DOR: https://dorl.net/dor/20.1001.1.28212606.1401.5.15.1.3

فصلنامه علمی آماد و فناوری دفاعی، سال پنجم، شماره پانزدهم، پاییز ۱۴۰۱

ارائه چارچوبی برای پیشگیری و مدیریت تهدیدات درون‌زا با رویکرد پدافند غیرعامل

مهناز میرزا ابراهیم طهرانی[۱]، غلامرضا جلالی فراهانی[۲]

تاریخ دریافت: ۱۴۰۱/۰۸/۰۱ تاریخ پذیرش:۱۴۰۱/۰۹/۰۵

چکیده:

مطالعه اسنادی و تحلیل شرایط نشان داده که امروزه دشمن راهبرد ترکیبی پنج لایه را در دستور کار خود قرار داده است. این پنج لایه عبارت‌اند از؛ تهدیدات درون‌زا شامل نفوذ انسانی، شبکه‌ای و سایبری، کشف و به دست آوردن آسیب‌پذیری زیرساخت‌های سایبری به‌ویژه زیرساخت‌های خدمت رسان به مردم، قطع خدمات ضروری به مردم، انتقال پیامد قطع خدمات به مردم و مدیریت افکار عمومی بر بستر شبکه‌های اجتماعی خارج پایه و درنهایت ایجاد آشوب و عملیات ضد امنیتی شامل شورش، تخریب و درگیری. لذا برای مقابله باید مطابق این پنج لایه اقدامات و استراتژی داشته باشیم. این اقدامات می‌بایست شامل؛ کور کردن لایه نفوذ و کاهش تهدیدات درون‌زا، تقویت پدافند سایبری زیرساختی، تداوم کارکردهای ضروری و تضمین فعالیت زیرساخت‌های خدمت رسان به مردم، مدیریت رسانه و افکار عمومی و بازنگری امنیت فیزیکی باشد. امروزه سازمان‌ها از هر نوع و اندازه‌ای در معرض تهدیدات درون‌زا می‌باشند. ماهیت تهدیدات درون‌زا به‌گونه‌ای است که برنامه‌های کاهش تهدیدات درون‌زا در سازمان‌ها دقیقاً شبیه هم نبوده و تلاش‌ها را برای کاهش اثرات این نوع تهدیدات پیچیده و سخت می‌نماید. در این میان انعطاف‌پذیری و سازگاری در بخش‌های امنیتی و حفاظتی بسیار مهم است چراکه جنس، نوع، اندازه و ابزار تهدید به‌طور مداوم متحول می‌شوند و فناوری‌ها به‌سرعت تغییر می‌کنند. لذا سؤال اصلی این است که با چه الگویی می‌توان تهدیدات درون‌زا را مدیریت نمود. شاخص‌های خودی‌های مستعد ایجاد تهدیدات داخلی کدامند؟

[۱] استادیار و عضو هیئت علمی دانشگاه آزاد اسلامی تهران شمال (نویسنده مسئول) Tehrani_mah@iau.ac.ir

[۲] دانشیار و عضو هیئت علمی دانشگاه و پژوهشگاه عالی دفاع ملّی و تحقیقات راهبردی defaeistrategic@sndu.ac.ir

برای پاسخ به این سؤالات این مقاله یک الگو جهت حفاظت از دارایی‌ها و زیرساخت‌های حیاتی؛ پیشگیری از خشونت، مقابله با حوادث ناخواسته، جلوگیری از خسارت مالی ارائه می‌نماید. برای ارائه یک الگوی منسجم و پاسخگو با تشکیل جلسات خبرگی و بر اساس روش طوفان مغزی اطلاعات در کارگروه تخصصی با حضور کارشناسان خبره و با طرح سؤالات مبتنی بر "چه می‌شود اگر" گردآوری و مورد تجزیه‌وتحلیل قرار گرفت.

واژگان کلیدی: تهدیدات درون‌زا، اقدامات خرابکارانه، زیرساخت حیاتی، ریسک

مقدمه:

تهدیدات درون‌زا همواره وجود دارد زیرا سازمان‌ها با توجه به شرایط به کارکنان خود اعتماد کرده و دسترسی می‌دهند. سازمان‌ها برای انجام هر عملکردی از ابتدایی‌ترین تا حساس‌ترین عملکرد های یک کسب‌وکار به کارکنان خود متکی هستند. درک تهدیدات داخلی مستلزم آن است که سازمان‌ها بفهمند یک فرد داخلی کیست و اینکه چگونه وضعیت داخلی می‌تواند منجر به خطراتی برای یک سازمان شود.[3]

شکل‌گیری تهدیدات درونی ممکن است برای بسیاری از سازمان‌ها مشابه باشد. یک فرد معتمد که از دسترسی و دانش خود برای آسیب رساندن به یک سازمان استفاده می‌کند. اما روند تغییرات تهدیدات ممکن است بسیار متفاوت باشد، بسته به ماهیت سازمان، نوع کار یا بخش، محصولات و خدمات انجام‌شده و مهم‌تر از همه دارایی‌های سازمانی که باید از خسارت، به خطر افتادن، آسیب یا سرقت محافظت شوند. برخی از سازمان‌ها اقدامات امنیتی و حراستی را برای کاهش تهدیدات داخلی اتخاذ کرده‌اند، مانند بررسی کارکنان، ساز کارهای احراز هویت، آموزش، نظارت، تفکیک وظایف و غیره.[۷]به‌طورکلی، جدیت و خسارات حملات رخ‌داده، نیاز مبرمی به توسعه سیستم‌های پیشگیری از تهدیدات داخلی را ایجاد کرده است. شناسایی تهدیدات از درون دارای پیچیدگی‌هایی بوده و کاهش اثرات آن‌ها به‌راحتی با روش‌های سنتی انجام نخواهد شد. [۹].

بیان مسئله:

افرادی که انواع دسترسی‌ها و دارایی‌های یک سازمان به آن‌ها سپرده‌شده است، می‌توانند عامل و منشأ تهدیدات متنوع داخلی می‌باشند. این افراد ممکن است کارمندان فعلی، سابق یا هر شخص دیگری باشند که اجازه دسترسی به اسناد یا محل‌های ویژه را دارا بوده و می‌توانند عامل اعمال هر نوع اختلال درونی باشند که ممکن است آسیب قابل‌توجهی به تجهیزات، کارکرد ها، فرآیندها، کارکنان و عملکرد یک زیرساخت یا سازمان وارد نمایند. بر این اساس مدیریت و کاهش تهدیدات درون‌زا در سازمان‌ها نیازمند تدوین و اجرای یک برنامه پیشگیرانه است. این برنامه می‌تواند قبل از اینکه رفتارهای آسیب‌زا در یک حادثه داخلی رخ دهد، تهدیدات درونی سازمان را که منحصر به محیطش هست شناسایی و کشف نموده، ریسک آن‌ها را ارزیابی و مدیریت نماید[6] .

این مقاله به دنبال پاسخ به سؤالات زیر هست؛

۱. اساساً تعریف تهدیدات درون‌زا چیست؟
۲. تفاوت تهدیدات درون‌زا با آسیب‌پذیری‌ها چیست؟
۳. تهدیدات درون‌زا در چارچوب چه راهبردی از دشمن اقدام می‌شود؟
٤. راهکارها و راه‌حل‌ها در کاهش و مدیریت تهدیدات درون‌زا چیست؟

این مقاله با استفاده از روش تحقیق مطالعات اکتشافی با بررسی اسناد کتابخانه‌ای و تحولات تهدیدات درونی با بهره‌گیری از جامعه آماری نخبگی برای صحت سنجی و ارزیابی نتایج اقدام می‌کند.

برنامه مدیریت و کاهش تهدیدات درون‌زا روش های مختلفی را که خودی ها می‌توانند برای سازمان ایجاد کنند، تشریح می‌نماید. قبل از بررسی جزئیات تهدیدات داخلی و چگونگی پیشگیری و کاهش آن‌ها، ارائه درک اساسی از اصطلاحات مختلف مهم است. به‌عبارت‌دیگر تعاریف واژگان، درک مشترکی برای کمک به طرح بحث تهدیدات داخلی فراهم می‌کنند، که اولین قدم مهم در ایجاد یک برنامه کاهش تهدیدات داخلی است[5] .

تهدیدات داخلی، صرف‌نظر از اندازه، برای هر سازمانی ازنظر اعتبار و هزینه بالقوه یک ریسک غیرقابل‌قبول است. تأثیر مالی بر سازمان‌ها می‌تواند سبب ویرانگری آن ها شود، به‌ویژه برای شرکت‌هایی که کمتر از ۵۰۰ کارمند دارند. به‌طورکلی هزینه‌های ناشی از تهدیدات داخلی عبارتاند از:[8]

- صدمه به زیرساخت‌ها
- صدمه به شهرت و نام سازمان
- سرقت فناوری
- ایجاد اختلال در بهره‌برداری از زیرساخت‌ها
- سرقت مالکیت معنوی
- انتشار تصادفی داده‌ها و اطلاعات

مبانی نظری

پیشینه شناسی:

با توجه به اهمیت موضوع و در ارتباط با آن، پژوهش‌های مختلف و متعددی ارائه گردیده است که در ادامه به برخی از این پژوهش‌ها و نتایج حاصل از آن‌ها در جدول ۱ اشاره می‌شود.

محقق	عنوان	نتیجه
رفعتی، حمیدرضا و صنیعی، محمدحسین پاییز ۱۳۹۶	برآورد تهدیدات سیاسی با رویکرد کنترل و مهار و نقش آن در ارتقاء امنیت ملی	در این مقاله تهدیدات سیاسی با رویکرد کنترل و مهار و نقش آن در ارتقاء امنیت ملی موردتوجه قرارگرفته است. نتایج حاکی از آن است که هر تهدید دارای بستر اجتماعی در گذشته و هویت نامحسوس در درون جامعه است.
عسگری، محمود ۱۳۹۹	رویکردی به تهدیدات داخلی ج.ا.ایران از منظر فرماندهی معظم کل قوا	در این پژوهش با توجه به اهمیت شناسایی تهدیدات داخلی، سعی شده است تا بیانات مقام معظم رهبری موردتوجه قرار گیرد. نتایج حاصل نشان داد که داده‌های حاصل از تجزیه‌وتحلیل بیانات مقام معظم رهبری در خصوص تهدیدات داخلی را می‌توان در شش مضمون سازمان دهنده می‌توان دسته‌بندی نمود
Cybersecurity and Infrastructure Security Agency-2020	Insider Threat Mitigation Guide	ادبیات موضوع تهدیدات داخلی و چارچوبی جهت مدیریت و کاهش این‌گونه تهدیدات در قالب خطوط راهنما ارائه‌شده است.
The Transportation Security Administration (TSA)-2020	guiding principles and strategic priorities	نقشه راه کاهش تهدیدات از درون به‌ویژه برای حوزه حمل‌ونقل به‌عنوان یکی از زیرساخت‌های حیاتی ارائه‌شده است.
The DHS ۲۰۲۰–published	Insider Threat Programs for the Critical Manufacturing Sector Implementation Guide.	برنامه مقابله با تهدیدات درون‌زا برای حوزه‌های صنعتی ارائه‌شده است.

جدول ۱: پیشینه تحقیق

بررسی پیشینه‌ها نشان می‌دهد که پرداختن به موضوع تهدیدات داخلی (درون‌زا) به‌عنوان یک رویکرد اثرگذار در پیشبرد اهداف و دستیابی به مصون‌سازی و پایداری کشور ضروری هست.

مفهوم شناسی:

تهدید درون‌زا[1]: به تهدیداتی اطلاق می‌گردد که توسط کارکنان یک سازمان یا شبکه‌های همکار (پیمانکاران و سایرین) به‌صورت فردی یا شبکه‌ای، خواسته یا ناخواسته با همکاری یا هدایت عوامل بیگانه یا بدون پشتیبانی آن‌ها از سطح دسترسی مجاز، دانش و اختیارات خود برای آسیب رساندن به سازمان استفاده کنند.[4]

این امر می‌تواند شامل سرقت اطلاعات و فن‌آوری انحصاری، خسارت به تأسیسات، سیستم‌ها، تجهیزات، کارکردها و فرآیندها، صدمه به کارمندان، توقف فعالیت‌های ضروری و یا اقدامات دیگری (صدمه زدن به مأموریت سازمان و منابع) باشد که دستگاه را از ادامه ارائه خدمات خود بازدارد. این تهدیدات می‌توانند از طریق عوامل انسانی، فیزیکی و سایبری اعمال گردد.

مقابله با تهدیدات درون‌زا: منظور از مقابله با تهدیدات درون‌زا مجموعه اقداماتی است که منجر به پیشگیری، کشف، شناسایی، مدیریت و کاهش آثار ناشی از یک تهدید درون‌زا هست.

خودی (فرد داخلی)[2]: خودی به مدیران، کارکنان و اشخاص ثالثی که به‌نوعی به منابع سازمان، اطلاعات، تجهیزات، شبکه‌ها و سامانه‌ها و ... به روش قانونی دسترسی داشته یا از آن‌ها آگاهی داشته باشد.[4]

انواع تهدیدات درون‌زا: به‌طورکلی تهدیدهای درون‌زا از به دو قسمت تقسیم می شود: غیرعمدی و عمدی.[4]

۱. **تهدیدات غیرعمدی** را می‌توان بیشتر به اعمال سهل‌انگارانه و تصادفی یا سودجویانه تقسیم‌بندی کرد. این‌گونه تهدیدات را آسیب‌پذیری نیز می‌نامند.

نکته: تفاوت تهدیدات درون‌زا با آسیب‌پذیری‌ها این است که آسیب‌پذیری‌ها با منشأ داخلی هستند اما تهدیدات درون‌زا با منشأ خارجی ولی متمرکز بر آسیب‌پذیری‌های داخلی می‌باشند.

---

[1] Insider threat
[2] insider

۲. **تهدیدهای عمدی:** به‌طورمعمول، تهدیدهای عمدی اقدامات مخربی است که توسط خودی‌های ناراضی و یا معارض و افراد سودجو با استفاده از ابزارهای فنی با هدف ایجاد اخلال یا توقف در فعالیت های منظم سازمان، شناسایی نقاط ضعف، به دست آوردن اطلاعات طبقه‌بندی‌شده انجام می‌شود.

این اقدامات می‌تواند شامل هرگونه خرابکاری فیزیکی و یا تغییر داده‌ها یا قرار دادن بدافزار یا سایر نرم‌افزارهای مهاجم برای ایجاد اختلال در سیستم‌ها و شبکه‌ها باشد.

تهدیدهای تبانی[1]: این تهدید زمانی نمایان می‌شود که یک یا چند فرد داخلی با یک عامل داخلی یا خارجی همکاری کنند تا سازمان را به خطر اندازند.[4]

تهدیدات طرف سوم (شخص ثالث)[2]: تهدیدهای طرف سوم یا شخص ثالث با پیمانکاران یا فروشندگانی در ارتباط است که اعضای رسمی سازمان نیستند، اما به آن ها به صورت موقت سطح دسترسی به امکانات، سیستم‌ها، شبکه‌ها یا افراد و ... برای تکمیل کارشان داده‌شده است.

تروریسم[3]: تروریسم به‌عنوان یک تهدید درونی، استفاده غیر قانونی یا تهدید به استفاده از زور و خشونت توسط کارمندان داخلی، اعضا یا سایر افرادی است که با سازمان در ارتباط هستند تا به یک هدف سیاسی یا اجتماعی دست یابند. در این تهدید، افراد داخلی از حداکثر آشنایی خود با ساختار سازمان، امنیت، چیدمان ساختمان‌ها و دانسته‌های دیگر برای به حداکثر رساندن تلفات یا افزایش تأثیر خرابکاری استفاده می‌کنند.[4]

جاسوسی[4]: جاسوسی روشی برای کسب اطلاعات به‌صورت محرمانه مخفیانه و غیر قانونی از دولت، سازمان، نهاد یا اشخاص است برای دستیابی به اهداف امنیتی نظامی، سیاسی، استراتژیک یا مالی و ... هست.[4]

---

[1] Collusive Threats
[2] Third-Party Threats
[3] Terrorism
[4] Espionage

خرابکاری[1]: خرابکاری شامل اقدامات آگاهانه‌ای است که می‌تواند به زیرساخت‌های معنوی، فیزیکی یا مجازی سازمان آسیب برساند ازجمله تخریب اعتماد داخلی سازمانی، اخلال در روش‌های نگهداری یا فناوری اطلاعات، آسیب رساندن به امکانات فیزیکی و ... .[4]

خرابکاری فیزیکی: خرابکاری فیزیکی شامل اقدامات آگاهانه‌ای است که باهدف آسیب رساندن به زیرساخت‌های فیزیکی سازمان (به‌عنوان‌مثال دارایی‌ها، تجهیزات و منابع انسانی) انجام می‌شود[4] .

خرابکاری سایبری: خرابکاری سایبری شامل اقدامات آگاهانه‌ای است که باهدف آسیب رساندن به زیرساخت‌های فیزیکی و سایبری و اختلال در انجام مأموریت سازمان در بستر فضای سایبر انجام می‌شود.[4]

سرقت[2]: سرقت شامل انواع سرقت مادی و اطلاعاتی است. (دارایی‌های ملموس و ناملموس)[4]

تهدیدهای ناخواسته: این نوع تهدیدات در اثر غفلت و سهل‌انگاری کارکنان روی می‌دهند. به‌عنوان‌مثال می‌توان به مهندسی اجتماعی، فیشینگ، ارائه اطلاعات و ... در فضای مجازی بدون نیت سوء اشاره کرد[4] .

توافقنامه عدم افشاء[3]: قرارداد عدم افشا یک قرارداد قانونی الزام‌آور است و تعهدی را ایجاد می‌کند که به‌موجب آن افشای هرگونه اطلاعات مرتبط با سازمان را به‌طور غیرمجاز منع می‌کند

خود حفاظتی[4]: مجموعه اقداماتی شامل برنامه‌ریزی، سازمان‌دهی، آموزش، تجهیز، تمرین و ارتقاء آمادگی که مدیران هر دستگاه با استفاده از تجهیزات و کارکنان در اختیار خود به‌منظور مقابله با هوج اولیه تهدیدات باید انجام دهند.

شغل کلیدی: به پست‌های سازمانی اطلاق می‌شود که میزان دسترسی مجاز به اطلاعات، اماکن و تجهیزات مرکز/دستگاه/زیرساخت به‌گونه‌ای است که فرد در صورت سوءاستفاده از موقعیت شغلی خود می‌تواند به مرکز/دستگاه/زیرساخت صدمات جبران‌ناپذیری وارد نماید.

منشأ تهدیدات درون‌زا

---

[1] Sabotage
[2] Theft
[3] Non disclosure agreement
[4] Self protection

منشأ تهدیدات درون‌زا عامل خودی هست. همان‌طور که گفته شد خودی فردی است که به لحاظ قانونی دسترسی به اماکن و اطلاعات طبقه‌بندی‌شده را داشته باشد. عامل خودی می‌تواند از کارکنان داخلی سازمان، پیمانکار یا مشاور بوده و با استفاده از علم و فناوری به اهداف خود دست یابد.

مدل مفهومی تحقیق:

به‌منظور ارائه مدل مفهومی جهت مدیریت و کاهش تهدیدات داخلی ضروری است ابتدا عوامل و زمینه‌های رشد این نوع تهدیدات شناسایی‌شده و بر اساس نقش آسیب‌پذیری‌های موجود در سیستم به نحوه ارتباط دشمن از بیرون به درون سازمان پرداخت و بر این اساس زنجیره اقدامات دشمن را ترسیم نمود؛

عوامل و زمینه‌های رشد تهدیدات درون‌زا

۱. نارضایتی خودی‌ها (به دلایل؛ مشکلات مالی، عدم ارتقاء شغلی، درگیری با همکاران، مشکلات خانوادگی، بیماری روانی)
۲. نفوذ دشمن (بر اساس اقدامات جنگ شناختی)
۳. ورود علم و فناوری بدون ارزیابی تهدیدات ناشی از آن
٤. افزایش آسیب‌پذیری‌ها و آشکار شدن آن

نقش آسیب‌پذیری‌ها و انواع آن در این چارچوب

آسیب‌پذیری عبارت است از هر نقطه‌ضعفی که توسط دشمن مورد بهره‌برداری قرار می‌گیرد تا دشمن به‌طور غیرمجاز به دارایی‌های یک زیرساخت دسترسی پیدا کند و متعاقباً به آن‌ها خسارت وارد نموده یا آن‌ها را سرقت نماید.[5]

در تعریف دیگری، آسیب‌پذیری میزان صدمات و خساراتی است که از عوامل و پدیده‌های بالقوه یا بالفعل خسارت زا نسبت به نیروی انسانی، تجهیزات و تأسیسات با شدت صفرتا صد ناشی می‌شود. به بیانی دیگر می‌توان آسیب‌پذیری را تأثیر تهدید بر نقاط ضعف تعریف نمود.[2]

با توجه به تعاریف فوق در صورت وجود نقاط ضعف در سازمان‌ها اعم از نقاط ضعف در ساختارها و رویه‌ها و همچنین ضعف در مدیریت منابع انسانی و حفاظت از اطلاعات طبقه‌بندی شده می‌توانند زمینه‌ساز رشد تهدیدات از درون گردد.

نحوه ارتباط دشمن از بیرون به درون

نحوه ارتباط دشمن از بیرون به درون می‌تواند با عنوان نفوذ صورت پذیرد. نفوذ و رخنه در طول تاریخ، از روش‌های دشمنان اسلام بوده تا از طریق آن بتوانند از پیشبرد اهداف جامعه اسلامی جلوگیری کنند. نفوذ به معنای رخنه، اثر کردن، راه‌یابی و جاری شدن آمده است. گاه مجازاً به معنای تأثیر گذاشتن بر کسی، راه یافتن پنهانی در گروهی یا جایی به‌منظور هدفی نیز به‌کاررفته است. (دهخدا، ۱۳۷۷). نفوذ دشمن دارای ویژگی‌هایی است ازجمله آرام و تدریجی صورت می‌گیرد. نکته دیگر تداوم نفوذ دشمن است. دشمن با استفاده از نقاط ضعف سازمان می‌تواند به اهداف شوم خود از طریق نفوذ دست یابد.

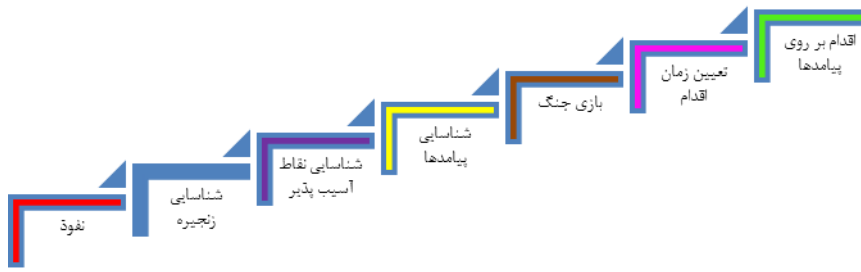
نقش شبکه‌های اجتماعی در توسعه تهدیدات درون‌زا

در چند سال اخیر شبکه‌های اجتماعی مجازی با محبوبیت کم‌نظیر جهانی روبرو شده‌اند. به‌طوری که میلیون‌ها نفر از سراسر جهان در این شبکه‌ها عضویت دارند و روابط انسانی، نوع همکاری، وابستگی حرفه‌ای، و بسیاری از امور اجتماعی، فرهنگی، سیاسی و اقتصادی خود را در بستر این شبکه‌ها ایجاد و دنبال می‌کنند. بنابراین به لحاظ گستره کاربری می‌توان گفت در فضای شبکه‌های اجتماعی چیزی بیش از یک فضای اطلاعاتی جهانی وجود دارد. لذا این فضای اطلاعاتی زمینه ساز مناسبی برای دستیابی دشمن به اهداف خود و نفوذ در لایه‌های مختلف سازمانی هست.

بررسی زنجیره اقدام دشمن در فعال کردن تهدیدات داخلی

- **گام اول:** نفوذ به درون سازمان از طریق خودی‌ها
- **گام دوم:** شناسایی زنجیره تولید و عملکردهای کلیدی سازمان
- **گام سوم:** شناسایی نقاط آسیب‌پذیر در فرآیند زنجیره تولید و عملکردهای کلیدی
- **گام چهارم:** شناسایی پیامدهای ناشی از قطع فعالیت‌ها
- **گام پنجم:** بازی جنگ و تعیین سناریوها

- **گام ششم**: تعیین زمان اجرای عملیات
- **گام هفتم**: اقدامات بر روی پیامدها و ایجاد آشوب و ناامنی



شکل ۱-زنجیره اقدام دشمن در فعال کردن تهدیدات داخلی (محقق،۱۴۰۱)

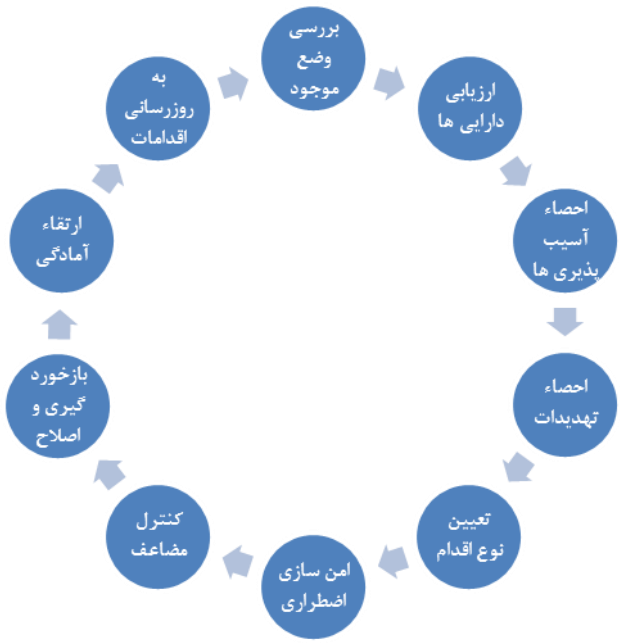
عوامل افزایش آسیب‌پذیری‌ها در درون

- عوامل انسانی
- عوامل سایبری
- عوامل ساختاری
- عوامل قراردادی، پیمانکاری و برون‌سپاری

فرآیند کاهش و مدیریت تهدیدات داخلی

۱. بررسی وضعیت موجود
۲. ارزیابی دارایی‌ها
۳. احصاء آسیب‌پذیری‌های موجود
٤. احصاء تهدیدات پایه
٥. تجزیه‌وتحلیل و انتخاب نوع اقدام
٦. امن سازی اضطراری و مصون‌سازی
۷. کنترل مضاعف و حصول اطمینان از برطرف شدن اشکالات
۸. بازخورد گیری و اصلاح
۹. ارتقاء آمادگی

۱۰. به‌روزرسانی اقدامات



شکل ۲- چرخه کاهش و مدیریت تهدیدات داخلی (محقق،۱۴۰۱)

روش‌شناسی تحقیق

این تحقیق از نوع کاربردی- توسعه‌ای ا ست و روش آن، تو صیفی-تحلیلی ه ست و با ا ستفاده از مطالعات اسنادی و کتابخانه‌ای، پرسشنامه، مصاحبه و تعامل فکری با نخبگان (میز اندیشه و طوفان مغزی) در حوزه تهدیدات از درون، داده‌های لازم جمع‌آوری گردیده ا ست. در ا ین تحقیق، تو سعه کاربردی اصول و ملاحظات پدافند غیرعامل در صیانت از زیرساخت‌ها، منابع و دارایی های ک شور در برابر تهدیدات درون‌زا مدنظر است. به‌واسطه راهبردی بودن آن ازنظر سطح شامل گستره در سطح ملّی هست. در این تحقیق با توجه به ویژگی‌های آن حجم جامعه آماری موردبررسی ۱۵ نفر از متخصصان

و کارشناسان خبره پدافند غیرعامل در حوزه حفاظت اطلاعات و تهدیدشناسی بوده‌اند که به لحاظ یکی بودن حجم نمونه با حجم جامعه، روش نمونه‌گیری به‌صورت تمام شمار بوده است. همچنین در این تحقیق برای احصاء عوامل تأثیرگذار در چارچوب مدیریت تهدیدات درون‌زا از روش نخبه‌گی با برگزاری جلسات طوفان مغزی استفاده‌شده است.

تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

ازآنجایی‌که دستیابی به یک سیستم حفاظت مؤثر و ظرفیت پاسخگویی به حوادث و تهدیدات از درون نیازمند شناسایی عوامل تأثیرگذار بر این نوع تهدیدات در سازمان‌ها هست. با توجه به منشأ بروز تهدیدات داخلی مبتنی بر عوامل انسانی، علم و فناوری، سایبر، شبکه‌های اجتماعی، ساختار و مدیریت مورد پرسش قرارگرفته و نتایج آن‌ها در قالب اقدامات مدیریت و کاهش تهدیدات درون‌زا به شرح ذیل دسته‌بندی می‌گردد:

الف-مدیریت و کاهش تهدیدات ناشی از عوامل انسانی

۱. تهیه برآورد تهدیدات ناشی از نیروی انسانی و آسیب‌پذیری‌های دستگاه به‌صورت سالانه
۲. غربالگری نیروی انسانی (ملاحظات استخدامی، امنیتی، روحی و روانی)
۳. اجرا و پیاده‌سازی طرح امنیتی مشاغل
٤. انجام سطح‌بندی امنیتی قسمت‌های مختلف
٥. تعریف دسترسی‌های اشخاص برابر طرح حیطه‌بندی/ تدوین و اجرای نظام دسترسی‌های فیزیکی و اطلاعاتی
٦. اخذ ضمانت‌نامه بر مبنای نوع و میزان دسترسی‌ها و دارا بودن اطلاعات
۷. اخذ سند منع افشاء اطلاعات از کارکنان
۸. رعایت اصل حفاظتی جهت افرادی که دسترسی، دانش و اطلاعات و اختیارات دارند
۹. اخذ گواهی‌های سلامت جسمانی، روانی، تخصص و احصاء امنیتی لازم در شرایط امنیتی موردنیاز
۱۰. تدوین و اجرای طرح حفاظت از شخصیت‌ها
۱۱. تغییر منظم و نوبه‌ای دسترسی‌ها به اماکن طبقه‌بندی‌شده

۱۲. توسعه فرهنگ مسئولیت‌پذیری بین کارکنان

ب- مدیریت و کاهش تهدیدات مبتنی بر فناوری

۱. تهیه برآورد تهدیدات مبتنی بر فناوری
۲. احصاء و ارزیابی آسیب‌پذیری‌های دستگاه به‌صورت سالانه
۳. کنترل و نظارت بر تجهیزات و فناوری‌های ورودی به دستگاه
٤. ارزیابی امنیتی و فنی سامانه‌ها و شبکه در برابر تهدیدات مرتبط با اپلـنت ها و بدافزارهای سخت‌افزاری
٥. طراحی، معماری و پیاده‌سازی، پشتیبانی و ارتقاء شبکه زیرساخت‌ها و اجزای آن بـر ا ساس الزامات پدافند غیرعامل

ج-مدیریت و کاهش مبتنی بر تهدیدات سایبری

۱. تهیه برآورد تهدیدات و آسیب‌پذیری‌های دستگاه به‌صورت سالانه
۲. تغییر منظم و نوبه‌ای دسترسی‌ها به شبکه سایبری دستگاه
۳. کنترل مضاعف در عین اعتماد (Zero trust)
٤. اجرای معماری امنیتی حفاظتی یا پدافند سایبری مناسب در تمام سطح شبکه
٥. استفاده از فناوری‌های بومی و امن در تمام سطوح طراحی، نصب و پیاده‌سازی نرم‌افزار ها و سخت‌افزارها
٦. زمان‌بندی پشتیبان گیری از داده‌ها برحسب تغییرات یا به صورت ساعتی، روزا نه، هفت گی، ماهانه و یا برحسب نیاز کاربران
۷. در زیرساخت‌های حیاتی و حساس برون‌سپاری امنیت سایبری ممنوع است.

د- مدیریت و کاهش مبتنی بر تهدیدات شبکه‌های اجتماعی

۱. تهیه برآورد تهدیدات شبکه‌های اجتماعی و آسیب‌پذیری‌های دستگاه به‌صورت سالانه

۲. محدودسازی و کنترل استفاده اداری از شبکه‌های اجتماعی خارج پایه
۳. محدودسازی و کنترل هرگونه خدمتی اعم از اداری و شخصی به شبکه‌های اجتماعی خارج پایه
٤. محدودسازی و کنترل تشکیل گروه‌ها و کانال‌های ارتباطی اجتماعی مبتنی بر کارکنان هر زیرساخت در شبکه‌های اجتماعی خارج پایه
٥. رصد و پایش و کنترل شبکه‌های اجتماعی مرتبط با دستگاه
٦. توجیه و آموزش‌های لازم اطلاعاتی کارکنان نسب به مخاطرات شبکه‌های اجتماعی (ترویج و انتشار و رعایت محرمانگی اطلاعات شخصی)

ه- مدیریت و کاهش مبتنی بر تهدیدات مدیریت، ساختار و نظامات

۱. تهیه برآورد تهدیدات مدیریتی، ساختاری و نظامات
۲. احصاء و ارزیابی آسیب‌پذیری‌های دستگاه به‌صورت سالانه
۳. تعریف مشاغل حساس و ارائه طرح طبقه‌بندی مشاغل
٤. غربالگری و مراقبت‌های لازم مبتنی بر نوع وظایف (صندلی)
٥. امضای تعهد عدم افشای اطلاعات اسناد با کارکنان و طرف‌های سوم برابر فرم مصوب ابلاغی.
٦. ارائه الزامات حفاظتی و اطلاعاتی مشاغل حساس
۷. رعایت الزامات و ملاحظات پدافند غیرعامل توسط مجری و پیمانکاران در مراحل مختلف اعم از طراحی، نصب و پیاده‌سازی و هرگونه ارائه خدمات

ارائه چارچوب کاهش و مدیریت تهدیدات داخلی

به‌منظور کاهش و مدیریت تهدیدات داخلی می‌بایست چارچوبی را ارائه نمود تا افراد خودی را از دوره قبل از پیوستن به یک سازمان تا پس از خروج آن‌ها در برگیرد تا دیدی جامع از مشکلات تهدید خودی ارائه دهد. هدف در نظر گرفتن اقدامات «پیشگیرانه» است که باید برای جلوگیری از تهدیدات داخلی در مقابل اقدامات «واکنشی» انجام شود.

این چارچوب شامل سه مؤلفه اصلی است: اقدامات پیشگیرانه، اقدامات مقابله‌ای گروه پیشگیری از تهدید داخلی و تصمیم‌گیری.

مؤلفه اول پیشگیری از تهدیدات داخلی شامل شناسایی، پیشگیری و اصلاح است. این امر با استفاده از تنظیم مقررات، آموزش و آگاهی‌رسانی‌های امنیتی، نظارت فنی و رفتاری صورت می پذیرد. هدف از این اقدامات بررسی و تهیه پرونده‌های رفتاری و روانی فعالیت‌های یک خودی به‌منظور پیشگیری از اعمال تهدیدات داخلی است. مؤلفه دوم اقدامات مقابله‌ای هست به این صورت که با بررسی این پرونده‌ها خودی با توجه به انگیزه، فرصت و توانایی وی برای انجام یک حمله ارزیابی می شود. درنهایت، در مؤلفه تصمیم‌گیری، اقدامات بازدارنده و پیشگیرانه با توجه به امتیاز ریسک محاسبه شده فعال می‌شود.

الف-اقدامات قبل از به‌کارگیری خودی‌ها

مؤلفه تصمیم‌گیری برای هشدار به افراد مشکوک به‌عنوان مکانیزم بازدارنده اقدامات مخرب در سازمان توجه می‌شود. باید اقدامات پیشگیرانه را قبل از دسترسی افراد داخلی به دارایی های مختلف سازمان (اعم از دارایی‌های فیزیکی و مجازی) اعمال نماید. این امر را می توان با انجام اقدامات مختلف (به‌عنوان‌مثال، بررسی خودی، حیطه‌بندی دسترسی، آموزش و آگاهی‌رسانی امنیتی) به دست آورد. در این بخش باید جزئیات حیطه‌بندی دسترسی و استفاده از اطلاعات توجه نمود.

ب-اقدامات در حین به‌کارگیری خودی‌ها

پس از اطمینان از قابل‌اعتماد بودن اطلاعات افراد داخلی، تخصیص دقیق امتیازات دسترسی/استفاده (حیطه‌بندی) با به‌کارگیری آگاهی‌های امنیتی، به‌عنوان لایه حفاظتی دوم اقدام می شود. به عبارتی نظارت و بررسی فعالیت‌های فنی، رفتاری و روانی افراد خودی صورت می‌گیرد. اقدامات فنی بر فعالیت‌های خودی‌ها در سطح عملیات نظارت می‌کند درحالی‌که اقدامات رفتاری، رفتارهای خودی ها را در محل کارشان ردیابی می‌کند (به‌عنوان‌مثال، تعهد آن ها به تبعیت از سیاست‌ها و ابلاغیه‌های ساعات کاری و وظایف محوله). اقدامات روان‌شناختی، ذهنیت‌ها و انگیزه‌های خودی‌ها را که ممکن است آن‌ها را به انجام اعمال مخرب سوق دهد، ارزیابی می‌کند.

ج-اقدامات پس از به‌کارگیری خودی‌ها

مؤلفه‌های قبلی بر اعمال اقدامات مقابله با تهدیدات درون‌زا قبل از پیوستن افراد خودی به محیط کاری آن‌ها در یک سازمان تمرکز دارند. اقدامات پس از مقابله، به آینده فرد یعنی دوران اعلان استعفا/فسخ قرارداد و همچنین پس از خروج خودی‌ها از یک سازمان می‌پردازد. بنابراین، اقدامات حفاظتی متفاوتی را می‌توان برای اطمینان از سطح بیشتر حفاظت در پایان و پس از به‌کارگیری یک خودی در یک سازمان اعمال کرد.

نتیجه‌گیری و پیشنهاد:

الف- نتیجه‌گیری

افراد درون یک سازمان به‌طور همزمان قوی‌ترین عناصر یک برنامه امنیتی و بیشترین عناصر آسیب‌پذیری آن هستند. سازمان‌های برای بقای خود نیاز به دستر سی کارمندان به امکانات، منابع، سیستم‌ها، مالکیت معنوی، داده‌ها هست، که هر یک آسیب‌پذیری ایجاد می‌کند. اثرات مخرب حوادث مربوط به عوامل خودی، ایمنی و امنیت سازمان را به خطر می‌اندازد. باوجوداین واقعیت ها نیازمند اجرای یک برنامه کاهش و مدیریت برای تهدیدات داخلی ایجاد نماییم.

پیشگیری از حوادث تهدیدات داخلی زمانی امکان‌پذیر است که سازمان‌ها بر موارد زیر تمرکز کنند:

- متناسب کردن برنامه تهدیدات داخلی خود با مأموریت، فرهنگ و فضای تهدید منحصربه‌فرد سازمان، به‌ویژه تمرکز بر دارایی‌هایی که بیشترین ارزش را برای آن‌ها دارد
- استفاده از چارچوب کشف و شناسایی، ارزیابی و مدیریت برای پیشگیری، حفاظت و کاهش تهدیدات داخلی
- آموزش افراد در زمینه شناخت رفتارها و نحوه گزارش‌گیری
- ایجاد فرهنگ مثبت برای گزارش دهی و اطمینان از این که افراد می‌دانند برنامه کاهش و مدیریت تهدیدات داخلی برای کمک به آن‌ها و همچنین سازمان طراحی‌شده است

- ایجاد یک گروه مدیریت تهدید که از توانایی های چند رشته‌ای موردنیاز برای ارزیابی واقعیت‌ها و رفتارهای مربوط به تهدید داخلی بالقوه استفاده می‌کند
- ایجاد توانایی‌های ارزیابی و مداخله و اقدامات مدیریتی که همراه با حفظ احترام با شند و شأن، حقوق و حریم خصوصی یک کارمند را در نظر بگیرند
- فراهم آوردن یک محیط امن و غیر تهدیدآمیز که در آن افرادی که ممکن است تهدیدی اعمال کنند، شناسایی‌شده و قبل از اینکه اقداماتشان آسیب برساند به آن‌ها کمک شود

یک برنامه کاهش تهدید درونی، امنیت فیزیکی، اطمینان از کارکنان و اصول اطلاعات محور را باهم در نظر می‌گیرد. اهداف آن درک تعامل خودی در داخل سازمان، نظارت بر تعامل داخلی و مداخله برای مدیریت این تعامل است هنگامی‌که تهدیدی برای سازمان محسوب می شود. برنامه‌های موفقیت‌آمیز کاهش تهدیدات داخلی ضمن پرداختن به سه اصل اساسی، که برای سازمان‌ها در هر اندازه و بلوغ اعمال می‌شوند، این اهداف را محقق می‌کنند:

۱. ترویج فرهنگ حمایتی و پشتیبانی در کل سازمان
۲. حفاظت از دارایی‌های باارزش سازمانی ضمن رعایت حریم خصوصی افراد
۳. سازگاری با تغییرات سازمانی

ب–پیشنهادات

پس از اجرای برنامه مدیریت تهدیدات داخلی لازم است به این منظور باید شاخص‌های خشونت در ارزیابی تهدید شناسایی و کشف گردد:

کشف و شناسایی تهدید فرآیندی است که طی آن افرادی که ممکن است خطر تهدید داخلی داشته باشند موردتوجه سازمان یا گروه تهدیدات داخلی قرار می‌گیرند، این امر اغلب درنتیجه رفتار های قابل‌مشاهده کشف می‌شود.

درحالی‌که دانش لازم برای کشف و شناسایی تهدیدات داخلی همچنان در حال رشد است، محققان دفاعی و امنیتی چهاراصل اساسی رفتاری را شناسایی کرده‌اند که باید موردتوجه قرار گیرند.

۱. خطر خودی شدن به‌طور تصادفی در بین هیچ جمعیتی توزیع نمی‌شود. افراد خاص بیشتر تهدید می‌شوند.

۲. تهدیدهای داخلی در یک زمینه اجتماعی اتفاق می‌افتد. برخی از محیط‌ها به‌احتمال‌زیاد رفتار تهدید داخلی را تسهیل می‌کنند.
۳. تبدیل یک فرد از یک خودی مطمئن به یک بازیگر مخرب یک‌روند است، نه یک رویداد.
٤. رفتار تهدید داخلی با تأثیر زیاد و با فرکانس پایین با شاخص‌های مشترکی که می‌توانند مشاهده، مدل‌سازی و کاهش یابند همبستگی دارد و قبل از آن وجود دارد.

فهرست منابع:

الف– منابع فارسی

داخلی:

۱. رفعتی، حمیدرضا و صنیعی، محمدحسین پاییز ۱۳۹٦– برآورد تهدیدات سیاسی با رویکرد کنترل و مهار و نقش آن در ارتقاء امنیت ملی–فصلنامه امنیت ملی–سال هفتم. شماره ۲۵
۲. عسگری، محمود ۱۳۹۹–رویکردی به تهدیدات داخلی ج.ا.ایران از منظر فرماندهی معظم کل قوا – فصلنامه امنیت ملی–سال دهم. شماره ۳۵
۳. افتخاری، اصغر –۱۳۸۷–کالبدشکافی تهدید، تهران: انتشارات دانشگاه عالی جنگ سپاه پاسداران

خارجی:

4. Cybersecurity and Infrastructure Security Agency “Insider Threat Mitigation Guide” 2020
5. The Transportation Security Administration (TSA) published the “Insider Threat Roadmap - 2020,” to provide a holistic approach, including guiding principles and strategic priorities, for the establishment of a collaborative program that comprehensively and continuously identifies and mitigates the insider risk to the TSA and the Transportation Systems Sector community.
6. The DHS published ۲۰۲۰–“Insider Threat Programs for the Critical Manufacturing Sector Implementation Guide” to provide guidance and information for critical manufacturing organizations to establish insider threat programs.
7. The NITTF’s “Insider Threat Guide - 2017” provides best practices that accompany the National Insider Threat Minimum Standards

8. The TSA published slides from the Insider Threat Awareness International Civil Aviation Organization Global Aviation Security Symposium in 2018 that discussed key elements of insider risk and how to mitigate the unique security risks associated with those with privileged access.
9. Veriato sponsored the “2019 Insider Threat Program Maturity Model Report” to help professionals assess their ability to monitor, detect, and respond to insider threats including budgeting for an effective program.
10. “DoD Insider Threat Mitigation. Final Report of the Insider Threat Integrated Process Team.” US Department of Defense, Office of the Assistant Secretary of Defense (Command, Control, Commuications, and Intelligence).Available from https://acc.dau.mil/CommunityBrowser.aspx?id=37478 (last viewed March 2011),2000.
11. C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, *Aspects of Insider Threats*. Springer, 2010, ch.in [44].