود، سیستم های خبره با یک زیرساخت جدید مبتنی بر تکنولوژی knowledgebased ادغام شدند.

سیستم های مبتنی بر دانش، شبکه های عصبی مصنوعی و منطق فازی، رویکردهای امیدوار کننده ای از AI برای برنامه های کاربردی مانند خرابی ها و نظارت بر وقایع، تشخیص، انزوا، عیب یابی، نظارت و کنترل تطبیقی، کنترل مستقیم (Rodd، 1992) هستند. کنترل تطبیقی به توانایی سیستم برای تنظیم(تطبیق) خود با خروجی مطلوب با وجود تغییر اهداف کنترل و شرایط فرآیند یا عدم قطعیت در پویایی فرآیند اشاره دارد. تکنیک های مرتبط با کنترل هوشمند شامل کنترل فازی، خبره و عصبی هستند (Hentea، 1997؛ Passino & Ozguner، 1996). سیستم های هوشمند برای اتوماسیون تولید در شرکت فورد موتور (Rychtyckyj، 2005) توسعه داده شده اند.

یک سیستم چند عاملی به عنوان چند عامل تعامل کننده طراحی و اجرا می‌شود. سیستم های چند عاملی برای نشان دادن مشکلاتی که دارای روش های متعدد حل مسئله و دیدگاه های متعدد هستند، مناسبند. عوامل هوشمند در جایی که مناسب بوده و تعامل اجتماعی داشته باشند، با دیگر عوامل مصنوعی و انسان‌ها به منظور تکمیل حل مسئله و کمک به دیگران با فعالیت‌هایشان، اقدام به عمل می‌کنند.

اگرچه تکنیک های مبتنی بر AI برای پشتیبانی مدیریت امنیت اطلاعات در حال ظهور هستند، اما هنوز روی محدوده محدودی تمرکز دارند. به تازگی روش های AI برای ایجاد سیستم های تشخیص و پیشگیری از نفوذ قوی مورد بررسی قرار گرفته اند. چندین تکنیک و نمونه از برنامه های کاربردی برای سیستم های تشخیص نفوذ و سیستم های پیشگیری در (Hentea، 2005b) مورد بحث قرار گرفته است. سیستم های هوشمند برای مدیریت عملکرد شبکه مانند نظارت، تشخیص و یا مدیریت منابع شبکه خاص در (Berenji، 1994، Hentea، 1999؛ Turban، Aronson & Liang، 2005) بحث شده اند. به عنوان مثال، نرم افزار WatchGuard شامل یک

عامل هوشمند است که از قابلیت های محدود برای مدیریت پیکربندی فایروال پشتیبانی می کند (http://www.watchguard.com). تکنیک های شبکه های عصبی مصنوعی برای برنامه های شناسایی بیومتریک پیشنهاد شده است (Kung، Mak & Lin، 2005). یک سیستم مبتنی بر عامل شبکه عصبی برای مدیریت سرور پست در Willow (2005)مورد بحث قرار گرفته است.

تکنیک های AI می توانند در ساخت مدل های هوشمند برای بهبود مدیریت امنیت اطلاعات، قابلیت تشخیص نفوذ و پیشگیری، کارایی مدیریت رویداد امنیتی و تصمیم گیری (Hentea، 2003، 2004، 2005b، 2005c) استفاده شوند. سیستم های هوشمند به نام "دستیار هوشمند" به کاربران در فرایند تصمیم گیری برای پیکربندی و نظارت بر معیارهای خاص، خرابی ها و ارتباطات رویدادها کمک می کند که میتواند منجر به شناسایی و پیشگیری از حملات سایبری شود. مدیریت امنیت اطلاعات کارآمد نیازمند یک سیستم هوشمند است که از رویکرد مدیریت رویداد امنیتی ،با افزایش قابلیت‌های بلادرنگ، تطبیق و تعمیم برای پیش‌بینی حملات احتمالی و حمایت از اقدامات بشر، پشتیبانی می‌کند. بخش زیر مفاهیم اساسی و توابع اصلی سیستم هوشمند برای مدیریت امنیت اطلاعات (ISISM) را توصیف می کند.

معماری ISISM

هر سیستم هوشمند متشکل از دو بخش است (Meystel & Albus، 2002):

۱- داخلی یا محاسباتی که می تواند به چهار زیر سیستم هوشمند داخلی ، به شرح زیر،تقسیم شود :

a. پردازش حسی- ورودی های سیستم های هوشمند از طریق حسگر ها تهیه و پردازش می شوند تا وضعیت ثابتی از دنیا را ایجاد کنند. سنسورها برای نظارت بر وضعیت دنیای خارج و سیستم هوشمند خود استفاده می شوند.

b. مدل سازی جهانی - برآورد وضعیت جهان است؛ این شامل پایگاه داده های دانش مربوط به جهان است و شامل یک ماژول شبیه سازی است که اطلاعاتی در مورد وضعیت های آینده جهان ارائه می دهد.
c. تولید رفتار - ماژول تصمیم گیری است که اهداف و برنامه ها را انتخاب می کند و وظایف را اجرا می کند.
d. قضاوت ارزش - هر دو حالت مشاهده‌شده و حالت پیش‌بینی‌شده را ارزیابی می‌کند؛ و اساس تصمیم‌گیری را فراهم می‌کند.

۲- خارجی یا رابط ؛ ورودی و خروجی بخش داخلی سیستم های هوشمند از طریق سنسورها و فعال کنده هایی که می توانند بخش های خارجی باشند، تعمیم داده می شوند.

در تمام سیستم های هوشمند، یک سیستم پردازش حسی، داده های سنسورها را برای به دست آوردن و حفظ یک مدل داخلی (نماینده) جهان، پردازش می کند. سپس، یک زیرسیستم تولید رفتار تصمیم گیری می کند که اقدامات لازم برای دستیابی به هدف انجام شود. زیرسیستم تولید رفتار، فعال کننده ها را برای پیگیری اهداف رفتاری در زمینه مدل جهان درک شده ، کنترل می کند. خروجی های سیستم های هوشمند، دستورات یا اقدامات را برای کنترل سیستم هدف تولید می کنند.داده ی سنسورها، برای ایجاد پایگاه های دانش، اختراع دانش جدید، شناسایی و پیش بینی حملات سایبری، و تصمیم گیری های به موقع، بنیادی و مهم هستند . نمونه هایی از داده سنسورها شامل اندازه گیری های مربوط به عملکرد، امنیت، وضعیت برای موارد زیر می باشد:

- دستگاهی مانند عملکرد CPU، کارایی حافظه، فضای دیسک استفاده شده، تعداد دفعات استفاده از پرونده ها، تعداد اتصالات باز، تعداد ورودی های شکست خورده، تعداد تراکنش ها (پرس و جو، به روز رسانی، حذف)، درخواست های کاربر جدید، درخواست های نرم افزاری جدید، کاربر پایانی، زمان پاسخ، تعداد دسترسی کاربران به سیستم در یک زمان، تعداد کاربران همزمان، تغییرات پیکربندی، دسترسی به فایل ها در هر استفاده، تعداد فراخوانی های سیستم، تعداد هشدارها، تعداد شکست های تأیید هویت کاربر، تعداد اتصالات

در حال انتظار، زمان وقفه دوره ها، زمان اجرای برنامه، کارایی فایل های سیستمی، کارایی کتابخانه های عمومی، پروتکل های هماهنگ سازی ساعت، ساعت سیستم، دسترسی کاربر به داده ها و فایل های اجرایی، اندازه پرونده ها و غیره

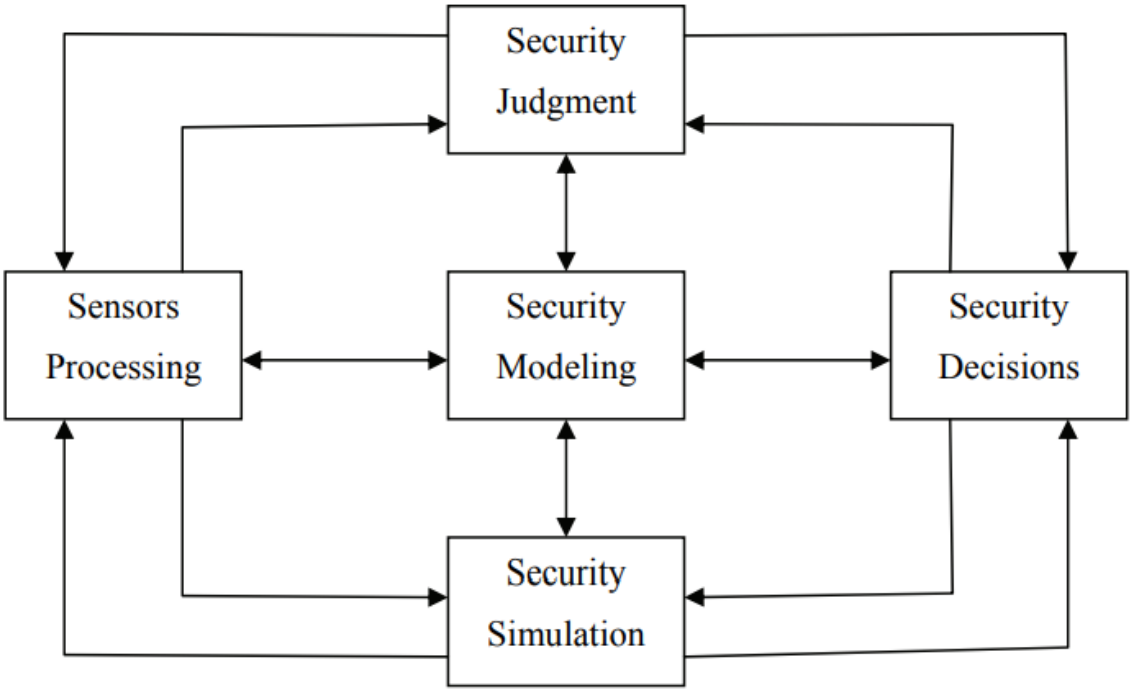
- شبکه ای مانند پهنای باند موجود، تاخیر، درخواست دسترسی به شبکه، تعداد منابع ناموجود برای مدت زمان طولانی، درخواست پروتکل جدید، تعداد پورت های باز هم همزمان، تعداد معاملات همزمان در اینترنت، تعداد معاملات همزمان اینترانت، تغییرات پیکربندی، نویز زیاد در مدار مورد نیاز برای ارسال مجدد، تعداد بسته ها، تعداد پیام های پست الکترونیکی، تعداد پیام های کنسول، استفاده از پروتکل ها و غیره
- رابطه ای مانند آمارهای مصرف
- محیطی (درجه حرارت، درب باز، درب قفل شده، هشدار)
- محافظ های امنیتی (فایروال ها، سیستم های تشخیص نفوذ، نرم افزار ضد ویروس، شبکه خصوصی مجازی، رمزنگاری) مانند: تعداد اتصالات انکار شده، تعداد هشدارها، تعداد positives کاذب، تعداد negatives کاذب، خرابی، زمان نگهداری، تعداد نرم افزار به روز رسانی، فعالیت های شناسایی، تعداد کلید های رمزگذاری و رمزگشایی، دسترسی از راه دور و غیره
- سیاست های امنیتی (تاریخ انتشار، تاریخ تجدید نظر، اهداف و غیره)
- خطرات (پذیرفته شده، کاهش یافته، انتقال یافته)
- برنامه های احتمال وقوع و بازیابی
- فعالیت های امنیتی و شبکه ای مدیران (ورود به سیستم، تغییرات پیکربندی، نصب نرم افزار، به روز رسانی نرم افزار، آزمایش، تعداد پیام های اعلان، برنامه های کاربر اجرا شده، و غیره).

ما معماری سیستم اشاره شده در (Meystel & Abus، 2002) که براساس تکنیک های کنترل واقعی (RCS) است، را تطبیق می دهیم.(Meystel & Albus (2002, p. 19 اشاره می کند که "هوش در سیستم ها بوسیله یک معماری قطعی ایجاد می شود که عملکرد مشترک دستگاه های دیگر غیر هوشمند را سازماندهی می کند". تمام عناصر هوش مبتنی بر حلقه عملکرد اولیه (عامل

خود مختار) هستند که اجازه می دهند تا روابط کاربردی و جریان اطلاعات ایجاد شوند. شکل ۱ اجزای اساسی یک عامل خود مختار(مستقل) برای امنیت را نشان می دهد. امنیت سایبری یک شرکت مشاهده و یا کنترل شده به عنوان وسیله ای برای فعالیت های اولیه حلقه عملکرد، عمل می کند. این عامل به عنوان ورودی ها و اقدامات به عنوان خروجی های آن (از طریق سنسورها) وارد می شوند (از طریق سنسورها به نام عملگرها).

این عامل به عنوان ورودی ها و اقدامات به عنوان خروجی های آن (از طریق سنسورها) وارد می شوند (از طریق سنسورها به نام عملگرها). عامل های نرم افزار، واحد های محاسباتی هستند که بارها در سیستم هوشمند در سطوح مختلف مختلف تکرار می شوند که به عنوان واحدهای اطلاعاتی در تمام زیر سیستم ها، به نهادها، حوادث، موقعیت ها و اهداف تجزیه شده به اقدامات زیر اهداف و تولید یا دستورات، جمع می شوند. در هر حلقه، سنسورهای امنیتی پردازش و مدلسازی امنیتی، یک پایگاه اطلاعاتی با محدوده و رزولوشن مشخص ،را حفظ می کنند. در هر سطح، برنامه ها با افق های برنامه ریزی مختلف ساخته و به روز می شوند. در هر سطح، حافظه کوتاه مدت داده حسی را، بر روی فواصل زمانی مختلف داده های مختلف، نشان می دهد. در هر سطح، حلقه های کنترل بازخورد، یک مشخصه دارند. به عنوان مثال، متغیرهای کنترل شده می توانند پهنای باند و تاخیر شبکه باشند.

این مدل یک سلسله مراتب چند حلقه ای از حلقه های محاسباتی، بینش عمیقی در زمینه پدیده های رفتار، ادراک، شناخت، حل مسئله و یادگیری ، به دست می دهد. معماری یک سیستم هوشمند، چارچوب خاصی از عوامل است و هر عامل معماری خاص خود را دارد. در هسته هر سیستم هوشمند، مفهوم عامل ، عمومی است. عامل های با عملکرد مشابه می توانند به تدریج در یک نوع عامل گروهی که یک عامل تعمیم یافته است، توزیع شوند. عامل گروهی ،نماینده جدید جهان را (یا گرانولاسیون جدید یا قطعنامه جدید) ارائه می دهد. علاوه بر این، عوامل گروهی را می توان در یک ساختار سلسله مراتبی به یک عامل تعمیم یافته بیشتر (گروهی از عوامل گروهی) تقسیم کرد. این معماری مدلی از مدیریت امنیت اطلاعات را پشتیبانی می کند.



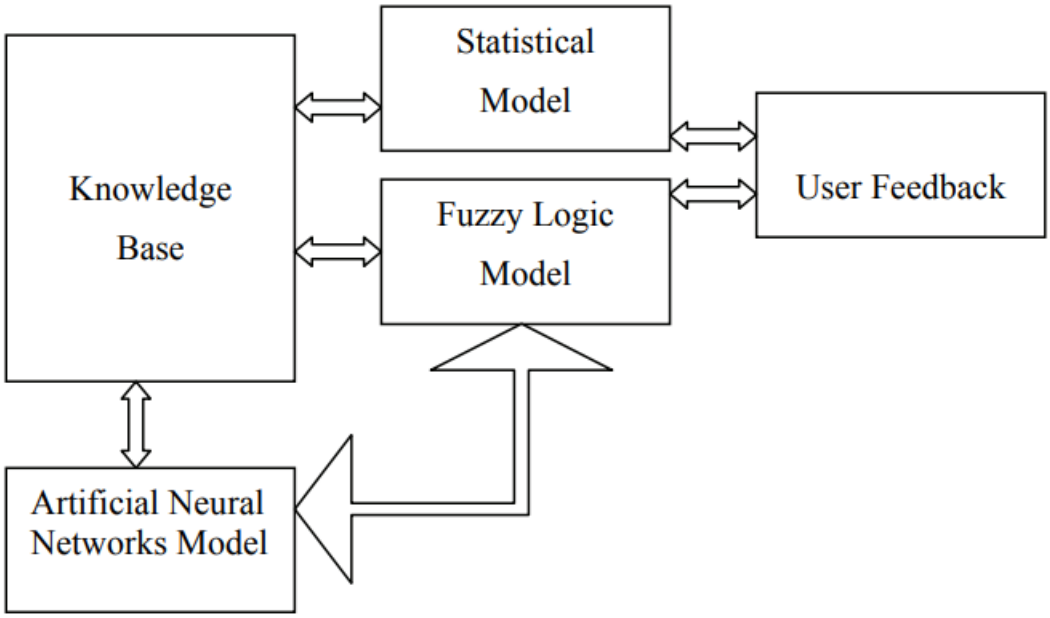
شکل ۱: عامل خودمختار، اقتباس شده از (Meystel & Albus، 2002)

عامل های نرم افزاری که می توانند مکان خود را در سیستم تغییر دهند عامل های سیار نامیده می شوند. عوامل سیارمی توانند در یک شبکه حرکت کنند و وظایف را بر روی ماشین های دیگر انجام دهند. این کار به شما این امکان را می‌دهد که از کامپیوتر به کامپیوترمهاجرت کرده و به مبدا آن‌ها برگردید. همچنین، فرایند مهاجرت به کد اجرایی اجازه می دهد تا با پایگاه های داده، سیستم های فایل، سرویس های اطلاعاتی و عوامل دیگر ارتباط برقرار کند. عاملهای سیازبرای شناسایی سرویس های شبکه در محیط های زندگی (شبکه های سیار adhoc) استفاده می شوند (Kopena et al, 2005). فضاهای هوشمند مبتنی بر دستگاه های هوشمند در حال تبدیل شدن به برنامه های رایج در خانه های هوشمند، محل کار، کلاس های درس، بیمارستان ها و خدمات حمل و نقل هستند (Yang & Wang، 2005).

معماری پیشنهادی شامل عناصر هوش برای ایجاد روابط کاربردی و جریان اطلاعات بین زیر سیستم های مختلف است. عناصر هوش مبتنی بر اجزاء مورد استفاده یک یا چند تکنیک AI: پردازش زبان

طبیعی، شبکه های عصبی مصنوعی، منطق فازی هستند. علاوه بر این، مزایایی را در توسعه سیستم هوشمند، مرکب از تکنیک های AI با تکنیک های دیگر مانند برنامه نویسی معمول و بسته های آماری که معماری یک سیستم هوشمند ترکیبی را ایجاد می کنند ،می بینیم(Zahedi، 1993).

شکل ۲ معماری پیشنهادی سیستم دستیار هوشمند مبتنی بر ادغام روش های آماری سنتی و تکنیک های مختلف AI را برای پشتیبانی از یک سیستم کلی که به طور خودکار، سازگار و فعالانه عمل می کند، را نشان می دهد.



شکل ۲: مولفه های مدل هوشمند

معماری سیستم مبتنی بر رویکرد ترکیبی است که قدرت و عمق درک تصمیم گیری را با استفاده از مدل های هوشمند به ارمغان می آورد. هدف این سیستم بهبود فرآیندهای نظارت و تصمیم‌گیری باوسیله میزان نتیجه است که بالاتر از یک متخصص در امنیت است. علاوه بر این، این سیستم مکانیسم هایی را برای ارتقای ساخت دانش فعال در مورد تهدیدات، سیاست ها، رویه ها و خطرات فراهم می کند. این مدل سازگار است و از پردازش و طبقه بندی رویدادها و داده ها که منجر به پیش بینی حملات می شوند، پشتیبانی می کند. هر گونه وقوع فعالیت می تواند یک رویداد در نظر گرفته شود، از اجرای برنامه اسکن ویروس تا ورود به یک دستگاه.

یکی از اجزای اصلی طراحی، توسعه یک مدل هوشمند برای تحلیل و همبستگی وقایع و داده ها در زمان واقعی برای افزایش قابلیت تشخیص و پیشگیری از تکنولوزی های امنیتی است: سیستم های تشخیص نفوذ، فایروال ها، نرم افزارهای ضد ویروس، فیلتر های هرزنامه ، سیستم های ارزیابی آسیب پذیری و غیرهبه عنوان مثال، مدل های عصبی و فازی باید سازگار باشند و از پردازش و طبقه بندی رویدادها و داده ها پشتیبانی کنند که منجر به پیش بینی حملات و همچنین توصیه به کاربر از طریق رابط بازخورد کاربر می شود. همچنین مدل منطق فازی از مدیریت ریسک، یک مرحله بحرانی در چرخه حیات مدیریت امنیت اطلاعات، پشتیبانی می کند (Hentea، 2006). این مدل‌ها همچنین باید گسترش داده شوند تا شامل ورودی طرح‌های امنیتی و معیارهای کنترل شبکه، حسابرسی، کنترل‌های دسترسی فیزیکی و منطقی باشند. این مدل ها باید از وظایف مدیریت امنیت اطلاعات مانند نظارت، ردیابی، شناسایی تهدیدها و همچنین جلوگیری از حمله با اقدامات پیشگیرانه در صورت لزوم، ارائه اطلاعات مفید در مورد حمله مداوم و پیش بینی حملات احتمالی، پشتیبانی کنند.

نتایج حسگرها درون مولفه پردازش سنسور کدگذاری، فیلتر و پردازش شده است و به سایر اجزای عامل خودمختار (حلقه عملکردی اولیه) که در شکل ۱ نشان داده شده است، ارائه می شوند. هر جزء از حلقه در حال کار ابتدایی ممکن است شامل یک یا چند مدل از شکل ۲ باشد. داده ها به مدل سازی امنیتی، شبیه سازی امنیت و یا مولفه های رفتاری ژنراتور منتقل می شوند که سازماندهی، طبقه بندی، ترکیب و ارتباط داده ها یا دانش جدیدی را که در پایگاه دانش ذخیره می شود تولید می کنند.

سیستم ترکیبی ، ادغام مدل های مختلف برای مدیریت رویداد امنیتی سازگار با تکنیک های AI و سایر روش های مبتنی بر رویکرد آماری و سنتی است. ایده اصلی مدل های چندگانه این است که توابع مستقل مختلف با اقدامات مختلف را اجرا کنند و ضعف های یک مدل با نقاط قوت مدل دیگری تکمیل کنند. برای مثال، شبکه های عصبی مصنوعی میتوانند برای طبقه بندی الگوهای شناسایی استفاده شوند، اما خروجی ها یا پارامترها میتواند به یک سیستم خبره منطق فازی ارائه شوند که میتواند دادهها را برای انسان تفسیر کند. از آنجا که خروجی مدل ها در بعضی از شرایط

نامعلوم و مبهم است و کارشناسان انسانی می توانند برخی از شهود و یا دانش در مورد ویژگی های اطلاعات ارائه شده را داشته باشند، یک مدل خبره منطق فازی می تواند نتایج مدل های شبکه های عصبی را بهبود بخشد و یا فقط نتایج را از مدل های دیگر در قالب هایی که انسان ها با آن ارتباط بیشتری دارند، تفسیر کند. علاوه بر این، از مدل منطق فازی برای یادگیری قوانین فازی استفاده می شود در صورتی که هیچ اطلاعات قبلی درباره قوانین فازی و مجموعه های فازی وجود نداشته باشد.

این مدل بر اساس تکنولوژی عامل برای نظارت، کشف و شناسایی تهدیدها و جلوگیری از حمله با ارائه اطلاعات مفید قبل از حمله است. برنامه های کاربردی مبتنی بر عامل در تولید، کنترل فرایند، سیستم های مخابراتی، کنترل ترافیک هوایی، مدیریت ترافیک و حمل و نقل، فیلتر کردن و جمع آوری اطلاعات، تجارت الکترونیک، مدیریت فرایند کسب و کار، سرگرمی و مراقبت های پزشکی مورد استفاده قرار گرفته اند(Jennings، Sycara & Wooldridge، 1998) . وانگ (۲۰۰۵) درباره کنترل مبتنی بر عامل هوشمند سیستم های مدیریت ترافیک شبکه و سیستم های حمل و نقل صحبت می کند.

سیستم باید شامل توابع برای کارهای خودکار مانند جمع آوری داده ها، کاهش داده ها، فیلتر کردن، و همبستگی رویداد بر اساس تکنولوژی های چند عاملی باشد. عوامل هوشمند از معیارهای امنیت اطلاعات، نظارت، تحلیل و کنترل پشتیبانی می کنند. سیستم ممکن است دستوراتی برای پایان دادن به پردازش ها یا انتقال پردازش به دستگاه دیگر زمانی که علائم رفتاری مشکوک یا خرابی شناسایی می شوند تولید کند.Devi & Ramachandran (2002) یک سیستم چند عامله برای مدیریت شبکه را توصیف می کند که در آن عوامل در مورد عملکرد پردازنده ها در شبکه خوشه ای، که عملکرد خدمات کاهش می یابد، مذاکره می کنند.

علاوه بر این، سیستم ما یک دستیار هوشمند برای ارائه بازخورد کاربر مانند کمک به تصمیم گیری و اقدامات است. علاوه بر این، سیستم باید شامل یک رابط کاربری مبتنی بر چند رسانه ای برای پشتیبانی از عملیات مدیر شبکه و یک پایگاه دانش برای حفظ اعتبار به عنوان تغییر و سازگاری سیستم باشد. این پایگاه دانش باید سازگار باشد و از طریق وب به اشتراک گذاشته شود. اعتبار

سنجی تصمیمات تولید شده توسط کامپیوتر را می توان بوسیله مقایسه با تصمیمات کارشناسان انجام داد. این روش علاوه بر روش‌های خودکار برای کشف دانش، امکان ایجاد پایگاه دانش برای تصمیم‌گیری و اتخاذ اقداماتی با استفاده از تجربه و تجربه انسانی را فراهم می‌آورد.

ماژول بازخورد کاربر باید بازخورد های مختلفی را به یک مدیر شبکه یا کارکنان امنیتی ارائه کند. نوع بازخورد موجود، مهم است. بازخورد مستقیم شامل اطلاعات خاصی در مورد نتایج و تأثیر هر بازخورد احتمالی می شود. بازخورد غیر مستقیم در سطح بالاتری است، بدون اطلاعات خاص در مورد تغییر فرد یا پیش بینی، اما آیا برنامه یادگیری می تواند استراتژی های جدید و تغییرات را پیشنهاد دهد. این یک جنبه مهم یادگیری ماشین است.بخش عمده‌ای از تحقیقات یادگیری ماشین به جای ایجاد بازخورد به عنوان اطلاعات مفید برای تصمیم گیری کاربر، روی بخش یادگیری متمرکز شده‌است. هدف سیستم هوشمند در حال توسعه، تکنیک های یادگیری است که می تواند از کسب و کار پشتیبانی کند و تصمیم گیری قبل از حمله به اطلاعات یا ایجاد سیستم ناموجود را به کاربر توصیه کند. یکی دیگر از عوامل مهم در نظرگرفتن این است که سیستم ها و سیاست های امنیتی در طول زمان و در سراسر سیستم پلت فرم ها و کسب و کارها تغییر می کنند. این شرایط ویژه باید به راحتی و به موقع در برنامه یادگیری ماشین برای حمایت از کاربر گنجانده شوند. علاوه بر این، برنامه یادگیری ماشین باید از یک پایگاه دانش برای غنی سازی محیط یادگیری پشتیبانی کند.

مسائل طراحی

تصمیم اصلی در طول طراحی معماری، این است که باید شامل چه عواملی شوند.انواع مختلف عوامل را می توان برای مدیریت امنیت اطلاعات طراحی کرد (Norvig, 2003& Russell). در سیستم پیشنهادی، عوامل کلیدی باید عامل تصمیم گیرنده و عامل کنترل کننده باشند.

یک عامل هوشمند به عنوان ترکیبی از کارکردها و قابلیت‌های هوشمند (توانایی عمل در یک محیط نامطمئن، یادگیری، سازگاری، احتمال موفقیت)دیده می‌شود. ویژگی ها (در بعضی متدولوژی

ها،نقش ها نامیده می شوند) عوامل مؤثری هستند که با نگاه به ترکیب ویژگی ها انجام می شوند. اگر چه بحث های زیادی در مورد آنچه که یک عامل را تشکیل می دهد، وجود دارد واینکه کدام ویژگی های مهم است، اجماع نظر این است که یک عامل هوشمند ، مستقل، واکنش پذیر، پیشگیرانه و اجتماعی قرار گرفته است. اصلی ترین عامل در زمینه عوامل مستقل، هوش مصنوعی است.

با توجه به پیچیدگی وظایف مدیریت امنیت اطلاعات، سیستم پیشنهادی براساس ادغام انواع مختلف عوامل هوشمند، یک معماری ترکیبی تحت محدودیتهای زمان واقعی است. عوامل هوشمند در خودکار سازی وظایف مختلف مانند جمع آوری اطلاعات، فیلتر کردن و استفاده از آن برای پشتیبانی تصمیم گیری کمک می کنند و می توانند به بهبود بهره وری مدیر شبکه کمک کنند. طراحی و برنامه ریزی عوامل باید بر روی حداکثر سازی معیار عملکرد آنها تمرکز داشته باشد که شامل ملاک موفقیت یک رفتار عامل است (Russell & Norvig, 2003). سایر مسائل مهم دیگری که مورد نیاز هستند عبارتند از قابلیت حمل، ثبات، انعطاف پذیری و امنیت عامل ها و سیستم ها (Bradshaw et al، 2001؛ Hamidi & Mohammadi، 2006). رابط کاربری باید ویژگی های هوشمند را ارائه دهد که به کاربر در تصمیم گیری کمک می کند و اقداماتی را برای کنترل فرایند امنیتی انجام می دهد.

معیارهای عملکرد باید مطابق با آنچه در محیط مدیریت امنیت اطلاعات مورد نیاز است به جای توجه به اینکه چگونه یک نماینده باید رفتار کند طراحی شود. علاوه بر این، فاز طراحی باید نوع بازخورد موجود برای یادگیری را شناسایی کند، زیرا معمولا مهمترین عامل تعیین ماهیت، مسئله یادگیری است که عامل با آن مواجه است. یادگیری ماشین معمولا موارد یادگیری نظارت شده و بدون نظارت را تشخیص می دهد. دامنه مدیریت امنیت اطلاعات گسترده است و نیازمند استفاده از یک یا ترکیبی از هر دو شکل برای بدست آوردن بهترین نتایج است. مشخصه دیگری که باید در نظر گرفته شود تحرک پذیری است که در آن عوامل از طریق شبکه به آن سفر می‌کنند.

علاوه بر این، نماینده و نمایش داده ها (ورودی مدل برای یادگیری و خروجی مدل ها) نقش مهمی در طراحی دارد. عامل دیگری که در طراحی وجود دارد در نظر گرفتن در دسترس بودن دانش قبلی برای برخی از وظایف مدیریت امنیت اطلاعات است. اکثریت یادگیری با هیچ دانش و اطلاعاتی در

مورد آنچه که عامل سعی دارد یاد بگیرد شروع خواهد شد. یادگیری زمانی رخ می‌دهد که عامل تعاملات خود را با محیط و فرآیندهای تصمیم‌گیری خودش حفظ می‌کند. یادگیری یک فرایند خود بهبود و در نتیجه یک ویژگی مهم رفتارهای هوشمند است.

توابع اجرا شده توسط هر جز را می توان براساس روش توسعه حلزونی توسعه داد. مجموعه ای از قابلیت های ISISM بر اساس الزامات امنیتی هر سازمان است. منظور از اجرای مدلها بستگی به منابع و نیازها دارد. در زیر توضیح مختصری از ویژگی‌هایی که در پروژه‌های مختلف توسعه‌یافته و مورد استفاده قرار گرفتند، آورده شده‌است:

- داده کاوی به تجزیه و تحلیل خودکار و تفسیر داده ها و رویدادهای جمع آوری شده از منابع مختلف و همچنین کشف ارتباطات بین داده ها و رویدادها و بازخورد کاربر انسانی کمک می کند. مثال هایی از استفاده از تکنیک های داده کاوی و کشف دانش در (Hentea, 2004; Ibrahim, Folorunso & Ajayi, 2005) بحث شده است.
- شبکه های عصبی مصنوعی به طبقه بندی، ارتباط و پیش بینی حملات سایبری آینده بوسیله یادگیری و سازگاری داده ها و رویدادهای گذشته و حال، کمک می کنند. برای مثال، الگوهای شناسایی را می توان با استفاده از شبکه های عصبی بر اساس یادگیری بدون نظارت(Hentea، 2005b، 2005c) طبقه بندی کرد.
- منطق فازی اجازه پردازش متغیرهای کمی و استدلال تقریبی وقتی که پیشنهادها نادرست و مبهم هستند را می‌دهد.یک مدل برای ارزیابی ریسک استفاده شده است(Hentea، 2006)
- دستیار هوشمند و تکنیک های بازخورد کاربر در (Hentea، 1997) بحث شده است.
- رویکردهای آماری در (Hentea، 1997، 2006) بحث شده است.

با این حال، یک همکاری بین رویکردهای مختلف می تواند به بهبود و برجسته کردن جنبه های کیفی هر یک از مدل ها بپردازد، در نتیجه دانش و هوش را برای کمک به انسان برای تصمیم گیری ایجاد می کند. یک راه ممکن برای ادغام داده کاوی، شبکه های عصبی و سیستم های خبره فازی در رسیدگی به تلاش های نفوذ، استفاده از داده کاوی و شبکه عصبی برای کشف و طبقه بندی الگوهای شناسایی و ویژگی های آن است. این اطلاعات را می توان به سیستم خبره فازی اطلاع داد

که می تواند پس از آن به مشاوره به انسان پاسخ دهد تا اقدامات را بر اساس وضعیت تلاش های نفوذ انجام دهد. علاوه بر این، شبکه های عصبی می توانند الگوها را شناسایی و پیش بینی های حملات سایبری احتمالی را انجام دهند. همچنین شبکه های عصبی می توانند نتیجه ای از داده های فازی یا نامشخص در مورد یک وضعیت داده شده را ترسیم کنند. پایگاه دانش شامل دانش برای حوزه امنیتی مانند داده های خام و رویدادها، معیارهای عملکرد، الگوها، سیاست ها و تصمیمات است. علاوه بر این، پالایش دانش، نمایش دانش و کشف دانش، اجزای ضروری در یک سیستم مدیریت دانش هستند. نیاز دیگر هزینه های توسعه و نگهداری است. سیستم باید مقرون بصرفه باشد تا سازمان بتواند از فناوری های پیشرفته (داده کاوی، شبکه های عصبی مصنوعی، منطق فازی و پایگاه دانش) برای حفاظت و پیشگیری از امنیت استفاده کند (Wallich، 2003). اگرچه ما چندین قابلیت را برای این سیستم توصیف کردیم، اما ما یک لیست کامل از الزامات را ارایه نکردیم. هدف از این مقاله ارائه یک چارچوب برای طراحی یک سیستم هوشمند برای مدیریت امنیت اطلاعات است. سیستم های هوشمند مشابه برای تولید در (ISAM، 2007) شرح داده شده است.

نتیجه

تکنیک های پیشرفته بلادرنگ بر اساس مدل سازی، تجزیه و تحلیل حسگر و عوامل هوشمند که با روش های سنتی رویه ای و آماری ترکیب شده اند را می توانند رویدادها و اطلاعات جمع آوری شده توسط سنسورها و منابع مختلف را تشخیص ، فیلتر و مرتبط کنند. این تکنیک ها توانایی ارائه بازخورد خودکار برای اصلاح مشکلات از جمله توصیه های مفید برای انسان برای انجام اقدامات و جلوگیری از حملات مداوم را پشتیبانی می کنند. ما یک معماری جدید از یک سیستم هوشمند برای مدیریت امنیت اطلاعات پیشنهاد می دهیم. معماری پیشنهادی مبتنی بر نمونه های چند رشته ای است که شامل مدیریت امنیت اطلاعات، ارتباطات شبکه، اتوماسیون (کنترل فرآیند)، علوم کامپیوتر، هوش مصنوعی، نظریه کنترل مدرن، آمار، علوم اجتماعی، نظریه و رفتار سازمانی، علم مدیریت، استراتژی های تجاری، آنالیز ریسک و اقتصاد است. هیچ روش واحدی نمی تواند رشد و پیشرفت پیچیدگی تهدیدات اینترنتی را حل کند (Gordon، Loeb & Lucyshyn، 2006). ما

نیازمند بکارگیری چندین نمونه برای برآورده کردن اهداف مدیریت امنیت اطلاعات برای سازمان مدرن قرن بیست و یکم هستیم. براساس کار بنیادی در حوزه هوش مصنوعی و حوزه‌های دیگر، فن‌آوری عامل هوشمند کاربرد قابل‌توجهی در امنیت سایبری دارد. برخی از محققان تکنولوژی عامل هوشمند را به عنوان جانشین طبیعی برنامه نویسی شی گرا در نظر می گیرند. هیچ نمونه اولیه یا سیستمی از این نوع شناسایی نشده است. با این حال، نمونه‌های اولیه از ویژگی‌ها یا مولفه‌های منفرد و ایزوله شده در حال ظهور هستند، اما این مولفه‌ها نیازمند توسعه و یکپارچه‌سازی عمیق‌تر هستند. این سیستم باید وفقی و قادر به کشف و ایجاد دانش جدید برای حوزه امنیت اطلاعات باشد. کار آینده باید به دنبال یک اثبات مفهوم سیستماتیک باشد که تمام ماژول ها را برای پشتیبانی از مدیریت امنیت ادغام می کند.

منابع

Berenji, H.R. (1994). The unique strength of fuzzy logic control. IEEE Expert, 9 (4), 4.

Bhatti, R., Bertino, E., Ghafoor, A., & Joshi, J.B.D. (2004). XML-based specification for web services

document security. IEEE Computer, 37 (4), 41-49.

Bradshaw, J.M., Suri, N., Canas, A.J., Davis, R., Ford, K., Hoffman, R., Jeffers, R., & Reichherzer, T.

(2001).Terraforming cyberspace. Computer, 34 (7), 48-56.

Bradshaw, J. M. Cabri, J., & Montanari, R. (2003). Taking back cyberspace. IEEE Computer, 36 (7), 89-

92.

Cardoso, R.C. & Freire, M.M. (2005). Security vulnerabilities and exposures in internet systems and services. In M. Pagani, (Ed.), Encyclopedia of multimedia technology and networking (pp. 910-916). Hershey, Pennsylvania, IDEA GROUP REFERENCE.

Chan, H. & Perrig, A. (2003). Security and privacy in sensor networks. IEEE Computer, 36 (10), 103-105.

Chang, R.K.C. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial.

IEEE Communications Magazine, 40 (10), 42-51.

Devi, S.S.E. & Ramachandran, V. (2002). Agent based control for embedded applications. Retrieved December 16, 2006, from http://www.hipc.org/hipc2002/2002Posters/AgentControl.pdf

Dowd, P.W. & McHenry, J.T. (1998). Network security: it's time to take it seriously. IEEE Computer, 31

(9), 24-28.

Giarratano, J. & Riley, G. (1989). Expert systems principles and programming. Boston, Massachusetts,

PWS-KENT Publishing Co.

Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2003). Information security expenditures and real options: A

wait-and-see approach. Computer Security Journal, XIX (2), 1-7.

Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2006). Computer and cyber security breaches: Schumpeter to

the rescue. Computer Security Journal, XXII (4), 9-10.

Hamidi, H., & Mohammadi, K. (2006). Modeling fault tolerant and secure mobile agent execution in distributed systems. International Journal of Intelligent Information Technologies, 2 (1), 21-36.

Heimerl, J.L. & Voight, H. (2005). Measurement: The foundation of security program design and management. Computer Security Journal, XXI (2), 1-20.

Hentea, M. (1997). Architecture and design issues in a hybrid knowledge-based expert system for intelligent quality control. PhD Thesis, Illinois Institute of Technology, Chicago, Illinois.

Hentea, M. (1999). Intelligent approach for network management system: Architecture and design issues for ATM computer

networks. Proceedings of 1999 Advanced Simulation Technologies Conference, San Diego, California.

Hentea, M. (2003). Intelligent model for cyber attack detection and prevention. Proceedings of the ISCA

12th International Conference Intelligent and Adaptive Systems and Software Engineering, San Francisco, California, 5-10.

Hentea, M. (2004). Data mining descriptive model for intrusion detection systems. Proceedings of the

2004 Information Resources Management Association International Conference, New Orleans, Louisiana, 1118-1119.

Hentea, M. (2005a). Information security management. In M. Pagani, (Ed.), Encyclopedia of multimedia

technology and networking (pp. 390-395). Hershey, Pennsylvania, IDEA GROUP REFERENCE.

Hentea, M. (2005b). Improving intrusion awareness with a neural network classifier. Proceedings of the

ISCA 14th International Conference Intelligent and Adaptive Systems and Software Engineering, Toronto, Canada, 163-168.

Hentea, M. (2005c). Use of reconnaissance patterns for intelligent monitoring model. Proceedings of the

2005 Information Resources Management Association International Conference, San Diego, California, 160-163.

Hentea, M. (2006). Enhancing information security risk management with a fuzzy model. Proceedings of

19th International Conference on Computer Applications in Industry and Engineering, Las Vegas, Nevada, 132-139.

Hwang, M3-S. Tzeng, S-F. & Tsai, C-S. (2003). A new secure generalization of threshold signature

scheme. Proceedings of International Technology for Research and Education, 282-285.

Ibrahim, S.A., Folorunso, O. & Ajayi, O.B. (2005). Knowledge discovery of closed frequent calling patterns in a telecommunication database. Proceedings of the 2005 Informing Science and IT Education

Joint Conference, Flagstaff, Arizona, 137-148. Available at

http://proceedings.informingscience.org/InSITE2005/P13f80Ibra.pdf

ISAM. (2007). An intelligent systems architecture for manufacturing (ISAM): A reference model architecture for intelligent manufacturing systems. Retrieved January 15, 2007, from

http://www.isd.mel.nist.gov/projects/rcs/isam/ISAM_web.htm#framework

Jennings, N.R., Sycara, K. & Wooldridge, M. (1998). A roadmap of agent research and development. In N.

Jennings, K. Sycara, M. Georgeff (Eds.), Autonomous Agents and Multi-Agent Systems, 1 (1), pp. 7-38.

Boston, Massachussetts, Kluver Academic Publishers.

Kephart, J.O. & Chess, D.M. (2003). The vision of automatic computing. IEEE Computer, 36 (1), 41-50.

Kopena, J., Sulatanik, E., Naik, G., Howley, I., Peysakhov, M., Cicirello, V.A., Kam, M., & Regli, W.

(2005). Service-based computing on manets: Enabling dynamic intero-perability of first responders.

IEEE Intelligent Systems, 19 (5), 17-25.

Kung, S.Y., Mak, M.W., & Lin, S.H. (2005). Biometric authentication. Upper Saddle River, New Jersey,

Prentice Hall Professional Technical Reference.

Leighton, F.T. (2004). Hearing on the state of cyber security in the United States government. Computer

Security Journal, XX (1), 15-22.

Lindqvist, U. & Porras, P. A. (2001). eXpert-BSM: A host-based intrusion detection solution for Sun Solaris. Proceedings of the 17th Annual Computer Security Applications Conference, 240-251.

Maiwald, E. (2004). Fundamentals of network security. New York, New York, McGraw-Hill/Technology

Education.

Manikopoulos, C. & Papavassiliou, S. (2002). Network intrusion and fault detection: A statistical anomaly

approach. IEEE Communications Magazine, 40 (10), 76-82.

Mena, J. (2004). Homeland security connecting the DOTS. Software Development, 12 (5), 34-41.

Meystel, A.M. & Albus, J.M., (2002). Intelligent systems architecture, design, and control. New York,

New York, John Wiley & Sons, Inc.

Miller, S.K. (2001). Facing the challenge of wireless security. IEEE Computer, 34 (7), 16-18.

Moore, D., Paxson, V., Savage, S., Shannon, C, Stanford, S., & Weaver, N. (2003). Inside the Slammer

worm. IEEE Security & Privacy, 1 (4), 33-39.

Passino, K.M., & Ozguner, U.U. (1996). Intelligent control: From theory to application. IEEE Expert Intelligent System and Their Applications, 11 (2), 28-30.

Ramanujan, S. & Capretez, M.A.M (2005). ADAM: A multi-agent system for autonomous database administration and maintenance. International Journal of Intelligent Information Technologies, 1 (3),

14-33.

Rodd, M.G. (1992). Real-time AI for industrial control: A review. ICARV ’92 Second International Conference on Automation, Robotics and Computer Vision, Singapore, 36-38.

Russell, S. & Norvig, P. (2003). Artificial intelligence a modern approach (2nd ed.). Upper Saddle River,

New Jersey: Prentice Hall.

Rychtyckyj, N. (2005). Intelligent systems for manufacturing at Ford Motor company. IEEE Intelligent

Systems, 19 (5), 16-19.

Tassabehji, R. (2005). Information security threats. In M. Pagani, (Ed.), Encyclopedia of multimedia technology and networking (pp. 404-410). Hershey, Pennsylvania: Idea Group.

Turban, E., Aronson, J.E. & Liang, T-P. (2005). Decision support systems and intelligent systems (2nd ed.).

Upper Saddle, New Jersey: Prentice Hall.

Volonino, L. & Robinson. (2004). S.R. Principles and practice of information security. Upper Saddle

River, New Jersey: Pearson Prentice Hall.

Wallich, P. (2003). Getting the message. IEEE Spectrum, 40 (4), 39-42.

Wang, F-Y. (2005). Agent-based control for networked traffic management systems. IEEE Intelligent Systems, 19 (5), 92-96.

Wang, W. (2005). The intelligent proactive information assurance and security technology. Retrieved on

January 5, 2005, from

http://security.ittoolbox.com/browse.asp?c=SecurityPeerPublishing&r=http%3A%2F%2Fhosteddocs%

2Eittoolbox%2Ecom%2FIntelligentIPDMTheWinningFormula%2Epdf

Willow, C.C. (2005). A neural network-based agent framework for mail server management. International

Journal of Intelligent Information Technologies, 1 (4), 36-52.

Yang, L. & Wang, F-Y. (2005). Driving into intelligent spaces with pervasive communications. IEEE Intelligent Systems, 19 (5), 12-15.

Yao, Y., Wang, F-Y., Zeng, D. & Wang, J. (2005). Rule + exception strategies for security information

analysis. IEEE Intelligent Systems, 19 (5), 52-57.

Zahedi, F. (1993). Intelligent systems for business expert systems with neural networks. Belmont, California: Wadsworth Publishing Company.