امنیت اطلاعات

محافظت کردن در جهت توانمندسازی

مدیریت ریسک و امنیت اطلاعات به روایت
مدیر ارشد امنیت اطلاعات شرکت اینتل

مالکوم هارکینس

برگردان
سعید شمسیان
محمدعلی عظیمی

NAGHOOS PUBLICATION

مرکز پخش: انتشارات ناقوس
میدان انقلاب، خیابان کارگر شمالی، خیابان ۱۲فروردین، بین وحید نظری و روانمهر، بن‌بست حقیقت،
پلاک۴ تلفن و فکس: ۵۸ و۶۶۴۷۸۹۵۷ پیامک: ۳۰۰۰۰۴۵۲۳۲۳ www.naghoospress.ir

سرشناسه : هارکینس، مالکوم Harkins, Malcolm
عنوان و پدیدآورنده : امنیت اطلاعات: محافظت کردن در جهت توانمندسازی مدیریت ریسک و امنیت اطلاعات به روایت مدیر ارشد امنیت اطلاعات شرکت اینتل/ مالکوم هارکینس؛ برگردان سعید شمسیان، محمد علی عظیمی.
مشخصات نشر : تهران: ناقوس، ۱۳۹۵.
مشخصات ظاهری : XI، ۱۶۸ص.: مصور، جدول.
شابک : 978-964-377-846-0
وضعیت فهرست‌نویسی : فیپا
یادداشت : عنوان اصلی: Managing Risk and Information Security ,c2013
عنوان دیگر : محافظت کردن در جهت توانمندسازی مدیریت ریسک و امنیت اطلاعات به روایت مدیر ارشد امنیت اطلاعات شرکت اینتل
موضوع : کامپیوترها-- ایمنی اطلاعات
موضوع : منابع اطلاعاتی الکترونیکی-- کنترل دستیابی
شناسه افزوده : شمسیان، سعید، ۱۳۶۸-، مترجم
شناسه افزوده : عظیمی، محمدعلی،۱۳۶۱-، مترجم
رده‌بندی کنگره : ۱۳۹۵ ۲هـ ۹ QA۷۶
رده‌بندی دیویی : ۰۰۵/۸
شماره کتابخانه ملی : ۴۲۰۰۶۹۲

نام کتاب: امنیت اطلاعات: محافظت کردن در جهت توانمندسازی
نویسنده: مالکوم هارکینس
مترجمان: سعید شمسیان، محمدعلی عظیمی
ویرایش فنی و ادبی: علی حسینی، مهری تقی‌پور (موسسه فرهنگی، هنری سنجاقک سرزمین پارس)
طراحی جلد و صفحه‌آرایی: الهه رحیمی توانا (دپارتمان گرافیک موسسه فرهنگی، هنری سنجاقک سرزمین پارس)
لیتوگرافی: نوین
چاپ و صحافی: کهنمویی
نوبت چاپ: نخست، بهار ۱۳۹۵
شمارگان: ۱۰۰۰ نسخه
بها: ۱۵۰۰۰۰ ریال

فهرست

مقدمه مترجمان

این کتاب تجربه‌نگاری‌های مالکوم هارکینس، مدیر ارشد امنیت اطلاعات اینتل و تیم او است که در حیطه مدیریت ریسک و امنیت اطلاعات، دانش تجربی ارزشمندی را به خوانندگان منتقل می‌کند. به‌اشتراک‌گذاری این دانش و تجربه، به‌ویژه از سوی مدیر ارشد امنیت اطلاعات یکی از بزرگ‌ترین شرکت‌های حوزه فناوری، هم از حیث علمی و هم اخلاقی، کار ارزشمند و قابل تقدیری است که به قول سعدی:

کنونت که امکان گفتار هست — بگو ای برادر به لطف و نکوئی
که فردا چو پیک اجل در رسید — به حکم ضرورت زبان در کشی

تجربه و دانش تجربی یا همان پیاده‌سازی اصول و قواعدی که در کتاب‌ها و متون آکادمیک آورده شده است، برای افرادی که می‌خواهند همان راه را دوباره طی کنند بسیار حائز اهمیت است. مالکوم هارکینس و تیم او پیاده‌سازی سیاست‌های امنیتی را در اینتل آزموده‌اند، نکات را ارزیابی و نقاط قوت و تأثیرهای پیموده شده را استخراج کرده‌اند و حاصل آن، به‌صورت سندی ارزشمند و جامع گردآوری شده است که خواندنش به علاقه‌مندان مقوله امنیت توصیه می‌شود؛ چه آن‌که سعدی، شیخ اجل، در مدح تجربه، می‌فرماید:

مرد خردمند هنرپیشه را — عمر دو بایست در این روزگار
تا به یکی تجربه آموختن — با دگری تجربه بردن به کار

اما صد حیف که تنها یک بار می‌توان زندگی کرد. پس باید از تجارب ارزشمند دیگران استفاده کنیم تا خطاهای احتمالی به حداقل کاهش یابد.

کتاب پیش رو با حساسیت فراوان مترجمان در تمام مراحل آماده‌سازی شکل گرفته است. بسیار روان به رشته تحریر درآمده است و تلاش کرده‌ایم از لغات نامانوس و خودساخته استفاده نکنیم و تا حد امکان

از لغات و ترکیباتی بهره ببریم که در زبان فارسی رایج‌تر هستند تا خوانندگان بتوانند بدون دغدغه کتاب را مطالعه کنند. در این اثنا سعی کردیم به متن اصلی امانتدار باشیم، ولی در مواردی اضافه یا حذف ترکیباتی از متن اصلی میزان تأثیرپذیری آن را دو چندان می‌کرد که پس از بازخوانی‌های مکرر این کار را انجام دادیم.

چندباره خوانی‌ها و گاهی بحث‌های جدی بر سر انتخاب یک ترکیب از میان ترکیب‌های موجود، به ما نشان داد که همیشه ترکیب بهتری هم وجود دارد. بنابراین، مدعی بهترین ترجمه ممکن از کتاب مذکور نیستیم، ولی تمام تلاش‌مان را برای تولید محتوایی فاخر و ماندگار انجام داده‌ایم.

امید است این اثر گامی هر چند کوچک در ارتقاء سطح دانش امنیت سایبری کشور باشد و مورد رضایت صاحب‌نظران قرار گیرد. هم‌چنین از شما خوانندگان گرامی هم صمیمانه خواستاریم اگر در جهت هر چه بهتر شدن کتاب انتقاد، پیشنهاد یا دیدگاهی دارید با ما درمیان بگذارید.

این کتاب برای مدیران ارشد امنیت اطلاعات سازمان‌ها، مدیران فناوری اطلاعات مراکز، مدیران ریسک امنیت، مشاوران امنیتی در تمام سطوح، مدیران امنیت اطلاعات، تحلیل‌گران، پژوهش‌گران، متخصصان، کارشناسان حرفه‌ای‌های امنیت اطلاعات، استادان و مدرسان امنیت و دانشجویان امنیت مناسب است و مطالعه آن به همه علاقه‌مندان توصیه می‌شود.

در پایان، لازم می‌دانیم از مهندس مسعود راستکار، مهندس پرهام ایزدپناه مدیرعامل محترم مؤسسه سنجاقک سرزمین پارسه و همچنین جناب آقای تجملی مدیریت محترم انتشارات ناقوس و تمام عزیزانی که با رهنمودها و ایده‌هایشان ما را در تهیه این کتاب یاری کرده‌اند، کمال تشکر و قدردانی را داشته باشیم.

سعید شمسیان[1]، محمدعلی عظیمی[2]

بهار ۱۳۹۵

1. shamsian@rayana.ir
2. info@jazanet.edu.ir

پیش‌گفتار

آن دسته از مدیران ارشد امنیت اطلاعات که به‌تازگی قدم به این حیطه نهاده‌اند، زود درمی‌یابند وسعت جایگاهی که آن‌ها تصدی کرده‌اند، اغلب بیش از چیزی است که خود را برای آن آماده کرده بودند. سرشت کار امن‌سازی یک سازمان، بیم‌آور و کلافه‌کننده است. برای موفقیت در این حیطه، هیچ چک‌لیست یا نقشه راهی وجود ندارد. بسیاری از مهارت‌های فنی امنیتی که یک مدیر ارشد امنیت اطلاعات در مراحل نخست حرفه خود کسب کرده است، شاید برای او نوعی «حس ششم» یا مهارت درون‌یابی به ارمغان آورد، اما تخصص فنی به تنهایی مدیر ارشد امنیت اطلاعات را برای مقابله با چالش‌های مدیریتی و رهبری که لازمه موفقیت است، آماده نمی‌کند.

اثر دانینگ ـ کروگر[1] «یک‌جور جانب‌داری آگاهانه است که در آن اشخاص غیرماهر از برتری خیالی رنج می‌برند و به اشتباه توانمندی خود را بسیار بیش از حد متوسط برآورد می‌کنند» (به نقل از ویکی‌پدیا). مدیران ارشد موفق امنیت اطلاعات عموماً نادانسته‌های خود را درمی‌یابند و می‌پذیرند. من در حرفه خود با خبره‌های ارشد زیادی در حیطه امنیت دیدار داشته‌ام و متوجه شده‌ام آن‌ها که موفق هستند مجموعه ویژگی‌های مشترکی دارند. آن‌ها عموماً حس کنجکاوی زیاد، توانایی خودآگاهی و «بد اندیشیدن» (برای این‌که بدانند دشمن چگونه می‌اندیشد) را از خود بروز می‌دهند و ارتباطات آن‌ها قوی است و وقتی اطلاعات جدیدی ارائه می‌شود، در اندیشیدن و موقعیت‌ها سازگار و تطابق‌پذیر هستند. آن‌ها مهارت‌های رهبری خود را گسترش می‌دهند و ساختارهایی را پدید می‌آورند که به ایجاد تعادل کمک می‌کند. آن‌ها علاوه بر این، استعدادها را تشخیص می‌دهند و خود را به محاصره تیم‌هایی درمی‌آورند که از تکنولوژیست‌های توانمند امنیتی و به

1. Dunning-Kruger Effect

عبارت دیگر، متخصصان واقعی، تشکیل شده‌اند.

رهبران زبده امنیت آموخته‌اند که ریسک سیاه و سفید نیست و باید تعادل برقرار شود. آن‌ها صریح و خوش‌برخورد هستند. دوست من مالکوم همه این معیارها را دارد.

او در کتاب «مدیریت ریسک و امنیت اطلاعات: محافظت کردن در جهت توانمندسازی»، دانش صعب‌الحصول خود را که در دوران حرفه‌ای‌اش به‌عنوان رهبر تجاری و امنیتی فراگرفته است در چهارچوبی فشرده خلاصه می‌کند، به‌گونه‌ای که مدیران ارشد امنیت اطلاعات را قادر می‌کند از آشفتگی‌های مرتبط با امن‌سازی سازمان به سلامت عبور کنند. درس‌های این کتاب را فرا بگیرید و با تداوم بررسی و نوآوری، آن را غنی کنید. تهدیدها، تغییرهای مداوم سازمانی و فناوری‌ها همواره در حال تکامل و دگرگونی هستند و ما در مقام خبره‌های امنیت باید درس‌های خلاصه شده در این‌جا را به کار بگیریم و خود را به‌طور مداوم با چالش‌ها هم‌گام کنیم.

پاتریک هایم[1]

مدیر ارشد اعتمادبخشی[2] **شرکت سیلزفورس**[3]

1 Patrick Heim
2 Chief Trust Officer
3 Salesforce.com, Inc

درباره نویسنده

مالکوم هارکینس[1]، نایب رییس گروه فناوری اطلاعات، مدیر ارشد امنیت اطلاعات و مدیر کل ریسک و امنیت اطلاعات اینتل است. این گروه مسئول مدیریت ریسک، کنترل‌ها، حریم خصوصی، امنیت و دیگر فعالیت‌های تطبیقی مرتبط برای همه دارایی‌های اطلاعاتی اینتل است. هارکینس پیش از تصدی پست مدیریت ارشد امنیت اطلاعات اینتل، در بخش مالی اینتل فراهم‌آوری و عملیات نیز ایفای نقش کرده است. او تلاش‌ها برای محک‌زنی فناوری اطلاعات و تطابق‌پذیری سیستم‌ها با قانون ساربنز ـ آکسلی را مدیریت کرده است. هارکینس پیش از آغاز به کار در بخش فناوری اطلاعات، مدیر سود و زیان گروه محصولات فلش اینتل و نیز مدیرکل قابلیت‌های سازمانی و مسئول ارائه و پشتیبانی سیستم‌های مالی و منابع انسانی اینتل بود. همچنین، در یکی از دادوستدهای تجاری مخاطره‌پذیر اینتل متمرکز بر خدمات زبانی تجارت الکترونیک نیز ایفای نقش کرده است.

هارکینس در گذشته در مؤسسه CIO در دانشکده بازرگانی آندرسون[2] دانشگاه کالیفرنیا، لس‌آنجلس، تدریس کرده است و در سال ۲۰۰۹ استاد مدعو دانشگاه ساسکوهنا[3] بود. او در سال ۲۰۱۰ در کنفرانس RSA جایزه عالی حیطه امنیت را دریافت کرد. مجله کامپیوتر ورلد[4] نیز او را در فهرست صد رهبر برتر فناوری اطلاعات در سال ۲۰۱۲ جای داد. به‌علاوه، کنسرسیوم بین‌المللی[5] صدور گواهی‌نامه امنیتی سامانه‌های اطلاعاتی موسوم به (ISC)2 در سال ۲۰۱۲ با اعطای جایزه رهبری امنیت اطلاعات از او تقدیر کرد.

هارکینس درجه کارشناسی خود در رشته اقتصاد را از دانشگاه کالیفرنیا در ارواین[6] و مدرک مدیریت ارشد کسب‌وکار در رشته علوم مالی و حسابداری را از دانشگاه کالیفرنیا در دیویس[7] دریافت کرد.

1. Malcolm Harkins
2. Anderson School of Business
3. Susquehanna University
4. Computerworld
5. University of California Irvine
6. Master of Business Administration در Uni
7. University of California at Davis

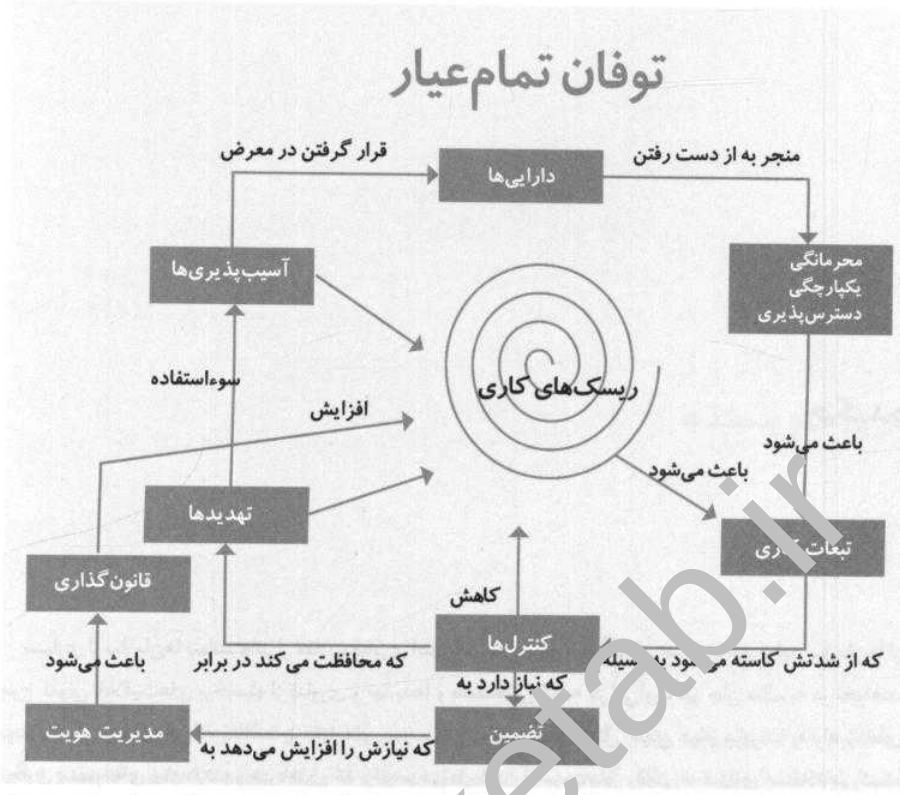
چکیده

بسیاری از سازمان‌ها نتوانسته‌اند از انقلاب فناوری اطلاعات جان سالم به در ببرند. تعداد زیادی از این سازمان‌ها از موج کنونی خلاقیت‌های برخاسته از فناوری و تهدیدها و ضعف‌هایی که به بار می‌آورد نیز جان سالم به در نخواهند برد. سازمان‌ها برای این‌که بتوانند در بازارهای پیچیده و بسیار به‌هم متصل جهان دوام بیاورند، به راهبردهای تجاری متهورانه‌ای نیاز دارند؛ راهبردهایی که برای برخوردار شدن از مزیت‌های رقابتی از فناوری استفاده می‌کنند. تیم‌های ریسک و امنیت اطلاعات در سازمان‌ها و جمع‌های کلان، هم می‌توانند این راهبردها را با مانع مواجه و هم به پیش‌برد آن کمک کنند. مدیریت مؤثر ریسک و امنیت اطلاعات، بدون ممانعت از حرکت سریع سازمان، کلید تداوم کسب‌وکار خواهد بود. از همین رو است که من سه سال پیش مأموریت گروه ریسک و امنیت اطلاعات شرکت اینتل را به «محافظت کردن در جهت توانمندسازی» تغییر دادم. همچنین مشغول نوشتن این کتاب شدم.

در ژانویه ۲۰۰۲، برای اجرای برنامه‌ای موسوم به امنیت و تداوم تجسم کار استخدام شدم. این برنامه پس از حوادث ۱۱ سپتامبر و ویروس‌های کد قرمز/نیمدا[1] در خلال تابستان سال ۲۰۰۱ پدید آمد. این برنامه در اصل بر نگرانی‌های مرتبط با ریسک‌های دسترسی در آن زمان تمرکز داشت. من در حیطه امنیت سابقه فنی نداشتم. حدود ده سال در موقعیت‌های مختلف کاری که تقریباً بیشترشان در حیطه مالی بود، با اینتل کار کرده بودم. در همان چند ماه نخست که مشغول فراگیری بودم برایم آشکار شد که جهان دگرگونی جدیدی را آغاز کرده و «توفانی تمام‌عیار» در حال شکل‌گیری است. این موضوع را با کنار هم نهادن شکل ۱ با مدیر خود، مدیر ارشد فناوری اطلاعات و هر شخص دیگری که به من گوش بسپارد توضیح می‌دهم. از آن‌جا که درباره تهدیدهای مرتبط با دسترسی همه تلاش‌مان را صورت دادیم.

در فوریه ۲۰۰۴ از این برنامه جدا شدم. من جدا شدم تا کارهای مربوط به هماهنگ کردن سازوکارهای سیستم‌مان با مصوبه ساربنز ـ آکسلی[2] را پیش ببرم (قانون اصلاح حسابداری شرکت‌های سهامی عام و محافظت از سرمایه‌گذار). سابقه کاری من در حیطه‌های مالی، نقش‌های گوناگون کاری که قبلاً عهده‌دارشان بودم و سال‌های زیادی که حول مبحث فناوری اطلاعات گذرانده بودم و نیز کارهایی که در سال‌های ۲۰۰۲ و ۲۰۰۳ رهبری کردم،

1 Code Red/Nimda
2 Sarbanes-Oxley Act (SOX)



موقعیت کاری اخیر را به گزینه‌ای کاملاً م[illegible] سال می مبدل کرد. اما چیز دیگری هم ذهنم را به خود مشغول کرده و آن همین تصویر بود. آن‌چه فکرم را به خود مشغول کرده بود، ترس از ریسک‌هایی نبود که شاید اتفاق می‌افتادند، بلکه حس کنجکاوی و عطش دانستن این بود که چگونه باید این توفان تهدیدها را کنترل کرد. پس در سال ۲۰۰۵، همین که تلاش‌های اولیه ما در ارتباط با مصوبه [illegible] کامل شد، به حیطه امنیت اطلاعات بازگشتم، اما این بار با انگیزه و آرزو برای تلاش در جهت پیوند دادن همه عناصر اصلی سازوکارهای ریسک، امنیت و کنترل اطلاعات با هم تا بتوان با مارپیچ تهدید مقابله کرد. از این رو، در [illegible] گذشته، درباره همین موضوع پژوهش کرده‌ام.

در این کتاب، مطالب بسیاری را که در یازده سال مدیریت جنبه‌های گوناگون ریسک و [illegible] اطلاعات در اینتل فرا گرفتم، پوشش خواهم داد. همچنین، شیوه‌های تفکر درباره ریسک و شیوه‌های نگرش به فرایند حاکمیت را به‌اشتراک خواهم گذاشت. من مشارکت‌های داخلی و خارجی را برای به‌اشتراک‌گذاری اطلاعات و همکاری درباره آن‌ها بررسی خواهم کرد که این اقدامات می‌توانند تعیین‌کننده باشند. نمونه‌هایی از چیزهایی را که ما در اینتل انجام دادیم و چیزهایی را که می‌خواهیم انجام دهیم تا تهدیدهای‌مان را بهتر مدیریت و کاربران آی‌تی خود را توانمندتر کنیم، به‌اشتراک خواهم گذاشت. سرانجام، به آینده نگاه خواهم کرد و نیز دورنمای خود درباره مهارت‌های مورد نیاز مدیران ارشد امنیت اطلاعات در قرن بیست و یکم را با شما سهیم خواهم شد.

مدیریت ریسک و امنیت اطلاعات؛ محافظت کردن در جهت توانمندسازی یک کنکاش است، اما خط پایانی ندارد. رویکرد ما در مدیریت ریسک اطلاعات باید با همان سرعتی تکامل یابد که کسب‌وکارها و فناوری تغییر می‌کند. امید دارم که مردم این کتاب را بخوانند و کنکاش شخصی خود را آغاز کنند.