نام کتاب

شناسنامه

فهرست مطالب

مقدمه ناشر

تقدیروتشکر

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت های او ندانند و کوشندگان، حق او را گزاردن نتوانند. و سلام و دورد بر محمّد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز...

تقدیم به

پدر و مادر عزیز و مهربانم

که در سختی‌ها و دشواری‌های زندگی همواره یاوری دلسوز و فداکار و پشتیبانی محکم و مطمئن برایم بوده‌اند.

با تشکر و سپاس از استاد دانشمند و پر مایه ام جناب آقای **عادل کریمی** که از محضر پر فیض ایشان ، بهره ها برده ام.

پیشگفتار

کتابی که در حال حاضر پیش روی شماست بیانگر راهکارهـای پیـاده سـازی و مـدیریت شکار تهدید سایبری می باشد. در این کتاب سعی شده اسـت تـا مباحـث مـدیریتی کـه برای راه اندازی شکار تهدید در سازمان مورد نیاز است بصورت عملی ارائه گردد.

هدف ما در این کتاب برطرف کـردن سـوءتفاهمات در مـورد ماموریـت شـکار و ارائـه ی توصیه هایی برای ساختاربندی تیم شکار و بینش عملی بـرای اسـتفاده از تکنیـک هـای شکار می باشد که با استفاده از یک استراتژی مبتنی بر حملـه، سـازمان هـا مـی تواننـد کنترل شبکه های خود را به دست بگیرند و از دارایی هـای بسـیار مهـم خـود محافظـت کنند.

شایان ذکر است در ترجمه این کتاب از منابعی همچـون مقـالات شـرکت Endgame، Sqrrl، FireEye، Red Canary استفاده شده اسـت، لازم بـه ذکـر اسـت در برخـی بخش ها توضیحات بیشتر لحاظ کرده یا از جملات و کلمات دیگری برای ارائـه مفهمـوم مورد نظر به شخص خواننده استفاده کـرده ام، تـا بتـوانم حـداکثر مطالـب کتـاب را بـه شخص خواننده منتقل کنم. با این حال مجموعه حاضر خالی از اشکال نمی باشد. لـذا از تمام اساتید ارجمنـد، صـاحب نظـران و دانشـجویان محتـرم اسـتدعا دارم بـا نظـرات و پیشنهادات خودشان من را راهنما باشند.

محمد قنبری

www.linkedin.com/in/mghanbari7

mghanbari777@gmail.com

مقدمه مولف

صرف نظر از بخش صنعتی، سازمان ها در سراسر جهان یک چالش مشترک را به اشتراک می گذارند: یافتن یک روش موثر برای شناسایی و اقدام سریع علیه تهدیدات سایبری. با در نظر گرفتن " dwell time" متوسط 150 روز، مهاجمین زمان زیادی برای برنامه ریزی و انجام سرقت مالکیت معنوی، اطلاعات مشتری و سایر اطلاعات ارزشمند دارند. به علاوه، با دسترسی آسان و ارزان به ابزارهای پیشرفته ی هک و سرویس های "اجاره یک هکر" از طریق دارک وب، مهاجمین هرساله نوع و تعداد حملات را افزایش داده اند. برای سخت تر کردن موفقیت مهاجمین نیاز داریم که از راه حل ها و تکنولوژی های جدید برای مقاوم سازی سازمان ها و دارایی های خود استفاده کنیم.

ابزارهای تشخیص حملات موجود در طول زمان ازکار افتاده به نظر می رسند. آن ها برای این که کشف کنند چه اتفاقی افتاده است، از روش های Big Data کلاسیک مانند کشف یا جستجو در مجموعه ای از داده ها مانند (لاگ ها و ...) گذشته استفاده می کنند. زمانی که یک حمله موفقیت آمیز کشف می شود، آن ها قوانینی برای هدایت کشف وقوع حملات مشابه بعدی وضع می کنند. هدف این کار یادگیری از گذشته و پشتیبانی در برابر تلاش های آینده است. فقط یک مشکل وجود دارد: این که احتمالا حملات بعدی متفاوت است.

سال ها است که ما (گروه های امنیتی) به خوبی با دشمنانی که به سیستم های سازمان ما حمله می کنند مبارزه کرده ایم. ما برای سیستم عامل ها و برنامه های کاربردی خود در سریع ترین زمان

ممکن وصله هایی را مورد استفاده قرار داده ایم. ما به آنتی ویروس ها، فایروال ها، سیستم های جلوگیری از نفوذ (IPS) و سایر ابزارها برای ممانعت از حمله متکی هستیم.

زمان آن است که بپذیریم رویکردهای متداول برای امنیت سازمان کافی نمی باشد. ما نیاز داریم که یک قدم به عقب بازگردیم و در فرضیات خود تجدید نظر کنیم. به جای آن که تمام تمرکزمان را بر روی امنیت reactive بگذاریم و برای یک هشدار منتظر بمانیم، باید یک رویکرد proactive برای امنیت استفاده کنیم و تلاش کنیم آن ها را پیدا کنیم و به سرعت از محیط خود حذف کنیم.

این به این معنی نیست که کنترل های امنیتی موجود را از بین ببریم، پیشگیری هنوز هم بسیار اهمیت دارد. اما به این معنی است که به منظور تشخیص دشمنان یا مهاجمین و حذف آن ها از شبکه هایمان باید بسیار بیشتر فعال بود. بهترین روش برای تغییر موقعیت از reactive به proactive، شکار می باشد که که هدف این کتاب است.

من هر روزه در مورد شکار تهدید با سازمان ها صحبت می کنم. بعضی تصور می کنند که شکار تهدید استفاده از شاخص های شناخته شده ی آلودگی[1] یا IoC از فیدهای هوش تهدید[2] و جستجوی آن ها می باشد. اما با این حال خوب است که بدانید آیا نسبت به حملات کشف شده ی پیشین حساس هستید یا نه، این مانند این است که در حین رانندگی تنها به آینه ی عقب نگاه کنید.

همه ی ما می دانیم که حوادث سایبری اجتناب ناپذیر هستند. حال با این دانش چگونه عمل می کنیم؟ برای متوقف کردن یک نفوذ چگونه می توانیم متفاوت عمل کنیم؟ این صنعت نیازمند روش جدیدی است که به اندازه ی این تهدیدات و محیط سازمان ها پویا باشد. سازمان ها به دنبال روش هایی هستند که با تشخیص و مسدود کردن دشمنان پیش از وقوع آسیب، از رویداد های ناگوار و سانحه جلوگیری کنند. نگاه به آینه ی عقب و واکنش پس از اتفاق دیگر کافی نیست. متاسفانه راه حل

1 compromise
2 threat intelligence feed

های امنیتی به سرعت دشمنان و مهاجمین پیشرفت نکرده است. با این کـه تکنولـوژی در زمـان گیـر افتاده است، صنعت با به کاربردن نام های جدید برای راه حل های منسوخ و آراستن اصطلاحات علمی ادامه می دهد.

شکار اغلب با قابلیت های جستجوی شاخص یا طبقه بندی *لاگ* های غنی شده اشتباه گرفته می شود ولی این تشخیص و حذف به صورت proactive، پنهانی و دقیق دشمنان و مهاجمین در شبکه بـدون وجود شاخص های شناخته شده ی آلودگی می باشد. شکار یک استراتژی مبتنی بر حملـه مـی باشـد؛ شکارچی مانند مهاجم فکر می کند. اگر شما مهاجم بودید، چه چیز را با چـه هـدفی و چگونـه مـورد حمله قرار می دادید؟ مهاجمین یک ماموریت دارند. شکار باید بتواند ایـن ماموریـت را از مسـیر خـارج سازد.

شکار تهدید نسبتا یک تخصص جدید به شمار می آید. با این وجود که خود این فعالیت جدید نیسـت، اما ابزارهای مخصوص شکار تهدید، مدل ها و بهترین روش ها در طی سال های اخیر توسعه یافته انـد. اغلب ابهاماتی در مورد حوزه های این فعالیت وجـود دارد همـانطور کـه در مـورد تمـامی حـوزه هـای تحقیقی جدید این ابهامات به وجود می آید. همانطور که رویکردهای متعارفی در مورد چگونگی انجـام چنین فعالیت هایی وجود ندارد تعاریف خوبی نیز ارائه نشده است.

شکار می تواند تعادل را به نفع مدافعین تغییر دهد اما نیـاز دارد کـه از حالـت واکنشـی بـه ذهنیـت و نگرش مهاجمین تغییر کند. اگر شما دقیقا ندانید که کدام یک از روش های مهاجمین را مسدود کنیـد نمیتوانید آلوده سازی و نفوذ را متوقف کنید. اکثر دشمنان و مهاجمین بدون توجه بـا اهدافشـان بایـد توانایی دسترسی اولیه، تقویت امتیازات (escalate privileges)، سرقت credentialها، حرکـت در تمام دارایی ها، دور زدن استحکامات، تجهیزات دفاعی و پایداری[3]در شبکه ها را دارا باشـند. تشـخیص این ساختارها مولفه ی اصلی شکار است زیرا به شما می گوید که کجا شکار کنید. به جـای تمرکـز بـر

3 Persistence

گذشته مانند بدافزارها یا شاخص های آلودگی که قبلا کشف شده است، سازمان ها مـی تواننـد شـکار کنند و مانع تمام انواع تکنیک های مهاجمین شوند، بـه ایـن معنـی اسـت کـه مـی تواننـد در مقابـل تهدیدات ناشناخته به دفاع بپردازند. به علاوه، شکار سیستماتیک به سـازمان اجـازه مـی دهـد کـه بـه سادگی به جمع آوری و آنالیز اطلاعات صحیح موجود در دارایی بپردازد تا بتواند فعالیت های مشکوک و مخرب را پیدا کند.