بسمه تعالی

مقاله:

تحلیل ریسک امینت اطلاعات(Risk Assessment)

علی ثاقب موفق – فوق لیسانس فناوری اطلاعات

ارزش دارایی ها و اطلاعات یک سازمان در میزان مخاطرات متوجه آن موثر است به طوریکه می تواند ریسک آن را کم یا زیاد کند. ارزیابی ریسک امنیت اطلاعات یکی از مهمترین و در عین حال پیچیده ترین مراحل امن سازی سیستم های اطلاعاتی و ارتباطی را تشکیل می دهد. اهمیت ارزیابی ریسک از آنجا سرچشمه می گیرد که نتایج حاصل از ارزیابی ریسک در کنار سیاستگذاری امنیت اطلاعات به عنوان یکی از مبانی انتخاب مکانیزم های کنترلی مورد استفاده قرار گرفته و براساس آن روش های امن سازی انتخاب و پیاده سازی می شوند. بدیهی است ارزیابی ریسک امنیت اطلاعات برای تمامی پروژه های حوزه ICT ضروری است و این مهم به عهده مدیران و مسئولین مربوطه خواهد بود.

ریسک امنیتی و محاسبه مقدار آن

ریسک را در ساده ترین حالت می توان به صورت زیان احتمالی ناشی از وقوع حالتی ناخواسته در سیستم(اعم از سیستم های ساده یا مرکب) بیان کرد. یکی از فرمول هایی که معمولاً برای محاسبه ریسک به آن مراجعه می شود به شکل زیر است.

احتمال وقوع حالت ناخواسته × زیان ناشی از وقوع حالت ناخواسته = میزان ریسک

یا

$$R_S = L_S \times P_S$$

که در آن:

R_S : ریسک ناشی از یک حالت ناخواسته

L_S : زیان ناشی از وقوع حالت ناخواسته

P_S : احتمال وقوع حالت ناخواسته

به عنوان مثال اگر زیان ناشی از قطع برق در یک مرکز داده (شامل هزینه های بازیابی اطلاعات از دست رفته، فرصت از دست رفتـه و راه اندازی مجدد سیستم)یکصد میلیون ریال و احتمال قطع برق در یک دوره یکساله ۲۰٪ باشد ریسک ناشی ازقطع بـرق در یـک دوره یکساله را می توان به صورت زیر محاسبه نمود:

L(قطع برق در یک دوره یکساله)=۱۰۰/۰۰۰/۰۰۰/- ریال

P(قطع برق یک دوره یکساله) =۰/۲

R(قطع برق در یک دوره یکساله) =۱۰۰ /۰۰۰/۰۰۰×۰/۲ = ۲۰ /۰۰۰/۰۰۰/- ریال

در فرمول فـوق مشـکل اول تخمـین حـوزه هـای اثـر قطـع بـرق و بـرآورد هزینـه ناشـی از آن و مشـکل دوم تخمـین احتمـال قطـع برق می باشد.

تخمین حوزه های متأثر از قطع برق فقط وقتی امکانپذیر است که اولاً سـابقه هـای مسـتند وکـاملی از شـرایط قطـع بـرق درگذشـته و حوزه های اثر آن وجود داشته باشد و ثانیاً افراد خبره و دارای تجربه کافی به تخمین حوزه اثر بپردازند.

برای تخمین احتمالی قطع برق نیز احتیاج به سوابق زمانی قطع برق می باشد. به عنوان مثال اگر علیرغم استفاده از UPS و ژنراتور برق اضطراری سوابق زمانی نشان می دهد که در پنج سال گذشته فعالیت مرکز داده یکبار به علت مواجه شدن با قطع بـرق متوقـف شـده است می توان احتمال قطع برق در یکسال را معادل ۰/۲ تخمین زد.

از طرف دیگر فقط قطع برق نیست که ادامه فعالیت مرکز داده را با خطر توقف مواجه می کند. عوامل متعدد دیگری ممکن است باعث این وضعیت شود. خرابی تجهیزات، خطاهای انسانی(سهوی یا عمدی)، اشکال های نرم افزاری، قطع کانال هـای ارتبـاطی و ده هـا عامـل شناخته شده یا ناشناخته دیگر می توانند موجب توقف فعالیت مرکز داده شوند. هریک از این عوامل می توانند بر اجزای مختلف مرکـز داده تأثیر گذار باشند. بنابراین علاوه بر شناخت عوامل تهدید کننده فعالیت داده و زیان ناشی از فعال شدن آنها باید اجزای تحت تأثیر نیز شناسایی شوند تا درک بهتری ازنحوه عملکرد و نوع تأثیر آنها(بر مقدار زیان های حاصله)و احتمال وقوع هریک ایجاد شود.

بنابراین برای محاسبه ریسک یک مرکز داده (یا به طورکلی هر سیستم متشکل از اجزای مختلف)از فرمول زیر استفاده می شود:

$$R=R_{is}\sum_{i=1}^{n}\sum_{s=1}^{m}$$

که در آن i نشاندهنده جزء n ام از سیستم و s نشاندهنده حالت های ناخواسته ایی است که ممکن است هر جزء با آن مواجه شود.

آنچه که باید مورد توجه قرار گیرد این موضوع است که پیش بینی حوزه های اثر یک واقعه امنیت اطلاعات همیشه به سادگی امکانپذیر نیست. به عنوان مثال وقتی دیسک سخت رایانه خراب شود ممکن است حالت های مختلفی پیش آیند که عبارتنداز:

- خرابی برد کنترلی
- خرابی هد خواندن ـ نوشتن
- خرابی سطح دیسک

درحالت اول می توان با تعویض برد کنترلی داده های مندرج در دیسک را احیا نمودو به دلیل وجود مکانیزم های خودکار نوشتن ـ خواندن که از سوی سیستم عامل به کار گرفته می شود، می توان انتظار داشت هیچ بخشی از داده ها از دست نرود بنابراین در این حالت زیان ناشی از خرابی دیسک فقط به هزینه تعویض برد محدود می شود.

در حالت دوم ممکن است داده هایی که در بازه زمانی بین وقوع خرابی هد تا کشف خرابی نوشته یا خوانده شده است فاقد اعتبار شده باشند. در این هزینه تصحیح خرابی ناشی ازخواندن نادرست اطلاعات یا وارد کردن و بازنویسی اطلاعات نیز به هزینه تعمیر اضافه می شود.

در حالت سوم ممکن است وضعیتی پیش آید که دسترسی به اطلاعات غیر ممکن شود. خرابی سطح دیسک یکی از بدترین وضعیت هایی است که ممکن است پیش آید در این حالت ممکن است اطلاعاتی که بازسازی یا جمع آوری مجدد آنها غیر ممکن است از دست برود. هزینه های احتمالی در این حالت بسیار زیاد خواهد بود.

بدیهی است اگر قبلاً از داده های موجود بر روی دیسک سخت نسخه پشتیبانی تهیه شده باشد در کلیه حالت هـای فـوق هزینـه هـای احتمالی(زیان های ناشی از وقوع حالت ناخواسته)معادل هزینه تعمیر قطعه معیوب خواهند بود. البته به شرط آنکه نسخه پشتیبانی قابـل بازیافت باشدکه این موضوع نیز خود به صحت روش پشتیبان گیری و سلامت تجهیزات پشتیبان بستگی دارد.

حالت بدبینانه ایی نیز وجود دارد. اگر در مراحل تعمیر دیسک فردی غیر مجاز به اطلاعات حساس یا محرمانه موجود روی آن پی ببرد یا این اطلاعات به نحوی افشاء شوند محاسبه زیان ناشی از وقوع این حالت به طبع آن محاسبه ریسک مربوط بسیار دشور خواهد بود.

بنابراین مشاهده می شود سناریوهای مختلفی قابل پیش بینی و بررسی است. هرچه تعداد این سناریوها در مرحله طراحی مکانیزم هـای امن سازی(و یا اصولاً طراحی سیستم)بیشتر باشد کارآیی روش های امن سازی که براساس آنها انتخاب می شوند بیشتر و به دنبـال آن ریسک ناشی از بکارگیری سیستم کمتر خواهد بود.

تهدید و محاسبه ریسک براساس آن

تهدید عبارت است از وضعیتی که در صورت وقوع آن یک عامل (عامل تهدید)می تواند از یک وضعیت بنیادی یا ناشی از روش بهـره برداری یک موجودیت(آسیب پذیری)سو استفاده کرده و بر آن تأثیر سوء گذارد.

به عنوان مثال قابل حمل بودن نوت بوک یک آسیب پذیری برای آن محسوب می شود و رها کردن نوت بوک بـدون مراقـب موجـب بروز تهدید سرقت آن می شود. به عبارت دیگر نوت بوک بدون مراقب همیشه در معرض تهدید سرقت است. عامل تهدیـد در اینجـا همیشه یک انسان است که می تواند از عناصر وابسته به سیستم (عامل تهدید داخلی) و یا عناصر بیگانه(عامل تهدید خارجی) باشد.

اگر بخواهیم عامل تهدید را در فرمول محاسبه ریسک دارد کنیم از فرمول زیر استفاده می شود:

$$R=V\times T\times F$$

که پارامترهای موجود در آن عبارتند از :

R : ریسک

T : شدت تهدید

F : دفعات وقوع شرایط تهدید آمیز

V: ارزش موجودیت

در فرمول فوق مقدار احتمال در پارامترهای T و F نهفته است به عبارت دیگر T برآوردی از شدت تهدید امنیت که ممکن است موجودیت تحت مطالعه را تحت تأثیر قرار دهد و F نیز برآورد تعداد دفعات وقوع شرایط تهدید آمیز در طول یک دوره زمانی مشخص می باشد.

فرمول اخیر کاربرد بیشتری در ارزیابی ریسک دارد زیرا استخراج مقادیرL_Sو P_S که در فرمول قبلی به کار می روند با دشواری های بسیار همراه است. استخراج مقادری مورد استفاده در فرمول اخیر ساده تر است زیرا:

مقدار V (ارزش موجودیت)را می توان از طریق استخراج ارزش دفتری دارایی(درخصوص دارایی های خریداری شده) و یا محاسبه مقدار هزینه صرف شده برای کسب آن موجودیت(مثل حقوق پرداخت شده به پرسنل برای جمع آوری یا تولید داده های یک بانک اطلاعاتی یا کسب اعتبار در حوزه ایی خاص) محاسبه کرد.

مقدار T (شدت تهدید) را می توان با استفاده از معیارهای کیفی(مثل بسیار پرشدت، پرشدت، شدید و کم شدت) و تبدیل آن به شاخص های کمی با استفاده از جدول ارزش گذاری(مانند نمونه زیر) تعیین نمود.

T : شدت تهدید

معیارکیفی	شاخص کمی
بسیار پرشدت	۱۶
پرشدت	۴
شدید	۲
کم شدت	۱

مقدارF از طریق کنترل سوابق سازمانی یا کسب نظر افراد خبره قابل استخراج است. مثلاً اگر حادثه ای یک بار در سال احتمال وقوع داشته باشد به آن مقدار ۱ و یا اگر هرماه احتمال وقوع داشته باشد به مقدار آن ۱۲ تخصیص داده می شود.

برای سادگی می توان مقادیر V (ارزش موجودیت) را نیز دسته بندی کرده و براساس دسته بندی های مرتب(مثل بسیار پرارزش، پرارزش، کم ارزش) به آن شاخص های متناسب(مانند جدول زیر) تخصیص داد.

ارزش دارایی

ارزش ریالی	معیار کیفی	شاخص ارزش
بیش از ۲۰/۰۰۰/۰۰۰ ریال	بسیار پر ارزش	۹
کمتر از۲۰/۰۰۰/۰۰۰ و بیش از ۵۰۰/۰۰۰ریال	پر ارزش	۳
تا ۵۰۰/۰۰۰ ریال	کم ارزش	۱

ممکن است به نظر برسد با فرمول بندی و دسته بندی های فوق ارزیابی ریسک به کاری ساده تبدیل شده است.

دشواری های محاسبه ریسک امنیت اطلاعات

محاسبه ریسک امنیت اطلاعات برای استخراج شاخص ریسک امنیت اطلاعات انجام می شود. شاخص ریسک امنیت اطلاعات یک سیستم عبارت است مجموع مقادیر ریسک محاسبه شده برای کلیه اجزای آن سیستم .

اجزای یک سیستم عبارتند از:

- داده ها
- نرم افزارها
- سخت افزارها
- زیرساخت های شبکه(فیزیکی و منطقی)

- تجهیزات و تسهیلات پشتیبانی(برق اضطراری، تهویه، تخلیه شارژرهای اضافی الکتریکی، مقابله با حوادث)
- منابع انسانی
- فرآیندها و روش های اجرایی ارائه خدمات اطلاعاتی ـ ارتباطی

برای محاسبه ریسک یک سیستم اطلاعاتی باید ریسک تک تک اجزای به کار گرفته شده در آن به تفکیک حالت هایی که ممکن است برای هر جزء حادث شود، محاسبه گردد. برای این کار لازم است آسیب پذیری های کلیه اجزاء شناسایی شده و شرایطی که ممکن است باعث سوء استفاده از آسیب پذیری ها شود(تهدید ها) استخراج شوند، همچنین لازم است توسط دفعات وقوع آن شرایط (احتمال وقوع) برآورد شود. نکته دیگری که نباید از آن غافل شد بروز شرایط تشدید آسیب پذیری یا تهدیدات ترکیبی است. به عنوان مثال اتصال رایانه حاوی اطلاعات محرمانه رمزنگاری نشده به اینترنت می تواند موجب تشدید آسیب پذیری شود. در این حالت تهدید افشای اطلاعات از طریق دسترسی با تهدید افشاء از طریق دسترسی راه دور ترکیب شده و سیستم را در مقابل نقض محرمانگی به شدت آسیب پذیر می نماید.

سیال بودن مرز بین نرم افزار و سخت افزار در تجهیزات رایانه ایی یکی دیگر از عوامل تشدید دشواری ارزیابی ریسک است. در سیستم های پیچیده تعریف مرزی دقیق بین برنامه کاربردی، ابزارهای سیستم، سیستم عامل و نرم افزارهای نهفته و آن بخش از منطق کار که بین سخت افزار و نرم افزار توزیع شده است، دشوار است. همچنین ارزش گذاری دقیق داده ها و اطلاعاتی که در طول زمان بدست آمده و یا زیان ناشی از فقدان آن ها درحین پردازش(به دلیل نقص نرم افزاری یا سخت افزاری) تقریباً غیر ممکن است.

از طرف دیگر شاخص ریسک هر سیستم اطلاعاتی شاخص یکتا است که باهیچ شاخص دیگری بجز شاخص هایی که در زمان های مختلف در مورد همان سیستم محاسبه شده اند قابل مقایسه نیست. به عبارت دیگر نمی توان شاخص ریسک سیستم اطلاعاتی به کار گرفته شده در یک سازمان را با شاخص ریسک سیستم اطلاعاتی به کارگرفته شده در سازمانی دیگر را (حتی اگر اجزای آن کاملاً مشابه باشند) مقایسه نمود.

نیاز به تکرار پذیری روش ارزیابی ریسک یکی دیگر از دشواری های ارزیابی ریسک(در کلیه سیستم ها) است.

روش بکار گرفته شده برای ارزیابی ریسک باید به نحوی باشد که تکرار آن توسط افراد مختلف منجر به تولید پاسخ های یکسان شود. به عبارت دیگرلازم است معیارهای قابل اندازه گیری در ارزیابی ریسک(به عنوان مثال مقادیر T، V و F)بـه قـدری دقیـق تعریـف شوند که اولاً تفسیر ناپذیر باشندو ثانیاً به آسانی بتوان مقدار آنها را برای هر موجودیت با دقت بسیار زیاد تخمین زد.

یکی دیگر از دشواری های تحلیل ریسک تناسب روش ارزش گذاری موجودیت ها و برآورد تهدیدها با ماهیت و نوع عملکرد سازمان می باشد. بدیهی است در یک سازمان کوچک که در محدوده خاصی فعالیت می نماید نیازی به اختصاص انـواع و اقسـام تهدیـدهای موجود در حوزه فناوری های اطلاعاتی نمی باشد اما در سازمان های بزرگ که به ارائه خدمات در حوزه هـای کشـوری یـا مـؤثر بـر امنیت ملی می پردازند لازم است تحلیل (ارزیابی)ریسک باسخت گیری کامل انجام شده و بدبینانه ترین فرض ها درخصوص آسـیب پذیری ها و عوامل تهدید از نظر دور نگهداشته نشود. تشخیص نوع سازمان و درجه ایی از دقـت کـه تحلیـل(ارزیـابی) ریسـک بایـد براساس آن انجام شود کاری مشکل است و باید توسط افراد کاملاً خبره انجام شود.

مرجع : جزوه ارزیابی ریسک امنیت فناوری اطلاعات (از مجموعه کتب دستورالعمل های ISMS) – آقای مهندس میرمعینی

من ا... التوفیق

علی ثاقب موفق – فوق لیسانس فناوری اطلاعات